Львівський державний університет внутрішніх справ

В. П. ЗАХАРОВ,
В. І. РУДЕШКО

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В XXI СТОЛІТТІ ТА ЇХ ВИКОРИСТАННЯ ПРАВООХОРОННИМИ ОРГАНАМИ

Посібник

Львів
2015

УДК 343.982.34
ББК 67.52
З-38

Рекомендовано до друку Вченою радою
Львівського державного університету внутрішніх справ
(протокол № 11 від 24 червня 2014 р.)

Р е ц е н з е н т и:
***В. Л. Ортинський**, доктор юридичних наук, професор,*
заслужений юрист України,
директор Навчально-наукового інституту права та психології
Національного університету «Львівська політехніка»,
генерал-лейтенант міліції у відставці;
***В. К. Грищук**, академік Академії наук вищої освіти України,*
член-кореспондент Національної академії правових наук України,
доктор юридичних наук, професор,
директор Інституту права, психології та економіки
Львівського державного університету внутрішніх справ

Захаров В. П., Рудешко В. І.
З-38 Біометричні технології в XXI столітті та їх використання правоохоронними органами: посібник. – 2-ге вид., доп. / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2015. – 492 с.

ISBN 978-617-511-169-7

Ознайомлює читачів із сучасним застосуванням біометричних технологій, дає уявлення про можливості використання досягнень біометрії у повсякденному житті, а також у діяльності правоохоронних органів.

Для слухачів спеціальних навчальних установ, працівників правоохоронних і силових структур, науковців і практиків, а також усіх тих, хто досліджує використання досягнень біометрії.

УДК 343.982.34
ББК 67.52

ISBN 978-617-511-169-7

З М І С Т

ПЕРЕДМОВА

Перше видання посібника «Використання біометричних технологій правоохоронними органами у XXI столітті» було видано у 2009 році. Тоді і тепер для написання посібника використовувалась інформація, що була отримана з відкритих джерел. Слід зазначити, що в Україні майже не має узагальнюючих публікацій щодо всього спектра використання сучасних досягнень біометричних технологій.

За п'ять років, які минули після першого видання посібника, в галузі біометричних технологій відбулися суттєві зміні, що пов'язані з широкомасштабним впровадженням біометрії у посякденне життя. Тепер ми безпосередньо стикаємось із біометрією у нашому житті – від отримання закордонного паспорта або візи до придбання сучасного гаджета з біометричним сканером.

Під час роботи над другим виданням посібника була опрацьована інформація із 628 першоджерел, причому порівняно з виданням 2009 року першоджерела зазнали оновлення приблизно на 44,9%, тобто до відомостей із 346 публікацій до 2010 року додались дані з 282 джерел, що були опубліковані за період із 2010 до квітня 2014 року. У новому виданні з'явилися три нових підрозділа: «Запровадженя систем контролю й управління доступом (СКУД) у провідних аеропортах світу», «Біометричні технології у мобільних пристроях» і «Використання біометричних технологій у виборчих системах світу». Поява нових підрозділів відображає ту увагу, яка приділялася цим напрямам біометрії у другому десятиріччі нашого століття.

У новому варіанті посібника є інша назва – «Біометричні технології в XXI столітті та їх використання правоохоронними органами». Назву було скориговано через те, що матеріали посібника відображають повний спектр застосування біометричних технологій у сучасному житті, а не тільки у діяльності правоохоронних органів світового співтовариства. У новому виданні розглянуті всі відомі на час написання сучасні напрями використання біометричних технологій. Але біометричні технології не перебувають у статичному положенні, вони невпинно розвиваються, причому нові застосування біометрики інколи відбуваються у зовсім неочікованому напрямі.

Так, наприклад, у квітні 2014 року з'явилася інформація, що американський уряд може виступити зі спеціальною законодавчою ініціативою, у разі ухвалення якої власники вогнепальної зброї у Сполучених Штатах Америки будуть змушені носити спеціальні біометричні браслети і модифікувати свою вогнепальну зброю так, щоб стріляти з неї міг тільки власник зброї після здійснення процедури аутентифікації за допомогою біометричного браслета. Але це ще не все. Американська влада для більш дієвого контролю над власним населенням планує під час переобладнання приватної зброї шляхом упровадження електронних обмежувачів і створення регіональних центрів спеціального електронного обладнання мати можливість блокування стрілянини з такої зброї на певній території, наприклад, у зоні введення надзвичайного положення[1].

[1] Правительство США хочет заставить всех владельцев огнестрельного оружия носить биометрические браслеты // Информатор. – 2014. – 21 апреля. [Электронный ресурс]. – Режим доступа: http://www.uintelligencer.org/...

Нині ціла низка нових методик біометричної ідентифікації або аутентифікації перебувають на ранніх стадіях розвитку, зокрема: швидкісна ДНК-ідентифікація, розпізнавання ходи та запаху тіла, ідентифікація за формою вуха, біометрія мозкових хвиль і навіть тестування солоності тіла.

Біометрія – це не сенсація сьогодення. Розробка сучасних біометричних технологій продовжується вже понад п'яти десятиліть, а розробка різноманітних стандартів і тестів дозволяє цим технологіям найефективніше сприяти розвитку та уніфікації різних систем безпеки.

Нині практичне використання біометричних методів ідентифікації та верифікації, якщо і не є одним із найголовніших шляхів розвитку інформаційних технологій, то становить доволі значну їх складову.

Технологіями біометричної ідентифікації та аутентифікації користуються сотні мільйонів людей на всіх континентах і в різних країнах світу. Значні проекти реалізуються й урядовими, й комерційними структурами. Застосування біометричних технологій є одним із найважливіших чинників, який визначає успішність і конкурентоспроможність будь-якого суб'єкта суспільного життя – чи приватної особи, компанії чи держави.

2001 року обсяг біометричного ринку в світі становив усього 300 млн доларів, а вже в 2006 році він зріс до 2 млрд доларів. За оцінкою Міжнародної біометричної групи «International Biometric Group» обсяг біометричного ринку в світі у 2009 році становив 3,4 млрд доларів США, у 2012 році – 7 млрд доларів, а в 2014 році має зрости до 9,4 млрд доларів. У квітні 2014 року експерти компанії «MarketsandMarkets» оприлюднили прогноз, згідно з яким обсяг глобального ринку в 2020 році може сягти 23,54 млрд доларів. Цей висновок є найоптимістичнішим з усіх відомих авторам посібника прогнозів, які були оприлюднені в ЗМІ на час підготовки до його другого видання. Загалом оцінки різних консалтингових компаній цього показника у 2020 році відрізняються, але всі вони показують невпинне зростання доходів від продажу біометричних систем.

Основною перевагою біометричних технологій (біометрії або біометрики) є можливість швидкої й простої ідентифікації або аутентифікації (верифікації) без спричинення якихось незручностей індивідуумові.

Нині біометричні системи є другим поколінням систем безпеки, а біометрія – наука, яка використовує унікальні вимірювальні параметри людини для її ідентифікації та верифікації.

Упровадження заходів з ідентифікації та верифікації необхідне під час вирішення таких проблем:

– боротьби з тероризмом, насамперед із міжнародним, і злочинністю (організованою, транскордонною, пов'язаною з викраденням людей і работоргівлею, тощо);

– протидії нелегальній міграції, що призвело в XXI столітті до реорганізації прикордонних служб усіх розвинених держав (у цьому напрямку також просувається й Україна);

– припинення шахрайств у сфері електронної та мобільної комерції, зловживань із кредитними картами (крадіжки і привласнення шляхом обману повноважень законного користувача з розпорядження грошовими коштами).

Біометричні системи ідентифікації охоплюють системи доступу за зображеннями відбитків пальців (дуже рідко долонь), райдужної оболонки ока, геометричних рис обличчя, малюнка вен руки або пальця, форми вуха, а також використанням ДНК, температури шкіри, електронного підпису та голосу. І це далеко не повний перелік, який має стійку тенденцію до розширення.

Для біометричної ідентифікації практично можна застосовувати багато різних характеристик і рис людини. Найбільш розвиненими нині технологіями залишаються розпізнавання за відбитками пальців, райдужною оболонкою очей і зображенням обличчя. Причому ідентифікація за папілярним малюнком пальця нині за застосуванням та доступністю з фінансового погляду випереджає всі інші технології.

Розширення сфер застосування біометрії насамперед пов'язують із постійно зростаючою потребою державних органів і бізнесу в забезпеченні необхідного рівня безпеки, уразливістю персональних комп'ютерів й існуючих інформаційних мереж та безупинним зростанням комп'ютерної злочинності.

Головним стимулом розвитку світової біометрії в середині другого десятиліття XXI сторіччя, як і на початок нового тисячоліття, залишається необхідність ефективного протистояння терористичним загрозам і нелегальній міграції. Значення біометричних технологій у комплексному забезпеченні безпеки постійно зростає, що підтверджується невпинним зростанням їх застосування в аеропортах та інших важливих інфраструктурних об'єктах.

Розвинуті світові держави вже запровадили або завершують запроваджувати електронні паспорти та ID-Card з біометричними відомостями щодо власників; багато фірм у своїх офісах запровадили біометричні системи контролю за доступом; персональні комп'ютери, ноутбуки та різні мобільні пристрої оснащуються засобами біометричної аутентифікації користувача; силові та інші служби безпеки використовують сучасні системи відеонагляду в комплексі з біометричними базами даних для виявлення розшукуваних злочинців у громадських місцях – таких прикладів дедалі більше.

Що стосується нашої держави, то слід констатувати, що в практичному впровадженні досягнень сучасної біометрії Україна дедалі більше відстає не тільки від провідних світових країн, але і від своїх сусідів: Білорусії, Польщі, Росії, Словаччини, Угорщини і навіть Молдови та Румунії.

Це стосується не тільки створення всієї необхідної державної інфраструктури для здійснення процедури автоматичної ідентифікації всіх виїзджаючих і в'їзджаючих осіб в Україну на предмет відповідності особистості власників їх документам, створення інформаційно-біометричних баз даних спеціального призначення і використання цих відомостей усіма силовими та правоохоронними структурами, але і навіть запровадження сучасних електронно-біометричних закордонних паспортів.

Власники молдавських біометричних паспортів із травня 2014 року одержали від Європейського союзу право на безвізовий в'їзд до ЄС, а в нашій країні на час написання посібника ще так і не ухвалено остаточного рішення щодо виробника біометричних паспортів із відомостями про відбитки пальців. Незважаючи на те, що ще у жовтні 2009 року асамблея Інтерполу одностайно затвердила український консорціум «ЄДАПС» виробником електронних або біометричних паспортів для співробітників цієї організації.

Що стосується застосування досягнень біометрики спецслужбами та іншими силовими структурами, то, крім створення мультибіометричних баз даних на десятки і навіть сотні мільйонів фігурантів, останнім часом дедалі більше приділяється увага проблемам організації взаємодії різних спецслужб і силових структур не тільки на національному, але й на міжнародному рівні, їх ефективному й якісному функціонуванню як єдиного співтовариства.

За час, який минув із появи першого видання посібника, у світі з'явилися бази даних (БД) із персональними відомостями, зокрема й біометричними, на сотні мільйонів осіб, а в майбутньому і понад мільярд осіб (проект присвоєння індійським громадянам ідентифікаційних номерів «Aadhar»; кількість населення Індії за офіційними даними становить 1,289 млрд осіб).

У Сполучених Штатах Америки створені перші у світі бази даних силових структур із біометричними відомостями на близько 100 млн фігурантів, а в майбутньому обсяг баз має перевищити показник у сто мільйонів. Насамперед йдеться про такі автоматизовані системи біометричної ідентифікації, як: система Федерального бюро розслідування США Next Generation Identification (NGI); система Міністерства оборони США Defense Automated Biometric Identification System (Dod ABIS); система Міністерства національної безпеки (Department of Homeland Security /DHS/) США US-VISIT з базою даних IDENT.

На сучасному етапі розвитку цивілізації у світовій спільноті пришвидшеними темпами створюються механізми швидкісного обміну інформацією між тими інстанціями, які за видом своєї діяльності повинні адекватно реагувати на всі загрози, що виникають і на національному, і міжнародному рівні. Створення єдиного інформаційного потоку між усіма спецслужбами, правоохоронними та іншими силовими структурами дозволяє ефективніше виконувати завдання захисту окремих держав і співтовариств країн від наявних терористичних та інших загроз. Особливо це видно на прикладах держав Євросоюзу, а також США, Австралії, Британії, Канади та Нової Зеландії. Останні п'ять держав входять у Конференцію п'яти країн (Five Country Conference – FCC). Учасники FCC мають домовленість про те, що для зміцнення безпеки кордонів, боротьби з незаконною міграцією та іншими виявами злочинних дій вони обмінюються біометричними даними стосовно осіб, що становлять інтерес у кримінальному плані.

Упродовж останніх п'яти – десяти років відбувалось інтенсивне впровадження біометрії у системи контролю фізичного доступу та захисту корпоративних інформаційних ресурсів. Нині можна констатувати, що біометрія перетворилась у невід'ємну частину і важливий чинник еволюції ринку систем контролю та управління доступом (СКУД). А нові технології організації доступу і захисту інформації, що використовують біометричні технології, є не тільки найнадійнішими, але і найзручнішими для користувачів – зникла необхідність запам'ятовувати складні паролі та постійно носити із собою смарт-карти або апаратні ключі.

Щодо поширення біометричних технологій у майбутньому, то більшість експертів прогнозують, що найбільший рівень їх застосування буде в діяльності державних структур, зокрема в обороні та міграційному контролі, а також у банківській і фінансовій сфері. Біометрика й надалі буде все більше застосовуватися у системах контролю за доступом, зокрема в різних медичних закладах, не тільки біометричними, але навіть і мультибіометричними дедалі частіше будуть ставати ідентифікаційні карти, різні електронні документи, системи голосування. Новою істотною тенденцією є широке застосування досягнень біометрії у споживчій електроніці та забезпеченні безпеки житла. Що стосується недоліків біометрії, то головний недолік цієї технології – можливість перехоплення ідентифікаційних даних індивідуума, зокрема й в електронному вигляді. Тут доречним є вислів, що юристи – знавці права, а злочинці – знавці можливостей.

Тому, за висновками експертів, найліпший захист будь-якої інформації можуть гарантувати тільки найновіші засоби забезпечення інформаційної безпеки, однією з яких є технології біометрично-криптографічного шифрування. Інтеграція біометричних і криптографічних технологій створює нові перспективи строгої ідентифікації, забезпечення інформаційної безпеки та захисту персональних даних.

Основним завданням посібника є ознайомлення читачів з основними відомостями щодо прикладного використання досягнень сучасних біометричних технологій насамперед у світлі потреб правоохоронних органів, спецслужб та інших силових структур. Зокрема застосування біометричних можливостей у існуючих баз даних Європолу, Інтерполу та прикордонних служб суміжних держав на практиці повинно сприяти зростанню розкриттю злочинів в Україні.

ВСТУП

Біометрія належить до тих галузей сучасних технологій, темп розвитку яких пришвидшився на початку XXI століття – після відомих подій 11 вересня 2001 року в Сполучених Штатах Америки. Сучасні тенденції політичного світового розвитку вказують на те, що XXI століття почалося з посилення конфронтації різних цивілізацій. Ці конфлікти породжуються насамперед наявними відмінностями в культурі, релігії, економіці та політиці держав. Процес глобалізації разом із серйозною зміною світової економіки є каталізатором стрімкого розвитку нелегальної міграції, тероризму та міжнародної організованої злочинності.

У зв'язку зі зростанням кількості терористичних актів поширенням нелегальних міграційних процесів і транснаціональної злочинності актуальними стали питання адекватної реакції на негативні виклики сучасності та розробка новітніх заходів для забезпечення зовнішньої та внутрішньої безпеки всіх членів світової спільноти. Сучасні досягнення науки і техніки використовуються для подальшого вдосконалення різних технологій систем безпеки та їх впровадження на національному і міжнародному рівнях. Як наслідок – стрімкий світовий розвиток електроніки та інформатики, нанотехнологій, зокрема й біометричних технологій.

Недавнім часом біометрія дедалі більше привертає до себе уваги як одна з інформаційних технологій, яка стрімко почала розвиватися у XXI столітті та визначає розвиток засобів систем ідентифікації і верифікації фізичних осіб, що дозволило з надзвичайно високою надійністю використовувати досягнення біометричної науки в сучасних різноманітних системах контролю й управління доступом для забезпечення безпеки і на державному, і на приватному рівнях. У минулому столітті термін «біометрія» мав набагато ширше тлумачення та належав в основному до методів математичної статистики, які застосовувалися для математичного опису процесів будь-яких біологічних явищ. Тепер значення цього терміна стало значно вужчим – під біометрією і біометричними технологіями, як правило, розуміють автоматизовані методи встановлення чи розпізнавання будь-якої особистості за її біологічними характеристиками або за їх проявами.

Основною перевагою біометричних технологій (біометрії або біометрики) є можливість швидкої і простої ідентифікації або верифікації здебільшого без спричинення якихось незручностей індивідуумові. У публікаціях із біометрики часто виражаються два протилежні погляди. Перший із них – «ура-біометрика», тобто рівень її розвитку дуже високий і вже вирішені майже всі проблеми. Другий – біометричні технології ще недостатньо надійні[1].

За останнє десятиріччя біометричні технології зробили величезний крок у своєму розвитку і практично стали самостійною галуззю зі зростаючою перспективою. Експерти компанії «Biometrics Research Group» передбачають, що до 2020 року мобільними платежами будуть користуватися близько 700 млн людей[2].

Починаючи з 2007 року, в засобах масової інформації (ЗМІ) помічено справжній бум публікацій із розвитку різних методів біометричної ідентифікації і верифікації

[1] Мифы биометрии. [Электронный ресурс]. – Режим доступа: http://www.cbio.ru/modules/news/…

[2] Биометрические технологии в смартфонах и мобильных платежах: битва Apple и Samsung // BIOMETRICS.RU. – 2013. – 24 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

та розробки на їх основі новітніх систем біометричних технологій. Необхідно констатувати, що в практичному впровадженні досягнень сучасної біометрії Україна дедалі більше відстає не тільки від провідних світових країн, але й своїх сусідів: Білорусі, Польщі, Росії, Словаччини, Угорщини і навіть Молдови та Румунії. Це стосується не тільки утворення всієї необхідної державної інноваційної інфраструктури для проведення перевірок на прикордонних КПП, створення відповідних інформаційно-біометричних баз даних і використання цих відомостей усіма силовими і правоохоронними структурами, але й темпів запровадження сучасних біометричних закордонних паспортів із біометричними показниками.

Як наслідок, в Україні не так багато публікацій про використання сучасних досягнень біометричних технологій. На сторінках українських ЗМІ часто можна простежити лише матеріали, які пов'язані з різними скандалами, що супроводжують упровадження і видачу українським громадянам паспортно-візових документів нового покоління. Причому ця проблема у друкованих виданнях розглядається тільки з погляду умов отримання закордонних паспортів нового покоління, можливості надання українським громадянам безвізового режиму з країнами Європейського Союзу та США, водночас зовсім не висвітлюються можливості використання останніх досягнень біометрії для потреб і виконання завдань, що стоять перед українськими силовими структурами, і найперше перед спецслужбами та правоохоронними органами.

Варто зазначити, що узагальнюючих друкованих матеріалів, виданих на території України у XXI столітті та присвячених проблемам використання сучасних систем біометрики й інформаційних баз із біометричними даними, дуже мало. Тому в посібнику авторами були використані матеріали Інтернет-видань і низка публікацій щомісячного інформаційного бюлетеня «Боротьба зі злочинністю за кордоном» (за матеріалами зарубіжної преси).

Біометрія – це не сенсація сьогодення. Розробка сучасних біометричних технологій продовжується вже п'яте десятиліття, а розробка різноманітних стандартів і тестів дозволяють цим технологіям найефективніше сприяти розвитку та уніфікації різних систем безпеки.

На початку XXI століття практичне застосування біометричних методів ідентифікації та верифікації, якщо і не є одним із найголовніших шляхів розвитку інформаційних технологій, то становить доволі значну їх складову.

Ще в середині 70-х років минулого сторіччя біометричні системи забезпечення безпеки застосовувалися лише для захисту державних і військових секретів, а також найважливішої комерційної інформації. Але після серії терористичних актів на початку нового тисячоліття біометричними системами контролю доступу почали обладнувати аеропорти, великі торгові центри та інші громадські місця. З'явився підвищений попит на біометричні пристрої, що зумовило зростання досліджень у цій галузі і, як наслідок, появу спеціальних технологій і апаратних рішень.

2001 року обсяг біометричного ринку становив усього 300 млн доларів, а в 2006 році він зріс до 2 млрд доларів[1].

Згідно з прогнозом 2007 року «Acuity Market Intelligence» щорічний оборот біометричного ринку мав сягти до 2020 року 10 млрд доларів США, але прогнози 2014 року свідчать, що він може становити 23,54 млрд доларів. У прогнозі 2007 року було виокремлено два ключові сегменти ринку:

– суспільно-державний (електронні системи прикордонного контролю, електронна ідентифікація, «електронний уряд» тощо);

– комерційний (корпоративна та інформаційна безпека, фінансові транзакції та ін.).

[1] Американские университеты готовят специалистов по биометрии // BIOMETRICS.RU. – 2007. – 30 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Дійсність поки що повністю підтверджує прогнози стосовно цих сегментів ринку. У контексті еволюції цих секторів ринку проводяться інтенсивні дослідження для розвитку основних прикладних сфер застосування біометрії – ідентифікації і верифікації особи, особливо в системах відеоспостереження, контролю фізичного доступу та захисту інформації[1].

За оцінкою аналітиків компанії Global Industry Analysts (GIA), до 2017 року обсяг біометричного ринку становитиме 16,47 млрд доларів[2].

Нині біометричні системи є другим поколінням систем безпеки, а біометрія вважається такою наукою, що використовує унікальні вимірювальні параметри людини для її ідентифікації та верифікації. Впровадження заходів з ідентифікації і верифікації необхідно під час вирішення таких проблем:

– боротьби з тероризмом, особливо з міжнародним, та злочинністю (організованою, транскордонною, пов'язаною з викраденням людей і работоргівлею тощо);

– протидії нелегальній міграції, що призвело в XXI столітті до реорганізації прикордонних служб усіх розвинених держав (у цьому напрямку також просувається й Україна);

– припинення шахрайств у сфері електронної та мобільної комерції, зловживань із кредитними картами (крадіжки та привласнення шляхом обману повноважень законного користувача з розпорядження грошовими коштами).

Також ефективних і надійних засобів і систем масової ідентифікації конче потребують і законослухняні громадяни. Їм необхідні зручні, надійні, швидкозчитувальні і максимально захищені від підробок документи при таких подіях:

– проходженні паспортного та прикордонного контролю – закордонні паспорти, візи, внутрішні ідентифікаційні документи (ID-карти) або їх аналоги, що засвідчують особистість пред'явника;

– підтвердженні свого особливого статусу і/або повноважень на здійснення спеціальних видів діяльності, зокрема професійної (права водія, посвідчення моряка, студентські квитки, пенсійні посвідчення, посвідчення біженця і т. д.);

– зверненні до систем медичного і соціального забезпечення, страхування, у бібліотеки, музеї, інші установи культури та науки тощо;

– взаємодії з державними органами, зокрема в межах «електронного уряду» (до цієї сфери належать також участь у виборах, референдумах та інших формах волевиявлення);

– користуванні фінансовими системами, програмами лояльності, додатковими сервісами на транспорті (програми супроводу авіапасажирів, які часто мандрують, тощо)[3].

Головним стимулом розвитку світової біометрії є необхідність ефективно протистояти терористичним загрозам і нелегальній міграції. Значення біометричних технологій у комплексному забезпеченні безпеки постійно зростає, що демонструється невпинним зростанням їх застосування в аеропортах та інших важливих інфраструктурних об'єктах.

Згідно з прогнозом компанії «Frost & Sullivan» «Аналіз світового ринку прикордонного контролю і біометрії» (Global Border Control and Biometrics Market Assessment) дохідність ринку в 2012 році мала становити 5,836 млн доларів США та повинна сягнути 15,836 млн доларів США до 2021 року.

---

[1] Прогноз развития биометрического рынка на долгосрочную перспективу // BIOMETRICS.RU. – 2007. – 6 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Объем мирового биометрического рынка к 2017 году превысит 16 миллиардов долларов // BIOMETRICS.RU. – 2011. – 17 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Массовая идентификация. – 2007. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/civil_id.php

Дослідження охоплює системи безпеки для цивільних, військових, державних потреб, зокрема й правоохоронних органів[1].

Використання досягнень комп'ютерно-інформаційних і телекомунікаційних технологій дозволяють здійснювати ідентифікацію користувача в режимі реального часу. Біометричні технології засновані на інтеграції досягнень у галузі електроніки, інформатики, математики, медицини й біометрії, а останнім часом і на основі нанотехнологій, що дозволяє істотно зменшити габарити використовуваної апаратури для біометричних систем, що розробляються.

Нині одним із найперспективніших напрямів є розробка і виробництво різних біометричних інтелектуальних систем безпеки.

Біометричні системи ідентифікації охоплюють системи доступу за відбитками пальців і долонь, райдужної оболонки ока, геометрії обличчя, малюнком вен на руці або пальці, ДНК, форми вуха, температури шкіри, підпису та голосу. І це ще не повний перелік, який має стійку тенденцію до розширення.

Розширення сфери застосування біометрії насамперед пов'язано з постійно зростаючою потребою державних органів і бізнесу в забезпеченні безпеки, з вразливістю персональних комп'ютерів й існуючих інформаційних мереж та безупинним зростанням комп'ютерної злочинності.

Запровадження біометричних систем ідентифікації відбувається практично скрізь: на прикордонних контрольно-пропускних пунктах, митних терміналах, в аеропортах, у системах контролю й управління доступом до наявних комп'ютерних баз даних і систем, на об'єктах інфраструктури життєзабезпечення, у місцях масового скупчення громадян і так далі, не кажучи вже про різні режимні об'єкти. Разом з ідентифікацією такі системи можуть мати й низку інших функцій, які використовуються абсолютно в інших сферах, наприклад, для обліку і контролю пасажиропотоків, діагностики стану здоров'я та психофізичних можливостей людини[2].

Зі стрімким розвитком Інтернет-технологій провідні зарубіжні фірми, які спеціалізуються у сфері інформаційних технологій, щорічно вкладають значні кошти у створення відповідного інструментарію інтелектуальної обробки текстової, мовної і графічної інформації. Насамперед це пов'язано з тим, що на застосуванні названих інтелектуальних технологій обробки даних базуються перспективні концепції управління силами і засобами в складних обставинах.

Сьогодні на основі їх активного використання передбачається активна підтримка політичних, економічних та інших рішень. На їх базі розробляються і ґрунтуються складні біометричні системи ідентифікації і верифікації, які використовуються як для потреб державних і правоохоронних структур, так і для виконання завдань щодо забезпечення безпеки комерційних організацій[3].

Останнім часом у найрозвинутіших країнах світу дедалі більше приділяється уваги проблемам організації взаємодії різних спецслужб і силових структур не тільки на національному, але і на міжнародному рівні, їх ефективному й якісному функціонуванню як єдиного співтовариства.

Вельми важливим для реформування розвідувально-правоохоронного співтовариства для боротьби з такими загрозами XXI століття, як міжнародний тероризм, незаконна міграція, транснаціональна злочинність і подібні явища є вирішення проблеми швидкісного обміну даними між різними спецслужбами і силовими структурами як на національ-

[1] Биометрические системы пограничного контроля: новый прогноз // BIOMETRICS.RU. – 2013. – 10 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Общие сведения о биометрии. – 2007. – 25 июля. [Электронный ресурс]. – Режим доступа: http://www.biopassport.ru/ru/biometric/about/...

[3] Минаев В. А. Современные технологии обеспечения информационной безопасности / В. А. Минаев // Biometrics.ru. – 2008. – 31 янв. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

ному, так і на міжнародному рівні. У сучасних складних умовах необхідно відійти від правила відомчої пріоритетності прав на добування та використання спеціальної і закритої інформації.

На нинішньому етапі розвитку цивілізації у світовій спільноті пришвидшеними темпами створюються механізми швидкісного обміну інформацією між тими інстанціями, які за видом своєї діяльності повинні адекватно реагувати на всі загрози, що виникають і на національному, і міжнародному рівні.

Створення єдиного інформаційного потоку між усіма спецслужбами, правоохоронними та силовими структурами дозволяє ефективніше виконувати завдання захисту окремих держав і співтовариств країн від наявних терористичних та інших загроз початку нинішнього століття.

Особливо це видно на прикладах держав ЄС, а також США, Канади й Австралії. Наприклад, як очевидно з опублікованої в лютому 2008 року щорічної доповіді директора Національної розвідки США, якому тоді були підпорядковані всі американські спецслужби, перед членами сенатського комітету США з розвідки, вказане відомство посилено працює над створенням єдиної інформаційної інфраструктури, яка діятиме на користь усіх спецслужб США.

Крім того, доступ до нових технологій, програмного забезпечення матимуть й інші федеральні відомства Сполучених Штатів Америки (їх налічується близько 50).

Для вдосконалення діяльності розвідувально-правоохоронних та інших силових структур однією з необхідних умов є прискорення процесів збору відомостей та їх аналізу. Це завдання планується виконати за допомогою впровадження найостанніших досягнень інформаційно-аналітичних технологій. Особлива увага приділяється якнайшвидшому створенню і введенню в дію національних біометричних банків даних, які були б сумісні не тільки на національному, але і на міжнародному рівні, а також створенню програм і відповідної апаратури доступу та обміну електронними відомостями за закритими каналами зв'язку[1].

Згідно з прогнозом компанії «Fujitsu» до 2013 року лише 5% населення у розвинутих країнах не матиме предметів, які не будуть містити у тому чи іншому виді різні біометричні пристрої чи їх елементи. Це такі документи або артефакти, як паспорти або посвідчення особи (ID-cards), водійські посвідчення, банківські карти, карти клієнтів супермаркетів, різна комп'ютерна техніка, мобільні телефони, різноманітні замки та інше, в які будуть вмонтовані спеціальні елементи на основі найновіших досягнень біометрії[2].

Сучасна біометрія ще не розкрила всіх своїх можливостей, згодом на основі використання останніх досягнень біометричних технологій будуть пропонуватися нові апаратно-програмні рішення.

Експерти компанії «Frost & Sullivan» у своєму огляді виокремили такі перспективні напрями розвитку світового біометричного ринку:

– використання технологій біометрики у діяльності правоохоронних і силових структур;

– зростання кількості біометричних проектів, що реалізуються під патронатом державних структур (біометричні паспорти, візи, ID-картки, організація контролю доступу за вказаними документами);

– інтенсивне впровадження біометрії у системи контролю фізичного доступу та захисту корпоративних інформаційних ресурсів;

---

[1] Иванов В. В разведывательном сообществе США полным ходом идет перестройка / В. Иванов // Независимое военное обозрение. – 2008. – 7 марта. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/spforces/...

[2] Биометрия: будущее начинается сегодня // Bankir.Ru. – 2008. – 3 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

– застосування біометричних технологій для потреб користувачів – фізичних осіб (наприклад: у мобільних пристроях, протиугонних автомобільних системах і т. д.).

Аналітик «Frost & Sullivan» Арчана Рао (Archana Rao), коментуючи презентацію нового огляду, зазначив, що укріплення позицій біометричних систем на ринку рішень з ідентифікації сприяє зростання їх продуктивності та розширення можливостей їх інтеграції з іншими інформаційними технологіями[1].

На початку XXI століття в деяких навчальних закладах США, Великобританії, Канади і низки інших країн розпочато викладання дисципліни біометрії. У американському Університеті Західної Вірджинії (West Virginia University – WVU) викладання цієї дисципліни здійснюється з 2001 року.

Курс біометрії має міждисциплінарний характер і охоплює обчислювальну й електронну техніку, біологію і статистику. Після закінчення університету студенти, які освоїли курс біометрії, отримують, як правило, дипломи з технічних наук і обчислювальної техніки.

На базі West Virginia University діє науковий Центр із досліджень у сфері технологій ідентифікації (Center for Identification Technology Research /CITeR/). У його роботі беруть участь понад 20 комерційних компаній і федеральних агентств[2].

Метою написання та публікації другого видання посібника насамперед є ознайомлення слухачів (студентів) і викладачів навчальних закладів МВС, працівників правоохоронних і силових структур, науковців і практиків, з останніми досягненнями біометричних технологій та існуючими базами даних для потреб спецслужб і правоохоронних органів.

У підсумку, після ознайомлення з матеріалами посібника, читачі, на думку авторів, матимуть уявлення про стан сучасної біометрії, перспективи використання біометричних технологій, про можливості сучасних баз даних із біометричними та персональними даними громадян. У майбутньому одержані знання повинні знайти практичне втілення у разі потреби застосування біометричних систем та пошуку необхідних відомостей під час безпосереднього виконання своїх функціональних обов'язків.

Викладені у посібнику матеріали надають повне уявлення про можливість реалізації спецслужбами розвинених країн ідеї тотального автоматизованого контролю за можливими переміщеннями громадян у більшості світових держав.

[1] Объем мирового биометрического рынка к 2016 году превысит пять миллиардов долларов // BIOMETRICS.RU. – 2011. – 22 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Университет Западной Вирджинии готовит специалистов по биометрии // BIOMETRICS.RU. – 2009. – 26 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

ЗАГАЛЬНА ЧАСТИНА

Розділ 1

ІСТОРІЯ, ПОНЯТТЯ ТА СУЧАСНЕ УЯВЛЕННЯ ПРО БІОМЕТРІЮ

1.1. Стисла історія виникнення наукової дисципліни «біометрія» та її основні поняття

Поняття «біометрія» виникло в кінці XIX століття і під ним розуміли розділ науки, який займається кількісними біологічними експериментами із залученням методів математичної статистики. У кінці XX сторіччя інтерес до біометрії значно зріс завдяки тому, що цю галузь науки застосовано в розробках нових технологій безпеки, суть яких зводилася до використання комп'ютерних систем розпізнавання особи за параметрами унікального генетичного коду людини.

В історії людства використання біометрії сягає в далеке минуле. Так, ще в ассирійців і стародавніх єгиптян використовувався відбиток пальця на документах. У Британському музеї зберігається глиняна ассирійська дощечка – акт про продаж землі в Ассирії, на якій є відбиток витисненого сліду пальця і запис, що цей відбиток зроблено продавцем землі.

Зважаючи на це, своєрідний спосіб скріплення та засвідчення торгових операцій послугував приводом для застосування пальцьових відбитків як особистої печатки. Із незапам'ятних часів китайці, індуси, араби, сіамці та інші народи Сходу засвідчують відбитками пальців дійсність різних торгових операцій і договорів. Узори на шкірі внутрішньої сторони рук людини були відомі й представникам стародавньої медицини. Так, опис філігранних малюнків на кінчиках пальців рук уперше простежується у знаменитого анатома XVII століття Мальпіги.

Учені XIX століття – Пуркиньє, Алікс, Гершель, Фольдс і Гальтон – детально вивчали папілярні узори на пальцях рук. У результаті ґрунтовних досліджень у цій галузі були встановлені дві основні властивості папілярних пальцьових узорів – індивідуальність і незмінність їх із моменту утворення та впродовж усього життя[1].

Загальновідомо, що найцікавіші дисципліни виникають на стику галузей декількох наук. Такою суміжною дисципліною і стала біометрія. Біометрію започаткував

[1] История развития идентификации. – 2005. – 2 мая. [Электронный ресурс]. – Режим доступа: http://www.magicpc.spb.ru/journal/...

Френсіс Гальтон (1822–1911 рр.). У його книзі, присвяченій природній спадковості, яка була видана 1889 року, ним уперше було вжито термін «biometry», і саме тоді він розробив основи кореляційного аналізу. Ф. Гальтон заклав підвалини нової науки і назвав її. Проте сформував її у наукову дисципліну математик Карл Пірсон (1857–1936 рр.).

Подальший етап розвитку біометрії пов'язаний з іменем великого англійського статистика Рональда Фішера (1890–1962 рр.). Ним були розроблені теорія вибіркових розподілів, методи дисперсійного та дискримінантного аналізу, теорія планування експериментів, метод максимальної правдоподібності та багато іншого, що є основою сучасної прикладної статистики і математичної генетики.

У 1901 році К. Пірсоном і Ф. Гальтоном було засноване видання журналу «Biometrika». Із 1945 року почав виходити журнал «Biometrics», а з 1959 р. – «Biometrische Zeitschrift». У 1938 р. була створена Біометрична секція американської статистичної асоціації. У 1947 р. у Вудс-Холі (США) була проведена «Перша міжнародна біометрична конференція», на якій було засноване Міжнародне біометричне товариство. Конференції Міжнародного біометричного товариства відбулися в 1949, 1953, 1958, 1963, 1967 та інших роках[1].

Гершель, який вивчав із 1858 року відбитки пальців, першим запропонував скористатися ними для ідентифікації людей. Основи ідентифікації він виклав 1877 року в листі начальникові тюремного управління в Індії, а трохи пізніше (1880 р.) опублікував у виданні «Nature» свої дослідження в сфері ідентифікації за відбитками пальців. Того ж року Фольде абсолютно незалежно від Гершеля також запропонував скористатися відбитками пальців для ідентифікації людей.

1882 року А. Бертільон розробив антропометричний спосіб розпізнання особи. Цей спосіб встановлення тотожності особи ґрунтується на такому встановленому факті: у природі не може бути двох цілком тотожних предметів, тому не можна знайти двох людей, у яких розміри частин тіла повністю б збігалися. Антропометричний спосіб розпізнання особи полягає у вимірюванні деяких частин тіла і подальшої досить оригінальної класифікації отриманих розмірів.

Через деякий час А. Бертільон доповнив цей спосіб впізнання особи введенням опису форм деяких частин тіла, очей, волосся й особливих прикмет. На заповненій цими відомостями карті наклеювалися фотографії у фас і профіль. Ця технологія відома як система Бертільона.

Але засновником дактилоскопічного методу ідентифікації є Ф. Гальтон, який своїми ґрунтовними дослідженнями розробив основи дактилоскопії і класифікував папілярні узори відбитків пальців. Розроблений ним метод з огляду на точність, простоту і придатність застосування до всіх осіб незалежно від віку згодом абсолютно витіснив систему А. Бертільона.

Таким чином, висловлюючись словами представника Французької Академії Наук, «пальцьовий відбиток є свого роду тілесним підписом, підробки якого побоюватися не доводиться».

1894 року було введено в кримінальну практику дактилоскопію як методу ідентифікації людини, коли англійським парламентом була видана синя книга «The Identification of Habitual Criminals».

[1] Леонов В. П. История биометрики и её применения в России / В. П. Леонов // Международный журнал медицинской практики. – 1999. – Вып. 4. – С. 7–19. [Электронный ресурс]. – Режим доступа: http://www.biometrica.tomsk.ru/history.htm

Підставами для дактилоскопічного методу ідентифікації людського індивідуума (надалі просто індивідуума) є такі висновки вчених:

1. Незмінний характерний малюнок папілярних узорів пальців із моменту формування плоду в утробі матері й до кінця життя (навіть і пізніше, до розкладання трупа).

2. Папілярні узори пальців є суто індивідуальні, тобто цей малюнок з усіма подробицями його структурної побудови не може повторитися у іншої особи.

3. Незважаючи на надзвичайно велику різноманітність узорів пальців, їх можна поділити на невелику кількість груп і підгруп, тобто піддати класифікації[1].

Перші автоматичні пристрої дактилоскопічного розпізнавання з'явилися в основному в кінці 70-х – початку 80-х років минулого століття. До 11 вересня 2001 року біометричні системи забезпечення безпеки доступу застосовувалися в основному тільки для захисту військових і державних секретів та найважливішої комерційної інформації. Зростання попиту на такі пристрої спричинило інтенсивні дослідження в цій сфері, що, своєю чергою, зумовило появу нових пристроїв і цілих технологій, зокрема біометричних.

Біометрія – це ідентифікація людини за унікальними, властивими тільки їй, біологічними або поведінковими ознаками.

Фізіологічні особливості людини, наприклад, такі, як папілярний узор пальця, геометрія обличчя, температура шкіри обличчя, модель райдужної оболонки ока, геометрія долоні, сітківка ока, структура ДНК, структура кровоносних судин, форма вуха, особливості клавіатурного набору та підпису і багато інших є постійними і незмінними характеристиками або такими, що практично не змінюються з часом.

Зараз біометрія є сукупністю автоматизованих методів і засобів ідентифікації або верифікації людини, яка заснована на її фізіологічних або поведінкових характеристиках[2].

Біометрія – це одна з найперспективніших інформаційних технологій ідентифікації, що активно розвивається. Біометричні пристрої ідентифікації й верифікації використовуються понад чотири десятки років. У XXI столітті біометричні рішення швидко стали популярними у найрізноманітніших сферах життя: від паспортно-візових документів нового покоління до попередження і розкриття злочинів, а в майбутньому – і злочинних намірів окремих індивідуумів.

Нині системи доступу і захисту інформації, які використовують біометричні технології, за висновками фахівців, є не тільки найнадійнішими, але і найзручнішими для користувачів – не потрібно запам'ятовувати складні паролі, постійно носити з собою смарт-карти або апаратні ключі. Потрібно лише прикласти до сканера палець або руку, підставити для сканування в інфрачервоному промінні око, обличчя, руку або палець, щонебудь сказати, щоб ідентифікувати особу та надати їй можливість проходу на територію об'єкта, що знаходиться під охороною, або доступу до комп'ютерних мереж та інформації з обмеженим доступом.

Причини популярності біометричних технологій загальновідомі: це їх достатня надійність, безпечність, ефективність і комфортність. На відміну від інших технологій, біометрія працює безпосередньо з людьми й ідентифікує їх індивідуальні ознаки, інакше біометричні пристрої просто не змогли б діяти.

---

[1] Бычков С. Биометрия в мэйлерах / Сергей Бычков. [Электронный ресурс]. – Режим доступа: http://www.magicpc.spb.ru/journal/...

[2] Что такое биометрия? [Электронный ресурс]. – Режим доступа: http://universalkey. boxmail.biz/cgi-bin/guide…

У широкому розумінні біометрія – вимірювання унікальних фізичних і/або поведінкових характеристик індивідуума.

У вузькому розумінні (який зараз в основному і використовується) в це поняття включають технології і системи автоматичної ідентифікації людини і/або підтвердження її особистості, засновані на аналізі унікальних біометричних параметрів.

Нині найпоширенішою біометричною технологією є ідентифікація за відбитками пальців. За даними фахівців компанії «BioLink», ця технологія займала у 2008 році понад 50% від його обсягу та залишається ведучою серед технологій біометрики[1].

У своєму огляді за 2013 рік експерти компанії GIA прогнозують, що технології ідентифікації за відбитками пальців будуть домінувати й надалі. До 2018 року обсяг цього сегмента галузевого ринку має сягти 10 млрд доларів, тоді як відповідний показник для технологій ідентифікації за обличчям і голосом буде становити лише 2,9 млрд $.

Суттєво, що домінуюче застосування технологій ідентифікації за відбитками пальців прогнозують і для державних, і комерційних структур. Але сферою, де очікується найбільше застосування сканерів для зняття відбитків пальців, це виробництво портативних і мобільних комп'ютерних пристроїв (ноутбуків, планшетів тощо) та смартфонів.

Автори огляду вважають, що статус найбільшого ринку для вказаної технології і надалі буде належати США. Але найдинамічніше технології ідентифікації за відбитками пальців будуть розвиватися в державах Азіатсько-Тихоокеанського регіону: середньорічні темпи росту, що обчислюються у так званих складних відсотках (CAGR), у період до 2018 року становитимуть 20%.

Для субсегмента біометричних систем, які ідентифікують своїх користувачів за відбитками пальців і які застосовуються у комерційному та суспільному секторах, показник CAGR за цей період становитиме 16%, і цей субсегмент буде найбільш швидкозростаючим[2].

1.2. Завдання, які вирішуються за допомогою біометрії, та сфери застосування біометрії

Біометричні характеристики властиві всім людям, тому для представників низки соціальних і демографічних груп (діти, пенсіонери, громадяни, які погано бачать і чують або не вміють читати та писати, тощо) біометрична ідентифікація є якщо не єдиним, то основним засобом засвідчення особи і/або її розпізнавання.

Крім біометричних засобів, як засоби ідентифікації також використовуються різні варіанти смарт-карт і токенів. Нині у більшості країн у різні типи документів, які засвідчують особу пред'явника, активно впроваджують сучасні засоби ідентифікації і верифікації, для чого часто повністю змінюють їх традиційний «паперовий» вигляд на рішення, засновані на технологіях або симбіозі технологій смарт-карт, штрих-кодів, електронного підпису, шифрування, біометричної або радіочастотної (RFID) ідентифікації.

[1] Технологии // BioLink. – 2008. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/

[2] Применение технологий биометрической идентификации по отпечаткам пальцев будет расширяться. – 2013. – 14 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

В Україні прикладами ідентифікаційних документів нового покоління є біометричні закордонні паспорти, банківські картки нового зразка та ідентифікаційні картки допуску на режимні об'єкти.

Із другої половини першого десятиліття XXI століття в нашій країні, як і у всьому світі, дедалі активніше починають застосовувати біометричні технології ідентифікації.

Без біометричних технологій практично неможливо виконати завдання масової ідентифікації індивідуумів, яке вкрай потрібне під час вирішення таких проблем:

– боротьби з тероризмом і злочинністю – організованою, транскордонною, пов'язаною з викраданнями людей, новими формами работоргівлі (дорослими і дітьми), тощо;

– протидії нелегальній міграції;

– припинення шахрайств у сфері електронної і мобільної комерції та зловживань із кредитними картами (так званих «крадіжок особи» – розкрадання і/або привласнення шляхом обману повноважень законного користувача з розпорядження грошовими коштами).

Одночасно законослухняні громадяни також потребують ефективних і надійних засобів і систем масової ідентифікації. Їм необхідні зручні, надійні й безпечні процедури посвідчення особи під час таких ситуацій:

– проходження паспортного і прикордонного контролю (закордонні паспорти, візи, внутрішні ідентифікаційні картки чи їх аналоги, посвідчення платника податків тощо);

– підтвердження свого особливого статусу і/або повноважень на здійснення спеціальних видів діяльності, зокрема професійної (права водія; різні посвідчення: моряка, пенсіонера, біженця; студентські квитки);

– звернення до систем медичного і соціального забезпечення, страхування, в бібліотеки, музеї, інші установи культури та науки і т. д.;

– участі у виборах, референдумах та інших формах волевиявлення;

– взаємодії з державними органами, особливо в межах системи так званого «електронного урядування»;

– користування фінансовими системами, програмами лояльності, додатковими сервісами, які можуть надавати транспортні підприємства (програми супроводу авіапасажирів, які часто мандрують, тощо)[1].

Нині основою системи інформаційної безпеки (ІБ) є засоби ідентифікації користувачів і управління їх доступом до корпоративних інформаційних ресурсів. Інформаційні технології та ресурси – невід'ємна складова діяльності будь-якої компанії, тому забезпечення безпеки цього цінного активу є стратегічним пріоритетом у її діяльності.

У низці ідентифікаційних засобів захист інформації забезпечується шифруванням, генерацією одноразових паролів, електронним підписом і цифровими сертифікатами. Але найефективнішим є використання будь-яких засобів ідентифікації у комплексі з біометричними технологіями. Біометричні ідентифікатори також можуть використовуватися і самостійно.

У будь-якому варіанті використання біометрії зберігається її основна перевага – точна, безпечна, швидка і зручна ідентифікація користувача[1].

[1] Массовая идентификация // BioLink. – 2008. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/civil_id.php

Усі системи біометричної ідентифікації виконують дві основні функції:

1. Реєстрації – за декількома вимірюваннями за допомогою зчитувального біометричного пристрою формується цифрова модель (шаблон) відповідної біометричної характеристики (залежно від методу ідентифікації або верифікації: відбитку пальця, малюнка райдужної оболонки ока, зображення обличчя та ін.) особи, яка реєструється.

2. Ідентифікації – одне або декілька вимірювань контрольованої біометричної характеристики зчитувальним пристроєм, яка трансформується в придатну для використання цифрову форму і потім порівнюється:

а) з єдиним шаблоном, який належить особі, котру перевіряють. Шаблон вибирається за номером або кодом, який заздалегідь був внесений у базу даних. Результат порівняння виводиться на екран пристрою ініціатора запиту.

Така процедура називається *верифікацією або порівнянням «один до одного».* Результат зазвичай виводиться у вигляді числа, яке показує ступінь вірогідності того, що шаблони, які порівнювались, належать одній особі.

Потім, за допомогою якого-небудь математичного критерію, ухвалюється рішення про ідентичність шаблонів;

б) з усіма зареєстрованими в базі даних шаблонами (без попереднього вибору шаблону за допомогою введення номера або коду). Як підсумковий результат надається список декількох найбільш подібних шаблонів (із зазначенням найбільшого ступеня вірогідності, отриманого за результатами порівняння). Потім, як і у попередньому випадку, за допомогою спеціального математичного критерію ухвалюється рішення про ідентичність шаблонів. Така процедура має назву аутентифікації *або порівняння «один до багатьох»*[2].

Технології, які застосовують біометрію, привертають увагу багатьох фахівців із державних установ і найрізноманітніших галузей економіки. Постійні дослідження, які проводяться співробітниками фірм-розробників засобів ідентифікації, підтверджують, що використання унікальних людських характеристик (відбитків пальців, райдужної оболонки очей, зображення обличчя і т. д.) є одним із найліпших нині рішень для досягнення приватності, конфіденційності, аутентифікації, управління доступом, безперебійності у роботі та цілісності інформації.

Біометричні системи значною мірою перевершують традиційні способи аутентифікації, які використовують систему паролів або спеціальних ідентифікаційних смарт-карток, або токенів. Безумовною перевагою біометрії є спосіб авторизації, під час якого система перевірить, чи індивідуум, котрий намагається ввійти до системи, є саме тією особистістю, яка має на це право, а не особою, котра знайшла загублену смарт-картку або записник із паролями. Отже, біометричні системи, що не потребують паролів та ідентифікаційних карток, привносять додатковий елемент безпеки в роботу організацій, установ, підприємств[3].

Технології, які застосовують біометрію, повинні відповідати вимогам, які пред'являють до біометричної ідентифікації і створюваних на її основі документів, провідні міжнародні, регіональні та галузеві організації, а також міждержавні структури й урядові органи.

---

[1] Защита информации // BioLink. – 2008. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/security.php

[2] Биометрические технологии. [Электронный ресурс]. – Режим доступа: http://universalkey.boxmail.biz/cgi-bin/guide...

[3] Прохоров А. Мой дом – моя крепость, мое лицо – мой пропуск / А. Прохоров // КомпьютерПресс. – 2000. – 2 июля. [Электронный ресурс]. – Режим доступа: http://www.computerpress.ru/Archive/CP/2000/7/2/

Застосування біометричних технологій найрізноманітніше. Це доступ до робочих місць і мережевих ресурсів, захист інформації, забезпечення доступу відвідувачів до певних ресурсів і побудова систем безпеки. А ведення електронного бізнесу і доступ до електронних інформаційних систем, особливо урядових, можливий тільки після дотримання певних процедур щодо ідентифікації особи. Біометричні технології використовуються в галузі безпеки банківських звернень і транзакцій, інвестування та інших фінансових переміщень, охороні правопорядку, а також у роздрібній торгівлі, питаннях охорони здоров'я й у сфері соціальних послуг, не говорячи про паспортно-візові документи нового покоління.

Відповідно до даних дослідження компанії «Frost & Sullivan» «Аналіз світового ринку прикордонного контролю та біометрії» (Global Border Control and Biometrics Market Assessment), прибутковість ринку в 2012 р. оцінювалась у 5,836 млн доларів США і згідно з прогнозами може сягнути 15,836 млн доларів США до 2021 р.

За словами аналітика «Frost & Sullivan» Кшиштофа Рутковського (Krzysztof Rutkowski), розширення міжнародного співробітництва в галузі забезпечення безпеки пасажирів підштовхує уряди багатьох держав до впровадження систем електронного документообігу. Вищезазначене, своєю чергою, сприяє підвищенню бізнес процесів у аеропортах і службах прикордонного контролю у всьому світі[1].

Електронні документи такі, як електронні паспорти та картки автоматичної системи ідентифікації особи «eGate» дозволяють пасажирам значно зменшити час, необхідний для проходження прикордонного контролю. Ця методика показала себе як економічно ефективна, тому необхідно очікувати інтенсивного запровадження подібних технологій в аеропортах і транспортних вузлах усього світу. Нині багато західних країн уже впровадили технології електронних паспортів і систем ідентифікації «eGate».

Згодом там, де буде необхідна персональна ідентифікація, біометричні системи активніше будуть застосовуватися у всіх сферах нашого життя. У майбутньому використання біометрії окремо або в симбіозі з смарт-картками, ключами й електронними підписами застосовуватимуться у всіх сферах економіки і приватного життя людини.

1.3. Сучасні уявлення про біометрію, біометричні технології та біометричні характеристики. Біометричні системи ідентифікації за біологічними ознаками людини та критерії оцінки їх надійності

Стрімко запроваджуючись, нові технології змінюють звичні значення начебто досить сталих і відомих термінів. Як уже зазначалось, ще недавно термін «біометрія» мав набагато ширше тлумачення і належав в основному до методів математичної статистики, які застосовувались до будь-яких біологічних явищ. Нині його значення стало вужчим. *Сучасне поняття «біометрія» – це методи автоматичної ідентифікації людини і підтвердження її особистості (персоналізації), засновані на фізіологічних або поведінкових*

[1] Биометрические системы пограничного контроля: новый прогноз. – 2013. – 10 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/biometricheskie_sistemi_pogranichnogo_kontrolja_novii_prognoz/.

характеристиках конкретної особи. Тобто під біометрією нині розуміють вимірювання унікальних фізіологічних (фізичних) і поведінкових характеристик індивідуума для його розпізнання або посвідчення особи.

Біометричне розпізнавання індивідуума полягає у порівнянні фізіологічних чи психологічних особливостей суб'єкта, який перевіряється, з його раніше знятими характеристиками, що розміщені в електронному вигляді у спеціальних базах даних біометричних систем (архівах) або в спеціальних документах (картках). Головна мета біометричної ідентифікації полягає у створенні такої системи реєстрації, яка б вкрай рідко відмовляла у доступі легітимним користувачам і водночас повністю виключала несанкціонований прохід осіб до режимних приміщень (територій), а також регламентувала відповідний доступ до комп'ютерних сховищ інформації. Загальноприйнято, що порівняно з смарт-картками, токенами і паролями біометричні системи забезпечують набагато надійніший захист, адже власні фізіологічні та поведінкові характеристики індивідуума не можна ані забути, ані втратити[1].

У XXI сторіччі більшого значення набуває ідентифікація особистості індивідуума – споживача інформації. Звідси – величезний інтерес до біометричних технологій як до одного з засобів санкціонованого доступу та ідентифікації користувача у локальних відомчих інформаційних мережах і базах даних, але не тільки. Адже біометрія – це наука, яка досить активно розвивається та є однією з найперспективніших інформаційних технологій.

Біометричні рішення дуже швидко стають популярними у найрізноманітніших сферах життя сучасного світового співтовариства: паспортно-візових документах нового покоління, охороні правопорядку, різних фінансових і платіжних системах, наданні соціальних послуг, організації супроводу авіапасажирів, які часто мандрують, і дедалі більше поширюються в таких галузях, як освіта, охорона здоров'я, «електронне врядування» тощо. Нині сферою, де очікується найбільше використання біометричних технологій розпізнавання фізичних осіб, є виробництво смартфонів і портативних, і мобільних комп'ютерних пристроїв (ноутбуків, планшетів).

Причини популярності біометричних технологій – їх досить висока надійність, безпека, ефективність, комфортність. На відміну від інших дозвільних технологій, біометрія працює з конкретною особою і виокремлює суто її індивідуальні ознаки – інакше біометричні рішення просто не змогли б діяти.

У широкому розумінні біометрія – вимірювання унікальних фізичних або поведінкових характеристик будь-якого індивідуума. У вузькому розумінні (який зараз в основному й використовується) у це поняття включають технології та системи автоматичної ідентифікації людини та підтвердження її особистості, які засновані на аналізі унікальних біометричних параметрів та їх порівняння з наборами еталонних параметрів, які зберігаються в спеціально створених базах даних[2].

Найпоширеніші біометричні методи вимірювання фізичних параметрів включають одержання відбитків пальців, зняття характеристик рис обличчя та райдужної оболонки ока, термограм кисті (долоні) або пальця (так звані статичні характеристики)[3]. До поведінкових характеристик (так звані динамічні характеристики) належать особли-

[1] Шаров В. Биометрические методы компьютерной безопасности / В. Шаров // Bytemag.ru. – 2005. – № 4. –13 апреля. [Электронный ресурс]. – Режим доступа: http://bytemag.ru...

[2] Технологии // BioLink. – 2008. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology

[3] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art103.html.

вості поведінки або характерні риси, що з часом змінюються, тобто сам підпис і динаміка підпису, голос (що має також і фізичну складову), особливості роботи з клавіатурою (динаміка натиснення на клавіші) та хода. Низка ідентифікаційних параметрів і технологій, що розроблені на їх основі, набули більшого поширення, ніж інші, проте загалом те, що біометрія отримала визнання у галузі ідентифікації індивідуумів і контролю доступу, не підлягає сумніву[1].

Усі фізіологічні та поведінкові характеристики класифікують за видами біометричних даних. Вибраний вид біометричних даних визначає конкретну біометричну технологію, яку будуть застосовувати. Станом на кінець 2003 року офіційно було зареєстровано 19 методів розпізнавання (можливе розширення цього списку під час затвердження такої версії формату): комбінації методів і методи, які засновані на розпізнаванні форми обличчя, голосу, відбитків пальців, сітківки ока, райдужної оболонки ока, геометрії кисті руки, долоні та пальця, динамік підпису і клавіатурного набору, руху губ, термографій обличчя, кисті і пальця, ходи, запаху тіла, ДНК, форми вуха, малюнка вен на руці або пальці[2].

Біометрія працює на основі унікальних і вимірювальних характеристик людини, які придатні для автоматичної ідентифікації чи верифікації. Термін «автоматично» означає, що біометричні технології повинні розпізнавати або верифікувати особу автоматично та досить швидко в режимі реального часу. Ідентифікація за допомогою біометричних технологій вимагає порівняння раніше внесеного в інформаційну базу даних електронного біометричного зразка з біометричними даними, які щойно були отримані або передані[3].

Всі біометричні системи працюють практично за однаковою схемою. По-перше, система запам'ятовує зразок біометричної характеристики (ця дія називається процесом запису).

Під час формування еталонного зразка для запису в більшості біометричних систем необхідно декілька разів здійснити процедуру зняття вибраної біометричної характеристики для того, щоб отримати найточніше зображення зразка контрольного ідентифікатора. Потім зібрана інформація обробляється і перетворюється на математичний код.

Крім того, система може «попросити» провести ще деякі дії задля того, щоб «прописати» біометричний зразок до конкретного індивідуума. Наприклад, персональний ідентифікаційний номер (PIN) прикріпляється до певного зразка, або смарт-картка, що містить зразок, вставляється у зчитувальний пристрій. У такому разі зразок знятої біометричної характеристики порівнюється з існуючим зразком і додатковими ідентифікуючими даними.

Ідентифікація в будь-якій біометричній системі проходить чотири стадії:

– запис – фізичний або поведінковий зразок запам'ятовується системою;

– виокремлення – унікальна інформація (характерні ознаки) виокремлюються з відзнятого/их/ зразка/ів/ і аналізуються системою;

– порівняння – отриманий зразок порівнюється з наявним еталонним зразком;

---

[1] Бирман Н. Перекрестная биометрия / Н. Бирман // Security News: Газета международных новостей по техническим средствам и системам безопасности. – 2006. – 15 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Задорожный В. Иерархия биометрических стандартов / В. Задорожный // Pcweek.ru. – 2003. – 18 ноября. [Электронный ресурс]. – Режим доступа: http://www.pcweek.ru/themes/detail...

[3] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art103.html.

– збігання/незбігання – система визначає, чи збігаються представлені біометричні зразки, і ухвалює відповідне рішення[1].

Нині існує безліч методів біометричної аутентифікації та ідентифікації, які поділяються на дві групи методів: ***статичні*** та ***динамічні.***

Статичні методи біометричної аутентифікації ґрунтуються на фізіологічній (статичній) характеристиці фізичної особи, тобто унікальній характеристиці, яка надана їй від народження, яка є невід'ємною складовою індивідуума і яка не змінюється з часом. Це такі методи, які засновані на розпізнанні:

Відбитка пальця. В основі цього методу є унікальність для кожної людини малюнка папілярних узорів на його пальцях. Відбиток, знятий за допомогою спеціального сканера, перетворюється на цифровий код (згортку), і порівнюється зі збереженим контрольним еталонним зразком, який був отриманий раніше. Апаратно-програмна технологія, яка використовує папілярні узори пальців, була, є і залишається найпоширенішою за обсягом продажу на ринку порівняно з іншими методами біометричної аутентифікації.

Форм долоні (геометрія долоні, кисті руки або пальця – використовується в доволі вузькому сегменті ринку). Цей метод ґрунтується на суто індивідуальній геометрії долоні, кисті руки або пальця. За допомогою спеціального пристрою, що складається з камери і декількох підсвічувальних діодів (включаючись по черзі, вони дають різні проекції об'єкта), вибудовується тривимірне зображення долоні (кисті руки або пальця), за яким формується згортка і відбувається розпізнавання індивідуума.

Малюнка вен на долоні або пальці руки (відповідна технологія стає більш поширеною, але, зважаючи на досить високу вартість необхідного обладнання, поки що не значно поширилася). За допомогою інфрачервоної камери зчитується малюнок вен на лицьовій стороні долоні (кисті руки) або пальця, отримане зображення обробляється і за схемою розташування вен формується відповідна цифрова згортка.

Райдужної оболонки ока. Малюнок райдужної оболонки ока є унікальною характеристикою людини, причому для її сканування достатньо портативної камери та спеціалізованого програмного забезпечення, за допомогою якої сканується відповідна частина обличчя і виділяється зображення ока, з якого відокремлюється малюнок райдужної оболонки і формується відповідний цифровий ідентифікаційний код людини. Розповсюдження технології ідентифікації за райдужною оболонкою ока стримувалося патентними обмеженнями фірм виробників і досить високою ціною необхідного устаткування.

Сітківки ока. Це спосіб ідентифікації за малюнком кровоносних судин очного дна. Для того, щоб цей малюнок став видимим і його можно було зафіксувати, людині потрібно подивитися на віддалене світлове джерело-цятку, і тоді очне дно, що підсвічується, сканується спеціальною камерою.

Нині цей спосіб із низки причин майже не застосовується для ідентифікації.

За формою обличчя. У цьому методі ідентифікації формується двовимірне або тривимірне зображення обличчя людини. На обличчі виокремлюються контури брів, очей, носа, губ і т. д., вираховується відстань між ними і формується не просто образ обличчя, а ще досить багато його варіантів на випадки повороту обличчя або нахилу, а також змін виразу. Кількість образів формується і записується у базу даних залежно від мети використання цього способу (для аутентифікації, верифікації, віддаленого пошуку на великих територіях тощо). Необхідно зазначити, що нині у друкованих джерелах цей статичний

[1] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art103.html

метод поділяють на два самостійні: форма і геометрія обличчя (з цими ідентифікаторами працюють технології розпізнавання двовимірних зображень лиця, які отримуються з фотографій і відеоряду, – так званий 2-D метод) і форма та побудова черепа (компанії, які працюють у цій сфері, вважають перспективнішою технологію розпізнавання людини за тривимірною моделлю обличчя – так званий 3-D метод)[1].

Термограмі обличчя, термографії руки або пальця (засновані на використанні цих ідентифікаторів технології застосовуються в основному у банківській сфері та не отримали поки що поширення).

Основою цього способу аутентифікації є унікальність розподілу на кожній частині людського тіла артерій, які забезпечують постачання крові на вибрану ділянку шкіри та формують на ній специфічний тепловий фон. Для отримання термограм використовуються спеціальні камери інфрачервоного діапазону. Цей метод дозволяє розрізнити навіть близнят.

ДНК. Переваги цього способу загальновідомі, проте нині використовувані методи отримання й обробки ДНК досить трудомісткі й довготривалі (поки що відсутня можливість роботи у режимі реального часу), тому системи, які застосовують цей метод, в основному використовуються тільки для спеціалізованих експертиз.

За допомогою інших методів. Окрім наведених методів, існують ще інші унікальні способи – аутентифікація за піднігтьовим шаром шкіри, за кількістю відібраних для сканування пальців, формою вуха, запахом тіла та низкою інших характеристик. Але головним недоліком усіх цих не дуже поширених способів є те, що автоматичних систем і баз даних для можливого масового розпізнавання індивідуумів, які використовували б ці ідентифікатори, практично ще не створено. Насамперед це стосується аутентифікації за запахом тіла і формою вуха.

Динамічні методи аутентифікації ґрунтуються на аналізі поведінкових характеристик особи – особливостей, властивих кожному індивідуумі під час виконання будь-яких рухливих дій. Вони побудовані на особливостях, характерних для підсвідомих рухів під час відтворення будь-якої дії. Динамічні методи істотно поступаються статичним у точності й ефективності, тому, як правило, використовуються як допоміжні або додаткові.

Методи аутентифікації цієї групи такі:

За рукописним почерком. Як правило, для цього виду аутентифікації або ідентифікації фізичної особи використовується її підпис (іноді написання кодового слова). Цифровий ідентифікаційний код формується залежно від необхідного ступеня захисту і наявності необхідного устаткування (графічний планшет, екран кишенькового комп'ютера тощо).

Ідентифікація за рукописним почерком буває двох типів:

– за самим підписом, тобто для ідентифікації використовується просто ступінь збігу двох картинок;

– за динамічними характеристиками написання підпису (динаміка підпису), тобто для ідентифікації формується цифрова згортка, в яку входить інформація за безпосередньо часовим режимом підпису, тобто часовими характеристиками ставлення підпису і статистичними характеристиками динаміки натискання на поверхню матеріалу, на якому ставиться підпис.

[1] Общая характеристика биометрических технологий. Основные группы биометрических идентификаторов и технологий. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/biometric.php

За клавіатурним почерком (динаміка клавіатурного набору). Метод загалом аналогічний попередньому, але замість підпису використовується набір якогось кодового слова (коли для цього застосовується особистий пароль користувача, таку аутентифікацію називають двофакторною) і не потребує зовні жодного спеціального устаткування, окрім переобладнаної і дооснащеної стандартної клавіатури.

Основною харатеристикою, за якою формується згортка для ідентифікації, є динаміка набору кодового слова.

За голосом. Одна з найстаріших технологій, нині її розвиток вийшов на новий рівень, оскільки виникла потреба її більш ширшого використання. Існує багато способів формування кодів ідентифікації за голосом, але, як правило, це різні поєднання частотних і статистичних характеристик голосу.

За допомогою інших методів. Окрім вищеперелічених найпоширеніших динамічних методів, існують ще такі унікальні способи, як: ідентифікація за рухом губ під час відтворення кодового слова, за ходою, за динамікою повороту ключа в дверному замку тощо.

Узагальнюючими характеристиками всіх методів і способів біометричної ідентифікації й аутентифікації є суто статистичні кількісні показники: наявність помилок «першого роду» (не пустити в систему «свого») і помилок «другого роду» (допустити в систему «чужого»).

Сортувати і порівнювати описані біометричні методи за показниками помилок першого роду дуже складно, оскільки вони надто різняться через високу залежність від якості апаратури, що використовується, на якій вони реалізовані, причому навіть для одних і тих же методів.

За показниками помилок другого роду (можливість допущення в систему «чужого») загальне сортування найпоширеніших методів за якістю біометричної аутентифікації виглядає так (від кращих до гірших):

– ДНК;
– райдужна оболонка ока, сітківка ока;
– відбиток пальця, термографія обличчя, форма долоні;
– форма обличчя, розташування вен на кисті руки і долоні;
– підпис;
– клавіатурний почерк;
– голос.

Необхідно наголосити, що статичні методи ідентифікації набагато якісніші, ніж динамічні, але водночас значно дорожчі. Сегментація біометричного ринку за 2007 рік за поширенням використання біометричних ідентифікаторів наведена на мал. 1. Слід зазначити, що і нині ця картина суттєво не змінилася.

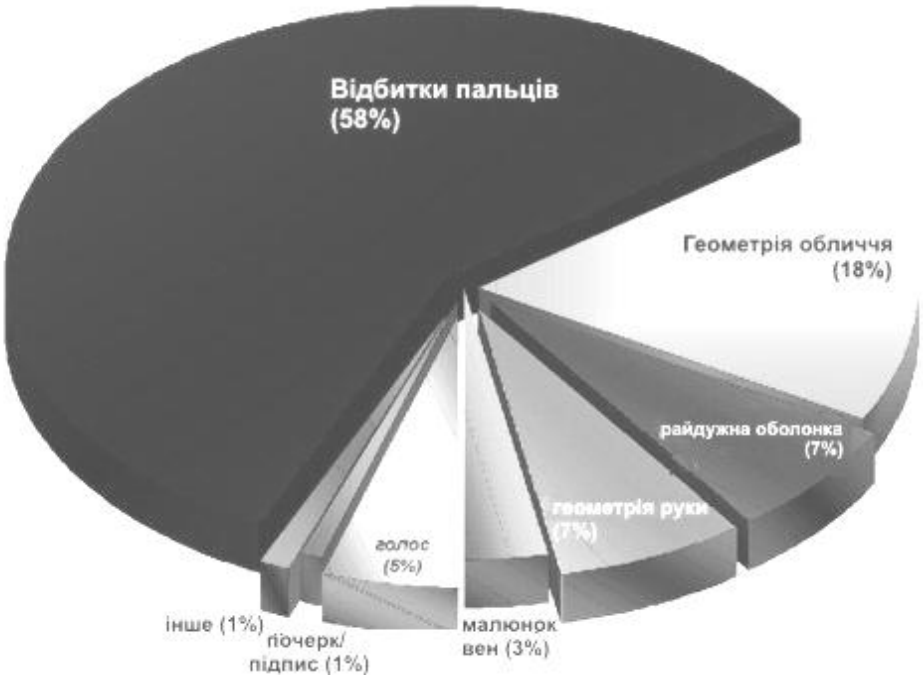
Нагадаємо ще раз чотири основні етапи, які використовуються під час реалізації всіх біометричних технологій ідентифікації:

– реєстрація ідентифікатора (запис) – збір відомостей про фізіологічну або поведінкову характеристику, що надалі перетворюється у форму, котра доступна комп'ютерним технологіям та яка вноситься в пам'ять біометричної системи;

– виокремлення – з ідентифікатора, що пред'являється індивідуумом для контролю, формуються та виокремлюються унікальні ознаки, які аналізуються системою;

– порівняння – зіставляються відомості про той, який пред'являється, та раніше зареєстрований ідентифікатори;

– ухвалення рішення – ухвалення висновку про збігання або незбігання того, що пред'являється, та раніше зареєстрованого ідентифікатора.



Мал. 1. Сегментація біометричного ринку за 2007 рік за поширенням використання біометричних ідентифікаторів (дані компанії «Acuity Market Intelligence»)

Висновок про збігання/незбігання ідентифікаторів може надалі транслюватися іншим системам (контролю доступу, захисту інформації тощо), які надалі свій алгоритм дій реалізують залежно від отриманої інформації про збігання/незбігання отриманих параметрів біометричного/их/ ідентифікатора/ів/ з шаблоном/ами/, які зберігаються в пам'яті систем[1].

Біометричні ознаки – це чіткі, індивідуальні, біологічно обумовлені характеристики кожної людини. У принципі не існує двох людей із абсолютно однаковими біометричними ознаками. Необхідно зазначити, що різні біометричні методи ідентифікації дуже сильно залежать від мети призначення і сфери застосування. Поки що тільки три біометричні методи довели свою масову практичність: розпізнавання за відбитками пальців, райдужною оболонкою очей та за рисами обличчя (2D і 3D-методи)[2].

Основна функція будь-якого біометричного пристрою – розпізнавання індивідуума. Але контроль за доступом вимагає не тільки ідентифікації особи: система може також відмикати двері, дозволяти або забороняти доступ залежно від часу доби і за необхідності включати сигнал тривоги. Як правило, біометричні системи виконують ці завдання різними способами.

Порівняно з традиційними біометричні методи ідентифікації особи мають низку переваг, а саме:

– біометричні ознаки дуже складно фальсифікувати;

– через унікальність біометричних ознак достовірність ідентифікації дуже висока;

[1] Технологии. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp?group...

[2] Общая характеристика биометрических технологий. Основные группы биометрических идентификаторов и технологий. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/biometric.php…

– біометричний ідентифікатор не можна забути, як пароль, або втратити, як пластикову картку.

Найважливіший чинник успіху біометричної системи – це її сприйняття користувачами. Воно, своєю чергою, залежить від декількох факторів. По-перше, скануючий пристрій не повинен викликати у користувача відчуття занепокоєння або дискомфорту. Можливо, це суб'єктивний показник, але він дуже важливий для розуміння проблем користувачів. Якщо люди будуть боятися використовувати пристрій, то, швидше за все, вони поводитимуться з ним не так, як треба, а в підсумку можуть не пройти контроль, тобто не отримати право доступу. По-друге, біометричний пристрій має бути досить простим у використанні. Клієнтам до вподоби пристрої, з якими легко працювати. По-третє, біометричний пристрій повинен функціонувати надійно, чітко і точно.

Проте жоден пристрій не може бути абсолютно досконалим, і біометричні системи – не виняток, вони теж можуть допускати помилки. Як уже зазначалось, можливість помилок оцінюється рівнем помилкових відмов і хибних допущень, тобто показниками надійності біометричних систем є вірогідність помилок першого і другого роду. Помилки першого роду визначають вірогідність помилкової відмови і виникають у разі відмови в доступі легальному користувачеві системи. Помилки ж другого роду (хибних допущень) показують вірогідність помилкового допуску і виникають під час надання доступу сторонній особі. Існуючі сучасні біометричні системи поки що мають достатньо широкий розкид цих характеристик.

Біометричну систему також можна характеризувати рівнем однакової ймовірності помилок першого і другого роду – точкою, в якій вірогідність помилки першого роду дорівнює вірогідності помилки другого роду. На підставі рівня однакової ймовірності помилок і робляться висновки про відносні переваги та недоліки різних біометричних методів. Чим нижчий рівень вірогідності помилок, тим ліпше. Наприклад, рівень в один відсоток означає, що з 100 спроб розпізнавання особи лише один раз їй буде помилково відмовлено або помилково дозволено у доступі.

Існує ще один параметр, на який обов'язково необхідно зважати під час вибору й установки біометричної системи: її пропускна спроможність. По суті, це час, який потрібен людині для контакту з скануючим пристроєм та здійснення процедури її розпізнання.

Роблячи вибір системи контролю доступу на основі біометричних методів ідентифікації особистості, окрім декларованої надійності та ціни, необхідно зважати і на такий чинник, як сумісність з уже існуючими системами, які використовуються.

Розглядаючи конкретну біометричну ідентифікаційну систему контролю доступу до інформаційно-обчислювальних ресурсів, необхідно переконатися в коректності її роботи з наявним устаткуванням і програмним забезпеченням (ПЗ), а також проаналізувати можливість її сумісності з уже використовуваними системами захисту, якщо такі є.

Крім того, потрібно оцінити наскільки прийнятна система для користувачів, які будуть її використовувати. Під прийнятністю для користувача в цьому випадку розуміється його особисте ставлення до процесу аутентифікації або ідентифікації. Так, відживаюча процедура взяття відбитків пальців на паперовий носій здебільшого може розглядатися як щось принизливе, що викликає асоціації з застосуванням такої процедури в криміналістиці. Із цього погляду ідентифікація за відбитками пальців руки за допомогою сканера виглядає набагато привабливішою.

Суттєвим параметром під час вибору практично будь-якої системи ідентифікації є швидкість проведення реєстрації та верифікації абонентів. Більшість пропонованих на ринку систем виконують аутентифікацію і/або ідентифікацію в реальному масштабі часу.

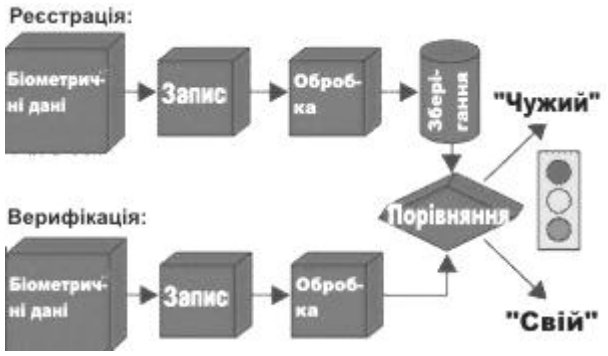
Тривалість реєстрації нового абонента від декількох десятків секунд до декількох хвилин також прийнятна, оскільки ця процедура виконується раз.

Сучасна біометрична ідентифікаційна система повинна бути багаторівневою й охоплювати комплекс не тільки технічних, але й адміністративних рішень. Найліпші результати досягаються, коли розпізнання особи проводиться і біометричними, і традиційними методами. Чим більше вихідних даних, тим більший потенціал розвитку систем безпеки, але у будь-якому випадку біометрія є основною складовою для досягнення оптимального рішення.

Один із способів, що набуває дедалі більшої популярності, – розпізнання рис зовнішності індивідуума. Люди легко впізнають один одного за обличчям, але автоматизувати таке розпізнання не так уже й легко. Необхідне для ідентифікації зображення отримують за допомогою фотографування, використання вже наявних фотозображень чи записів відеокамер спостереження. Тільки у США і Німеччині над технологіями розпізнавання за рисами (формою) обличчя працюють декілька десятків компаній, яким виділяються спеціальні урядові гранти або субсидії. Спочатку результати розробок використовувалися виключно для потреб спецслужб, але згодом вони почали застосовуватись і для комерційних цілей.

Сучасні впізнавальні технології дозволяють сканувати людські обличчя і проводити їх розпізнання у режимі реального часу. На відміну від інших біометричних технологій (ідентифікації за відбитками пальців, райдужної оболонки ока або за голосом) система розпізнавання за рисами обличчя не вимагає безпосереднього контакту з людиною, особа якої встановлюється. Непотрібно знімати відбитки пальців, дивитися в об’єктиви спеціальних камер або вимовляти якісь контрольні слова. Використання будь-якої біометричної ознаки має свої переваги і недоліки. Тому в жодному випадку не можна очікувати, що який-небудь окремий метод здобуде пріоритетне визнання. Більшість експертів вважають, що споживач залежно від вимог завдання повинен сам зробити вибір конкретного методу або потрібної комбінації методів[1].

Будь-яка біометрична ідентифікаційна система повинна мати можливість розпізнавання за наявним шаблоном і встановлювати за його допомогою автентичність конкретних фізіологічних або поведінкових характеристик користувача. Цілком логічно, що будь-яку біометричну систему (мал. 2) поділяють на дві частини: модуль реєстрації і модуль верифікації (ідентифікації).



Мал. 2. Блок-схема біометричної системи

[1] Борзенко А. Биометрические системы распознавания внешности / А. Борзенко // Платформы и технологии. – 2002. – № 11. – 10 декабря. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

Модуль реєстрації відповідає за те, щоб система навчилася ідентифікувати конкретну людину. На етапі реєстрації біометричні датчики сканують її необхідні фізіологічні або поведінкові характеристики, перетворюючи їх у електронний цифровий вигляд. Спеціальний модуль обробляє цю отриману електронну цифрову послідовність для того, щоб виокремити характерні особливості та згенерувати їх у компактне електронне представлення (шаблон). Для зображення обличчя такими характерними особливостями можуть бути розміри і відомості про відносне розташування очей, носа і рота. Електронний шаблон для кожного користувача зберігається в базі даних біометричної системи.

Модуль верифікації (аутентифікації) відповідає за розпізнавання людини. На цьому етапі біометричний датчик знімає та реєструє відповідні характеристики людини і перетворює ці характеристики в той цифровий формат, в якому зберігається контрольний шаблон. Отриманий шаблон для проведення верифікації порівнюється з тим, що зберігається, для того, щоб визначити, чи збігаються ці шаблони. Наприклад, під час використання у процесі аутентифікації технології ідентифікації за папілярними узорами пальців установчі дані (ім'я) користувача попередньо вводяться та зберігаються в пам'яті модуля попередньої реєстрації, а відбиток пальця, отриманий унаслідок сканування під час проходження процедури контролю, замінює пароль. Ця технологія використовує установчі дані (ім'я) користувача як покажчика для отримання облікового запису абонента системи, який зберігається, та перевірки відповідності «один до одного» (аутентифікація або верифікація) між шаблоном, отриманого під час верифікації параметрів біометричного показника, і вже наявним для цього імені користувача шаблоном. У іншому випадку (процедура ідентифікації) шаблон параметра біометричного показника, що пред'являється, зіставляється з усім набором шаблонів, що зберігаються[1].

За всього теоретичного різноманіття можливих біометричних методів на практиці їх застосовується небагато. Нині найпоширенішими є три методи: розпізнавання за відбитками пальця, за зображенням обличчя (двовимірний або тривимірний /2D або 3D/) та за райдужною оболонкою ока. Як приклад, розглянемо і порівняємо основні якісні характеристики цих біометричних методів (див. табл. 1), наведених співробітниками російських НВО «Інформація» і «A4Vision» А. Вакуленком та А. Юхиним[2].

Таблиця 1

Характеристики трьох основних біометричних методів

Система розпізнавання	Універсальність	Унікальність	Перманентність	Вимірність	Стійкість до навколишнього середовища	Стійкість до підробок	Соціальна прийнятність	Точність
Райдужна оболонка	Добре	Відмінно	Відмінно	Погано	Добре	Погано	Погано	Добре
Палець	Добре	Добре	Добре	Погано	Погано	Погано	Погано	Добре
Обличчя (3D)	Відмінно	Добре	Добре	Добре	Добре	Відмінно	Відмінно	Добре
Обличчя (2D)	Відмінно	Погано	Погано	Добре	Погано	Погано	Відмінно	Погано

[1] Шаров В. Биометрические методы компьютерной безопасности / В. Шаров // Bytemag.ru. – 2005. – № 4. – 13 апреля. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

[2] Вакуленко А. Биометрические методы идентификации личности: обоснованный выбор / Андрій Вакуленко, Артем Юхин // BYTE/Россия. – 2006. – 16 января. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

Для порівняння використовуються ті критерії, яким повинен тією чи іншою мірою відповідати будь-який біометричний метод.

Розглянемо докладніше кожен із критеріїв.

Універсальність. Кожна людина повинна володіти тією характеристикою, яка потрібна для цього біометричного методу. Насправді кожен метод має обмеження, оскільки декотрі індивідууми, які мають певні вади, в принципі не можуть їх використовувати (наприклад, ті особи, у кого немає пальця або ока).

Унікальність (розрізнюваність). На відміну від аутентифікації користувачів за паролями або унікальними цифровими ключами, біометричні технології завжди вірогідні, оскільки постійно зберігається незначний шанс, що у двох людей із низки причин під час розпізнавання можуть збігатися порівнювані біологічні характеристики. Через це в біометрії запроваджені та використовуються низка важливих ключових термінів:

FAR (False Acceptence Rate) – відсотковий поріг, що визначає вірогідність того, що одна людина може бути прийнята за іншу. Величина, яка дорівнює 1, в FAR називається специфічністю.

FRR (False Rejection Rate) – вірогідність того, що людина може бути не розпізнана системою. Величина, яка дорівнює 1, в FRR має назву чутливості.

Verification (Верифікація) – порівняння двох біометричних шаблонів один до одного.

Identification (Ідентифікація) – ідентифікація біометричного шаблону людини серед наявної вибірки інших шаблонів. Тобто ідентифікація – це завжди порівняння одного до багатьох.

Biometric template (Біометричний шаблон). Набір даних, як правило, в закритому двійковому форматі, що створюється біометричною системою на основі характеристики, що аналізується. Існує спеціальний стандарт **CBEFF** для структурного обрамлення біометричного шаблону[1].

Загальновідомо, що біометрична характеристика не може бути однаковою у двох різних людей. **Унікальність** визначається як мінімальне досяжне для цього типу біометрії значення FAR (False Acceptance Rate) – ймовірність помилкового розпізнавання, тобто вірогідність того, що система зможе сплутати двох індивідуумів, визнавши «чужого» за «свого».

На практиці зменшення FAR завжди призводить до зменшення чутливості методу або, що еквівалентно, до збільшення FRR (False Rejection Rate) – ймовірності помилкового невпізнавання, тобто до того, що система не розпізнає відомого їй суб'єкта. Так мінімальне досяжне значення FAR відповідає дуже високому значенню FRR і не є показовим значенням.

Перманентність. Біометрична характеристика не повинна змінюватися з часом (так зване старіння біометричного шаблону). Оцінити перманентність біометричного методу можна залежністю FRR (за фіксованого значення FAR) від часу між тестами, проведеними на одній і тій же вибірці індивідуумів.

Вимірність. Її можна кількісно оцінити величиною FTE (Failure to enroll) – відсотком індивідуумів, які не змогли пройти реєстрацію (система не змогла сформувати їхні біометричні шаблони), і середнім часом розпізнавання (recognition time). Під часом розпізнавання мається на увазі час верифікації або ідентифікації, залежно від режиму, в якому працює система.

[1] [Електронний ресурс]. – Режим доступу: http://ru.wikipedia.org/wiki/

Під час вирішення завдань контролю доступу, особливо на транспорті, час розпізнавання безпосередньо визначає швидкість людського потоку через контрольований прохід. FTE визначає той відсоток людей, які не зможуть скористатися послугами системи, тобто будуть відсіюватися (не пропускатися) і, відповідно, блокувати прохід. Сюди належать і ті випадки, коли в індивідуумів потрібна біометрична характеристика відсутня (див. «Універсальність»), але це такі випадки, коли потрібний біометричний параметр є в наявності у особи, але з тих або інших причин його вимірювання на обладнанні, що використовується, неможливе або суттєво ускладнене.

Для багатьох людей можуть виникнути труднощі із розпізнаванням за відбитком пальця – для працівників, які працюють фізично, осіб із не чіткими та стертими папілярними узорами, для літніх людей із сухою шкірою або індивідуумів із дерматологічними дефектами. Крім того, через постійний контакт скануючі пристрої відбитків пальців можуть просто забруднюватися і, як наслідок, давати збої.

Стійкість до навколишнього середовища. Біометричний метод повинен бути стійким до змін навколишнього середовища. Експлуатаційні якості різних біометричних методів суттєво залежать від умов оточуючого середовища в місці експлуатації скануючих пристроїв і можуть погіршувати стабільність своїх характеристик у разі зміни цих умов. Так, у сканерів відбитків пальців у разі забруднення контактного місця значно погіршується якість їх роботи, двовимірні методи розпізнавання обличчя занадто залежать від зовнішнього освітлення тощо.

Стійкість до підробки. Біометрична система повинна бути стійкою до можливих підробок біометричних параметрів, що вимірюються. Це призводить до несанкціонованого доступу. Систему розпізнавання за двовимірним (2D) зображенням обличчя можна легко «обдурити», пред'явивши їй якісну фотографію «конкретної» особи з числа «знайомих системі».

Для отримання несанкціонованого доступу за відбитком пальця буває достатньо просто подихати на залишений на контактному місці сканера попереднім індивідуумом відбиток пальця або нанести графітову пудру і натиснути на місце контакту через тонку плівку.

Соціальна прийнятність. Згода суспільства на збір і використання тих чи інших біометричних даних є необхідною умовою для масового запровадження біометричних методів у повсякденному житті. Існують різні причини, за якими збір і зберігання певних біометричних характеристик може стати неприйнятним для суспільства. Наприклад, зняття відбитків пальців на паперовий носій традиційно асоціюються з розслідуванням злочинів. Для багатьох істотним є і те, що розпізнавання за папілярними узорами пальців (контактний спосіб) вимагає дотику до контактого місця сканера, якого перед тим торкалися інші особи.

Ще один серйозний недолік сканування за відбитками пальців – можливість їх крадіжки і використання не тільки для несанкціонованого доступу, але і для фальсифікації доказів. Основне заперечення проти використання методу розпізнавання за райдужною оболонкою ока пов'язане з можливостями іридодіагностики й отриманням тим самим приватної інформації щодо хвороб людини.

Двовимірна фотографія обличчя індивідуума є найбільш прийнятною для суспільства, оскільки є безконтактним і найтрадиційнішим способом ідентифікації особи. Тривимірна цифрова фотографія у цьому сенсі нічим не відрізняється від звичайної, але набагато підвищує точність автоматичної ідентифікації. Зовнішність людини, на відміну від інших характеристик, – її найбільш природний ідентифікатор, який може використовуватися оператором-людиною для перевірки рішення, ухваленого комп'ютером.

Точність. Будь-яку біометричну систему можна налаштувати на різний ступінь «пильності», тобто на різне значення ймовірності помилкового розпізнавання FAR. Водночас, як вже згадувалося, чим нижче значення FAR, тобто чим пильніша система, тим вища вірогідність помилкового нерозпізнавання FRR (система стає менш чутливою). Залежно від конкретного завдання система налаштовується на певний компроміс між допустимими значеннями FAR і FRR, або, як їх прийнято називати в теорії статистичних рішень, помилками 1-го і 2-го роду[1].

У низці країн із метою організації та регулювання використання біометричних характеристик ухвалюються спеціальні нормативні документи. Прикладом такого нормативного акту, який був ухвалений весною 2009 року на теренах Співдружності Незалежних Держав (СНД), може слугувати Постанова Кабінету Міністрів Азербайджану «Правила організації і регулювання діяльності біометричних інформаційних служб за видами надання біометричних послуг».

Відповідно до затверджених правил, повинні бути створені відповідні стандарти послуг, що надаються. В Азербайджані до біометричних інформаційних відомостей включені ідентифікація зовнішності, ідентифікація та дактилоскопічна реєстрація відбитків пальців і долонь, ідентифікація за голосом, його аналіз і конвертація, ідентифікація й аналіз почерку та підпису на папері, аналіз і ідентифікація за ДНК, організація контролю і безпеки за індивідуальним ідентифікаційним номером, ідентифікація й аналіз за райдужною оболонкою ока.

Також у документі відображено методи і форми організації служб з обробки біометричної інформації, процедури їх здійснення, організація безпеки послуг, що надаються, та ін.[2]

1.4. Поняття ідентифікації й аутентифікації (верифікації) фізичних осіб

Нині існує безліч біометричних систем, які використовуються на різних рівнях і призначені для виконання різноманітних практичних завдань. Водночас усі біометричні системи, як правило, поділяються на *ідентифікаційні* та *верифікаційні.* Тобто в біометрії розмежовують поняття термінів *«ідентифікація»* і *«верифікація» (аутентифікація).*

У випадку *ідентифікації* система встановлює, кому належить цей зразок, порівнюючи його з наявними шаблонами у базі даних для того, щоб здійснити пошук шляхом відповідності «один з багатьох» (цей процес називають відповідністю «один до багатьох»).

Верифікація (аутентифікація) – це порівняння, за якого біометрична система намагається аутентифікувати (верифікувати) особистість людини, тобто встановлення достовірності шляхом порівняння «один до одного». У цьому випадку отриманий біометричний зразок порівнюється з раніше отриманим і таким, що зберігається, взірцевим

[1] Вакуленко А. Биометрические методы идентификации личности: обоснованный выбор / Андрій Вакуленко, Артем Юхин // BYTE/Россия. – 2006. – 16 января. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

[2] В Азербайджане утверждены правила обработки биометрической информации // Ru.apa.az.. – 2009. – 6 апреля [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

зразком. Порівнюючи ці два зразки, система повинна дати відповідь на питання, чи дійсно пред'явник є тією особою, за кого він себе видає.

У процесі ідентифікації система порівнює один зразок із багатьма, що зберігаються у спеціальному сховищі або базі даних (БД), тоді як під час аутентифікації або верифікації порівнює отриманий зразок із тим, що конкретно зберігається, тобто один до одного. Для простішого розуміння можна образно уявити, що ідентифікаційна система ставить питання «Ви хто?», а система верифікації ж питає «Ви дійсно той, за кого себе видаєте?»[1].

Перед тим, як перевіряти істинність (правдивість) користувача, його потрібно ідентифікувати (з'ясувати, «хто є хто»), тобто з багатьох користувачів, зареєстрованих у системі, вибрати за унікальним ідентифікатором одного. Його система і буде дійсно перевіряти. Ідентифікатор – це ім'я (установчі дані), під яким(и) зареєстрований користувач у комп'ютерній системі, яка його перевіряє.

Інакше кажучи, ідентифікація користувача – це отримання відповіді на питання «Хто ти?» А аутентифікація – це вимога «А зараз доведи по суті, що ти саме той користувач, за якого себе видаєш» та подальша перевірка наданих доказів. Тобто перевірка, чи дійсно користувач є тією особистістю, за яку він себе видає.

У комп'ютерних системах аутентифікація користувачів зазвичай виконується за допомогою спеціального програмного модуля, встановленого безпосередньо на комп'ютері, за допомогою якого пред'явник намагається отримати прямий або віддалений доступ. Усю роботу цього модуля можна умовно поділити на два етапи.

Попередній, на якому модуль формує «еталон користувача, що перевіряється», наприклад, потрібно ввести пароль користувача (як правило, цей самий пароль потрібно ввести двічі, щоб виключити помилку його введення) – за ним особа користувача розпізнаватиметься згодом.

Пароль (або інший еталон) може і назначатися (присвоюватися) користувачеві – так буває, наприклад, у різних системах доступу в Інтернет. Зазвичай модуль аутентифікації зберігає наявні еталонні зразки у таблиці відповідностей «користувач – еталон».

І завершальний етап, коли пред'явник-користувач проходить аутентифікацію й у нього запрошується аутентифікаційна інформація, яка порівнюється з еталоном. На підставі цього порівняння він вважається розпізнаним або нерозпізнаним.

За віддаленої верифікації аутентифікаційна інформація, яка пред'являється користувачем, і її еталонний зразок можуть доповнювати один одного, беручи в такому разі участь у будь-яких криптографічних перетвореннях. Для цього випадку використовуються різні протоколи мережевої аутентифікації[2].

Засоби аутентифікації можна поділити на три групи (три методи) відповідно до принципів, що використовуються:

1. Принцип «що Ви знаєте» («you know»). Під час створення систем безпеки вбачається, що це «знання» не може бути тільки одним ідентифікатором особистості: у будь-якому разі не рекомендовано його застосовувати багаторазово, необхідно обмежити термін використання «знання». Як приклад, «знання» можна навести пароль під час звертання до комп'ютера під час входу в оперативну систему або PIN-код доступу до банківської картки.

[1] Идентификационные и верификационные системы. В чём отличие? // ЮНИСКАН. – 2004. – 25 октября. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/...

[2] Панасенко С. Аутентификация пользователей / С. Панасенко // МИР ПК. – 2006. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

2. Принцип «що Ви маєте» («you have»). «Мати» – це якийсь механізм, котрий показує, що клієнт «володіє» певною річчю з визначеними параметрами. У такому разі в теорії безпеки вважається, що річ може бути передана третій особі, тобто є ймовірність її дублювання (підробки) або неправомірного вживання. Приклади таких «речей»: картка в будь-якому її вигляді, USB-ключ, Touch-memory, якийсь пропуск.

3. Принцип «хто Ви є» («you are») або «бути» – використовує персональні властивості користувача та насамперед описує фізичні особливості тіла, тобто щось невіддільне від особистості індивідуума. Насамперед це зовнішній вигляд особи (поєднання росту, ваги, об'ємів частин тіла), зображення обличчя (фотографії у профіль, фас, тривимірне /3D/ зображення), відбитки пальців і долонь, райдужна оболонка ока, термограма долоні або пальця тощо. Окрім фізичних параметрів, для ідентифікації можуть використовуватися поведінкові ознаки – будь-які рухи частин тіла клієнта, якого ідентифікують (як один із варіантів – власний підпис на папері або touchpad-е), і особливості голосу. Системи строгої верифікації використовують як мінімум два або більше параметри за аутентифікації користувачів[1].

Кожен із зазначених методів має свої переваги та недоліки. Для усунення останніх у комп'ютерних системах, як правило, використовують комбінації різних методів аутентифікації, наприклад, смарт-картку у вигляді предмета з унікальним вмістом (наприклад, криптографічним ключем), коли перед отриманням доступу до нього необхідно ввести PIN-код. Тобто користувач для входу в систему не тільки повинен мати при собі смарт-картку, але і пам'ятати унікальну парольну послідовність знаків – PIN-код. Така аутентифікація називається двофакторною – за кількістю параметрів, які перевіряються.

Визначимо позитивні якості та недоліки вищенаведених методів.

Пароль

Нині засоби аутентифікації першої групи («що Ви знаєте» – «you know») є найекономічнішими за вартістю, але одночасно і найменш надійними.

За парольним принципом формуються прості системи аутентифікації, в яких користувачеві досить ввести правильний пароль для отримання доступу до потрібного йому ресурсу.

Парольна аутентифікація поки що є найбільш поширеною, оскільки: по-перше, це найпростіший із відомих методів аутентифікації (що є єдиною її позитивною якістю), по-друге, вона з'явилась набагато раніше за інші види, тому й досі застосовується у значній кількості для організації програмного доступу.

Проте недоліків у парольній аутентифікації є дуже багато.

По-перше, часто користувачі послуговуються зовсім простими або легко вгадуваними паролями, які є:

– будь-якою похідною від самого ідентифікатора користувача (часто безпосередньо сам ідентифікатор);

– словом із його рідної мови (дуже поширеними є випадки, коли парольне слово є власним іменем: кличка собаки, назва улюбленої футбольної команди тощо) або загальновживаною фразою (такі паролі підбираються зловмисниками шляхом словникової атаки – послідовним підбиранням слів і найбільш вживаних фраз за наявними електронними словниками);

[1] Голов А. Аутентификация пользователей – современные методы / А. Голов, И. Прудников. – 2006. – 17 декабря. [Электронный ресурс]. – Режим доступа: http://www.cio-world.ru/, http://biometrics.ru/document...

– особливо результативним попередній вид підбору пароля буває у випадках, коли користувачі застосовують незначну кількість знаків у парольному слові.

По-друге, пароль можна підглянути або перехопити під час введення.

По-третє, пароль може стати відомим через застосування насильства до його власника.

Нарешті, існують і застосовуються зловмисниками спеціальні соціально-психологічні методи (так звані методи соціальної інженерії), за допомогою яких можна отримати пароль користувача шляхом обману, – недосвідчений користувач сам назве його зловмисникові, якщо той зможе видати себе за адміністратора системи. Одним із поширених методів, які застосовують кіберзлочинці, є фішинг: користувача під будь-яким приводом заманюють на фальшиву веб-сторінку, що імітує, наприклад, потрібну сторінку сайта його банку, – там він залишає дані своєї кредитної картки, з якої потім кіберзлочинці знімають гроші. До речі, можливість фішингу можно виключити за допомогою методу взаємної аутентифікації, коли не тільки сервер перевіряє користувача, але і користувач переконується, що це саме сервер його фінансової установи.

Потрібно зазначити, що технічний прогрес щодо парольної аутентифікації не стоїть на місці. Не припиняються спроби розробити достатньо ефективну аутентифікацію, яка поєднувала б зручність і надійність із простотою застосування паролів. Але поки що всі удосконалення, які запроваджуються, лише ускладнюють парольну аутентифікацію, основний позитив від якої – простота застосування.

Унікальний предмет (пристрій)

Для аутентифікації користувачів найчастіше застосовуються смарт-картки, картки з магнітною стрічкою, електронні таблетки iButton, USB-токени.

Системи строгої аутентифікації, які сформовані за принципом «що Ви маєте» («you have»), надають набагато більше можливостей для посилення захисту. Наприклад, роботу токенів, що генерують одноразові паролі, не з'єднуючись із самою системою, дуже складно підробити, а сам пароль застосовується тільки один раз і повторно не може бути використаний.

Унікальність спеціальних предметів, які вживаються під час проведення більш захищеного процесу аутентифікації, визначається інформацією, яку вони містять. У звичайному випадку ця інформація є ідентифікатором і паролем користувача, яка просто зчитується з носія і передається модулю аутентифікації. Більш складний випадок – носій містить криптографічний ключ, який застосовується в одному з протоколів під час проведення віддаленої аутентифікації.

До речі, мікропроцесорні смарт-картки й USB-токени можуть самостійно виконувати криптографічні перетворення і бути активною стороною у верифікаційних (аутентифікаційних) процесах.

Унікальні предмети самі собою досить рідко застосовуються: найчастіше це лише один з елементів двофакторної верифікації.

Недоліків у «предметної» аутентифікації значно менше, ніж у парольної. Наведемо основні з них:

– сам носій може бути викрадений або силою вилучений у його власника;

– потрібна додаткова спеціальна апаратура під час застосування систем, які сформовані на використанні унікальних пристроїв-предметів;

– на практиці спостерігаються випадки виготовлення копій або емуляторів таких «унікальних предметів».

Але незважаючи на вказані недоліки, унікальні носії аутентифікаційної інформації займають велику частку ринку і досить широко застосовуються у нашому житті.

Особливо це стосується USB-токенів, для використання яких не потрібно жодного додаткового устаткування – цілком достатньо тільки комп'ютера. Наприклад, для аутентифікації за допомогою USB-токенів у операційних системах (ОС) від «Windows 2000» і вище необхідний тільки спеціального формату програмний драйвер, тобто в ці ОС вже за їх розробки закладена можливість підтримки такого виду аутентифікації.

Біометрична аутентифікація

Системи строгої аутентифікації, які сформовані на використанні чинника «хто Ви є» («you are») та часто підсилені рішеннями на основі принципу «що Ви маєте» («you have»), нині вважаються одними з найнадійніших систем доступу.

Під час застосування біометричної верифікації як ідентифікатора застосовуються оригінальні та невід'ємні характеристики людини. Нині найбільш практичне використання мають біометричні системи, які застосовують аутентифікацію на основі технологій так званих «трьох великих біометрик», які дозволяють розпізнавати індивідуальні ознаки людини з досить великим коефіцієнтом ефективності.

Біометричне розпізнавання полягає у порівнянні фізіологічних або психологічних особливостей особи, яку перевіряють, з її характеристиками-шаблонами, що зберігаються в базі даних (архіві) контрольної системи. Системи, які використовують біометричні характеристики, порівняно з парольними та картковими принципами рішень доступу, забезпечують набагато надійніший захист об'єкта, який охороняється.

На практиці використовуються всі вищезазначені види (типи) аутентифікації. Вибір виду верифікації залежить від ступеня важливості інформації чи об'єкта доступу, що захищається. Наприкінці першого десятиріччя – початку другого десятиріччя XXI століття найбільше поширилися системи з дво- або трифакторною аутентифікацією, основним недоліком яких є їх досить висока вартість. Але все ще поширеною залишається парольна аутентифікація, всі недоліки якої компенсуються простотою реалізації цього способу доступу. Як чинник, який суттєво позначається на прискоренні практичного застосування біометричних засобів аутентифікації, необхідно навести загальносвітову тенденцію зниження цін на пристрої сканування, зокрема та біометричні технології загалом[1].

Для ліпшого розуміння значення термінів «ідентифікувати» і «верифікувати» («аутентифікувати») необхідно знати, що ці терміни мають іншомовне походження, тобто і в українській, і в російській мові є запозиченими. У перекладі з англійської ці дієслова означають: «identify» – впізнавати, узнавати, «verify» – перевіряти, підтверджувати. Тому, зважаючи на ці значення слів, поняття ідентифікації та верифікації формулюються відповідно як процеси порівняння «один до багатьох» (1 : N) та «один до одного» (1 : 1).

За ідентифікації ідентифікатор, що пред'являється, порівнюється (зіставляється) з усіма раніше зареєстрованими в системі. Тобто можна сказати, що в режимі ідентифікації біометрична система шукає відповідь на питання «Хто Ви?», зіставляючи отримані дані з усіма наявними, що зберігаються в пам'яті бази (архіві). Системи, що діють у режимі ідентифікації, можуть бути або частково автоматизованими (під час здійснення порівняння формується перелік можливих «кандидатів» на збігання з ідентифікатором, що пред'являється, які розташовуються в міру зменшення ймовірності збігання, а прерогатива ухвалення остаточного рішення залишається за оператором системи) або повністю автоматизованими (система ухвалює рішення без участі людини).

Отже, *біометрична ідентифікація* – це процес визначення особистості, яка перевіряється, шляхом зіставлення її біометричних даних із такими, що зберігаються в базі

[1] Панасенко С. Аутентификация пользователей / С. Панасенко // МИР ПК. – 2006. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

даних. У такому разі в базі даних може міститись досить великий набір персональних біометричних відомостей різних фізичних осіб. А під час створення такої бази (архіву) персональні біометричні дані кожної особи перетворюються на окремий індивідуальний шаблон. Шаблон зразка, який потрібно ідентифікувати, порівнюється з кожним із шаблонів, які містяться в базі даних, представляючи за кожним із параметрів абсолютну або відносну величину відхилення від шаблону зразка для кількісної оцінки ступеня подібності. Система відбирає ті шаблони і, відповідно, виводить персональні дані тих осіб, з якими розбіжності є найменшими. Щоб запобігти помилковій ідентифікації людини, дані якої в базі просто відсутні, для системи встановлюється певний рівень подібності. У разі, коли цей рівень не досягається, результат обнуляється.

Варто зазначити, що системи, які діють у режимі верифікації, в основному є повністю автоматизованими (тобто ухвалюють рішення без участі людини). Для біометричних систем, де бази даних обчислюються сотнями тисяч і навіть мільйонами шаблонів, суто аутентифікаційні (верифікаційні) системи є лише складовою ідентифікаційних систем.

Прикладом реально існуючих верифікаційних систем є системи, які відомі за абревіатурою *INSPASS* і які встановлені в аеропортах США для полегшення процедури реєстрації пасажирів, котрі часто користуються авіапослугами[1].

Одним з основних завдань біометричних технологій є забезпечення надійності та ефективності проведення звірок документів, а також електронне документування виконаних звірок. Для виконання цих завдань використовують методи *подвійної або потрійної верифікації.*

Подвійна верифікація – це проведення звірки біометричного шаблону, записаного в електронну пам'ять паспорта або візи, з відповідними біометричними характеристиками суб'єкта, який перевіряється.

Потрійна верифікація, своєю чергою, вимагає, крім проведення дій, передбачених подвійною верифікацією, додаткової звірки шаблону, що перевіряється, з електронними даними, які зберігаються у загальнодержавному реєстрі біометричних даних. За таких дій будь-яка спроба підробки документа втрачає сенс, оскільки потрійна верифікація встановить невідповідність із шаблоном, внесеним у державний реєстр під час видачі паспортно-візових документів нового зразка.

Така потрійна перевірка рекомендована міжнародною організацією цивільної авіації ІСАО, але такий варіант дій вимагає спочатку створення спеціальної державної інфраструктури, яка могла б виконувати в режимі реального часу запити на ідентифікацію осіб за біометричними даними[2].

Проте поділ біометричних систем на суто верифікаційні та ідентифікаційні за ознакою множинності порівнянь, які вони проводять, є не зовсім коректний. Для підтвердження цього розглянемо класифікацію реально існуючих та найпоширеніших біометричних систем для забезпечення інформаційної безпеки. Такі системи традиційно прийнято вважати верифікаційними, оскільки вони підтверджують особистість користувача і надають йому право на вхід в інформаційну систему. Проте алгоритм дій таких систем за ознакою множинності порівнянь – ідентифікаційний, оскільки він порівнює біометричний зразок, що перевіряється, із зареєстрованими зразками всіх відомих користувачів із банку даних.

[1] Идентификационные и верификационные системы. В чём отличие? // ЮНИСКАН. – 2004. – 25 октября. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/

[2] Современные биометрические системы безопасности // Byte. – 2006. – № 6 (94). – июнь. [Электронный ресурс]. – Режим доступа: http://www.bytemag. ru/articles/detail.php

Крім того, і для власне верифікаційних систем з ознакою перевірки один до одного (1:1) на етапі проведення реєстрації виникає необхідність здійснення перевірки з метою виявлення можливості внесення шаблону-зразка в базу даних раніше. Ця перевірка здійснюється шляхом послідовного порівняння зразка з усіма наявними в банку даних зразками і, по суті, є негативною ідентифікацією. Отже, вказані системи є одночасно ідентифікаційними та верифікаційними за своєю суттю, зважаючи на множинності порівнянь.

Із наведених прикладів зрозуміло, що розподіл систем на аутентифікаційні (верифікаційні) та ідентифікаційні є доволі умовним.

Іншим поширеним критерієм для диференціації біометричних систем в англомовному біометричному співтоваристві є твердження так званого типу «claim» (твердження типу). Конкретне значення формулювання твердження типу «claim» залежить від типу використованої системи та завдання її призначення.

Наприклад, під час верифікації твердження можна представити реченням такого змісту: «цей індивідуум є джерелом біометричного шаблону «А» в базі даних». Таке твердження володіє двома важливими характеристиками щодо факту реєстрації в базі даних.

Характеристики поділяються на позитивні (тобто такі, що стверджують факт реєстрації цього користувача в базі даних) і негативні (заперечують факт реєстрації такого користувача в базі даних). За відношенням до певного шаблону бази даних поділяються на специфічні – (стосуються шаблону, що визначається) і неспецифічні (не стосуються шаблону, що визначається). Для того, щоб відобразити можливі варіанти відповідей (стверджень) системи, які видаються, зведемо в таблицю можливі результати порівнянь конкретного зразка-шаблону із зареєстрованими в базі даних (див. табл. 2):

Таблиця 2

Можливі варіанти порівняння вихідного зразка із зареєстрованими в базі даних шаблонами

Характеристика	Специфічне	Неспецифічне
Позитивна	**Специфічно позитивна відповідь:** Я (Він, Вона) – джерело біометричного зразка «А» (конкретного) в базі даних	**Неспецифічно позитивна відповідь:** Я (Він, Вона) – джерело якого-небудь біометричного зразка в базі даних
Негативна характеристика	**Специфічно негативна відповідь:** Я (Він, Вона) – не є джерелом біометричного зразка «А» в базі даних	**Неспецифічно негативна відповідь:** Я (Він, Вона) не є джерелом будь-якого біометричного зразка в базі даних

Як бачимо, маємо чотири можливі результати порівнянь:

– *специфічно позитивна відповідь;*

– *специфічно негативна відповідь;*

– *неспецифічно позитивна відповідь;*

– *неспецифічно негативна відповідь.*

Варіант *специфічно негативної відповіді* можна не брати до уваги, оскільки подібних завдань у реальному житті не існує. Отже, зважаючи на такий підхід, можна вважати, що і є фактично загальноприйнятним, що *верифікаційні (аутентифікаційні)* системи

працюють зі *специфічно позитивними відповідями,* а інші два варіанти є ознаками *ідентифікаційних* систем.

Проте за своєю суттю системи, що працюють зі специфічно позитивними відповідями, здійснюють порівняння отриманого зразка-шаблону тільки з одним шаблоном бази даних (конкретний шаблон для проведення порівняння вказується), тобто все зводиться до диференціації систем за ознакою множинності порівнянь.

Цікавий підхід до розмежування біометричних систем застосовується групою експертів Міжнародної організації з стандартизації (ISO**).** Він ґрунтується на відмінностях у відповідях, які видаються біометричними системами *верифікації* та *ідентифікації.*

У спрощеному вигляді сутність цього підходу така: в результаті проведеного порівняння системи *верифікації* надають відповідь *«підтверджую»* або *«не підтверджую»* без здійснення пошуку конкретного шаблону в базі даних, з яким би проводилося порівняння. У цьому просто немає потреби.

Ідентифікаційні системи повинні як відповіді видати шаблон або список шаблонів, котрі б збігалися з біометричним взірцем, який перевіряється. Однак і цей спосіб має суперечності.

Сучасні системи інформаційної безпеки формуються з урахуванням рівня доступу різних користувачів. Для цього кожному шаблону, що міститься в базі даних, додатково надається спеціальна позначка, яка відносить його до однозначно визначеного рівня доступу.

Для організації доступу конкретного користувача система видає ідентифікатор зі спеціальною позначкою. Але ця позначка не є універсальним критерієм для диференціації біометричних систем.

Питання розмежування біометричних систем на верифікаційні (аутентифікаційні) та ідентифікаційні на основі об'єктивних характеристик самої системи остаточно не вирішене і залишається відкритим. Окрім того, в деяких публікаціях необхідність такого розмежування ставиться під сумнів.

По суті, робота будь-якої біометричної системи ґрунтується на основному алгоритмі – порівнянні архівного біометричного шаблону та зразка, отриманого від користувача, а також встановленні ступеня їх подібності, а все інше – архітектура, інтерфейси, настройки – залежать від умов конкретного завдання.

Багато фахівців вважають, що для практичного використання така диференціація біометричних систем є найбільш доцільною[1].

Для з'ясування якісних можливостей основних методів верифікації й ідентифікації за видами ідентифікаційних параметрів наведемо оцінку якостей застосовуваних методів ідентифікації (табл. 3), можливість змін їхніх параметрів від часу й оцінку терміну служби (табл. 4), а також витратність на підробку різних за принципами дій пристроїв і простоту можливого вчинення шахрайських дій (табл. 5). Ці таблиці були опубліковані у квітні 2008 року[2].

У табл. 3 оцінка параметрів наведена за п'ятибальною шкалою для систем безпеки, що застосовують різні ідентифікаційні механізми. Причому 1 – найнижча оцінка вказаного параметра, а 5 – найвища оцінка відповідного методу ідентифікації.

[1] Идентификационные и верификационные системы. В чём отличие? // ЮНИСКАН. – 2004. – 25 октября. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/...

[2] Радостин А. Перспективы использования биометрии в системах лояльности / А. Радостин // RB.RU. – 2008. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Таблиця 3

Зведена таблиця оцінки деяких методів ідентифікації

Механізм	Поширеність	Доступність	Вартість	Помилки*
Пароль	5	5	5	–
Картка	4	4	4	4
Картка з PIN-кодом**	4	4	4	4
USB-ключ	1	4	3	-
Touch-memory	3	4	3	5
RFID – позначка	2	4	3	4
Пропуск (фото)	4	5	4	4
Відбиток пальця	2	4	5***	4
Відбиток долоні	1	2	2	4
3d-образ обличчя	1	2	2	3
Малюнок сітківки	1	2	1	4
Підпис	1	2	4	3
Голос	–	–	– (відсутні на ринку)	2 (оцінка)

* У цій таблиці «помилка» – бал імовірності за належного рівня контролю «не прийняти за свого».

** Кращий захист виходить за комбінації методів, в цьому випадку комбінуються «знати» і «мати».

*** Вартість самої системи не є мінімальною, проте відсутні як такі прямі витрати на виготовлення ідентифікаційної «копії клієнта», тобто для технології карток із PIN-кодом, наприклад, необхідно виготовити картки, забезпечити їх видачу і заміну кожному клієнтові, а у випадку з біометричними ознаками нічого подібного не потрібно.

У табл. 4 наведена часова стійкість різних видів ідентифікуючих параметрів і термін їхньої служби.

Таблиця 4

Стійкість параметрів у часі, оцінка строку служби

Механізм	Період змін ознаки	Звичайний термін служби ідентифікатора
1	2	3
Пароль	(не застосовується)	1 рік (звичайна заміна)
Картка	(не застосовується)	До 3 років (фізичний знос)
Картка з PIN-кодом	(не застосовується)	До 3 років (фізичний знос)
USB-ключ	(не застосовується)	До 5 років (фізичне пошкодження)
Touch-memory	(не застосовується)	До 10 років (фізичне пошкодження)
RFID – позначка	(не застосовується)	До 20 років (фізичний знос)
Пропуск (фото)	До 10 років	До 3 років (фізичний знос)
Відбиток пальця	До 50 років	Довічно*

Продовження таблиці 4

1	2	3
Відбиток долоні	До 10 років	Довічно
3d-образ обличчя	До 5 років	До 5 років (вікові зміни)
Малюнок сітківки	До 25 років	Довічно
Підпис	1 рік	До 5 років (тимчасові зміни)
Голос	1 рік	До 3 років (навколишнє середовище, зовнішні чинники)

* Оцінка «довічно» означає, що один і той же параметр може залишатися постійним упродовж усього часу та існує можливість ідентифікації за цією ознакою. Проте це не означає, що з часом не слід передбачати механізми оновлення біометричних даних.

У табл. 5 наведена розроблена А. Радостіним класифікація витратності та доступності технологій на предмет можливості шахрайських дій із кожним механізмом ідентифікації, який нині застосовується в системах безпеки.

Таблиця 5

Затратність і простота шахрайських дій

Механізм	Витрати на підробку ознаки	Недоступність технології
Пароль	1	1
Картка	2	2
Картка з PIN-кодом	4	2
USB-ключ	3	4
Touch-memory	3	4
RFID – позначка	4	4
Пропуск (фото)	1	1
Відбиток пальця	4	4
Відбиток долоні	5	5
3d-образ обличчя	5	4
Малюнок сітківки	4	4
Підпис	1	1
Голос	2	2

1.5. Революційний розвиток біометричної індустрії на початку XXI століття

Використання біометрії для ідентифікації створює низку унікальних можливостей. Біометрія дозволяє ідентифікувати людину за допомогою її ж самої. Смарт-картки, картки з магнітною стрічкою, ідентифікаційні картки, ключі та подібні речі можуть бути загублені, викрадені, скопійовані або просто забуті вдома. Паролі теж можуть бути забуті або вкрадені. Електронний бізнес, що постійно розвивається, робота з інформацією,

представленою в електронному вигляді, вимагають від людини запам'ятовувати безліч паролів і персональних ідентифікаційних номерів (PIN-кодів) для комп'ютерних і банківських рахунків, електронної пошти, міжнародних переговорів, веб-сайтів тощо. Біометрія пропонує швидкий, зручний, точний, надійний і вже не надто дорогий спосіб ідентифікації з великою кількістю найрізноманітніших застосувань.

Біометричні рішення стрімко стають популярними в найрізноманітніших галузях – від паспортно-візових документів нового покоління до фінансових і платіжних систем, освіти, охорони здоров'я, програм лояльності та супроводу авіапасажирів, які часто мандрують.

Останнім трендом для застосування біометричних технологій стало оснащення різних мобільних пристроїв сканерами відбитків пальців. Згідно з прогнозом компанії «Goode Intelligence» три мільярда чотириста мільйонів людей будуть використовувати біометричні технології на своїх мобільних пристроях у 2018 році[1].

Причини популярності біометричних технологій очевидні: їх надійність, безпека, ефективність, комфортність. На відміну від інших технологій, біометрія працює безпосередньо з людьми і виокремлює їх індивідуальні особливості, інакше біометричні рішення просто не змогли б спрацьовувати.

Немає такої єдиної біометричної технології, яка задовольнила б усі потреби. Кожна з біометричних технологій має свої переваги та недоліки. Проте є загальні риси, які роблять кожну біометричну технологію корисною. Принцип дії будь-якої біометричної системи повинен бути заснованим на характеристиці, яка була б розпізнавальною й унікальною.

Останні розробки нових біометричних технологій можуть мати дуже точні розпізнавальні властивості, але водночас вимагатимуть додаткових даних для підтвердження їх унікальності.

Інший доволі суттєвий аспект – наскільки проста («комфортна») кожна технологія. Процес повинен бути швидким і простим, наприклад, встати перед відеокамерою, сказати декілька слів у мікрофон або доторкнутися до відведеного місця у сканері відбитків пальців. Головною вимогою до біометричних технологій, яка і є їхньою суттєвою перевагою, є швидка і проста ідентифікація без спричинення яких-небудь незручностей людині.

Застосування біометричних технологій досить різноманітні: доступ до робочих місць і мережевих ресурсів, захист інформації, забезпечення контролю доступу на територію об'єктів, встановлення установчих даних особи тощо.

Електронний бізнес і впровадження технології «електронного уряду» можливе тільки після запровадження і виконання певних процедур для ідентифікації особи. Біометричні технології застосовуються в паспортно-візових документах нового покоління, охороні правопорядку, в галузі безпеки банківських транзакцій, інвестування й інших фінансових переміщень, роздрібній торгівлі, питаннях охорони здоров'я[2], а також у сферах соціальних послуг і особистого життя.

У майбутньому біометричні технології відіграватимуть головну роль у питаннях персональної ідентифікації в багатьох сферах. Використовувані окремо або спільно зі

[1] На мобильных технологиях биометрические компании заработают восемь миллиардов долларов // BIOMETRICS.RU. – 2013. – 06 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрия и шифрование: позитивная сумма технологий // BIOMETRICS.RU. – 2007. – 18 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

смарт-картками, токенами, різними електронними ключами і підписами, біометрія надалі буде все більше застосовуватися у всіх сферах економіки й особистого життя[1].

Згідно з прогнозами багатьох експертів у галузі біометричних технологій, біометрія є одним із найдинамічніших сегментів світового ринку інформаційних технологій, що посилено розвиваються.

Сучасні біометричні ідентифікаційні технології впроваджуються в життя на різних рівнях: як у глобальному і міждержавному масштабі, так і в регіональному, галузевому й особистому. Біометричні системи, що використовуються, повинні відповідати стандартам, які пред'являють до біометричної ідентифікації провідні міжнародні, галузеві й регіональні організації, міждержавні та урядові структури.

До цих організацій, співтовариств, країн, їх урядових структур і програм, що ними реалізуються, належать:

– Організація Об'єднаних Націй (UN/OOH), Міжнародна організація цивільної авіації (ICAO/ІКАО), Міжнародна організація зі стандартизації [ISO/ICO (програма машинозчитуваних транспортних документів, зокрема електронних або біометричних закордонних паспортів];

– країни Шенгенської зони й інші держави – члени Євросоюзу (загальноєвропейська система біометричної ідентифікації за відбитками пальців EURODAC, інформаційна візова система країн Шенгену VIS, система біометричних віз для іноземців, що мають намір відвідати територію Великобританії);

– Великобританія, Португалія, Іспанія та низка інших країн – програми видачі внутрішніх біометричних ідентифікаційних карт громадянам цих держав, що реалізовуються наприкінці першого – початку другого десятиріччя XXI століття;

– Німеччина – видача з 2007 року закордонних біометричних паспортів другого покоління;

– США – програма «US VISIT», що вимагає безумовну біометричну ідентифікацію всіх претендентів американських віз (із реєстрацією відбитків усіх десяти пальців рук), окрім громадян 37 країн, які мають право на безвізовий режим за умови наявності біометричного закордонного паспорта другого покоління та передачу зображень відбитків усіх 10-ти пальців; президентська директива з національної безпеки (HSPD), яка зобов'язує всіх державних службовців і працівників підприємств, що працюють за державними контрактами, оформляти біометричні ідентифікаційні картки; створення Федеральним бюро розслідувань (ФБР) у кооперації з правоохоронними органами Великобританії, Канади, Австралії і Нової Зеландії (FCC) глобальної всесвітньої бази біометричних даних, в якій повинні міститися зведення про сотні мільйонів людей усієї земної кулі[2].

Найпоширеніша нині біометрична технологія – ідентифікація за відбитками пальців. Ця технологія продовжує домінувати на ринку, займаючи майже 50% від його обсягу. Вона ввібрала всі сучасні досягнення біометрії і за правом посідає позиції лідера. Другою за ступенем поширеності технологією є ідентифікація за обличчям (15–20% ринку). Вона активно застосовується в «електронних паспортах» та інших документах, які засвідчують особу людини і має тенденцію до невпинного збільшення. Третє місце (майже 7%) оспорюють технології ідентифікації за райдужною оболонкою ока і геометрії та розташування

[1] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art...

[2] Массовая идентификация. – 2007. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/civil...

кров'яних судин руки або пальця, хоча більшість експертів третє місце віддають технології райдужної оболонки ока[1].

Розробка і застосування мультибіометричних рішень – найперспективніший напрям розвитку галузевого ринку. У мультибіометричних системах розпізнавання здійснюється не за однією ідентифікаційною ознакою, а за декількома. Мультибіометричні рішення стають більш популярними: так, наприклад, в електронні паспорти другого покоління та ідентифікаційні картки (ID-Cards), що випускаються різними державами, вносяться не тільки цифрові фотографії власників цих документів, але й відомості про відбитки їх пальців.

Окрім власне мультибіометричних технологій, в один клас із ними прийнято об'єднувати мультимодальні та багатофакторні рішення.

У мультимодальних системах ідентифікатори одного й того ж типу (наприклад, відбитки пальців) обробляються за допомогою різних алгоритмів. Головна мета – підвищення надійності ідентифікації.

У багатофакторних системах разом із біометричними застосовуються також й інші ідентифікатори (PIN-код, пароль, смарт-картка тощо). У цьому разі для підтвердження своєї особи і/або повноважень користувачеві необхідно пройти біометричну ідентифікацію та пред'явити або ввести додаткові ідентифікатори[2].

Нині дедалі більше уваги приділяють технологіям розпізнавання людей за формою обличчя. Ці технології розвиваються дуже швидкими темпами. Так, наприклад, алгоритми розпізнання за обличчям у 2007 році порівняно з 2002 роком покращились приблизно вдесятеро, а з 1995 року – в сто разів. Причому найліпші з протестованих технологій набагато перевершують відповідні здібності більшості людей[3].

Оскільки компетентні органи особливо цікавляться можливостями тотального автоматизованого контролю за всіма переміщеннями та комунікаціями громадян, із середини 1990-х років спецслужби багатьох країн намагаються реалізувати цю ідею в різних варіантах. Ознаки цього процесу можна побачити і в експериментах зі співробітниками крупних державних відомств на кшталт Міністерства оборони США, де в останньому десятилітті XX сторіччя почали забезпечувати співробітників універсальними беджами, які відігравали роль і перепустки, і гаманця, і медичної книжки. А також в експериментах початку 2000-х років з ув'язненими особами і школярами, яким видавали спеціальні браслети або ID-картки з RFID-чіпами для контролю переміщень будівлею в'язниці або школи та практично всюди запроваджуваних біометричних паспортах або інших документах із RFID-технологіями (радіочастотною ідентифікацією). І нарешті навіть у так званій соціальній картці киянина, яку українська столична влада планує запровадити і перетворити на єдиний документ, який повинен замінити мешканцю міста Києва паспорт, пенсійне посвідчення, водійські права, медичну книжку і, навіть, проїзне посвідчення. До речі, соціальна картка вже запроваджена у столиці Росії Москві і за наявними відомостями досвід впровадження й експлуатації цієї новації вивчався у низці обласних міст України.

Про тенденцію впровадження технологій тотального автоматизованого контролю також свідчить і світове зростання вживання так званих «технологій подвійного застосу-

---

[1] Технологии // BioLink. – 2008. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/...

[2] Мультибиометрические технологии // BIOLINK.RU. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/multibiometric.php...

[3] Берд Киви. Лица, подлежащие опознанию / Киви Берд // COMPUTERRA.RU. – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

вання». У різних біометричних конкурсах беруть участь не тільки компанії, що спеціалізуються на технологіях ідентифікації для служб безпеки й охоронних структур (типу «Viisage» і «Identix»). Серед учасників стає дедалі більше корпорацій-гігантів таких, як «Toshiba» і «Samsung», інформаційно-технологічні фірми, що орієнтуються на широке побутове застосування своїх технологій (зокрема «Neven Vision» – одне з придбань свого часу компанії «Google»), а також дослідницькі центри університетів Кембриджа, Карнеги-Меллона й Пекіна. Таке широке представництво свідчить, що передові біометричні технології, особливо технології розпізнавання за обличчям індивідуумів, цікавлять не тільки силові структури та служби безпеки й охорони. Зокрема ефективне розпізнавання за обличчям було б дуже корисне у всьому, що стосується організації цифрових фотоальбомів і швидкого пошуку фотографій у них.

Прості функції розпізнання осіб уже реалізовані в цифрових фотоапаратах багатьох фірм, зокрема «Canon», «Pentax» і «Fuji». Вбудовані програми пошуку можуть автоматично знаходити в картинці відеошукача людські обличчя за характерними ознаками – очами, вухами, носом тощо. Якщо особа одна, камера сама може налаштувати фокус виключно на її обличчя, якщо ж осіб декілька – вибрати узагальнюючий фокус для всіх лиць осіб. А фірма «Sony» розробила таку цифрову камеру, яка утримує затвор від спрацьовування доти, поки люди не почнуть усміхатися. Спеціальна програма аналізує обличчя осіб «на предмет щасливого виразу», досліджуючи положення кутів рота, розтулення губ, мімічні зморшки навколо очей[1].

У XXI столітті чітко сформувалась тенденція зростання біометричного ринку, який дедалі більше розвертається у бік масштабних проектів, що реалізовуються в інтересах замовників не тільки серед державних структур, але й комерційних.

Одним із наймасштабніших прикладів біометричних проектів, які реалізуються державними структурами, є створення Федеральним бюро розслідувань (ФБР) США системи Next Generation Identification (NGI), Міністерством оборони США системи Defense Automated Biometric Identification System (Dod ABIS), експлуатація Міністерством національної безпеки США системи US-VISIT.

Що стосується комерційних проектів, то американські банкіри і страховики вже масово застосовували та продовжують застосовувати біометрію під час роботи з особами, котрі бажають отримати кредити, із вкладниками, а також під час видачі компенсацій особам, які постраждали від ураганів «Ріта» і «Катріна». Біометрична ідентифікація покупців у платіжній системі «Pay by Touch» дозволила не в теорії, а на практиці запровадити технології персоналізованого маркетингу.

Але наймасштабнішим проектом у світі є індійський біометричний проект «Aadhaar», в якому 2014 року унікальні ідентифікаційні номери на основі сканування відбитків пальців і радужної оболонки ока отримають понад 600 млн індійців, що становить половину мешканців країни[2].

Очікується, що з допомогою ідентифікаційних номерів буде значно розширений доступ звичайних індійських громадян, більшість яких не вміє читати і писати, до різних послуг: банківських, фінансових, медичних, телекомунікаційних, освітніх. Активне застосування біометрії також дозволить забезпечити справедливе розподілення соціальної та продовольчої допомоги серед представників найбідніших верств населення.

[1] Берд Киви. Лица, подлежащие опознанию / Киви Берд // COMPUTERRA.RU. – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document. asp...

[2] Центральный банк Индии призвал активнее применять биометрические технологии // BIOMETRICS.RU. – 2012. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Досягнення біометрії в більшому обсязі починають використовувати комерційні структури, орієнтовані на роздрібний ринок.

За результатами дослідження, проведеного інформаційною групою «TNS», понад 60% американців підтримують застосування біометричної ідентифікації під час роботи з дебетовими та платіжними картками; серед постійних відвідувачів європейських готелів частка тих, котрі підтримують практичне застосування біометричних технологій вища 87,3% (за даними Вищої школи готельного бізнесу в Лозанні); мільйони пакистанців використовують біометричні платіжні кіоски.

У країнах, які утворилися на території колишнього СРСР, також упроваджуються сучасні біометричні технології. Окрім запровадження державними структурами біометричних технологій у паспортно-візових документах нового покоління, в Естонії підписаний із місцевим представництвом IBM та його субпідрядниками контракт на постачання системи біометричної ідентифікації для використання у сфері регулювання міграційних потоків. Низка банків приступили до промислової експлуатації системи біометричної ідентифікації користувачів корпоративної інформаційної мережі. У Росії на багатьох підприємствах застосовується нова версія системи обліку робочого часу і контролю «BioTime».

До галузей, де застосування біометрії також набуває масового характеру, впевнено входить авіатранспорт. У США, Англії, Японії та Канаді в найбільших аеропортах введені в дію програми супроводу авіапасажирів, які часто мандрують. Учасники цієї програми завдяки ідентифікації за відбитками пальців, райдужною оболонкою ока та зображенням обличчя проходять передпольотний контроль приблизно за 30 секунд.

Федеральна служба США із забезпечення безпеки авіаперельотів замовила розробку біометричної системи, яка покликана виявляти потенційних правопорушників на борту літаків. Відповідно доповіді, опублікованій за підсумками 2007 року агентством «Frost & Sullivan» і присвяченій перспективам інтегрованого ринку смарт-карток і біометричних технологій у державах Азійсько-Тихоокеанського регіону (АТР), було вказано, що кількість проектів національних ідентифікаційних карт, що реалізовуються в цьому регіоні, демонструє значний потенціал, яким володіють смарт-картки, що інтегровані з біометрією.

Як констатують автори доповіді, у низці держав (наприклад, в Індії, Малайзії та Пакистані) вже з самого початку реалізації загальнонаціональних ідентифікаційних проектів вводяться саме біометричні ID-картки, влада Японії та Китаю теж планують рухатися в цьому напрямі. Нині застосування біометричних технологій розглядається як найважливіша початкова умова старту та подальшої реалізації програм «національної ідентифікації». На думку авторів доповіді, інтеграція технологій смарт-карток і біометрії не тільки надає більшу безпеку, але й унеможливлює застосування різних засобів ідентифікації. На практиці це означає, що користувачам не доводиться витрачати свій час, щоб пригадати паролі або знайти потрібний ключ.

Очікується, що таке широке сприйняття інтегрованих технологій смарт-карток і біометрії забезпечить цьому спеціалізованому ринку значні перспективи зростання, ще у 2007 році прогнозували експерти «Frost & Sullivan»[1].

Важливу роль надійної та ефективної ідентифікації усвідомлюють усі, хто причетний до роботи з різними інформаційними системами, – їх розробники, постачальники, системні інтегратори, користувачі. Біометричні вирішення ідентифікації стають дедалі

[1] Новые перспективы биометрических смарт-карт // BIOMETRICS.RU. – 2007. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics. ru/document.asp…

більш популярними та престижними. І ринок біометричних засобів ідентифікації демонструє стабільне зростання. У період з 1998 до 2002 рік обсяг ринку зріс більше ніж утричі[1].

Проте прогнози на майбутнє навіть з одних і тих же джерел, але наданих у різний час, відрізняються один від одного. Так, у 2003 році авторитетна в професійному співтоваристві дослідницька компанія «International Biometric Group» (IBG) оцінювала обсяг світового біометричного ринку в 2007 р. в 4,03 млрд доларів США, а в кінці 2006 року в такому ж прогнозі навела цифру лише у 3,01 млрд[2].

Консалтингова компанія «Acuity Market Intelligence» підготувала прогноз розвитку біометричного ринку на довгострокову перспективу. Згідно з прес-релізом у 2007 році «Acuity Market Intelligence» щорічний оборот біометричного ринку сягне до 2020 року 10 млрд доларів США[3].

У листопаді 2008 року був опублікований прогноз Міжнародної біометричної групи «International Biometric Group», згідно з яким обсяг галузевого ринку в світі зросте з 3,4 млрд доларів США в 2009 році до 9,4 млрд в 2014 р., тобто очікується збільшення в 2,7 раза[4].

Основою зростання повинне стати поєднання дії декількох чинників. До них автори прогнозу включають: цифрову ідентифікацію в IT-системах (їй належить головна роль), зростання мобільності населення і децентралізацію управління робочою силою, розширення сервісів «електронного уряду», загальну залежність від електронних транзакцій, а також неминучість настання ери широкосмугового доступу. Інтегрована дія всіх згаданих чинників, своєю чергою, вимагатиме нагальну потребу в ідентифікації такого рівня, який може надати тільки біометрія, констатують автори прогнозу.

Улітку 2009 року компанія «Acuity Market Intelligence» здійснила новий прогноз розвитку біометричного ринку на найближчі 8 років. Згідно з цим прогнозом, обсяг світового ринку засобів біометричної ідентифікації у 2017 році сягне 11 млрд доларів, а середньорічні темпи зростання, обчислені в складних відсотках, у період з 2009–2017 рр. становитимуть 19,69%.

Вплив економічної кризи 2008 року на біометричну індустрію був істотним, але таким, що не спустошує, – констатують експерти. За їхніми оцінками біометричні проекти в суспільному секторі сповільнилися або взагалі зробити крок назад. Що ж стосується комерційних проектів, то в цій сфері істотно змінилися акценти: з розвитку довгострокових інфраструктурних програм ставка зроблена на такі впровадження, що гарантують швидке повернення інвестицій за короткий період. Проте унікальна здатність біометрії реалізовувати ідентифікацію й аутентифікацію залишається як і раніше затребуваною в IT-рішеннях, для яких дуже важливе ефективне розпізнавання користувачів, тому біометрична індустрія продовжить демонструвати зростання як до 2017 року, так і згодом.

Істотні зрушення відбудуться в розподілі доходів, які отримуються учасниками суспільних і комерційних проектів у сфері біометричної ідентифікації. Доходи від комер-

---

[1] Боровко Р. Мировой рынок средств идентификации / Р. Боровко // CNews Analytics. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security/...

[2] Лукашов И. Биометрия становится индустриальной технологией / И. Лукашов // CNews. – 2007. – 21 августа. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security2007/articles/biomarket.shtml…

[3] Прогноз развития биометрического рынка на долгосрочную перспективу // BIOMETRICS.Ru. – 2007. – 6 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] За пять ближайших лет объем мирового биометрического рынка вырастет более чем в 2,5 раза // BIOMETRICS.Ru. – 2008. – 14 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

ційних проектів до 2014 року зрівняються з доходами від проектів у суспільному секторі, а згодом і перевершать їх. Якщо оцінювати зростання обсягу комерційних проектів у 2009–2017 роки, то воно може становити від 41 до 55%.

Не менш значні зміни очікуються і на регіональних ринках. Темпам зростання світового біометричного ринку загалом упродовж найближчих восьми років буде характерна значна мінливість: відповідні щорічні процентні показники будуть коливатися в діапазоні від 4 до 13%. Очікується, що найбільш високі темпи зростання продемонструють країни Центральної і Південної Америки: середньорічні показники зростання цього ринку в регіоні становитимуть 39,46%.

Якщо зараз у світі домінують біометричні ринки США та країн Європи, Близького Сходу й Африки, то надалі вони мають поступитися азійсько-тихоокеанському ринку. До 2017 року частка США та країн Європи, Близького Сходу й Африки в загальному обсязі світового біометричного ринку має зменшитись із 37% до 26% і з 38% до 29% відповідно, тоді як для азійсько-тихоокеанського ринку цей показник повинен сягти 32%.

Відповідно до прогнозу, єдиною зоною стабільності повинна залишитися сегментація світового біометричного ринку за технологіями ідентифікації. Як і раніше, більшість ринку до кінця періоду, що аналізується, займатимуть засоби розпізнавання користувачів за відбитками пальців. Ривок повинні здійснити технології ідентифікації за райдужною оболонкою очей і обличчям, але навіть разом вони не сягнуть третини всього світового біометричного ринку. Частка засобів ідентифікації за технологіями, що використовують малюнок і термографію вен, голос і підпис, повинна зрости з 3 до 6, з 2 до 5 і з 0,7 до 1,6%.

Якщо аналізувати конкретні сфери застосування біометричних технологій, то до 2017 року вони, як і раніше, понад усе будуть затребувані в різних державних програмах ідентифікації. Очікується, що частка відповідного сегмента зменшиться з нинішніх 65 до 47%, але залишиться найбільшою. На друге місце вийде сегмент фінансових інститутів із часткою ринку в 18,22%; на третьому місці опиниться застосування біометрії у сервісах «електронного уряду» (14,23%). Використання біометричних засобів у різних IT-рішеннях буде дорівнювати 12,21%, а в системах відеоспостереження (8%), проте останній сегмент ринку буде розвиватися найдинамічніше і продемонструє середньорічні темпи зростання майже 61%[1].

Автори у новому варіанті посібника спеціально залишили дані прогнозів, що були опубліковані у 2007–2009 роках. Адже цікаво подивитись, наскільки вони здійснилися.

Експерти компанії «Global Industry Analysts» (GIA) передбачають такі основні тенденції регіональної еволюції розвитку світового біометричного ринку в 2012–2017.

Найбільшим сегментом ринку біометрії і надалі залишається США, але за темпами розвитку на перше місце вийдуть країни Азіатсько-Тихоокеанського регіону (АТР): середньорічні темпи росту біометричного ринку в цих державах, обчислені в складних відсотках (Compound Annual Growth Rate – CAGR), становитимуть 23,8%.

Разом із АТР автори доповіді покладають великі надії і на біометричний ринок Латинської Америки. Цим двом регіонам характерні загальні тенденції: бурхливе зростання економіки, приплив іноземних інвестицій і підвищена ділова активність загалом, а також порівняно нерозвинений приватний сегмент ринку систем безпеки на загальному тлі досить значної злочинності. Перелічені чинники обумовлять зростання потреби

[1] Новые тенденции выявлены в развитии мирового биометрического рынка // BIOMETRICS.RU. – 2009. – 7 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

в застосуванні сучасних біометричних систем. У доповіді «GIA» зазначається, що у Латинській Америці особливо будуть затребувані системи, які засновані на технологіях ідентифікації за обличчям і райдужною оболонкою ока.

Аналітики компанії «GIA» вважають, що в 2012–2017 рр. найбільш інтенсивно розвиватимуться технології ідентифікації за райдужкою ока: показник CAGR для відповідного сегмента біометричного ринку становитиме 25,9%[1].

Із вищенаведених даних бачимо, що, згідно з прогнозом Міжнародної біометричної групи «International Biometric Group», обсяг біометричного ринку в світі у 2009 році становив 3,4 млрд доларів США, а в 2014 році має сягнути до 9,4 млрд доларів. За відомостями компанії «Biometrics Research Group» у 2012 році обсяг біометричного ринку у світі становив 7 млрд доларів, а в 2015 році має сягти 15 млрд доларів США[2].

Як видно з наведених даних, дійсність перевершує найсміливіші прогнози. Темпи зростання світового біометричного ринку вищі прогнозованих. Але необхідно зауважити, що існують розбіжності в цифрах, наведених у прогнозах різних компаній. Так, за даними компанії «Biometrics Research Group» у 2012 році обсяг біометричного ринку в світі становив 7 млрд доларів, а в прогнозі, наданим компанією «Wintergreen Research», згаданий показник становив лише 5,2 млрд доларів США[3].

Також потрібно вказати, що компанія «Wintergreen Research» у своїй доповіді (дата публікації на російському порталі BIOMETRICS.RU листопад 2013 р.) надає прогноз, згідно з яким у 2019 році обсяг світового біометричного ринку сягне 16,7 млрд доларів. Але інша компанія «Global Industry Analysts» (дата публікації на російському порталі BIOMETRICS.RU листопад 2011 р.) спрогнозувала, що до 2017 року обсяг цього ринку становитиме 16,47 млрд доларів[4]. Як бачимо, є певні розбіжності, що зумовлені як часом надання прогнозів, так, можливо, й відмінностями у методиках формування прогнозів. Але чітко простежується тенденція невпинного зростання обсягів світового біометричного ринку.

Спробуємо відповісти на таке питання, що сприяє зростанню світового біометричного ринку?

Звісно, всі тенденції навести неможливо, але виокремимо основні:

– збільшення витрат США й Євросоюзу на біометрію;

– значне зростання біометричного ринку в фінансовій сфері;

– вибухове зростання використання біометрії в мобільних обладнаннях;

– реалізація масштабних біометричних проектів у Індії й Пакистані, які насамперед мають соціальну спрямованість;

– запровадження систем автоматизованого прикордонного контролю та програм супроводу авіапасажирів, які часто мандрують;

– початок масового застосування біометричних технологій у різних ком'ютерних і мобільних пристроях (смартфони, планшети і ноутбуки).

---

[1] Эволюция мирового биометрического рынка: региональные аспекты // BIOMETRICS.RU. – 2011. – 25 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Объем мирового биометрического рынка к 2015 году удвоится // BIOMETRICS.RU. – 2012. – 10 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Новый оптимистичный прогноз развития биометрического рынка // BIOMETRICS.RU. – 2013. – 12 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Объем мирового биометрического рынка к 2017 году превысит 16 миллиардов долларов // BIOMETRICS.RU. – 2011. – 17 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

У державах, які виникли на теренах колишнього СРСР, очікується:

– масове запровадження біометричних паспортів другого покоління;

– подальша активізація біометричних систем прикордонного контролю й забезпечення транспортної безпеки;

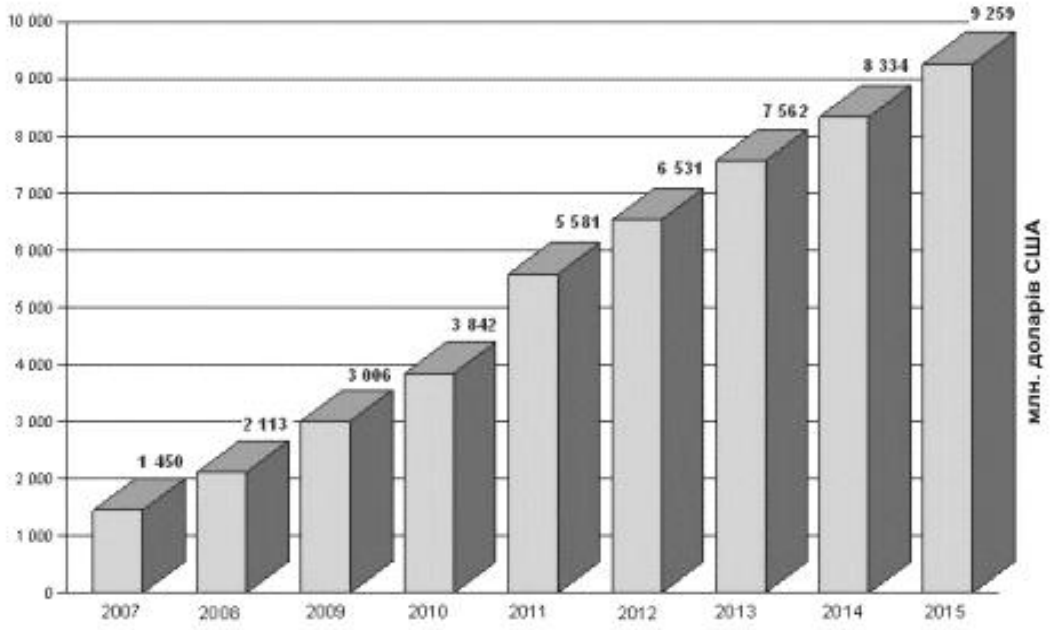
– зростаюча кількість запроваджень біометричних систем контролю доступу й обліку робочого часу, а також підвищення ролі біометрії в системах інформаційної безпеки.

1.6. Перспективи розвитку біометричного ринку та різних типів технологій біометричної аутентифікації та ідентифікації

Біометрія швидко набуває індустріальних рис. Це промислові масштаби виробництва, багатомільйонні замовлення державних і комерційних структур, формування професійного співтовариства.

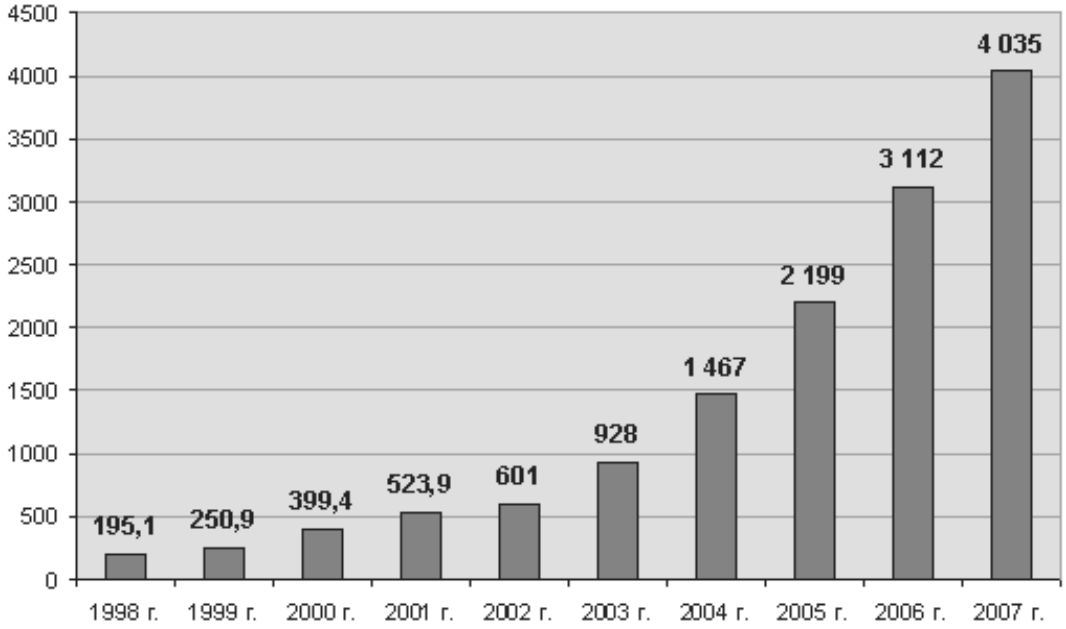
На цьому ринку зростає сегментація і диверсифікація; зростають потреби у стандартизації та уніфікації; загострюється конкуренція, активізуються процеси об'єднань і поглинань. Та, незважаючи на існуючі розбіжності перспективної оцінки обсягу світового біометричного ринку, всі дослідницькі та консалтингові фірми вважають – буде збережена загальна тенденція до подальшого зростання біометричного ринку.

Динаміка зростання світового біометричного ринку, згідно з прогнозом «Acuity Market Intelligence» з 2007 до 2015 року, наведена на мал. 3.



Мал. 3. Динаміка світового біометричного ринку (млн дол.)
(за даними «Acuity Market Intelligence»/AMI/, 2007 р.)

Для підкреслення стійкості тенденції зростання світового біометричного ринку наведемо дані «International Biometric Group» (IBG) про обсяги ринку біометрії в 1998–2007 роках в млн доларів (див. мал. 4)[1].



Мал. 4. Обсяг ринку біометрії в 1998–2007 роках (млн дол.)

Джерело: «International Biometric Group» /IBG/

Як видно з наведених рисунків, незважаючи на розбіжність в обсязі ринку біометрії в 2007 році (погрішність у 2,8 раза), бачимо тенденцію тривалого і стійкого зростання ринку, причому з хорошою динамікою зростання і в минулому (1998–2008 рр.), і в майбутньому (2009–2015 рр.).

Щодо розбіжностей прогнозів, то для порівняння наведемо оцінку обсягу ринку біометрії згідно з даними аналітиків «Frost & Sullivan». Так, 2006 р. він становив 2 млрд дол., а до 2012 р. відповідно до прогнозу повинен був зрости до 7,4 млрд дол.[2]

Якщо порівняти прогноз «Frost & Sullivan» з даними «IBG» за 2006 рік і «AMI» в 2012 році, то похибки становили майже 1,5 раза на користь «IBG» за 2006 р. і 1,13 – на користь «Frost & Sullivan» в 2012 р., відповідно.

Як було наведено у підрозділі 1.5, за даними компанії «Biometrics Research Group» у 2012 році обсяг біометричного ринку у світі становив майже 7 млрд доларів (що збігається з передбаченням аналітиків «Frost & Sullivan»), а в аналізі, наданим компанією «Wintergreen Research», згаданий показник становив лише 5,2 млрд доларів[3].

[1] Боровко Р. Мировой рынок средств идентификации / Р. Боровко // CNews Analytics. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security/...

[2] Союз лица и пальца // Ведомости. – 2007. – 1 февраля. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/digest/...

[3] Новый оптимистичный прогноз развития биометрического рынка // BIOMETRICS.RU. – 2013. – 12 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Значно більше єднання експерти демонструють в оцінці часток ринку, які стосуються різних технологій ідентифікації, – так званої сегментації біометричного ринку. Загалом російські експерти вважають, що найбільш вдалі об'єктивні оцінки ринку біометричних технологій сьогодні та в майбутньому надає компанія «Acuity Market Intelligence»[1].

Першість належить технологіям на основі засобів розпізнавання за папілярними узорами відбитків пальців. Оцінки частки інших технологій у різних оглядах відрізняються, але загальна ієрархія найбільш значущих типів технологій знову-таки збігається. Питома вага кожної технології ідентифікації в загальному обсязі біометричного ринку в 2007 році наведена в табл. 6.

Таблиця 6

Питома вага (%) технологій ідентифікації в загальному обсязі біометричного ринку в 2007 році

Технологія	Частка ринку	
	IBG	Acuity Market Intelligence
Автоматизовані системи ідентифікації за відбитками пальців/«живе» сканування	33,6%	33%
Розпізнавання за відбитками пальців	25,3%	25%
Розпізнавання за обличчям	12,9%	18%
Розпізнавання за райдужною оболонкою ока	5,1%	7%
Розпізнавання за геометрією руки	4,7%	7%
Розпізнавання за голосом	3,2%	5%
Розпізнавання за малюнком вен	3,0%	3%
Розпізнавання за підписом	–	1%
Мультибіометрія	2,9%	–
Програмне забезпечення «проміжного рівня»	5,4%	–
Інше	4,0%	1%

Джерело: Biolink, 2007.

Найближчими роками три великі біометрики (технології ідентифікації за відбитками пальців, обличчям, райдужною оболонкою ока) збережуть домінуючі позиції, але загалом їхня сукупна частка знижуватиметься. Однак передбачається, що до 2017 р. популярність райдужної технології поступиться лише популярності ідентифікації за відбитками пальців, а на третє-четверте місце за популярністю можуть вийти методи ідентифікації людину за голосом.

Але ставити питання: яка ж технологія біометричної ідентифікації краща, – не можна. Адже все залежить від конкретної сфери її застосування. Наприклад, ідентифікацію особи у повній темряві (якщо в цьому є необхідність), краще здійснювати

[1] Митин Владимир. Биометрические технологии, которые мы выбираем / Митин Владимир // PC Week/RE. – 2010. – 09 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

за голосом, а застосування методик, що використовують відбитки пальців, 3-D зображення обличчя або унікальний малюнок райдужної оболонки ока найчастіше використовують під час виготовлення документів, які посвідчують особу, в програмах супроводу авіапасажирів, які часто мандрують, під час перетинання кордону та в інших випадках[1].

Несподіванкою 2007 року можна вважати зниження оцінки перспектив технологій розпізнавання за обличчям на тлі загальносвітового поширення біометричних документів, які посвідчують особу і де цей ідентифікатор поки що є обов'язковим. Негативний прогноз вочевидь обумовлений труднощами, які виникли під час практичної реалізації привабливої ідеї інтегрувати ідентифікацію за обличчям з системами відеоспостереження. У доповіді Європейської комісії був зроблений висновок, який стосується технології розпізнання за обличчям: Точність знижується, коли реєстрація і подальша ідентифікація виявляються віддалені у часі. Вбачається, що буде потрібна регулярна перереєстрація через певний час.

Але в 2012–2013 рр. з'явилось багато публікацій, де наводяться приклади досить успішного використання технології ідентифікації осіб, особливо авіапасажирів, за зображенням обличчя. Експерти вважають, що технології автоматизованого відеоспостереження та розпізнавання людей за обличчям у майбутньому очікує радикальне поліпшення ефективності й якості. Так, у США в інтересах департаменту держбезпеки (DHS) за контрактом вартістю понад 5 млн доларів фірмою «Electronic Warfare Associates» створюється система, яка має абревіатуру BOSS («Biometric Optical Surveillance System (BOSS) at Stand-off Distance» – «Біометрична система для дистанційного оптичного спостереження»). Згідно з наявною інформацією, алгоритми розпізнавання індивідуумів за формою обличчя працюють чудово з світлинами (фотографіями) типу «для документів», однак у реальних умовах за допомогою відеоспостереження одержати на вулицях і в інших громадських місцях якісні знімки, які б були придатні для ідентифікації фігурантів спостереження, дуже складно.

Але практично всі фахівці з біометрії вважають, що такі системи «прийшли, щоб залишитися». У деяких ситуаціях вони досить ефективно працюють сьогодні, але загалом стрімкий прогрес таких технологій очевидний і він відбувається дуже швидко[2].

Позитивною новиною є значне зміцнення позицій засобів ідентифікації за малюнком вен у сфері банківських технологій. Але необхідно зазначити, що нині набула поширення ідентифікація за малюнком вен поки що тільки в Японії. Крім того, проблеми може створити і боротьба, що посилюється, між двома конкретними видами імплементації цієї технології (сканування малюнка вен на долоні та на пальці).

Останнім часом позитивні перспективи отримали також засоби ідентифікації за голосом – вони набувають дедалі більшого поширення, особливо у фінансовій сфері (телефонний банкінг тощо) і в складі автоматизованих кол-центрів.

За результатами дослідження галузевого ринку, опублікованого Біометричним інститутом у Лондоні у вересні 2013 року (було опитано 276 експертів, які є членами згаданого інституту, а також представляли інші галузі IT-індустрії), двома найважливішими трендами нині є подальше впровадження біометричних технологій у прикордонному

[1] Митин Владимир. Биометрические технологии, которые мы выбираем / Митин Владимир // PC Week/RE. – 2010. – 09 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Технологии биометрической идентификации по лицу могут повысить свою эффективность // DGL.RU. – 2013. – 02 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

контролі та їх більше поширення у повсякденному житті. Що ж стосується майбутнього галузі, то учасники опитування вважали, що незабаром відбудеться активна інтеграція біометричних і мобільних технологій. Ці прогнози підтвердились.

Щодо сегментації галузевого ринку, то фахівці були одностайні в своїх висновках про те, що найпопулярнішими були та залишаються системи, які реалізують технології ідентифікації за відбитками пальців і за обличчям; третє й четверте місця ділять рішення, що засновані на розпізнаванні користувачів за малюнком вен і голосом.

Головними причинами, що перешкоджають подальшому й ще більшому поширенню біометричних систем, учасники опитування вважають їхню досить високу вартість і слабку поінформованість осіб, котрі ухвалюють рішення про переваги біометричних технологій[1].

Розглянемо деякі особливості розвитку державного та корпоративного секторів біометричного ринку.

Державний сектор у перспективі буде ключовим замовником біометричних компаній і головним рушієм ринку. Але він зумовлює в основному екстенсивний розвиток галузі. Разом із традиційним використанням біометричної ідентифікації в криміналістичних цілях сьогодні біометрія активно запроваджується в прикордонному контролі й у зв'язку з цим завершується масовий перехід до паспортно-візових документів нового покоління; без біометричних технологій неможливо уявити сучасні національні ідентифікаційні картки та інші ідентифікаційні документи (наприклад, посвідчення державних службовців, водійські посвідчення нового типу). У майбутньому в більшості країн держсектор і суспільний сектор повинні збільшити свою частку через реалізації програми так званого електронного урядування.

Увага держсектора до біометрії позитивно вплине ще на два аспекти. Перший із них пов'язаний з гармонізацією і стандартизацією технологій: зрозуміло, що за всього прагнення до суверенітету інформація в біометричних паспортах громадян однієї країни повинна без проблем зчитуватися технічними засобами, які використовуються прикордонниками інших держав. Другий аспект допускає активну участь державних замовників у фінансуванні ресурсоємних розробок у галузі мультибіометрії. У 2007 році Міністерством оборони США було виділено 70 млн доларів на формування єдиного репозиторію (банку даних), в який почали об'єднувати наявні дані, що були зібрані різними підрозділами Пентагону. В єдину базу даних об'єднували такі біометричні ідентифікатори, як відбитки пальців і долонь, зображення лиця осіб, райдужної оболонки очей, ДНК і ін. У 2008–2009 рр. цим же відомством аналогічна щорічна сума була витрачена на закупівлю мобільних засобів ідентифікації за відбитками пальців, обличчям та райдужною оболонкою ока, що були використані насамперед у гарячих точках земної кулі (Ірак, Афганістан тощо).

Корпоративний або комерційний сектор стимулює інтенсифікацію розробок нових продуктів і послуг. Разом зі збереженням традиційного інтересу до біометричних рішень щодо забезпечення інформаційної безпеки, контролю фізичного доступу і ведення обліку робочого часу комерційні структури зараз відчувають нагальну потребу в ефективних системах управління ідентифікацією користувачів фінансових послуг, заохочення купівельної лояльності, обслуговування пасажирів транспорту (насамперед авіаційного).

[1] Биометрический институт опубликовал результаты очередного исследования отраслевого рынка // BIOMETRICS.RU. – 2013. – 06 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Як самостійний сегмент можна виокремити так званий «*суспільний»* (тобто в основному некомерційний) *сектор*. Найважливішими споживачами якого є освітянські установи, наукові організації, культурні та медичні установи.

Останнім часом стрімко збільшує свою частку на ринку «*споживчий» сектор* (consumer ID), де засоби біометричної ідентифікації використовують приватні особи для власних потреб. Як ключові сфери застосування біометрії тут можна виокремити захист інформації, що зберігається у ноутбуках, лептопах і смартфонах (для чого здебільшого використовують вбудовані в комп'ютерні пристрої сканери відбитків пальців), ідентифікацію користувачів стільникових телефонів та подібних пристроїв, а також підтвердження транзакцій в системах мобільної комерції (зокрема, які здійснюються за технологією «Near Field Communications» /NFC/)[1].

На ринку біометричних продуктів, разом із відомими лідерами – «Identix», «Digital Persona», «Precise Biometrics», «Visionics», «Ethentica», «BioScript», «Secugen», «AcSys Biometrics», з'являються нові корпорації, які не є спеціалізованими в галузі біометрії, наприклад, «Sony», «LG», «Compaq», «Apple», «Sumsung» та ін. Цей факт засвідчує значне зростання привабливості біометричного ринку і те, що незабаром біометричні пристрої стануть звичним явищем у нашому побуті.

1.7. Різні типи технологій аутентифікації та ідентифікації – суперництво чи співпраця

Практично всі системи інформаційної безпеки застосовують для контролю доступу різні засоби аутентифікації та ідентифікації користувачів. Як вже зазначалось, ідентифікація користувача – це отримання від нього відповіді на питання: «Хто ти?». А аутентифікація – це вимога: «А зараз доведи, по суті, що ти саме той користувач, за якого себе видаєш» і подальша перевірка наданих доказів. Тобто перевірка чи дійсно користувач є тією особою за кого себе видає.

Отже, аутентифікація (верифікація) – це порівняння, за якого біометрична система намагається аутентифікувати (верифікувати) особу користувача, тобто з'ясувати факт її достовірності: чи ти та особистість, за яку себе видаєш. Ще раз нагадаємо, що засоби аутентифікації за принципами дії можно поділити на три групи: «що Ви знаєте» («you know»), «що Ви маєте» («you have») і «хто Ви є» («you are»). Усі пристрої аутентифікації та ідентифікації користувачів використовують як засоби верифікації спеціальні носії інформації, які застосовують один із вказаних принципів або їх комбінацію. Кожен із перелічених методів має свої позитивні якості та недоліки. Розглянемо основні з них.

У парольному принципі («що Ви знаєте») вимагається наявність PIN-кода, але як свідчить практика досить часто паролі забуваються, відтак користувачі записують їх на видному місці, передають іншим особам, а головне у разі потреби вони можуть бути підібрані за допомогою спеціальних програм (питання тільки в часі, необхідному для підбору).

[1] Лукашов И. Биометрия становится индустриальной технологией / И. Лукашов // CNews. – 2007. – 21 августа. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security2007/articles/biomarket.shtml…

Із 1997 року і досі в системах контролю доступу неподільно панували смарт-картки (принцип дії – «що Ви маєте»), оскільки вони до початку масового використання біометричних технологій були найбільш оптимальні з погляду безпеки та зручності використання (можливості підключення до корпоративних ресурсів поза офісом, із так званого «ворожого» середовища). За всіх плюсів смарт-карток у них є тільки один досить значний недолік: для їх використання необхідний зчитувач. Це призводить, по-перше, до зниження мобільності: наприклад, користувачеві, котрий відправляється у відрядження з ноутбуком, доводиться брати з собою додатковий пристрій. А, по-друге, підвищує ціну рішення[1].

Смарт-картки пройшли певну еволюцію: спочатку на ринку з'явилися Memory Card, потім – картки із захищеною пам'яттю – Protected Memory Card. Пізніше з'являються CPU Card (мікропроцесорні) – картки з чіпом, що реалізовують апаратним шляхом алгоритми шифрування. Сучасні смарт-картки мають значну захищену пам'ять, підтримують технології, які реалізовані в операційних системах (Smartcard Logon, MS CAPI, PKCS #11 і т. д.), легко можуть бути інтегровані в операційні системи та більшість програмних додатків крупних вендорів (наприклад, можна навести додатки IBM – Lotus Notes, Tivoli).

У 1998–1999 роках на стику смарт-карткових технологій і технологій електронних ключів для захисту програмного забезпечення з'явився новий пристрій – USB-токени (після появи в пристроях персональних комп'ютерів уніфікованого роз'єму – USB-порта). Фірма «Aladdin Knowledge Systems», яка представляла ізраїльські технології і яка згодом стала компанією зі світовим ім'ям, першою створила і запатентувала USB-ключ. У межах міжнародної співпраці був створений «eToken RIC». USB-токени абсолютно аналогічні смарт-карткам за своїми функціональними характеристиками і ступенями захищеності, але виконані у вигляді брелка.

Зчитувач, по суті, розміщений разом зі смарт-карткою в єдиному USB-пристрої. Відповідно, ціна у токенів нижча і вони за такого ж рівня безпеки забезпечують ще і мобільність користувачів.

Смарт-картки і USB-ключі як засоби аутентифікації повинні відповідати таким умовам:

– можливості зберігання «digital ID» тобто сукупності ідентифікаційної інформації в одному пристрої;

– універсальності та зручності застосування;

– мати вбудований криптопроцесор;

– наявності великого об'єму захищеної пам'яті з PIN-кодом;

– можливості підтримки індустріальних стандартів, а також міжнародних і державних стандартів безпеки, наприклад, таких, як FIPS, Common Criteria, ДСТУ (ГОСТів);

– максимальній відкритості архітектури з збереженням належного рівня безпеки.

Вважається, що подальший розвиток смарт-карткових технологій пов'язаний із застосуванням технологій безконтактних смарт-карток і розробки біометричної ідентифікаційної карти із вбудованим сканером відбитків пальців.

На ринку інформаційної безпеки за наявності інших однакових умов застосування тієї чи іншої технології визначається можливістю вибору рішень, які зможуть підтриму-

[1] Груздев С. Интервью: Мы наблюдаем заметный рост интереса к обеспечению внутренней безопасности компании / Сергей Груздев // CNews. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security/interview/aladdin/...

вати максимальну кількість стандартів: і індустріальних, і міжнародних сертифікаційних стандартів[1].

Останніми роками безконтактний зв'язок на короткій відстані став об'єктом окремого промислового напряму, якому приділяють все більшу увагу. RFID (Radio Frequency Identification – радіочастотна ідентифікація) нині став загальновизнаною технологією для світової транспортної галузі. Розміщення на товарах і вантажних піддонах мініатюрних радіопередавачів, так званих RFID-бірок, стало новим методом ідентифікації, який витісняє традиційний спосіб, заснований на використанні штрих-кодів.

Після започаткованого охоронними бізнес-структурами використання RFID-технології виник підвищений інтерес до можливості застосування цієї технології для маркування товарів громадського споживання та для контролю потоків товарів на всьому шляху їх доставки до кінцевого користувача. Реалізація цієї ідеї стала можливою кілька років тому, коли такі компанії, як «Alien Technologies» і «Hitachi» почали виробництво RFID-бірок розміром менше головки англійської шпильки для їх розміщення на різних товарах.

Особливо широкий вжиток застосування RFID-бірок набуло на суспільному транспорті та в операціях із кредитними картками.

Транспортні оператори з великим інтересом стежать за процесом розробки безконтактних квитків, які можуть стати гідною заміною широко вживаних магнітних стрічок, що нанесені на папір або картон. За наявності безконтактного квитка цілком достатньо, щоб він просто опинився у «полі зору» зчитувача. Причому пристрої з RFID-зчитувачем не будуть зношуватися, як ті, що обробляють квитки з магнітною стрічкою.

Але головна перевага безконтактних квитків, які застосовують RFID-технологію, повною мірою виявляється у збільшенні пропускної спроможності в години пік – секунди, заощаджені на обробці проїзного документа кожного пасажира, дають значний ефект у тих випадках, коли йдеться про щільні пасажирські потоки. Перші пристрої з використанням безконтактної технології на транспорті пройшли випробування в Гонконзі понад 10 років тому, після чого цей досвід почали використовувати багато інших світових транспортних операторів, зокрема в Парижі та Лондоні.

У бізнесі, пов'язаному з використанням кредитних карток, увагу на безконтактні картки звернули в останні десять років, причому всі основні гравці в цьому секторі зараз мають свої програми з розробки та використання безконтактного устаткування. Виробники кредитних карт вже опанували цю технологію – як наслідок, значно знизилися ціни на мікрочіпи, що поєднують традиційну технологію смарт-карток із вбудованими безконтактними функціями.

Для фірм-гігантів, що працюють у сфері кредитних карт, використання нововведення допомагає їм завоювати додаткову частку ринку в дрібних грошових переказах, які раніше традиційно здійснювалися готівкою. У разі продажу в роздріб зменшення черг перед касами є головним стимулом введення нової технології. Чим менше часу необхідно для обслуговування клієнта, тим більша виручка і менше нарікань від відвідувачів таких закладів.

У сфері забезпечення безпеки безконтактні технології в новому столітті використовуються у найрізноманітніших цілях. Так, вони застосовуються в пристроях, що забезпечують контроль доступу, – дедалі більше компаній обирають безконтактні брелки

[1] Груздев С. Интервью: Мы наблюдаем заметный рост интереса к обеспечению внутренней безопасности компании / Сергей Груздев // CNews. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security/interview/aladdin/

(токени) або безконтактні пропуски з вбудованими відповідними чіпами замість традиційних карт із магнітною стрічкою. На ринку безпеки безконтактні технології вважаються вже цілком сталими і надійними.

Більшість безконтактних пристроїв використовують безконтактний зв'язок на дуже коротких відстанях. Із технічного погляду існують три різні діапазони зчитування: індуктивний зв'язок для близьких відстаней, що призначений для радіусів зчитування в 1 або 2 см, дистанційний зв'язок, що функціонує на відстані приблизно до 1 м, і зв'язок для великих відстаней. Нині дев'ять із десяти безконтактних систем використовують дистанційний зв'язок.

Якщо бути точнішим, дистанційний зв'язок підрозділяється на дві підгрупи – надблизький і близький. Надблизький зв'язок, який вперше почав пропонуватися на ринку США за абревіатурою NFC (near field communication), працює на відстанях до 5–15 см і зазвичай базується на стандарті ISO 14443. Сьогодні ця технологія є домінуючою в таких галузях, як, наприклад, зчитування кредитних карт або ринок радіочастотних чіпів. Радіус дії близького зв'язку дещо більший – до 1 м. Для пристроїв, що використовують близький зв'язок, також існує міжнародний стандарт – ISO 15963.

Збільшення дистанції зчитування має і переваги, і потенційні проблеми. Зі зростанням радіуса дії підвищується ймовірність одночасного отримання даних із декількох радіочіпів, що знаходяться в цьому радіусі, або ж небезпека зняття інформації особою, котра не має на це відповідних повноважень.

Остання обставина викликає особливу занепокоєність у проектах, пов'язаних із використанням нових електронних документів, які зараз посилено вводяться у всьому світі, і містять як біометричні дані, так і мікропристрої для безконтактного зчитування інформації (відповідно до стандарту ISO 14443). От чому такі документи нового покоління забезпечуються ще і кодовим захистом, який значно затруднює можливість зчитування електронної інформації.

Посадова особа на пункті прикордонно-паспортного контролю насамперед повинна перевірити серійний номер паспорта, який він використовує як ключ до безконтактного зчитування інформації з чіпа. Так, PIN-код у поєднанні зі спеціальною системою безпеки, які закладені в мікрочіп, можуть використовуватись у кредитних картках для зниження небезпеки неавторизованого доступу до інформації[1].

Нині безпека і комфорт ідентифікації дедалі більше забезпечуються біометричними рішеннями, побудованими за використанням принципу «хто Ви є», які стають більш популярними та престижними.

Стала очевидною необхідність точної ідентифікації в місцях масового скупчення людей, за контролю перепусток і звірки документів. Насамперед ця проблема стосується безпеки транспортних систем – аеропортів, вокзалів, морських портів, метрополітену, а також безпеки інформаційних державних і міждержавних систем – паспортно-візових, митних, міграційних і оперативних служб. Звичайних паспортного і фейс-контролю (контроль за лицем особи) стало явно недостатньо. Всі надії тепер пов'язані з використанням біометричних технологій, що дозволяють перевіряти особистості великої кількості індивідуумів, що проходять через точку контролю.

Для збільшення точності в режимі ідентифікації доцільно використовувати декілька біометричних методів водночас – так звані мультибіометричні, мультимодальні і комбіновані системи, а також багатофакторні системи.

---

[1] Школа технологий рынка безопасности // БДИ. – 2008. – № 1. [Электронный ресурс]. – Режим доступа: http://www.bdi.spb.ru/arch...

Одне з найпоширеніших мультимодальних рішень – розпізнавання за відбитками декількох пальців. Точність, що досягається у разі ідентифікації всіх п'яти або десяти пальців, поки що залишається однією з найвищих. Але, незважаючи на це, із низки причин практичне використання таких систем поки що обмежене.

Мультимодальним є і розпізнавання особи, що охоплює дво- і тривимірні зображення (так звані 2D- і 3D-методи). Об'єднання 2D- і 3D-методів розпізнавання особи дозволяє звести в єдине ціле переваги кожного з цих способів. Основні виробники вже почали інтеграцію цих двох методів. Найімовірніше, що незабаром розпізнавання особи з використанням обох методів впізнавання розглядатиметься як один біометричний метод.

Там, де необхідна ідентифікація за базами даних у декілька сотень тисяч або мільйонів чоловік (це може бути, наприклад, виконання завдання пошуку людини із заданими біометричними характеристиками в державній базі даних виданих паспортів або віз), найбільш доцільним є використання можливостей мультимодальних і комбінованих мультибіометричних систем типу: «багато пальців», «палець (пальці) + обличчя», або «палець (пальці) + райдужна оболонка ока» тощо.

Останнім часом для забезпечення безпеки під час експлуатації сучасних транспортних терміналів і організації контрольованого доступу в службові приміщення, які критично важливі з погляду безпеки, більшого поширення набувають ідентифікаційні системи, які застосовують метод поєднання біометрики та ідентифікаційних карт або жетонів (так званий «багатофакторний» метод), що дозволяє, на думку експертів, значно підвищити ефективність такої багатофакторної системи.

У банківській сфері дедалі більше поширюються інтелектуальні смарт-картки з мікропроцесорами, в яких зберігається біометрична інформація. У смарт-картках із мікропроцесорами може зберігатися не тільки цифрова фотографія власника, але й відбитки пальців та інші унікальні параметри.

Першими такого ступеня розвитку подібні технології досягли в Японії, де смарт-картки ще в минулому десятилітті зберігали інформацію про райдужну оболонку ока та малюнок вен на руках[1].

Одним із прикладів сучасних розробок біометричної смарт-картки є карта типу FSC-3012 компанії «Fidelica Microsystems». Прес-реліз компанії повідомляє, що нова смарт-картка повністю відповідає галузевим стандартам ISO 7810/16 і оснащена вбудованим сканером відбитків пальців.

За словами віце-президента «Fidelica Microsystems» з маркетингу і розвитку бізнесу Роберта Аллена (Robert Allen), FSC-3012 включає також мікропроцесор і програмне забезпечення для розпізнавання біометричних ідентифікаторів власника картки. Як основні сфери застосування цього нововведення називають системи контролю фізичного доступу та системи захисту інформації.

До ключових переваг біометричної смарт-картки належать:

1. Наявність в карті вбудованого сканера відбитків пальців, внаслідок чого не потрібно будь-якої модифікації інформаційних систем, в яких може застосовуватися FSC-3012.

2. Виключення втрат часу під час обміну інформацією між карткою і зовнішнім зчитувачем – на практиці помічено відсутність конфліктів між цими пристроями.

3. Цифрова модель біометричних ідентифікаторів зберігається в пам'яті самої смарт-картки і нікуди не транслюється.

[1] Толкачева Е. Стопроцентный результат / Е. Толкачева // CNews. – 2007. – 9 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Крім того, біометрична смарт-картка компактна і вартість її прийнятна[1].

Але не все так просто з впровадженням біометричної смарт-картки. Так, на початку 2012 року фонд «Eurostars», сформований Єврокомісією для підтримки інноваційних бізнесів у країнах ЄС, виділив грант в 12 млн норвезьких крон, який спрямований на розробку біометричної ідентифікаційної карти із вбудованим сканером відбитків пальців. Грант одержали норвезька фірма «IDEX» та її французький партнер – компанія «UINT».

Упродовж двох років розробники зобов'язалися створити смарт-карту, в яку буде інтегрований надзвичайно тонкий сканер відбитків пальців. Таке рішення дозволить звести до мінімуму кількість процедур, пов'язаних з обробкою біометричних персональних даних користувача: всі вони виконуватимуться самою картою і не будуть вимагати участі у цьому процесі пристроїв, які розташовані поза межами такої картки.

Окрім того, у смарт-карті мають застосовуватися бездротові технології комунікацій близького поля (near field communication – NFC). На практиці це означає, що власник карти зможе в безконтактному режимі використовувати її в різних платіжних системах (наприклад, для оплати проїзду в суспільному транспорті, оплачувати паркування, придбання товарів у магазині тощо), швидко, легко й безпечно підтверджувати свої повноваження на проведення відповідної трансакції[2].

Наведемо основні етапи процесу реєстрації і видачі сучасної багатофакторної та мультибіометричної смарт-карти:

1. Введення необхідних установчих даних (прізвище, ім'я, інколи й по батькові, демографічні відомості тощо).

2. Сканування та кодування обраних біометричних ідентифікаційних параметрів:

– електронне фотографування;

– сканування й кодування відбитку/ів/ пальця/ів/;

– сканування й кодування райдужної оболонки ока.

3. Запис біометричних кодів на смарт-карту з криптозахистом.

4. Збереження інформації в локальній і центральній базах даних.

5. Друк і розміщення фотографії та персональних даних на смарт-картці[3].

Уряди багатьох країн вивчають можливості масового застосування смарт-карток, які інтегровані з біометричними технологіями. На думку експертів, проекти «Національної ідентифікації» вже можна розглядати як основні рушії ринку, особливо в Азіатсько-Тихоокеанському регіоні. Біометричні ідентифікаційні картки широко запроваджуються в Індії, Пакистані та Малайзії. Влада Японії та Китаю також розпочали пілотні проекти. Про масштабність проектів свідчить інформація, що компанія «Daon» (США), яка спеціалізується на розробці програмного забезпечення, допомагає уряду Індії запроваджувати загальнодержавну біометричну програму, в межах якої посвідчення особи повинні одержати понад 1 млрд людей[4].

---

[1] Биометрическая смарт-картка со сканером отпечатков пальцев // BIOMETRICS.RU. – 2007. – 12 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Еврокомиссия профинансировала разработку биометрической смарт-карты // BIOMETRICS.RU. – 2012. – 19 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] PAPILLON.RU. [Электронный ресурс]. – Режим доступа: http://www.papillon.ru/biometric_passportt1.php...

[4] Биометрические идентификационные карты в США обрели второе дыхание // Экспертный центр электронного государства. – 2013. – 23 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

За висновком експертів агентства «Frost & Sullivan», інтеграція біометрії і смарт-карток забезпечує високий рівень безпеки, якого не можна досягти, застосовуючи відокремлено ці технології.

Замовники (особливо, урядові кола) чудово усвідомлюють потенціал використання цих інтегрованих рішень у різних галузях: від розвитку сільськогосподарських районів країни до забезпечення найвищого рівня безпеки та контролю під час охорони будівель державних організацій[1].

Слід згадати, що через майже десятиліття після виходу Президентської директиви про національну безпеку США HSPD-12, Міністерство внутрішньої безпеки (МВБ) почало реалізовувати амбіційний проект з інтеграції в національні – ID-карти нових біометричних параметрів.

У травні 2013 року МВБ США опублікувало умови підряду на суму 102 млн доларів із виконання робіт із відновлення ID-системи та імплементації до неї таких біометричних даних, як розпізнання за обличчям, за відбитками пальців і райдужної оболонки ока.

За Директивою адміністративно-бюджетного управління США, яка спрямована на подальше впровадження директиви HSPD-12, PIV-карта, яка здійснює верифікацію особи, стане основним інструментом аутентифікації повноважень для доступу до послуг, мереж й інформаційних систем.

Як вважають фахівці, процедура координації багатьох біометричних ідентифікаторів буде надскладним процесом, а вартість сховища для зберігання інформації в межах такого проекту – дуже високою. Ще однієї проблемою для МВБ стане підтримка всієї системи в ефективному й актуальному стані.

Оскільки діяльність Міністерства внутрішньої безпеки охоплює широкий спектр напрямів – від безпеки кордонів до реагування на надзвичайні ситуації, – то саме воно може виступати законодавцем моди у частині організації безпечної ідентифікації для організацій на всіх рівнях влади та у промисловості.

Який вид матиме нова смарт-карта?

Зовнішньо вона може виглядати як ламінована пластикова карта старого зразка, але буде містити в електронному вигляді набагато більше даних, ніж прізвище та ім’я, адреса та фото. Вбудовані комп’ютерні чіпи зможуть виконувати ідентифікацію різних відомостей, зокрема оцифрованих відбитків пальців, райдужної оболонки ока та форми лиця особи.

PIV-карта може мати не тільки штрих-код, RFID-позначку (радіочастотна ідентифікація) і магнітну машинозчитувальну стрічку-смужку, але й вбудований процесор даних для сегментування та зберігання інформації, зокрема для автоматичного віддаленого відновлення інформації.

Фахівці вважають, що може знадобитися приблизно 30 етапів дій, необхідних для виробництва такої карти[2].

Отже, невід’ємна риса сучасного IT-ринку – інтеграція смарт-карток і біометрії як найбільш перспективних й ефективних складових сучасних інформаційних технологій доступу.

[1] Новые перспективы биометрических смарт-карт // BIOMETRICS.RU. – 2008. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрические идентификационные карты в США обрели второе дыхание // Экспертный центр электронного государства. – 2013. – 23 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

І в національних ідентифікаційних картах (ID-cards), і в паспортно-візових документах нового покоління активно застосовуються як біометричні технології, так і технології смарт-карток.

Але технології інтелектуальних смарт-карток уже стали багатофункціональними: їх використання виходить за межі проектів «Національної ідентифікації» та банківської діяльності й охоплюють торгові, транспортні, медичні, страхові, телекомунікаційні компанії, підприємства житлово-комунального господарства, паспортно-візові служби, установи соціального захисту, сфери обслуговування, готелі тощо[1].

Ще одна досить широка сфера комплексного застосування технологій смарт-карток і біометрики – забезпечення безпеки доступу до інформаційних мереж, систем і комп'ютерних пристроїв.

Тепер власники смарт-карток, у пам'ять яких записаний цифровий сертифікат для входу в Windows, можуть замінювати введення PIN-коду картки простою, зручною і надійною ідентифікацією за унікальними невідчужуваними біометричними параметрами – відбитками пальців.

[1] BIOMETRICS.RU – информационный спонсор выставки CARDEX & IT SECURITY // BIOMETRICS.RU. – 2008. – 29 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Розділ 2

ДАКТИЛОСКОПІЯ. ІДЕНТИФІКАЦІЯ ЗА ВІДБИТКАМИ ПАЛЬЦІВ І ДОЛОНЬ. ВИКОРИСТАННЯ ДЛЯ ІДЕНТИФІКАЦІЇ ГЕОМЕТРІЇ І ТЕРМОГРАМ РУК І ПАЛЬЦІВ

2.1. Загальна історія дактилоскопії

Шкірні узори на внутрішній стороні рук людини були відомі ще представникам стародавньої медицини. Зараз неможливо точно встановити у кого, де і коли виникла думка використовувати відбиток пальця для встановлення особистості. Навіть не відомо, хто перший почав використовувати термін «дактилоскопія» (за деякими даними цей термін увів Жуан /Хуан/ Вуцетич /Вусетич/).

Дактилоскопія є однією із найдавніших наук. Як уже було зазначено, ознаки знання дактилоскопії можна простежити у стародавніх ассирійців і вавилонян, які використовували відбиток пальця як особисту печатку або підпис, залишаючи відбитки на глиняних табличках і захищаючи ці документи від підробок. Очевидно, у стародавньому Вавилоні та Ніневії знали, що за допомогою відбитка пальця можна однозначно встановити особу.

Якщо ж зважати на історичні факти, виникнення дактилоскопії потрібно шукати в древньому Китаї. 1904 року китайський археолог Ліу Тьєйін випустив у Шанхаї книгу, де наведені факсиміле стародавніх китайських глиняних печаток, що належать до дохристиянської ери. Частина печаток – це зафіксовані на глині відбитки пальців. Так власник печатки мав можливість довести своє право на володіння цією печаткою. Використання відбитків папілярних узорів пальців як унікального і непідробного підпису власника впроваджувалося у Китаї впродовж століть. Поступово відбитки пальців почали використовуватися не тільки як підпис або особисту печатку власника – папілярний узор почали вивчати і наділяти конкретним змістом. Так, в Китаї було прийнято передбачати долю саме за папілярним узором. Окрім того, кожна мати чудово знала відбитки пальців своєї дитини, а опис цього узору навіть розглядався в суді як доказ материнських прав. У Китаї використання відбитків пальців широко застосовувалося не тільки в побуті, але й криміналістиці.

Ось що пише про це Гейндль Роберт у статті «Дактилоскопія та інші методи кримінальної техніки в справі розслідування злочинів», яка була надрукована 1927 року:

Китайці застосовують цей спосіб, принаймні в частині країни, для того, щоб ідентифікувати осіб, що скоїли тяжкі злочини. Ми фотографуємо їх обличчя – вони отримували відбитки їх пальців, які зберігалися в спеціальному каталозі. Якщо злочинець знову потрапляв до рук поліції, повторно отриманий відбиток порівнювався з наявними. Китайці вважають свій метод надійнішим і простішим за наше фотографування, оскільки обличчя злочинця з часом може бути змінене до невпізнання, а також бути замаскованим волоссям, бородою та іншими штучними засобами[1].

У Європі на можливість використання відбитків пальців для ідентифікації особи звернули увагу значно пізніше. Першим європейцем, який зацікавився узорами папілярних ліній і почав їх вивчати, був професор анатомії Болоньського університету Марселло Мальпіги. 1686 року у своєму творі він досить детально дає опис ліній на долонній поверхні руки. Але тільки 1823 року професор з Університету міста Бреслау (нині Вроцлав) Іоганн Пуркиньє опублікував тези про можливість класифікації папілярних узорів, використовуючи для обґрунтування наявність дев'яти різних типів узорів. І хоча запропонована ним система класифікації не була належно підтримана, це було першою спробою створення системи дактилоскопічної класифікації.

Сучасну історію становлення європейської дактилоскопії пов'язують з іменами англійців Вільяма Гершеля і Генрі Фолдса.

Вільям Гершель служив у Індії в 1853–1878 роках та був першим європейцем, котрий вирішив використовувати відбитки пальців для розшуку або встановлення конкретних індивідуумів. Напевно, до такого рішення його підштовхнуло тісне спілкування з місцевими жителями, які вже тоді мали мали уявлення про унікальність папілярних узорів пальців. Спочатку В. Гершель використовував дактилоскопію під час виплати допомоги місцевим жителям. Індуси, які для європейця були одинакові, часто користувалися цим, намагаючись отримати гроші, що їм виплачувались, повторно. Щоб унеможливити подібні махінації, В. Гершель велів ставити відбитки пальців на платіжних квитанціях і в спеціальній реєстраційній книзі для порівняння, що дозволяло безпомилково встановлювати особу одержувача. Потім В. Гершель почав застосовувати дактилоскопію в одній із в'язниць округу. У кожного новоприбулого ув'язненого знімали відбиток пальця, щоб судді й інші чиновники, які приводили до в'язниці тих, хто завинив, могли ідентифікувати приведеного та переконатися, чи не допустив підміну особи тюремний сторож, виводячи злочинця з тюрми, оскільки помилки в персональному розпізнанні злочинців у ті часи відбувались досить часто.

Думку про використання відбитків пальців для встановлення особистості висловив Генрі Фолдс, котрий працював тоді в токійському госпіталі. Генрі Фолдс почав вивчати відбитки пальців із 1870 року, після того, як виявив відбиток пальця на стародавньому гончарному виробі. 1880 року в британському науковому журналі «Nature» була опублікована його стаття про використання папілярних відбитків пальців для встановлення особи. Крім того, доктор Генрі Фолдс розробив свою систему класифікації відбитків пальців і вперше провів ідентифікацію за відбитком, залишеним на скляній пляшці. Г. Фолдс видав і посібник для зняття відбитків пальців, де запропонував знімати відбитки всіх пальців.

Після опублікування результатів своїх досліджень Г. Фолдс надіслав пояснення до створеної ним системи класифікації і методу реєстрації відбитків пальців Чарльзу Дарвіну. Знаменитий учений не зміг внаслідок старості та хвороби особисто поспілкуватися

[1] Пахомов С. Отпечаток пальца вместо пароля / Сергей Пахомов // КомпьютерПресс. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Archive/...

із Г. Фолдсом, але передав усі матеріали відомому англійському антропологові серові Френсісу Гальтону (1822–1911 рр.).

Ідеї В. Гершеля і Г. Фолдса отримали подальший розвиток у працях Френсіса Гальтона, в яких були викладені основи так званої класичної дактилоскопії. Використовуючи праці доктора Г. Фолдса і В. Гершеля, Ф. Гальтон встановив індивідуальність і незмінність відбитків пальців упродовж усього життя. Перші дані своїх досліджень Ф. Гальтон виклав у своїй книзі «Finger prints», що була надрукована в Лондоні 1892 року. У цій роботі він обґрунтував можливість використання дактилоскопії для ідентифікації особи і виклав розроблену ним систему класифікації відбитків пальців. Основу системи класифікації Френсіса Гальтона становили три базові узори – у формі петлі (loop, L), дуги (arch, A) і завитка (whorl, W), а також їх розподіл на десяти пальцях, наприклад, LLAWL/LWWLL.

Ф. Гальтон довів, що всі 10 пальців однієї і тієї ж особи мають 10 різних узорів. Унікальність папілярних узорів ґрунтувалася на тому, що, за розрахунками Ф. Гальтона, можливі 64 млрд узорів сосочкових ліній, відмінності в яких можна встановити цілком точно. Загальна кількість людей на планеті тоді становила приблизно 1,6 млрд осіб, тобто ймовірність збігу двох відбитків пальців, що належать різним людям, була надзвичайно малою. Система класифікації Френсіса Гальтона згодом отримала подальший розвиток: почали розглядатися не тільки типи узорів, але й унікальні особливості самих ліній. Виникло навіть таке поняття, як «minutiae», або деталі Гальтона.

Упровадження дактилоскопії в Європі відбувалося зовсім непросто. В Європі вже існувала та широко використовувалася біометрична система ідентифікації особистості, розроблена 1870 року французьким антропологом Альфонсом Бертільоном. Упродовж декількох років А. Бертільон працював над системою реєстрації карток із характеристиками злочинців, завдяки якій за декілька хвилин можна було встановити чи є у картотеці відомості про людину, яка цікавить поліцію. На початок січня 1883 року картотека А. Бертільона налічувала 500 карток, в середині січня – 1000, а на початок лютого – вже приблизно 1600. Співробітники паризької поліції, які застосовували метод А. Бертільона, охрестили його «бертільонажем».

Основою системи А. Бертільона були фізичні розміри і різні ознаки такі, як ширина черепа, довжина стопи, довжина середнього лівого пальця, колір волосся, колір очей тощо. Групуючи індивідуальні характеристики людини, її можна було віднести до однієї із 243 категорій, що передбачалися класифікаційною системою. Антропометрія як спосіб ідентифікації особи досить успішно використовувався впродовж 30 років, будучи першою європейською системою ідентифікації особи, проте після виходу в світ книги Ф. Гальтона її доля була приречена.

Хуан Вусетич, який перебував на службі в поліції Аргентини, також працював над системою класифікації відбитків пальців, ґрунтуючись на працях Ф. Гальтона.

1892 року він провів першу ідентифікацію злочинця: за кривавими відбитками пальців вдалося встановити, що спочатку жінка вбила двох своїх синів, а потім наклала на себе руки. Розроблена Х. Вусетичем система, яка вперше була викладена в опублікованій 1904 року книзі «Dactiloscorna Comparada», досі є затребуваною у більшості іспаномовних країн.

1895 року дактилоскопія була взята на озброєння Скотланд-Ярдом, а в червні 1897 року антропометрична система А. Бертільона була замінена на класифікаційну систему Річарда Генрі, яка до того стала офіційним методом ідентифікації злочинців у всій Індії. 1900 року в Англії припинили застосовувати бертільонаж і відтоді ідентифікація злочинців почала формуватися тільки на дактилоскопічному методі.

1901 року Річард Генрі, який тоді обіймав пост помічника комісара поліції Лондона, започаткував першу в світі картотеку відбитків пальців. Упродовж подальших 25 років система класифікації Річарда Генрі почала використовуватися як універсальний метод ідентифікації злочинців.

Ця система класифікації і зараз застосовується, хоча нині існує декілька різних варіантів системи класифікації Р. Генрі.

Із 1900 року дактилоскопія почала активно застосовуватися в Сполучених Штатах Америки. Особливо зміцнилися позиції дактилоскопії після одного досить цікавого випадку в 1903 році. У в'язницю штату Канзас був доставлений злочинець Уїлл Вест. Після зняття метрики за системою А. Бертільона з'ясувалося, що в цій в'язниці вже є засуджений на ім'я Уїльям Вест із такими ж антропометричними даними, який був братом-близнюком Уїлла Веста.

Єдина відмінність між ними була у відбитках пальців. Після цього випадку система А. Бертільона повністю втратила довіру. Всі організації США, що займалися розслідуванням злочинів, почали надсилати зареєстровані певним чином відбитки пальців у Національне бюро кримінальної ідентифікації (National Bureau of Criminal Identification). Картотека цього бюро згодом склала початкове ядро картотеки Федерального бюро розслідувань (ФБР), коли там була утворена відповідальна за дактилоскопічну реєстрацію структура.

Уже до 1956 року, коли керівником ФБР був Едгар Гувер, у картотеці було більше 140 млн карток із відбитками пальців, причому 112 млн із них належали не злочинцям, а чесним громадянам. 1971 року ця картотека налічувала майже 200 млн карток із папілярними відбитками.

Із кінця 20-х років минулого століття ФБР почало розробляти та випробовувати різні автоматизовані системи ідентифікації за відбитками пальців. У результаті, була створена система AFIS (Automated Fingerprint Identification System – автоматична система ідентифікації за відбитками пальців) – автоматизована комп'ютерна система управління базою даних відбитків пальців, в якій використовуються відбитки всіх десяти пальців. Спочатку система AFIS була заснована на записах відбитків пальців на перфокартах і не мала можливості автоматично порівнювати відбитки пальців, а автоматизація полягала лише в їх класифікації за окремими групами.

Із появою першої операційної системи математичних програм у кінці 1970-х років у ФБР почали використовувати сканування карт із зображенням папілярних узорів відбитків пальців. За допомогою автоматичної системи ідентифікації за відбитками пальців спочатку проводилося грубе порівняння, далі – точне, а потім на підставі отриманих результатів – остаточне порівняння шляхом візуального аналізу відбитків експертами-криміналістами.

Звичайно, така система ідентифікації мала деякі істотні обмеження, тому в ФБР постійно проводилися роботи з поліпшення функціональних можливостей системи AFIS. 1989 року було ухвалено рішення про перегляд усього дактилоскопічного процесу та розробку нової автоматизованої комп'ютерної системи, яка отримала назву IAFIS (Integrated AFIS), котра планувалася до запровадження в 1999 році. Спочатку система IAFIS використовувала базу даних, що зберігалась більш ніж на 10 тисячах CD-дисках, що дозволяла в автоматичному режимі порівнювати понад 62 тис. відбитків пальців за день, а згодом продуктивність була підвищена до 80 тис. відбитків[1].

[1] Пахомов С. Отпечаток пальца вместо пароля / Сергей Пахомов // КомпьютерПресс. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Archive/...

Отже, систему А. Бертільона, що мала досить короткий термін використання, замінила дактилоскопія. Для кінця XIX – початку XX століття вона була домінуючою. Нині дактилоскопію замінено біометрією, точніше біометричні системи ідентифікації. Дактилоскопія стала складовою біометрії, причому кардинально змінилася її технічна сторона – валик, друкарські фарби та ручні картотеки замінено сканерами і комп'ютерними інформаційними базами відбитків пальців або базами електронних шаблонів відбитків пальців.

Переводити у цифровий формат вигини природних папілярних ліній пальців і долонь дуже складно, для цього використовують спеціальні математичні алгоритми.

Засновник сучасної класифікації пальцьових узорів Френсіс Гальтон виокремив усього лише три різновиди малюнків: петлі, дуги та завитки. Нині фахівці з дерматогліфіки налічили ще 39 підвидів основних узорів. Раніше експерти вручну і на око визначали нахил елементів малюнків і підраховували кількість шкірних «гребнів». Тепер комп'ютер видає параметри узорів у вигляді готової таблички, з якою може працювати фахівець[1].

2.2. Дактилоскопія. Історія застосування на території царської Росії, СРСР і СНД

Згідно з Великим тлумачним словником сучасної української мови, дактилоскопія – це наука, що вивчає капілярні узори кінцевих фаланг пальців рук із метою встановлення особи людини[2].

Уперше дактилоскопія як метод реєстрації кримінальних злочинців 1895 року була запроваджена на території Великобританії. Різні країни світу вводили у себе дактилоскопічні методи впродовж подальших півтора-двох десятиліть. Однією з останніх була Франція. У Росії дактилоскопія почала застосовуватися з 1906 року[3].

Наприкінці XX століття поняття «дактилоскопія» («пальцероздивляння»: від грець. «daktylos – палець» і «skopeo – дивлюся») – це розділ криміналістики, що вивчає будову шкірних узорів внутрішніх (долонних) поверхонь нігтьових фаланг пальців рук для ідентифікації особистості, кримінальної реєстрації та розшуку злочинця. На долонній поверхні кінцевих (нігтьових) фаланг пальців рук є рельєфні лінії – так звані папілярні, побудова яких обумовлена рядами гребневих виступів шкіри, розділених своєрідними рівчаковими заглибленнями.

Ці лінії утворюють складні шкірні узори, які мають такі властивості: індивідуальність (різноманітна сукупність папілярних ліній, які створюють неповторний малюнок узору за їх конфігурацією, місцеположенням, взаєморозташуванням і які практично ніколи не відтворюються в іншому узорі); порівняну стійкість (незмінність зовнішньої будови

[1] Астахова А. Руку мне дай / А. Астахова. [Электронный ресурс]. – Режим доступа: http://www.cbio.ru/v5/modules/...

[2] Великий тлумачний словник сучасної української мови / уклад. і голов. ред. В. Т. Бусел. – К.; Ірпінь: ВТФ «Перун», 2003. – С. 207.

[3] Дактилоскопия. Материал из Википедии – свободной энциклопедии. [Электронный ресурс]. – Режим доступа: http://ru.wikipedia.org/wiki/...

узору, що виникає ще в період внутрішньоутробного розвитку людини і зберігається впродовж усього його життя і навіть після смерті, аж до розкладання трупа); відновлюваність (за поверхневого порушення шкірного покриву папілярні лінії через деякий час відновлюються у колишньому вигляді).

Ці чинники дозволяють здійснювати:

– криміналістичну ідентифікацію особи за відбитками пальців рук, виявлених на місці злочину;

– встановлення злочинця, який був зареєстрований як раніше судимий, за допомогою дактилоскопічної реєстрації;

– ідентифікацію невпізнаного трупа;

– розшук осіб, які зникли безвісти;

– встановлення факту вчинення декількох злочинів однією особою або одного злочину декількома особами.

Якщо уважно придивитися до структури шкірного покрову на пальцях рук, то можна побачити наявність складного рельєфного малюнка (так званий папілярний узор), утвореного рядом валиків-гребнів (заввишки 0,1–0,4 мм та завширшки 0,2–0,7 мм), і рівчаковими заглибленнями (борозенками – шириною 0,1–0,3 мм). Папілярний узор повністю формується на сьомому місяці розвитку плоду. Окрім того, в результаті проведених досліджень було встановлено, що відбитки пальців є різними навіть в однояйцевих близнят, хоча показники ДНК (дезоксирибонуклеїнова кислота) у них ідентичні.

Також папілярний узор неможливо змінити – ні порізи, ні опіки, ні інші механічні пошкодження шкіри не мають принципового значення, оскільки стійкість папілярного узору забезпечується регенеративною здатністю основного шару епідермісу шкіри. Тому можна стверджувати, що нині дактилоскопія є одним із надійних способів ідентифікації особи.

Незважаючи на все різноманіття папілярних узорів, вони піддаються чіткій класифікації, яка забезпечує процес їх індивідуалізації та ідентифікації. Всі папілярні узори, як вже зазначалось, поділяються на три основні типи: дугові, петльові та завиткові, які є фундаментом їх класифікації.

Дугові узори утворюються потоком папілярних ліній і в середній частині узору мають вигин – внутрішню дугу, будова і форма якої слугує для розділення їх на підвиди. Так, згідно з російською системою класифікації (у різних країнах використовуються різні системи класифікації, в Україні система класифікації аналогічна російській), дуговий узор може бути простим, шатровим, із невизначеною побудовою центру, помилково (хибно)-петльовим, помилково-завитковим і аномальним.

Петльові узори утворюються з потоків папілярних ліній, що починаються з одного краю пальця, загинаються вгору та до центру і, утворюючи петлю, повертаються до того ж краю. Петльовий узор складається із низки петель, що знаходяться одна в іншій, але для віднесення узору до петльового типу необхідно, щоб в центрі узору хоча б одна лінія утворювала завершену головку петлі або повну петлю. Залежно від форми петель, взаємного розташування ніжок петель та їх положення у площині петльові узори підрозділяються на підвиди, яких усього дев'ять, зокрема: простий, зігнутий, половинчастий, замкнутий, з системою петель паралельні петлі, з системою петель «зустрічні петлі», помилково-завиткові та петльові узори, що нечасто спостерігалося.

Завиткові узори утворюються таким потоком, папілярні лінії якого в середній частині зігнуті у вигляді кіл, овалів, спіралей, що огинають один одного або утворюють різні поєднання. Різновиди завиткових узорів зумовлені особливостями їх внутрішньої будови. Визначають такі 12 підвидів завиткових узорів: простий узор – коло, простий узор – овал,

простий узор – спіраль, петля-спіраль, петлі-спіралі, петля-равлик, зігнута петля, неповний завитковий узор, петлі-клубки з різностороннім і одностороннім розташуванням ніжок петель і завиткові узори, які часто простежуються.

Необхідно зазначити, що в різних країнах використовуються відмінні системи класифікації, тому підвиди базових папілярних узорів можуть бути різними[1].

У СРСР дактилоскопічна реєстрація велася на спеціальних бланках – десятипальцьових дактилоскопічних картах, в які вносилися за певною системою відбитки пальців кримінальних злочинців із зазначенням їхніх прізвищ, імені, по батькові, року і місця народження, особливих прикмет тощо.

Для дактилоскопічної ідентифікації застосовувалися розроблені в криміналістиці прийоми та засоби виявлення і збереження відбитків пальців із подальшим їх порівняльним дослідженням із відбитками пальців рук або з відповідними дактилоскопічними картами осіб, що підозрюються у вчиненні злочину[2].

У такому вигляді система дактилоскопічної реєстрації ще використовується у низці країн СНД, зокрема в Україні.

Нині одним із найважливіших підсумків розвитку дактилоскопії слід визнати появу системи засобів і методів виявлення та експертного дослідження латентних слідів рук. Проте криміналістичні служби різних країн нині з низки об'єктивних і суб'єктивних причин опинилися на різному рівні запровадження ефективних дактилоскопічних методів. У цьому плані цікавою є історія і сучасний стан судово-дактилоскопічної експертизи в країнах, що виникли на території СРСР.

У царській Росії перша публікація про дактилоскопію з'явилася в «Юридичній Газеті» 8 липня 1892 року. Вона називалася «Відбитки рук і їх значення в судовій практиці». Причиною появи цієї статті стало видання в Англії у тому ж році книги сера Френсіса Гальтона «Відбитки пальців».

Практичне впровадження дактилоскопічних методів у розшукову і судову практику царської Росії розпочалося лише в першому десятиріччі XX століття. Наприкінці 1906 року було засноване Центральне дактилоскопічне бюро Головного тюремного управління. Із 1908 року дактилоскопічна реєстрація почала застосовуватися в поліцейських установах, які займалися розшуком. У цьому ж році дактилоскопічні методи почали застосовуватися для встановлення злочинців за їх слідами рук, які залишалися на місцях злочинів.

Перша дактилоскопічна експертиза в суді царської Росії була проведена у Санкт-Петербурзі 1912 року за кримінальною справою щодо вбивства провізора Харламовської аптеки. Відбитки пальців рук були знайдені на уламку розбитого шкла дверей. За одним із слідів був ідентифікований один зі знайомих сторожа аптеки, який згодом визнав свою причетність до вчинення цього злочину. Як експерт у суді виступив відомий російський криміналіст В. І. Лебєдєв.

1912 року був створений Кабінет науково-судової експертизи при прокуророві Санкт-Петербурзької судової палати. Утворенню Кабінету передувало ознайомлення російських судових і поліцейських чиновників із діяльністю криміналістичних установ Парижа, Берліна, Лондона, Рима, Лозанни й інших міст Європи, вивчення досвіду робіт А. Бертільона, Р. Рейсса. Група російських криміналістів на чолі зі старшим

[1] Пахомов С. Отпечаток пальца вместо пароля / Сергей Пахомов // КомпьютерПресс. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Archive/...

[2] Дактилоскопия // Slovari.yandex.ru. – 2005. – 25 февраля. [Электронный ресурс]. – Режим доступа: http://slovari.yandex.ru/art...

юрисконсультом Міністерства юстиції С. М. Трегубовим прослухала в 1911 році у Лозанні курс лекцій професора Р. А. Рейсса.

1914 року були організовані такі ж кабінети у Москві, Києві та Одесі. Ці кабінети були першими в Росії багатопрофільними криміналістичними лабораторіями, що проводили трасологічні, дактилоскопічні, документопроваджувальні, хімічні й інші експертні дослідження.

Питання виявлення та дослідження латентних слідів рук детально розглядалися у виданих до революції книгах В. І. Лебєдєва («Дактилоскопія» – 1909 р., 1912 р.), С. М. Трегубова («Основи кримінальної техніки» – 1915 р.), А. Міллера («Сучасний кримінальний розшук. Реєстрація злочинців. Дактилоскопія» – 1911 р.), М. С. Бокаріуса («Судова медицина у викладі для юристів» – 1915 р.), М. А. Жабчинського («Застосування дактилоскопії в розшуковій справі» – 1907 р., «Про реєстрацію злочинців і прийомах дослідження злочинів» – 1913 р.).

За 25 років, що минули з моменту першої публікації про дактилоскопію до 1917 року, в Росії були закладені сучасні основи дактилоскопічної реєстрації й експертизи, створені базові криміналістичні установи, підготовлені хоч і в невеликій кількості висококваліфіковані кадри експертів, встановлені тісні наукові та практичні зв'язки з західноєвропейськими вченими та судово-медичними установами.

У лютому 1917 року в Росії перестала існувати монархія і був утворений Тимчасовий уряд. 11 березня Тимчасовий уряд скасував Департамент поліції і заснував Тимчасове управління у справах суспільної поліції, яке проіснувало до 15 липня. Із 15 липня і до 25 жовтня 1917 року центральним органом правопорядку було Головне управління у справах міліції та забезпеченню особистої і майнової безпеки громадян.

У перші дні Лютневої революції Петроградський кабінет науково-судової експертизи був знищений під час пожежі будівлі колишнього окружного суду Петрограда. Київський і Одеський кабінети збереглися, але працювали із труднощами та перебоями. Московський кабінет проіснував до 1918 року. Дактилоскопічні та реєстраційні бюро, що були в розшукових поліцейських установах, були знищені разом з усіма поліцейськими структурами.

Після приходу до влади в жовтні 1917 року більшовиків усі старі установи правосуддя та правоохоронні органи були ліквідовані. На зміну їм негайно почали утворюватися нові інституції: суди, трибунали, міліція, ЧК, що діяли як знаряддя диктатури пролетаріату. Більшість старих фахівців кримінального розшуку була піддана фізичному знищенню, частина емігрувала. Деякі криміналісти перейшли на службу в Білу армію. Зокрема в Особливому відділі Штабу Головнокомандуючого збройними силами на півдні Росії навіть було створено Центральне дактилоскопічне бюро і видана «Коротка інструкція по дактилоскопіюванню». Серед тоді відомих криміналістів на сторону більшовіків перейшли М. А. Жабчинський, С. П. Потапов, В. О. Русецький та ін.

Відновлення системи дактилоскопічної реєстрації та судово-дактилоскопічної експертизи в більшовицькій Росії почалося з 1918 року. На засіданні Колегії НКВС 5 жовтня 1918 року було ухвалено Положення про організацію в органах внутрішніх справ РРФСР кримінально-розшукових установ, і вже 10 жовтня цього ж року Центральне управління кримінального розшуку РРФСР надіслало в губернські відділи міліції циркуляр № 694 про необхідність надання протягом місяця трьох екземплярів дактилокарт на всіх злочинців. 30 жовтня були затверджені Правила фотографування і дактилоскопіювання затриманих злочинців.

15 лютого 1919 року Колегія НКВС розглянула і затвердила кошторис на організацію при Центророзшуку Реєстраційно-дактилоскопічного Бюро. У квітні 1919 року

в Москві за рішенням Уряду були відкриті курси з підвищення кваліфікації та підготовки кадрів для кримінального розшуку.

У 1920 році був створений науково-технічний підвідділ Управління кримінального розшуку ЦАУ (Центральне адміністративне управління) НКВС. На цей підвідділ разом з іншими завданнями було покладене завдання організації в центрі і на місцях дактилоскопічної реєстрації й експертизи. 1920 року П. С. Семеновським на основі системи Гальтона-Генрі і Рошера була розроблена класифікація пальцьових узорів для виведення дактилоскопічних формул і розкладки за ними дактилокарт. За цією системою з невеликими змінами ще й досі ведуться ручні дактокартотеки в країнах Співдружності Незалежних Держав (СНД), зокрема й в Україні.

Точних відомостей про проведення перших дактилоскопічних експертиз після Жовтневої революції, на жаль, не збереглося. Відомо лише, що Кабінет судової експертизи при Кримінальному розшуку почав функціонувати з 1 березня 1919 року, в квітні цього ж року він практично злився з реєстраційно-дактилоскопічним бюро. Першим керівником нової служби був призначений П. С. Семеновський.

До 1927 року в СРСР існувало вже 358 реєстраційно-дактилоскопічних бюро. У Центральному реєстраційно-дактилоскопічному бюро на цей час було накопичено понад 400 000 дактилокарт. За допомогою дактилоскопії в 1927 році були встановлені особистості 1200 рецидивістів, які переховувалися під чужими прізвищами. Для кримінально-розшукових апаратів було придбано 218 камер Бертільона і 219 дактилоскопічних наборів. У майстернях Головповітрофлоту на замовлення кримінального розшуку було виготовлено 200 луп.

На початку 1928 року був проведений перший набір на 6-місячні курси науково-технічних експертів при ВКР (відділ /відділення/ карного розшуку) НКВС у кількості 18 чоловік. Усього відбулося три випуски цих курсів.

На початок 30-х років минулого століття в органах міліції СРСР вже була організована досить розгалужена мережа науково-технічних апаратів. У цей період структура і підлеглість експертних підрозділів і їх назви мінялися досить часто. У березні 1932 року створюється науково-технічне відділення (НТВ) у складі оперативного відділу Головної інспекції міліції ОДПУ СРСР. До його складу було передане НТВ Управління кримінального розшуку НКВС РРФСР. Начальником першого союзного науково-технічного відділення був призначений Я. М. Яковлєв, а його помічником із РРФСР С. М. Потапов. У НТВ було створено спеціальне іноземне бюро, яке очолив визначний російський мовознавець того часу С. С. Ігнатов.

Почала перекладатися з іноземних мов (англійської, німецької, французької, італійської, іспанської, японської та низки інших) криміналістична література, яка видавалася за кордоном, а також статті з окремих поліцейських журналів (переважно з дактилоскопічних питань).

1932 року при Московському кримінальному розшуку почав функціонувати кабінет експертизи, який 1935 року був реорганізований у науково-технічне відділення, а на початку 1941 року – в науково-технічний відділ.

До 1940 року в кожній республіці, краю, області СРСР науково-технічні підрозділи були оснащені необхідним устаткуванням і апаратурою і для оглядів місць подій, і для проведення криміналістичних експертиз, зокрема й дактилоскопічних. Частина устаткування для проведення експертиз була закуплена за кордоном.

Діяльність криміналістичних експертних підрозділів продовжувалася і під час війни СРСР з фашистською Німеччиною. Здійснювалася підготовка експертів у Центральній школі міліції. Реєстраційно-дактилоскопічна служба була евакуйована з Москви

в місто Уфу і довідки наводилися шляхом запитів телефоном або телеграфом. Для ефективного використання дактилокартотеки був розроблений спеціальний код дактилоформул, який передавався за допомогою телефонного зв'язку «ВЧ». Час, необхідний на здійснення перевірки однієї особи за дактообліками, становив 2–3 години.

1942 року в Ташкенті експертом Назаровим була проведена перша з відомих нині в СРСР пороскопічна експертиза.

У наявному сліді пальця, вилученому з місця події, була лише одна традиційна деталь – вилка. Зазвичай експерти визнавали подібні сліди непридатними для ідентифікації. У цьому випадку ідентифікація злочинця була здійснена за порами.

1943 року після звільнення Харкова відновив свою діяльність Харківський науково-дослідний інститут судових експертиз. Народним комісаріатом внутрішніх справ СРСР у 1943 році був виданий невеликий за обсягом посібник «Сліди пальців рук». 1944 року було організовано криміналістичне відділення у Центральній судово-медичній лабораторії Головного медичного управління Збройних сил СРСР. На це відділення покладалося проведення, крім інших, також і дактилоскопічних експертиз. На базі відділення були організовані курси підвищення каліфікації експертів-криміналістів.

У грудні 1945 року в складі НТВ (науково-технічного відділу) ГУМ головного управління міліції) МВС СРСР як одного з його підрозділів був організований науково-дослідний інститут криміналістики (НДІК).

У складі НДІК була лабораторія криміналістичної експертизи, яка виконувала трасологічні та деякі інші традиційні види досліджень. 1956 року НДІК був перетворений у НДІ міліції МВС СРСР з наданням функцій із вдосконалення слідчої тактики та методики розслідування злочинів.

Слід зазначити, що у складі НДІК була організована експериментальна лабораторія з розробки криміналістичної техніки. Надалі інститут неодноразово перейменовувався і має назву ВНДІ (Всеросійський науково-дослідний інститут) МВС Російської Федерації (РФ).

1970 року при Оперативно-технічному управлінні МВС СРСР була організована Центральна криміналістична лабораторія (яка згодом отримала назву Центральної науково-дослідної криміналістичної лабораторії). У її складі був слідчий сектор, якому було доручено проведення дактилоскопічних експертиз і досліджень.

Нині в МВС РФ головним криміналістичним підрозділом є Експертно-криміналістичний центр, який здійснює керівництво проведенням експертиз в органах внутрішніх справ Росії, самостійним проведенням повторних і додаткових досліджень, ведення низки криміналістичних обліків і проведення науково-дослідних робіт у галузі криміналістики[1].

1945 року при оперативному відділі Управління міліції МВС УРСР вперше було створено науково-технічне відділення, яке вже через три роки було реорганізовано в самостійний Науково-технічний відділ Управління міліції МВС України. 1981 року службу було перейменовано в Експертно-криміналістичне управління, а в 1992 році – в Центр криміналістичних досліджень, у складі якого функціонували такі відділи досліджень: грошей і документів; балістичних; дактилоскопічних; фоноскопічних; фізико-хімічних; наркотичних; біологічних; оперативного пошуку, знешкодження та дослідження вибухових пристроїв і речовин.

[1] Хазиев Ш. История дактилоскопии в России 1867–1994 гг. Судебно-экспертное исследование латентных следов рук в России / Ш. Хазиев. [Электронный ресурс]. – Режим доступа: http://www.forensic.ru/sudexpert14.html...

6 травня 1998 роки Ухвалою Кабінету Міністрів України від № 617 був створений Державний науково-дослідний експертно-криміналістичний центр МВС України, який об'єднав Експертно-криміналістичне управління, Центр криміналістичних досліджень і вибухово-технічну службу, а з 2000 року – Експертну службу МВС України.

Основними завданнями Експертної служби є:

– судово-експертне і техніко-криміналістичне забезпечення діяльності органів внутрішніх справ, інших правоохоронних структур із метою запобігання, виявлення, розкриття та розслідування злочинів;

– організація виїздів на огляди місць учинення злочинів, здійснення експертиз і досліджень (47 видів) у кримінальних, цивільних і арбітражних справах, дослідження при позасудовому провадженні;

– проведення сертифікації зброї, боєприпасів, вибухових речовин і піротехнічних засобів;

– проведення підготовки і підвищення кваліфікації експертів[1].

Державний науково-дослідний інститут (ДНДІ) МВС України створений відповідно до ухвали Кабінету Міністрів України від 8 вересня 2005 року № 880 «Про реорганізацію вищих учбових закладів і науково-дослідних установ Міністерства внутрішніх справ» на підставі наказу Міністерства внутрішніх справ України від 27 вересня 2005 року № 827 з метою здійснення наукового і науково-технічного забезпечення діяльності системи органів МВС України». Інститут є правонаступником НДІ спеціальної техніки, НДІ проблем боротьби зі злочинністю Національної академії внутрішніх справ України (НАВСУ), Державного науково-дослідного центру (ДНДЦ) з безпеки дорожнього руху і діяльності ДПС (дорожньо-патрульна служба) міліції[2].

Своєрідний шлях розвитку пройшли в СРСР і в країнах Співдружності незалежних держав (СНД) експертні установи системи Міністерства юстиції.

На початку 1935 року в складі Інституту кримінальної політики при Прокуратурі, Верховному Суді і НКЮ (Народний комісаріат юстиції) РРФСР була організована лабораторія науково-судової експертизи. У кінці 1936 року ця лабораторія перейшла у ведення Прокурора СРСР, де в січні 1937 року наказом Прокурора СРСР отримала найменування лабораторії з науково-дослідної роботи і функціонувала при слідчому відділі Прокуратури СРСР. У ній проводилися консультації слідчих і здійснювалося провадження судових експертиз. 1939 року лабораторія Прокуратури СРСР була передана в Інститут права АН СРСР, де на її базі була заснована в системі секції судового права криміналістична лабораторія.

1944 року в Москві на базі цієї лабораторії і криміналістичної лабораторії Московського юридичного інституту, створеної в 1935 році, була організована Центральна криміналістична лабораторія Міністерства юстиції СРСР. 1950 року була утворена мережа судово-експертних установ міністерств юстиції союзних республік.

1962 року на базі Центральної криміналістичної лабораторії був утворений Центральний НДІ судових експертиз (ЦНДІСЕ) РРФСР. Дактилоскопічна експертиза в цьому інституті проводилася співробітниками лабораторії трасологічних і балістичних експертиз. Після організації в 1970 році Міністерства юстиції СРСР ЦНДІСЕ РРФСР був перепідпорядкований Мін'юсту й отримав найменування Всесоюзного науково-дослідного інституту судових експертиз (ВНДІСЕ).

[1] Джерело: сайт МВС України. [Електронний ресурс]. – Режим доступу: http://mvs.gov. ua/mvs/control/uk/publish/article/…

[2] Там само.

Після припинення існування СРСР ВНДІСЕ в грудні 1991 року перейшов у ведення Міністерства юстиції Російської Федерації і почав називатися Всеросійським науково-дослідним інститутом судових експертиз (абревіатура залишилась без змін – ВНДІСЕ).

Із грудня 1994 року ВНДІСЕ був перейменований у Російський федеральний центр судових експертиз (РФЦСЕ) при Міністерстві юстиції РФ.

Нині дактилоскопічна експертиза в судово-експертних установах Міністерства юстиції проводиться в трасологічних (трасолого-балістичних) підрозділах науково-дослідних лабораторій судових експертиз, які є в республіканських, крайових і більшості обласних центрів Росії.

Основна частина дактилоскопічних експертиз здійснюється за завданням прокуратури та судів.

Ці лабораторії оснащені основними технічними засобами та матеріалами, необхідними для проведення судово-дактилоскопічних експертиз. Співробітники лабораторій проводять дактилоскопічні дослідження у стаціонарних умовах і лише в окремих випадках і у складних кримінальних справах беруть участь у дослідженні місць подій із метою пошуку слідів пальців і долонь.

Окремо спеціалізації співробітників на проведенні тільки експертиз із дактилоскопії, на жаль, немає і вони, як правило, здійснюють усі види трасологічних експертиз, іноді поєднуючи їх із проведенням балістичних експертиз[1].

В Україні станом на 2009 рік існували такі науково-дослідні установи судових експертиз:

– Науково-дослідний центр судової експертизи з питань інтелектуальної власності;
– Вінницьке відділення Київського НДІСЕ (науково-дослідний інститут судових експертиз);
– Волинське відділення Львівського НДІСЕ;
– Дніпропетровський науково-дослідний інститут судових експертиз;
– Донецький науково-дослідний інститут судових експертиз (ДНДІСЕ);
– Київський науково-дослідний інститут судових експертиз (КНДІСЕ);
– Кіровоградське відділення Одеського НДІСЕ;
– Кримський науково-дослідний інститут судових експертиз;
– Луганське відділення Донецького НДІСЕ;
– Львівський науково-дослідний інститут судових експертиз (ЛНДІСЕ);
– Миколаївське відділення Одеського НДІСЕ;
– Одеський науково-дослідний інститут судових експертиз (ОНДІСЕ);
– Полтавське відділення Харківського НДІСЕ;
– Севастопольське відділення Харківського НДІСЕ;
– Сумське відділення Харківського НДІСЕ;
– Тернопільське відділення Київського НДІСЕ;
– Харківський науково-дослідний інститут судових експертиз (ХНДІСЕ);
– Херсонське відділення Одеського НДІСЕ;
– Черкаське відділення Київського НДІСЕ;
– Чернігівське відділення Київського НДІСЕ.

[1] Хазиев Ш. История дактилоскопии в России 1867–1994 гг. Судебно-экспертное исследование латентных следов рук в России / Ш. Хазиев. [Электронный ресурс]. – Режим доступа: http://www.forensic.ru/sudexpert14.html...

Експертно-кваліфікаційні комісії діють тільки при таких науково-дослідних інститутах судових експертиз:

– Київського НДІСЕ;
– Донецького НДІСЕ;
– Львівського НДІСЕ;
– Одеського НДІСЕ;
– Харківського НДІСЕ[1].

Проведення дактилоскопічних експертиз нештатними експертами або незалежними криміналістами-консультантами в Україні не практикується.

У криміналістиці на території СРСР, а нині й колишніх країн СНД, зокрема і в Україні, численні методи виявлення латентних слідів рук людини прийнято класифікувати на фізичні, фізико-хімічні та хімічні.

На початку 70-х років минулого століття в СРСР розроблялися основи застосування термовакуумного напилення (ТВН) для виявлення латентних слідів рук. Найбільш активно цим методом займалися у Львівському відділенні Київського НДІСЕ. 1982 року львів'янами був запатентований метод виявлення латентних слідів рук, заснований на послідовному нанесенні у вакуумі двошарової проявляючої плівки. Нині термовакуумне напилення виявлення латентних слідів пальців людини практично не використовується.

Фізико-хімічні методи виявлення латентних слідів рук людини охоплюють обробку слідів парами йоду, ауторадіографію і рентгенівські методи.

Через відсутність у колишньому СРСР ефективних автоматизованих систем дактилоскопічної ідентифікації проблемам встановлення особи за допомогою відбитків долоні, пальця, а також ділянки папілярного узору, що залишились відображеними у виявленому сліді на місці злочину, приділялася значна увага. Було розроблено декілька систем локалізації узору, які ґрунтувались на обліку й обробці статистичних показників виявлених морфологічних особливостей узорів відбитків.

Вивчення історії розвитку і сучасного стану методів судово-експертного дослідження слідів рук в Україні та Росії дозволяє констатувати такі основні тенденції:

1. Незважаючи на велику завантаженість, експерти продовжують дослідницьку діяльність у галузі пошуку нових засобів і методів виявлення та дослідження патентних слідів.

2. Відсутність у СРСР, а зараз в Україні та Росії, загального дактилоскопіювання населення зумовило постійний підвищений інтерес учених і криміналістів-практиків до питань отримання зі слідів максимальної інформації про людину (стать, вік, ріст, патології тощо). Така інформація дуже потрібна для звуження кола осіб, котрі підозрюються.

3. До початку Другої світової війни, особливо в 20–30-ті роки минулого століття, найбільш суттєвий вплив на російську дактилоскопічну науку і практику здійснювала німецька криміналістична школа і, відповідно, німецька система організації дактилоскопічної служби. Зараз відчутно посилився вплив американської системи, що супроводжується збільшенням надходження науково-практичної інформації із США та Канади.

4. У 90-ті роки XX сторіччя досить популярною була ідея про необхідність спеціалізації експертів у галузі дактилоскопії і виокремлення дактилоскопічної служби зі складу трасологічних або трасолого-балістичних підрозділів. Це було зумовлено як усвідомленням складності та специфічності великої кількості методів виявлення і дослідження латентних слідів, так і накопиченням в арсеналі дактилоскопії значного обсягу

[1] Джерело: сайт Міністерства юстиції України. [Электронный ресурс]. – Режим доступа: http://www.minjust.gov.ua/0/str_ust_inst

методичної інформації, яка вимагала проведення тривалої та скрупульозної підготовки експертів.

5. Помилкові експертні висновки, які простежуються періодично, а також певне зниження якості проведених дактилоскопічних експертиз, що спостерігаються останніми роками, могли б бути значною мірою подолані за умови проведення в законодавстві змін, скерованих на забезпечення реальної конкурентності у галузі здійснення судово-дактилоскопічних експертиз[1].

У пострадянській Росії з 1 січня 1999 р. набув чинності закон про добровільне дактилоскопіювання населення (Закон «Про державну дактилоскопічну реєстрацію в Російській Федерації»). В обов'язковому порядку її мусять пройти ті громадяни, які перебувають на державній службі «у погонах», чия професія пов'язана з ризиком для життя. Крім того, зняття відбитків пальців обов'язкове для мігрантів та інших іноземних громадян, біженців та ін.

Проведення дактилоскопіювання є обов'язковим для тих осіб, які підозрюються у скоєнні злочинів, перебувають під слідством.

Подібні заходи передбачені й в казахському варіанті законопроекту. На Україні поки що в обов'язковому порядку дактилоскопіювання проходять особи, які перебувають під слідством і підозрюються у вчиненні злочинів чи вчинили їх.

Законослухняні громадяни в Росії не хочуть здавати відбитки своїх пальців. Основною проблемою, яка позбавляла закон практичного втілення в Російській Федерації у першому десятилітті XXI, була стара процедура зняття дактилоскопічних відбитків у громадян на паперову картку за застарілою методикою з використанням друкарської фарби, як це зазвичай роблять під час дактилоскопіювання злочинців[2].

Але у сучасному цивілізованому світі відбиток пальця розглядається лише як один із багатьох біометричних ідентифікаційних параметрів людини (обличчя, рука, райдужна оболонка ока, підпис, голос, генетичний код тощо), який відрізняється від інших більшою вивченістю і, як наслідок, суттєвою інформативністю. Такому новому підходу до отримання папілярних слідів пальців сприяє застосування новітніх електронних пристроїв останніх розробок і способи зняття відбитків пальця за їх допомогою, що дозволяє відділити у масовій свідомості старий метод зняття відбитків пальців, який призначався насамперед для злочинців, від сучасного електронного дактилоскопіювання, що використовується найперше для організації та забезпечення фізичної, інформаційної, банківської та подібної безпеки доступу громадян.

Отже, розвиток комп'ютерної техніки істотно позначився на дактилоскопії. У 90-х роках минулого сторіччя у світі почалася ера отримання відбитків пальців за допомогою спеціальних сканерів. Але для масового запровадження нових методів зняття відбитків пальців необхідне проведення цілого комплексу заходів, основним з яких є загальна комп'ютеризація країни. У минулому столітті термін «біометрія» мав набагато ширше тлумачення та належав в основному до методів математичної статистики, які використовувались для математичного опису процесів будь-яких біологічних явищ. Тепер значення цього терміна стало значно вужчим – під біометрією і біометричними технологіями розуміють автоматизовані методи встановлення або розпізнавання будь-якої особистості за її біологічними характеристиками або їх виявами.

---

[1] Хазиев Ш. История дактилоскопии в России 1867–1994 гг. Методы выявления и исследования латентных следов рук в современной России / Ш. Хазиев. [Электронный ресурс]. – Режим доступа: http://www.forensic.ru/sudexpert...

[2] Готовьте «пальчики». [Электронный ресурс]. – Режим доступа: http://zonakz.net/articles/4print.php…

2.3. Біометрична ідентифікація за відбитками пальців. Відмінність сканування відбитків пальців від дактилоскопіювання

Як відомо, існує наука про побудову папілярних узорів – дерматогліфіка. Переводити в цифровий формат примхливі вигини природних ліній надзвичайно складно і нині для цього використовуються математичні алгоритми, які свого часу створювалися для управління авіаційними та космічними польотами.

Якщо засновник сучасної класифікації папілярних узорів пальців Френсіс Гальтон виокремлював усього три різновиди малюнків узорів, то фахівці з дерматогліфіки нині визначають 39 основних підвидів узорів.

Раніше експерти вручну за допомогою спеціальної лупи визначали особливості елементів малюнків і підраховували кількість шкірних гребнів. Тепер комп'ютер видає параметри узорів у вигляді готової таблиці, з якою працюють спеціалісти[1].

Фізіологічно відбиток пальця – це структура, що складається з виступів, які містять пори, і западин між ними (рівчакові поглиблення). Безпосередньо під цією структурою розташовується структура кровоносних судин. Морфологія (форма) відбитка пальця тісно пов'язана з певними електричними і температурними характеристиками шкіри. Це означає, що для отримання зображень відбитків пальців можуть бути використані світло, тепло й електрична ємність (або їх поєднання). Як вже вказувалося, відбиток пальця людини формується в ембріональному стані, він не міняється з віком і відновлюється в колишньому вигляді після пошкодження[2].

Якщо ж один із пальців пошкоджений, для ідентифікації можна скористатися резервними відбитками інших пальців, відомості про які, як правило, також вносяться до біометричної системи під час реєстрації користувача.

Слід особливо відзначити, що між дактилоскопіюванням (відповідно до традиційного поняття, – це отримання відтисків шляхом зняття відбитків пальців і долонь на паперові носії) і скануванням є істотна різниця. Вона полягає у тому, що здебільшого під час сканування відбитків пальців замість збереження повного зображення папілярного узору зберігається тільки інформація про набір його головних характерних точок, причому відновити повне зображення відбитка пальця за інформацією, яка зберігається, практично неможливо. Ця обставина і виявилась вирішальним чинником для широкого застосування сканування відбитків пальців серед цивільного населення.

Взагалі у більшості сучасних систем біометричної ідентифікації ідентифікатори, що скануються, зокрема й відбитки пальців, зазвичай у вигляді зображення оригіналу не зберігаються. Зображення перестає існувати, як тільки потрапляє у комп'ютер: за допомогою спеціального програмно-математичного апарату воно перетворюється в спеціальний код – цифровий модуль або шаблон. Саме у такому цифровому вигляді більшість будь-яких індивідуальних біометричних показників і зберігаються в серверах. Назад відновити зображення практично неможливо.

---

[1] Астахова А. Руку мне дай / А. Астахова. – 2007. [Электронный ресурс]. – Режим доступа: http://www.cbio.ru/v5/modules/news/article....

[2] Бишоп П. Технология биометрической защиты ATMEL FINGERCHIP / П. Бишоп // Электронные компоненты. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.efo.ru/doc/Atmel/Atmel...

Ототожнити цифровий модуль із конкретним відбитком можна тільки за допомогою спеціального алгоритма, тобто необхідна умова – знання і використання для кожного варіанта систем біометричної технології певного алгоритму. Отже, тільки використавши унікальний програмно-математичний алгоритм, який є оригінальним для кожної конкретної системи, можна встановити, однакові або різні порівнювані біометричні параметри: пальці (долоні), обличчя, райдужна оболонка ока, голос тощо[1].

Із усього різноманіття біометричної продукції, яка представлена на світовому ринку систем ідентифікації, найпопулярнішими є автоматичні системи розпізнавання відбитків пальців (Automated Fingerprint Identification System – /AFIS/). Сканування відбитка пальця – найстаріший метод з усіх існуючих біометричних методів і тому найпоширеніший.

На системи AFIS припадає майже половина обсягу продажу всього ринку біометрії, а з урахуванням криміналістичних систем (які досить часто називають поліцейськими дактилоскопічними системами) – всі 80%. AFIS використовується поліцією й іншими силовими структурами на всій території США, а також автоматичні системи розпізнавання відбитків пальців у 2002 році використовувалися приблизно у 30-ти інших країнах світу[2].

У Сполучених Штатах Америки пристрої контролю доступу за відбитком пальця встановлені у всіх державних установах, а першими почали їх використовувати військові.

Зазвичай системи розпізнавання відбитків пальців розділяють на два типи: для ідентифікації – AFIS (Automatic Fingerprint Identification Systems) і верифікації. У першому випадку використовуються відбитки всіх десяти пальців і подібні системи широко застосовуються в криміналістиці. Пристрої верифікації зазвичай оперують з інформацією про відбитки одного, нечасто – декількох пальців.

Відбитки зображень усіх 10 пальців рук (а в низці країн і долонь) зберігаються тільки у спеціальних базах даних деяких силових структур, насамперед спецслужб і правоохоронних органів. Але навіть і в цьому випадку для зменшення часу пошуку в автоматизованій дактилоскопічній інформаційній системі (АДІС) використовується спеціальний електронний шаблон у вигляді цифрового модуля, отриманого шляхом перетворення відсканованого зображення за допомогою спеціального алгоритму. Принципи перетворення, зберігання і зіставлення біометричних параметрів і використовуваних програмних продуктів становлять ноу-хау цих структур.

Підтвердження ідентичності користувачів за відбитками пальців у промислових і бізнес-застосуваннях значно відрізняється від біометричних технологій, що використовуються державними установами для ідентифікації громадян у масштабах країни. Інформація, яка знімається з відбитків пальців програмними засобами підтвердження ідентичності користувача, використовується не більше ніж для персональної верифікації. Програмне забезпечення створює математичний шаблон, який стискається і кодується цифровим шляхом, але зберігає водночас відомості про всі характерні особливості відбитка пальця. Як правило, отримані шаблони зберігаються в зашифрованих файлах і використовуються для ідентифікації користувачів[3].

---

[1] Биометрия: тотальный контроль (отпечаток пальца). – 2003. – 16 сентября. [Электронный ресурс]. – Режим доступа: http://www.cherry.ru/interes/...

[2] Минкин В. Дактилоскопический паспорт – каждому россиянину! / В. Минкин // БДИ. – 2002. – № 1 (41). [Электронный ресурс]. – Режим доступа: http://www.iching.ru/6/Bezopasnost-9.html

[3] Идентификация по отпечаткам пальцев – применения в бизнесе и промышленности. – 2006. – 18 декабря. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/ foreign/…

Електронний зліпок відбитка пальця (Template) – це оцифрований вигляд відбитка пальця завдовжки до 500 байт, що становить числовий опис векторної моделі особливостей відбитка, за яким неможливо відновити вихідний відбиток[1].

Отже, за традиційних криміналістичних досліджень, а також зіставлення за допомогою автоматизованої дактилоскопічної інформаційної системи (АДІС чи в англомовному варіанті AFIS) відбувається ідентифікація особи за наявними відбитками пальців, а коли говорять про застосування біометричних ідентифікаційних систем для створення систем безпеки, то мають на увазі верифікацію особи.

Ще раз нагадаємо, що під час ідентифікації особи за відбитком пальця встановлюється, кому належать відбитки пальців. Для цього здійснюється пошук і порівняння дактилоскопічного відбитка пальця особи, яка ідентифікується, згідно з виведеною експертом формулою за всією дактилоскопічною картотекою, що зберігається в певному порядку, або пошук відповідного електронного шаблону аналогічного взірцевому в базі даних АДІС. У разі збігу зразків відбитків пальців, що ідентифікуються, з наявними у картотеці або в базі даних АДІС відбувається ідентифікація, тобто в підсумку під час пошуку одного зразка за багатьма отримуємо відповідь на питання, якій особі належить відбиток, що досліджується.

А під час процесу верифікації мається на увазі порівняння відсканованого відбитка пальця з одним або декількома шаблонними відбитками для встановлення, чи є ця людина саме тією, за кого вона себе видає[2].

Використання відбитка пальця для ідентифікації особи – один із найзручніших і порівняно дешевих засобів з усіх біометричних ідентифікаційних методів, які застосовуються нині. Ймовірність помилки під час ідентифікації користувача є набагато меншою порівняно з іншими методами біометрії та поступається тільки технологіям ідентифікації райдужної оболонки очей (до уваги не береться ДНК-метод, який ще зараз використовується здебільшого тільки під час проведення експертиз). Останнім часом почали з'являтися повідомлення, що точнішим є метод ідентифікації за малюнком вен долоні або пальця, але поки що цей метод не отримав у світі достатнього поширення і застосовується переважно у банківській сфері Японії.

Якість розпізнавання особливостей отриманого відбитка і можливість його подальшої обробки математичним алгоритмом надто залежить від стану поверхневого шару шкіри пальця і його положення щодо поверхні скануючого елемента. Різні системи пред'являють суттєво відмінні вимоги до цих двох параметрів, основні характеристики яких залежать, як вже було наголошено, від наявного алгоритму, що застосовується. Наприклад, розпізнавання за характерними точками дає сильний рівень шуму за поганого стану шкіри поверхні пальця. Розпізнавання за всією поверхнею позбавлено цього недоліку, але для використання цього способу потрібно дуже точно розміщувати палець на поверхні віконця скануючого елемента.

Урядові та цивільні організації всього світу давно використовують відбитки пальців як один із основних методів встановлення особи. Відбитки пальців залишаються однією з найпростіших технологій щодо будь-якого користувача, а також найбільш вигідним за ціною використовуваного устаткування. Саме цю технологію поряд з іншими в США застосовують ФБР, Секретна служба, Агентство національної безпеки,

[1] Радостин А. Перспективы использования биометрии в системах лояльности / Александр Радостин // RB.RU. – 2008. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Пахомов С. Отпечаток пальца вместо пароля / С. Пахомов // КомпьютерПресс. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Archive/...

міністерства фінансів і оборони, відділи транспортних засобів адміністрацій низки штатів, «MasterCard» тощо. Технологія розпізнавання відбитків пальців усуває потребу в паролях для користувачів, зменшує кількість звернень до служби комп'ютерної підтримки і знижує витрати на мережеве адміністрування[1]. Але слід зазначити, що починаючи з кінця першого десятиліття XXI сторіччя, у США й Великобританії почали проводитися роботи з утворення та використання мультибіометричних систем (замість AFIS використовуються системи IAFIS).

Отже, підсумовуючи викладене, переваги технологій доступу за відбитком пальця полягають у простоті використання, зручності, достатній надійності та економічності. Як уже було зазначено, відомо два основні алгоритми розпізнавання відбитків пальців: за окремими деталями (характерними точками) і рельєфом усієї поверхні пальця. У першому випадку пристрій вибирає та реєструє дані тільки деяких ділянок, які є унікальними для конкретного відбитка, а потім зафіксовує їх взаємне розташування. А в другому – обробляється зображення всього отриманого відбитка. Сучасні біометричні системи дедалі частіше застосовують комбінацію цих двох способів. Це дозволяє уникнути недоліків, які характерні окремо кожному алгоритму, і, внаслідок цього підвищити достовірність ідентифікації.

Процес ідентифікації триває секунди і не вимагає особливих зусиль і умов. Так, наприклад, продукт «BioLink Technologies» дозволяє за 0,1 секунди відсканувати зображення папілярної картини пальця, за 0,2 секунди розпізнати його та ухвалити рішення на право доступу власника пальця на об'єкт. Сучасні сканери відбитків пальців ергономічні та малі за розміром, що дозволяє інтегрувати їх у комп'ютерні миші, клавіатури або ноутбуки[2].

Принцип роботи пристроїв на основі технології ідентифікації за відбитками пальців, як і будь-яких інших пристроїв на основі технологій біометричної верифікації або ідентифікації, досить простий і охоплює чотири базові етапи:

– запис (сканування) біометричних характеристик (в цьому випадку – відбитка/ів/ пальця/ів/);

– відокремлення характерних деталей папілярного узору за рядом точок;

– перетворення отриманих характеристик у відповідний електронний формат;

– порівняння отриманого електронного формату біометричних характеристик із наявними в пам'яті автономного пристрою або базі даних системи електронними шаблонами (форматами);

– ухвалення рішення про збігання або незбігання отриманого під час перевірки біометричного зразка із шаблоном[3].

Процедура реєстрації відбитка пальця людини на оптичному сканері триває недовго. Крихітна CCD-камера, виконана у вигляді окремого пристрою або вбудована у клавіатуру, робить знімок відбитка пальця. Потім за допомогою спеціальних алгоритмів отримане зображення перетворюється на унікальний шаблон – карту мікроточок відбитка, які визначаються наявними в ньому розривами та перетинами ліній. Цей шаблон (а не сам відбиток) потім шифрується і записується в базу даних для верифікації

[1] Борзенко А. Биометрические технологии / А. Борзенко // Bytemag.ru. – 2001. – 10 октября. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

[2] Евангели А. Биометрические технологии / А. Евангели // Bytemag.ru. – 2004. – № 4 (68). – 10 апреля. [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/ articles/detail.php…

[3] Пахомов С. Отпечаток пальца вместо пароля / С. Пахомов // КомпьютерПресс. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Archive/...

(аутентифікації) користувачів. В одному шаблоні може бути виокремлено і збережено від декількох десятків до кількох сотень мікроточок.

У такому разі користувачі можуть не турбуватися про конфіденційність персонального відбитка, оскільки фотозображення узору відбитка пальця не зберігається і не може бути відтворено з електронного шаблону, крім передбачених законом винятків для спеціальних баз даних спецслужб і правоохоронних органів[1].

Принцип утворення біометричних шаблонів досить простий: спочатку реєструється особа користувача на основі її біометричних даних, наприклад, відбитків пальців – цей процес називається реєстрацією. Під час цього процесу пристрій сканує прикладений палець тричі.

Зчитані біометричні параметри зберігаються централізовано або децентралізовано, в останньому випадку на смарт-картках, токенах або інших подібних виробах.

Далі залежно від встановлюваної системи безпеки вибирається один принцип дії із двох варіантів для розпізнання людини – ідентифікацію або верифікацію (аутентифікацію). Як уже відомо з попередніх матеріалів посібника, в першому варіанті (за ідентифікації) користувач не повідомляє жодних своїх персональних даних. Після дотику пальця до спеціально призначеної для цього поверхні сканера починається пошук у базі даних аналогічного відбитка.

Ця процедура застосовується для здійснення авторизованого доступу до інформаційних систем, будівль або об’єктів, які захищаються.

У другому варіанті, тобто у разі верифікації, навпаки, користувач надає відповідну інформацію за допомогою смарт-картки або будь-якого іншого спеціального документа. Система допуску зіставляє надану інформацію з відсканованими під час перевірки розпізнавальними ознаками – у цьому випадку зі зчитаним відбитком пальця. Прикладом може бути будь-яке біометричне посвідчення або інший документ, коли система порівнює відскановані під час перевірки біометричні параметри власника посвідчення з даними, що зберігаються в документі.

Переваги такого підходу полягають у тому, що він дозволяє забезпечити як захист персональних даних, так і належний рівень контролю[2]. Тому фонд «Eurostars», сформований Єврокомісією для підтримки інноваційних бізнесів у країнах ЄС, виділив грант у 12 мільйонів норвезьких крон, який буде використаний для розробки біометричної ідентифікаційної карти із вбудованим надтонким сканером відбитків пальців. За відомостями російського біометричного порталу BIOMETRICS.RU грант одержали норвезька фірма «IDEX» та її французький партнер-компанія «UINT».

Упродовж двох років вони зобов’язалися створити смарт-карту, в яку буде інтегрований надзвичайно тонкий сканер відбитків пальців. Це рішення дозволить звести до мінімуму кількість процедур, які використовуються для обробки біометричних персональних даних користувача: усі вони будуть проводитися самою новою картою і не передаватимуться назовні.

Крім того, в смарт-карті будуть застосовуватися бездротові технології комунікацій близького поля (near field communication – NFC). Це означає, що власник карти зможе в безконтактному режимі використовувати її в різних платіжних системах (наприклад, для оплати проїзду в суспільному транспорті, вартості паркування, придбання товарів

[1] Борзенко А. Биометрические технологии / А. Борзенко // Bytemag.ru. – 2001. – 10 октября. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

[2] Кюн Мэнди. Защита доступа биометрическими методами / Мэнди Кюн // LAN. – 2007. – 2 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru /document.asp?group…

у магазині тощо), швидко, легко й безпечно підтверджуючи свої повноваження на проведення відповідної транзакції[1].

Технології отримання відбитків пальців і алгоритми розпізнавання їх узорів зараз є достатньо досконалими для того, щоб в автоматичному режимі одержувати еталонні шаблони відбитків пальців. У міжнародній спільноті існують стандарти на електронні еталони, зокрема й на шаблони відбитків пальців. Зазвичай такі стандарти застосовуються до еталонів, принцип дії яких побудований на виокремленні характерних деталей узору відбитків.

У світі найбільш відомим є стандарт Національного інституту стандартів і технологій США (NIST). Проте застосування стандартів майже завжди звужує сфери можливого застосування розроблених алгоритмів і обмежує право інтелектуальної власності на розробку. Тому часто доводиться вибирати між стандартизацією і швидкістю та точністю.

Враховуючи унікальність папілярного узору відбитка пальця, його з успіхом використовують замість пароля для аутентифікації особи, забезпечуючи тим самим достатньо надійний захист від зловмисників. Це стало однією з умов поширення комп'ютерних сканерів відбитків пальців. Нині ці сканери розміщуються в різноманітних виробах, а не тільки в спеціальному устаткуванні для проведення електронного дактилоскопіювання.

Дактилоскопічні сканери вбудовуються у вироби, що виконують функції електронного замка і регулюють доступ у приміщення. Спеціальними сканерами сьогодні оснащується низка моделей сейфів, а сучасні досягнення електроніки дозволяють оснащувати ними банківські кредитні картки. Банківська індустрія, яка особливо потерпає від діяльності шахраїв, із середини першого десятиліття XXI століття почала масове використання біометричних технологій. Поширилися комп'ютерні пристрої із вмонтованими сканерами, за допомогою яких здійснюється контроль доступу до комп'ютерів і комп'ютерних мереж.

Для електронно-програмних систем, що використовуються в різних інформаційно-комп'ютерно-телекомунікаційних технологіях, розроблена велика кількість сканерів, що підключаються, зокрема USB-інтерфейсом. А в багатьох ноутбуках такі сканери розміщені безпосередньо на лицьовій панелі. Зараз дедалі більше поширюються комп'ютерні миші та клавіатури, які, крім виконання своїх прямих функцій, через деякий проміжок часу сканують відбитки пальців працюючої особи, в такому разі особистість користувача[2].

За оцінками експертів і фахівців у галузі біометричних технологій і досі ідентифікація за відбитками пальців залишається домінуючою біометричною технологією у світі, переважаючи як за обсягом продажу, так і різноманітністю сфер застосування. До основних переваг ідентифікації за відбитками пальців, які зумовлюють лідерство на біометричному ринку, відносять достатньо високу точність і надійність розпізнавання користувачів, порівняно невисоку вартість апаратного забезпечення цього методу ідентифікації та чудову пристосованість цієї технології до виконання найрізноманітніших завдань контролю.

---

[1] Еврокомиссия профинансировала разработку биометрической смарт-карты // BIOMETRICS.RU. – 2012. – 19 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Пахомов С. Отпечаток пальца вместо пароля / Сергей Пахомов // КомпьютерПресс. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Archive/...

За оцінкою фахівців компанії «Frost & Sullivan» ідентифікація за відбитками пальців, безумовно, утримує першість, наприклад, у такій важливій галузі, як захист інформації (цій технології належить 88,7% від загального обсягу продажу біометричних рішень у цій сфері /дані 2007 року/)[1]. Враховуючи все зростаюче використання сканерів відбитків пальців у смартфонах і ноутбуках, цей показник, на думку авторів, не повинен зменшуватися.

За інформацією біометричного інституту в Лондоні експерти, які брали участь у дослідженні галузевого ринку за 2013 рік, одностайно зазначили, що найпоширенішими біометричними системами залишаються та будуть залишатися рішення, які реалізують технології ідентифікації за відбитками пальців і зображенням обличчя[2].

Із перегляду публікацій у ЗМІ очевидно, що технології персональної ідентифікація та аутентифікація за відбитками пальців збережуть першість за показниками прибутковості та загальної кількості інсталяцій у майбутньому. Це лідерство зумовлено досить високою точністю, невеликою вартістю апаратної частини порівняно з іншими методами біометричної ідентифікації та широким спектром застосування на практиці, зокрема у банківській та фінансовій сферах. Системи ідентифікації за папілярними узорами відбитків пальців вигідно відрізняються від інших біометричних систем за ознаками захищеності, часу незмінності самої біометричної ознаки та ціновими показниками.

За підсумками дослідження, проведеного компанією «Unisys» в 2008 році, сканування відбитків пальців увійшло до найпопулярніших методів ідентифікації користувачів. Майже 2/3 опитаних (67%) висловили довіру дактилоскопічним технологіям, які використовуються у світі урядовими установами, фінансовими, банковими і приватними організаціями.

Загалом біометричні рішення найбільш популярні у жителів Малайзії, Австралії та Великобританії. Саме у цих країнах за даними «Unisys» поки що малопоширені в інших країнах методи ідентифікації отримали більш широке визнання. Але у Гонконзі метод сканування відбитків пальців випередив усі інші технології ідентифікації[3].

Порівняно з популярними донедавна традиційними системами на картках (мається на увазі банківські пластикові картки, які не використовують біометричну ідентифікацію) технології біометричної ідентифікації за відбитками пальців мають низку переваг, особливо у так званих системах лояльності. Для систем лояльності головне – встановити особу людини, а точніше – історію платежів (покупок) клієнта. Біометричні системи ідентифікації мають такі переваги:

– об’єкт, за допомогою якого ідентифікується фізична особа, завжди при ньому. Його неможливо втратити або забути вдома;

– палець неможливо передати іншій особі, у зв’язку з чим у системі можливе створення механізму «прив’язки» електронних шаблонів пальців до одного конкретного обліковуючого рахунку. Цей же механізм дозволяє, «прив’язавши» до одного клієнта шаблони двох його пальців, знівелювати наслідки можливого пошкодження одного з них;

---

[1] Идентификация по отпечаткам пальцев остается главной биометрической технологией, применяемой финансовыми институтами // BIOMETRICS.RU. – 2007. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрический институт опубликовал результаты очередного исследования отраслевого рынка // BIOMETRICS.RU. – 2013. – 6 сентября. [Электронный ресурс]. – Режим доступа http://www.biometrics.ru/news/...

[3] Потребители доверяют сканерам отпечатков пальцев // Компьюлента. – 2008. – 16 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

– деякі клієнти можуть відчувати відразу та, як наслідок, дискомфорт через потребу контакту зі скануючим пристроєм, тобто присутні підвищена гидливість і особливі звички, що спричинюють неприємні відчуття від дотику до сканера. Для вирішення цієї проблеми клієнту потрібно нагадати про те скільки відбувається дотиків до грошових купюр, які є в нього у гаманці;

– у технологіях, заснованих на біометричних показниках, здебільшого унеможливлюється присутність реклами. Тобто на звичайних картках можуть бути вказані реквізити магазину, розміщені приваблива картинка, логотип, схема проїзду тощо. Для систем із суто біометричними ідентифікаторами такого предмета-носія реклами не існує;

– системи з ідентифікацією за відбитками пальця можуть нагадувати про ідею тотального контролю або тотального стеження. Для нейтралізації цієї загрози клієнтам супермаркетів необхідно роз'яснювати, що в системах лояльності не зберігається жодної особистої інформації, окрім електронного шаблону відбитка пальця, і налічувати знижку не конкретній особі за відомими персональними даними, а невідомому із таким відбитком пальця;

– у разі появи можливих труднощів під час розпізнавання пальця (палець прикладений під кутом, частково забруднений або пошкоджений), для успішної ідентифікації клієнта у таких випадках потрібно мати резерв значних обчислювальних ресурсів. Однопроцесорні сервери початкового рівня нині можуть забезпечити швидкість порівняння до 10 тисяч пар відбитків у секунду, що може виявитися недостатнім під час використання таких систем у великих супермаркетах і, як наслідок, вимагати додаткових затрат або запровадження додаткових вимог під час розпізнавання: введення ймовірної моделі пошуку клієнта, зміни алгоритму обслуговування клієнта або надання йому додаткового коду, що дозволить зменшити кількість переборів (порівнянь)[1].

Персональна ідентифікація за відбитками пальців – одна з найпопулярніших технологій, яка застосовується для забезпечення контролю доступу до комп'ютерів і комп'ютерних мереж. Завдяки цій системі користувачам більше не потрібно набирати пароль, адже доступ забезпечує одне доторкання до скануючого пристрою. Біометрична технологія на основі папілярних узорів пальців нині має найбільшу кількість застосувань і напрямів використання з усіх біометричних технологій, які вживаються у різних сферах людської діяльності.

Наприклад, у низці штатів США перевіряють відбитки пальців кандидатів на соціальну допомогу для того, щоб унеможливити випадки обману. У Нью-Йорку ще 2007 року почала функціонувати така база даних, яка налічувала приблизно 900000 тис користувачів. Тут неможливо не згадати проект присвоєння індійським громадянам ідентифікаційних номерів «Aadhar», який уже налічує понад 0,6 млрд фігурантів.

Також у світі ширше використовується організація доступу до мережевих ресурсів і комп'ютерів шляхом сканування та подальшої перевірки пред'явлених відбитків пальців користувачів.

Переваги цього способу доступу полягають у його майже загальному сприйнятті, зручності та надійності[2].

---

[1] Радостин А. Перспективы использования биометрии в системах лояльности / Александр Радостин // RB.RU. – 2008. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp?group...

[2] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art103.html...

2.4. Технологічні методи та принципи побудови сканерів, які використовуються для отримання зображень відбитків пальців

Відомо, що нині використовуються або розробляються декілька різних технологій електронного зняття (сканування) відбитків пальців. Найбільш поширені та відомі такі методи: *оптичний, ємкісний, радіо, натискувальний, мікроелектромеханічний і температурний.* Відповідно, для отримання зображень відбитків пальців розроблені та застосовуються різні спеціалізовані сканери, що використовують зазначені технології електронного одержання малюнків папілярних узорів відбитків пальців. Коротко розглянемо технологічні особливості вказаних методів.

Оптичний метод. Для отримання оптичного зображення відбитка пальця використовується пристрій, який подібний до цифрової камери. Кінчик пальця прикладається до поверхні скляної пластини, яка в цей час повинна бути відповідно освітлена. Потрібен лише об'єктив, що може працювати безпосередньо на невеликій відстані від об'єкта зйомки. Захоплення зображення відбувається за допомогою матриці елементів із зарядним зв'язком (CCD) або елементів потрібного вирішення (CMOS) і перетворюється на зображення з відтінками сірого кольору (на практиці цілком вистачає використання від 2-х до 16-ти відтінків). Одним із недоліків цієї технології є те, що непомітний для ока відбиток пальця залишається на поверхні скляної пластини і може бути використаний вдруге. Цей метод має ще один суттєвий недолік: він не завжди може відрізнити справжній палець від добре виконаного імітатора (муляжу).

Але використання останніх технічних досягнень і разом із цією технологією низки доповнюючих розробок призвели до того, що нині одну з найдосконаліших технологій ідентифікації за відбитками пальців забезпечують саме оптичні сканери. Вони дещо дорожчі за сканери інших типів, але позбавлені багатьох їх вад, є довговічними, а тому й економічними, відрізняються зручністю та доволі прості у використанні. Зображення відбитків, які отримуються на основі цього методу, є досить високої якості. А проведені дослідження довели, що в антибактеріальному відношенні оптичні сканери відбитків пальців цілком безпечні.

Ємкісний метод. Коли кінчик пальця торкається спеціальної матриці елементів, яка досить чутливо реагує на будь-який електричний заряд, різниця в електропровідності виступів-гребенців (які містять багато води) і западин (що наповнені повітрям) шкіри пальця призводить до локальної зміни ємності елементів матриці. Це дозволяє визначити загальну картину положення виступів і западин й сформувати зображення відбитка. Незважаючи на такий недолік, що цей метод дуже чутливий до різних електростатичних розрядів та інших паразитних електричних полів, що значно знижує його ефективність, він є одним із досить поширених для одержання зображень відбитків пальців. Але такі сканери порівняно легко можна «обдурити» імітованим муляжним відбитком або прихованим відбитком на поверхні сканера.

Ємкісні сканери є найдешевшими, проте під час експлуатації вони не довговічні, оскільки зображення відбитків у цих сканерах формується за допомогою різниці електричних потенціалів різних ділянок шкіри пальця і, як наслідок, ці сканери надзвичайно чутливі до залишкової статичної електрики. На практиці дуже часто вони виходять із ладу відразу ж після того, як до них торкнулася людина, якої руки були наелектризовані внаслідок тертя об одяг із вовняної або шовкової тканини.

Також якість зображення відбитків, що отримуються за допомогою ємкісних сканерів, досить низька.

Радіометод. Якщо опромінити кінчик пальця радіохвилями низької інтенсивності, то різницю у відстанях між поверхнею виступів і западин шкіри пальця можна визначити за допомогою матриці відповідно налаштованих антенних елементів. У такому разі потрібно, щоб кінчик пальця контактував із випромінюючим елементом датчика у всій периферії.

Оскільки метод заснований на фізіологічних властивостях шкіри, його дуже складно «обдурити» імітацією пальця. Слабким місцем методу є необхідність якісного контакту у всій периферії пальця з джерелом радіохвиль, який може бути досить гарячим за інтенсивного використання сканера.

Натискувальний метод. Для одержання візерунка папілярних ліній відбитка пальця, який прикладається, може застосовуватися матриця із чуттєвих до натискання п'єзоелектричних елементів. Незважаючи на наявність низки суттєвих недоліків цього методу (низька чутливість, нездатність відрізнити палець від муляжу /імітації/, схильність до ушкоджень через надмірно докладене зусилля), багато компаній використовують його у пристроях, які вони виробляють.

Мікроелектромеханічний метод. Цей метод (MEMS) поки що перебуває у проміжній стадії між науково-дослідними лабораторними розробками та впровадженням. Для визначення візерунка виступів і западин відбитка пальця використовується спеціальна матриця мікромеханічних датчиків, але поки ще не досягнута необхідна стійкість до зносу. Недолік методу полягає в тому, що він не дозволяє відрізнити муляж від реального пальця людини.

Температурний метод. Піроелектричний матеріал може перетворювати різницю температур на певну напругу. Цей ефект отримується за допомогою інфрачервоних камер. Температурний сканер відбитків пальців на основі такої технології вимірює різницю температур за допомогою чутливих елементів у місцях, що перебувають у контакті з виступами шкіри (гребінцями), і місцях, які не контактують зі шкірою пальця (западинами).

Температурний метод має багато переваг. Це й висока стійкість до електростатичного розряду, і відсутність необхідності опромінювати кінчик пальця радіохвилями низької інтенсивності. Температурний датчик однаково надійно працює як за граничних, так і звичайних (кімнатних) температур. Його практично неможливо обдурити штучною імітацією пальця. Але недоліком технології є те, що тривалість зберігання зареєстрованої картини зображення досить малий. У разі прикладання пальця в перший момент різниця температур, а отже і рівень сигналу досить значні, але впродовж нетривалого часу (менше десятої частки секунди) зображення зникає, оскільки палець і датчик набувають температурної рівноваги.

Більшість сканерів відбитків пальців використовують два технологічні способи отримання відсканованого зображення відбитка пальця: *нерухоме або рухоме зображення під час сканування.*

Перший спосіб *(нерухоме зображення під час сканування)* полягає в тому, що використовується нерухомий чутливий елемент розміром із потрібний відбиток і прикладати треба до нього палець на час, який необхідний для одержання зображення. Перевага цього способу полягає у тому, що одержання та передача всього зображення відбувається одночасно і за один раз. До недоліків належать умова, відповідно до якої контактний елемент повинен мати порівняно великі розміри, тому і його ціна є вищою, а також те, що на поверхні нерухомого елемента залишається непомітний для ока відбиток попередньо відсканованого цілого пальця, що надає можливість за певних умов відтворити його.

Другий спосіб *(рухливе зображення під час сканування)* використовує чутливу матрицю шириною з відбиток пальця та висотою всього в декілька елементів, за яким вертикально проводять пальцем. Під час використання цього способу отримують декілька частин зображень, а ціле зображення формується або конструюється з одержаних частин за допомогою спеціальних математичних програм. Перевагами такого методу є малий розмір самої контактної матриці (і, як наслідок, – її низька вартість), стабільність зображення під час використання в комплексі з температурним методом, а також те, що матриця фактично самоочищується, тобто на ній не залишається відбитка цілого пальця після сканування. Ця технологія є обов'язковою під час використання методу температурної матриці через нетривалий час збереження малюнка отримуваного зображення[1].

Контактне місце сканування у більшості сканерів становить прямокутник із розмірами 20 × 25 (20S25) або 15 × 15 (15S15) мм.

За своїми якісними характеристиками та технологічністю прокатні сканери, в яких зображення відбитка формується шляхом прокатування пальця вузьким контактним віконцем сканера (звідси і назва), а повне зображення для ідентифікації «зшивається» з декількох окремих кадрів, займають середнє положення з загальної кількості тих, що використовуються. Від користувачів такого сканера потрібне постійне дотримування одноманітності у швидкості та манері «прокатування» відбитків, що на практиці реалізувати доволі складно[2].

У роботі сканерів, як і будь-яких інших пристроїв, цілком можливе виникнення помилок, які залежать від таких характеристик, як якість і чутливість розрішення сканування, розмірів віконця сканера та кількості характерних особливих точок, що використовуються у процесі порівняння. Поява помилок залежить також від якості використовування математичних алгоритмів, які описують процедури базових етапів ідентифікації відбитків пальців.

Для зменшення виникнення помилок сканери відбитків пальців мають шкляне віконце у місці прикладання пальця, яке виконується із високоякісного шкла з високою стійкістю до виникнення подряпин. Проте одержання високоякісного відбитка залежить не тільки від наявного розрішення сканера, але повинна бути забезпечена висока контрастність зображення за відсутності такого явища, як паралакс. Але навіть під час отримання досить контрастного зображення за відсутністю паралакса та високим розрішенням, для поліпшення загальної картини отриманого папілярного узору застосовують спеціальні фільтри-маски, що зменшують рівень шуму і так званого відлуння від попереднього сканування і тільки тоді проводять саму процедуру аналізу (порівняння).

Особливо це стосується сканерів, що використовують принцип нерухомого зображення під час сканування. Під час сканування відбитка пальця на шкляній поверхні віконця сканера залишається невидимий для ока відбиток пальця, який зумовлений виділенням поту і який може вплинути на точність одержання зображення нового відбитка пальця.

Розробкою сканерів у світі в кінці першого десятиріччя XXI століття займалися понад 50 фірм-виробників. В огляді, наданим у середині 2013 року компанією «Technavio», прогнозується, що середньорічні темпи зростання ринку сканерів біомет-

[1] Бишоп П. Технология биометрической защиты ATMEL FINGERCHIP / П. Бишоп // Электронные компоненты. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.efo.ru/doc/Atmel/...

[2] Идентификация по отпечаткам пальцев // Biolink. – 2007. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/ technology/fingerprint.php…

ричних ідентифікаторів у 2012–2016 роках, обчислених у складних відсотках, будуть становити 17,1%.

Фахівці фірми «Technavio» виокремлюють два головні чинники, які сприяють розвитку аналізованого сегмента ринку. Перший із них є зовнішнім і полягає в збільшенні загальної кількості високотехнологічної апаратури для потреб безпеки з боку урядових структур. Другий «внутрішній» чинник стосується самого біометричного ринку: його виявом є досить виразна останніми роками тенденція до злиття діючих на ринку компаній та до поглинання дрібних гравців більшими.

Як приклади, що ілюструють цю тенденцію, автори огляду наводять такі два найбільші злиття: покупку французькою групою «Safran» американської фірми «L-1 Identity Solutions» (за 1,1 млрд доларів) і придбання компанією «3M» фірми «Cogent» (за 943 млн доларів)[1].

Популярність сканерів відбитків пальців зумовлена тим, що вони мають низьку вартість, досить компактні та за статистикою дають дуже високу ймовірність ідентифікації. За останніми публікаціями зараз використовуються три види сканерів: оптичні, напівпровідникові й ультразвукові, вони відрізняються за фізичним принципом дії та вартістю[2].

За останні 10 років характеристики систем розпізнавання за пальцями не дуже змінилися, але самі сканери для зняття відбитків пальців продовжують розвиватися в декількох напрямах. Насамперед це комбінування з іншими біометричними системами, зокрема заснованими на зчитуванні малюнка вен. Сканер венозного малюнка використовує близький інфрачервоний діапазон, тому зчитування відбудеться навіть тоді, коли особа, яку ідентифікують, не знімає рукавички.

Перевага поєднання звичайного сканера відбитків пальців із цією технологією полягає в тому, що коли навіть самі пальці індивідуума будуть пошкоджені та їх не вдасться нормально відсканувати, то з кровоносною системою долоні чи пальця таких проблем не виникне, крім того, створити муляж для обману подібного сканера навряд чи можливо.

Ще один шлях – подальше удосконалення сканерів, що аналізують біологічні особливості людини, а саме – хімічний склад поту. Компанія «Intelligent Fingerprinting» наприкінці 2012 року представила сканер відбитків пальців, який може визначити: чи вживала людина наркотики. Розроблена система здійснює експрес-аналіз невеликої кількості поту, який завжди є на кінчиках пальців. Розвиток цієї технології може призвести до того, що в базу зберігаючих даних будуть вноситися не тільки папілярні візерунки, але й біохімічні шаблони кожної людини. Але такий підхід має суттєві складності, оскільки хімічний склад людського поту може змінюватися від загального стану організму, а саме: перебування у стресовому стані, стану здоров'я, та залежить від продуктів харчування тощо. Але зараз у системах контролю управління доступом (СКУД) такі сканери можуть застосовуватися для перевірки на наркотичне або алкогольне сп'яніння під час допуску співробітників на роботу.

Компанія «Advanced Optical Systems» (AOS) зробила ставку на принципово новий рівень сканерів відбитків пальців. 2011 року AOS розробила систему «Airprint», яка дозволяє обійтися без безпосереднього прикладання долоні або пальця до сенсора. За допомогою двох 1,3-мегапіксельних камер і джерела поляризованого світла сканер

[1] Мировой рынок биометрических сканеров продолжит расти // BIOMETRICS.RU. – 2013. – 22 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрические технологии в системах контроля доступа // Cleper.ru. – 2013. – 21 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

«Airprint» може зчитувати папілярні візерунки з відстані двох метрів і обробляти їх за декілька секунд.

Прототип обладнання діяв тільки на фіксованій відстані, але наступні моделі успішно працювали й під час руху людини. Звичайно, зараз ще необхідно спеціально простягнути руку в сторону сканера, однак у перспективі процес верифікації може проходити без будь-яких додаткових дій і фактично бути непомітним. Але успішність застосування подібної біометричної системи прямо залежить від удосконалення алгоритмів, які застосовуються під час обробки зчитуваних відбитків[1].

2.5. Автоматизовані дактилоскопічні ідентифікаційні системи (АДІС)

Порівняння відбитків пальців є однією із найпоширеніших технологій біометричної ідентифікації завдяки простоті використання, відсутності можливості стороннього втручання, надійності та ціни порівняно з іншими видами біометричної ідентифікації.

Для розпізнавання за порівнянням відбитків пальців використовуються два основні алгоритми. Перший алгоритм – це метод, який базується на виокремленні ключових точок, а другий – алгоритм, який використовує принцип порівняння або зіставлення узорів. Ці методи по-різному оцінюють зображення відбитків пальців: метод виокремлення ключових точок зіставляє особливі деталі папілярного узору відбитка пальця, а метод порівняння узорів повністю зіставляє характеристики наявних відбитків пальців.

Постійний розвиток біометричних технологій, які засновані на аналізі зображень відбитків пальців, призвели до появи точніший алгоритмів біометричної аутентифікації, що об’єднують переваги і традиційних методів виокремлення ключових точок, і методів порівняння папілярних узорів (наприклад, технологія, що отримала назву «Precise BioMatch»).

Такий подвійний підхід дозволяє отримати максимум інформації з кожного відбитка пальця для проведення якісного аналізу та гарантувати достовірну аутентифікації або ідентифікацію. Технологія подвійного підходу була розроблена не тільки для алгоритмів аутентифікації особистості у великих базах даних (наприклад, алгоритм AFIS /Automated Fingerprint Identification System/ – автоматичної системи розпізнавання відбитків пальців), але і для найліпшого підтвердження особи індивідуума за логічного і фізичного доступу.

Розглянемо метод виявлення ключових точок. Картина кожного відбитку пальця складається з певної кількості смуг і чистих місць між ними. Смуги – це виступаючі частини шкірного покриву (гребенці), а чисті місця на відбитку папілярного узору – рівчаки (борозни), тобто западини між гребенцями.

Початок і закінчення кожної смуги становлять так звані ключові точки: кінці смуг (там, де смуги закінчуються) і роздвоєння – там, де вони розгалужуються. Ключові точки одного й того ж відбитка пальця мають раз і назавжди сформовані місця розташування, тому ці місця можливо точно визначити, а параметри їх місцезнаходження зареєструвати. На основі отриманих даних створюється зразок (шаблон) – постійна у часі

[1] Биометрические технологии в системах контроля доступа // Cleper.ru. – 2013. – 21 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

інформація, що згодом буде використовуватись для підтвердження (засвідчення) особи користувача.

На етапі порівняння (зіставлення) зчитане за допомогою сканера зображення відбитка пальця піддається попередній обробці, під час якої визначаються та «витягуються» основні ключові точки. Вони порівнюються з уже зареєстрованим зразком (шаблоном), водночас програма шляхом зіставлення знаходить і порівнює у потрібних місцях якомога більшу кількість подібних точок у межах отриманого/их/ і заданого/их/ зразків. Підсумком проведеного зіставлення є деяка кількість ключових точок, що збіглися між собою у зразках, що порівнюються. Далі задається обраний поріг числа збігання, який встановлює прохідний бар'єр для проведення подальшого більш детального зіставлення отриманого відбитка пальця з обраними для ототожнення зразками.

Позитивні моменти цього методу:

– використовується в додатках AFIS (Automatic Fingerprint Identification Systems – автоматичної системи ідентифікації за відбитками пальців);

– досить широко відомий і добре досліджений метод;

– алгоритм підходить для множинного зіставлення, тобто ідентифікації.

Негативні моменти цього способу:

– оскільки цей спосіб пред'являє досить жорсткі умови до чутливості (розрішення) та розмірів датчика, він може бути застосований не у всіх технологіях, які використовують зчитування відбитків пальців. Під час використання сканерів, які мають менш досконалі параметри, ніж апаратура AFIS-класу, отримуються досить неякісні результати;

– особи, які зовсім не мають або мають невелику кількість ключових точок (зумовлено особливим станом поверхні шкіри) не можуть використовувати таку систему. Загальна кількість ключових точок (їх мінімальна кількість) може бути обмежувальним чинником для безпеки використання цього методу (алгоритму);

– можливі збої у технологічній системі через появу хибних ключових точок (виникнення ділянок, що містять помилкові ключові точки, які виникли внаслідок низької якості реєстрації та відтворення зображення або нечіткого відбиття виступаючих частин шкірного покриву /гребенів/).

Важливою властивістю другого алгоритму – *методу порівняння (зіставлення) візерунків* – є те, що до уваги беруть не тільки окремо взяті характерні точки, але й інші, більш всеосяжні характеристики відбитка пальця. Ці характеристики можуть охоплювати певний відсоток додаткових даних таких, як товщина смуг папілярних ліній, їхня кривизна або ущільненість.

Через збільшення кількості даних, що перевіряються, алгоритм, заснований на порівнянні візерунків, менше залежить від величини вікна сканера (місця прикладання пальця) й абсолютно не залежить від кількості ключових точок у відбитку пальця. Алгоритм, що використовує зіставлення візерунків, – на відміну від методу виокремлення ключових точок дає значно кращі результати під час розпізнавання відбитків пальців не досить високої якості.

Процес порівняння починається з попередньої обробки зчитуваного зображення відбитка. Зразки (шаблони) із зареєстрованими візерунками зіставляються із зображенням відбитка, який перевіряється, щоб визначити, наскільки зразки збігаються із зображенням, що перевіряється.

Позитив цього алгоритму:

– чудово працює з усіма відомими типами сканерів відбитків пальців;

– навіть не дуже високої якості відбитки можуть бути зареєстровані тоді, коли вони не мають зовсім або мають невелику кількість ключових точок;

– підходить для виконання роботи з обмеженою кількістю обчислювальних ресурсів, наприклад, смарт-картки.

Негатив цього алгоритму:

– не може використовувати шаблони, що є в базі даних AFIS, проте використовує для верифікації оригінали зображень;

– не оптимізований для ідентифікації (тобто для встановлення конкретної особи в схемі «один до багатьох»).

Симбіоз цих двох алгоритмів – *технологія подвійного підходу* використовує і метод виокремлення ключових точок, і алгоритм зіставлення візерунків. Об'єднання двох різних технологій в одну дозволяє ефективніше працювати з різними видами зображень та з відбитками низької якості.

У разі застосування технологій, що використовують тільки один з алгоритмів, індивідуумові, який має відбиток пальця з невеликою кількістю ключових точок або з нечітким візерунком, майже завжди буде відмовлено в реєстрації, а у разі використання технології подвійного підходу (змішаної технології) за тих же умов буде отриманий позитивний результат.

Використовуючи терміни теорії інформації, можна зазначити, що два описані методи застосовують різні підмножини даних про відбиток і в якомусь сенсі ці підмножини можна назвати *ортогональними* (тобто незалежними, що не можуть виражатися один через одного).

У результаті поєднання ортогональних підмножин отримуємо алгоритм із дуже добрими характеристиками розпізнавання: високим співвідношенням якісного (правильного) розпізнавання до числа помилкових (Receiver Operating Characteristic)[1].

Розпізнавання відбитків пальців застосовуються в різноманітних сферах людської діяльності, але всі методи розпізнавання в різних галузях застосування мають подібні основні процедури. Вони не залежать від вживаних технологій зчитування та програмного забезпечення, які використовуються для отримання зразків та еталонів (шаблонів) і методик зіставлення відбитків, які перевіряються з еталонними даними.

Розглянемо основні процедури розпізнання відбитків пальців, що мають однакову послідовність дій.

Реєстрація. Реєстрація полягає в одержанні та збереженні (реєстрації) еталонних шаблонів відбитків пальців індивідуума. Процедура повинна відбуватися у спокійній і безпечній обстановці, яка не передбачає можливості одержання еталонного відбитка від підставної особи або зміни будь-яким чином отриманих для еталона даних. Одержаний малюнок візерунка відбитка або набір електронних даних, які містять основні характеристики папілярного візерунка, має назву зареєстрованого еталона фізичної особи. Він записується у відповідний персональний магнітний носій (наприклад, смарт-картку) або жорсткий магнітний диск (вінчестер) сервера, на якому зберігаються відомості спеціального банку даних.

Одержання зображення. Одержання зображення полягає у створенні растрового зображення з потрібним розрішенням усього відбитка пальця або його частини. Під час використання прокатних сканерів отримують зображення у вигляді кадрової послідовності окремих складових. У такому разі обов'язково треба проводити реконструкцію для одержання цілого зображення.

[1] Технология биометрической аутентификации Precise BioMatch // Morepc.ru. – 2006. – 20 октября. [Электронный ресурс]. – Режим доступа: http://www.morepc.ru/security/authentication/precise...

Реконструкція зображення. За умовою, що палець переміщався датчиком сканера з необхідною швидкістю, елементи зображення, що повторюються на суміжних кадрах, дають можливість реконструювати зображення папілярних ліній відбитка у одну цілісну картину. Ця операція виконується автоматично за допомогою відповідного програмного забезпечення.

Вимоги до реконструйованих зображень наведені у стандарті IQS ФБР США. Зазвичай реконструйоване зображення має розміри 25 х 14 мм, що еквівалентно 500280 точкам. Під час використання 8 біт на прив'язку однієї точки потрібно для зберігання 140 Кб пам'яті лише на одне зображення. Із такого зображення можуть бути отримані малюнки більшого або меншого розміру за допомогою стандартних процедур обробки зображень залежно від обставин, що виникли.

Витяг еталонів і зразків. За вимогами безпеки, а також через обмеження, що пов'язано з обсягом пам'яті, зберігати зображення папілярних візерунків відбитків у системі розпізнавання в оригінальному вигляді не рекомендовано (еталонне оригінальне зображення під час реєстрації може зберігатися в спеціальному добре захищеному сховищі як запасного варіанта у разі надзвичайних обставин, але сам оригінал зображення не потрібен для нормальної роботи більшості систем).

Стандартна процедура розпізнавання охоплює можливість витягу унікального еталона папілярного відбитка у разі потреби для розпізнавання характерних рис або деталей візерунка. Загалом при реєстрації отримуємо еталон, та під час перевірки – зразок. Процедура розпізнавання в обох випадках є однакова. Це обумовлено декількома причинами. Розглянемо їх.

Як правило, типовий шаблон охоплює набір 36 дрібних деталей, кожна з яких займає 4 байти пам'яті – всього потрібно 144 байти. Це дає значне зменшення пам'яті, яка необхідна для збереження одного «електронного» зображення.

Вважається, що повний візерунок відбитка пальця не може бути реконструйований із електронного еталона. Такий факт зменшує можливість незаконного використання електронних еталонів відбитків зловмисниками або недобросовісними співробітниками.

Еталони можуть бути зменшені у розмірах (стиснуті) будь-яким стандартним алгоритмом стискування даних, а за необхідності – зашифровані. Це дуже важливо під час використання в таких формах практичного застосування, як смарт-картки, токени, де обсяги пам'яті обмежені, а вимоги до безпеки високі.

«Діставання» еталонних зразків або просто еталонів виконується спеціальним програмним забезпеченням, розробленим відповідно до стандартної процедури розпізнавання, опису та представлення деталей відбитків.

Зіставлення зразків і еталонів. Останньою стадією технологічного процесу є порівняння отриманого зразка з набором уже наявних зареєстрованих еталонів (ідентифікація) або з одним конкретно облікованим еталоном (аутентифікація) у випадку, якщо потрібне підтвердження особистості індивідуума. Як показала практика, малоймовірно, щоб зразок і шаблон (еталон) збіглися з точністю до байта. Це неможливо через технічні обмеження під час використання різних моделей сканерів (наприклад, розрішення у 50 мкм досить далеке від ідеалу), неточного зіставлення зображень і помилок так званої приблизності, що одержуються на етапі витягу дрібних деталей. Відповідно, потрібен такий алгоритм порівняння (зіставлення), що може перевіряти різні орієнтації зображення та відповідність дрібних деталей і оцінювати рівень збігання за числовою шкалою. Під час перевищення деякого заздалегідь визначеного порога числа збігань вважається, що процес ідентифікації або аутентифікації відбувся, тобто засвідчується сам факт відповідності зразка, який перевіряється, еталонному.

За таким підходом існує два типи можливих помилок:

– *помилковий (хибний) допуск*, коли зразок, що перевіряється, і еталон належать різним індивідуумам, але мають досить високий рівень подібності та визнаються системою контролю ідентичними. У підсумку стороння особа успішно проходить контроль. Імовірність такої події називається коефіцієнтом помилкового допуску;

– *помилкове (хибне) відмовлення*, коли зразок, який перевіряється, і еталон належать одному й тому ж індивідуумові, а система контролю видає недостатній рівень збігання (відповідності) і, як наслідок, особа, яка є зареєстрованою у системі, не проходить процедуру контролю. Ймовірність такого результату називається коефіцієнтом помилкового відмовлення.

Розробники всіх систем розпізнання відбитків пальців прагнуть мінімізувати коефіцієнти помилкового допуску і помилкової відмови, але на практиці досягається компромісних значень коефіцієнтів. Адже зниження одного коефіцієнта зумовлює збільшення іншого, і навпаки.

Пороговий рівень підбирається так, щоб максимально мінімізувати наслідки можливих помилок.

Деякі системи контролю з метою мінімізації наслідків можливих помилок, окрім допуску та відмови у допуску, передбачають наявність третього варіанта: від особи, яка не пройшла з першого разу ідентифікацію, система вимагає повторення проходження процедури контролю або надання спеціальної додаткової інформації. Тобто, необхідне здійснення процедури повторного сканування того ж пальця або провести сканування іншого пальця, якщо програмою передбачена наявність резервного еталона (шаблону).

Процес порівняння (зіставлення) зразка і шаблону (еталона) виконується повністю за допомогою спеціального програмного забезпечення і не залежить від технологій, за допомогою яких отримуються відбитки пальців. Проте найважливішою вимогою залишається отримання зображень якомога вищого розрішення. Виконання цієї умови дає можливість звести кількість помилок до мінімуму[1].

Як відомо, біометричні системи кінця XIX – початку XX століть мали своє основне і, мабуть, єдине призначення – вони використовувались лише у криміналістиці. Але згодом застосування дактилоскопічних систем розширилося. Аналітики розділяють системи ідентифікації особистості індивідуума за відбитками пальців на два класи – AFIS (Automatic Fingerprint Identification Systems) і Fingerprint.

Як правило, AFIS застосовують силові структури й правоохоронні органи. В такому разі використовуються відбитки пальців, які споконвічно отримувались за допомогою паперу та барвника (на практиці ці відбитки скануються і переводяться в електронний вигляд). Пошук у базі даних відбитків проводиться автоматично, але остаточне рішення ухвалює експерт. Різновид таких систем – AFIS/Livescan дозволяє сканування відбитків пальців за допомогою сканерів.

Системи типу Fingerprint застосовують різні несилові державні та комерційні організації. У них використовується тільки електронне сканування, а самі візерунки відбитків пальців ніде не зберігаються (у базі даних зберігаються лише еталонні цифрові моделі /шаблони/)[2].

---

[1] Бишоп П. Технология биометрической защиты ATMEL FINGERCHIP / П. Бишоп // Электронные компоненты. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.efo.ru/doc/Atmel/...

[2] Митин Владимир. Биометрические технологии, которые мы выбираем / Владимир Митин // PC Week/RE. – 2010. – 09 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Зробимо невеликий екскурс у світову історію створення автоматизованих дактилоскопічних ідентифікаційних систем (АДІС), що створювалися для підвищення ефективності боротьби зі злочинністю.

Приблизно із середини шістдесятих років минулого століття вчені багатьох країн почали інтенсивно займатися розробкою автоматизованих методів і необхідного обладнання для надання допомоги криміналістам у вирішенні проблеми швидкісного дактилоскопічного пошуку. Практичному вирішенню цієї проблеми сприяв бурхливий розвиток нових напрямів науки і техніки, а саме: кібернетики, методів розпізнавання образів, електронної обробки зображення, появи електронно-обчислювальних машин (ЕОМ) і розробки програмно-математичного забезпечення до них.

Наприкінці 70-х – початку 80-х років минулого сторіччя правоохоронними органами розвинених країн почали надходити перші автоматизовані дактилоскопічні *ідентифікаційні* /в деяких джерелах – *інформаційні*/ системи (АДІС). Там, де ці системи впроваджувались, суттєво зростала кількість розкритих злочинів.

У СРСР у минулому столітті в МВС зі середини 70-х років у кожному УМВС (ГУМВС) були розгорнуті машинотехнічні програмні комплекси, але автоматизовані дактилоскопічні інформаційні системи так і не були впроваджені. Роботи зі створення системи АДІС були тільки на дослідницькому етапі.

1987 року в м. Челябінськ Віталій Шмаков, нині полковник міліції у відставці, запропонував метод математичного індексування папілярних візерунків, який дозволив значно спростити й пришвидшити процес звірки відбитків пальців. Завдяки запропонованому методу вдалося математично описати папілярний візерунок і, як наслідок, ввести його в електронну пам'ять ЕОМ. 1991 року почалася практична експлуатація АДІС «Папілон»[1].

За іншими відомостями в деяких регіонах Росії автоматизована дактилоскопічна інформаційна система (АДІС) «Папілон» почала функціонувати з 1989 року[2].

Нині система «Папілон» поширена на всій території Російської Федерації (РФ) та за її межами: у країнах Африки і Латинської Америки. На базі АДІС «Папілон» створені та розвиваються національні системи автоматизованих дактилоскопічних обліків для потреб поліції Казахстану, Албанії, Нігерії. Постачання обладнання також здійснювалося до В'єтнаму, Монголії, Польщі, Таджикистану, Туркменістану[3].

Влітку 2013 року МВС РФ підготувало проект наказу голови відомства Володимира Колокольцева про створення принципово нової єдиної системи контролю, обліку й систематизації пальчиків на базі діючої «Системи автоматизованих банків даних дактилоскопічної інформації».

Відповідно до планів міністерства, запуск єдиної загальної бази даних був запланований на 1 жовтня 2013 року.

Досі більшість регіональних підрозділів користувалися лише власними картотеками пальчиків на основі АДІС «Папілон» і «Дакто 2000». Використання різних систем значно ускладнювало обмін дактилоскопічною інформацією та проведення швидкої ідентифікації.

---

[1] Малкова Марина. Челябинский создатель системы «Папилон» стал почетным ветераном МВД / Марина Малкова // Chelyabinsk.ru. – 2013. – 26 февраля. [Электронный ресурс]. – Режим доступа: http://chelyabinsk.ru/text/newsline/...

[2] МВД создаст всероссийскую дактилоскопическую базу данных // Известия. – 2013. – 5 августа. [Электронный ресурс]. – Режим доступа: http://izvestia.ru/news/...

[3] Успех биометрии от Папилон на Milipol'2007 (Париж, Франция) // Папилон. – 2008. – 11 января. [Электронный ресурс]. – Режим доступа: http://www.papillon.ru/news.php...

Наприклад, навіть Москва й Московська область використовували різні системи автоматичних баз даних.

Відповідальним за запуск системи призначений Головний інформаційно-аналітичний центр (ГІАЦ) МВС РФ: саме він виділяв і надалі виділятиме кошти на установку, монтаж і обслуговування потрібного устаткування в межах держоборонзаказу.

Відповідно до планів МВС Росії, комплекс АДІС має бути встановлений в усіх регіональних управліннях, федеральних суб'єктах Росії й у спеціалізованих управліннях. Наприклад, у транспортній поліції. До системи згодом підключать російське бюро Інтерполу. Як наслідок – це можливість взаємодії з аналогічними іноземними базами даних.

У МВС РФ на нову систему покладають великі надії. Автоматизована система дозволить значно підвищити ефективність роботи розшукових і слідчих підрозділів. За інформацією прес-центра МВС співробітники органів внутрішніх справ навіть із периферії зможуть упродовж дуже короткого часу отримати інформацію з єдиної бази[1].

Створення єдиної системи контролю, обліку й систематизації дактилоскопічної інформації, як зазначалося, зумовлено тим, що в Росії використовувались різні АДІС: «Папілон» (розробник РФ), «Дакто 2000» (РФ – Республіка Білорусь), «SONDA» (РФ), «Узор-3» (РФ), «MORPHO» (Франція), «Дельта-С» – США і деякі інші[2].

У Росії, відповідно до закону про добровільну дактилоскопічну реєстрацію, на час запровадження єдиної системи контролю, обліку й систематизації дактилоскопічної інформації вже була накопичена база в декілька десятків мільйонів відбитків пальців. Вона охоплює тих, хто пройшов реєстрацію за службовим обов'язком, – військовослужбовців, співробітників МВС і МНС, різних служб безпеки. Крім того, в Російській Федерації існувала велика база відбитків пальців злочинців.

Загалом у РФ з 2002 року створювалася багаторівнева система автоматизованих дактилоскопічних обліків органів внутрішніх справ, яка охоплювала федеральний рівень, рівень федеральних округів (міжрегіональні АДІС) і регіональний рівень. 2006 року завершилося створення федеральної АДІС ГІАЦ (головного інформаційного автоматизованого центру) МВС Російської Федерації, обсяг бази даних якої перевищив 32 млн дактокарт. Наприкінці 2013 року перевірка одного сліду у всьому масиві мала здійснюватися за декілька хвилин[3].

Дактилоскопічні бази даних збирають й інші відомства. Наприклад, Федеральна служба виконання покарань (російська абревіатура – ФСИН) створює генетичну базу всіх ув'язнених на теренах Росії. Цією базою зможуть користуватися всі російські силовики, але насамперед оперативники карного розшуку МВС.

Із проектом створення єдиної автоматизованої дактилоскопічної бази також виступила Федеральна міграційна служба (ФМС) – відомство запланувало зібрати відбитки пальців у всіх московських мігрантів і звести їх у єдину автоматизовану дактилоскопічну базу, а з часом до неї будуть включені дані всіх мігрантів на території РФ[4].

---

[1] МВД создаст всероссийскую дактилоскопическую базу данных // Известия. – 2013. – 5 августа. [Электронный ресурс]. – Режим доступа: http://izvestia.ru/news/...

[2] Современное состояние и перспективы развития дактилоскопических учетов. [Электронный ресурс]. – Режим доступа: http://ua.coolreferat.com...

[3] Перов С. Таких массивов и такой системы сбора дактоинформации нет ни в одной стране мира / Сергей Перов. – 2007. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/gov2007/int/mvd/…

[4] МВД создаст всероссийскую дактилоскопическую базу данных // Известия. – 2013. – 5 августа. [Электронный ресурс]. – Режим доступа: http://izvestia.ru/news/...

Автоматизована дактилоскопічна ідентифікаційна система (АДІС) ФМС, згідно з конкурсною документацією, повинна бути створена не пізніше 5 грудня 2012 року. Водночас АДІС ФМС мала бути сумісна з АДІС МВС РФ[1].

У ком'ютерній базі даних Федеральної міграційної служби РФ станом на грудень 2013 року вже зберігалася інформація у вигляді досьє на 126 млн іноземців, які перетнули кордон Росії за останні роки. Із них більше 16 млн перетнули кордон Росії у 2013 році. База даних дозволяє вирахувати, яка кількість іноземних громадян перебуває не тільки у кожному суб'єкті федерації, але навіть у кожному окремому муніципальному районі Москви.

2013 року майже 300 тис іноземців, які порушили російське законодавство, за рішеннями судів були вислані за межі Російської Федерації на підставі інформації, наданої ФМС[2].

Загалом у 2013 році на територію Росії заборонено в'їзд 427 тис іноземців, зокрема 25 тис українців. Заборона на в'їзд іноземцям видається незалежно від громадянства за допомогою автоматизованої системи міграційного обліку[3].

Окрім вищезазначених відомств, користувачами «Системи Папілон» у Росії також є підрозділи інших силових структур: Федеральної служби за контролем обороту наркотиків, Міністерства оборони, Федеральної служби безпеки та ін.

Розробником АДІС «Папілон» є російське підприємство «Системи Папілон» (*Росія, 456320, Міас, Челябінська обл., просп. Макєєва, б. 48, адреса сайту: www.papillon.ru*), яке виготовляє електронно-оптичні сканери для зняття відбитків пальців і програмне забезпечення для їх зберігання та порівняння. Підприємство «Системи Папілон» є одним із відомих розробників системи ідентифікації за відбитками пальців і системи електронного дактилоскопіювання в СНД.

Біометричні модулі підприємства «Системи Папілон» можуть бути застосовані до будь-яких систем безпеки, де важлива надійна ідентифікація особи та контроль за її переміщенням. Системи працюють і з одним параметром (відбиток/ки/ пальця/ів/ або райдужна оболонка ока), і з їх комбінацією. Підприємство «Системи Папілон» поставляє як завершені системи з готовим рішенням для біометричних документів, так і SDK-продукти. Основні замовники – силові структури Росії та інші зарубіжні країни.

Ідентифікаційні системи російської компанії працюють із базами даних до сотень мільйонів відбитків. Одна з розробок використовувала суперкомп'ютер, який входив у трійку найліпших, які були встановлені на території СНД. Основні розробки та технічні рішення підприємства захищені патентами. Всі розроблені програмні і технічні рішення відповідають міжнародним стандартам ISO[4].

Розглянемо можливості автоматизованої дактилоскопічної ідентифікаційної системи (АДІС) «Папілон». Вона призначена для автоматизації оперативно-довідкових і оперативно-розшукових дактилоскопічних обліків ОВС. Сферою застосування системи

---

[1] ФМС объявила конкурс на создание системы дактилоскопического учета мигрантов. – 2013. – 23 августа. [Электронный ресурс]. – Режим доступа: http://top.rbc.ru/spb_sz/23/08/2012/665955.shtml…

[2] Как функционирует информационно-аналитическая система Федеральной миграционной службы. – 2013. – 7 декабря // Агентство ООН по делам беженцев, Российская Федерация (УВБК ООН). [Электронный ресурс]. – Режим доступа: http://unhcr.ru/index.php...

[3] ФМС России отказала во въезде 25 тысячам украинцев // УНИАН. – 2013. – 17 декабря. [Электронный ресурс]. – Режим доступа: http://vz.ru/news/...

[4] Биометрические модули предприятия «Системы Папилон» // Exponet.ru. – 2006. [Электронный ресурс]. – Режим доступа: http://www.exponet.ru/exhibitions/online/safetymo2006/sistemyI.ru.html…

«Папілон» є автоматизація обробки дактилоскопічної інформації і на місцевому (районному, міському), і на централізованому (обласному, регіональному /республіканському/ і державному) рівнях.

Застосування АДІС забезпечує виконання таких завдань:

– зменшення трудовитрат і часу та підвищення ефективності розкриття і розслідування злочинів завдяки більш точній та своєчасній інформації, яка надається оперативним службам;

– можливість встановлення особистості як живих осіб, так і невпізнанних трупів за відбитками пальців рук або за невеликим фрагментом тільки одного відбитка (навіть у разі значних змін);

– автоматичну перевірку дактилоскопічної інформації за базою даних АДІС при постановці на дактилоскопічний облік і під час виконання оперативних запитів;

– пришвидшення обробки дактилоскопічної інформації при постановці на облік і суттєве зменшення часу відповіді на запити;

– підвищення результативності дактилоскопічних обліків;

– поліпшення якості дактилоскопічної інформації, яка надходить завдяки запровадженню оптоелектронних пристроїв безфарбового дактилоскопіювання – так званих «живих» сканерів;

– можливість об’єднання обліків у єдину державну автоматизовану систему;

– реалізація міжрегіональної взаємодії автоматизованих дактилоскопічних обліків.

АДІС «Папілон» із високою точністю і надійністю ідентифікує у базі даних сліди пальців і долонь, які виявлені на місцях злочинів; невпізнанні трупи; встановлює особу затриманого.

Вона сформована як модульна система, яка дозволяє поетапно збільшувати як обсяг бази даних (від 10–20 тис. до 150 млн дактилокарт), так і пропускну спроможність. «Папілон» повністю задовольняє технічні вимоги МВС РФ, підтримує стандарти ФБР, ANSI та NIST.

Можливості автоматизованої дактилоскопічної інформаційної системи «Папілон»:

– введення і зберігання в базі даних (БД) дактилокарт, фотозображень осіб і їх особливих прикмет, словесного опису індивідуумів;

– введення і зберігання в БД слідів пальців рук і долонь, вилучених із місць злочинів;

– проведення автоматичних пошуків типів «карта-карта», «карта-слід», «слід-карта», «слід-слід»;

– пошук за словесним описом;

– здійснення пошуку та ідентифікація слідів пальців і відбитків долонь;

– автоматизоване виведення дактилоформул;

– автоматизований дактилооблік: проведення різноманітних вибірок, сортування списків БД, видалення і редагування записів тощо;

– виведення графічних зображень (дактилокарт, фотозображень, слідів із місць злочинів) на монітор і на принтер, друк документів, списків, довідок, статистичної інформації;

– віддалене введення дактилоскопічної інформації, віддалений доступ до Центральної БД, формування розподільчих систем;

– багаторівневе розмежування доступу та закриття інформації, яка передається за каналами зв’язку і зберігається у базі даних;

– взаємодія з іншими видами автоматизованих обліків;

– імпорт/експорт дактилокарт і слідів у форматах Інтерполу, ФБР, МВС Росії.

В інформаційній системі «Папілон» максимально автоматизовані всі технологічні процеси обробки дактилоскопічної інформації. Доволі високі характеристики надійності

та вибірковості системи забезпечують мінімальні розміри рекомендаційних списків, що видаються. Тому навіть дуже великі БД обслуговуються невеликим штатом співробітників. Користувачі відзначають «дружність» інтерфейсу всіх програмних модулів і простоту експлуатації системи[1].

Для нормального доступу до центральних обліків необхідні канали доступу. Тому з 2005 року почалася реалізація Програми МВС Росії «Створення єдиної інформаційно-телекомунікаційної системи органів внутрішніх справ» (ЄІТКС), яка була розрахована на 2005–2008 роки.

В рамках реалізації однієї з її підпрограм «Реконструкція і технічне переозброєння інформаційних центрів МВС, ГУВС, УВС суб'єктів Російської Федерації, УВСТ» в 2005–2006 роках повністю оснащені типовими програмно-технічними комплексами (ПТК) «ІБД-Регіон» 82 регіональних інформаційних центрів, які забезпечують автоматизоване формування та використання оперативно-довідкових, розшукових і криміналістичних обліків.

У 2007–2009 роках практично завершилось створення єдиної інформаційної вертикалі ГІАЦ-ІЦ (інформаційний центр) МВС, ГУВС, УВС за суб'єктами Російської Федерації, які групують і об'єднують усі криміналістичні, статистичні та оперативно-довідкові обліки ОВС, забезпечивши доступ і обмін даними між ними за допомогою сучасної корпоративно-інформаційної інфраструктури. Проведені заходи сприяли об'єднанню всіх наявних у МВС Росії інформаційних потоків, що надало можливість максимально забезпечити необхідною інформацією (оперативною, криміналістичною, довідковою та ін.) всіх співробітників органів внутрішніх справ, які забезпечують виконання завдань із боротьби зі злочинністю, охорони громадського порядку, профілактики правопорушень тощо.

На базі ГІАЦ МВС Росії створена міжвідомча автоматизована інформаційна система ведення Регістра Федерального інтегрованого інформаційного фонду (РІФ). Одинадцять міністерств і відомств створили на базі МВС центральний масив посилально-відсилальної інформації, яка необхідна для роботи правоохоронних, контрольно-наглядових і фінансових органів Російської Федерації. 2007 року обсяг Регістра становив приблизно 19 млн одиниць інформації. Вирішується питання про приєднання до автоматизованої інформаційної системи РІФ ще низки міністерств і відомств[2].

1992 року в м. Чолпон-Ате (Казахстан) було ухвалене рішення про створення Міждержавного інформаційного банку (МІБ). Загалом у вересні 2013 року загальний обсяг даних МІБ становив понад 77,5 млн об'єктів обліку, з яких 59 млн поставило на облік МВС Росії, 6,5 млн – МВС України.

2012 року за дактилоскопічними обліками МІБ було перевірено 14222 запитів, які надійшли з МВС України. Внаслідок було підтверджено особистості 3110 громадян і встановлено особистості 891 невпізнаних трупів. У першому півріччі 2013 року відповідні показники становили: 133 запити, підтвердження особистості 9 громадян і розпізнання 8 невпізнаних трупів.

У грудні 2012 року за запитом МВС України з використанням можливостей федеральної автоматизованої дактилоскопічної інформаційної системи «АДІС-МВС»

---

[1] Автоматизированная дактилоскопическая информационно-поисковая система по отпечаткам и следам пальцев и ладоней рук «АДИС». [Электронный ресурс]. – Режим доступа: http://www.papillon.ru/adis.php...

[2] Перов Сергей. Таких массивов и такой системы сбора дактоинформации нет ни в одной стране мира / Сергей Перов. – 2007. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/gov2007/int/mvd/…

виконана перевірка 5957 файлів, які містили дактилоскопічні карти невпізнаних трупів, які були виявлені на теренах України. В результаті було встановлено особи 862 невпізнаних трупів.

2013 року під час перевірки за українською базою відомостей «Дакто-2000» 12 тисяч дактилоскопічних карт осіб, оголошених у розшук російською стороною, встановлена (підтверджена) особистість 34 обвинувачених, які розшукувались російською стороною, з яких 8 перебували у міждержавному розшуку, а також ідентифіковано 70 невпізнаних трупів[1].

Розглянемо ситуацію з автоматизацією дактилоскопічних обліків у Білорусі. Датою взяття на республіканський білоруський новий облік першої дактилокарти є 1945 рік. Відомості, які надходили зі всієї республіки, збиралися спочатку в регіональні та республіканську дактокартотеки, а у 1998 році було ухвалено рішення про створення електронної автоматизованої дактилоскопічної бази даних, яка знаходиться у Державному експертно-криміналістичному центрі МВС Білорусі.

Програмно-математичне забезпечення для електронної системи було розроблене білоруськими вченими.

2000 року вперше запрацювала відома тепер кожному білоруському оперативному співробітникові й експерту АДІС «Дакто-2000». Спочатку в електронній дактилоскопічній системі були відбитки пальців і рук тільки раніше судимих осіб. Згодом база даних почала поповнюватись відбитками громадян інших категорій.

21 квітня 2010 року в Білорусі набрав чинності закон про обов'язкове дактилоскопіювання всіх військовозобов'язаних громадян. Унаслідок було розкрито значну кількість злочинів, зокрема й резонансних[2].

В Україні поки що не створена у повному обсязі єдина багаторівнева система автоматизованих дактилоскопічних обліків органів внутрішніх справ, яка б охоплювала районний, регіональний і державний рівні, тобто була аналогічна єдиній російській загальнодержавній дактилоскопічній базі даних, яка повинна була розпочати свою діяльність на теренах Росії з 1 жовтня 2013 року.

Є відомості про функціонування АДІС «Дакто-2000» в окремих експертно-криміналістичних центрах при УМВС (ГУМВС) і у МВС України[3].

В Україні технології біометричної ідентифікації стають дедалі більш затребуваними великою кількістю замовників серед державних і комерційних структур.

Що стосується функціонування сучасних автоматизованих дактилоскопічних інформаційних систем (AFIS) або IAFIS (Integrated Automated Fingerprint Identification System) у провідних західних країнах світу, то слід зазначити, що в спецслужбах цих держав уже діють мультибіометричні інтегровані системи автоматичної ідентифікації за декількома біометричними показниками. Тобто автоматизовані суто дактилоскопічні

[1] Про оголошення рішень спільного засідання колегій міністерств внутрішніх справ України і Російської Федерації: додаток № 2 до Наказу МВС Росії від 26.09.2013 року № 757. [Електронний ресурс]. – Режим доступу: http://mvd.ru/upload/site1/marina...

[2] Ядченко Василий. Дактилоскопия 110 лет на вооружении у правоохранителей / Василий Ядченко // Сайт Министерства внутренних дел Беларуси. – 2012. – 10 мая. [Электронный ресурс]. – Режим доступа: http://mvd.gov.by/main.aspx...

[3] Експерти-криміналісти транспортної міліції провели день відкритих дверей для майбутніх міліціонерів. – 2013. – 21 лютого // УМВС України на Південній залізниці. [Электронний ресурс]. – Режим доступу: http://mvs.gov.ua/mvs/control/pz/ru/publish/...; Про оголошення рішень спільного засідання колегій міністерств внутрішніх справ України і Російської Федерації: додаток № 2 до Наказу МВС Росії від 26.09.2013 року № 757. [Електронний ресурс]. – Режим доступу: http://mvd.ru/upload/site1/marina/...

ідентифікаційні системи стали складовою мультибіометричних інтегрованих систем автоматичної системи ідентифікації за біометричними показниками. Так, ще наприкінці першого десятиріччя XXI століття з'явилася інформація, що американське Федеральне бюро розслідувань (ФБР) створює одну з найбільших у світі базу біометричних даних, що отримала назву Next Generation Identification (NGI), яка повинна значно розширити можливості біометричної системи Integrated Automated Fingerprint Identification System (IAFIS), котра експлуатувалася у ФБР. За інформацією ЗМІ у банку даних IAFIS на час появи інформації про початок робіт зі створення NGI містилося 55 млн електронних зразків відбитків пальців.

У проекті, підготовленому ФБР для представлення в Міністерство юстиції США, зазначено, що NGI надаватиме відомості й для авторизованих цивільних структур. Сама система буде функціонувати впродовж року цілодобово без вихідних і перерв на профілактику, як є під час експлуатації IAFIS.

Статистика арештів у США свідчить, що 2005 року дактилоскопічні відомості використовувалися для ідентифікації особи порушників закону в 46% випадках. До кінця 2008 року ця цифра мала становити 55%. А точність проведених ідентифікацій до 2010 року планувалось підвищити приблизно до 100%[1].

У Сполучених Штатах Америки 70% злочинів розкриваються завдяки комп'ютеризованим системам[2].

Загалом, щоб мати уявлення про масштаби функціонування електронних обліків у провідних західних країнах наприкінці XX сторіччя, наведемо такі відомості.

У США система електронних обліків даних про населення практично була всеохоплюючою. Національний центр інформації, що належить ФБР, налічував на комп'ютерному обліку електронних досьє на понад 160 млн громадян США. Використання інформації й право на неї регламентовані законодавчо.

У Великобританії є мережа урядових баз даних про населення Сполученого Королівства, що пов'язує автоматизовані системи Національного обчислювального центру поліції, військові, фінансові, паспортні та митні обліки країни. Ще у 1980–1987 роках у Великобританії були розроблені й введені в дію закон про захист даних і урядова програма автоматизації обліків даних про населення.

У Німеччині в комп'ютерах поліцейських органів і спецслужб зберігаються електронні досьє на понад 10 млн німців. Робота з інформацією та контроль над діючими автоматизованими системами строго регламентовані законом.

До цього переліку також належить Австрія, Бельгія, Іспанія, Франція й інші розвинені країни[3].

Методи застосування біометричних, зокрема й дактилоскопічних, обліків постійно удосконалюються. Дуже цікавим є повідомлення з Великобританії про те, що підрозділ британської поліції, який обслуговує метрополітени (Uk's Metropolitan Police Service /MPS/), влітку 2012 року приєднано до нової системи доступу до біометричних баз даних, котра за допомогою мобільних технологій дозволяє швидко встановлювати особистість громадян, які зацікавили правоохоронні органи. Російський біометричний портал

[1] Блинкова О. Идентификация Борна / О. Блинкова. – 2008. – 31 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрические технологии повысят эффективность работы азербайджанской полиции // Vesti.Az. – 2012. – 9 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] АДИС против преступности. – 2002. – 11 февраля. [Электронный ресурс]. – Режим доступа: http://www.km.ru/v-rossii/2002/02/11/sotsialnye-problemy-v-rossii/...

BIOMETRICS.RU повідомив, що MPS стало 25-м поліцейським підрозділом Сполученого Королівства, яке приєднано до нової системи.

Ця інновація створена завдяки діяльності Національного агентства з поліпшення діяльності поліції (National Policing Improvement Agency /NPIA/). Дія системи заснована на технологіях ідентифікації за відбитками пальців: поліцейський за допомогою мобільного пристрою сканує ці біометричні ідентифікатори в особи, яка його зацікавила, а отримана інформація передається в NPIA, де порівняється з даними загальнонаціональної бази відбитків пальців індивідуумів, які зацікавили поліцію. Якщо порівняння дало позитивні результати, то затриманого перепроваджують у відділення поліції для подальшого проведення потрібних дій, в іншому випадку його відпускають, а відомості про відсканові відбитки пальців знищуються у пам'яті мобільного пристрою та видаляються з системи біометричної ідентифікації.

Головною перевагою інновації є істотне зменшення часу для встановлення особистості людини, яка зацікавила поліцейського. Якщо раніше на таку процедуру затрачали майже годину, то зараз вона триває не більше двох хвилин.

Відповідно, «боббі», які патрулюють метрополітен, не потрібно відвідувати свої відділення: перевірити отримані біометричні показники за центральною базою даних вони можуть відразу на місті затримання підозрілої особи.

Це означає, що поліцейські зможуть набагато ефективніше займатися своєю безпосередньою діяльністю, забезпечуючи безпеку такого важливого і вразливого транспортного об'єкта, як метрополітен[1].

[1] Биометрические технологии повысят безопасность лондонского метро // BIOMETRICS.RU. – 2012. – 1 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розділ 3

ІДЕНТИФІКАЦІЯ ЗА ДОПОМОГОЮ РАЙДУЖНОЇ ОБОЛОНКИ ТА СІТКІВКИ ОКА

Навколо чорної зіниці ока людини розташоване кільце – *райдужна оболонка*, яка визначає колір ока і містить певний візерунок, унікальний для будь-якої людини і для кожного ока. Райдужну оболонку ока (далі райдужка) видно без збільшувальних оптичних пристроїв. За різних умов освітленості, коли зіниця змінює свої розміри (збільшується в темряві та зменшується при яскравому світлі), можна побачити більшу або меншу частину райдужки, причому розмір частини райдужної оболонки залежить від того, як широко розплющене око[1].

Райдужна оболонка ока має дуже складний малюнок, який відрізняється навіть в однояйцевих близнят, причому малюнок райдужки формується у віці від шести місяців до двох років і залишається незмінним упродовж усього життя, а сама райдужка практично несхильна до поранень і забруднення. Необхідно акцентувати, що райдужки правого і лівого ока мають різні малюнки, які суттєво відрізняються. Ідентифікація за райдужною оболонкою ока є однієї з найточніших з усіх біометричних ідентифікаційних технологій (деякі експерти навіть прирівнюють їх до ДНК-технологій), причому малюнок райдужки практично неможливо підробити. Коефіцієнт помилкової ідентифікації є дуже низьким і практично дорівнює нулеві. Технології ідентифікації за райдужною оболонкою застосовуються впродовж багатьох років і на практиці засвідчили свою надійність і точність, причому успішно були апробовані на різних етнічних групах і національностях[2].

Обмеження для їх ширшого використання в основному пов'язані з вартістю обладнання[3].

Отже, ідентифікація за допомогою райдужки є унікальною характеристикою і заснована на аналізі кольорової райдужної оболонки ока, яка оточує зіницю. Малюнки райдужних оболонок стають доступними для процесу ідентифікації за допомогою відеосистем. Однією з переваг цієї ідентифікаційної системи є відсутність необхідності особистого контакту зі сканером. Для сканування цілком достатньо портативної відеокамери та комп'ютера з спеціалізованим програмним забезпеченням. Відеозображення ока отримується з відстані 1–1,5 м, що дозволяє застосовувати ці пристрої у банкоматах[4].

---

[1] Биометрики глаза: различия радужной оболочки и сетчатки. [Электронный ресурс]. – Режим доступа: http://www.npo-inform.com/biomert/analitika/glaz/...

[2] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art103.html

[3] Еще одна новая система биометрической идентификации по радужной оболочке глаз // Security News (http://www.secnews.ru). – 2007. – 14 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Биометрия тотальный контроль (отпечаток пальца). – 2003. – 16 сентября. [Электронный ресурс]. – Режим доступа: http://www.cherry.ru/interes/90.html...

Отже, раніше для сканування райдужки треба було стояти дуже близько до камери. Але нові технології та відповідне обладнання дозволяють здійснити ідентифікацію на відстані та навіть під час руху. Система «Iris on the Move» компанії «SRI International» фіксує райдужку із трьох метрів і здатна обробити райдужки 30 людей за хвилину. Коштує обладнання 75 тис доларів[1].

Практичне широкомасштабне застосування технології ідентифікації «розпізнавання на відстані» було здійснено 2011 року в аеропорту Гатвік, який обслуговує столицю Великобританії. Технологія «розпізнавання на відстані» дозволяє пасажиру не завмирати перед сканером райдужної оболонки ока на строго фіксованій відстані та чекати поки пройде ідентифікація: він просто продовжує рухатися, а сканер автоматично обробляє інформацію про його біометричні ідентифікатори, і якихось додаткових зусиль з боку особи, яку ідентифікують, не потрібно.

У такий спосіб вдалося виконати відразу два завдання. З одного боку, система біометричної ідентифікації надзвичайно чутливо реагує на будь-які помилкові пересування авіапасажира, який через неуважність або ж свідомо намагається пройти на посадку не на свій рейс. З іншого боку, заходи контролю не призводять до додаткових витрат часу та сил з боку пасажирів і відтак не передбачається ймовірність виникнення довгих черг[2].

Скануючі пристрої практично є телекамерами високої якості, що спричиняє деякі незручності під час їх використання, які пов’язані з самою процедурою сканування. 2001 року через великі габарити телекамер того часу та їх вартість рівень застосування цієї біометричної технології становив майже 5%[3].

У 2009 році на райдужку припадає вже 8%, а у 2017 за прогнозами експертів на цю технологію буде припадати 19% світового ринку (сукупний виторг учасників ринку в 2017 році може становити 10,9 млрд доларів)[4].

Розвиток електронних технологій дозволив істотно зменшити розміри камер сканування і загалом знизити вартість систем, заснованих на цьому методі ідентифікації.

Нині використовуються системи з часом ідентифікації райдужки 0,3 с, що оптимально підходить для ідентифікації пасажирів у аеропортах і для контролю за доступом на підприємства та установи в різних сферах людської діяльності. Останні розробки ідентифікаційних систем на основі технології райдужної оболонки ока мають високий коефіцієнт безпеки з можливістю помилкової ідентифікації 1 з 1,2 мільйонів завдяки використанню індивідуальних відмінностей складних малюнків райдужки людини[5].

Для отримання чіткого знімку райдужної оболонки ока необхідно, щоб око потрапило в кадр камери – людині потрібно зайняти певну позицію (зпозиціонуватися) перед камерою або за неї цю процедуру виконає автоматика.

---

[1] Обретут ли второе дыхание технологии идентификации по радужной оболочке глаз? // Компьюлента. – 2011. – 7 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Новая биометрическая система внедрена в лондонском аэропорту // BIOMETRICS.RU. – 2011. – 12 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Мифы биометрии. [Электронный ресурс]. – Режим доступа: http://www.cbio.ru/v5/modules/news/article.php…

[4] Обретут ли второе дыхание технологии идентификации по радужной оболочке глаз? // Компьюлента. – 2011. – 7 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[5] Еще одна новая система биометрической идентификации по радужной оболочке глаз // Security News (http://www.secnews.ru). – 2007. – 14 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Зазвичай розрізняють активні та пасивні системи розпізнавання. У системах першого типу користувач повинен сам налаштувати камеру, пересуваючи її для більш точного наведення.

Пасивні системи простіші у використанні, оскільки камери в них налаштовуються автоматично. Апаратура для цих систем розпізнавання характеризуються дуже високою надійністю. Перевага сканерів для райдужної оболонки ока, які створені на базі цифрових камер, полягає в тому, що вони не вимагають чіткого зосередження користувача на якомусь об'єкті, тому що взірцеві зразки плям на райдужці є безпосередньо на поверхні ока[1].

Вихідне зображення райдужної оболонки ока може бути збережене в пам'яті комп'ютера в будь-якому графічному форматі, а надалі програма розпізнавання може перетворити його у свій внутрішній формат, тобто отримане зображення райдужки перетворюється в комп'ютерний код і надалі порівнюється з наявними даними в базі.

Тривалий час спосіб зйомки, формат збереження оброблених даних зображення райдужної оболонки ока й основних методів розпізнавання перебували під захистом міжнародних патентів, що сильно обмежувало їхній розвиток і застосування.

Першим технології райдужної оболонки ока запропонував у 1936 році Френк Берч, офтальмолог із Сент-Пола (штат Міннесота, США), який вказав на те, що борозни, рубчики, кільця та точечки райдужної оболонки ока у кожної людини мають свій унікальний і неповторний малюнок. Але тільки в 1987 році двоє інших докторів, Леонард Флом і Аран Сафір, одержали патент на нову концепцію технології ідентифікації.

Леонард Флом і Джон Даугман із Кембриджського університету (Великобританія) розробили метод автоматичної ідентифікації за райдужкою, який Д. Даугман запатентував у 1994 році. Перші комерційні продукти стали доступні через рік.

Термін дії патенту, який стосувався основної концепції, завершився в 2005 році, що дозволило багатьом компаніям почати розробку власних технологій. 2011 року завершилася дія патенту 1994 року[2].

Основним недоліком технології розпізнання за райдужною оболонкою ока є можливість застосування кольорових контактних лінз, що створюють певні труднощі під час використання цього методу розпізнавання, а контактні лінзи з нанесеним на них візерунком радужки іншої людини здатні обдурити біометричну систему[3].

Розпізнавання користувачів досить суттєво залежить від зовнішніх умов та насамперед від освітленості: зміна освітленості призводить до того, що значно змінюється розмір самої зіниці, а це, своєю чергою, ускладнює процедуру розпізнавання.

Зміни розмірів зіниць під впливом освітлення досить значні й можуть коливатися в діапазоні від 0,8 до 8 мм.

Для вирішення цієї проблеми низка фахівців пропонують ідентифікувати користувачів за рухами зіниць, які виникають під час змін їх розмірів. Так, Семмі Фанг (Sammy Phang), співробітниця технологічного університету Квінсленда (м. Брісбен, Австралія), запропонувала нову технологію ідентифікації райдужної оболонки очей, яка заснована на зміні розміру зіниць.

---

[1] Борзенко А. Биометрические технологии / А. Борзенко // Bytemag.ru. – 2001. – 10 октября. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

[2] Обретут ли второе дыхание технологии идентификации по радужной оболочке глаз? // Компьюлента. – 2011. – 7 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Биометрики глаза: различия радужной оболочки и сетчатки. [Электронный ресурс]. – Режим доступа: http://www.npo-inform.com/biomert/analitika/glaz/...

Унікальність рухливості зіниці під впливом зміни освітлення була підтверджена під час тестів, які провела С. Фанг, і вона впевнена, що нова технологія розпізнавання допоможе істотно підвищити продуктивність і ефективність роботи біометричних систем, які ідентифікують користувачів за райдужкою. Недоліком цього підвиду методу ідентифікації за райдужною оболонкою очей є необхідність застосування високошвидкісних камер-сканерів, які повинні мати можливість фіксувати до 1200 кадрів за секунду[1].

Метод ідентифікації за райдужною оболонкою ока має один із найбільш високих ступенів надійності, проте відповідні пристрої одержання зображення райдужкою ока поки що мають значно вищу ціну, ніж апаратура для отримання відбитків пальців і зображень обличчя осіб. Факт відсутності двох людей з однаковою райдужною оболонкою ока був доведений ученими ще декілька десятиліть тому, як і факт, що навіть у однієї людини райдужні оболонки очей відрізняються одна від однієї, проте необхідне програмне забезпечення, здатне автоматично здійснювати пошук і встановлювати відповідність зразків-шаблонів і отриманого під час проходження контролю зображення, з'явилося лише наприкінці XX століття. Тому в кінці минулого століття системи розпізнавання райдужної оболонки в основному лише забезпечували авторизований доступ до закритих зон, які охоронялися. Технологія допуску, що заснована на скануванні райдужки ока, з кінця минулого сторіччя успішно застосовується в державних установах США, у в'язницях, в організаціях із високим ступенем секретності (зокрема на заводах із виробництва ядерного озброєння), в закритих інформаційних центрах. Розробками технологій ідентифікації особистості на основі принципу сканування райдужної оболонки ока займалось понад 20 компаній[2]. Але після 2011 року (завершення терміну дії патенту Даугмана) їх кількість повинна суттєво збільшитись.

Нині технологія розпізнавання за райдужкою ока використовується у багатьох аеропортах у всьому світі для забезпечення виконання таких завдань, як контроль під час перетинання державних кордонів, забезпечення обмеження доступу, а також для поліпшення сервісного обслуговування авіапасажирів. У Великобританії система «Iris» у 2005 році проходила тестування на державному рівні, райдужна оболонка ока, по суті, є своєрідним «паспортом» під час в'їзду до Канади, Нідерландів і Об'єднаних Арабських Еміратів, де підтвердження особистості під час проходження прикордонного та митного контролю здійснюється за допомогою технології розпізнавання райдужної оболонки ока.

Ця ж технологія починає широко використовуватися і в галузі охорони здоров'я. Системи, що засновані на розпізнаванні райдужки ока, за допомогою яких обмежують доступ до історій хвороб у шпиталях та інших медичних закладах, успішно працюють у таких штатах США, як Вашингтон, Колумбія, Пенсільванія, Алабама, Північна Кароліна та ін.

У Федеральній республіці Німеччина пологові будинки обладнані системами доступу на базі технологій розпізнавання райдужної оболонки ока, завдяки чому доступ у блок до новонароджених мають тільки батьки, лікарі та медсестри.

Окрім державних і приватних систем контролю доступу, які забезпечують виконання особливо жорстких вимог щодо безпеки доступу, метод ідентифікації за райдужкою ока ширше застосовується в галузі охорони електронної інформації[3].

---

[1] Новая технология идентификации по радужной оболочке глаз // BIOMETRICS.RU. – 2007. – 12 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрические системы безопасности // БДИ. – 2002. – № 1 (41). [Электронный ресурс]. – Режим доступа: http://www.iching.ru/6/Bezopasnost-9.html...

[3] Распознавание радужной оболочки глаза на службе безопасности // UNISXCAN. – 2005. – 19 сентября. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art502.html...

Планувалось, що однією з головних особливостей нового смартфона «Samsung Galaxy S5» мав стати сканер райдужної оболонки ока (в оригіналі статті вказана сітківка ока, але це малоймовірно). Але з низки причин у моделі «Samsung Galaxy S5», продаж якої розпочався з квітня 2014 року, був застосований сканер для контролю за відбитками пальців. Поява нової версії смартфона зі сканером райдужної оболонки ока з різних причин відкладена на майбутнє.

Використання технологій ідентифікації за райдужною оболонкою ока регулюється міжнародним стандартом ІСО/МЕК 19794-6:2005 «Інформаційні технології. Формати обміну біометричними даними. Частина 6: Дані зображення райдужної оболонки ока» (ISO/IEC 19794-6:2005 «Information technology – Biometric data interchange formats – Part 6: Iris image data»).

Вказаний стандарт входить до комплексу стандартів «Ідентифікація біометрична» і його рекомендовано використовувати разом з іншими стандартами цього комплексу. Стандарт встановлює формати обміну біометричними даними зображення райдужної оболонки ока і призначений для обміну їх зображеннями у цифровому вигляді[1].

Відповідно до прес-релізу агентства «Frost & Sullivan», який був опублікований улітку 2008 року, технологія ідентифікації за райдужною оболонкою ока посідає проміжне місце серед технологій ідентифікації за відбитками пальців і за тривимірною моделлю черепа[2].

У майбутньому має розширитися застосування технологій, які засновані на методі ідентифікації за райдужкою очей, а саме: в системах прикордонного контролю, у тих програмах, що реалізовуються урядовими органами для ідентифікації населення, у фінансовій сфері (в банкоматах), а також у системах контролю фізичного доступу (переважно на підприємствах енергетичного, хімічного, оборонного комплексів і в установах особливо таємних структур). За оцінками деяких фахівців реалізація розглянутих перспектив розвитку ринку засобів ідентифікації за райдужною оболонкою ока пов'язано з виконанням двох умов. По-перше, повинна радикально підвищитися якість розпізнавання райдужки ока, незалежно від умов. По-друге, ці засоби повинні стати більш зручними та забезпечувати користувачеві максимально можливий комфорт, не вимагаючи від нього жодних додаткових зусиль для проходження процедури розпізнавання[3].

За повідомленням одного з керівників корпорації «Northrop Grumman» Брюса Уокера (Bruce Walker) в його компанії розроблено технологію біометричного розпізнання, яка дозволяє сканувати райдужку ока на відстані до п'яти метрів. А через специфіку завдань, що ставляться перед технологіями безпеки, серед найважливіших чинників під час порівняльної оцінки різних методів ідентифікації неодмінно є відстань, за якою можливе проведення ідентифікації, а також загалом відносна складність можливості підробки людиною свого біометричного параметра[4].

---

[1] С 1 июля 2007 года вводится в действие ГОСТ. Р ИСО/МЭК 19794-6-2006 «Автоматическая идентификация. Идентификация биометрическая. Форматы обмена биометрическими данными. Часть 6. Данные изображения радужной оболочки глаза» // Cntd.ru. – 2007. – 9 апреля. [Электронный ресурс]. – Режим доступа: http://www.cntd.ru/ manage/page…

[2] Новые перспективы биометрии в пограничном контроле // BIOMETRICS.RU. – 2008. – 4 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Идентификации по радужной оболочке глаз пророчат светлое будущее // BIOMETRICS.RU. – 2007. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Берд Киви. Лица, подлежащие опознанию / Киви Берд // Компьютерра. – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Нині мобільний і дистанційний аспекти розпізнавання осіб за допомогою біометрії становлять значний інтерес для багатьох сфер застосування біометрії, але найбільше у цьому зацікавлені силові структури. У Сполучених Штатах Америки фірма «Retica Systems» (штат Массачусетс) отримала від одного з інвестиційних фондів 5,4 млн доларів США на розробку нової системи дистанційної ідентифікації за райдужною оболонкою очей, яка отримала назву «Орлине око». За відомостями джерел «BizJournals», для ідентифікації використовується переносний пристрій, який зовні нагадує бінокль і здатний розпізнавати людину з відстані в декілька метрів, водночас порівнюється малюнок райдужної оболонки очей з електронними шаблонами, що зберігаються в базі даних. За повідомленням старшого консультанта Міжнародної біометричної групи Віктора Лі, аналогічні засоби мобільної ідентифікації вже використовуються на контрольно-пропускних пунктах військових баз, на пунктах прикордонного контролю та на вулицях Лос-Анджелеса. За його словами: «Дистанційна ідентифікація за райдужною оболонкою очей – це та головна мета, яку намагаються досягти багато компаній і, якщо «Retica» змогла змусити «Орлине око» запрацювати, то це буде величезним досягненням».

За повідомленням голови компанії «Retica Systems» Девіда Мюллера, поставки «Орлиного ока» військовим повинні були розпочатися з кінця 2007 року. Вартість кожного мобільного пристрою, яке здатне ідентифікувати людину за райдужкою очей із відстані до 20 метрів, орієнтовно оцінювали в п’ять тисяч доларів США[1].

Але у впровадженні «розпізнавання на відстані» були невдачі. У березні 2009 року надійшла звістка, що Міністерство внутрішніх справ Об’єднаних Арабських Еміратів відмовилося використовувати дистанційну ідентифікацію за райдужною оболонкою очей. Ця технологія проходила тестування в міжнародному аеропорту Абу-Дабі, а негативний висновок був зроблений за підсумками експерименту.

На жаль, нова технологія виявилася тоді доволі недосконалою. За словами генерал-майора Ахмеда Насер аль-Раїсі, який займався в поліції Абу-Дабі проектом з її впровадження, ніхто не ставив завдання досягти стовідсоткової точності ідентифікації. МВС Об’єднаних Арабських Еміратів було готове примиритися навіть із показником у 75%, проте і цей рубіж не був досягнутим.

У підсумку програмно-апаратне рішення застосування дистанційної ідентифікації за райдужною оболонкою очей було визнано поки що неприйнятним, з чим погодився навіть сам постачальник необхідних для застосування цієї технології апаратних і програмних засобів. Але поліція ОАЕ вирішила спробувати технологію ідентифікації за райдужною оболонкою очей в русі (Iris-on-the-Move technology). Засоби ЗМІ повідомили, що тестування мало проходити знову в аеропорту Абу-Дабі[2].

Нині одним із найсуттєвіших недоліків, що істотно обмежують можливість використання методу ідентифікації за райдужною оболонкою ока державними структурами, є практична відсутність у багатьох державах реальних банків даних зображень райдужок очей індивідуумів, а саме їх відсутність значною мірою і є причиною того, що переважно використовуються методи ідентифікації за відбитками пальців і обличчям осіб (фейс-контроль). Який же сенс знімати біометричні дані людини, якщо їх нема з чим порівнювати? За повідомленнями ЗМІ, база даних відповідних структур США наприкінці

[1] «Орлиный глаз» будет идентифицировать людей по радужной оболочке // BIOMETRICS.RU. – 2007. – 10 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Технология дистанционной идентификации по радужной оболочке глаз признана ненадежной // BIOMETRICS.RU. – 2009. – 10 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

2004 року містила приблизно 1,2 млрд фотографій та 150 млн відбитків пальців. А кількість зображень райдужної оболонки очей тоді становила всього декілька сотень тисяч[1].

За останніми відомостями Федеральне бюро розслідувань США уважно аналізує останні можливості технологій ідентифікації за райдужною оболонкою очей. До кінця першого півріччя 2015 року ці технології будуть тестуватися в 20 підрозділах ФБР, які діють на рівні окремих штатів й округів. На думку незалежних спостерігачів, відповідне обладнання насамперед будуть встановлювати у виправних установах. За підсумками тестування керівництво ФБР має вирішити питання про доцільність застосування цих біометричних технологій у подальшій діяльності свого відомства[2].

На території СНД розробкою та випуском відповідного устаткування для систем ідентифікації за райдужкою ока займається російське підприємство «Системи Папілон». Система «Циркон», що розроблена цим підприємством, призначена для захисту від несанкціонованого доступу до об'єктів різного виду (приміщень, складів і сховищ, банкоматів, комп'ютерів, комп'ютерних мереж тощо).

У мінімальній конфігурації «Циркон» складається з сканера райдужної оболонки ока та персонального комп'ютера з операційною системою (ОС) Linux, на якому зберігається БД оцифрованих зображень райдужок осіб, які мають право доступу до об'єкта, та здійснюються пошуки і видаються залежно від результатів пошуку необхідні управлінські команди для виконавчих механізмів.

Система «Циркон» легко інтегрується в стандартні мережеві технології. У разі потреби контролю за декількома виконавчими механізмами необхідна кількість сканерів і персональних комп'ютерів може взаємодіяти з єдиним пошуковим сервером за допомогою локальної комп'ютерної мережі[3].

Доктор наук із найстарішого академічного центру Британії – Кембриджського університету – Джон Доман прогнозує пришвидшення процесу поширення біометричної ідентифікації за райдужною оболонкою ока. На його думку, з кінця першого десятиріччя XXI століття в різних країнах світу розпочнеться значне впровадження нових проектів на основі цього типу біометричної ідентифікації, особливо в аеропортах і системах прикордонного контролю в місцях перетину кордону.

Технології біометричної ідентифікації за райдужною оболонкою очей до вересня 2008 року використовувалися в аеропортах Мілана, Токіо і в Схіпхолі (Амстердам, Нідерланди). У Сполученому Королівстві ці технології застосовувались у 10 британських аеропортах. До них учений включає п'ять терміналів лондонського Хітроу, перший термінал аеропорту Бірмінгема, термінали №№ 1 і 2 в аеропорту Манчестера, південний і північний термінали аеропорту Гатвік, який також обслуговує британську столицю. Як підкреслює Д. Доман, біометрія дозволяє не тільки пришвидшити обслуговування авіапасажирів, але й ефективно контролювати доступ у режимні зони та приміщення аеропортів.

Що ж до застосування цих технологій у прикордонному контролі, то нині наймасштабніший проект реалізований в Об'єднаних Арабських Еміратах (ОАЕ). На території цієї країни постійно проживають 5,4 млн іноземців, із них 85% – гастарбайтери. Відповідно, міграційні потоки в ОАЕ дуже великі та постійно зростають. У цих умовах виник-

[1] Мюррэй С. Биометрия против терроризма / Сара Мюррэй // Деловая неделя. – 2004. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document. asp...

[2] ФБР вошло во вкус использования биометрических технологий // BIOMETRICS.RU. – 2013. – 3 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические технологии «Циркон» // Papillon.ru. [Электронный ресурс]. – Режим доступа: http://www.papillon.ru/zircon.php...

ло завдання пришвидшити здійснення прикордонного контролю, одночасно забезпечивши його високу надійність. Це завдання було виконане за допомогою технологій ідентифікації за райдужною оболонкою очей: сканери, що дозволяють реалізувати цю технологію, діють на всіх прикордонних пунктах. Система біометричної ідентифікації щодня здійснює до 14 млрд порівнянь даних стосовно зображень райдужок очей.

Із 2008 року систему біометричної ідентифікації за райдужною оболонкою очей почали розповсюджувати і на інші арабські країни – Йорданію й Оман. Планувалося зв'язати базу даних ОАЕ з банком даних, який діє в Саудівській Аравії. Загалом у цьому королівстві біометричні технології використовуються не тільки з метою прикордонного контролю, але і в системі національних ID-карт, що видаються саудівським громадянам[1].

Розглянемо методи ідентифікації за *сітківкою ока*. Цей метод практично почав вивчатися приблизно з середини 50-х років XX сторіччя. Сітківка – світлочутлива частина ока, що міститься на задній стінці ока – очному дні. Вона містить відростки зорового нерва – палички і колби, які дозволяють нам бачити, а також кровоносні судини. За допомогою спеціальних приладів на очному дні можна розгледіти судини, диск зорового нерва, а також жовту пляму – ділянку, що відповідає за підвищену гостроту зору в кольорі. Для розпізнавання індивідуума використовується малюнок кровоносних судин, що є унікальним для кожної особи (жовта пляма і диск очного нерва мають розпливчасту форму, його геометрія може змінюватися від огляду до огляду). Для сканування сітківки використовується інфрачервоне випромінювання низької інтенсивності, скероване через зіницю до кровоносних судин на задній стінці ока. Із отриманого сигналу виокремлюють декілька сотень первинних характерних точок, інформація стосовно яких усереднюється та зберігається в спеціально кодованому файлі.

Для того, щоб зробити чітку фотографію кровоносних судин очного дна, кришталик ока повинен бути в певному положенні, за якого світло, що проходить через нього, мінімально заломлюється, тобто око повинно перебувати в чітко визначеній позиції. Водночас автоматиці потрібен час для визначення найліпшого положення ока й якості отримуваного зображення[2].

Сканери сітківки ока використовуються у системах контролю доступу на особливо секретні об'єкти, оскільки у них є один із найнижчих відсотків відмови в доступі зареєстрованих користувачів і практично не буває помилкового дозволу доступу[3].

До недоліків подібних систем насамперед належить психологічний чинник: не кожна особа готова дивитися в невідомий темний отвір, де щось світить в око. Крім того, треба контролювати положення ока щодо отвору, оскільки подібні системи, як правило, чутливі до відхилення орієнтації сітківки. Також устаткування для ідентифікації за сітківкою ока занадто дороге, а у разі хвороби (помутніння) кришталика ока (катаракті) отримати повне зображення очного дна просто неможливо.

У липні 2005 року в ЮАР на засіданні біометричного підкомітету ISO з тексту міжнародного стандарту, що описує формат зберігання зображень кровоносних судин, були виключені всі слова, пов'язані з сітківкою. Ця ініціатива була підтримана всіма країнами-учасниками підкомітету: жодна з країн практично не потребує такої стандартизації,

[1] Ученый из Кембриджа предрекает дальнейшее распространение технологий идентификации по радужной оболочке глаз // BIOMETRICS.RU.

[2] Биометрики глаза: различия радужной оболочки и сетчатки. [Электронный ресурс]. – Режим доступа: http://www.npo-inform.com/biomert/analitika/glaz/...

[3] Биометрические системы безопасности // БДИ. – 2002. – № 1 (41). [Электронный ресурс]. – Режим доступа: http://www.iching.ru/6/Bezopasnost...

оскільки немає масових виробників такої спецтехніки і компаній-інтеграторів, які були б зацікавлені в просуванні методу розпізнавання за сітківкою ока.

Отже, незважаючи на те, що розпізнавання за сітківкою є одним із найбільш точних, винятково стійких до можливих підробок методів, ця технологія не почала широко застосовуватися на практиці: дуже висока ціна використовуваного устаткування, надто тривалий час сканування зображення сітківки (майже 2 хв), не кожна людина здатна пройти процес сканування (наприклад, діти, які не можуть потрібним чином керувати рухливістю ока) і, що дуже важливо, знімок очного дна містить велику кількість інформації про здоров'я людини, в зв'язку з чим значно обмежується застосування цього методу ідентифікації[1].

Як вже зазначалось, ідентифікація за сітківкою ока застосовується у надсекретних системах контролю доступу, котрі виробляються практично поштучно і в яких є один із найнижчих відсотків відмови доступу зареєстрованим користувачам і майже нульовий відсоток помилкового доступу[2].

В Ізраїлі розроблена нова технологія біометричної ідентифікації за допомогою зіниць очей. Апаратне забезпечення нової біометричної системи нагадує сканер райдужної оболонки очей, але фіксує характер руху зіниць у особи, яку ідентифікують, коли вона відстежує спеціально рухомий певний об'єкт. Як сканер може використовуватися вебкамера, а для демонстрації рухомих об'єктів застосовується звичайний комп'ютерний монітор. За повідомленням розробника нової технології, алгоритми розпізнавання цього методу засновані на новітніх досягненнях анатомії, фізіології, хімії та останніх результатах аналізу структури ока.

Також задекларовано, що нова технологія відрізняється високим рівнем безпеки, оскільки характер міміки рухів зіниць, який супроводжує відстежування рухомого об'єкта людиною, яка дивиться на нього, суто індивідуальний і його неможливо підробити. Було поставлено завдання довести це рішення до рівня готового продукту, причому тестування апаратного рішення в практичних умовах мало розпочатися в 2009–2010 роках.

Розробники нової технології сподівались, що їх рішення може бути затребуваним під час проведення ідентифікації користувачів онлайнових платіжних систем[3].

---

[1] Биометрики глаза: различия радужной оболочки и сетчатки. [Электронный ресурс]. – Режим доступа: http://www.npo-inform.com/biomert/analitika/glaz/...

[2] Биометрия: тотальный контроль (отпечаток пальца). – 2003. – 16 сентября. [Электронный ресурс]. – Режим доступа: http://www.cherry.ru/interes/...

[3] Пользователей платежных сервисов предлагают идентифицировать по характеру движения глаз. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Розділ 4

ІДЕНТИФІКАЦІЯ ЗА ДОПОМОГОЮ ЗОБРАЖЕННЯ ОБЛИЧЧЯ

У повсякденному житті, як правило, впізнають людей за обличчям. У зв'язку з цим цілком слушною була думка застосовувати цей метод для створення біометричних систем розпізнавання особистостей за допомогою зображень лиця осіб.

Прийнято вважати, що ідентифікація за обличчям є другою за ступенем поширеності та популярністю біометрична технологія. Хоча деякі експерти оспорювали це твердження (наприклад, аналітик агентства «Frost & Sullivan» Ніліма Сагар, інформація 2008 року), вважаючи, що друге місце після технології ідентифікації за відбитками пальців посідає технологія встановлення особи за райдужною оболонкою очей[1].

На початку 2013 року маркетингова компанія «GIA» опублікувала огляд, присвячений розвитку технологій біометричної ідентифікації за обличчям і голосом. За оцінкою авторів прогнозу, обсяг відповідного сегмента світового ринку може до 2018 року сягти 2,9 млрд доларів. Для сегмента технологій біометричної ідентифікації за рисами обличчя загальносвітовий показник CAGR, обчислений у складних відсотках, сягне 19%.

Аналітики «GIA» вважають, що зростанню потреби в застосуванні біометрії (зокрема технологій ідентифікації за рисами обличчя) буде сприяти зростаюча необхідність забезпечення безпеки, насамперед протидія терористичним атакам, злочинності, насильству на расовому й етнічному ґрунті та іншим протиправним діям[2].

Вважалось, що технологія ідентифікації за обличчям є допоміжною та в основному може застосовуватися у комплексі з одним із інших біометричних методів (наприклад, водночас із ідентифікацією за відбитками пальців) або з іншими небіометричними способами встановлення або підтвердження особистості людини.

Ідентифікація людини за рисами обличчя – один із найдинамічніших напрямів у біометричній індустрії, яка постійно розвивається. Привабливість цього методу полягає в тому, що він найбільш наближений до звичайного людського розпізнавання індивідуумів за допомогою обличчя. Зростання мультимедійних технологій, зокрема всезростаюче використання відеокамер у громадських місцях таких, як міські вулиці та площі, аеропорти, авто- та залізничні вокзали й інші місця скупчення людей, зумовили необхідність розвитку цього напряму.

Відповідно до даних дослідження у квітні 2013 року компанії «Frost & Sullivan» «Аналіз світового ринку прикордонного контролю й біометрії», світовий ринок систем прикордонного контролю та біометрії продовжить свій поступальний розвиток – насамперед це є наслідком підвищеної уваги світового співтовариства до проблеми забезпечен-

[1] Новые перспективы биометрии в пограничном контроле. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Технологии биометрической идентификации по лицу и голосу: новые перспективы. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

ня безпеки пасажирів. Цей ринковий сегмент має значний потенціал, але його подальший розвиток залежить від показників прибутковості й економічної доцільності інвестицій. Дослідження стосувалося систем безпеки для цивільних, військових і державних потреб, зокрема й потреб правоохоронних органів.

Багато країн уже запровадили технології електронних паспортів і автоматичних систем ідентифікації осіб «*egate»,* яка дозволяє значно зменшити час проходження індивідуумами прикордонного контролю. Акцентуємо, що більшість проектів у Європі перебували тоді на стадії тестування, причому 62,5% систем використовували технологію ідентифікації осіб за рисами обличчя[1].

У деяких країнах значна кількість мешканців висловлюються за розширення застосування біометричних технологій у прикордонному контролі. Наприклад, 95% громадян Австралії підтримують використання технологій біометричної ідентифікації за рисами обличчя, яка широко застосовується в аеропортах п'ятого континенту в системах прикордонного контролю. Ці результати були отримані компанією «Unisys» в результаті проведення чергового соціологічного опитування.

Австралійці також досить зацікавлені в тому, щоб на основі біометричних технологій підвищувалась ефективність роботи правоохоронних органів[2].

Основою будь-якої системи розпізнавання особи є застосування математичного методу кодування. Цей математичний метод заснований на аналізі локальних характеристик для представлення зображення особи у вигляді статистично обґрунтованих і стандартних блоків даних. Він ґрунтується на тому, що обличчя будь-якої особи може бути виокремлено з репрезентативної вибірки зображень лиця осіб із використанням сучасних статистичних прийомів. Отримуваний складний математичний код індивідуальної ідентичності обличчя містить інформацію, яка дозволяє з достатньою високою точністю відрізнити лице конкретної особи від мільйонів інших зображень обличчя. Тому нині біометричні технології, зокрема й методи розпізнавання за зображенням обличчя, і надалі є провідними інноваціями в індустрії безпеки, особливо в боротьбі зі злочинністю та тероризмом.

Для таких сфер практичного застосування, як прикордонний контроль, обслуговування та реєстрація пасажирів, робота з електронними ідентифікаційними документами та картками, попередження і розкриття злочинів за «гарячими» слідами, питання безпеки, – нині неможливо обійтись без автоматизованих систем, що застосовують біометричні методи розпізнавання. Сьогодні дедалі інтенсивніше розвивається і застосовується технологія розпізнавання особистості при скупченні людей у громадських місцях за умови наявності у базі даних потрібного шаблону зображення обличчя конкретного індивідуума.

Технології розпізнавання рис обличчя спрямовані вести пошук у режимі «один до багатьох», тобто зіставляти конкретне обличчя з тисячами інших, зображення яких перебуває у базі даних. Технології сканування лиця осіб, як правило, працюють із відеозображеннями з розрішенням 320 × 240 пікселів на дюйм зі швидкістю 3–5 кадрів у секунду. Можливість зйомки з більш високим розрішенням та частотою значно підвищують надійність впізнання. У разі розпізнавання обличчя з великої відстані результат ідентифікації залежить від якості відеокамери.

---

[1] Биометрические системы пограничного контроля: новый прогноз. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Австралийцы поддерживают расширение практики использования биометрических технологий. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Є декілька способів розпізнавання особистостей за їх лицем. До них належать такі типи:

– метод власних характеристик (eigenfaces) – аналіз зображення в градаціях сірого кольору для виявлення унікальних параметрів;

– метод виявлення відмінних рис – найпопулярніший, він є адаптованим до змін міміки;

– метод на основі нейронних мереж – порівняння за «особливими точками», зокрема використовується для ідентифікації зображення лиця індивідуумів у складних умовах проведення відеоспостереження;

– метод автоматичної обробки зображення – визначення та виокремлення відстаней та співвідношень відстаней між особливостями рис обличчя, що легко відзначаються – рекомендовано застосовувати у разі поганого освітлення місця зйомки.

У системах статистичного розпізнавання на основі набору біометричних даних та їх обробки формується електронний зразок-шаблон, який складається з унікального набору чисел, що є характеристикою конкретної особи. Системи на базі нейромереж і на основі реалізації методу автоматичної обробки зображення лиця схожі до «людської» інтерпретації проблеми розпізнавання. Ці системи можуть «самонавчатися» і тому підходять під час використання базових параметрів для ідентифікації таких рис обличчя, що змінюються з часом і віком: наявність різних зачісок волосся, бороди, окулярів та деяких інших чинників. Під час використання апаратури, що побудована за принципами дії цих двох останніх методів, можливе застосування для ідентифікації і верифікації осіб старих фотографій або рентгенівських знімків.

Основні етапи процесу розпізнавання особи – це сканування лиця особи або наданого фотозображення, визначення і виокремлення індивідуальних характеристик, формування шаблону і порівняння отриманого шаблону з наявними у базі даних. Перше сканування обличчя під час формування еталонного шаблону триває 20–30 секунд, унаслідок його проведення отримують декілька зображень.

Якісні зображення в електронному вигляді займають об’єм пам’яті 50–300 Кб, а сформований еталонний шаблон – 1,3 Кб. Процес ідентифікації полягає у створенні нового шаблону пред’явленого обличчя в режимі реального часу та порівнянням його з файлом еталонного шаблону[1].

Методи розпізнавання за зображенням лиця можуть працювати з двовимірним або з тривимірним зображеннями (так звані 2D- і 3D-зображення). Ідентифікація людини за рисами обличчя нині є одним із найдинамічніших напрямів у біометричній індустрії. Привабливість цього методу полягає в тому, що він найбільш схожий до звичайного зорового способу, за яким люди розрізняють одного індивідуума від іншого. Розвиток мультимедійних технологій та їх використання у громадських місцях скупчення людей забезпечило необхідність посиленого розвитку цього напряму.

Розпізнавання лиця особистості передбачає виконання однієї з таких функцій: аутентифікації (встановлення достовірності «один до одного») або ідентифікації (пошук за принципом «один з багатьох»). Система автоматично оцінює якість представленого зображення обличчя для можливості розпізнавання і, якщо потрібно, спроможна у деяких випадках здійснити процедуру його поліпшення. Вона також відтворює зображення лиця з наявних сегментів даних, створює цифровий код або внутрішній шаблон, що є унікальним для кожного індивідуума.

[1] Евангели А. Биометрические технологии / А. Евангели // Bytemag.ru. – 2004. – № 4 (68). – 10 апреля. [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/ articles/…

Для виконання завдання верифікації, особливо під час здійснення перевірки документів громадян при перетині кордонів, досить комбінованого (2-D + 3-D) методу розпізнавання обличчя. Цей безконтактний метод забезпечує максимальну вимірюваність цієї біометричної характеристики (інакше кажучи, максимальну швидкість верифікації і, як наслідок, проходу), а відтак пришвидшує проходження пасажиропотоку через точку контролю. Точність 3-D, а тим більше комбінованого методу (2-D + 3-D) є досить високою, відповідає вимогам верифікаційного та ідентифікаційного режимів. Крім того, використання звичайної двомірної фотографії, по-перше, поки що є загальноприйнятою практикою, а по-друге, дозволяє операторові ухвалити остаточне рішення щодо ідентичності облич або у разі сумніву здійснити візуальне порівняння з декількома найбільш подібними фотозображеннями індивідуумів із банку даних[1].

У січні 2006 року в японському місті Кіото на засіданні Міжнародного підкомітету зі стандартизації у галузі біометрії при ISO була затверджена перша версія проекту поправки до міжнародного стандарту в галузі біометрії (ISO/IEC 19794-5). Суть поправки полягала у включенні тривимірного цифрового (3-D) зображення обличчя разом із звичайною двовимірною фотографією у формат даних, який призначений для зберігання, обміну і використання даних у електронному вигляді під час здійснення процедури автоматичного розпізнавання особи. Із лютого 2006 року після затвердження вказаної поправки під цифровим зображенням особи почали розуміти такий формат даних, у який включено і звичайне двовимірне, і тривимірне фотозображення обличчя.

Тривимірне фотозображення – одна з новітніх біометричних технологій. Трипросторове фото, яке займає всього 5 Кб, записують разом із двовимірною фотографією у мікрочіп біометричного паспорта; воно збільшує точність ідентифікації особи і підвищує надійність проведення автоматичної звірки документів. Експерти зазначають, що рівень розпізнавання тривимірної фотографії з чіпу документа становить понад 90% (дані 2006 року), тоді як у двовимірного зображення цей показник не перевищує 50%.

Прецедент такого швидкого узгодження міжнародного стандарту за технологією розпізнавання за цифровим 3D-зображенням обличчя особи пояснюється тим, що цифрове зображення лиця – це одна з трьох головних так званих «великих біометрик», які використовують для автоматичного розпізнавання особистості індивідуума. Саме цифрове зображення особи було визнане обов'язковим у всіх країнах для паспортно-візових документів нового покоління, тоді як два інших біометричних параметра – відбитки пальців і зображення райдужної оболонки ока – тривалий час вважалися додатковими, і тільки з кінця 2009 року один із цих двох видів став обов'язковим для паспортно-візових документів другого покоління.

Необхідність введення тривимірної фотографії у формат даних для біометричних паспортів обстоювали й експерти-криміналісти. Адже тривимірні (геометричні) дані особи безпосередньо зв'язані з антропометричними характеристиками, які є унікальними для кожної людини, тому вони є більш надійними ознаками для комп'ютерних алгоритмів розпізнавання, ніж інформація, яку можно отримати зі звичайних двовимірних фотографій. Але традиційні двовимірні фото краще інтерпретуються людиною-оператором, який «ручним» способом може перевірити комп'ютер і ухвалити остаточне рішення під час розпізнавання особи за його фотозображенням.

Отже, включення тривимірної фотографії разом із двовимірною у формат даних цифрового зображення обличчя особи істотно збільшує точність ідентифікації індивідуу-

[1] Современные биометрические системы безопасности. [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/detail.php...

ма під час допуску в приміщення або при перетині державних кордонів і підвищує надійність автоматичної звірки документів. Крім того, запис у мікрочіп паспорта тривимірної фотографії власника значно полегшить завдання рятувальників, судмедекспертів та інших фахівців, які займаються непростою справою ідентифікації загиблих. Це особливо важливо через зростаючу кількість катастроф, стихійних лих, терористичних атак та інших випадків масової загибелі людей.

Тривимірне розпізнавання осіб разом із іншими біометриками проходить подальше ретельне тестування в багатьох країнах світу. Результати обнадійливі: ця технологія істотно збільшує точність автоматичного розпізнавання, а головне – не уповільнює, а спрощує процедуру контролю на кордоні та реєстрації на авіарейси, водночас істотно збільшуючи надійність ідентифікації[1].

Прикладом нової 3D-системи ідентифікації за обличчям особи слугує комерційний пристрій «VisionAccess 3D Face Reader» компанії «L-1 Identify Solutions». Цей пристрій оснащений спеціальним сканером, який за допомогою спеціального програмного забезпечення (ПЗ) аналізує структуру поверхні обличчя людини і здійснює необхідні геометричні виміри. Далі ПЗ порівнює ці цифрові дані з шаблонами клієнтів, які зберігаються у банку даних (один подібний зразок займає приблизно 10 Мб, гранична чисельність записів у базі даних – 60 тис співробітників /відомості 2008 року/), і якщо результат порівняння позитивний, особа вважається ідентифікованою[2].

До переваг геометрії обличчя як біометричного ідентифікатора насамперед належить безконтактний спосіб отримання даних. На відміну від інших біометричних технологій (ідентифікації за відбитками пальців, райдужної оболонки ока або за голосом) система розпізнавання за рисами лиця пасивна, тобто не вимагає безпосереднього контакту (або визначених дій) з людиною, особистість якої встановлюється. Не потрібно просити громадян залишати відбитки пальців, дивитися в об'єктив або вимовляти якісь слова. Для криміналістів важливим є той факт, що цей метод ідентифікації має досить широкий вибір джерел для одержання потрібних відомостей: фотографії, відеоряд, дані відеоспостереження. Крім того, кількість можливих зразків ідентифікаторів набагато менша, ніж, наприклад, під час ідентифікації за відбитками пальців – одне обличчя у кожної людини проти відбитків 10 пальців рук.

Під час ідентифікації біометрична система автоматично виділяє й обробляє відомості, що характеризують окремі найхарактерніші ділянки і особливості обличчя: контури носа, губ, брів, відстань між ними тощо. На основі цих відомостей, відповідно до загальних принципів біометричних технологій, формуються цифрові моделі ідентифікаторів, які потім порівнюються між собою[3].

Технічна реалізація технологій ідентифікації за обличчям є більш складним із математичного погляду завданням, ніж розпізнавання за відбитками пальців, і, крім того, потребує апаратури, яка значно дорожча від потрібної для ідентифікації за папілярними візерунками пальців (необхідна цифрова відео- або фотокамера й електронний пристрій у вигляді спеціальної плати захоплення відеозображення). Але у цього методу є один великий плюс: для зберігання даних одного зразка ідентифікаційного шаблону (за характерними ознаками лиця) потрібна невелика кількість пам'яті. Адже людське обличчя можна

[1] Современные биометрические системы безопасности // Byte. – 2006. – № 6 (94). – июнь. [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/detail.php...

[2] Планируются продажи сканеров, формирующих трехмерные модели черепов. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp

[3] Идентификация по лицу. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/facial.php...

поділити на порівняно невелику кількість ділянок, які є незмінними у всіх людей. Наприклад, для створення (обчислення) унікального шаблону конкретної людини потрібно обробити дані лише про 12–40 характерних ділянок її обличчя[1].

Проте на практиці реалізувати технологію розпізнавання за обличчям людини не так вже й просто. На превеликий жаль, технології ідентифікації за обличчям надто чутливі до зовнішніх умов (освітленості, повороту голови, кута її нахилу тощо) і змін зовнішності людини (поява або зникнення окулярів, бороди, нанесення макіяжу). Через зазначені чинники ці технології все ще мають недостатній відсоток успішного розпізнавання користувачів і порівняно високий відсоток помилкових спрацювань, коли біометрична система помилково приймає одну людину за іншу (особливо під час порівняння з аналогічними показниками двох інших «великих біометрик» – технологій ідентифікації за відбитками пальців і райдужної оболонки ока).

Водночас технології ідентифікації за рисами лиця достатнього ефективні тоді, коли, наприклад, потрібно порівнювати фотографії – за умов, що знімки хорошої якості, а користувач не докладає спеціальних зусиль для того, щоб навмисно змінити свою зовнішність.

Розробники технологій ідентифікації за обличчям продовжують удосконалювати свою продукцію для того, щоб істотно підвищити її функціональність[2].

Метод розпізнавання за лицем особи – це єдиний біометричний спосіб ідентифікації персон із погляду багатоцільового застосування. На відміну від інших біометричних методів, що застосовуються тільки для контролю доступу або порівняння в базах даних, технологія розпізнавання образу особи дозволяє знайти обличчя індивідуума у відеокадрі для подальшого порівняння з еталонами в базі даних або, навпаки, щоб сховати його від випадкових оглядин. Завдяки вбудованим інфрачервоним випромінювачам комп'ютер легко може розпізнати каучукову муляжну маску під час імітації іншої особи. Об'єкт, стосовно якого проводиться спостереження, повинен мати людську шкіру, природну міміку і бути «живим», інакше спрацьовує спеціальний попереджувальний звуковий сигнал.

Над технологіями розпізнавання за рисами обличчя в кінці XX століття – початку XXI століття в США та Німеччині працювали декілька десятків компаній, яким були надані урядові гранти. Спочатку розробки призначалися виключно для потреб спецслужб, але з часом результати цих досліджень почали використовувати і для комерційних цілей[3].

Із кінця першого десятиріччя XXI століття технології розпізнавання за рисами лиця вже дозволяли сканувати обличчя людей у режимі реального часу. Відеокамера підключалась до термінала і система визначала чи відповідає лице особи у кадрі фотозображенням, що внесені в обслуговуючу базу даних.

Принцип роботи системи ідентифікації за рисами обличчя застосовує спеціальний алгоритм оцифрування зображень, що дозволяє вибирати на кадрах лице конкретної людини й оцифровувати його, використовуючи водночас потрібну кількість характерних параметрів (так звані базові точки – форму та розташування вилиць і губ, колір і форму очей, ширину перенісся тощо). Отже, кожного індивідуума можна описати за допомогою унікального набору параметрів, причому навіть із деяким надлишком. Для ідентифікації

---

[1] Борзенко А. Биометрические технологии / А. Борзенко // Bytemag.ru. – 2001. – № 10. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/?ID=600497...

[2] Идентификация по лицу. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/facial.php…

[3] Борзенко А. Биометрические системы распознавания внешности / А. Борзенко // Платформы и технологии. – 2002. – № 11. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

з високим ступенем точності потрібно не більше 40 характерних точок лиця, тоді як система зазвичай може виокремити близько двох тисяч оціночних параметрів. Це дає змогу забезпечити високу надійність ідентифікації незалежно від положення голови, наявності окулярів, косметики. Фотозображення та цифровий опис обличчя кожного індивідуума (шаблон обличчя) вносяться в спеціальну базу даних, за якою згодом здійснюється пошук і розпізнавання осіб.

Загалом на ринку систем автоматичного розпізнання за рисами обличчя в основному панують два типи систем. Перша ґрунтується на статистичному методі: на основі набору біометричних даних та їх обробки формується електронний зразок у вигляді унікального числа, що належить тільки конкретній людині. Такий тип систем досить поширений, але ідентифікація за їхньою допомогою, як правило, недостатньо надійна.

Методи, які засновані на іншому типі, схожі до людського сприйняття та впізнання конкретної особи. Цей принцип моделює «людський підхід»: одна людина розглядає обличчя іншого індивідуума для здійснення ідентифікації її особистості. Як і аналіз особистого підпису, визначення ідентичності за фотографією в документі належить до найбільш доступного та визнаного методу ідентифікації особи. На роботу систем, що побудовані за цим принципом, практично не впливають такі чинники, як вік, наявність вусів, бороди або окулярів. Крім того, для ідентифікації та верифікації можна використовувати старі фотографії. Технологія в принципі дозволяє працювати навіть із рентгенівськими знімками.

Метод розпізнавання за рисами лиця використовується в різних сферах охоронної і, особливо, правоохоронної діяльності. Крім пошуку й порівняння з відомостями, які є в базах даних оцифрованих фотозображень (ідентифікацією), а також і класичного контролю доступу (верифікацією), за допомогою цього методу можна безконтактно впізнавати людей як у негрупових, так і в групових кадрах, але в останньому випадку з деякими обмеженнями.

Розпізнавання за рисами обличчя особи може відбуватися на відстані, непомітно, непривертаючи водночас уваги об’єкта стеження. Із погляду служб безпеки та спецслужб це явна і безперечна перевага методу біометричної ідентифікації індивідуумів за зображеннями осіб. Але правозахисники вважають, що застосування подібних технологій порушує право людини на приватність й анонімність. Виробники технологій розпізнання за рисами лиця підготувалися до протестів, і, як вони запевняють, подбали про права осіб. Згідно з їхніми оприлюдненими заявами, у разі, якщо система не виявить збігань із відомостями щодо осіб у банках даних, то у пам’яті системи не залишається жодної інформації стосовно індивідуума, котрий був зафіксований камерою. Виробники також акцентують на тому, що в системах застосовуються звичайні стандартні камери відеоспостереження. Суспільство давно звикло до цих камер, використання яких у більшості країн уже врегульоване законодавством. У супермаркетах, магазинах і інших установах і підприємствах розвинених країн прийнято попереджати про те, що в приміщенні здійснюється спостереження за допомогою відеокамер. А чи є термінал для проведення впізнання відвідувача в кабінеті служби безпеки чи ні – яка, мовляв, до цього справа законослухняному громадянину.

Основні споживачі подібних біометричних систем – не тільки служби безпеки приватних закладів (банків, аеропортів, фірм, супермаркетів, казино тощо), але й державні установи (силові відомства, міністерства, інші спеціальні структури)[1].

[1] Борзенко А. Биометрические системы распознавания внешности / А. Борзенко // Платформы и технологии. – 2002. – № 11. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

Один із відомих міжнародних експертів у галузі біометрії доктор Джозеф Атік (засновник, президент і виконавчий директор біометричної корпорації «Visionics», згодом і голова правління фірми «Identix», яка утворилася після укрупнення «Visionics») та його колеги розробили систему «FaceIt» – спеціалізоване програмне забезпечення для розпізнавання лиця осіб, які автоматично виокремлюються в кадрах відеозйомки телекамер і записах відеокамер спостереження, з метою подальшого пошуку їх у базах даних різних категорій індивідуумів, зокрема й тих, що перебувають у кримінальному розшуку.

Принцип дії системи «FaceIt» такий. Відеосигнал від камери постійного спостереження перетворюється на послідовність цифрових фотографій. Програма сканування виокремлює на фотозображенні обличчя осіб і вимірює низку лицьових параметрів, використовуючи як точку відліку місцерозташування очей «об'єкта». Отримані у такий спосіб відомості порівнюються з відповідними параметрами шаблонів лиць, що заздалегідь накопичені у базі даних. Коли виявляється «близька» відповідність під час здійснення процедури порівняння, система видає оператору сигнал тривоги.

Зокрема в програмі «FaceIt», яка була розроблена «Visionics», процедура порівняння фотозображень проводиться так. Два фото порівнюються (співвідносяться) один з одним за шкалою від 0 до 10. Тут «0» означає відсутність збігу параметрів, а «10» – ідеальне збігання. У «FaceIt» як порогове значення для «близької подібності» вибрана величина 8,5. Взагалі поріг визначається оператором і наслідки неправильного вибору головним чином впливають на ефективність дії програми. Якщо задати поріг дуже високим, то збігань просто не буде. Якщо задати дуже низьким, то, навпаки, – система починає сигналізувати безперервно, реєструючи практично постійні збігання. На помилкове розпізнавання впливає досить багато різних чинників: зміни в освітленні об'єкта, наявність предметів на задньому фоні, конкретне положення лиця особи та його вираз, розташування знімальної камери, такий її параметр, як максимальне розрішення і, врешті, якість картинки виокремленого кадру. Ці чинники, а також і низка інших, здійснюють суттєвий вплив на результат розпізнання та стосуються не тільки зображень, які фіксуються відеокамерою, але й еталонних зразків (шаблонів) із бази даних.

Незважаючи на всі труднощі, на думку доктора Д. Атіка, система «FaceIt» набагато результативніша порівняно з іншими аналогічними засобами, що використовуються для розпізнання злочинців і терористів, оскільки зазначені особи не надають заздалегідь відбитків своїх пальців і знімків райдужної оболонки очей, а ось фотографії або фотороботи набагато легше отримати за допомогою прихованої оперативної зйомки «об'єкта», яким цікавляться, або свідчень свідків подій.

Технологія «FaceIt» не досліджує «поточний» вигляд обличчя. Тут робота здійснюється за допомогою аналізу проведених вимірювань характерних лицьових елементів та їх взаємною відповідністю розташування. Проведені дослідження довели, що місцерозташування деяких характерних особливостей на обличчі людини є практично постійним. Важливих рис-особливостей налічують близько 80, тоді як для проведення впізнання за допомогою програми «FaceIt» потрібно лише 14. Взагалі деякі особливості обличчя можна приховати під волоссям або змінити за допомогою силіконових ін'єкцій, але основна кількість характерних рис є сталою і незмінною в часі, що дозволяє досить успішно проводити ідентифікацію за обличчями осіб[1].

Технології ідентифікації за рисами обличчя постійно удосконалюються. Під час біометричної ідентифікації людей за відеозображеннями джерелами потрібних ознак

[1] Жажда биометрии. [Электронный ресурс]. – Режим доступа: http://gbop.nm.ru/ htm/gbop-8-2.htm…

можуть бути не тільки зображення лиць осіб – такий висновок зробили дослідники з Університету штата Техас і Національного інституту стандартів й технологій (NIST) США.

Під час дослідів учені використовували три види зображень людей – лиця й верхньої частини тулуба людини, тільки обличчя та верхньої частини тулуба зі скритим обличчям. За результатами проведених дослідів учені зробили висновок, що використання для ідентифікації інформації не тільки про обличчя, але й про інші елементи тіла людини може суттєво поліпшити якість розпізнавання в біометричних системах.

Загалом ідентифікація людей проводилась досить точно, коли на зображеннях були присутні й лице, й верхня частина тіла. У разі маскування обличчя ідентифікація була майже такою точною. Але коли на фотографіях були присутні тільки зображення лиця, оператори і комп'ютерні системи ідентифікації, що були задіяні у дослідах, не завжди однозначно могли ідентифікувати запропонованих індивідуумів.

Однак під час відповіді на поставлене запитання практично всі особи-оператори, які брали участь у дослідженнях, повідомили, що ідентифікували індивідуумів тільки за рисами їх лиця. Щоб пояснити цей парадокс, дослідники вирішили записати рух очей піддослідних операторів. Виявилося, що у разі неможливості ідентифікувати людину за рисами її лиця, піддослідні негайно починали розглядати наявні на фотографіях частини тіла[1].

Той факт, що метод автоматизованого розпізнавання індивідуума за обличчям широко застосовується на практиці, не підлягає сумніву. Цю технологію використовують такі відомі установи, як «Deutsche Bank», Європейський центр ядерних досліджень (CERN), російський «Центробанк», Національний банк Литви, корпорації «Microsoft» і «Siemens», Федеральна друкарня Німеччини та багато інших. Атомні електростанції та секретні об'єкти також охороняються за допомогою зазначеної технології.

Перша електронна база даних цифрових фотографій для системи автоматичного розпізнавання особи була створена в «ZN Vision Technologies» (http://www.zn-ag.com) і дозволила численним поліцейським службам у ФРН, США та Польщі оптимізувати слідчі дії і якісно поліпшити заходи для розшуку злочинців. Інтелектуальний сучасний відеоконтроль гарантує безпеку і захист у місцях скупчення людей, оскільки дозволяє за допомогою спеціальних інформаційних банків даних виявляти небажаних або небезпечних персон у режимі реального часу та вжити адекватних заходів[2].

У кінці травня 2007 року Національний інститут стандартів і технологій США підбив підсумки конкурсу FRVT-2006 (Face Recognition Vendor Test, або «Тестування постачальників систем для розпізнавання осіб»). Компетентне журі констатувало, що загалом комп'ютерні технології розпізнавання людей розвиваються дуже швидко. Зокрема алгоритми впізнання осіб із 2002 року поліпшили свою якість приблизно вдесятеро, а з 1995 року – в сто разів. Причому кращі з протестованих технологій значно перевершують відповідні людські можливості.

Співробітник національного інституту стандартів і технологій США Джонатан Філіпс (Jonathan Phillips), який відповідав за організацію конкурсу та підготовку підсумкового звіту, вважає, що таке помітне зменшення помилок розпізнавання (одного з найважливіших параметрів біометричних систем) досягнуто завдяки застосуванню фотозображень високого розрішення і тривимірних алгоритмів впізнання осіб. Більшість технологій тривимірного розпізнання були розроблені після 2006 року.

[1] Биометрическая идентификация по лицу: новые возможности // Security News. – 2013. – 3 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

[2] Борзенко А. Биометрические системы распознавания внешности / А. Борзенко // Платформы и технологии. – 2002. – № 11. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/

В рамках конкурсу FRVT – 2006 було вперше проведене тестування шести нових 3D-алгоритмів. Головна спрямованість нових алгоритмів – аналіз інформації щодо об'ємних форм і співвідношень деталей лиця індивідуумів. Серед переваг нової технології відзначалась здатність методу 3D-ідентифікації до виокремлення відмінних рис на лицьовій поверхні обличчя людини. Наприклад, тривимірних кривих для лінії очних ямок, носа, підборіддя, вилиць, де кістки та тканини, що їх обтягують, найбільш доступні огляду на відстані та які майже не змінюють форму з часом. Крім того, як вже зазначалось, якість роботи традиційних 2-D систем розпізнавання лиць осіб надто сильно залежить від освітлення. А форми обличчя, що аналізуються 3D-системами, не так суттєво залежать від змін в освітленні.

За свідченням експерта з Інституту робототехніки при Університеті Карнегі-Мелона Ральфа Гросса, 3D-системи розпізнання осіб за обличчям можуть ефективно ідентифікувати людей за різних кутів повороту голови й аж до вигляду в профіль. Традиційні 2D-системи досить непогано працюють із зображеннями в анфас і за повороту голови на кут до двадцяти градусів. Але як тільки кут зйомки збільшується і положення голови особи наближається до профільного зображення, системи, що застосовують 2D-метод, починають давати збої. Пояснюється це тим, що на ранній стадії розвитку цієї технології основним завданням систем розпізнавання була робота сканера лиця осіб на пунктах контролю пропуску або допуску, де індивідуум вимушений співпрацювати з системою, підставляючи обличчя для контрольної зйомки в анфас і за заздалегідь визначеного і незмінного в часі освітлення. Нині головною вимогою стало розпізнавання людей у натовпі, де кут повороту голови й умови освітленості обличчя особи є довільними.

Ще один чинник істотного прогресу в технологіях комп'ютерного розпізнавання осіб – здатність сучасних камер робити знімки високого розрішення. Зокрема, завдяки цьому факту стає реальністю ретельний комп'ютерний аналіз текстури шкіри обличчя людини. За такого аналізу будь-яка з ділянок шкіри, яка отримала назву шкірного відбитка (skin print), може фіксуватися як окремий образ, а потім розбиватися на ще менші фрагменти, які алгоритми перетворюють на математично зафіксовані співвідношення між зморшками, порами й іншими характеристиками шкірної текстури. Коли всі ці характеристики переведені в електронні параметри, вони дозволяють розрізнити навіть близнят, що звичайним системам розпізнавання лиць осіб поки що не під силу. За свідченням експерта Ральфа Гросса комбінування стандартних можливостей біометричної ідентифікації за обличчям з аналізом шкірних текстур може зразу підвищувати точність розпізнання на 20–25 відсотків.

Серед висновків підсумкового звіту конкурсу FRVT-2006 слід зазначити пункт про те, що деякі з систем розпізнавання лиця осіб демонструють якості, що набагато перевершують людські можливості.

Технології біометричної ідентифікації загалом та алгоритми розпізнання за обличчям, зокрема, нині дедалі більше використовуються у різних системах безпеки. Про системи контролю й управління доступу відомо практично всім, але є й значна кількість інших технологій, де запроваджуються ці порівняно нові ідентифікаційні методи. Наприклад, у США декілька десятків штатів уже застосовують автоматизовану систему отримання цифрових фотографій за допомогою сканування обличчя для видачі нового типу водійських посвідчень (так званих біометричних або електронних). Аналіз цифрових фотографій допомагає виявляти осіб, які подали заяви на нові права водіїв у різних штатах (кожен штат має свою базу даних, тобто не має єдиного державного централізованого банку даних) або ж в одному штаті, але під різними установчими даними. Проте і в цій вельми успішно діючій системі умови для розпізнання обличчя осіб створені ідеальні – на

водійському посвідченні знімок зроблений за однаковими для усіх власників умовами: обов'язково в анфас і при стабільно визначеній освітленості. Для спецслужб, поліції, інших органів безпеки інтерес становлять істотно відмінні інші системи, що здатні швидко аналізувати обличчя осіб у натовпі та ефективно виявляти серед них тих людей, які цікавлять правоохоронні структури.

Автори звіту в 2006 році Національного інституту стандартів і технологій США зробили висновок, що біометричні системи візуального пошуку людей за обличчям поки що недостатньо якісні, щоб забезпечити майже 100% результат у пошукових заходах. Тому німецькі криміналісти, визнаючи загалом перспективність технології ідентифікації за лицем особи, припустили, що більш практичними повинні стати технології, які застосовують і розвивають метод на основі 3D-систем розпізнання лиць осіб[1]. Але навіть нині ця технологія поки що до необхідної кондиції ще не доведена. Загалом вважається, що повинен використовуватися симбіоз 2D- і 3D-технологій із деякими доповненнями.

Було опубліковано низку недостатньо райдужних прогнозів фахівців щодо використання існуючих технологій розпізнавань обличчя осіб, що обумовлені результатами тестувань практичної реалізації проектів ідей інтеграції ідентифікації за лицями індивідуумів із системами відеоспостереження. Так, під час проведення експерименту в аеропорту Бостона (США), подібна інтегрована система перевірялася на здатність виявляти в автоматичному режимі у натовпі «терористів» серед добровільних волонтерів, але допускала помилки у чотирьох випадках із десяти. Також несприятливий висновок містився у доповіді Європейської комісії, що була опублікована в 2007 році. Точність (розпізнавання за обличчям особи) знижується, коли реєстрація та подальша ідентифікація виявляються віддаленими у часі. Вважається, що буде необхідна регулярна перереєстрація[2].

Учені та фахівці з біометрії багатьох країн світу продовжують посилено працювати і здійснювати відповідні дослідження з метою створення більш якісних автоматизованих систем впізнання лиця людей.

Наприклад, в кінці 2007 року дослідники з Лондонського університетського коледжу проводили дослідні роботи зі створення нового варіанта такої системи розпізнавання. На відміну від інших аналогічних систем впізнання, у цій розробці намагались усунути залежність від положень розташування лиця особи (наприклад, обов'язково у фас), а також його міміки й умов освітлення.

Отже, основні зусилля досліджень спрямовані на усунення чинника обов'язкової співпраці системи з індивідуумом, чиє лице розпізнається. Замість створення тривимірних (3D) моделей у системі застосовуються статистичні методи аналізу декількох зображень однієї і тієї ж людини. Але для здійснення процесу розпізнавання необхідною умовою є використання як мінімум двох різних знімків.

Здійснення досліджень підтримує британське Національне агентство покращення правопорядку (National Policing Improvement Agency) та Міністерство внутрішніх справ Великобританії[3].

---

[1] Берд Киви. Лица, подлежащие опознанию / Киви Берд // Компьютерра. – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp?group_id=11&nItemID=2684&sSID=3.7

[2] Лукашов И. Биометрия становится индустриальной технологией / И. Лукашов // Cnews.ru. – 2007. – 21 августа. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security2007/articles/...

[3] Британские ученые создают новую систему распознавания лиц // CNews.ru. – 2007. – 15 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

На час написання другого варіанта посібника практично всі експерти з біометрії в своїх прогнозах свідчили, що автоматизовані системи розпізнання лиця людей «прийшли, щоб залишитися». У деяких ситуаціях вони досить ефективно працюють вже сьогодні, а прогрес подібних технологій цілком очевидний і такі технології масово впроваджуються у наше життя. У другому півріччі 2013 року газета «Нью-Йорк Таймс» опублікувала копії низки урядових документів, згідно з якими для технологій автоматизованого відеоспостереження і розпізнавання людей за обличчям у майбутньому очікується радикальне поліпшення ефективності й якості.

Зокрема ці документи свідчать, що для спецслужби DHS (Department of Homeland Security /Департамент держбезпеки США/) за контрактом вартістю понад 5 млн доларів створюється особлива шпигунська технологія, яка має абревіатуру BOSS. Ця назва розшифровується як «Біометрична система для дистанційного оптичного спостереження» або мовою оригіналу «Biometric Optical Surveillance System (BOSS) at Stand-off Distance».

Стисло надамо ключові моменти техзавдань цієї системи:

1) служба DHS відповідає за біометричну ідентифікацію людей – для визначення того, чи не перебувають особи, що з'являються у зоні спостереження, у федеральному списку осіб, які відслідковуються. Для виконання цього завдання, підрозділам DHS потрібна можливість встановлювати або перевіряти особистість людей у потайному, ефективному, точному й оперативному режимі;

2) такі можливості повинні охоплювати масовий збір, зберігання та передачу-прийом біометричних і біографічних даних про людей. Набуті під час реалізації проекту можливості повинні бути у робочому стані в широкому спектрі різноманітних умов (тобто працездатними вночі й вдень, у сухому і вологому кліматі, не залежати від температурних перепадів повітря);

3) дані на виході системи BOSS повинні бути придатними і для здійснення пошуку у великомасштабних базах даних (виявлення одного серед багатьох), і для встановлення однозначної відповідності раніше отриманим біометричним зразкам (верифікація – 1 до 1);

4) програмне забезпечення BOSS повинно забезпечити формування взірця та ідентифікувати особу індивідуума за технологією 3-D біометричної сигнатури лиця людини на відстані до 100 метрів.

Головним підрядником DHS, яка створює для спецслужби таку вражаючу систему, є фірма «Electronic Warfare Associates» військово-промислового комплексу США, що базується в штаті Кентуккі.

Хоча строки розробки, визначені за контрактом, минули у листопаді 2012 року, відомо, що роботи з доведення системи BOSS до кондиції продовжувались упродовж 2013 року[1].

Як відомо, 11 вересня 2001 року більшість терористів використовували під час посадки на літаки, за допомогою яких були здійснені терористичні акти на території США, права водіїв. Із наведеного факту очевидно, що критично важливо встановити дійсну особистість конкретної людини та мати водночас відомості щодо її благонадійності. Адже різні силові та правоохоронні відомства та спецслужби США володіли загалом негативною інформацією стосовно осіб, які здійснили вересневий теракт (вказані структури мали у своєму розпорядженні розрізнені дані, які не були відповідно систематизова-

[1] Технологии биометрической идентификации по лицу могут повысить свою эффективность // DGL.RU. – 2013. – 2 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

ні, що більшість осіб, причетних до терактів вересня 2001 року, належали до міжнародних терористичних організацій). Але відсутність можливості проведення контролю пасажирів авіарейсів за базами даних спецслужб і недостатня перевірка наданих відомостей та документів на предмет дійсного встановлення особистості пред'явника під час процедури видачі водійських прав у штатах США створили умови для успішного здійснення терористичного акту[1].

Ця подія і стала поштовхом для введення на початку XXI століття біометричних документів для ідентифікації особистості спочатку в США, а потім і в усьому світі, зокрема і для використання цифрових фотографій у водійських посвідченнях та інших документах, що засвідчують особу індивідуума. Нині у більшості штатів США та низці інших країн проводяться роботи з використання біометричних і деяких інших ідентифікаційних технологій під час видачі різних документів, що засвідчують особистість одержувача. Крім того, за прикладом США, у всіх державах під час видачі документів, які посвідчують особу, здійснюється перевірка претендентів за всіма наявними банкам даних різних спецслужб і правоохоронних структур.

Нині цифрове фото є біометричним параметром. Сучасні методики отримання такого фотозображення та внесення його в документ дозволяють практично однозначно ідентифікувати, що це фотографія конкретної особи і що відомості, які внесені в електронний чіп документа, відповідають дійсності. Із середини першого десятиліття XXI століття більшість держав масово видають різні біометричні посвідчення особистості: паспорти, водійські посвідчення, соціальні картки, військові квитки тощо. Порівняно з традиційними такі документи дозволяють надійно встановити, чи є пред'явник документа його дійсним власником, підвищити захищеність документів від підробки, полегшити шляхом автоматизації роботу співробітників прикордонних контрольно-пропускних пунктів та істотно пришвидшити процедуру перевірки власника документів.

Міжнародна організація цивільної авіації (ICAO) і Міжнародна організація з стандартів (ISO) ввели додаткові вимоги до фотографій і даних, які розміщуються в документах, що значно полегшило та стандартизувало використання систем автоматичного розпізнавання.

На прикордонних контрольно-пропускних пунктах (КПП) низки країн використовують технології встановлення та впізнання обличчя особи разом із технологією порівняння та розпізнавання відбитків пальців індивідуумів. Системи, що використовуються (наприклад, біометричні системи доступу «Identix»), дозволяють виконувати такі дії:

– порівняння у реальному часі фотозображення особи, що отримане під час проведення контролю, з цифровим зображенням або електронним шаблоном, що зберігається в документі, який пред'являється;

– зняття відбитків пальців і здійснення порівняння в реальному масштабі часу з шаблонами, що зберігаються у документі, котрий пред'являється, а також здебільшого з даними центрального сервера на предмет визначення їх відповідності.

Рішення типу «Identix» допомагають:

– засвідчити особистість під час пред'явлення проїзних документів, які є біометричними, або ухвалити відповідне рішення щодо встановлення дійсності особи за результатом проведення контролю за візовою базою даних;

– налагодити реєстраційні системи проходу пасажирів для забезпечення швидкісного контролю і так званої «імміграційної чистки»;

[1] Преимущества биометрических систем // Secnews.ru. – 2004. – 6 декабря. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/...

– скласти автоматизовану декларацію в'їзду/виїзду;

– зняти високоякісні відбитки пальців для електронного пред'явлення у системи AFIS (ідентифікація за відбитками пальців) або IAFIS;

– отримати прямі зображення чи виокремити фотозображення обличчя з наданих проїзних документів для пошуку в базах даних зображень обличчя особи (система ABIS);

– пришвидшити процес фонової перевірки осіб, які бажають отримати візу, звернулися з проханням надання політичного притулку або зміни громадянства;

– виконувати пошуку за радіоінформацією (установчі дані, отримані за допомогою безпровідного зв'язку) з віддалених місць, пунктів пропуску з сухопутних або морських кордонів[1].

Зараз відбувається поширення застосувань біометричних технологій у різних комерційних проектах. Так, прості функції розпізнання обличчя осіб уже реалізовані у цифрових фотоапаратах багатьох фірм, зокрема таких популярних, як «Canon», «Pentax» і «Fuji». Спеціальні програми пошуку, що записані у мікропроцесори, які вмонтовані в останні моделі фотоапаратів, можуть автоматично знаходити в картинці видошукача людські обличчя за характерними ознаками – очами, вухами, носом тощо. Якщо людина одна, камера сама може навести фокус виключно на нього, якщо ж осіб декілька, то вона автоматично обчислює та встановлює усереднений фокус для всієї групи. За потреби може сфокусувати об'єктив лише на особах переднього плану[2].

За останні декілька років значно збільшилась кількість застосувань біометричних технологій у різних мобільних пристроях: смартфонах, планшетах тощо. 2012 року за даними компанії «ABI research» 20% смартфонів здійснювали ідентифікацію своїх власників за допомогою технології ідентифікації за обличчям.

Фахівці фірми «ABI research» вважають, що протягом 2013–2017 років щорічна кількість смартфонів і планшетів, що реалізують цю біометричну функцію або можуть здійснити пошук фото в Інтернеті за допомогою лиця осіб, має сягти 665 млн штук. Ця кількість не може не вражати, особливо зважаючи на той факт, що зараз у більш-менш значних обсягах біометричну ідентифікацію за лицем особи підтримують мобільні операційні системи Google – Ice Cream Sandwich і Jelly Bean, а найяскравішим представником біометричних смартфонів є Samsung Galaxy SIII. Експерти компанії «ABI research» запевняють, що протягом 2013–2014 років кількість мобільних операційних систем, які будуть володіти можливостями біометричної ідентифікації користувачів гаджетів, суттєво збільшиться.

Як зазначає старший аналітик «ABI research» Джош Флуд, ефективність технологій біометричної ідентифікації за обличчям за останні 10 років суттєво підвищилася. Хоча на результати ідентифікації як і раніше впливають зовнішні умови (наприклад, рівень освітленості) і вираз лиця користувача, зараз розпізнавання власників гаджетів успішно здійснюється в дев'ятьох випадках із десяти. Д. Флуд вважає, що подальше підвищення розрішення камер цифрових пристроїв і збільшення потужності процесорів гаджетів будуть сприяти подальшому покращенню цього показника.

У огляді за 2012 рік підкреслена ще одна можливість, яка дозволить підвищувати точність біометричної ідентифікації за обличчям. Вона полягає в оснащенні мобільних пристроїв 3D-фотокамерами замість 2D-камер. На думку аналітиків «ABI research»,

[1] Биометрические системы доступа Identix // Борьба с преступносью за рубежом (по материалам зарубежной печати). – 2008. – № 4. – М.: ВИНИТИ.

[2] Берд Киви. Лица, подлежащие опознанию / Киви Берд // Компьютерра. – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

збільшення енергоспоживання, яке спричинить подібне переоснащення, не буде критичним[1].

Проаналізуємо принцип дії розпізнання лиця особи на основі тривимірного 3D-принципу, основні положення якого вперше були розроблені в Російській Федерації (РФ).

На форумі учасників національного проекту «Освіта», який пройшов у рамках виставки «Цифрова школа» в РФ у 2007 році, науково-виробниче об'єднання (НВО) «Інформація» представило біометричну систему, яка працювала за технологією тривимірного розпізнавання обличчя особи. Принцип роботи цієї системи такий. Спочатку сканується зображення лиця та з субміліметровою точністю вибудовується його просторова модель. Далі за допомогою математичного алгоритму модель транслюється в цифровий код (біометричний шаблон) розміром лише 5 Кб і розміщується в архівне зберігання у базу даних. Після цього за кожної контрольної процедури процес сканування повторюється, а отриманий новий цифровий код порівнюється з оригіналом, що зберігається у базі даних і, якщо електронний код збігся з шаблоном, апаратура розпізнання ідентифікує людину. Ця безконтактна операція триває впродовж 1–1,5 секунди. Як гарантії надійності виробник навів статистику проведення загальної кількості процедур розпізнання, причому стверджував, що система здатна відрізнити навіть однояйцевих близнят, її неможливо ввести в оману за допомогою гриму і вона може працювати навіть в умовах слабкої освітленості.

НВО «Інформація» повідомила, що наприкінці 2007 року система почала впроваджуватися у Росії в установах з обмеженим доступом, у так званих «чистих» зонах, сховищах музеїв, будівлях аеропортів і на нафтохімічних підприємствах.

У першому десятиріччі нового тисячоліття найбільш масштабне впровадження 3D-методу в Російській Федерації було реалізоване в Реставраційно-сховищном центрі Державного Ермітажу.

«Ця система в комбінації з іншими методами контролю фізичного доступу в приміщення Ермітажу забезпечує високий рівень безпеки музейного сховища, а також зменшує можливість учинення протиправних дій, – переконаний заступник генерального директора Державного Ермітажу Олексій Богданов. Однак у декількох наших співробітників існує якийсь психологічний бар'єр: не прагнуть вони, щоб десь зберігалося 3D-зображення їх голови! І ми, діючи в рамках закону, нічого не можемо з ними вдіяти. Тому вони проходять на свої робочі місця за допомогою традиційної пропускної картки. У той же час за рік експлуатації дана система продемонструвала виняткову ефективність – вона нечутлива до повороту голови, а також до наявності в співробітника бороди, вусів, окулярів, головного убору і тому подібного. Так, бувають інколи ситуації, коли ця система з першого разу не впізнає нашого співробітника (розпізнавання проводиться за той короткий час, коли людина йде від вхідних дверей до турнікету), але жодного разу не було випадку, щоб ця система дозволила вхід чужому». За словами Олексія Богданова, час на введення в базу даних 3D-фотографії голови співробітника та відомостей про його доступ до різних приміщень музею триває приблизно три хвилини[2].

У багатьох розвинутих державах аналогічні системи застосовуються в навчальних закладах, де вони допомагають забезпечити безпеку учнів і педагогів. Також за їх допомогою здійснюється облік відвідування занять, підтримується на належному рівні

[1] Скоро каждый пятый смартфон станет биометрическим. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

[2] Биометрические технологии, которые мы выбираем // Week/RE. – 2010. – 9 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

дисципліна й обмежується доступ як безпосередньо в навчальні заклади, так і в декотрі їх приміщення.

У багатьох навчальних закладах Західної Європи та США за допомогою біометричних ідентифікаційних систем можна оплачувати харчування в їдальнях. Потрібно лише пред'явити сканеру лице або відбиток пальця – і плата автоматично знімається з рахунків батьків.

Так вдалося позбутися від крадіжок і вимагання грошей в учнів, виключити безпосередньо грошові фінансові розрахунки в межах школи, а батькам надавати повний звіт щодо витрат дитини в межах навчального закладу. Крім того, діти із малозабезпечених сімей, яким держава надає допомогу у вигляді різних пільг, під час застосування такої схеми оплати харчування можуть зайвий раз не афішувати свій вразливий соціальний статус[1].

Інноваційні програмно-технологічні рішення розпізнавання індивідуумів за їх обличчям широко використовуються в проектах створення державних систем паспортно-візових документів нового покоління в багатьох країнах, зокрема й в Україні. Нині також розроблені та продовжують розроблятися різноманітні типи рішень у галузі забезпечення безпеки за державними програмами у громадсько-суспільному секторі та в комерційній сфері.

Використання 3D-технологій розпізнання лиця особи здатне забезпечити досить високу точність ідентифікації. Вони також зручні у використанні та дозволяють уникнути процедур, що мають негативний суспільний резонанс, наприклад, як у випадку класичної ідентифікації за райдужною оболонкою ока. Тривимірні технології мають доволі різноманітний спектр застосування: від сфери безпеки і біометричного методу розпізнавання тривимірного зображення обличчя до промислового сканування різних об'єктів, медичної діагностики, судово-медичної експертизи та збереження тривимірних образів археологічних знахідок і музейних цінностей. Сьогодні технології 3D-сканування активно задіяні у вирішенні різних державних завдань і в комерційному секторі. За оцінками фахівців потенціал цього методу не вичерпаний, його застосування буде невпинно розширюватися.

У реальних життєвих ситуаціях підвищені вимоги до безпеки і зручності сьогодні підштовхують найбільш активних користувачів до потреби використання мультибіометричних зчитувачів, а загалом тільки застосування у комплексі можливостей домінуючих біометрик може гарантувати максимальний захист і надійність[2].

Японська компанія «NEC» на початку 2008 року розробила технологію розпізнання лиця людей, що з'являються у кадрах відео. На думку розробників, таке застосування допомагає суттєво полегшити пошук необхідного матеріалу в архівах. Застосовувати це рішення можливо і для розпізнавання осіб у зображеннях, отриманих за допомогою мобільних телефонів, теле-, відеокамер, фотоапаратів, а також «знятих» з Інтернету.

Програма від «NEC» здійснює пошук із будь-яких відеозображень індивідуумів, де є їх обличчя, потім групує отримані дані у спеціальні списки з огляду на отримані коефіцієнти рівня подібності (для цього програма виконує досить складний процес групування зображень людини під різними кутами нахилу голови і за значних відмінностях

[1] Биометрическая идентификация для школ // Pcweek.ru. – 2007. – 23 ноября. [Электронный ресурс]. – Режим доступа: http://pcweek.ru/themes/detail...

[2] Компания НПО «Информация» выступила организатором первой российской конференции разработчиков технологий трехмерного сканирования. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

в освітленості). За відомостями розробника, точність роботи цієї технології поки що становить 80%[1].

За повідомленням агентства «France Presse» у столиці Японії м. Токіо мала бути запроваджена система відеоспостереження, яка заснована на тривимірному розпізнаванні обличчя особи. Вона дозволяє у режимі реального часу здійснювати аналіз лиця осіб, які потрапляють у об'єктиви камер, тобто порівнювати за 3D-технологією отримані фотозображення індивідуумів зі знімками злочинців і терористів, які є у базі даних правоохоронних органів. За виявлення збігу система генеруватиме сигнал тривоги.

Розробка нової системи безпеки здійснюється на замовлення правоохоронних структур Японії низкою компаній і наукових організацій. На реалізацію дослідного варіанта проекта потрібно було близько 110 млн ієн (приблизно один мільйон доларів США). Тестування комплексу мало здійснюватись у 2010 році.

У перспективі, як очікується, тривимірна система відеоспостереження дозволить поліпшити ситуацію з безпекою у громадських місцях і зменшити кількість неприємних інцидентів під час проведення масових заходів.

Прикладом використання систем відеоспостереження з подальшим розпізнаванням індивідуумів є застосування системи замкненого відеоспостереження в м. Ньюхем (невеликого містечка поблизу англійської столиці). У листопаді 1998 року міський комітет Ньюхема ухвалив рішення розгорнути на своїх вулицях комплексну систему відеоспостереження, яка складалась із 206 камер, інтегрованих у систему автоматичного розпізнавання обличчя особи з живого відео «Facelt». Система замкнутого відеоспостереження контролювала найбільш важливі райони міста, відеосигнал, що надходив, негайно в автоматичному режимі оброблявся програмою, яка здійснювала пошук за приєднаним поліцейським банком даних на осіб, що за відомостями правоохоронних структур є злочинцями або підозрювалися у вчиненні злочинів. За певної подібності лиць система сигналізувала оператору, пропонуючи здійснити додаткову перевірку людини і визначитись, чи варто поліції надалі приділяти йому увагу, чи ні. Якщо збігання не відбувалось, то зображення лиця осіб, які були дистанційно відскановані системою для здійснення процедури порівняння, видалялися з пам'яті системи. Підсумки застосування програми розпізнавання вражали: відсоток пограбувань у контрольованих громадських місцях знизився на 21%, заподіяння майнових збитків громадянам зменшилося на 26%, а кількість крадіжок мало безпрецедентне зниження на 39%[2].

Дослідники з Х'юстонського університету (University of Houston) розробили комп'ютерну програму під назвою «UrxD», яка за допомогою технології тривимірних зображень здатна розпізнавати обличчя людей і надавати кожному з них свій унікальний ідентифікаційний біометричний код. Отже, на думку вчених, проблема із запам'ятовуванням безлічі паролів і секретних шифрів може бути вирішена незабаром.

Програма, яка пройшла тестування, може стати в нагоді у найрізноманітніших ситуаціях – від перевірки особистості у кожному конкретному випадку з метою надання доступу до надсекретної державної інформації та використання звичайними покупцями своїх кредитних карток.

Для використання програми потрібно лише сфотографуватися за допомогою спеціально обладнаного комплексу, а далі, за запевненнями дослідників системи, – справа техніки. За заявою розробників програма, «UrxD» набагато ліпша з погляду безпеки за

[1] Биометрическая идентификация по лицу в видеоряде // 3DNews Daily Digital Digest. – 2008. – 23 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

[2] Биометрические системы безопасности // БДИ. – 2002. – № 1 (41). [Электронный ресурс]. – Режим доступа: http://www.iching.ru/6/Bezopasnost-9.html...

системи, де використовують паролі, оскільки підробити зображення обличчя особи набагато складніше, ніж викрасти пароль або підібрати ідентифікаційний PIN-код[1].

Учені різних країн продовжують шукати різні можливості з метою підвищення ефективності ідентифікації за допомогою обличчя. Двоє вчених з Інституту офтальмології при Каліфорнійському університеті розробили цікавий спосіб «запису» зображення обличчя людини у вигляді так званого штрих-коду. Людське обличчя є унікальним ідентифікатором, що дозволяє отримати необхідну інформацію про конкретну персону, наприклад, визначити стать, вік і настрій співрозмовника. Для соціальних істот, якими є люди, вміння «читати за мімікою обличчя» є основою для найрізноманітніших взаємодій. Доктор Стівен Дакін і професор Роджер Ватт виявили, що практично всі дані, що необхідні для успішної ідентифікації людини за допомогою обличчя, містяться у горизонтальних лініях таких, як лінія брів, лінія очей та лінія губ. Здійснені дослідження виявили, що вказану інформацію можна представити у вигляді набору чорних і білих ліній, інакше кажучи, у вигляді штрих-коду. Штрих-код, яким переважно позначаються товари в супермаркеті, володіє низкою переваг, головною з яких є гранична легкість обробки прямих, одновимірних ліній. Обробка двовимірних символів, якими предсталяються в електронному вигляді цифри, становить уже набагато складніше завдання.

Доктор С. Дакін вважає, що це відкриття може використовуватися для вдосконалення існуючих систем розпізнавання рис обличчя, наприклад, таких, які встановлюються в аеропортах і дозволяють виявляти певних осіб у натовпі пасажирів. Останніми роками подібні технології зробили значні кроки вперед, проте поки що існуючі системи не мають необхідної точності ідентифікації осіб у громадських місцях[2].

У другій половині 2013 року Біометричний інститут у Лондоні оприлюднив прогноз щодо сегментації галузевого ринку. Експерти були одностайні в думці про те, що найбільше продаються системи, які реалізують технології ідентифікації за відбитками пальців та обличчя; третє й четверте місця ділять рішення, що розпізнають користувачів за малюнком вен і голосом[3].

[1] Лица против паролей // Washprofile.org/ru. – 2007. – 1 августа. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/6782

[2] Офтальмологи нашли радикальный способ повысить качество биометрической идентификации по лицу. – 2009. – 15 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Биометрический институт опубликовал результаты очередного исследования отраслевого рынка // BIOMETRICS.RU. – 2013. – 6 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розділ 5

ІНШІ МЕТОДИ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ

5.1. Ідентифікація за ДНК

1985 року започаткована методика «ДНК-експертизи». Вчені з Лестерського університету (Великобританія) вперше продемонстрували можливість ідентифікації людини на підставі аналізу її генетичних характеристик. Надалі змінювалися тільки технічні підходи та вдосконалювалося дослідницьке устаткування. Нині технологія вдосконалилася настільки, що дозволяє відбирати взірці та здійснювати аналіз ДНК із застарілих плям крові, плям сперми та волосся.

Вважають, що генетичний аналіз найбільш застрахований від помилок об'єктивного характеру і ненавмисного людського чинника. Для ідентифікації особистості на підставі генетичних характеристик застосовують складне та досить дороге обладнання – автоматизовані генетичні аналізатори, хоча в країнах СНД, зокрема й в Україні, ще досить широко використовуються дешеві старі методи проведення аналізу, що використовують ручні операції. Ручні методи проведення аналізу ДНК, що застосовуються на Україні, вимагають значної кількості часу, тому такі методики використовують, як правило, для спеціалізованих експертиз.

ДНК-дані – це нейтральна інформація, що складається з набору генетичних характеристик. Дезоксирибонуклеїнова кислота (ДНК) – високополімерне природне з'єднання, що міститься в ядрах кліток живих організмів. Разом із білками гістонами утворює речовину хромосом. ДНК – носій генетичної інформації, її окремі ділянки відповідають певним генам. Молекула ДНК складається з двох полінуклеотидних ланцюжків, які закручені один навколо іншого в спіраль. Будова ланцюжків складається з великої кількості мономерів чотирьох типів – нуклеотидів, специфічність яких визначається одним із чотирьох з'єднань на основі азотистих сполук (аденін, гуанін, цитозін, тимін).

Сполучення трьох поряд розташованих нуклеотидів у ланцюжок ДНК (триплети або кодони) становлять генетичний код будь-якої живої істоти. Порушення послідовності розташування нуклеотидів у ланцюжку ДНК призводить до спадкових змін в організмі – мутацій. ДНК точно відтворюється під час ділення клітин, що забезпечує передачу спадкових ознак і специфічних форм обміну речовин у наступних поколіннях клітин і організмів[1].

У передових спеціалізованих лабораторіях центрів судово-медичної експертизи СНД, особливо в Російській Федерації, замість ручних методик уже починають застосовувати генетичні аналізатори третього покоління. Ефективність цих приладів полягає

[1] Советский энцеклопедический словарь. – 3-е изд. – М.: Сов. энциклопедия, 1984. – С. 367.

у суттєвому підвищенні їх можливостей завдяки значному підвищенню чутливості: з початком їх використання для проведення експертизи виявились доступними мікрослідиі крові, слини та інших біологічних матеріалів, що раніше були недоступними для попередніх методик.

Як зрозуміло з самої назви генетичної експертизи, вона працює з генетичним матеріалом. Його джерелом є клітинна структура – тканини організму. На результати експертизи істотно впливають чинники зовнішнього середовища. ДНК хоч і стабільна молекула, але схильна до руйнування під дією ультрафіолетових променів, агресивних середовищ. У потожирових виділеннях, наприклад у відбитку пальця на склі, можна жодного генетичного матеріалу і не знайти. Ще один приклад: термічне руйнування в результаті кремації або сильної пожежі. Якщо всі тканини живої істоти згоріли і залишилася тільки мінеральна структура, а жодної органіки немає, то за цими залишками нічого встановити не можливо.

Принцип генетичної ідентифікації полягає у встановленні максимальної кількості генетичних ознак. Чим їх більше встановлено, тим достовірніше проведене досліджування. Іноді кількості отриманих ознак просто недостатньо, щоб можна було б говорити про достовірний результат. Нині одна з найбільш значущих проблем ДНК-методу і полягає якраз у тому, що не всі з цих генетичних ознак повністю індивідуальні та унікальні. Тому існує ймовірність помилки. Цей метод вимагає дуже високої кваліфікації судмедекспертів.

Вплив суб'єктивного чинника надзвичайно великий через: некфаліфікований підхід можна допустити помилку, яка буде критичною для слідства та суду, зважаючи на високу достовірність цього методу. Нині метод генетичної ідентифікації володіє найвищою доказовістю та найвищою ефективністю серед методів аналізу слідів біологічного походження. Суди сприймають результати ДНК-експертизи дуже серйозно, тому ступінь відповідальності експерта надзвичайно високий, а сама ця робота вимагає строгого контролю.

Проблема полягає ще й у тому, що не існує єдиного державного стандарту якості, кожен експерт працює як «може», а тому виникають можливості здійснення неякісного аналізу. На практиці це виявляється в можливості скерування зразків у лабораторії, де фахівці достатньо професійно кваліфіковані, але не виключається можливість представлення зразків для проведення досліджень у генетичні лабораторії, де підбір кадрів менш професійний[1].

У принципі можливий варіант, коли згодом ДНК-параметри будуть вноситися в посвідчення осіб, у так звані геномні паспорти з біочіпами, що означатиме створення відповідних ДНК-банків даних. Тільки в разі створення ДНК-баз даних геномна ідентифікація буде належно використовуватися і, як наслідок, зможе ще більше сприяти підвищенню рівня розкриття злочинів. Нині генетична експертиза не є панацеєю від злочинності, а ще одним кроком для боротьби з нею.

Прикладом ефективності генетичних тестів є перегляд розкритих у минулому кримінальних справ у США. Вчені з США провели свого часу новий розглядрозслідування розкритих кримінальних справ тих часів, коли у підозрюваних не відбиралися ДНК-зразки. Вони зробили шокуючий висновок: за підсумками їх розслідувань за допомогою ДНК-методу з в'язниць негайно слід було звільнити 208 жертв судових помилок, причому 15 із них перебували в камері смертників. За даними «Innocent Project» –

[1] ДНК привлекают в свидетели // Независимая газета. – 2008. – 22 апреля. [Электронный ресурс]. – Режим доступа: http://www.ng.ru/society/...

організації, яка допомагає жертвам судових помилок у США, – більшість чоловіків сиділи за звинуваченням у зґвалтуванні – злочині, що особливо легко розкривається за допомогою дослідження ДНК-підозрюваного. В середньому кожен із помилково засуджених провів за ґратами 12 років, а 15 осіб було засуджено до вищої міри покарання.

Робота з перегляду розкритих кримінальних справ у США, де 2,3 млн чоловік перебувають у місцях позбавлення волі, зумовила помітні зрушення у діяльності органів правосуддя. 42 штати зробили ДНК-тести під час розслідування злочинів обов'язковою процедурою. Понад 500 установ правоохоронних органів змінили звичайну практику проведення допитів: тепер дізнавач обов'язково повинен записувати весь допит на відео, щоб потім можна було об'єктивно встановити, за яких обставин були отримані свідчення, що доводили вину обвинувачених[1].

У Сполученому Королівстві Великобританія вперше у світовій криміналістичній практиці для відтворення зовнішності злочинця використовують ДНК-аналіз, який дозволяє правоохоронним органам отримати опис зовнішності порушника за особливостями його генного коду.

Британські криміналісти звернулися до цієї революційної технології з метою проведення досліджень крапель крові, лупи, лусочок відмерлої шкіри, волосся, що випало, або вій, які виявляють на місцях злочинів. За їх твердженням, середньостатистична людина залишає після себе величезну кількість слідів – ледве помітних неозброєним оком частинок, кожна з яких містить колосальний обсяг інформації. Серед відомостей, які можливо буде отримувати так, британці називають ріст, вагу, комплекцію, форму підборіддя, носа, вух, висоту лоба та колір очей. Якщо колір очей вже визначають достатньо точно, то з кольором волосся складніше – поки ДНК-аналіз надає інформацію лише про те, чи є людина рудоволосою. Однак скептики відзначають, що «природний відбір» і життєві обставини можуть настільки змінити зовнішність, що, наприклад, після якої-небудь вуличної колотнечі підозрюваного і «рідна мати не впізнає»[2].

Ідентифікація особи за методом ДНК-аналізу успішно використовується у Великобританії, США, Канаді та низці інших країн. У деяких країнах СНД готуються проекти законів «Про державну геномну реєстрацію». А в Російській Федерації Державна дума в IV кварталі 2008 року узаконила введення в країні державної геномної реєстрації – ДНК-аналізу. Розробники цього документа з МВС вважають, що це повинно підвищити ефективність боротьби зі злочинністю, зокрема з тероризмом і екстремізмом.

У законі виписані механізми отримання, зберігання та використання геномної інформації для ідентифікації особи. Має бути утворена федеральна база даних ДНК-інформації за невпізнанними трупами, невстановленими особами, біологічний матеріал яких вилучений під час слідства. У ДНК-базі свої генні сліди також повинні залишити підозрювані у вчиненні тяжких злочинів і всі засуджені за вироком суду. Крім того, передбачена обов'язкова генна реєстрація представників небезпечних професій, насамперед військових, МНС і МВС. У разі надзвичайної події вона дозволить ідентифікувати загиблого або тяжкопораненого, який не в змозі повідомити своїх даних. Розробники документа передбачили і можливість добровільної здачі громадянами своїх ДНК у тих випадках, коли люди захочуть підстрахувати себе або своїх близьких. Але така процедура буде платною, причому досить не дешевою. Адже один апарат – секвентор, який дозволяє виокремлювати ДНК із біологічних зразків, коштував у 2008 році майже 500 тис доларів.

[1] ДНК-тест реабилитирует несправедливо осужденных // Cnews.ru. – 2007. – 12 апреля. [Электронный ресурс]. – Режим доступа: http://rnd.cnews.ru/tech/biotech/news/...

[2] Преступников будут искать по анализу ДНК. – 2001. – 17 декабря. [Электронный ресурс]. – Режим доступа: http://www.membrana.ru/articles/inventions/...

Однак доступ до відомостей цієї бази даних буде обмежений. Таке право нададуть судам, органам дізнання, попереднього слідства й оперативним працівникам правоохоронних структур. Загалом у РФ налічуються 35 лабораторій, де проводять ДНК-аналіз. 2007 року з їх допомогою було розкрито більше тисячі злочинів, зокрема низки тяжких у Москві та Башкирії[1].

Прикладом використання генетичної ДНК-бази даних є Національний ідентифікаційний регістр (National Identity Register /NIR/) біометричних відомостей громадян Великобританії, який серед інших відомостей містить дані ДНК-зразків на 4,5 млн осіб, зокрема приблизно на 900 тис. дітей (відомості 2007 року). У британському NIR містяться відомості про тих громадян, що, починаючи з 2004 року, були заарештовані на території Англії й Уельсу (незалежно від причин затримання)[2].

Федеральне бюро розслідувань (ФБР /FBI/) США має широкі можливості з розпізнавання (forensic capabilities) осіб, що мають відношення до тероризму в світовому масштабі. Однією з найважливіших можливостей вважається ДНК-тестування. Точна ідентифікація окремих людей, причому і живих, і мертвих, необхідна. Для цього ФБР створює велику колекцію генетичних зразків (DNK-samples) для ідентифікації індивідуумів або для встановлення особи невпізнанних трупів, що виникають унаслідок конфліктних ситуацій. Наприклад, ДНК-тестування підтвердило висновок пакистанського уряду про те, що M. M. M. Atwah, бойовик «Аль-Каїди», який розшукувався США у зв'язку з вибухами в американських посольствах у 1998 році, був убитий під час повітряного нальоту пакистанськими військовими поблизу кордону з Афганістаном.

ДНК-тестування з погляду однозначної ідентифікації дедалі більше застосовується як остання інстанція під час встановлення особистості. Наприклад, незважаючи на те, що тіло A. M. al Zarqawi (Заркаві – відомий діяч «Аль-Каїди») після повітряного удару було ідентифіковано за відбитками пальців, татуюванням та шрамами, ДНК-зразок був скерований у криміналістичну лабораторію ФБР для ухвалення остаточного висновку щодо ідентифікації особи загиблого[3].

В Іраку командування американських окупаційних військ створювало базу ДНК на громадян країни, які мають доступ на територію американських баз або працюють у державних силових структурах.

В Україні Міністерство внутрішніх справ розробило концепцію державної цільової програми на 2009–2013 роки, що передбачала створення національної бази ДНК. Крім того, концепція передбачала кардинальне підвищення рівня експертного забезпечення діяльності правоохоронних органів із запобігання, виявлення, розкриття та розслідування злочинів проти життя, здоров'я, свободи, недоторканності людини, а також інших злочинів і правопорушень. Крім того, концепція повинна сприяти вирішенню питань автоматизації й удосконалення різних етапів ДНК-аналізу, а також застосуванню стандартних загальносвітових наборів реактивів для ідентифікації особи. На першому етапі в національну базу ДНК заплановано включити відповідні відомості щодо злочинців, потерпілих і невпізнанних трупів людей.

---

[1] В России создается база «генных паспортов» преступников, военных и простых граждан // Российская газета. – 2008. – 27 ноября. [Электронный ресурс]. – Режим доступа: http://secuteck.ru/newstext.php

[2] Британия. Всё большее число граждан поддерживает распространение биометрических идентификационных карт // BIOMETRICS.RU. – 2007. – 12 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Новые средства получения разведданных о террористах // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 4.

Реалізація положень концепції має на меті створення єдиної мережі баз даних ДНК міжрегіональних лабораторій з автоматизованим обліком ДНК особистостей, які обґрунтовано підозрюються та звинувачуються у вчиненні злочинів, обвинувачених, які засуджені судами, або осіб, що у встановленому порядку утримуються під вартою. Створення національної бази ДНК залежало від схвалення Кабінетом Міністрів цієї концепції, на реалізацію якої свого часу були необхідні кошти у розмірі понад 155 млн гривень[1].

На час написання посібника українська база даних зразків ДНК так і не створена. Хоча правоохоронним органам вкрай необхідна єдина Національна база обліку генетичних ознак людини. Про це у лютому 2013 року заявив перший заступник начальника Головного слідчого управління МВС України Олександр Гончаров під час круглого столу за участю представників Генпрокуратури, міністерств охорони здоров'я, юстиції, СБУ і вчених.

Як повідомляє прес-служба МВС, О. Гончаров зазначив, що створення такої бази «стримується через відсутність чіткого законодавчого врегулювання цього питання і недостатню кількість та малу пропускну спроможність наявних ДНК-лабораторій.

О. Гончаров закликав присутніх «проявити державний підхід та максимально сприяти затвердженню Концепції Державної цільової програми розширення мережі ДНК-лабораторій і створення Національної бази даних генетичних ознак людини для використання в оперативно-службовій діяльності ОВС на 2014–2020 роки».

Заступник начальника Головного слідчого управління МВС зазначив, що ДНК-аналіз дозволяє зі стовідсотковою ймовірністю ідентифікувати особу злочинця й ефективно довести його причетність до вчинення протиправних дій[2].

Цікавим є прогноз аналітиків із «Futuretimeline.net» на 2014 рік щодо технології розшифрування ДНК людини.

Вони стверджують, що технологія розшифрування генома людини дешевшає настільки стрімко, що незабаром ДНК будь-якого індивідуума можна буде розшифрувати всього за кілька годин і все це буде коштувати менш 100 доларів! Це стало можливим завдяки появі нової революційної наноструйної технології.

Аналітики стверджують, що з 2014 року методи лікування у провідних західних країнах будуть підбиратися строго індивідуально – відповідно до конкретного генетичного коду кожного пацієнта.

Наприклад, лікар проводить біопсію злоякісної пухлини, розшифровує її ДНК-код і використовує отриману інформацію для діагнозу та вибору методики лікування. Ще раз акцентуємо, що все це буде коштувати менш 100 доларів!

Якщо в пацієнта було діагностовано рак легенів, лікар зможе виявити всі генетичні зміни в клітинах злоякісної пухлини та вибрати найбільш дієвий варіант хіміотерапії. У батьків немовлят з'явиться можливість визначати ймовірність розвитку в малят багатьох захворювань і, наприклад, у разі схильності до розвитку діабету вибрати для дитини правильне харчування з першого дня життя, що виключить можливість переходу хвороби у важку стадію[3].

---

[1] У Луценко хотят создать национальную базу ДНК // Proua.com. – 2009. – 8 июля. [Электронный ресурс]. – Режим доступа: http://proua.com/news/...

[2] Міліція хоче створити єдину базу ДНК українців // Дзеркало тижня. – 2013. – 28 лютого. [Електронний ресурс]. – Режим доступу: http://dt.ua/UKRAINE/

[3] Василькевич Константин. Заглянем чуть дальше / К. Василькевич // Еженедельник-2000. – Вып. № 3 (638). – 2013. – 18–24 января. [Электронный ресурс]. – Режим доступа: http://2000.net.ua/2000/derzhava/realii/87273

Агентство національної безпеки (АНБ) США приділяє значну увагу розвитку можливостей пришвидшеної ідентифікації за ДНК. Разом із Національним інститутом стандартів і технологій (National Institute of Standards and Technology /NIST/) АНБ є здебільшого спонсором щорічних конференцій Біометричного консорціуму. Зокрема, NIST й АНБ спонсурували щорічну конференцію цього консорціуму, яка проходила з 27 до 29 вересня 2011 року в Центрі конгресів у місті Тампа (штат Флорида). Питання пришвидшеної ідентифікації за геномом людини аналізувалося на цьому заході у форматі панельної дискусії[1].

Група фахівців із Технологічного університету Окленда, Нова Зеландія, у 2013 році представила діючий прототип біометричної системи контролю й управління доступом (СКУД) нового покоління, де як основні біометричні характеристики використовується код ДНК.

Інформація генетичного коду в зчитувачі перспективної СКУД одержується з людської слини методом полімерної ланцюгової реакції. На практиці це виглядає так: людині потрібно взяти з термінала спеціальну одноразову «марку», лизнути її та помістити в одноразовий пластиковий контейнер, а його вставити в приймальне відділення термінала.

Ймовірність неправильного позитивного рішення для такої системи контролю й управління доступом становить менш 0,001%, що дозволяє використовувати такий продукт у сферах допуску з найвищими вимогами до надійності. За словами розробника прототипу Вирему Макдоналда основними ринками для нового класу СКУД можуть стати державний та фінансовий сектори.

Наприклад, аналіз ДНК може забезпечити доступ до банківського сховища чи секції архіву, що містить секретні документи.

Оскільки у багатьох країнах існують бази даних ДНК злочинців (зокрема з анонімними зразками), ДНК-СКУД могла б працювати за правилом так званого «чорного списку».

На жаль, поки що розробка є лише працюючим прототипом, яка не готова для комерційного впровадження. Головна причина – дуже низька швидкість роботи. «На сьогоднішній день (квітень 2013 року) в окремих випадках зчитувач обробляє один екземпляр біоматеріалу до 3-х годин», – зізнається В. Макдоналд. Крім того, вартість необхідних матеріалів для проведення одного аналізу становить 197 фунтів стерлінгів (однак у разі масового впровадження вартість процедури має бути значно нижчою). Але розробники сподіваються на комерційний успіх. Доведенням продукту до практичного використання надалі буде займатися компанія «Dnaccess Ltd»[2].

Останнім часом матеріалів у ЗМІ щодо нових досягнень ДНК-аналізу майже нема. Але навіть та невелика кількість, яку публікують, свідчить про те, що триває наполеглива робота у цьому напрямі.

Якщо вдасться суттєво зменшити час обробки одного біоматеріалу та здешевити вартість цієї процедури, то правоохоронні органи отримають досить надійний метод встановлення осіб, який особливо буде застосовуватися для розкриття тяжких злочинів, зокрема зґвалтувань.

---

[1] Национальный институт стандартов и технологий стал спонсором конференции Биометрического консорциума // BIOMETRICS.RU. – 2011. – 17 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

[2] Для биометрических систем контроля доступа разработана новая технология. – 2013. – 1 апреля. – Security News. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

5.2. Ідентифікація за зображенням кисті руки

Ідентифікація за геометрією кисті руки має ще одну назву – ідентифікація за формою долоні. Цей метод ідентифікації для розпізнавання використовує геометрію кисті руки. За допомогою спеціального пристрою, який складається з відеокамери та декількох діодів, що застосовуються для підсвітки (включаючись по черзі, вони дають можливість одержувати різні проекції форм долоні), формується тривимірне зображення кисті руки, з якої отримується згортка та здійснюється розпізнавання людини. Не слід плутати цей спосіб з іншим варіантом розпізнавання, де також використовується долоня руки – за розташуванням вен на лицьовій стороні долоні. У цьому варіанті розпізнання за допомогою інфрачервоної камери зчитується малюнок вен на лицьовій стороні долоні, а одержана картинка обробляється спеціальним чином, і за отриманою схемою розташування вен формується цифрова згортка зображення[1].

Ідентифікація за формою кисті руки використовується майже 30 років. Для того, щоб здійснити процедуру ідентифікування людини, системі досить зняти фізичні характеристики пальців або долоні руки такі, як довжина, ширина, товщина і поверхневі параметри зазначеної частини руки. Водночас проводиться оцінка понад 90 різних характеристик, починаючи з розмірів самої долоні (три вимірювання), довжини та ширини пальців, контурів суглобів тощо[2].

Суттєвою відмінністю цієї технології, яка на практиці становить особливий інтерес, є досить малий об’єм електронного шаблону біометричного зразка, за допомогою якого здійснюється процес розпізнання – лише декілька байтів[3].

Спосіб аутентифікації, заснований на аналізі зображення долоні руки, використовувався досить широко на рубежі XX і XXI століть (близько 25% пристроїв у 1999 році і близько 10% в 2001-му), але, як показала практика, він виявився не дуже надійним. Це пов’язано насамперед із великою варіабельністю форми кисті як протягом усього життя людини, так і у більш короткі терміни. Певним плюсом є малий розмір математичного «опису» долоні руки – близько 10 байт (за останніми уточненими даними – не більше 9 байт)[4].

Однак це і є водночас додатковим підтвердженням досить малої надійності цього методу: наявної інформації недостатньо для всіх можливих описів варіантів форми кисті, якими природа наділила людей[5].

2002 року в Росії набув відносно поширення пристрій «HandKey» (Хендкей), який використовує як ідентифікаційну ознаку параметри долоні руки. Цей пристрій трохи більший за телефонний апарат і є конструкцію з нішею, куди особа, яку перевіряють, під час здійснення процесу ідентифікації вміщує кисть своєї руки. Пристрій також має мініклавіатуру та рідиннокристалічний екран, на який виводяться відомості щодо

[1] Технологии. Методы биометрической аутентификации. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp

[2] Борзенко А. Биометрические технологии / А. Борзенко // Bytemag.ru. – 2001. – 10 октября. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/

[3] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art103.html

[4] Биометрические системы безопасности // БДИ. – 2002. – № 1 (41). [Электронный ресурс]. – Режим доступа: http://www.iching.ru/6/Bezopasnost-9.html

[5] Мифы биометрии. [Электронный ресурс]. – Режим доступа: http://www.cbio.ru/v5/modules/news/article.php; http://universalkey.boxmail.biz/cgi-bin/guide.pl

проходження ідентифікації. Достовірність особи визначається за фотозображенням долоні (у цифровому вигляді), водночас знімок руки порівнюється з еталоном. Під час проведення реєстраційної процедури індивідуумові надається персональний код, який вноситься в базу даних.

У разі поміщення долоні руки в «HandKey» вона фотографується в ультрафіолетовому випромінюванні в трьох проекціях. Сформований електронний образ обробляється процесором пристрою, інформація стискується до дев'яти байт, які можна зберігати в базі даних і передавати комунікаційними системами. Загальна тривалість усієї процедури становить від 10 с до 1 хв, хоча сама ідентифікація потребує 1–2 с. За цей час хендкей звіряє характеристики кисті руки з наявними в базі даних відомостями, а також перевіряє можливі обмеження користувача. Під час проведення кожної перевірки інформація, що зберігається у пам'яті пристрою, автоматично оновлюється, а відтак усі зміни, які сталися з долонею руки, постійно фіксуються.

«HandKey» може працювати і в автономному режимі, за якого він здатний запам'ятовувати до 20000 різних образів долоней рук. У його пам'яті може зберігатися календарний план на рік, в якому з точністю до хвилини можна зазначити, коли тому або іншому клієнтові дозволений доступ. Конструктори пристрою передбачили і можливість його роботи з комп'ютером, підключення до схем управління замком, налаштування його на емуляцію стандартних пристроїв зчитування кредитних карт, а також приєднання принтера для ведення протоколу роботи. У мережевому режимі до хендкею можна підключити до 31 зовнішнього пристрою з загальною довжиною лінії (вита пара) до 1,5 км. Не можна не повідомити і про таку особливість пристрою, як можливість його вбудування у вже існуючі системи управління доступом. Основний виробник «HandKey» – компанія «Escape»[1].

2002 року в США пристрої для зчитування зображень долонь були встановлені більш ніж на 8 000 об'єктах. Один із варіантів «Handkey» сканував і внутрішню, і зовнішню сторони долоні, використовуючи для цього вбудовану в пристрій відеокамеру й алгоритм стискання отриманої інформації. Пристрої, які могли сканувати й інші параметри руки, розроблялися декількома компаніями, зокрема такими, як «BioMet Partners», «Palmetrics» і «BTG»[2].

2007 року геометрія кисті руки використовувалась для ідентифікації користувачів у системі контролю управлінням доступу в 379-ому експедиційному корпусі американських військово-повітряних сил (ВПС). Біометричну ідентифікацію проходили насамперед представники місцевого населення тих країн, де розташовувалися частини експедиційного корпусу, і які працювали на території американських баз.

Персональні дані та відомості про біометричні ідентифікатори осіб, які перевіряються, надсилаються у спеціальний підрозділ Міністерства оборони США – Центр обробки біометричних даних (Biometric Fusion Center /BFC/), що розташований у Західній Вірджинії. 379-й експедиційний корпус свого часу був найбільшим підрозділом американських ВПС, що діяли за межами США. Частини корпусу були задіяні та досі використовуються у багатьох операціях, зокрема й на територіях Іраку та Афганістану[3].

---

[1] Барсуков В. С. Биоключ – путь к безопасности / В. С. Барсуков // Специальная техника. – 2007. – 6 июля. [Электронный ресурс]. – Режим доступа: http://www.vashdom.ru/articles/st_14.htm

[2] Биометрические системы безопасности // БДИ. – 2002. – № 1 (41). [Электронный ресурс]. – Режим доступа: http://www.iching.ru/6/Bezopasnost-9.html...

[3] На базе американских ВВС внедрена биометрическая система контроля доступа // BIOMETRICS.Ru. – 2007. – 16 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Наприкінці першого десятиріччя XXI століття розпізнавання за геометрією долоні в основному розглядалась як доповнювальна технологія. Вона використовувалась одночасно з іншими біометричними системами контролю, коли потрібно забезпечити особливий рівень безпеки доступу[1].

За період із 2009–2013 роки автори посібника не знайшли нових повідомлень щодо використання в системах ідентифікації методу геометрії долонь. Найімовірніше, що цей метод поступово витиснив так званий «Vein»-метод. Словом «Vein» (його буквальне значення «кровоносна судина») у закордонних публікаціях позначають методи ідентифікації осіб за малюнком вен.

Нині на ринку технологій ці методи представлено двома конкуруючими технологіями: ідентифікацією за малюнком вен на долоні й ідентифікацією за малюнком вен на пальці. Розглянемо ці методи у наступному підрозділі.

5.3. Безконтактна ідентифікація за малюнком вен долоні або пальця руки, а також термограми обличчя особи

Технологія ідентифікації людини за венами долоні була розроблена компанією «Fujitsu» через зростання кількості фінансових махінацій в Японії. Цей ідентифікаційний спосіб був обраний внаслідок його безпрецедентного ступеня захисту від підробок і відсутністю проблем, які характерні іншим біометричним технологіям. Розташування вен на долоні кожної людини унікальне, як і відбитки папілярних узорів пальців. Індивідуальний капілярний малюнок долоні закладається на стадії формування плоду людини в утробі матері та не змінюється впродовж усього життя. Пошкодити або імітувати малюнок вен неможливо, оскільки вони є всередині тканин кисті руки. Під час проведення ідентифікації не має необхідності у фізичному контакті людини зі скануючим пристроєм, через що цей метод найбільш прийнятний у медичній та фармацевтичній сферах, де питання гігієни має найважливіше значення[2].

За кордоном цей метод, як вже зазначалося, отримав назву «Vein»-методу. Доведено, що малюнок вен на долоні не змінюється з дворічного віку індивідуума. Практично співіснують дві конкуруючі технології: ідентифікація за малюнком вен на долоні та ідентифікація за малюнком вен пальця. В обох випадках сканування відповідної частини людського тіла здійснюється в інфрачервоному діапазоні. Кров, яка тече у венах, збіднена киснем і тому поглинає інфрачервоні промені, а інші ділянки долоні (або пальця) ці промені відбивають[3].

Суть цього способу полягає у безконтактній реєстрації за допомогою приймача інфрачервоного випромінювання малюнка венозних судин долоні або пальця. За

[1] Кюн Мэнди. Защита доступа биометрическими методами / Мэнди Кюн // LAN. – 2007. – 2 октября. [Электронный ресурс]. – Режим доступа: http://biometrics. ru/document.asp…

[2] Разработано программное обеспечение для сканера рисунка вен на руке. – 2007. – 23 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Митин Владимир. Биометрические технологии, которые мы выбираем / В. Митин // PC Week/RE. – 2010. – 9 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics. ru/document.asp…

дослідженнями, проведеними компанією «Fujitsu», просторова структура вен є унікальною навіть для однояйцевих близнят і не змінюється впродовж усього життя. Від дворічного віку до зрілого вона тільки пропорційно збільшується, що дає можливість використовувати це зображення як біометричний ідентифікатор будь-якого індивідуума. Зчитувати просторову картину розташування вен допомагає кисень у гемоглобіні венозної крові, кількість якого, власне, і реєструється протягом однієї-двох секунд за допомогою інфрачервоного датчика. Ця технологія розпізнає картину орнаменту вен тільки живої людини, оскільки прив'язана до певної концентрації гемоглобіну в крові[1].

За публікацією 2005 року в німецькому журналі «LAN», сканування знизу долоні попереджає проблеми, які можуть з'явитися в деяких випадках через волосяний покров або колір шкіри. За повідомленнями цього ж журналу, біометричне зображення ефектронного шаблону має розмір близько 3 Кб., що дає можливість легко розмістити його на смарт-картці.

Ще однією перевагою є конструкція самого датчика, що передбачає використання руху, необхідного для аутентифікації, котрий подібний до вітання рукою, який поширений на заході. Принаймні цей жест не викликає жодних негативних асоціацій[2].

За інформацією інженерів із «Fujitsu Laboratories», для отримання виразної картини орнаменту вен користувачеві, який ідентифікується, потрібно лише витягнути руку в напрямі сканера і пройти повз пристрій звичайною «пішохідною» швидкістю (близько 1 м/с). На отримання «Vein»-шаблону затрачається не більше однієї мілісекунди. Із подібною системою добре «знайомі» клієнти японського метро. Для того, щоб оминути загороджувальний турнікет, їм потрібно провести перед датчиком особливою безконтактною смарт-карткою[3].

За оцінкою розробника, властивості нової технології дають право на її висунення в лідери біометричних засобів аутентифікації за використовуваними характеристиками – насамперед за надійністю, захищеністю та оперативністю.

На думку фахівців, біометрія малюнка вен руки людини дуже перспективна. Точність подібного методу ідентифікації надто висока, оскільки форма малюнка вен у людини не змінюється впродовж усього життя. Ще одна перевагав технології – її безконтактність. Тобто, з одного боку, ця система ідентифікації найбільш захищена від можливості підробки, з іншого ж, такий метод ідентифікації гігієнічніший за найпоширеніший нині – за відбитками пальців. На думку одного з директорів фірми «NeuHaus» (компанія представляє інтереси «Fujitsu» на території Росії) Ігоря Артанова, біометрика малюнка вен може застосовуватися скрізь, де сьогодні використовуються технології за відбитками папілярних узорів пальців. Системи захисту, які застосовують біометрику долоні, використовуються в СНД на режимних об'єктах, де доступ суворо контролюється, наприклад, у сфері контролю доступу на об'єкти атомної енергетики. В Японії біометричні системи на базі малюнка вен руки людини вже використовуються для забезпечення контролю доступу в закриті зони японських аеропортів[4].

---

[1] Вашу руку! // PC Week. – 2007. – 26 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Йоханнес Вилле. Новые пути биометрии / Вилле Йоханнес // LAN. – 2005. – № 11. [Электронный ресурс]. – Режим доступа: http://www.osp.ru/lan/...

[3] Разрабатывается новая технология биометрической идентификации по рисунку вен на ладони. – 2009. – 24 июля. – SecurityLab.ru. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Кресп О. Венные карты / О. Кресп // ComNews. – 2007. – 19 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Технологія компанії «Fujitsu» («PalmSecure») має впровадження у різних сегментах бізнесу. Так, «Bank of Tokyo Mitsubishi UFJ» і «Suruga Bank» в Японії, а також бразильський «Banco Bradesco» застосували її для організації доступу до банківських касових терміналів і банкоматів, а також для обслуговування VIP-клієнтів. У японському «National Institute of Radiological Sciences» нову технологію використовують під час роботи з репозиторієм клінічних даних, для дотримання необхідних доз опромінювання електронами і важкими іонами хворих, для управління доступом до системи радіологічної інформації. У «Todholm Primary School» (Шотландія) рішення на базі «PalmSecure» використовуються для безготівкового розрахунку за сніданки у шкільному буфеті.

У СНД технологія представлена комплектом розробника, до якого входить інфрачервоний датчик «PalmSecure» і програмний інструментарій для створення рішень на базі «Vein Recognition Technology». Цей комплект у Російській Федерації просуває компанія «Нойхаус Груп», офіційний дистриб'ютор «Fujitsu» в Росії та інших країнах СНД[1].

Біометрична технологія безконтактної системи ідентифікації особистості за малюнком вен на долоні людини «PalmSecure» за наявними даними не була стандартизована, в зв'язку з чим експерти висловлюють сумнів у тому, що рішення на базі «PalmSecure» незабаром зможуть стати масовопоширеними. Але очікується, що попит на біометричні системи, які працюють за принципами цієї технології, збільшиться.

За повідомленням російського біометричного порталу «Biometrics.ru», російське НВО «Інформація» адаптує і просуває на ринку Росії системи безпеки з використанням розробки японської компанії «PalmSecure». На думку російських розробників, технологія «PalmSecure» може застосовуватися у системах для проведення моніторингу робочого часу, управління доступом у будівлі та споруди, надання доступу в різноманітних комп'ютерних системах, зокрема і за контролем доступу в Інтернет[2].

На території СНД поки що, в основному, замовниками біометричних систем за малюнком вен на долонях є державні структури, але, як очікувалося, з 2010 року розпочнеться формування масового ринку. Незважаючи на те, що біометрична технологія за «Vein»-методом дозволяє досягти дуже високого ступеня точності ідентифікації та захищеності від підробок, точність систем розпізнавання на основі цього методу через недосконалість існуючої апаратури все ще потребує удосконалення[3]. Але з 2010 року пристрої систем розпізнавання, що створювалися на базі цього біометричного параметра, почали досягати необхідної точності.

Розглянемо принцип дії такої біометричної системи та її апаратний склад на прикладі програмного забезпечення для біометричного безконтактного зчитувача вен долоні компанії «Аплана», який розроблений на замовлення англійської компанії-постачальника систем контролю та управління доступом «TDSi».

До системи входить зчитувач (сканер) із пристроями доступу до біометричної бази даних і робоче місце адміністратора сервера з центральною базою даних (у випадку не дуже великого обсягу інформації у базі даних (БД), що використовується, можливий і варіант розміщення даних бази безпосередньо на комп'ютері, який обслуговує сканер). Для підвищення рівня захищеності системи біометрична інформація може бути також розміщена на безконтактні смарт-картки. Програмний продукт реалізований із використанням найпоширеніших інтерфейсів передачі даних, що дозволяє застосовува-

[1] Вашу руку! // PC Week. – 2007. – 26 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Кресп О. Венные карты / О. Кресп // ComNews. – 2007. – 19 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Там же.

ти його в комплексі з широким спектром пристроїв, які випускаються основними світовими виробниками.

Біометричний сканер працює за принципом використання ближнього діапазону інфрачервоного світла, яке рівномірно розповсюджується за всією поверхнею кисті руки без жодного фізичного контакту. Ця розробка характеризується низькою ймовірністю допущення помилок, що становить 0,01%, водночас показник неправильно зчитуваних даних – 0,00008%[1].

Основним конкурентом методу вен долоні є технологія безконтактної ідентифікації за малюнком вен на пальці, розробку якої з 1997 року здійснює Центральний дослідницький інститут компанії «Hitachi». За цей час фірма захистила свою розробку низкою патентів у цій сфері досліджень. Із 2007 року компанія «Hitachi» почала продаж системи, яка отримала назву «Finger Vein». Принцип дії сканера на основі технології «Finger Vein» заснований на формуванні зображення малюнка вен будь-якого пальця особи, що обробляється за допомогою спеціального алгоритму та перетворюється на цифрову модель-згортку. Її, своєю чергою, можна зберігати у базі даних і надалі використовувати для порівняння з цифровою моделлю малюнка вен пальця особи, який отримується під час спроби доступу індивідуума до об'єкта, що контролюється відповідною системою безпеки. Як об'єкти, що підлягають захисту, фахівці «Hitachi» називають автомобілі та персональні комп'ютери. Цей засіб ідентифікації вбудовується у різні системи контролю фізичного доступу, зокрема до банкоматів, і використовується для персональної ідентифікації.

Розробники стверджують, що через фізіологічні особливості людського організму малюнок вен на пальці, як і на долоні, практично неможливо підробити, що є найбільшою перевагою цього методу ідентифікації. Вважається, що розташування венозних судин у середині тканин частин тіла особи, яку ідентифікують, повинно унеможливити несанкціоноване (без відома та згоди суб'єкта) отримання інформації щодо малюнка вен на пальці. До переваг сканера «Finger Vein» його виробники відносять той факт, що процес ідентифікації здійснюється безконтактним способом, як і в аналогічному методі розпізнання осіб за малюнком зображення вен на долоні.

Найоб'ємніші постачання фірма «Hitachi» здійснила фінансовим інститутам Японії. У 80% банкоматів, які розташовані на території країни, що використовують біометричну ідентифікацію, застосовуються саме сканери зображень малюнків вен пальців. Загалом помічається зростання продажу сканерів типу «Finger Vein» у Південно-Східній Азії (особливо в Сінгапурі). «Hitachi» очікує також активного застосування сканерів малюнка вен на пальці в системах контролю фізичного доступу фінансових установ на території США (нью-йоркське відділення «Shinkin Central Bank») та Європи. Мінімальні перспективи обсягу щорічного продажу сканерів «Finger Vein» одним тільки компаніям, що діють у сфері інформаційної безпеки, компанія «Hitachi» оцінює в 10 тис штук[2].

Улітку 2009 року «Hitachi» анонсувала створення модуля ідентифікації особи за судинним малюнком пальця завтовшки 3 мм. Порівняно з уже існуючими продуктами компанії, для яких цей параметр становить 23,5 мм, новий пристрій у сім разів тонший. Повний розмір – 30 × 25 × 3 мм. Широкомасштабний випуск вироба планувалось розпочати впродовж двох років.

---

[1] Разработано программное обеспечение для сканера рисунка вен на руке. – 2007. – 23 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Осенью начнутся массовые поставки средств идентификации по рисунку вен на пальце // Biometrics.ru. – 2007. – 24 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Запропонована ідентифікація за малюнком судин застосовує випромінювання інфрачервоного спектра для отримання зображення. Вірогідність того, що новий модуль не розпізнає особистість, становить 0,01%, а ймовірність прийняття сторонньої особи за достовірну персону дорівнює 0,0001%. Час перевірки – близько однієї секунди. Створити такий досконалий пристрій допоміг новий контактний плоский сенсор. Кожен піксель матриці площею 150 × 100 крапок має свій масив мікролінз. Крок між масивами становить 0,1 мм, проміжок між масивами заповнений спеціальним шаром речовини, яка блокує проходження світла. Завдяки такій конструкції на сенсор потрапляє тільки світло, що падає чітко перпендикулярно модулю. Тому, за заявою фахівців «Hitachi», є можливість отримати чіткий сфокусований знімок пальця навіть на дуже близькій відстані від поверхні[1].

За наявними даними кількість утримувачів кредитних і дебетових карт, які замість PIN-кода можуть авторизуватися за допомогою технологій «Vein»-методу в 2007 році оцінювалася приблизно у 5 млн чоловік. Очікується, що до 2015 року можливе триразове збільшення на ринку користувачів цієї технології. Проте прогноз може бути скоректований у сторону зменшення: поширення зазначені технології набули тільки в Японії. Проблеми може створити й розширення конкуренції всередині цього способу ідентифікації, тобто між двома конкретними імплементаціями цієї технології: скануванням зображення малюнка вен на долоні та на пальцях[2].

За оцінкою ринку біометричних технологій у майбутньому компанією «Acuity Market Intelligence» очікується, що в 2017-му році частка «Vein»-методів на світовому ринку засобів біометрії збільшиться порівняно з 2009 роком більш ніж удвічі: з 2,67 до 5,77%[3].

Існує ще подібний до технології ідентифікації за зображенням малюнків вен на долоні або пальці метод використання малюнків розташування кровоносних судин, який заснований на розпізнанні за термограмою обличчя особи, яку ідентифікують. Спосіб розпізнання за термограмою обличчя ґрунтується на результатах досліджень, які довели, що термограма (тобто схема розташування кровоносних судин обличчя особи) є унікальною для кожної людини. Для отримання термограми використовується спеціальна інфрачервона камера. За повідомленнями деяких інтернет-джерел, система дозволяє провести ідентифікацію навіть у тому разі, якщо людина перебуває на іншому кінці неосвітленої кімнати. Температура тіла, охолодження шкіри обличчя у морозну погоду, природне старіння організму людини, використання спеціальних масок, проведення пластичних операцій не впливають на точність цього термографічного методу. Внаслідок недостатньої уваги до проведення ґрунтовних досліджень методу ідентифікації за термограмою обличчя якість розпізнавання, яка поки що досягнута, не є дуже високою, тому особливого поширення цей метод нині не отримав[4].

---

[1] Анонсирован новый модуль биометрической идентификации по рисунку вен на пальце // 3dnews.ru. – 2009. – 31 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Лукашов И. Биометрия становится индустриальной технологией / И. Лукашов // Cnews.ru. – 2007. – 21 августа. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security2007/articles/biomarket.shtml

[3] Митин Владимир. Биометрические технологии, которые мы выбираем / В. Митин // PC Week/RE. – 2010. – 9 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Мифы биометрии. [Электронный ресурс]. – Режим доступа: http://www.cbio.ru/v5/modules/news/article.php…; http://universalkey.boxmail.biz/cgi-bin/guide.pl?action= article…

«Vein»-метод, крім фінансової сфери, найбільше використовується у медицинській. За матеріалами ЗМІ, найбільш поширеною у медицинській галузі є системи, які використовують технологію зображення малюнка вен на долоні.

Наглядові та контролюючі органи, що діють в американській галузі охорони здоров'я, неодноразово відзначали необхідність точної ідентифікації пацієнтів. У США інвестується мільйони доларів для підвищення безпеки пацієнтів у медицинській сфері, і завдання номер один – забезпечити коректну ідентифікацію пацієнтів, зв'язавши отриману під час цього процесу інформацію з відповідними електронними історіями хвороби. Якщо лікарі та медсестри використовують історії хвороби й іншу медичну інформацію, яка стосується конкретно цього пацієнта, це значно знижує ймовірність виникнення помилок.

Як правило, функціонуючі в медичному закладі біометрична і медична інформаційні системи – інтегровані. Це, з одного боку, гарантує безпеку персональних даних пацієнтів, а з іншого – забезпечує їхню швидку та точну ідентифікацію.

Технологія біометричної ідентифікації пацієнтів особливо ефективна у лікарнях або відділеннях швидкої медичної допомоги, де важлива кожна секунда. Якщо відома дата народження пацієнта і можливо відсканувати малюнок вен на його долоні, це єдине, що потрібно для негайної ідентифікації пацієнта і початку лікувального процесу.

Як тільки пацієнт зареєстрований у біометричній системі, ніхто не зможе скористатися його страховкою або виписати на його ім'я рахунок за медичні послуги, які були надані іншій людині. Якщо хто-небудь зможе скористатися чужими ідентифікаційними даними для одержання медичних послуг, то в історії хвороби відомості про цього пацієнта можуть змішатися з даними дійсного власника, що, своєю чергою, введе лікаря в оману. Це одна з головних причин, чому вживаються такі попереджувальні заходи з забезпечення безпеки персональних даних пацієнтів медичних закладів. Як правило, хворі проходять біометричну ідентифікацію на всіх етапах лікувального процесу, який контролюється медичною інформаційною системою.

Діагностика, будь-яке призначення, скерування пацієнта на аналізи або будь-які процедури супроводжуються його біометричною ідентифікацією – для того, щоб лікарі й медсестри могли переконатися, що ця послуга надається саме тому, кому вона необхідна[1].

Більшість інформації стосовно впровадження технологій зображення малюнка вен на долоні у різні сфери життя надходять із Сполучених Штатів Америки. Наприклад, на початку 2013 року мережа камер схову «Bluevault» запровадила у своїх відділеннях біометричну систему контролю доступу. «Bluevault» пропонує клієнтам послуги з надійного зберігання різних матеріальних цінностей: монет, злитків дорогоцінних металів, картин, інших творів мистецтва.

Вибір системи ідентифікації за малюнком вен був зроблений через надійність, швидкість та зручність цього методу розпізнавання[2].

На форумі розробників IDF, що проходив у Сан-Франциско в 2012 році, корпорація «Intel» продемонструвала цікаву розробку під назвою «Palm Secure». Ця інноваційна технологія використовує спеціальні відео-датчики й дозволяє ідентифікувати власника комп'ютера за малюнком вен на долоні.

---

[1] Калифорнийская больница перешла к биометрической идентификации пациентов // BIOMETRICS.RU. – 2009. – 17 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрические технологии в калифорнийских камерах хранения // BIOMETRICS.RU. – 2013. – 20 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Прототип системи, продемонстрований на форумі, ґрунтується на надійній методиці біометричної ідентифікації та гарантує ефективний захист від кібер-атак. Авторизація користувача за допомогою «Vein»-методу триває декілька секунд. Власнику комп'ютера потрібно піднести руку до спеціального детектора на панелі пристрою, після чого спеціальна програма виконує вхід у систему Windows 7 і надає користувачеві доступ до його банківського рахунку. А після завершення робочого сеансу прототип системи захисту самостійно блокує доступ до Windows і переводить комп'ютер у режим сну.

Біометричні датчики персонального комп'ютера (ПК) або ноутбука розпізнають малюнок вен на долоні користувача. Отриманий шаблон-пароль відрізняється від традиційних паролей підвищеною стійкістю до злому.

Після того, як користувач розпізнаний, його унікальний ідентифікатор передається у численні облікові записи. Після цієї процедури власникові ПК надається безперешкодний доступ до банківського рахунку, електронної пошти, соціальних мереж й інших додатків[1].

У США в низці галузей технологію малюнка вен на долоні використовують у системах контролю управління доступом.

У 2013 році мережа фітнес-центрів «MVP Sports Clubs» у всіх своїх відділеннях запровадила ідентифікацію відвідувачів за малюнком вен на долоні. Біометрична ідентифікація замінила картки, які відвідувачі фітнес-центрів постійно забували або втрачали. Тепер ці проблеми вирішили[2].

Також із 2013 року біометрична система контролює доступ у лабораторію інновацій в Школі інформатики та комп'ютерних наук Дональда Брена – одному з факультетів Каліфорнійського університету.

Лабораторія інновацій не тільки ознайомлює студентів із останніми досягненнями інформатики та кібернетики, але і регулярно проводить конкурси на розробку різних комп'ютерних програм-додатків. Зрозуміло, що у студентів такого інноваційного закладу немає ні часу, ні бажання користуватися під час доступу в лабораторію застарілою парольною технологією, крім того, паролі легко підгледіти або викрасти, що викликає особливу тривогу в учасників команд, які конкурують між собою на конкурсах програмних розробок.

Керівництво лабораторії знайшло ідеальний вихід із ситуації. Тепер, щоб пройти в лабораторію, студентові не треба згадувати та набирати пароль: досить просто показати свою долоню безконтактному сканеру, який і «зчитає» з неї малюнок вен. Якщо отримані дані про біометричний ідентифікатор збіглися з раніше зареєстрованими, двері лабораторії відчиняться перед студентом[3].

Оскільки біометричні ідентифікатори унікальні для кожної людини, їх не можна підгледіти чи забути, зате легко та просто пред'являти під час розпізнавання. Цей аргумент і є основним чинником, який дозволяє під час вибору системи контролю та доступу надати перевагу біометричній технології.

---

[1] Intel предложила заменить пароли биометрической идентификацией // СОФТ@Mail.Ru. – 2012. – 18 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Еще одна американская сеть фитнес-центров внедрила биометрические технологии // BIOMETRICS.RU. – 2013. – 19 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Продвинутые американские студенты освоят биометрический контроль доступа // BIOMETRICS.RU. – 2013. – 19 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

5.4. Ідентифікація за вушними раковинами

Нині у засобах масової інформації, матеріалах різних конференцій і семінарів з'являється дедалі більше повідомлень про розробку та використання нових підвидів біометричної ідентифікації і про можливі сфери їх застосування. Але серед цієї інформації досить рідко можна натрапити на повідомлення щодо біометричних рішень на базі технології ідентифікації людини за формою вуха. Зі зростанням обізнаності про можливості цієї технології цей спосіб ідентифікації починає також привертати до себе увагу.

Багато з того, що відоме про вухо як об'єкт для проведення ідентифікації або аутентифікації, розроблено фахівцем у цій галузі Іаннареллі та саме його ідентифікаційна система найчастіше згадується в повідомленнях ЗМІ. За його класифікацією, вушні раковини діляться на чотири типи за видами форм: овальні, круглі, прямокутні та трикутні. «Ідентифікація за формою вуха має значні переваги, тому що ця характеристика є однією з незмінних характеристик людини, – стверджує Іаннареллі. Форма вуха формується через 56 днів після зачаття, залишається незмінною протягом усього життя і довше інших носіїв людських біометричних ознак зберігається після смерті. Крім мочки вуха, яка може змінюватися під дією якихось механічних факторів, форма вуха зберігається набагато довше, ніж форми обличчя та папілярні візерунки пальців. Цей факт робить вухо особливо корисною ідентифікаційною характеристикою».

Ідентифікацію за формою вуха можна використовувати в багатьох ситуаціях. У деяких випадках, на думку Іаннареллі, відбитки пальців не можуть слугувати для ідентифікації через природжені дефекти, хвороби або рани. У таких випадках встановити особу загиблого чи померлого можна за допомогою його фотографії шляхом порівняння зображень вуха.

Цей вид ідентифікації використовується деякими компаніями поряд із більш відомими біометричними технологіями. Зокрема компанія «Integrated Management Services» розвиває ідентифікаційну систему, що заснована на системі Іаннареллі. Робота системи починається зі складання своєрідного відбитка вуха. Спеціальна програма за допомогою комп'ютера вибудовує зображення під певний стандарт. Потім стандартизований відбиток порівнюється з уже наявними в базі даних. Оскільки ідентифікація за формою вуха поки не має широкого розповсюдження, вона розглядається як додаткова в тих випадках, коли пальці, очі або обличчя не можуть достатньою мірою стати джерелом потрібної інформації, необхідної для ідентифікації.

Нині правоохоронні органи не мають у своєму розпорядженні значних банків зображень вух для здійснення процедур ідентифікації фізичних осіб. Але в деяких випадках саме вушні раковини допогли у розкритті злочинів[1].

Як відомо, майже всі злочинці під час вчинення неправомірних дій працюють у рукавичках. Тому досить часто на місці злочину не залишається жодних слідів відбитків пальців. Але злочинці, як правило, не піклуються про те, як заховати свої вуха, крім того, вони досить часто прикладають вухо до вікна або дверей, щоб зрозуміти, що відбувається в будинку. Отже, допомогти правоохоронцям можуть відбитки вух, що були зафіксовані під час огляду місць подій. Як показали проведені дослідження, вони є унікальними та неповторними, за ними можна розрізнити навіть близнят. Але поки що

[1] Идентификация по форме уха // ЮНИСКАН. – 2004. – 1 июня. [Электронный ресурс]. – Режим доступа: http://www.ean. ru/art1/art208.html…

правоохоронні органи дуже рідко використовують відбитки або зображення вух у своїй діяльності. Навіть якщо в матеріалах слідчих справ і є такий відбиток, здебільшого він не використовується, оскільки на практиці майже не існує відповідних банків даних. Але іноді допомогти представникам правоохоронних органів можуть відбитки вух, які були отримані під час огляду місць подій.

Наприклад, у Ванкувері Іаннареллі допоміг ідентифікувати вбивцю, який притулився вухом до дверей, перед тим, як увірватися в кімнату. У Великобританії слідчі тривалий час не могли розкрити злочин, вчинений у липні 2001 року в місті Борнем. Тоді зловмисник уночі пограбував будинок одного з місцевих жителів. Перед тим, як вчинити крадіжку, злодій приклав вухо до дверей, щоб переконатися у тому, чи не чути звуків, які свідчили б про те, що у приміщенні можуть перебувати люди, які ще не сплять. Єдиний слід злочинця, що змогли виявити викликані на місце крадіжки англійські «боббі», – це відбиток вуха оригінальної форми на дверях спальні. Відбиток зафіксували і долучили до матеріалів справи. Через три роки місцева поліція заарештувала підозрілого громадянина, який намагався продати мобільний телефон. Поглянувши на вуха заарештованого, які мали досить своєрідну форму, один поліцейський пригадав історію з відбитком вуха оригінальної форми з нерозкритої справи про пограбування. У підозрюваного був знятий відбиток вуха, який звірили з тим, що зберігався в матеріалах нерозкритої кримінальної справи, і вони збіглися. Злочинцеві, якого видали занадто прикметні вуха, довелося постати перед судом за пограбування трирічної давнини[1].

Відбитки вуха знімають так: спеціальний пластик прокатують вухом від його низу до верху, водночас залишається відбиток ліній вуха, який потім сканується і за допомогою спеціальної комп'ютерної програми перетворюється на цифрове зображення-шаблон, яке у відповідному електронному виді вноситься до комп'ютерної бази даних.

Процес пошуку відповідного зображення вуха триває недовго і вимагає чіткого зображення вушної раковини на фотозображенні та скрупульозного поетапного порівняння. Але, незважаючи на такий досить складний процес, деякі правоохоронні агентства використовують цю технологію ідентифікації. Оскільки вухо може бути сфотографоване з різних відстаней, система ефективна і за деяких інших обставин. Якщо відеокамера зафіксує в кадрі фотообраз злочинця, то зображення вуха може використовуватися для встановлення його особи.

Технології ідентифікації за вушними раковинами потрібно ще пройти великий шлях для досягнення рівня популярності й ефективності інших біометричних систем, але інтерес до цієї технології поступово зростає[2].

Професор Гай Ратті з університету Лідса (Великобританія) ще в 2004 році створив комп'ютеризовану систему, яка дозволяє автоматизувати процес порівняння зображень вушних раковин за допомогою спеціалізованих комп'ютерних програм. «Наскільки нам відомо, – підкреслив у своєму повідомленні професор Ратті, – це перша комп'ютеризована база даних відбитків і зображень вух».

Відбитки вух вилучаються англійськими криміналістами приблизно з 15% місць злочинів, а випадки встановлення злочинців за допомогою ідентифікації за вушними раковинами вже відбувалися в Нідерландах і Швейцарії[3].

---

[1] Из мира биометрических чудес // БДИ. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.bdi.spb.ru/55/biometria55.htm...

[2] Идентификация по форме уха // ЮНИСКАН. – 2004. – 1 июня. [Электронный ресурс]. – Режим доступа: http://www.ean. ru/art1/art208.html…

[3] Из мира биометрических чудес // БДИ. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.bdi.spb.ru/55/biometria55.htm...

На теренах СНД ученими Інституту математики і інформаційних технологій Академії наук Узбекистану був розроблений і запатентований наприкінці 2008 – початку 2009 років пакет прикладних програм для ідентифікації особистості за зображенням вушних раковин. Спеціальні математичні програми здатні заздалегідь обробити відеозображення, локалізувати вушну раковину та виокремити контурні лінії на зображеннях. «На них також за допомогою спеціальних програм визначаються ідентифікаційні ознаки, що і дозволяє розпізнати особу за зображенням вушних раковин», – відзначив представник узбецького патентного відомства[1].

Цікавим є і таке повідомлення щодо нової біометричної ідентифікаційної технології за допомогою вух. Суть цього методу полягає у можливості людських вух генерувати і проводити під дією зовнішнього джерела власні звуки (так звана отоакустична емісія). Тобто людське вухо є не тільки органом слуху, воно також проводить або генерує під впливом зовнішнього чинника власні звуки. Вловити ці звуки може тільки надчутливий мікрофон.

Якщо вченими буде доведено, що звуки ці унікальні для кожної людини, то цей факт допоможе суттєво підвищити рівень безпеки в системах телефонного банкінгу, позбавивши водночас клієнтів від необхідності запам'ятовувати складні паролі. Щось подібне можна буде запровадити і в конструкцію мобільних телефонів, крадіжка яких у такому випадку може стати абсолютно марною справою.

Нині над цим проектом працюють британські вчені з університету Саутгемптона. Впровадження нової технології очікувалось у 2010 році. Але перед тим ще потрібно було довести, що «почерк» (тональність) цих звуків не змінюється впродовж усього життя людини. Поява такої технології була передбачена ще в сорокових роках минулого століття[2].

5.5. Голосова ідентифікація

Голос – така ж невід'ємна риса кожної людини, як і її обличчя або відбитки пальців. Поширення засобів зв'язку (стаціонарні та мобільні телефонні мережі, інтернет-телефонія тощо) створюють великі можливості для застосування цього ідентифікатора. Крім того, розпізнавання за голосом є дуже зручним для користувачів і вимагає від них мінімум зусиль.

Необхідно зважати на те, що голос (разом із почерком, ходою та ін.) належить до так званих «поведінкових» ідентифікаторів і було б марно очікувати від цих «динамічних» технологій високої точності та надійності.

Технології та засоби ідентифікації за голосом застосовуються у таких сферах людської діяльності, що безпосередньо пов'язані з обробкою звернень користувачів по телефону (кол-центри /Call-center/) і т. д.), що дозволяє пришвидшити обслуговування абонентів і розвантажити операторів. У більш значущих із погляду конфіденційності

[1] В Узбекистане создали программу биометрической идентификации личности по форме ушей. – 2009. – 20 марта // ИА Regnum. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp?group...

[2] Уши вместо пароля? – 2009. – 15 апреля. – MobileDevice.r. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp?group...

проектах (особливо пов'язаних із необхідністю захисту секретної інформації) ідентифікація за голосом відіграє допоміжну роль і використовується разом з іншими біометричними технологіями (насамперед з ідентифікацією за відбитками пальців)[1].

Ідентифікація за голосом заснована на акустичних особливостях вимовлення, які у кожної особи особливі та деякою мірою унікальні. Акустичні зразки голосу кожного індивідуума відображають як низку його анатомічних відмінностей (наприклад, розмір і форму горла та рота), так і звички, що набуваються ним упродовж життя (гучність голосу, манера розмови).

Сучасна голосова біометрична технологія розбиває кожне вимовлене слово на низку сегментів. Записаний голосовий «відбиток» перетворюється на індивідуальний математичний код, який зберігається в спеціальному банку даних. Для проведення ідентифікації індивідуума його просять відповісти на декілька питань (здебільшого їх кількість не перевищує трьох), відповіді на які легко запам'ятовуються. Наприклад, повідомити прізвище, ім'я, по батькові та дату народження. Сучасні комп'ютерні системи автоматично створюють цифрову модель («відбиток») голосу, що надалі може зіставлятись із будь-якою фразою, вимовленою людиною[2].

Під час проведення голосової ідентифікації треба пам'ятати, що голос може істотно змінюватися під впливом емоційних чинників (настрою людини) і залежить від стану здоров'я (наявність ангіни, нежитю, бронхіту та інших хвороб легенів і верхніх дихальних шляхів). На якості ідентифікації можуть суттєво позначатися зовнішні умови (наприклад, шуми, що супроводжують дорожній рух, розмови інших людей). Якщо для передачі голосової інформації використовуються звичайні лінії зв'язку, то різні перешкоди, що супроводжують процес передачі-прийому звукових сигналів, також здатні створити проблеми під час розпізнання користувачів.

Під час утворення й обробки голосових ідентифікаторів людські мовні фрази розбиваються на послідовність окремих «звукових кадрів», які потім перетворюються на цифрову модель. Ці моделі прийнято називати «голосовими відбитками» (за не дуже вдалою аналогією з відбитками пальців). За подальшої ідентифікації порівнюються раніше зареєстрований (еталонний) та знов сформований (що перевіряється) «голосові відбитки».

Для підвищення надійності та пришвидшення розпізнавання користувача відповіді надаються на заздалегідь сформовані питання або вимовляється парольна фраза. У цьому випадку впізнання проводиться в режимі «верифікації диктора» (в цій ролі виступає сам користувач, який вимовляє певні відповіді чи пароль)[3].

Нині багато фірм випускають програмне забезпечення, яке здатне ідентифікувати людину за голосом. Водночас оцінюються такі параметри, як висота тону, модуляція, інтонація тощо. На відміну від розпізнавання за обличчям людини, цей метод не вимагає дорогої апаратури – достатньо лише звукової плати та мікрофона.

Ідентифікація за голосом, зручний, але не такий надійний спосіб, як інші біометричні методи. Наприклад, у застудженої людини можуть виникнути труднощі під час використання голосових систем. Голос формується з комбінації фізіологічних і поведінкових чинників, тому основна проблема, пов'язана з цим біометричним методом, – точність

[1] Идентификация по голосу. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/…

[2] Биометрия. Сам себе пароль. – 2007. – 07 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/...

[3] Идентификация по голосу. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/...

ідентифікації. Ідентифікація за голосом використовується в основному для управління доступом у приміщення середнього ступеня безпеки[1].

Останнім часом в інтегрованих системах безпеки, в системах відеоспостереження, в системах охоронного телебачення (СОТ) широко застосовується також звукозапис. Інформація, що отримується, використовується і для виявлення порушників, і для аналізу стану аудіообстановки з метою контролю дій персоналу та охорони. Аудіоінформація використовується також у системах передачі інформації (СПІ) телефонних переговорів, у системах оповіщення, тривожного виклику тощо. У зв'язку з цим актуальним стає вирішення завдань, що пов'язані з аналізом звукової інформації, яка отримана під час запису в системах безпеки і яка може використовуватися надалі для аналізу в спеціалізованих лабораторіях правоохоронних органів, лабораторіях і центрах судової експертизи, науково-дослідних і навчальних центрах із метою:

– ідентифікації особи за допомогою записаної фонограми;

– встановлення автентичності (достовірності) аналогових і цифрових фонограм записаних розмов;

– аналізу шумового фону, діагностики акустичної обстановки й умов проведення звукозапису;

– ідентифікації засобів звукозапису;

– підвищення якості та розбірливості у вже існуючих записах фонограм;

– захисту мовного сигналу від несанкціонованого доступу;

– стискання мовних повідомлень;

– встановлення дослівного змісту в низькоякісних фонограмних записах.

Під час вирішення завдань охорони фізичних об'єктів та інформаційних ресурсів від кримінальних і терористичних загроз дуже цікавим є використання аудіоінформації (звукових голосових записів) у системах контролю та управління доступом (СКУД). Особливість таких систем полягає в тому, що вони допускають віддалену (за допомогою телефону) та приховану аутентифікацію, що інколи є єдиним можливим засобом встановлення особистості співрозмовника.

Зручність для користувачів, простота, здатність до інтегрування з іншими методами розпізнання індивідуумів – це також досить суттєві чинники, що підтверджують доцільність застосування голосових технологій у біометричних системах як відокремлено від інших методів верифікації та ідентифікації особи, так і в комплексі з ними.

Як показав огляд інформаційних матеріалів за технологією голосової ідентифікації, нині спостерігається наступна стадія технічної еволюції цих систем. Уже з'явилися комерційні версії програмного забезпечення, що використовують голосові технології. Однак, якщо в кінці минулого сторіччя системам розпізнавання та ідентифікації за голосом пророкували в майбутньому досить широке застосування, то здійснені сучасні дослідження виявили, що в цій галузі існує низка проблем. У публікаціях XXI століття наголошується, що комп'ютерні програми розпізнавання за голосом доволі складні і не досить зручні у використанні, окрім того, мають доволі високу вартість.

Здебільшого вони застосовуються як додаткові засоби перевірки достовірності там, де необхідно забезпечити високий ступінь надійності систем ідентифікації або аутентифікації.

Тому продовжуються роботи з удосконалення алгоритмів обробки голосових сигналів для створення механізмів автоматичного розпізнання людини за голосом[1].

---

[1] Борзенко А. Биометрические технологии / А. Борзенко // Bytemag.ru. – 2001. – 10 октября. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

Наявні та майбутні системи голосової верифікації індивідуумів мають розмежовувати доступ користувачів до об'єктів з обмеженим доступом (контроль доступу до приміщень) або інформаційних ресурсів за парольною фразою. Системи, що застосовуються, повинні задовольняти необхідні вимоги безпеки, зводячи водночас до мінімуму незручності, що виникають під час користування ними.

Системи голосової текстозалежної верифікації диктора в засобах управління контролю за доступом (СКУД) формуються на базі програмного забезпечення, що використовує, як правило, фірмові розробки алгоритмів верифікації диктора за голосом, що захищені відповідними патентами, а також комп'ютерне обладнання у вигляді серверів обробки та зберігання голосової біометричної інформації. У складі системи обов'язково повинно бути обладнання для запису і передачі звукової інформації, а також засоби управління виконавчими пристроями СКУД.

Система має забезпечувати:

– визначення особистості користувача без безпосереднього контакту з ним;

– можливість використання як технічні засоби вводу для верифікації за голосом мікрофонів широкого вжитку;

– ефективне розпізнання саме живого голосу, виключаючи водночас можливість використання записаних фонограм для несанкціонованого доступу;

– мінімальне значення помилки FAR = 0,01%;

– регламентацію проходу визначеної кількості співробітників на території з різними рівнями доступу без введення особистого PIN-коду або використання верифікаційної смарт-картки.

Здебільшого система верифікації повинна мати такі можливості:

– точне налаштування системи для досягнення оптимального співвідношення безпеки і зручності її використання кожним користувачем;

– розмежування прав доступу абонентів до ресурсів через систему надання пріоритетів;

– зручне та швидке залучення нових користувачів до системи (неперериваючи роботу системи);

– забезпечення безперервного цілодобового режиму роботи системи та автоматичне ведення журналу доступу (проходу) абонентів і відвідувачів;

– наявність віддаленого доступу для виконання функцій адміністрування системи й аудиту користувачів, а також автоматичний запис на магнітні носії голосових біометричних звернень і також ведення в автоматичному режимі журналів верифікації користувачів.

СКУД у варіанті текстово-залежної верифікації диктора повинен виконувати такі завдання:

– у режимі забезпечення доступу на об'єкт мати апаратно-програмний комплекс, який дозволяє регламентувати прохід співробітників на територію, де існує режим різних рівнів доступу без введення особистого PIN-коду або використання особистої смарт-картки (за необхідності зі збереженням «інкогніто» абонента);

– під час використання віддалених каналів зв'язку – наявність апаратно-програмного комплексу розмежування доступу користувачів із каналів зв'язку (телефонної лінії):

[1] Крахмалёв А. К. Использование речевой информации для биометрической идентификации в системах контроля доступа / А. К. Крахмалёв. – 2008. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp…

а) до закритої інформації (банківський рахунок, підтвердження банківських транзакцій, біржові торги, платні інформаційні ресурси, міжміські або міжнародні дзвінки);

б) із персональних комп'ютерів до внутрішніх корпоративних мережевих ресурсів або ресурсів Internet без введення особистого PIN-коду.

Підсумовуючи наведену інформацію щодо голосової ідентифікації, слід зазначити, що:

– мова традиційно є найпоширенішою формою людського спілкування;

– з огляду на цю тезу, рішення завдання отримання голосових відбитків (мовних зображень) і, навпаки, – якісного синтезу мовного сигналу за цим електронним зображенням – дозволяють забезпечити достатньо широкий спектр можливостей застосування цієї технології не тільки в системах автоматизованого контролю доступу, але і в інших сферах інформаційної безпеки та зв'язку.

Нині існують десятки різних систем ідентифікації за голосом, які мають різноманітні параметри та реалізують різні вимоги до процесу мовної ідентифікації залежно від завдань, які виконуються.

Але мовна ідентифікація має низку недоліків, які є перешкодою на шляху широкого запровадження систем голосової текстово-залежної верифікації диктора. Це – складність процедури налаштування систем (процедура реєстрації користувачів), доволі висока вартість необхідного програмного забезпечення порівняно, наприклад, з дактилоскопічними системами, недостатньо висока точність верифікації та ідентифікації.

Проте існують і позитивні сторони у використанні систем ідентифікації за голосом: це насамперед те, що така технологія разом із віддаленою ідентифікацією індивідуумів за зображенням особи дозволяє проводити безконтактну, приховану та віддалену ідентифікацію індивідуумів, через що багато закордонних, зокрема і російських організацій, працюють над усуненням існуючих недоліків цієї технології.

Проаналізуємо позитивні та негативні якості голосових технологій ідентифікації та верифікації.

Основні переваги цього методу ідентифікації:

– дуже простий і звичний для людини спосіб проведення ідентифікаційних заходів;

– безконтактність;

– можливість віддаленої ідентифікації чи верифікації клієнтів;

– низька вартість кінцевих ідентифікаційних пристроїв (мікрофонів) під час реалізації у складі комплексних систем безпеки (найнижча серед усіх біометричних методів);

– складність або в деяких випадках навіть неможливість для зловмисника імітувати голос за допомогою магнітофона. По-перше, сучасні ідентифікаційні системи здатні контролювати відразу декілька біометричних ознак, що відрізняються від тих, які використовуються в мовно-слуховій системі, по-друге, під час відтворення магнітофонного голосового запису мініатюрні гучномовці, що відтворюють мовні парольні фрази, вносять до голосового сигналу шумові спотворення, які реєструються системою, котра видає сигнал заборони на проведення ідентифікації;

– можливість під час проведення ідентифікаційної процедури визначити, чи знаходиться людина під загрозою насильства, оскільки емоційний стан особи істотно впливає на голосові та мовні характеристики.

Основні недоліки цього методу ідентифікації:

– високий рівень помилок 1-го і 2-го роду порівняно з дактилоскопічними методами;

– необхідність у спеціальному шумоізольованому приміщенні під час проходження еталонної ідентифікації;

– можливість перехоплення парольної фрази за допомогою звукозаписувальних пристроїв;

– якість розпізнавання залежить від багатьох індивідуальних чинників клієнта (інтонації, швидкості вимовлення, фізичного, емоційного та психологічного стану, хвороб горла);

– необхідність підбору парольних фраз для підвищення точності розпізнавання;

– вікові зміни голосу на відміну від незмінності у часі папілярних узорів пальців. Це призводить до необхідності періодичного оновлювання голосового еталону індивідуума, що зберігається в пам'яті системи;

– надійність роботи системи суттєво залежить від якості каналу передачі мовного сигналу до апаратно-програмного комплексу, де відбувається сам процес ідентифікації, зокрема від таких характеристик передачі, як частотний діапазон, рівень нелінійних спотворень, співвідношення рівня сигналу до його шумової складової, нерівномірності частотної характеристики.

Найвища надійність роботи ідентифікаційної системи забезпечується у випадку, коли електронні сигнали голосового еталону клієнта та перевірочний варіант котрольної фрази для порівняння надходять поодинці й за одним і тим же каналом, наприклад, телефонним.

Нині основна сфера застосування систем голосової ідентифікації в системах контролю й управління доступом (СКУД) як доповнювальних засобів перевірки достовірності особи під час використання основних біометричних технологій там, де необхідне забезпечення високого ступеня надійності ідентифікації або верифікації та безпеки об'єктів, що охороняються[1].

Як приклад упровадження голосових мовних ідентифікаторів можна навести повідомлення Російського біометричного порталу, в якому йдеться про те, що низка зарубіжних банків оголосили про запровадження систем ідентифікації клієнтів за голосом. Але слід зазначити, що в цих банках переважна кількість операцій із рахунками клієнтів проводяться з використанням телефонних каналів або інтернет-телекомунікацій. У цьому контексті директор британської «SpeechStorm» Олівер Леннон (Oliver Lennon) вважає вельми перспективним застосування ідентифікації за голосом у багатьох фінансових інститутах Сполученого Королівства.

Особливо він відзначає, що відповідний сегмент біометричного ринку зростає так швидко, як збільшується у суспільстві розуміння переваг і необхідності біометричної ідентифікації[2].

У Великобританії більшість споживачів занепокоєні питаннями безпеки використання PIN-кодів (personal identification number), паролів та інших секретних даних, що використовуються у банківських Call-центрах для встановлення особи. Під час проведеного фірмою «SpeechStorm» влітку 2008 року дослідження було встановлено, що 86% респондентів визнали необхідним те, щоб використовувати або мовний біометричний метод встановлення особи (28%), або симбіоз із голосової біометричної ідентифікації

[1] Крахмалёв А. К. Использование речевой информации для биометрической идентификации в системах контроля доступа / А. К. Крахмалёв. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Отношение пользователей к идентификации по голосу станет изучаться в ходе социологического опроса // BIOMETRICS.RU. – 2008. – 09 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

та PIN-паролю (58%) для верифікації особистості під час проведення телефонного банкінгу.

Професор Майлк МакТеар, який проводить дослідження у сфері голосової аутентифікації в університеті Ольстера, констатує: «Багато клієнтів банків стурбовані загрозами викрадення персональних даних і пов'язаних з цим фінансових ризиків. Це дуже важливо, щоб у банках усіляко заохочували введення ефективних і легких у використанні додаткових заходів безпеки. Аутентифікація за голосом є одним з таких методів». Отже, більшість клієнтів не хочуть запам'ятовувати та вводити довгу послідовність цифр і букв, замість цього вони бажають відповідати на декілька простих питань своїм звичайним нормальним голосом[1]. Із початку другого десятиріччя XXI століття побажання клієнтів втілюються у життя.

Експерти пророкують світле майбутнє голосової біометрії. Люди вже звикли до використання їх голосу під час мобільного пошуку, контролю за обладнанням і диктуванні, тому правильний підхід до голосової авторизації незабаром може стати важливою частиною процесу ідентифікації індивідуума.

Такі висновки опублікованого на початку 2012 року дослідження «Voice Biometrics Authentication Best Practices: Overcoming Obstacles to Adoption» («Кращі приклади застосування голосової біометрії для встановлення особистості: долаючи перешкоди»). Головна мета дослідження полягала в тому, щоб оцінити попередні проекти використання голосової біометрії, а також проаналізувати стан цієї галузі та оцінити її перспективи.

На думку автора звіту, – компанії «Valid Soft» – голосова біометрія може стати частиною багаторівневого процесу розпізнавання для того, щоб знизити ризик платіжного онлайн-шахрайства. Проаналізована у звіті інформація дає підстави стверджувати, що кількість зареєстрованих голосових «відбитків» може збільшитися з 10 млн у 2012 році до більш ніж 25 млн у 2015 році[2].

У другій половині 2012 року компанія «Opus Research» випустила новий огляд, присвячений використанню технологій біометричної ідентифікації за голосом у фінансових організаціях. Автори дослідження відзначають, що використання цієї технології не тільки підвищує рівень безпеки банківських систем ідентифікації, але й реально знижує собівартість розпізнавання їх користувачів, значно спрощуючи процес авторизації в зазначених системах.

За оцінкою «Opus Research», у банківських установах станом на жовтень 2012 року налічується близько п'яти мільйонів користувачів «голосових» біометричних систем, а до 2015 року цей показник може сягти 90 млн. Головним чинником такого зростання, на думку експертів, є здатність систем голосової ідентифікації суттєво зменшити час на проведення фінансових транзакцій порівняно з іншими біометричними системами й одночасно бути доволі ефективним засобом протидії шахрайству, відмиванню грошей і спробам викрадання персональних даних[3].

Як бачимо, є значні розбіжності у кількості наявних голосових «відбитків» у системах голосової ідентифікації у 2012 році та прогнозованої їх кількості в 2015 році за відомостями компаній «Valid Soft» і «Opus Research», але в обох оглядах чітко окреслюєть-

[1] Большинство пользователей предпочли бы паролям биометрию // BIOMETRICS.RU. – 2008. – 11 июля [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Новые перспективы голосовой биометрии в финансовой сфере. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Технологии биометрической идентификации по голосу в финансовых институтах: новые перспективы. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

ся тенденція суттєвого зростання кількості користувачів, які проводитимуть майбутні фінансові транзакції за допомогою систем голосової ідентифікації.

У Російській Федерації впровадженням технологій, де використовуються мовні ідентифікатори, займається товариство з обмеженою відповідальністю «Центр мовних технологій» (ТОВ «ЦМТ»). Із 1990 року ТОВ «ЦМТ» поставляє свою продукцію для підрозділів МВС, Міністерства юстиції, МНС і МО Росії, служб екстреної допомоги, центрів обробки викликів, виробників засобів зв'язку та багатьом іншим споживачам, у діяльності яких особливе значення надається якісній передачі, реєстрації й обробці мовної інформації.

Серед замовників ЦМТ: апарати Адміністрації Президента РФ, Ради Федерації РФ, Уряду РФ, органи виконавчої та законодавчої влади суб'єктів Російської Федерації. Центр мовних технологій є співзасновником консорціуму «Російські мовні технології» і членом російського біометричного товариства. Сьогодні компанія має необхідні ліцензії на розробку та виробництво спеціальної і військової техніки. Понад одна третина обсягу продукції, що випускається, реалізується за межами Росії у 62 країнах світу.

Фірмою розроблені технології «VoiceKey» і «VoiceNet».

«VoiceNet» – технологія ідентифікації на основі порівняння біометричних мовних ознак. Сфери застосування:

– системи контролю та управління доступом;

– криміналістичні фонообліки;

– call-центри з обслуговування клієнтів.

Функції:

– можливість пошуку за голосом індивідуума в базі даних як за парольною фразою, так і за фрагментами вимовлених фраз;

– застосування двох незалежних методів ідентифікації: на основі порівняння формант і статистичних даних основного тону;

– досить висока швидкість виокремлення та порівняння голосових ознак.

«VoiceKey» – технологія розмежування доступу за парольною фразою. Сфери застосування:

– системи розмежування доступу;

– системи оперативної ідентифікації особистості та ведення фонообліків у правоохоронних органах;

– управління службами і сервісами за телефоном[1].

Ідентифікація або верифікація за допомогою технологій «VoiceKey» і «VoiceNet» здійснюється за парольними фразами тривалістю від 5 секунд або фрагментами спонтанних розмов тривалістю понад 16 секунд. Обидві технології використовують як індивідуальні характеристики голосу положення резонансних максимумів у спектрі голосу, що забезпечує належний рівень розпізнавання за наявності шумів і незначних змін емоційного стану людини. Але «VoiceKey» зоорієнтований на сигнали, що отримуються за допомогою мікрофонів, а «VoiceNet» адаптований до роботи з каналами зв'язку, зокрема телефонними лініями.

Системи, що використовують принципи дій цих двох технологій, забезпечують можливість віддаленої ідентифікації або аутентифікації клієнтів. Підвищення надійності аутентифікації досягається також завдяки одночасному використанню технологій

[1] Общество с ограниченной ответственностью «Центр Речевых технологий» // BIOMETRICS.RU. – 2007. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

ідентифікації за тембром голосу та мовного розпізнавання (пароль, що вимовляється). Звичайно, окрім позитиву, технології «VoiceKey» і «VoiceNet» мають і недоліки, на які потрібно зважати.

Голос, на відміну від папілярних узорів пальців або долонь, змінюється з віком. Отже, клієнтам доводиться періодично оновлювати записаний голосовий еталон вимовлення мовних фраз, що зберігається у пам'яті ідентифікаційної системи. На голосові параметри суттєво впливає фізичний та емоційний стан людини під час процесу мовлення. Так, наприклад, система може не розпізнати людину, якщо вона перебуває у стані алкогольного сп'яніння або у нього в роті під час вимовлення речень є жувальна гумка, або він щойно виконував фізичні вправи. Надійність роботи системи значною мірою залежить від якості каналів передачі мовного сигналу до ідентифікаційного комплексу[1].

Для криміналістів СНД дуже цікавою є розробка «Трал-М» – системи автоматизації фонообліків і експрес-досліджень голосових фонограм мови (мал. 5). Ця розробка захищена патентом Російській Федерації № 2230375 «Автоматизація криміналістичних фонообліків на основі виділення та порівняння біометричних ознак мови». Під час розробки і тестування комплексу «Трал М» використовувалася мовна база даних «RUSTEN».

Мал. 5. Схематичний принцип використання системи «Трал М»

Основні функції системи «Трал М»:

– впорядковане зберігання голосових фонограм мови;

– автоматичне виокремлення біометричних ознак голосу і мови осіб, які підлягають обліку;

– автоматичний пошук осіб із співпадаючими або наближеними біометричними характеристиками голосу та мови.

Відмінні риси:

– доволі висока ефективність роботи з реальними сигналами, вільною мовою;

– можливість встановлення особи за сигналами недостатньої якості;

– використання двох незалежних алгоритмів порівняння: формантного і статистичного методів аналізу основного тону (починаючи з версії 3.0);

[1] Идентификация по голосу: скрытые возможности // Connect! Мир связи. – 2006. – 18 сентября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

– максимальна автоматизації процесу здійснення пошуку та порівняння, що дозволяє мінімізувати вимоги до рівня підготовки обслуговуючого персоналу і підвищити швидкість ухвалення рішення;

– можливість зберігання у фонотеці разом із звуковою, текстовою та графічною інформацією;

– під час проведення пошуку можливість встановлення порогових значень помилок першого і другого роду;

– можливість створення власної форми облікових карток для проведення реєстрації та подальшого архівного зберігання.

Процедура здійснення пошуку індивідуума, яким цікавляться, полягає в автоматичному попарному порівнянні так званих «дикторських карток», в яких закодовано індивідуальні характеристики голосу й особливості вимовляння облікованих осіб. За наслідками здійсненої порівняльної процедури видається роздруківка або виводиться на монітор список фонограм, в яких за зменшенням значення ймовірності збігу вказуються індивідуальні дані осіб, які мають подібні «відбитки голосу»[1].

Нині «Центр мовних технологій» (ЦМТ) – світовий лідер з систем ідентифікації особи за голосом. За відомостями «Wikileaks», у грудні 2011 року ЦМТ потрапив у список виробників технологій спостереження, що постачаються у різні країни світу.

У липні 2011 року дочірнє підприємство «Центру мовних технологій», яке має назву «ЦМТ-Інновації» (російською «ЦРТ-Инновации»), стало резидентом Сколково, кластера високотехнологічних компаній, що створюється в Російській Федерації під Москвою.

За заявою представника «ЦМТ-Інновації», головним завданням нової компанії в Сколково є розробка технологій ідентифікації, які дозволять встановлювати особистість людини за голосом і за зображенням лиця особи.

У компанії свої розробки вважають унікальними за масштабністю і функціональністю – вони можуть зберігати багатомільйонні бази біометричних даних (зразків голосів і фотозображень) і знаходити потрібних індивідуумів у будь-яких каналах зв'язку та відеофайлах.

Передбачено можливість підключення додаткових функцій ідентифікації: за відбитками пальців, за райдужною оболонкою ока і т. д. Це програмне забезпечення орієнтоване на силові та правоохоронні структури, зокрема й на спецслужби, і передбачається, що воно може бути використане для розшуку злочинців.

За заявою генерального директора ЦРТ Михайла Хитрова: ««Центр мовних технологій» є світовим технологічним лідером на таких наукомістких ринках: синтез і розпізнавання мови, голосова біометрія, мовна аналітика та інше... Наше завдання – максимально реалізувати цей інноваційний потенціал на світовому та російських ринках».

У сфері створення систем розпізнавання голосів в інтересах спецслужб і поліції «Центр мовних технологій» сьогодні дійсно є одним із світових лідерів. Технології ідентифікації особи за голосом, які розроблені в Центрі, застосовують такі методи автоматичного дослідження голосу й мови, для яких не мають значення мова, акцент і використовуваний діалект: аналізуються фізичні параметри голосу людини.

У 2010 році ЦРТ завершив впровадження першого у світі національного проекту ідентифікації за голосом. Проект був реалізований у Мексиці, де була розгорнута система

[1] Общество с ограниченной ответственностью «Центр Речевых технологий» // BIOMETRICS.RU. – 2007. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp…

державного обліку голосів і біометричного пошуку, яка здатна ідентифікувати людину за фрагментами її розмови. У національну базу голосів внесли «голосові відбитки» не тільки злочинців і співробітників правоохоронних органів, але й низки законослухняних громадян: у деяких мексиканських штатах для одержання прав водія потрібно здати зразки голосу. Центр не обмежується голосовими розробками й займається створенням систем розпізнавання обличчя – компанія бере участь у тендерах російських спецслужб, а також активно експортує їх за кордон. 2012 року до створеної у Мексиці системи обліку голосів ЦМТ додав можливість ідентифікації людини за її фотографією.

Системи «Центру мовних технологій» експлуатуються в Казахстані, Киргизії, Узбекистані та Білорусії, де впроваджуються або запроваджені національні системи ідентифікації громадян.

ЦМТ успішно працює в Таїланді й Сінгапурі, намагається отримати доступ на ринок Китаю. Замовлення на свою продукцію Центр одержує з таких близькосхідних країн, як Саудівська Аравія, Алжир, Ємен і Туреччина.

У Латинській Америці ЦМТ одержав контракти від Колумбії й Еквадору, де запроваджувались розроблені Центром мовних технологій технологія розпізнавання за обличчям[1].

2008 року в Національному інституті стандартів і технологій США (NIST) було проведено чергове щорічне дослідження технологій ідентифікації голосу. Випередивши 45 учасників, перше місце отримала технологія, створена в сінгапурському Інституті інформаційно-комунікаційних досліджень (I2R). Порівняння «відбитків голосу» за цією технологією дозволяє зробити висновок щодо встановлення відповідності голосів із точністю до 97%. Системи ідентифікації за голосом можна застосовувати в досить складних акустичних умовах. Нині одним із найпоширеніших застосувань є виявлення «жартівників», які здійснюють фальшиві повідомлення, що призводять до хибних виїздів екстрених служб[2].

В інтерв'ю «Незалежній газеті» у лютому 2008 року тодішнього Міністра внутрішніх справ Російської Федерації Рашида Нургалієва було зазначено, що у 62 регіонах РФ функціонують лабораторії МВС, що займаються голосовою ідентифікацією[3].

Улітку 2009 року Національний Банк Австралії (NAB) представив нову послугу, яка має на меті підвищення безпеки клієнтів, – біометричну голосову перевірку за допомогою телефонного зв'язку. У травні цього ж року ця розробка пройшла пілотне випробування. За результатами тестування було ухвалене рішення про її розповсюдження на 3,3 млн клієнтів NAB. Громадяни, які користуються послугами банку, відтепер можуть зареєструвати зразок свого голосу, який, згідно з повідомленням адміністрації NAB, практично неможливо вкрасти. Нині це один із найбільш надійних засобів встановлення достовірності особистості, а порівняно з PIN-кодом або паролем цей спосіб має переваги ще й тому, що ці дані можна забути, а ось остаточно втратити голос навряд чи[4].

---

[1] Солдатов Андрей. Российские компании в обмене технологиями слежки / А. Солдатов, И. Бороган // Ежедневный журнал. – 2012. – 30 января. [Электронный ресурс]. – Режим доступа: http://www.agentura.ru/projects/identification/justbusiness/...

[2] Определена лучшая технология биометрической идентификации по голосу // Открытые системы. – 2008. – 25 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Интервью Министра внутренних дел Российской Федерации Рашида Нургалиева «Независимой газете». – 2008. – 5 февраля. [Электронный ресурс]. – Режим доступа: http://www.mvd.ru/press/interview/...

[4] Австралийский банк идентифицирует своих клиентов по голосу // MoneyNews.ru. – 2009. – 23 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Маркетингова компанія «GIA» опублікувала на початку 2013 року огляд, який висвітлює розвиток технологій біометричної ідентифікації за обличчям і голосом. За оцінкою авторів прогнозу, обсяг зазначених сегментів світового ринку може до 2018 року сягти 2,9 млрд доларів. Аналітики «GIA» вважають, що зростанню потреби в застосуванні біометрії (зокрема й технологій ідентифікації за обличчям і голосом) буде сприяти зростаючий попит на засоби забезпечення безпеки та необхідність протидії терористичним атакам, насильству на расовому й етнічному ґрунті, злочинності у будь-якій формі та іншим виявам протиправних дій. Найбільшим регіональним ринком у вказаних сегментах є Сполучені Штати Америки[1].

За даними компанії «Acuity Market Intelligence», в 2017 році частка засобів голосової біометрії збільшиться до 5,49% порівняно з 2,15% у 2009 році. Згідно з підсумками опитування читачів «PC Week/RE» «Біометричні технології в корпоративному сегменті», проведеного у Росії на початку 2010 року, третє місце за популярністю серед технологій посіли методи ідентифікації людини за голосом. У цій технології приваблює доступність периферії, що для бюджетних організацій є важливою умовою. За оцінкою «PC Week/RE» обсяг російського ринку систем транзакційної голосової аутентифікації в 2010 році становив 5–7 млн доларів. Але згідно з прогнозом подальше щорічне зростання може становити 50–70%. 2010 року експерти компанії «Frost & Sullivan» оцінювали можливий обсяг світового ринку голосової верифікації приблизно у 356,4 млн доларів, а в наступному році – в 533,7 млн доларів[2].

Компанія «TechCast» опублікувала прогноз щодо найбільш вірогідних сценаріїв розвитку людства в другому десятиріччі XXI століття, у якому зробили висновок, що зараз і надалі буде продовжуватися процес розвитку інформаційно-телекомунікаційних технологій, зокрема й електронної комерції. Зокрема, слід очікувати появи нових технологічних систем розпізнавання за голосом із метою їх подальшого використання для керування різними машинами та пристроями за допомогою голосових команд[3].

5.6. Ідентифікація за підписом. Підпис як засіб ідентифікації в епоху Інтернету. Здійснення біометричної ідентифікації за почерком особи

Підпис фізичної особи – такий же унікальний атрибут індивідуума, як і його фізіологічні характеристики. Крім того, це і звичайний для будь-якої людини метод ідентифікації, оскільки він, на відміну від отримання відбитків пальців, не асоціюється з кримінальними обліками.

[1] Технологии биометрической идентификации по лицу и голосу: новые перспективы // BIOMETRICS.RU. – 2013. – 5 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Митин Владимир. Биометрические технологии, которые мы выбираем / В. Митин // PC Week/RE. – 2010. – 9 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Экспертный проект TechCast опубликовал набор наиболее вероятных сценариев развития человечества на ближайшие десятилетия // Washprofile.org/ru. – 2008. – 8 августа. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/7910

Використання підпису як засобу авторизації документа відоме давно, проте він має недоліки. Перший із них пов'язаний із ненадійністю ідентифікації автентичності підпису на око (ймовірно, багато з читачів хоча б раз у житті успішно підписувалися за батьків у щоденнику). Другий полягає в тому, що за переходу на безпаперові технології ситуація з достовірністю підпису, що представлений у вигляді електронного знімка з оригіналу, стає проблемною. Наприклад, факсимільну електронну копію, що була отримана з документа, на якому після надрукованого тексту був наклеєний підпис із печаткою, майже неможливо відрізнити від копії з непідробленого документа. Вірогідність підробки і, як наслідок, недовіра до подібних документів суттєво гальмує оперативність ведення бізнесу.

Проблему вирішують електронні пристрої фіксації та розпізнання підпису. Такі системи мають високий рівень імовірності розпізнавання, зручні у використанні, забезпечують надійний захист «електронного підпису» і мають задовільну стабільність у часі.

Відомо два підходи до автоматизованої перевірки підпису: один із них перевіряє статичне зображення підпису, тобто здійснюється аналіз особливостей представленого для перевірки підпису (offline-розпізнання), а другий ґрунтується на динамічному аналізі самого процесу проведення підпису – тобто на аналізі особливостей дій під час утворення підпису (online-розпізнання).

На практиці звичайно виокремлюють два способи обробки даних щодо підпису: просте порівняння зі зразком і динамічну верифікацію. Вважається, що другий спосіб має вищий ступень надійності, оскільки, крім статичної інформації, містить ще й динамічну. Тому другий метод набув більшого поширення. Однією з перших систем, що використовувала для контролю динамічні властивості підпису, була програма «Sign-On», яка була розроблена компанією «Auto-Sign» ще в 1986 році. За інформацією розробника, такий пристрій вартістю близько 1000 доларів забезпечував надійність, що дорівнювала одній помилці на 2,5 млн підробок.

Процес перевірки достовірності підпису проходить декілька стадій: реєстрацію, порівняння й оцінку. Для розпізнавання підпису використовуються різні технології, однією з яких є технологія на базі нейронних мереж. Сотні патентів у цій сфері були видані таким компаніям, як «IBM», «NCR», «VISA», «Adapteck» та ін.

На етапі реєстрації (отримання самого підпису) більшість технологій фіксують динамічні особливості підпису, використовуючи для цього «цифрове» перо і підкладку, а розпізнають за допомогою оригінальних алгоритмів і програмного забезпечення, що становлять ноу-хау кожної фірми-розробника. Під час проведення підпису система реєструє не тільки зображення підпису, але також і дані, що характеризують саме динаміку підпису. Така методика дозволяє досягти високого ступеня розпізнавання підпису та забезпечити достатній рівень захисту від підробок.

Далі на цьому етапі необхідно провести фіксацію та схоронність отриманої динамічної картини підпису. Дані отриманого підпису, що зафіксовані в електронному вигляді, разом із введеними додатковими персональними відомостями формують так званий об'єкт підпису (SIGNOBJ), який зашифровується та розміщується у захищеному банку даних.

Відтворювання підпису складається з процесів розшифровки об'єкта підпису та реконструкції зображення. Програмно-апаратне забезпечення має засіб перегляду, який дозволяє розглядати особливості підпису суб'єктом, який отримує документ із підписом.

На порівняльному етапі дані про динамічні та статичні характеристики підпису, які надійшли разом із документом, фіксуються та перетворюються на цифровий біометричний запис, який надалі порівнюється із заздалегідь отриманим шаблоном, який був

одержаний на основі реєстрації узагальненого взірця підпису та зберігався у БД (до відома: шаблон утворюється шляхом узагальнення особливостей як мінімум із п'яти наданих варіантів підпису).

На етапі проведення оцінки ступінь тотожності отриманого електронного підпису з шаблоном відображається в процентному відношенні на шкалі 0–100%. Величина розпізнавального порогу (у відсотках), за якого підпис вважається справжнім, може регулюватися за бажанням користувача залежно від ступеня важливості транзакції.

Наведемо перелік основних біометричних параметрів, які фіксуються під час одержання «електронного» підпису:

– траєкторія підпису в просторово-часовому відбитті;
– вектори напрямків руху пера;
– дані про положення пера (кут нахилу) під час процесу підпису;
– дані про швидкість проходу пера в процесі підпису;
– дані про наявні пришвидшення пера під час проведення процедури підпису;
– дані про характер штрихів, що залишає перо;
– дані часу підпису;
– дані про поступальні та зворотні рухи.

Система проведення перевірки достовірності формується так, щоб одержувач зміг перевірити незмінність переданого тексту й одержаної інформації про того, хто підписав, що підписав і коли та чому документ був підписаний.

Відомо, що характер підпису змінюється з часом, як і почерк людини. Залежно від віку динаміка підпису проявляється по-різному. Для того, щоб зменшити вплив вікових змін на ймовірність відмов, технології ідентифікації за підписом передбачають здійснення періодичного оновлення електронних шаблонів, що значно підвищує надійність цього методу в часовому просторі.

Технологія електронної фіксації і розпізнавання підпису застосовується у таких галузях, як:

– банківська справа;
– страхова справа;
– електронна комерція;
– автоматизація офісної діяльності;
– автоматизація підписання державних паперів;
– контроль фізичного доступу;
– контроль ув'язнених;
– облік робочого часу тощо.

Нині цей метод набув найбільшого поширення у фінансовому середовищі суспільства.

Метод електронної фіксації та розпізнавання підпису дає можливість:

1. Забезпечити надійними рукописними підписами в електронному вигляді будь-який документ, який вимагає процесу ідентифікації особи, яка підписала документ.

2. Забезпечити можливість і динамічної, і візуальної перевірки підпису, оскільки, окрім динамічної інформації, ця технологія зазвичай створює графічний файл, який є еквівалентом рукописного підпису на папері.

3. Розширити сферу застосування безпаперової документації.

4. Виключити необхідність розробки додаткового апаратного забезпечення під час здійснення процедури розпізнання (використовується без значної модифікації той же апаратно-програмний комплекс, що й під час отримання електронного шаблону підпису).

5. Забезпечити криптографічний захист електронного підпису.

6. Проводити авторизацію процедури поєднання електронного документа з електронним підписом.

7. Безпечне підписання документів у відкритих або закритих середовищах.

8. Одночасну ідентифікацію документа та користувача.

9. «Прив'язувати» до документа разом із підписом як невід'ємної додаткової інформації відомості, які містять дату, час підписання, наміри підписувача, коментарі та інше, що полегшує достовірність ідентифікації.

10. Використовувати у разі потреби електронний підпис як частину створюваної бази даних.

11. Підвищити достовірність ідентифікації за підписом, оскільки шаблон електронного підпису містить середньостатистичну інформацію, яка набагато об'єктивніше відображає особливості підпису кожної людини на відміну від рукописного підпису, який змінюється у часі.

12. Відстежувати часовий процес зміни шаблону підпису[1].

За оцінками консалтингової компанії «Acuity Market Intelligence», популярність технологій та засобів ідентифікації за підписом або почерком нині досить швидко зростає – очікується, що до 2015 року цей вид біометричних технологій зможе претендувати вже на 10% світового біометричного ринку.

Ідентифікація за почерком в основному використовується для встановлення авторства рукописного документа. Почерк є унікальною рисою кожної людини. Для автоматичної (без участі експерта) ідентифікації за почерком потрібно лише декілька рядків тексту[2].

У Російській Федерації Інститут проблем інформатики Російської академії наук (*ІПІ РАН*) спільно з компанією «BioLink» розробили рішення для здійснення біометричної ідентифікації за почерком. Уперше ця розробка була представлена ІТ-фахівцям 2–5 жовтня 2007 року на виставці SofTool у Москві.

Ця російська розробка дозволяла автоматично, без додаткового залучення експертів, встановлювати авторство рукописного тексту. Для ідентифікації достатньо лише трьох рядків. Текст не обов'язково повинен бути змістовним і суцільним – високих результатів можна досягти, отримуючи потрібну інформацію з заяв, які написані від руки, а також власноруч заповнених анкет, записників, зошитів тощо.

Переведення цієї інформації у машинозчитуваний формат проводився за допомогою звичайних сканерів. Після процедури оцифрування моделі почерку вносились до бази даних біометричної системи.

За запитом на проведення ідентифікації ця система порівнювала відомості щодо раніше зафіксованих еталонів із отриманими зразками почерку та надавала результати пошуку, які охоплювали відомості стосовно проаналізованих ідентифікаторів «кандидатів» на роль творця тексту (за ступенем зменшення ймовірності визнання їх такими).

Розпізнання за почерком найефективніше у поєднанні з ідентифікацією за іншими біометричними параметрами: відбитками пальців, голосом, обличчям та ін. Цей комплексний підхід може застосовуватися як універсальна платформа ідентифікації в системах масового обслуговування: під час здійснення державних програм виготовлення,

[1] Прохоров А. Мой дом – моя крепость, мое лицо – мой пропуск / А. Прохоров // КомпьютерПресс. – 2000. – 7 февраля. – № 7. [Электронный ресурс]. – Режим доступа: http://www.computerpress.ru/Archive/...

[2] Идентификация по почерку. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/handwriting.php…

оформлення та контролю паспортно-візових документів нового покоління, у фінансовій індустрії, на транспорті, а також для забезпечення безпеки суспільства і держави[1].

Останнім часом дедалі більше компаній переходять на нові системи документообігу. Наприклад, у другому півріччі 2008 року канадська компанія «Praxis Group», що спеціалізується на наданні консультацій із фінансових питань приватним особам і корпоративним клієнтам, перейшла на нову систему документообігу, в якій задіяні біометричні технології. Відтак співробітники «Praxis» під час підписання документів і завірення їх електронним підписом та електронним еквівалентом печатки використовують інформаційні технології.

Насамперед співробітникам фірми необхідно пройти біометричну ідентифікацію: тим самим вони підтверджують своє право на доступ до системи документообігу та здійснення операцій з електронним документом. Після того, як будь-який співробітник засвідчив свої повноваження, він може завірити створений або змінений документ за допомогою електронного цифрового підпису (ЕЦП).

Як констатували представники «Praxis Group», до впровадження інноваційної технології спонукала висока вартість старої системи та її вразливість, яка обумовлена високою ймовірністю та легкістю підробки паперових документів[2].

5.7. Ідентифікація індивідуумів за динамікою натискання на клавіші (ритм друкування або клавіатурний почерк)

Динаміка натискання на клавіші (ритм друкування) аналізує особливості друку або манеру користувача натискати на клавіші з певною швидкістю. Переваги цього способу полягають у тому, що для нього потрібна тільки клавіатура, а сам процес ідентифікації чи верифікації відбувається безпосередньо на робочому місці. Значного поширення ця технологія поки що не має[3].

Але дослідження в цій сфері біометричної ідентифікації не припиняються. Так, наприклад, компанія «BioPassword Inc.» у 2007 році випустила нову версію програми для перевірки особистості працюючого за ритмічними характеристиками набору символів на базі служб каталогів «Windows Active Directory» та технологій «Citrix». Пакет «BioPassword Enterprise Edition 3.0» був доповнений новою програмою перевірки достовірності особи, яка проводить клавіатурний набір, містить розширені можливості для організації віддаленого доступу, а також підтримує клієнтську версію на базі «Windows XP Embedded».

Пакет «BioPassword Enterprise Edition» здійснює процедуру перевірки достовірності особи працюючого в два етапи. Користувач вводить своє ім'я та пароль – водночас додатково фіксується ритм натискання на клавіші, а далі зафіксований ритм порівнюється

[1] Новая технология биометрической идентификации по почерку // Secnews.ru. – 2007. – 12 октября. [Электронный ресурс]. – Режим доступа: http://www.secnews. ru/russian/…

[2] Канадские финансисты выбирают биометрию // BIOMETRICS.RU. – 2008. – 12 сентября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Биометрия. Сам себе пароль. – 2007. – 7 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art103.html

з раніше отриманим і збереженим біометричним шаблоном, в якому записані характерні для цього користувача параметри клавіатурного ритму натискань на клавіші. Програма обробки біометричних параметрів як основний компонент системи розпізнання перевіряє, чи та особа намагається ввійти під іменем користувача і його паролем або це самозванець.

Система біометричної авторизації за допомогою перевірки ритму натискання клавіш є досить перспективною технологією – вартість упровадження такої системи втричі нижча, ніж апаратні рішення на базі жетонів.

Особливістю роботи системи перевірки за клавіатурним почерком «Enterprise Edition 3.0» є реалізація нового компоненту багатофакторної перевірки достовірності – технології KBA (Knowledge-Based Authentication /Авторизація за знанням/). Якщо після перевірки ритму друку на клавіатурі у системи залишаються сумніви щодо достовірності особи користувача, технологія KBA ставить клієнту запитання, яке спеціально генерується комп'ютерною перевіряльною програмою, на котре може відповісти тільки істинний користувач[1].

Наприкінці 2011 року з'явилась інформація, що агентство перспективних оборонних досліджень DARPA (США) почало реалізовувати нову програму «Active Authentication Program» для створення нових інструментів біометричного розпізнання індивідуумів, щоб тільки уповноважені на це особи мали доступ входу в комп'ютерні системи, докладаючи мінімум зусиль для перевірки своєї особистості. Теоретично розроблені в рамках цієї програми інструменти ідентифікації повинні розпізнавати людину, яка сідає за клавіатуру комп'ютера, за її типовими діями та характерним тільки їй способами роботи.

За словами представників DARPA, нова програма змінює нинішній напрям у біометричній ідентифікації, позбавляючи людину від необхідності запам'ятовувати паролі та мати при собі будь-які таємні дані чи предмети. Головним секретним засобом, за допомогою якого тепер буде встановлюватись особистість, – є сама людина, її звички, манери та інші унікальні властивості. До цього часу для проходження біометричної аутентифікації індивідуумам треба було здійснювати низку спеціальних додаткових операцій – заглядати в об'єктив сканера райдужної оболонки ока, прикладати палець до віконечка сканера для отримання відбитка та інше.

У рамках нової програми DARPA прагне позбавити людей від зайвих дій і розпізнавати конкретних осіб за такими ознаками, як індивідуальність манери роботи за клавіатурою. Головна мета нової програми – забезпечити такого виду перевірку особистості користувачів у типовій обстановці офісів, які є звичними для Міністерства оборони США.

Зважаючи на вразливість традиційних систем парольного захисту, федеральні відомства США проводять активну роботу зі створення біометричних карток-жетонів для перевірки особистості і за райдужною оболонкою ока, і за відбитками пальців. Такі системи запроваджуються в обов'язковому порядку для всіх штатних федеральних службовців, підрядників і контрактних працівників. Із впровадженням цієї системи до будівель федеральних відомств США можна буде потрапити тільки за допомогою таких пристроїв, що засвідчують особистість власників. Загалом доступ до федеральних комп'ютерних систем США буде здійснюватись за допомогою багатофакторної біометричної антен-

[1] Новая версия программы для идентификации по клавиатурному почерку // BIOMETRICS.Ru. – 2007. – 25 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

тифікації (доступ до будівель місця роботи за ID-карткою та подальшою перевіркою кожного індивідуума за райдужною оболонкою ока і характерним клавіатурним почерком роботи).

Запровадження такого типу біометричної аутентифікації співробітників федеральних відомств обумовлено директивою президента США щодо національної безпеки (Homeland Security Presidential Directive 12) – багатофакторна система повинна бути заходом підвищення безпеки й ефективності роботи, зниження витрат та захисту персональних даних[1].

Якби багатофакторна біометрична аутентифікації була запроваджена в Агентстві національної безпеки (АНБ) з початку 2010 року, то наслідки публікацій Едвардом Сноуденом матеріалів щодо шпигунської діяльності США були набагато меншими. Відомо, що Е. Сноуден скопіював низку цілком таємних матеріалів АНБ, які згодом оприлюднив, немаючи до них офіційного доступу, використавши для цього паролі своїх знайомих співробітників Агенства.

5.8. Можливість ідентифікації шляхом аналізу біоелектричної активності мозку і за психофізіологічним станом людини загалом

Постійне розширення можливостей вимірювання й аналізу біометричних параметрів зумовлює розширення низки питань, які вирішуються за допомогою біометрії.

Одним із перспективних напрямів біометрії вважається можливість проведення аналізу психофізіологічного стану людини, яке більш відомо за терміном «детектор брехні» або поліграф.

Визначення справжніх думок і мети дій людини завдання не менш давнє, ніж встановлення або підтвердження її особистості. Воно вирішувалося, відповідно, у різні епохи доступними на тоді засобами, наприклад, тривалими тортурами у часи інквізиції або допитами з застосуванням поліграфа (детектора брехні) у наш час.

Одним з основних принципів психофізіологічних детекторів є визначення залежності між кількістю отримуваної інформації від особи, яку перевіряють, та часом тестування. Для отримання достовірного результату треба збільшувати або час проведення тестування, або ефективність зчитування біометричної інформації, яка залежить від швидкодії програмного забезпечення, що використовується.

Класичні поліграфи під час тестування вимірюють, зазвичай, декілька біометричних параметрів особи, яку перевіряють (пульс, електрокардіограму /ЕКГ/, шкірно-гальванічні реакції), водночас здійснюється приблизно 100–200 вимірювань за секунду, а час тестування може тривати декілька годин (див. повідомлення на інтернет-сайті www.polygraph.com). Застосування методу багатоканальної електроенцефалограми дозволяє підвищити швидкість зняття інформації до 1000 замірів за секунду, що зменшує час тестування до 30 хвилин (відомості з інтернет-сайту www.brainwavescience.com).

[1] В США стартовала программа поиска новых путей использования биометрических технологий. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Застосування детекторів брехні, котрі використовують метод голосової ідентифікації, дозволяє скоротити час тестування до декількох хвилин за досягнення продуктивності фіксації вимірювальних параметрів близько 10 тисяч відліків за секунду (повідомлення з сайту www.catchcheater.com). Отже, маємо безумовний прогрес у зменшенні часу проведення тестування, але, як і у вимогах до масового застосування інших ідентифікаційних систем, бажано час тестування зменшити взагалі до декількох секунд.

За наявними прогнозами фахівців, можна очікувати, що досягнення цієї мети можливе незабаром – протягом одного-двох десятків років[1].

Європейські вчені розробили експериментальний взірець електронної системи, яка може ідентифікувати особистість людини, зчитуючи унікальну картину ефектричної активності її мозку. Відомо, що 2007 року вона проходила тестування та здійснювалися роботи з її доопрацювання.

Дімітріос Цоварас (Dimitrios Tzovaras – в деяких повідомленнях ЗМІ у російськомовному варіанті написання прізвище інтерпретується як Зоварас) і його колеги з наукового центру «Centre for Research and Technology Hellas» у Греції розробляли нову систему біометричної ідентифікації особистості, принцип роботи якої нагадує електроенцефалографію. Як повідомляло «New Scientist Tech», очікувалось, що цю систему буде практично неможливо обдурити, і тому вона може застосовуватися для забезпечення найвищого рівня захисту. Принцип дії цієї системи заснований на досить поширеному методі вимірювання активності головного мозку – електроенцефалографії (ЕЕГ). «Оскільки активність мозку людини визначається унікальною картиною електропровідних шляхів нейронів у її мозку, то цей метод придатний для ідентифікації особи», – так охарактеризував принцип дії цього методу в своїх коментарях доктор Д. Цоварас.

Перед проходженням ідентифікації користувачеві необхідно зробити попередні вимірювання ЕЕГ, з якими потім порівнюватимуться отримані дані під час проведення тестування особи. Для зняття електроенцефалограми застосовується спеціальна шапочка з електродами, кількість яких зменшена порівняно з тим, що використовується під час звичайних вимірювань, проте отриманої інформації виявляється цілком достатньо для проведення заходів з ідентифікації особистості. Система здійснює моніторинг електричної активності мозку і надсилає інформацію на комп'ютер, використовуючи безпровідний зв'язок. Далі формується своєрідний цифровий портрет електроактивності мозку клієнта. Під час проведення ідентифікаційних заходів електроенцефалограма, що знімається, порівнюється з еталонною, і комп'ютер робить висновок про ступінь подібності мозкової активності особи, яка перевіряється, з наявною картиною шаблону. Поки що під час здійснення перевірки особистості користувача клієнт повинен сидіти мовчки із заплющеними очима. Але в перспективі кожному індивідуумові можливо буде запропоновано виконання певних тестів[2].

Система, що посилено розробляється, є частиною більш великого європейського проекту, який має назву «Моніторинг людини та ідентифікація його особистості із застосуванням біодинамічних індикаторів і поведінкового аналізу» (Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis – HUMABIO). Його метою є використання різних біометрик у єдиній технології для створення більш ефективної та захищеної глобальної системи.

---

[1] Минкин В. Биометрия. От идентификации личности к идентификации мыслей / В. Минкин. [Электронный ресурс]. – Режим доступа: http://www.elsys.ru/review5.php...

[2] Паспорт мыслей: новый вид биометрии? // Досье NEWSru.com. – 2007. – 17 января. [Электронный ресурс]. – Режим доступа: http://www.egovernment.ru/newstext.php...

Низка експертів і фахівців у цій сфері біометрії вважають, що практичне використання систем ідентифікації на основі електроенцефалографії буде ускладнено. Так, Джон Догман із Кембриджського університету (Великобританія) стверджує, що використання на практиці для масової ідентифікації шоломів з електродами виглядає доволі незграбно та непрактично[1].

Прикладом реального запровадження можливості проведення аналізу психофізіологічного стану людини є повідомлення на початку 2008 року британської газети «The Times» щодо розробки системи стеження за співробітниками, патентну заявку на яку подала компанія «Microsoft». Система дозволяє визначати ефективність роботи клієнта-користувача, його фізичне самопочуття та навіть компетентність.

За повідомленням, до системи входять безпровідні датчики, які вимірюють частоту серцебиття співробітників, температуру тіла, стежать за їх діями та рухами, виразом обличчя та кров'яним тиском. У заявці також зазначено, що датчики можуть знімати з співробітника електроміограму й уловлювати «сигнали мозку» (brain signals). У тих випадках, коли співробітник перебуває у стресовому стані, система пропонує йому допомогу.

Раніше подібний моніторинг проходили тільки пілоти літаків, астронавти та працівники пожежних частин. За відомостями видання, «Microsoft» стала першою компанією, яка запропонувала використання такої методики на звичайних робочих місцях. У зв'язку з цим представники профспілок висловили побоювання, що зібрані відомості можуть слугувати підставою для звільнення співробітників.

Повідомлення про наявність такої заявки було опубліковане тільки через 18 місяців після дати її подання[2].

Фантастичним виглядає повідомлення канадських дослідників-експериментаторів із м. Оттава. Вчені з Карлтонського університету здійснюють розробку біометричної системи, яка здатна ідентифікувати користувача за допомогою його думок. Суть ідеї аутентифікаційного пристрою, що розробляється, полягає у використанні так званих мозкових хвиль як паролю. Щоб пройти ідентифікацію, людині потрібно лише «промовити» якесь слово або число подумки або, як варіант, уявити наперед узгоджену картину або просто подумати про будь-яку подію. Тобто, ідентифікатором може бути будь-яка думка, але за заздалегідь узгодженою темою. Причому, за висловленнями канадських учених, підібрати або навіть повторити такий пароль неможливо в принципі: навіть, якщо дві людини подумають водночас про одне і те ж, їх мозкові імпульси все одно будуть значно відрізнятися.

На перший погляд, – це ідеальна система аутентифікації. Проте на практиці багато фахівців стверджують, що за всієї перспективності й оригінальності ідеї її втілення у реальний продукт дуже ускладнено або майже неможливе. Причина проста: біоелектрохімічне дослідження людських думок є дуже складним процесом на клітинному рівні, а з часом будь-який, хоч і найприємніший, спогад може змінитись. Тобто систему потрібно, як мінімум, ще навчити адекватно розрізняти ці зміни та зважати на них під час здійснення процесу ідентифікації користувача.

Проте фахівці з Карлтонського університету продовжують працювати над реалізацією цього надзвичайно амбітного проекту. Яких-небудь революційних досягнень поки що немає, проте перші кроки зроблені. Дослідникам уже вдалося налагодити систему, яка реагує на елементарне уявне «так»: людині одна за одною показуються цифри,

[1] Электроэнцефалография поможет установить личность человека // Компьюлента. – 2007. – 18 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp…

[2] «Microsoft» изобрела систему беспроводной слежки // Lenta.ru. – 2008. – 16 января. [Электронный ресурс]. – Режим доступа: http://bezpeka.com/ru/news/...

частина з яких вибирається буквально «силою» думки, внаслідок чого формується деяка послідовність біоелектросигналів, що і може стати паролем[1].

2008 року дослідники з Маастрихтського університету (Нідерланди), скориставшись технологіями нейровізуалізації (загальна назва методів, що дозволяють візуалізувати структуру, функції і біохімічні характеристики мозку) та останніми на той час досягненнями отримання мозкової інформації, змогли зареєструвати сигнали зміни мозкової активності, які відповідають за розпізнавання голосової та мовної інформації. Нова технологія може застосовуватися в комп'ютерних системах розпізнавання мовної інформації та ідентифікації індивідуумів за голосом[2].

Зважаючи на наведені відомості, можна зробити висновок, що вельми перспективним виглядає напрям біометрії, який ґрунтується на аналізі психофізіологічного стану людини. Проте для масового застосування «поліграфів» або «детекторів брехні» потрібно суттєво зменшити час тестування (спочатку хоча б до двох десятків секунд). Не виключено, що це незабаром може стати реальністю. У майбутньому можлива поява апаратно-програмних комплексів для ідентифікації намірів і мотиваційної структури психіки. Так з'явиться можливість припинення запланованих, ще нездійснених злочинів за допомогою автоматичного психофізіологічного тестування людини, що потрапляє в зону контролю. Саме таким майбутнє уявляють багато фахівців із біометричних технологій.

5.9. Ідентифікація за запахом

Унікальний запах, який характерний усім ссавцям, від мишей до людини, неможливо замаскувати, навіть змінивши дієту або за допомогою гостропахучих продуктів, наприклад часнику, – «запахові відбитки» все одно можна розпізнати. Про це зазначалося у статті, що була опублікована американськими вченими в журналі «PLoS ONE» у жовтні 2008 року. За висловленням одного з авторів статті Джея Куака: «Отримані дані показують, що індивідуальний запах, як і відбитки пальців, може бути використаний як метод встановлення особистості».

Індивідуальний запах ссавців так званий одортип обумовлюється особливостями певного комплексу генів, що пов'язані з імунною системою. «Запахові сліди» залишаються під час виділення поту та сечі з живого організму. Ці рідини містять велику кількість летючих органічних речовин, багато з яких мають сильний специфічний запах. Результати проведених досліджень дозволили зробити висновок, що «генетичний запах» може бути розпізнаний як за допомогою живих «сенсорів», так і хімічним методом за допомогою «електронного носа»[3].

Досвід британських учених також дозволяє однозначно стверджувати, що використовуючи унікальний запах, можна провести біометричну ідентифікацію людини. Група дослідників із низки університетів, що розташовані в Англії, Австрії та США,

[1] Биометрия теоретическая и прикладная // Русские документы. [Электронный ресурс]. – Режим доступа: http://www.rusdoc.ru/articles/...

[2] Людей можно идентифицировать по «отпечаткам» мозговой активности // Компьюленты. – 2008. – 12 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Американские ученые разрабатывают новую технологию биометрической идентификации // РИА Новости. – 2008. – 1 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

здійснили дослідження й удосконалили метод проведення аналізу слідів ароматичних речовин, які кожна людина залишає після себе. Вони сподіваються, що у підсумку на підставі проведених досліджень будуть розроблені судові методи електронної ідентифікації людини за запахом. Напрацьовані технічні рішення вже розглядаються з погляду можливого використання у судовій практиці, запропонована технологія подібна до методів аналізу ДНК і за відбитками пальців. Загалом, на думку дослідників, метод ідентифікації за запахом можливо застосовувати як біометричний параметр аналогічно способу ідентифікації за відбитками пальців.

За доступними відомостями, американські збройні сили замовили здійснення досліджень із метою розроблення пристроїв, які б могли встановлювати особистість людей за запахом, а Служба Судової медицини Великобританії проводить дослідження з метою визначення можливостей використання цього способу ідентифікації для потреб криміналістики. Європейська науково-дослідна організація звернула увагу на можливе використання у майбутньому пристроїв на основі одорологічних методів («електронного носа») для забезпечення безпеки аеропортів і контролю за доступом на літаки[1].

5.10. Відомості про інші методи ідентифікації, які поки що не набули поширення

Нині постійно з'являються повідомлення про нові способи ідентифікації та верифікації особистості людини. Більшість із них застосовуються як додаткові методи для поліпшення надійності роботи існуючих апаратно-програмних комплексів розпізнавання, тобто вони, як правило, використовуються як додатки до вже існуючих методів біометричної ідентифікації.

Наприклад, біометрія аналізу шкірної текстури здійснює пошук і виявлення унікальної текстури та індивідуально сформованих елементів певної ділянки шкірного покриву особи, що дозволяє сформувати унікальний ідентифікатор відбитка шкіри індивідуума. Оскільки технологія розпізнання за відбитками шкірного покриву однотипна до традиційної технології ідентифікації за обличчям і використовує одні й ті ж пристрої отримання зображень, вона легко вбудовується у системи розпізнавання лиця особи та забезпечує значно надійнішу ідентифікацію ніж тоді, коли застосовується тільки сама технологія ідентифікації за обличчям.

По суті, дві різні характерні особливості одного і того ж зображення (картини зображення обличчя особи загалом та текстури шкіри виокремленої ділянки обличчя) аналізуються водночас за допомогою двох технологій і сумарно збільшують якість розпізнавання, що зрештою позначається на надійності роботи використовуваної мультибіометричної системи ідентифікації за зображенням лиця особи[2].

Нині вчені університету Саутгемптона (Великобританія) розробляють систему біометричної ідентифікації людини за її ходою. Свого часу британське інтернет-видання

[1] Человека можно идентифицировать по запаху так же, как и по отпечаткам пальцев // KM.ru. – 2007. – 22 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрические системы доступа Identix // Борьба с преступностью за рубежом (по материалам зарубежной печати). – № 4. – М.: ВИНИТИ. – 2008.

«Computing» повідомляло, що дослідники мали створити промисловий зразок до Олімпійських ігор 2012 року в Лондоні.

За словами керівника проекту Джона Картера (John Carter), манера ходи кожної людини унікальна і за цією ознакою можна ідентифікувати індивідуумів (особливо працівників компаній, установ) під час їх пересування у закритих приміщеннях (наприклад, в аеропортах). За словами Д. Картера, нова технологія біометричної ідентифікації може бути цікавою також для поліції, армії та будь-якої бізнес-структури, де потрібно забезпечити контроль доступу. Вона фіксує пересування людей, формує тривимірну модель їх повного зображення, і на цій основі здійснює ідентифікацію. «Відеокамери також фіксують інформацію про лиця осіб – на той випадок, якщо перший метод ідентифікації не спрацює, – пояснює Д. Картер. – Ідентифікація за ходою не функціонує ізольовано, вона забезпечує додатковий рівень безпеки, який до того ж не такий нав'язливий».

Розробники нової технології підкреслюють, що їх рішення в жодному разі не є альтернативою традиційним методам ідентифікації за відбитками пальців, райдужною оболонкою очей та обличчям, а слугує лише для їх доповнення. Ця розробка демонструє можливості використання різних способів ідентифікації, крім поширеної «великої трійки». Основною метою використання доповнювальних засобів ідентифікації є підвищення рівня безпеки, адже забезпечення безпеки фізичних і юридичних осіб є однією з найважливіших вимог сучасності[1].

Із цим повідомленням деякою мірою перегукується інформація про нову систему біометричної ідентифікації за ходою, яку розробили вчені Національної лабораторії фізики Великобританії (NPL). Людей тепер можна ідентифікувати та відслідковувати навіть під час звичайної прогулянки. NPL разом із Центром сучасних комп'ютерних технологій (CAST) і ще декількома науковими інститутами винайшли технологію, за допомогою якої можна спостерігати за всіма переміщеннями людини.

Спеціальна комп'ютерна програма обробляє дані з мініатюрних камер прихованого спостереження. У кожному кадрі силует людини відділяється від фону навколишнього пейзажу, всі рухи фіксуються, а потім спеціальна комп'ютерна програма здійснює ідентифікацію людини. На основі цих даних можна дізнатися, де цей індивідуум бував і що робив.

Сканування райдужної оболонки очей та розпізнавання за обличчям можуть не спрацювати, якщо людину треба ідентифікувати на досить великій відстані. Для цього потрібно високоякісне розрішення, але цей параметр дуже низької якості у камерах прихованого спостереження. Водночас запропонований метод ідентифікації, який розпізнає силует за особливостями людської ходи, дає набагато більше можливостей для проведення ідентифікації[2].

На думку індійських експертів із біометричних технологій, неповторні особливості, що характерні ході кожної людини, можна використовувати для відстеження осіб, які підозрюються у сприянні тероризму, а також для встановлення кримінальних елементів чи осіб, що намагаються скористатися підробленими документами або маскують свою зовнішність.

Відомості, що дозволяють фіксувати особливості ходи індивідуумів, надходять із камер відеоспостереження. Система фіксує весь «закінчений» цикл рухів, що характери-

[1] Идентификация по походке: реальнее, чем кажется // Biometrics.ru. – 2007. – 27 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Новая система биометрической идентификации по походке изобретена в Британии // RT Russian. – 2012. – 25 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

зують ходу певної особи. Ці дані перетворюються на цифрову модель, яка, своєю чергою, обробляється за допомогою математичних методів статистичного аналізу (так званої ентропії Шеннона).

Під час формування електронної картини ходи насамперед аналізується висота підйому ніг і частота кроків об'єкта контролю. Ці результати порівнюються з відомостями, які вже накопичені в існуючому банку даних, їх також можна зіставляти з інформацією, що надходить безпосередньо від камер відеоспостереження за будь-який проміжок часу або можуть бути одержані з інших відеозаписів.

На думку авторів експерименту, їм вдалося досягти непоганих результатів розпізнавання, проте виникли й проблеми. Зокрема, на результати ідентифікації впливає кут, з якого була проведена відеозйомка: під час зіставляння електронних шаблонів зображень різних відеозйомок, де відмінність кута зйомки становила понад 10 градусів, відсоток розпізнання погіршувався.

Водночас нова система ідентифікації добре зарекомендувала себе в ситуаціях, коли учасники експерименту змінювали швидкість ходи.

Індійські фахівці вважають, що запропонована ними технологія буде затребувана в аеропортах, банках, місцях розташування військових об'єктів. За їх твердженням, головною перевагою нової технології є той факт, що ідентифікація здійснюється дистанційно, тобто на значній відстані, а тому в служби безпеки є деякий запас часу, протягом якого можна відповідно зреагувати на можливу загрозу від людини, рухи якої є «нестандартними»[1].

Цей метод може стати в нагоді особливо в тих випадках, коли є відеозапис рухів (ходи) невстановлених осіб у масках із місця вчинення злочину, в такому разі під час здійснення відеоспостереження в інших суспільних місцях з'являється можливість їх ідентифікації та отримання фотозображень лиця конкретних індивідуумів, що дає підстави для проведення щодо них подальших оперативно-розшукових заходів.

В Ізраїлі проходить тестування нова технологія біометричної ідентифікації – за фіксацією характерних рухів зіниць очей особи, яку ідентифікують, під час стеження за об'єктом, що переміщується. Як сканер використовується веб-камера, а для демонстрації рухомих об'єктів застосовується звичайний комп'ютерний монітор. За висловленнями одного з авторів нової технології, представлені алгоритми розпізнавання формуються на останніх досягненнях анатомії, фізіології, хімії та результатах досліджень структури ока.

На думку розробників, нова технологія визначається досить високою ефективністю, оскільки характер міміки рухів очей під час відстежування рухомого об'єкта суто індивідуальний, а відтак не піддається підробці.

Створення перших промислових зразків планувалось ще у 2009 році. Автори розробки вважають, що насамперед їх рішення може бути використане для ідентифікації користувачів онлайнових платіжних систем[2].

Технології ідентифікації осіб за рухом їх очей продовжують розвиватися. На міжнародному конкурсі, організатором якого є авторитетна міжнародна організація – Інститут інженерів по електротехніці та електроніці (Institute of Electrical and Electronics Engineers /IEEE/), мали бути протестовані можливості цієї технології. Конкурс мав

[1] Террористов узнаем по походке // Biometrics.ru. – 2008. – 11 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

[2] Пользователей платежных сервисов предлагают идентифицировать по характеру движения глаз // Biometrics.ru. – 2008. – 26 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

відбутися наприкінці 2013 року в рамках об'єднаної Міжнародної конференції з біометрії, яку також проводить IEEE[1].

2012 року компанія «Eyeverify» запатентувала нову технологію біометричної ідентифікації власників планшетів і смартфонів. Нова технологія біометричної ідентифікації власників цих пристроїв ґрунтується на їх розпізнаванні за малюнком вен, який одержується під час сканування білків очей.

За інформацією, наданою головою компанії «Eyeverify», для нового напряму непотрібне жодне додаткове устаткування: для одержання необхідного їй зображення біометричного ідентифікатора – досить буде скористатися цифровою камерою, вбудованої в смартфон або планшет.

Фірма тільки розробила відповідний мобільний додаток, який забезпечує зручність, точність і високу швидкість нової технології біометричної ідентифікації, яка повинна захистити гаджети від несанкціонованого доступу[2].

Нині з'являються нові приклади розробки сучасних технологій біометричної ідентифікації. У центрі біометричних досліджень Політехнічного університету Гонконгу для розпізнавання особистостей людей пропонується застосовувати метод сканування їх язиків. Доцент університету Леї Жанг (Lei Zhang) стверджує: «У різних людей і форма язика різна, й, таким чином, за його формою ми можемо встановити приналежність язика конкретній людині».

У розробках китайських фахівців для знімання інформації за цим екзотичним методом застосовується технологія лазерного сканування. З її допомогою формується тривимірна модель язика протягом двох-трьох секунд. Далі на моделі визначаються найбільш характерні ознаки, проводиться їх порівняння з наявними шаблонами язиків, що зберігаються у відповідній базі даних і ухвалюється рішення щодо ідентифікації користувача.

Про можливості практичного застосування, орієнтовну вартість такої системи ідентифікації і терміни представлення промислово-дослідних екземплярів апаратури не повідомлялось[3].

За останніми повідомленнями ЗМІ з'являється дедалі більше компаній, які інвестують гроші у розвиток нових технологій, зокрема таких, що дозволяють користувачам взаємодіяти з комп'ютерами та мобільними обладнаннями природнім для людини способом – за допомогою жестів, голосу, вираження обличчя тощо[4].

Компанія «Bionym» запропонувала використовувати нове біометричне обладнання для аутентифікації, яке реєструє електричну активність серця людини. Розробники вважають, що цю технологію неможливо обдурити. Прилад на базі цієї розробки має форму невеликого браслета. Фахівці «Bionym» дали йому назву «Nymi».

Сфера застосування «Nymi» є різною. Браслет можна використовувати як брелок для автомобіля чи ключа. За його допомогою можна оплачувати покупки. Крім того, браслет «розуміє» жести, тому його можна застосовувати як пульт дистанційного керування.

---

[1] Новая биометрическая технология будет протестирована в ходе международного конкурса // Biometrics.ru. – 2013. – 28 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Планшеты и смартфоны защитит новая биометрическая система // Biometrics.ru. – 2012. – 26 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Китайцы предлагают идентифицировать людей по форме языка // Biometrics.ru. – 2008. – 29 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp.

[4] Intel Capital продолжит инвестировать в биометрические системы // Biometrics.ru. – 2013. – 7 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

У продажі новий прилад мав з'явитися на початку 2014 року. Вартість браслета «Nymi» має становити приблизно 80 доларів[1].

Нову революційну мультибіометричну систему створюють фахівці з Університету Калгарі (Канада). Ця система буде здатна до самонавчання та здійснення когнітивних процесів. За наявними відомостями у новій розробці буде використовуватись розпізнавання людей за відбитками пальців, обличчям та райдужною оболонкою ока. А також мультибіометричну систему передбачається наділити здатністю до аналізу «поведінкової» біометрії, зокрема людської ходи та жестів, що повинно суттєво збільшити точність біометричної ідентифікації зменшити кількість небажаних спрацьовувань, коли одна людина може прийматися за іншу.

Одна з переваг подібного мультибіометричного підходу полягає в підвищенні гнучкості системи: вона не буде «прикута» лише до одного біометричного ідентифікатора, а зможе самостійно вибирати той, використання якого найбільш оптимальне в конкретних умовах. Але інноваційним рішенням є здатність до самонавчання, що має забезпечити використання технології нейронних мереж. Ці можливості будуть особливо потрібні під час здійснення біометричної ідентифікації конкретної особи за великого скупчення людей (наприклад, серед пасажирів аеропорту). Завдяки своєму штучному інтелекту система зможе самостійно відсіяти «інформаційний шум», який неминуче виникає під час руху натовпу, зміни умов освітлення або ж через не занадто вдале розташування камер відеоспостереження. У підсумку майже безпомилково здійснюється розпізнавання людини, чия присутність на транспортному об'єкті небажана.

Дату створення промислового зразка нової мультибіометричної системи вчені з Університету Калгарі не називають, заявляючи лише, що зараз вони здолали тільки половину потрібного шляху[2].

Загалом, підсумовуючи можливе впровадження інноваційних рішень, акцентуємо, що незабаром новинкою у біометричній галузі стане ідентифікація індивідуумів, що перебувають у русі, причому будуть задіяні можливості мультибіометричних систем.

Згідно з прогнозами «КПМГ» (KPMG – міжнародна мережа фірм, яка надає аудиторські, податкові та консультаційні послуги), у найближчі три роки до найбільш перспективних інноваційних розробок великі технологічні компанії відносять і біометричні технології. Найбільш стрімко будуть розвиватися системи ідентифікації за жестами (рухами), обличчям та голосом[3].

[1] Биометрический браслет узнает пользователя по активности сердца // Zhelezyaka.com. – 2013. – 4 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Новая мультибиометрическая система будет основана на технологиях нейронных сетей // Biometrics.ru. – 2012. – 18 июля.

[3] Биометрические технологии вошли в число самых перспективных и инновационных // CRN/RE. – 2013. – 5 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розділ 6

СУЧАСНІ НАПРЯМИ ЗАСТОСУВАННЯ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ. МАЙБУТНЄ БІОМЕТРІЇ

6.1. Основні напрями застосування біометричних технологій

У виданні «Business Standard» був опублікований прогноз індійських аналітиків щодо десяти ключових тенденцій розвитку інформаційних технологій (ІТ) у 2008 році. В огляді були зазначені такі тенденції:

– розвиток Grid-технології, яка займається віртуальними обчисленнями;

– подальше розповсюдження біометричних технологій;

– поширення «фотоелектричної енергетики», коли комп'ютерні та інші пристрої будуть отримувати живлення від сонячних батарей та інших подібних джерел живлення;

– надання програмного забезпечення (ПЗ) в оренду, коли користувачі платять авторам програм не за ліцензії на ПЗ, а за його експлуатацію (Software-as-a-service – Saas);

– розширення використання програмного забезпечення з відкритим кодом;

– підвищення «корпоративної мобільності» (за оцінками авторів огляду, чисельність мобільних користувачів у 2008 році сягне 800 млн чоловік);

– зростання популярності «мобільних розваг» (мобільне телебачення, онлайнові ігри, соціальні мережі тощо);

– активне застосування flash-пам'яті як різноманітних накопичувачів;

– подальше зростання комп'ютерної злочинності;

– зростання кількості загроз персональним комп'ютерам.

Нині ми можемо оцінити точність цього прогнозу. Наголосимо, що наша дійсність підтверджує правдивість цього передбачення. Більшість із вказаних тенденцій на час написання посібника значною мірою вже реалізовані. А передбачення щодо поширення біометричних технологій перевершило найсміливіші очікування.

Головним рушієм біометричного ринку автори огляду вважали державні органи. І вони не помилились. У багатьох країнах світу здійснені або перебувають на завершальній стадії програми запровадження біометричних закордонних паспортів, а в низці держав і впровадження загальногромадянських біометричних ID-карток, дедалі більшого поширення набувають ідентифікаційні картки платників податків, продовжують розвиватися біометричні системи контролю за доступом до приміщень і територій різних державних структур, завершується обладнання автоматичними системами контролю за перетином кордону контрольно-пропускних пунктів (КПП) на кордонах провідних держав світу.

Автори огляду констатували, що відбудеться подальше збільшення питомої ваги використання біометрики в корпоративних структурах, але найбільше зростання

відбудеться у приватній сфері. Розширення сфер застосування біометрії насамперед пов'язане із зростаючою потребою державних органів, бізнесу та простих громадян у забезпеченні належного рівня безпеки.

Але найбільше вражає передбачення авторів щодо прогнозу все зростаючого використання біометричних рішень у мобільних телефонах та інших пристроях персонального вжитку.

Як перспективні види біометричних технологій автори огляду, крім розпізнавання за відбитками пальців, відзначали методи ідентифікації за райдужною оболонкою очей, голосом, почерком і підписом, а також підкреслювали значний потенціал мультибіометрічних рішень і багатофакторних систем ідентифікації[1].

Нині експерти визначають такі основні напрями застосування біометричних технологій:

1. *Безпека суспільства і держави.* Біометричні технології широко використовуються для забезпечення безпеки та створення переваг постійним клієнтам у таких сферах людської діяльності, як транспорт (насамперед контроль доступу в аеропортах), проведення електронних транзакцій (банки, страхові компанії), надання послуг клієнтам торговельними і сервісними компаніями, а також дедалі ширше застосування біометрії в охороні здоров'я та освіті.

2. *Реалізація масштабних проектів* створення паспортно-візових, фінансових і об'єктно-транспортних ідентифікаційних систем.

3. *Контролю за доступом* – впровадження надійних й економічних засобів розмежування доступу на територію об'єктів, споруд і внутрішніх приміщень будинків.

4. *Облік робочого часу.* Дозволяє досягти достовірності та оперативності в управлінні таким ключовим активом, як персонал (особовий склад) установ, організацій, підприємств і компаній.

5. *Захист інформації.* Запроваджуються масштабні та багатофункціональні системи ідентифікації користувачів у інформаційних мережах, операційних системах, різних додатках до типового програмного забезпечення.

Постійний розвиток і здешевлення систем технологій біометричної ідентифікації дозволяє дедалі ширше застосовувати ці засоби в різноманітних рішеннях щодо забезпечення інформаційної безпеки комп'ютерно-телекомунікаційних мереж, у корпоративних системах обліку робочого часу (особливо для контролю бізнес-процесів, які вимагають строгої персоналізації і персональної відповідальності).

Отже, можна стверджувати, що біометрична ідентифікація в різних формах вже є і буде надалі залишатися основою майбутньої інфраструктури інформаційної безпеки будь-якої установи, а також використовуватиметься у багатьох прикладних рішеннях.

Відбитки папілярних узорів пальців, сканування обличчя або райдужної оболонки очей – у будь-якому випадку під час використання біометричних методів йдеться про підвищення рівня безпеки та комфорту. Насамперед за допомогою біометричних ідентифікаційних систем установи та підприємства всіх форм власності прагнуть захистити конфіденційну інформацію, забезпечити надійну охорону об'єктів і будівль, не кажучи вже про встановлення та підтвердження особистості індивідуума.

Ринок систем ідентифікації особистості за особливостями людського тіла нині інтенсивно розвивається. За дослідженнями компанії «International Biometrics Group» (IBG),

[1] Расширение использования биометрии – одна из ключевых тенденций развития информационных технологий // BIOMETRICS.Ru. – 2008. – 10 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

у 2006 році світовий обсяг продажу біометричних засобів сягнув 1,8–2 млрд доларів. 2010 року ця цифра становила майже 4,9 млрд доларів (дані «IBG»), що відповідає щорічному зростанню в 30%[1].

За даними аналітиків «Frost & Sullivan», загальносвітовий обсяг продажу біометричних засобів у 2012 році мав становити приблизно 7 млрд доларів. Але прогноз не справдився. Світова фінансова криза, яка почалася в другій половині 2008 року, внесла свої корективи. У огляді розвитку світового біометричного ринку, який був опублікований у 2011 році, компанія «Frost & Sullivan» прогнозувала, що у 2016 році обсяг цього ринку може сягти лише 5,3 млрд доларів[2]. Отже, світовий біометричний ринок невпинно нарощує обсяг продаж, тільки не завжди такими темпами, які вказуються у прогнозах.

Згідно з прес-релізом «Acuity Market Intelligence», основою цього зростання є дія таких чинників: біометрична ідентифікація користувачів у IT-системах (їй відводиться головна роль), зростання мобільності населення і децентралізація управління робочою силою, загальносвітове поширення електронних транзакцій, розширення надання сервісних послуг «електронного уряду». Інтегрована дія всіх наведених чинників, своєю чергою, зумовлює нагальну потребу в ідентифікації такого рівня, яку може надати тільки біометрія, констатують автори прогнозу.

У прес-релізі були наведені тенденції змін у сегментації біометричного ринку. Зокрема виокремлені два ключові сегменти: суспільно-державний (електронні системи прикордонного контролю /запровадження паспортно-візових документів нового покоління і вся необхідна для цього інформаційно-телекомунікаційна структура/, ідентифікація осіб, системи безпеки) і комерційний (корпоративна безпека і захист інформації, фінансові транзакції).

У контексті еволюції цих секторів відбуватиметься подальший розвиток основних прикладних сфер застосування біометрії – контролю фізичного доступу, захисту інформації, ідентифікації особистості, особливо за допомогою систем відеоспостереження[3].

У протистоянні з тероризмом унаслідок вчинення безперервних терористичних акцій у деяких країнах світу та відсутності гарантій унеможливлення їх учинення в інших державах серйозно змінилося ставлення до забезпечення внутрішньої безпеки відповідних державних структур і, отже, й доктрини національних безпек. Протидія можливим і наявним терористичним загрозам вимагає найтіснішої кооперації розвідувальних, контррозвідувальних, поліцейських, військових та інших органів. Комплексний менеджмент ризиками безпеки повинен охоплювати забезпечення безпеки на різних напрямах, включаючи інформаційно-технологічну, фізичну, екологічну й особисту безпеку. Стратегія безпеки повинна охоплювати весь ланцюжок, зокрема постачальників, субпідрядників і замовників[4].

Наведемо низку чинників, які, на думку аналітиків «Frost & Sullivan», сприяють зростанню впроваджень біометричних технологій у наше життя. По-перше, вартість біометричних систем постійно знижується, а це, своєю чергою, зумовлює збільшення

---

[1] Мэнди Кюн. Защита доступа биометрическими методами / Кюн Мэнди // LAN. – 2007. – 2 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Объем мирового биометрического рынка к 2016 году превысит пять миллиардов долларов // BIOMETRICS.RU. – 2011. – 22 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Прогноз развития биометрического рынка на долгосрочную перспективу // BIOMETRICS.Ru. – 2007. – 6 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Технические средства защиты от террористических угроз // Борьба с преступностью за рубежом (по материалам зарубежной печати). – М.: ВИНИТИ, 2008. – № 1. – С. 23–26

кількості їх замовників і користувачів. По-друге, застосування біометричних технологій забезпечує багаторівневий підхід до комплексного вирішення питань безпеки, що надає цим системам додаткову привабливість. По-третє, успішна реалізація масштабних біометричних проектів (наприклад, у сфері прикордонного та міграційного контролю) сприяє подальшому визнанню переваг біометрії.

Цікавим є підхід експертів «Frost & Sullivan» до виокремлення найбільш перспективних напрямів розвитку світового біометричного ринку. До них автори огляду включили:

– використання технологій біометрії в діяльності правоохоронних і силових структур;

– зростання кількості біометричних проектів, які реалізуються під патронатом урядових структур (біометричні паспорти, візи, ID-карти);

– інтенсивне запровадження біометрії в системи контролю фізичного доступу та захисту корпоративних інформаційних ресурсів;

– застосування біометричних технологій в інтересах споживачів, зокрема у різних гаджетах, інших мобільних пристроях, ноутбуках, протиугонних автомобільних системах тощо.

Аналітик «Frost & Sullivan» Арчана Рао (Archana Rao) особливо відзначав, що зміцненню позицій біометричних систем на ринку рішень з ідентифікації сприяє невпинне підвищення їх продуктивності та розширення можливостей їх інтеграції з іншими інформаційними технологіями[1].

Більш детально напрями розширення застосувань біометричних технологій викладені у розділі 7 «Майбутнє біометрії. Схвалення громадською думкою використання сучасних досягнень біометрії».

6.2. Три основні напрями застосування сучасних біометричних технологій

Фахівці з біометрики зазначають такі три основні напрями використання біометричних технологій, які не залежать від державної або недержавної форми власності об’єктів безпосереднього застосування біометричних технологій: системи контролю й управління доступом (СКУД), системи обліку робочого часу (СОРЧ), які в останніх технологічних рішеннях об’єднуються в єдиний комплекс із СКУД, та системи захисту інформації від несанкціонованого доступу на базі біометричної ідентифікації користувачів.

За оцінками експертів, наприкінці першого десятиріччя XXI століття приблизно 60% від загального обсягу біометричного ринку займали системи контролю й управління доступом. Як правило, засоби біометричної ідентифікації в цих системах використовуються разом з іншими існуючими стандартними засобами безпеки. Перспективним напрямом розвитку СКУД вважається об’єднання мультибіометричних технологій (коли розпізнавання здійснюється одночасно за декількома параметрами, наприклад, за відбитками пальців і 2D- або 3D-цифровою моделлю лиця особистості, яка ідентифікується)

[1] Объем мирового биометрического рынка к 2016 году превысит пять миллиардов долларов // BIOMETRICS.RU. – 2011. – 22 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

з іншими системами контролю за доступом (коли встановлення особистості користувачів для надання дозволу на прохід через турнікет, шлюз та інші пристрої здійснюється за допомогою ідентифікаторів, що використовують, крім біометричних параметрів, інші носії ідентифікуючих ознак: PIN-код, безконтактні проксиміти-картки, токени тощо).

Другий суттєвий напрям розвитку біометричних систем – це контроль робочого часу та розмежування доступу, що є системою реєстрації співробітників установ, підприємств і фірм на вході та виході з території чи приміщень об'єкта, на якому встановлені відповідні програмно-апаратні комплекси проведення контролю. Під час застосування таких систем один і той же співробітник вже не зможе відмітити при реєстрації свого проходження також прихід на роботу своїх друзів-колег (як це часто буває під час застосування карткових систем, які фіксують насправді явку на роботу не конкретного співробітника, а виданого йому матеріального ідентифікатора). Крім того, біометричні ідентифікатори неможливо втратити чи забути, тобто не потрібно витрачати гроші на постійні додаткові закупівлі небіометричних ідентифікаторів замість втрачених і зіпсованих[1].

Останнім часом з'являється дедалі більше повідомлень від компаній, що працюють на ринку біометричних технологій, про створення систем, в яких значно розширені функції контролю фізичного доступу й обліку робочого часу, та котрі оптимізовані для застосування не тільки на малих і середніх підприємствах, але й у великих компаніях, що мають доволі складну і розгалужену структуру.

У багатьох теперешніх біометричних розробках систем контролю й управління доступом підтримується багаторівнева організаційна ієрархія доступу до приміщень (території розташування) підрозділів, що входять до установи чи компанії, а облік робочого часу ведеться не тільки загалом у компанії, але і за кожним її структурним підрозділом. Крім того, передбачена можливість розмежування доступу керівників окремих підрозділів до відомостей, що характеризують діяльність організаційних структурних одиниць. Менеджери будь-якої служби можуть ознайомитися тільки зі звітами структурної одиниці, яку вони очолюють, а відомості щодо компанії загалом та за всіма її підрозділам доступні тільки керівникам, інспекторам та операторам, яким адміністратор корпоративної системи відповідно до існуючого дозволу керівництва надає право на доступ до всієї узагальнювальної інформації.

У більшості технологічних рішень, що були розроблені в 2006–2013 роках, істотно розширені функції підсистеми контролю за фізичним доступом, які реалізовані на базі термінала з вбудованим сканером відбитків пальців і контролером управління виконавчими механізмами: турнікетами, електромеханічними замками, шлюзами, хвірткими та іншими подібними пристроями. У разі потреби передбачена можливість автономного режиму функціонування термінала: якщо раніше для роботи необхідною умовою була наявність його постійного зв'язку з сервером, то тепер термінал здатний працювати у самостійному режимі. Навіть у разі збоїв у мережі та тимчасової недоступності сервера за будь-яких причин сучасні програмно-апаратні комплекси здатні продовжувати здійснення контролю за доступом у приміщення: клієнтам досить торкнутися вікна сканера відбитків пальців, щоб термінал зміг їх ідентифікувати і надати дозвіл на прохід або ж заборонити його, подавши відповідний сигнал до замка чи турнікета[2].

---

[1] Парамонова Н. Проба сканера отпечатков пальцев BioLink U-Match MatchBook / Н. Парамонова. – 2007. – 13 апреля. [Электронный ресурс]. – Режим доступа: http://www.terralab.ru/input/…

[2] Интегрированная система учета рабочего времени и контроля доступа BioTime: новый год, новая версия, новые возможности. – 2007. – 1 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Як правило, в останніх розробках СКУД використовується багатофакторний або мультибіометричний режими контролю доступу, коли ідентифікація користувачів для проходу через турнікет, шлюз і подібні пристрої здійснюється за поєднанням різних ідентифікаційних ознак: відбитків пальців, обличчя осіб, PIN-коду, безконтактних проксиміті-карток.

Розрізняють автономні системи контролю й управління доступом та системи мережевого контролю й управління доступом.

Автономні системи призначені для захисту локальних приміщень від проникнення небажаних осіб. В основному ці пристрої встановлюються на вхідні двері і швидко та надійно проводять розмежування осіб, які здебільшого перевіряються за відбитками пальців. Це пов'язано з тим, що системи контролю за папілярними візерунками пальців є найбільш привабливими за таким параметром, як співвідношення якість/ціна, тому здебільшого перевага надається системам ідентифікації за відбитками пальців. Хоча у разі потреби можуть використовуватися й інші біометричні характеристики або їх симбіоз. Зчитувач і контролер із вбудованою незалежною пам'яттю в автономних системах розташовуються в одному апаратному пристрої. Такі системи дуже легко встановлюються і доволі прості в експлуатації. Швидкість самого процесу ідентифікації не перевищує двох секунд.

Мережеві системи контролю за доступом призначені для корпоративного використання і розмежовують доступ співробітників організації на всій території об'єкта: у віддалених офісах, магазинах, складах і структурних підрозділах. Програмно-апаратний комплекс системи працює під управлінням центрального сервера, що дозволяє здійснювати облік подій у режимі реального часу та формувати звітність на підставі даних про вхідні–вихідні проходи. Ідентифікація за біометричними параметрами забезпечує високу надійність і зручність експлуатації комплексу, як правило, здебільшого жодних карток і ключів користувачам при собі мати не потрібно. Розроблені останнім часом системи дозволяють гарантувати те, що будь-який зареєстрований системою вхід або вихід із приміщення персонально здійснив безпосередньо тільки сам співробітник – носій відповідного біометричного параметра.

Ціни на сучасні біометричні системи контролю за доступом у кожному випадку індивідуальні та залежать від завдань, які виконуються за їх допомогою[1].

Сучасна система обліку робочого часу, окрім розмежування прав менеджерів організації на доступ до її даних згідно з рівнем розподілу управлінських функцій та підтримки функціонування територіально-розподіленої мережі, яка об'єднує в єдиний комплекс усі віддалені філії, надає користувачам можливість зручного та швидкого формування різноманітної звітності відповідно до встановленої ієрархічної вертикалі управління. Крім того, всі вони переважно використовуються одночасно з системами обліку робочого часу.

На думку спеціалістів, системи доступу та захисту інформації, що використовують біометричні технології, є не тільки найнадійнішими, але і найзручнішими для користувачів на сьогоднішній день. Оскільки не потрібно запам'ятовувати складні паролі, постійно носити з собою апаратні ключі або смарт-картки. Достатньо лише прикласти до сканера палець або повернути в його напрямку лице, підставити для сканування око або долоню, щось вимовити, щоб отримати дозвіл на проходження у приміщення або отримати доступ до відповідної інформації.

[1] Биометрия-1 // Biometrics.ru. – 2007. – 25 июля. [Электронный ресурс]. – Режим доступа: http://www.smart-home.spb.ru/bio...

І незважаючи на деякі існуючі проблеми, які будуть розглянуті окремо у спеціальному розділі, біометрія дедалі більше використовується для забезпечення безпеки та контролю за доступом до будь-яких режимних об'єктів, зокрема і до інформаційних мереж і баз даних.

Розглянемо більш детально практичну реалізацію кожного з трьох зазначених основних напрямів використання біометричних технологій.

6.3. Системи контролю й управління доступом (СКУД)

Проблема забезпечення безпеки стає з кожним роком дедалі актуальнішою. Це насамперед пов'язано з підвищенням рівня криміногенності, зростанням терористичних загроз, необхідністю захисту інформаційних ресурсів, комерційної таємниці та конфіденційної економічної інформації тощо.

Системи контролю й управління доступом (СКУД) відіграють особливу роль у системах безпеки, оскільки контроль доступу є фундаментальним поняттям процесу забезпечення безпеки. Будь-яка система безпеки повинна визначити на контрольованій території кожну людину за принципом «свій або чужий» для захисту об'єкта від проникнення на його територію сторонніх осіб чи для захисту людини від дії будь-яких небезпечних чинників за умови, якщо вони присутні на об'єкті. Контроль доступу або організація розмежування рівнів доступу є однією з суттєвих і необхідних умов для забезпечення захисту комп'ютерних систем і мереж та, відповідно, відомостей, що зберігаються в електронному вигляді в базах даних.

Обмеження доступу в небезпечні для людей приміщення і контроль за переміщенням персоналу територією об'єкта дозволяють підвищити рівень безпеки загалом та знизити ризик виникнення технологічних аварій. Наявність контролю за переміщенням персоналу територією об'єкта дисциплінує співробітників, дозволяє автоматизувати облік робочого часу, поліпшує якість охорони технологічних і комерційних секретів від промислового шпигунства, запобігає вчиненню крадіжок та інших злочинів на робочому місці та ін.

Системи контролю й управління доступом хоча б в рудиментарному вигляді функціонують у будь-якій установі. Базовим принципом роботи СКУД є здійснення процедури порівняння будь-яких ідентифікаційних ознак, представлених особою, яку перевіряють, з інформацією, яка була попередньо закладена та зберігається в пам'яті системи. Основними компонентами систем контролю доступу є пристрої ідентифікації, призначенням яких є здійснення процедури розпізнавання людини за певними ідентифікаційними ознаками під час її перебування у зоні контролю[1].

У сфері безпеки біометричні технології контролю доступу використовуються майже 25 років. Нині існує низка технологій біометричної ідентифікації, що використовують обличчя, голос, малюнок райдужної оболонки ока, геометрію руки та малюнок

[1] Крахмалёв А. К. Использование речевой информации для биометрической идентификации в системах контроля доступа / А. К. Крахмалёв // Связь и автоматизация МВД России-2008. – 2008. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

вен, але найпоширенішим через свою зручність, простоту та ціну був і залишається метод контролю за папілярними візерунками пальців[1].

Ефективний і надійний контроль доступу до будівель і приміщень – найважливіше завдання для будь-якої компанії чи установи, незалежно від форми власності, розміру та сфери діяльності.

Сучасні системи контролю доступу повинні забезпечувати:

– безпеку співробітників і відвідувачів;

– захист матеріальних цінностей, устаткування, майна та інших активів;

– комплексну багатофакторну ідентифікацію клієнтів за представленими ознаками: відбитком пальця, іншими біометричними ознаками, PIN-кодом, проксиміт-картками;

– універсальний модульний принцип побудови системи;

– прості та швидкі процедури первинної реєстрації;

– гнучкість налаштувань для забезпечення вимог підвищеної безпеки;

– обмін даними між керуючим комп'ютером і терміналами доступу;

– наочний і зручний моніторинг подій з автоматичною реєстрацією тривожних подій та можливістю перегляду в режимі реального часу;

– відображення персональних даних користувачів під час ідентифікації та контроль за загальним станом пропускних пристроїв;

– ведення бази даних усього персоналу та щоденного реєстраційно-контрольного модуля клієнтів;

– облік щоденного робочого часу персоналу, що у підсумку зумовлює обрання найбільш раціонального алгоритму управління персоналом.

Упровадження СКУД із використанням біометричних технологій дозволяє значно ефективніше організувати контроль за доступом, виключити можливість проходу за загубленими або вкраденими проксиміт-картками і, як наслідок, запобігти доступу небажаних осіб на об'єкти, які охороняються. Отже, підвищується загальний рівень об'єктової безпеки, забезпечується схоронність матеріальних цінностей та зменшується можливість витоку інформації[2].

Системи контролю управління доступом дозволяють виконати такі завдання:

– ідентифікацію всіх співробітників, які відвідують територію (будівлю чи приміщення) компанії або залишають її;

– ідентифікацію відвідувачів із забезпеченням контролю за їх подальшими переміщеннями територією об'єкта, що перебуває під охороною;

– розмежування доступу до приміщень (зон) посиленого захисту (виробничі ділянки, сховища матеріальних цінностей тощо);

– організацію проходу до сховищ, сейфів із забезпеченням доступу до них тільки за одночасного підтвердження своїх повноважень декількома незалежними особами (співробітник банку та його клієнт, представник служби безпеки й працівник функціонального підрозділу);

– забезпечити захист квартир, приватних володінь, апартаментів, готельних номерів від проникнення небажаних осіб;

– проведення розпізнавання відвідувачів торгових і розважальних центрів із подальшою диференціацією їх обслуговування (надання привілеїв постійним клієнтам,

[1] Биометрические технологии в системах контроля доступа // Cleper.ru. – 2013. – 21 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] НПЦ «ЭЛВИС» выиграл тендер МВД РФ по созданию биометрической СКУД // Secnews.ru/russian. – 2006. – 3 апреля. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/russian/...

недопущення проходу вже відомих антисоціальних осіб, запобігання продажу алкоголю та тютюнових виробів неповнолітнім та інше).

Усі ці завдання виконуються за допомогою різних технологій ідентифікації (верифікації), які охоплюють автоматичне розпізнавання користувачів за попередньо зареєстрованими у системі носіями індивідуальних ознак:

– потрібним біометричним параметром;

– контактними та безконтактними картками, брелками і т. д.;

– PIN-кодом.

Застосування перелічених ідентифікаторів можливе і окремо, і в різних поєднаннях[1].

Біометричні ідентифікатори (відбитки пальців, обличчя, райдужна оболонка ока тощо) є у кожної людини, тому ідея застосування біометрії у системах контролю управління доступом виглядає цілком природньо й логічно. Але практичне втілення цієї ідеї було досить тривале і не просте. Тільки з кінця першого десятиріччя нового тисячоліття біометрія нарешті перетворилась на невід'ємну складову і важливий чинник еволюції ринку СКУД.

Наведемо найхарактерніші тенденції, які властиві сучасному етапу використання біометричних технологій у системах контролю й управління доступом:

– поступальний розвиток ринку біометричних пристроїв загалом, який більшість експертів пов'язують саме з активізацією застосування біометрії у СКУД;

– біометрика й надалі розглядається як одна з найперспективніших технологій систем контролю й управління доступом;

– масове запровадження біометричної ідентифікації привертає дедалі більшу кількість нових замовників у цьому сегменті ринку;

– біометричні СКУД вже не є екзотичними й ексклюзивними технологічними рішеннями, які доступні тільки державним структурам або найбагатшим корпораціям, а стали масовим і буденним явищем;

– змінюється в кращу сторону громадська думка щодо використання досягнень біометрії для різних потреб суспільства, чому сприяє експансія біометричних технологій у різні сфери нашого життя (від паспортно-візових документів нового взірця, фінансових транзакцій до освіти й охорони здоров'я) та спростування міфів і стереотипів, котрі завжди супроводжують будь-яке нововведення.

Як основні тенденції, які характеризують розширення застосування біометричних технологій у системах контролю управління за доступом (СКУД), потрібно виокремити такі: інтеграція, конвергенція, перехід до «централізованого» управління користувачами, інтелектуалізація, впровадження мультибіометричних і багатофакторних рішень.

Розглянемо суть кожної зазначеної тенденції.

Інтеграція

Метою інтеграції є об'єднання в єдине ціле різних підсистем, що можуть функціонувати у складі СКУД. Нині актуальнішим завданням є поєднання систем відеоспостереження з дистанційною біометричною ідентифікацією. Шляхи та перспективи виконання цього завдання детальніше будуть розглянуті в підрозділі «Інтелектуальні мережі відеоспостереження».

Нині системи відеоспостереження дедалі більше використовуються у комплексі з іншими підсистемами СКУД, наприклад, з підсистемою управління рухом автотранс-

[1] Контроль доступа // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/access.php...

порту. Вже розроблені рішення, що дозволяють ідентифікувати водіїв і пасажирів автомашин за обличчям і райдужною оболонкою очей, причому, як би фантастично це не здавалося на перший погляд, клієнтам такої системи навіть не потрібно залишати салон або кабіну транспортного засобу. Під час упровадження подібних систем додатково може використовуватись режим верифікації державного реєстраційного номера автомобіля, що внесений у список авто, яким дозволений в'їзд на територію об'єкта, що перебуває під охороною[1].

Останні розробки систем контролю управління доступом досягли ефективності у виконанні багатьох завдань за контролем дій персоналу на території об'єкта, що охороняється. Наведемо перелік таких завдань:

– інтеграція обліку робочого часу – формування найрізноманітніших звітів (за запізненнями на роботу або дострокове залишення її, безпричинна відсутність у робочий час тощо);

– розмежування за часом доступу в будівлю чи приміщення (наприклад, з 9.00 до 18.00 для рядових співробітників, а цілодобово – для керівників, системних адміністраторів, співробітників служби безпеки);

– регулярне підтвердження впродовж робочого дня співробітником своєї присутності на робочому місці за допомогою біометричного ідентифікатора;

– дистанційна реєстрація користувачів без їх заїзду до центрального офісу (реєстрація у віддалених філіях);

– нарахування заробітної плати, зокрема беручи до уваги надбавочні і коефіцієнти за роботу в нічний або понаднормований час;

– складання списків співробітників підприємства, формування звітів і їх розсилання у відділи, департаменти та іші підрозділи[2].

Конвергенція

Розглянемо цю тезу на прикладі реалізації відповідної програми у Сполучених Штатах Америки. У США з 2001 року реалізовується програма «Конвергенція систем безпеки». Конвергенція систем безпеки – багаторівнева система управління для охорони фізичних і логічних активів об'єкта, який перебуває під охороною. Здебільшого системи конвергентної безпеки використовують так звані «перехресні» технології для поєднання в єдине ціле фізичних і логічних активів управління безпекою, не припиняючи водночас функцій контролю за доступом. Тобто з контролем фізичного доступу під час проходження прохідної одночасно повинні здійснюватися процеси запуску обліку робочого часу, розмежування фізичного доступу до приміщень або електронного доступу до комп'ютерних інформаційних систем. Фактично здійснюється повний контроль за діями фізичної особи від прохідної до робочого місця, а в наш час загальної комп'ютеризації – і за діями на автоматизованому робочому місці: фіксується час включення-виключення комп'ютера, з'єднання-роз'єднання з інформаційною базою даних, користування Інтернетом, електронною поштою тощо.

Підсумком програми «Конвергенція систем безпеки» має стати злиття фізичного і логічного блоків управління безпекою. У період з 2004 до 2008 року витрати на конвер-

[1] Лукашов И. Биометрия в системах контроля и управления доступом: вызовы времени и новые возможности / И. Лукашов // Системы безопасности. – 2008. – 10 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Контроль доступа и учет рабочего времени в корпоративном масштабе: новая версия биометрической системы BioTime. – 2008. – 24 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

генцію систем безпеки в Сполучених Штатах Америки були збільшені на 1650% (до 7 млрд доларів).

Основне фінансове навантаження лягло на федеральний уряд США: на цю програму він витратив понад 5 млрд доларів. Більшість із цих витрат були передбачені Директивою № 12 Міністерства національної безпеки США (HSPD-12), котра була видана у 2004 році і яка вимагає, щоб федеральні службовці та особи, котрі працюють за контрактом, мали однакові ідентифікаційні засоби для забезпечення фізичного доступу в урядові офіси та логічного доступу до їх ресурсів.

Але повна конвергенція – це поки що важкоздійснюване завдання, особливо у забезпеченні безпеки різних телекомунікаційних і комп'ютерних мереж, захисту інформації. Вартість створення повної конвергентної системи на сьогодні надто висока, що і зумовлює доцільність співпраці розробників різних рішень. Але поки що не існує однозначного алгоритму, відповідно до якого можна було б забезпечити виконання цього завдання загалом[1].

Централізоване (федеральне) управління користувачами

Ця тенденція тісно пов'язана з конвергенцією і допускає перехід від жорсткої та замкнутої концепції «identity management» (управління користувачами в рамках одного бізнес-додатку) до більш широкої та гнучкої концепції «identity federation». В ідеалі реалізація цієї концепції вимагає лише одноразової реєстрації користувача в єдиній базі даних із подальшим розповсюдженням його атрибутивних характеристик у всі бізнес-додатки і системи: від корпоративного порталу до СКУД і системи інформаційної безпеки. У цьому контексті бізнес-додатки перетворюються на постачальників відповідних сервісних послуг (доступу до будівлі, комп'ютерної мережі, зовнішніх Інтернет-ресурсів), а зміна повноважень користувача в одній підсистемі зумовлює ланцюжок оновлень в інших (наприклад, підвищення у посаді автоматично спричиняє зміну графіка роботи і форми обліку робочого часу).

Інтелектуалізація

Передача дедалі більшої кількості функцій машинному інтелекту. Повністю автоматизовану СКУД поки що уявити складно, проте низку важливих операцій уже можна довірити автоматиці. Наприклад, за допомогою саме біометричних технологій є можливість ефективної реалізації функції «antipass-back» або контролю за присутністю співробітника на робочому місці.

Під час використання технологій біометричної ідентифікації не передбачається можливість «обходу» СКУД за допомогою повторного проходу за іншою карткою (брелком) з метою реєстрації «чужого» виходу на роботу.

Мультибіометрія. Багатофакторність

Як відомо, мультибіометричними вважаються системи, що застосовують ідентифікацію за двома чи більше біометричними параметрами. Проте про справжню мультибіометрію може йтися лише тоді, коли біометрична ідентифікація проводиться інтегрально, тобто якщо недоліки одних технологій компенсуються перевагами інших.

Прикладом тут може слугувати об'єднання технологій ідентифікації за геометрією обличчя і відбитками пальців. Камери відеоспостереження «зустрічають» користувача на вході в будівлю або навіть на підступі до неї. Засоби ідентифікації за лицем фізичної особи визначають коло можливих кандидатів для здійснення процедури розпізнавання. Тому, коли клієнт сканує відбиток пальця на терміналі прохідної, його розпізнання

[1] Лоуренс Уолш. Конвергенция: новая волна безопасности / Уолш Лоуренс. – 2008. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document. asp...

здійснюється за шаблонами осіб, відібраних під час раніше проведеної «вибірки», що у підсумку істотно зменшує час ідентифікації.

Особливо надійним вважається спосіб підтвердження особистості, який поєднує біометрію з іншими технологіями ідентифікації, причому тут також можуть бути виокремлені різні ступені зрілості використовуваних технологій. Найпоширеніший варіант – проста багатофакторна система, коли повноваження користувача підтверджуються і біометричним ідентифікатором, і за допомогою пред'явлення матеріального носія чи введення PIN-коду. Складніший (але й перспективніший) шлях – фіксація відомостей про біометричний ідентифікатор у смарт-картці, пам'ять якої одночасно є захищеним сховищем не тільки аутентифікаційної, але й іншої інформації (електронних сертифікатів, ключів шифрування, цифрового підпису тощо)[1].

За висновками експертів, поки що найвищий рівень безпеки та надійності мають біометричні рішення у комбінації з іншими способами підтвердження користувачами своїх повноважень.

Біометричні ідентифікатори не можна втратити, забути, передати, викрасти, що є особливо важливим для виконання завдань контролю доступу.

Нині найбільш розвинутою й використовуваною біометричною технологією є ідентифікація за відбитками пальців, яка є однією з найкомфортніших для користувачів, має достатньо високу швидкість розпізнавання та найліпші параметри у співвідношенні ціна/якість.

Програмно-апаратне забезпечення останніх розробок СКУД дозволяє використовувати практично весь спектр електромеханічного устаткування, що входить до систем контролю доступу на будь-якому підприємстві: електромеханічні й електромагнітні замки, турнікети, шлюзи, хвіртки тощо. Управління цими пристроями здійснюють контролери виконавчих механізмів.

Контролери виконавчих механізмів можуть поставлятися в різних варіантах виконання:

– як самостійні пристрої (здебільшого для використання у комплекті з оптичним сканером відбитків пальців);

– у складі біометричних терміналів.

Контролер подає команду на відкриття керованого ним виконавчого механізму (замка, турнікета тощо) після завершення процедури позитивного розпізнавання користувача (тобто після пред'явлення клієнтом діючого ідентифікатора).

Найпоширенішими є термінали, що дозволяють ідентифікувати користувачів і за відбитками пальців, і за безконтактною карткою чи PIN-кодом. Фахівці зробили висновок, що для співробітників найліпше використовувати біометричні ідентифікатори, а для ідентифікації відвідувачів – видану на час візиту безконтактну картку.

Більшість сучасних розробок використовують тільки багатофакторну ідентифікацію, що переважно є двофакторною. Використання зазначеної ідентифікації дозволяє:

– пришвидшити рух співробітників через прохідну в періоди пікового навантаження, тобто на початку та завершенню робочого дня (найпоширеніше поєднання – відбиток пальця плюс PIN-код);

– можливість додаткового контролю за розмежуванням доступу в приміщення, що потребують особливого захисту (безконтактна картка плюс відбиток пальця).

[1] Лукашов И. Биометрия в системах контроля и управления доступом: вызовы времени и новые возможности / И. Лукашов // Системы безопасности. – 2008. – 10 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Двофакторна ідентифікація може бути також реалізована за розміщення відомостей щодо відбитків пальців у самій безконтактній картці. У цьому разі процес біометричної ідентифікації користувача здійснюється за порівнянням двох цифрових моделей відбитків пальців: раніше зареєстрованого (зберігається на картці) і нового, який пред'являється для ідентифікації.

Пристрої контролю управління доступом можуть використовуватися і локально (один термінал як самостійний пристрій), і в складі системи (деяка кількість терміналів контролю, яка під'єднується до системи з сервером, котрий виконує управлінські функції). Останній варіант є доцільнішим, оскільки дозволяє:

– централізовано здійснювати управління пунктами контролю доступу та перевіряти повноваження користувачів;

– проводити реєстрацію біометричних ідентифікаторів співробітника й інших персональних даних (прізвище, ім'я, по батькові, посада) одноразово та надавати працівникові право на доступ у будь-якому пункті пропуску, що входить до загальної системи контролю, відразу ж після здійснення процедури реєстрації;

– паралельно з подачею сигналу на відкриття замка, турнікета в автоматичному режимі фіксувати час приходу чи виходу співробітника;

– можливість складання різноманітних звітів як для контролю за використанням співробітником свого робочого часу, так і за його переміщеннями в офісі або на території підприємства – природньо у таких випадках, коли термінали контролю доступу функціонують також і на входах у внутрішні приміщення;

– формування так званих «вкладишних» контурів доступу, коли відстежується проходження співробітником усіх захисних рубежів і у випадку, коли працівник не зареєстрував свого прибуття на прохідній, йому забороняється доступ у внутрішні приміщення[1].

Системи контролю управління доступом безперервно удосконалюються, вони постійно зазнають змін; цей процес постійно стимулюється вимогами підвищення рівня безпеки й економічності, необхідністю зменшення часу на процедуру обслуговування та нагальною потребою досягнення більшої функціональності.

Індустрія контролю доступу зазнає кардинальних змін, широко запозичуючи технологічні рішення зі сфер інформаційно-телекомунікаційних і програмно-комп'ютерних технологій, мобільного зв'язку. Проведені роботи з стандартизації такої важливої ділянки систем контролю доступу, як канали передачі даних між інтелектуальними контролерами та центральним сервером. Розроблені уніфіковані вимоги, що стануть промисловим стандартом. Стандартизація виконується за технологічними вимогами, які використовуються під час конструювання спеціальних шин управління та за допомогою яких виконуються управлінські команди замками й іншими перемикаючими пристроями дверей, турнікетів, вікон, а також які реалізовані в апаратурі контролю. У цих шинах застосовуються унікальні схеми підключень до відповідних пристроїв, причому кожному з них обов'язково надається індивідуальна унікальна електронна адреса. Подібні шини управління вперше були використані в автомобілебудуванні для здійснення контролю за блокуванням і відкриттям замків дверей. Ці рішення автоіндустрії достатньо відпрацьовані та стандартизовані. Тому за аналогією шинне обв'язування виконавчих пристроїв дверей та інших об'єктів систем контролю доступу також виконуваються на базі відкритого стандарту. Із часом дедалі більше компаній зможуть запропонувати повний спектр усіх необхідних

[1] Контроль доступа // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/access.php...

компонентів для оснащення дверей необхідними пристроями для реалізації управлінських команд системи контролю (наприклад, керовані відповідним чином дверні собачки, магнітні й електронні замки, кнопки виклику, пристрої для зчитування карток) – тому без внутрішньогалузевої співпраці виготовити таку шину самостійно вдається небагатьом компаніям.

На думку фахівців, біометричний контроль за відбитками пальців і надалі буде найпоширенішим біометричним рішенням у системах контролю доступу, оскільки цей біометричний ідентифікатор все ще є основною біометричною технологією, яка є найприйнятливішою на ринку систем безпеки за ціновими показниками. Вважається, що в ідеалі порівняння шаблону-зразка та фактичного відбитка пальця має відбуватися за допомогою пам'яті мікрочіпа, що вмонтований у смарт-картку. У разі позитивної ідентифікації зчитувач надсилає унікальний код картки на пульт, і замок дверей спрацьовує. Масове запровадження біометричних зчитувачів залежить від спільної дії таких трьох чинників: наявності недорогих смарт-карток із великими обсягами пам'яті вмонтованих мікрочіпів, подальшого зростання потреби у підвищенні рівня безпеки та зниження цін на біометричні датчики.

На думку експертів, ці чинники вже «зійшлися в одній точці», що нині позитивно позначається на купівельній мотивації[1].

2011 року російський журнал «Кадрова справа» (рос. «Кадровое дело») опублікував матеріал для роботодавців про ключові можливості біометричних технологій.

Редакційна колегія видання виокремила низку принципових переваг використання біометричної системи контролю доступу й обліку робочого часу:

– простота використання;
– оптимізація кадрового діловодства;
– точність ідентифікації співробітника;
– зручність контролю;
– високий рівень безпеки[2].

Сферою застосування систем контролю й управління доступом (СКУД) на основі біометричних технологій є критично важливі об'єкти (об'єкти особливої важливості, підвищеної небезпеки, життєзабезпечення, крупні авіа- та транспортні вузли, прикордонні переходи тощо), а також об'єкти кредитно-фінансової системи.

Після трагедії 11 вересня 2001 року для підвищення безпеки всі суспільні місця в найбільш розвинутих світових країнах, насамперед аеропорти, вокзали, інші складові суспільного транспорту, торгові центри, підземні переходи повинні постійно контролюватися за допомогою передових систем відеонагляду, а там, де необхідний контроль доступу, – повинні застосовуватися відповідні зони доступу з використанням СКУД на базі багатофакторної ідентифікації.

Сучасні транспортні термінали, особливо великі аеропорти, обслуговуються тисячами співробітників. Усі вони мають доступ у ті чи інші службові приміщення, водночас багато з таких приміщень є надзвичайно важливими з погляду безпеки. Додаткову складність привносить така обставина, що частина персоналу (наприклад, члени екіпажів

[1] Пит Лау. Будущее систем контроля доступа / Лау Пит // Hi-Tech Security Solutions. – 2006. – 7 ноября. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/articles/...

[2] Почему биометрическая система BioTime популярна у HR-менеджеров? – 2011. – 15 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

літаків) не є постійними співробітниками аеропортів, куди вони здійснюють авіарейси, а з'являються там тільки за деякою періодичністю.

Використання біометричних технологій для контролю за доступом у службові приміщення, виходу на летовище та запобігання небажаним діям співробітників аеропортів сьогодні запроваджуються у практичну діяльність більшості великих міжнародних і внутрішніх аеропортів країн, які дбають про безпеку своїх громадян.

У рейтингу, складеному компанією «British Airways» (однією з найбільших авіакомпаній світу), запровадження біометричної ідентифікації авіапасажирів визнано однією з головних інновацій першого десятиріччя XXI століття[1].

На думку експертів, використання біометричних технологій з ідентифікаційними картками (жетонами) дозволяє істотно підвищити рівень безпеки. Якщо до такого програмно-апаратного комплексу додати системи відеоспостережень, які в змозі автоматично виокремлювати з «відеокартинки» фігури фізичних осіб та підраховувати їх кількість, виникає можливість виключити одночасний прохід декількох чоловік під час пропуску одного співробітника, який пред'явив системі матеріальний носій на право доступу в приміщення або на територію, яку охороняють.

Щоб здійснити цю безперервну й тотальну перевірку, систему відеоспостереження необхідно інтегрувати в загальну інформаційну мережу, яка буде управляти нею так легко, як і передачею мовних сигналів та інших даних. Отже, сучасні системи відеоспостереження повинні складатись із сотень відеокамер і виконувати велику кількість завдань.

За відомостями російської компанії «Biolinksolutions», на початок 2013 року більше половини (а за деякими оцінками і понад дві третини) біометричного ринку займають технологічні рішення, які використовують ідентифікацію за відбитками пальців. У сфері інформаційної безпеки є аналогічна ситуація: за даними «Frost & Sullivan», саме на цю біометричну технологію припадає 88,7% продажів біометричних засобів захисту інформації у фінансовому секторі.

Отже, лідерами на біометричному ринку є технології ідентифікації за папілярними візерунками пальців.

Сучасна біометрія здатна запропонувати корпоративним замовникам надійні рішення зі захисту інформації, що ефективно взаємодіють із загальною IT-інфраструктурою (відповідно до каталогу «Active Directory», платформ віртуалізації «тонких» клієнтів)[2].

Цікавою є інформація, що Пентагон постійно розширює використання біометричних систем контролю доступу. Біометричні СКУД, які засновані на ідентифікації за відбитками пальців і фотознімками користувачів, запроваджені на військовоповітряних базах Ендрюс (Joint Base Andrews Naval Air Facility /JBA/), на Окінаві (Японія), в окрузі Вічіта (штат Техас) і в Анкоріджі (штат Аляска). База Ендрюс знаходиться на відстані 16 кілометрів від Вашингтона та відома тим, що саме до неї належить «борт № 1» – літак американського президента[3].

---

[1] Биометрия 2010: 50 главных событий года // BIOMETRICS.RU. – 2011. – 13 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Лучшие биометрические решения по контролю доступа вошли в главный специализированный справочник // BioLink. – 2013. – 11 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Пентагон расширил использование биометрических систем контроля доступа // BIOMETRICS.RU. – 2011. – 5 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

6.4. Запровадженя систем контролю й управління доступом (СКУД) у провідних аеропортах світу

Застосування біометрії в аеропортах повинно не тільки полегшити життя авіапасажирам, але й забезпечити більш надійну їхню безпеку, значно підвищуючи водночас ефективність прикордонного контролю. 2010 року системи добровільної біометричної ідентифікації діяли у десятках аеропортів світу та налічували сотні тисяч користувачів; кожна п'ята авіакомпанія світу інвестувала кошти в інтегровані рішення з застосування біометричних технологій в обслуговуванні пасажирів[1].

2010 року компанії «Sita» і «IHS Jane's» провели спільний вебінар, під час якого були розглянуті основні можливості застосування біометричних технологій в аеропортах. Учасники вебінару визначили низку перспективних напрямів використання біометричних технологій в аеропортах, а у підсумку констатували, що головну вигоду від подальшої експансії цих технологій отримають авіапасажири.

До згаданих напрямів, зокрема увійшли: зручна реєстрація на рейс, пришвидшене проходження всіх форм контролю, зменшення часу під час посадки на борт літака та безпечна ідентифікація власників багажу. Перевагами технологій біометрики пасажири користуються не тільки під час відправлення в політ, але й в аеропортах прибуття, особливо при виконанні міжнародних авіарейсів: тут час авіапасажирів суттєво заощаджується за використання біометричних систем паспортного та візового контролю.

Тому цілком закономірно, що значну частину часу учасники вебінару присвятили питанню використання біометричних технологій у прикордонному контролі. Включення в електронні паспорти та візи відомостей щодо біометричних ідентифікаторів їх власників потрібно не тільки для того, щоб гарантувати, що власник проїзного документа насправді є тим, за кого він себе видає, але й для пришвидшення проходження паспортного або імміграційного контролю.

Директор біометричних проектів компанії «Sita» Сін Фаррелл (Sean Farrell) акцентував на ще одному суттєвому напрямі застосування біометричних технологій, який є надзвичайно важливим для спеціальних урядових структур, що відповідають за безпеку держави. Це перевірка особистості авіапасажирів для встановлення таких осіб, які можуть становити загрозу і для інших авіаційних пасажирів, і для національної безпеки тих країн, до яких вони прямують.

Йдеться про використання відомостей щодо біометричних ідентифікаторів у системах так званого ризик-менеджменту, і подібний підхід необхідно визнати надзвичайно конструктивним. Звичайний паспорт і візу можна підробити, чого й прагнуть представники кримінальних кіл, терористи та їх спільники, наркодилери, порушники візового і міграційного режиму, але вони не можуть змінити свої біометричні ідентифікатори, які є унікальними для кожної людини.

Отже, використання технологій біометрії є корисним і для авіапасажирів, і для урядових структур. Подальшу інтеграцію систем біометричних паспортів, біометричних віз і ризик-менеджменту на транспорті. С. Фаррелл вважає оптимальною комбінацією

[1] Биометрия 2010: 50 главных событий года // BIOMETRICS.RU. – 2011. – 13 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

та навіть називає її «золотим стандартом» у застосуванні біометрії, досягнення якого повинні прагнути уряди всіх світових країн[1].

2011 року в Сінгапурі в рамках щорічних 67-х загальних зборів Міжнародної Асоціації Повітряного транспорту (ІАТА) був представлений перший проект «Контрольно-пропускного пункту Майбутнього» (КПП). Як повідомляє ІАТА, проект спрямований на те, щоб збільшити рівень безпеки в аеропортах, водночас суттєво знизивши черги та відповідні незручності для авіапасажирів.

Як заявив генеральний директор і президент Асоціації Джованні Бісіньяні, світові аеропорти щорічно витрачають до 7,4 млрд доларів у рік на безпеку авіаперевезень, водночас пасажири стикаються з метушнею та нескінченними чергами. «Пасажири повинні проходити на посадку в літаки без принижень і штовханини. Це означає, що не повинно бути тривалих зупинок у чергах, розпакуванні речей і особистого огляду. Політ і передполітні процедури повинні проходити цивілізовано», – підкреслив президент ІАТА.

Діючий тип контрольно-пропускного пункту був розроблений ще 40 років тому. Головним пріоритетом тоді була необхідність виявлення потенційних терористів із металевою зброєю. В Асоціації впевнені, що необхідно переходити до нової системи, яка повинна відповідати сучасним вимогами. Новий підхід має бути заснований на використанні не тільки людських ресурсів, але і нових технологій.

Пасажири, що наближаються до сучасного контрольно-пропускного пункту, мають скеровуватися до одного з трьох його відділень: «Мандрівник», «Норма» і «Посилена безпека». Розподіляють пасажирів за зазначеними категоріями після ґрунтовної перевірки відомостей за наданими документальними даними, що містяться у біометричному паспорті або іншому проїзному документі. Отже, ступінь ризику буде оцінюватися задовго до того, як пасажир прибуде в той чи інший аеропорт. Передбачається, що туристи, які заздалегідь проходять перевірку даних із боку відповідних владних структур, будуть максимально швидко проходити контрольну процедуру в відділенні «Мандрівник». Відділення «Норма» призначена для більшості пасажирів і для тих, про кого у відкритому доступі міститься занадто мало інформації. Відділення «Посилена безпека» автори проекту пропонують для використання за необхідності здійснення додаткової посиленої перевірки.

Водночас перевірка у відділеннях КПП буде здійснюватися з використанням нових технологій, під час застосування яких пасажирам не доведеться знімати одяг і взуття, розкривати багаж і проходити особистий огляд.

Також передбачається, що система безпеки в аеропортах на «КПП Майбутнього» буде охоплювати митний та імміграційний контроль, що також суттєво спростить проходження процедури посадки на літак. Згідно з рішенням 67-х загальних зборів для розробки стандартів «КПП Майбутнього», проект спрямують до Міжнародної організації цивільної авіації (ІСАО). ІАТА також координує свої дії з американським відділом програми Національної безпеки.

ІАТА вже заявляє про готовність переходу на нову трирівневу систему «КПП Майбутнього», однак сам перехід вимагає розробки технологічнних підходів, на що потрібно декілька років[2].

---

[1] Биометрические технологии в аэропортах: новые вызовы и новые возможности // BIOMETRICS.RU. – 2010. – 23 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрия станет еще активнее использоваться в аэропортах // Туринфо. – 2011. – 8 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

На початку 2012 року компанія «Amadeus» (головний постачальник передових рішень у сфері інформаційних технологій, дистрибуції й електронної комерції для світової індустрії туризму та авіаперевезень, а також глобальної системи бронювання) у своєму огляді зазначила, що до 2020 року технологічні інновації дозволять зробити авіаподорожі менш напруженими, а пасажири зможуть відслідковувати в будь-який момент точне місцезнаходження свого багажу.

Автоматичні системи ідентифікації будуть ідентифіковувати особистість мандрівників за відбитками пальців, що майже повністю виключить наявність черг і затримок під час реєстрації на авіарейси.

Безпосередньо людський контроль за безпекою в аеропортах повністю замінять ефективні автоматизовані системи, що будуть здатні швидко контролювати переміщення великої кількості людей.

Проходження митниці та паспортного чи імміграційного контролю буде здійснюватися за допомогою біометричних технологій, причому перевагу можуть отримати технології сканування райдужки.

Аналіз «Amadeus» був підготовлений на узагальненні відповідей 18 експертів у сфері туризму і здійсненого онлайн-опитування, у якому взяли участь понад 1,4 тис. мандрівників із семи країн – Бразилії, Китаю, Росії, Іспанії, ОАЕ, Великобританії та США[1].

За період із 2010 – 1-й квартал 2014 року з'явилась велика кількість публікацій про використання систем контролю управління доступом в аеропортах світу. Причому в значній кількості матеріалів ЗМІ йдеться не про використання СКУД в аеропортах, а про застосування систем доступу під час здійснення прикордонного контролю. Найбільше цей факт засвідчує повідомлення про те, що у квітні 2013 року аеропорт Хітроу продав біометричну систему контролю Прикордонному агентству Британії за п'ять мільйонів фунтів (8,06 млн доларів)[2].

В ЄС планується, що незабаром біометричні технології повинні майже замінити прикордонників під час здійснення контролю. Більш детально використання біометричних технологій у прикордонному котролі буде розглянуто у 13 розділі.

У деяких аеропортах існують окремі програми ідентифікування особистостей мандрівників, які призначені для зменшення часу, необхідного для проведення посадки авіапасажирів на літаки.

Ці системи відмінні від біометричних систем автоматичного прикордонного контролю, які проводяться виключно за паспортно-візовими документами. Прикладом такої розробки є діяльність програми «Clear», учасники якої одержують можливість пришвидшеного проходження передпольотного контролю в аеропортах США.

Учасники програми попередньо реєструють свої біометричні ідентифікатори (райдужну оболонку очей і відбитки пальців) – ці відомості фіксуються у спеціальній картці, яка видається авіапасажирові.

Попередньо біометричні дані на кожну особу перевіряються Управлінням транспортної безпеки США, і, якщо воно дає «добро», учасникам програми надається можливість проходити передпольотний контроль в аеропорті у пришвидшеному режимі,

[1] Биометрические технологии позволят аэропортам отказатся от бумажных носителей // РИА Новости. – 2012. – 12 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Аэропорт Хитроу продал биометрическую систему пограничного контроля // BIOMETRICS.RU. – 2013. – 30 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

яке досягається завдяки надійній ідентифікації особистості пасажира за допомогою його картки учасника програми «Clear». Річна участь у біометричній програмі супроводу авіапасажирів, які часто подорожують, коштує 179 доларів[1].

Після прибуття в аеропорт учасники програми, реєструючись на рейс, знову проходять біометричну ідентифікацію, швидко, надійно й безпечно підтверджуючи свою особистість і зменшуючи час обов'язкового передпольотного контролю, тоді як звичайні авіапасажири змушені декілька годин чекати в черзі. Чисельність авіапасажирів-учасників програми «Clear» становила на кінець 2012 року приблизно 200 тис. людей[2].

Окрім програми «Clear», у найбільших міжнародних аеропортах США діє біометрична система «Global Entry». Ключовим компонентом цієї системи є електронні кіоски, де авіапасажири, що прибувають на американську територію, повинні пред'являти свої біометричні паспорти.

Додатково авіапасажирові потрібно відсканувати відбитки пальців, після чого порівнюються одержані відомості з даними, що зберігаються в чіпі паспорта. За відповідності цих відомостей у автоматичному режимі власникові біометричного паспорта дозволяється перетнути кордон. Програмою «Global Entry» користуються також у Канаді, Нідерландах і Південній Кореї[3].

Інтерес до програми виявили Франція, Сінгапур, Австралія й Нова Зеландія. Учасниками цієї програми є понад 200 тис. людей, а 137 її пунктів діють у 20 американських аеропортах. Міністерство національної безпеки США оголосило про намір розширити сферу дії біометричної системи прикордонного контролю «Global Entry»[4].

Наведемо низку відомостей про застосування систем контролю за доступом в аеропортах. Австралія: Сідней, Мельбурн, Перт, Брісбен, Аделаїда, Голд-Коста і Кернс. Аргентина: Буенос-Айрес і Езейза. Великобританія: Гатвік і Хітроу. Гонконг – міжнародний аеропорт Гонконгу. Ірландія – аеропорт Дубліна. Мальдіви – аеропорт Мале. Молдова – аеропорт Кишинів. Нова Зеландія – аеропорт Окленда. ОАЕ – аеропорт Дубай. Мальдіви – аеропорт Мале. Португалія – аеропорт Лісабону. США: міжнародний аеропорт Балтімора – Вашингтона (Baltimore/Washington International Airport – BWI), аеропорти Денвера й Орландо, міжнародний аеропорт Даллас/Форт-Уерт, міжнародний аеропорт Сан-Франциско, аеропорт нью-йоркського округу Уестчестер (Westchester County Airport – HPN), Міжнародний аеропорт Сан-Антоніо, аеропорт Сан-Хосе, аеропорт Техаса та інші. Філіппіни – міжнародний аеропорт Маніли. Японія – токійські аеропорти Ханеда і Наріта.

Біометричні технології також використовуються на залізничних вокзалах і морських та річкових портах. Так, є повідомлення про їх застосування у портах Бельгії (Антверпен і Зебрюгге) та Еквадору.

---

[1] Биометрическая программа сопровождения авиапассажиров возобновит свою работу // BIOMETRICS.RU. – 2010. – 29 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрическая система сопровождения авиапассажиров пришла в Нью-Йорк // BIOMETRICS.RU. – 2012. – 30 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Граждане Южной Кореи смогут воспользоваться американской биометрической системой пограничного контроля // BIOMETRICS.RU. – 2012. – 2 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] США: сфера действия биометрической системы пограничного контроля будет расширена // BIOMETRICS.RU. – 2012. – 27 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

6.5. Автоматизація обліку робочого часу за допомогою біометричних технологій

Стратегічний актив будь-якої компанії – це її співробітники та їх робочий час. Реальний облік робочого часу дозволяє якісно вирішувати питання, що є основою діяльності будь-якої організації:

– підвищення ефективності роботи компанії;

– сприяння зростанню продуктивності праці;

– зміцнення трудової дисципліни;

– сприяння раціональній організації і реалізації ключових бізнес-процесів;

– забезпечення відповідно до відпрацьованого часу нарахування заробітної плати співробітникам.

Нині загальновизнано, що в організаціях зі значною чисельністю працівників найоптимальнішим способом здійснення обліку робочого часу є його проведення за допомогою біометричної ідентифікації співробітників за їх унікальними невідчужуваними параметрами.

Зважаючи на такий показник, як співвідношення ціна–якість, нині найбільше поширені біометричні системи, котрі використовують відбитки пальців.

Як правило, такі системи обліку робочого часу виконують такі завдання:

– автоматичну реєстрацію приходу та виходу співробітників за допомогою їх унікальних біометричних характеристик;

– здійснення обліку робочого часу за кожним співробітником, підрозділом, компанією чи установою загалом (зокрема консолідація даних щодо територіально віддалених філій);

– формування за будь-який вказаний період комп'ютерної звітності та табелів виходу на роботу з можливістю їх подальшого експорту в різних форматах даних (наприклад: html, xls, xml);

– інформування в режимі реального часу («On-line») керівництва, служби безпеки, відділу кадрів та інших зацікавлених служб про перебування співробітників на робочих місцях або на території організації;

– надання відомостей щодо обліку робочого часу до бухгалтерії підприємства для подальшого нарахування заробітної плати відповідно до кількості відпрацьованого співробітниками часу (оперуючи тарифними ставками співробітників, можна задавати коефіцієнти для розрахунку оплати праці в нічні зміни і за понаднормовий час і отримувати в найкоротші терміни необхідні звітні документи);

– інтеграція обліку відпрацьованого часу з контролем фізичного доступу у визначені зони та приміщення контрольованого об'єкта[1].

Сучасні технології надають широкий простір для автоматизації обліку робочого часу. Можна «озброїти» персонал картками зі штрих-кодами, магнітними картами або контактними смарт-картами, які співробітники будуть пред'являти відповідним ридерам, відзначаючи свій прихід на роботу та відхід.

Однак дедалі більш популярними стають біометричні системи обліку робочого часу. Це пов'язане з тим, що будь-який матеріальний носій, зокрема й картки, має такий

[1] Учёт рабочего времени // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/time.php...

недолік: його можно відокремити від особи. Тобто карту можна передати іншій людині, що неприйнятно ні в системах обліку робочого часу, ні в контролі доступу.

У найостанніших розробках інтегрованих систем обліку робочого часу підсистема контролю фізичного доступу доповнилася режимом заборони повторного проходу (функція «antipass-back»). Не зареєструвавши свій вхід у приміщення, співробітник не отримує потім права на вихід (і навпаки). Отже, створюється забезпечення нового рівня безпеки і блокуються спроби «обману» замка, турнікета або шлюзу (якими управляють біометричні термінали).

Наприклад, коли співробітник, який спізнюється, проходить за працівником-колегою, що вже реєструється, і ним на контрольовану територію, сподіваючись, що факт запізнення на роботу буде незафіксованим[1].

Біометричні параметри людини унікальні, їх не можна відділити від особистості й тому вони зараз є найпоширенішими.

Найбільше використовуються системи, які базуються на технології ідентифікації за відбитками пальців. Але для сфер безпеки й автоматизації фінансів найбільш оптимальні багатофакторні біометричні термінали контролю доступу й обліку робочого часу, що дозволяють ідентифікувати користувачів за відбитками пальців і безконтактними картками або PIN-кодами.

Загальний алгоритм дії біометричних систем обліку робочого часу подібний до принципу функціонування карткових рішень, тільки зчитувачу-сканеру потрібно «пред'являти» відбиток пальця. У найбільш розвинених системах допускається використання і карток, і біометричних ідентифікаторів (двофакторні системи).

Архітектура біометричних систем обліку робочого часу

Біометричні системи складаються з 2-х частин: устаткування та спеціалізованого програмного забезпечення (ПЗ). До устаткування входять біометричні термінали та сканери відбитків пальців, а програмне забезпечення ці дані обробляє, спрямовує інформацію до бази даних, а в підсумку формує звітність для бухгалтерії, кадрів, керівництва підприємства та керівників відділів.

Одним із найважливіших вимог до ПЗ біометричних систем є можливість інтегрування з іншими програмними продуктами. Так, після закупівлі системи обліку робочого часу можна не заводити заново дані про співробітників (прізвище, ім'я, посаду і т. д.): для цього існує опція автоматичного імпорту даних із бухгалтерської програми 1С. Також в автоматичному режимі повинен здійснюватися експорт відомостей із біометричної системи в програму 1С для нарахування зарплати. Звичайно, надійність інтеграції з 1С повинна підтверджуватися офіційним сертифікатом; також важлива й наявність інших сертифікатів.

Наприклад, сертифікат на сумісність із MS Windows 7 не тільки гарантує, що облік робочого часу буде діяти у цій операційній системі, він підтверджує технологічність самого сертифікованого рішення: фактичну дійсність, що інсталяція біометричної системи буде здійснюватися коректно та не спричинить виходу з ладу IT-інфраструктури підприємства.

Достовірність відомостей про відпрацьований час – основний чинник будь-якої організації платити заробітну плату своїм співробітникам за реально відпрацьований час.

[1] Биометрическая система учета рабочего времени действует в Калифорнийском университете // BIOMETRICS.Ru. – 2007. – 15 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Критерії вибору біометричної системи обліку робочого часу

Під час вибору системи, її впровадження та подальшого використання важливо брати до уваги такі аспекти:

– необхідність дотримання норм Закону «Про захист персональних даних»;

– важливість таких характеристик, як масштабованість і гнучкість. Система обліку робочого часу повинна мати здатність до розширення (наприклад, у разі збільшення кількості співробітників і/або появі в компанії нових територіально розподілених офісів) та можливість керування з єдиного центру (щоб уникнути збору відомостей для бухгалтерії за кожним із таких офісів окремо);

– здатність обраної системи до інтеграції з іншими IT-рішеннями – наприклад, із змінами до платформи 1С (що в ідеалі повинно підтверджуватися офіційним сертифікатом);

– підтримка зчитувачами/терміналами різних мережних інтерфейсів;

– можливість ведення великої кількості звітів і формувань різноманітних графіків роботи (змінних, фіксованих, вільних, календарних і т. д.);

– надання постачальником можливості безкоштовного тестування системи перед її закупівлею[1].

Редакційна колегія журналу «Кадрова справа» (рос. – «Кадровое дело») визначила низку принципових переваг використання біометричної системи обліку робочого часу та контролю доступу:

– простота використання;

– оптимізація кадрового діловодства;

– точність ідентифікації співробітника;

– зручність контролю;

– високий рівень безпеки[2].

Згідно з дослідженням російського аналітичного порталу «Biometrics.ru», у Росії біометричні системи обліку робочого часу є найбільш популярними у ритейлі (23,0%,) та сфері послуг (24,3%). Значну частку займають виробничі (19%) та медичні (7,8%) установи.

Висока затребуваність таких систем у мережі роздрібної торгівлі пояснюється специфікою оплати роботи продавців – практично у всіх компаніях продавці-консультанти працюють за графіком погодинної оплати.

У ритейлі, індустрії харчування та інших галузях, де людський фактор має ключове значення (охорона здоров'я, освіта і т. д.) біометричні системи обліку робочого часу найбільш ефективні.

Дедалі більше російських компаній зі сфери ритейлу переходять на біометричний облік робочого часу. Нині до цих компаній належать мережі супермаркетів («Перехрестя», «Марка», «АБК», «Острів»), мережі модного одягу та взуття («Lacoste» і «Рандеву») та комп'ютерні магазини (OLDI), які використовують біометричну систему обліку робочого часу (СОРЧ–СКУД) для керування персоналом[3].

---

[1] Михайлов А. Автоматизация учета рабочего времени с помощью биометрических технологий / А. Михайлов // Biolink Solutions. – 2012. – апрель. [Электронный ресурс]. – Режим доступа: http://retail-tech.ru/fashion/articles/...

[2] Почему биометрическая система BioTime популярна у HR-менеджеров? // BioLink. – 2011. – 15 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Михайлов А. Автоматизация учета рабочего времени с помощью биометрических технологий / А. Михайлов // Biolink Solutions. – 2012. – апрель. [Электронный ресурс]. – Режим доступа: http://retail-tech.ru/fashion/articles/...

Наведемо низку думок незалежних експертів щодо актуальності використання біометричних технологій для автоматизації обліку робочого часу на сучасному ринку роздрібної торгівлі:

– біометричний облік робочого часу й аналіз його втрат – це можливість визначити показник початку процесу зниження мотивації в торгівельному підприємстві;

– сенс використання біометричної системи обліку робочого часу – в економії грошей роботодавця та у зміцненні функції управлінського контролю;

– застосування біометричного обліку робочого часу на торговельному підприємстві доцільне, а в деяких випадках дуже потрібне. Біометричну систему обліку робочого часу давно почали застосовувати європейські бізнесмени, адже вона допомагає чітко контролювати наявність співробітників на робочому місці[1].

Чим же зумовлена зростаюча популярність біометричних технологій у керуванні персоналом?

Традиційні методи ідентифікації, засновані на застосуванні паролів або матеріальних носіїв (пропуск, звичайний паспорт, електронний ключ або карта) вже не відповідають сучасним вимогам. Пароль можна забути або взнати (перехопити), матеріальний носій – скопіювати, втратити чи передати іншій особі. Тому дедалі більша кількість компаній переходить до використання біометричних систем ідентифікації, у яких перевірка повноважень користувача здійснюється на підставі унікальних біометричних особливостей кожної людини, причому ці ідентифікуючі ознаки не можуть бути забуті, загублені або позичені будь-кому іншому.

Консалтингова компанія «Acuity Market Intelligence» стверджує, що ці технології реалізують понад 70% компаній, що діють на світовому біометричному ринку, і надалі (5–7 років) вони збережуть домінуюче становище. Після ідентифікації за папілярними візерунками пальців друге місце посідає технологія ідентифікації за обличчям (13,7%), однак можливо, що згодом його зможуть зайняти системи ідентифікації за райдужною оболонкою очей, які із 7% у 2011 до 2017 року можуть сягти 18,8%.

Особливо лідерство систем, заснованих на ідентифікації за відбитками пальців, виявляється в сфері управління персоналом: 87% проектів у цій сфері, реалізованих у 2010–2011 роках і проаналізованих російським біометричним порталом «Biometrics.ru», використовують згадану технологію.

Найважливіша функція служби контролю за персоналом – аналіз ефективності використання робочого часу. За підрахунками Американської асоціації менеджерів із нарахування зарплат (American Payroll Association), махінації співробітників, що обмінюються своїми паролями або картками, за допомогою яких відзначають прихід на роботу та вихід із неї за принципом «за себе та за того хлопця» (buddy punching), обходиться компаніям США в 5% від сукупного річного фонду оплати праці.

Переваги біометричних систем настільки очевидні, що замовники часто поширюють їхню дію не тільки на управління персоналом. Наприклад, саме таку модель вибрала мережа підприємств швидкого харчування «Popeye's Chicken & Biscuits», яка запровадила сканери відбитків пальців і відповідне програмне забезпечення у 148 своїх ресторанах в Алабамі, Іллінойсі, Флориді, Джорджії, Луізіані, Міссісіпі та Міссурі.

Спочатку планувалося застосовувати систему біометрії тільки для обліку робочого часу працівників, однак згодом її почали використовувати й для обліку операцій

[1] Практика использования биометрического учета рабочего времени для эффективного управления магазином // BioLink. – 2012. – 16 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

у системі обслуговування відвідувачів. Адже, відповідно до прийнятої у мережі бізнес-моделі, скасовувати вже прийняті на виконання замовлення клієнтів можуть тільки менеджери, які пред'являють для цього спеціальні ID-картки. Однак вони для «пришвидшення обслуговування», передавали картки офіціантам, які, користуючись повноваженнями своїх начальників у ІТ-системі, скасовували в ній зроблені та насправді реалізовані замовлення, а гроші, що отримували від відвідувачів, привласнювали, незабуваючи водночас поділитися з менеджерами. Після переходу на біометричні технології подібні махінації зникли, оскільки кожна транзакція тепер здійснюється за пред'явленням відбитка пальця, який неможливо «позичити».

Цікаво, що такі ж подібні події відбувалися ще в одній американській мережі швидкого харчування – «Garden Fresh». Там почали використовувати біометрію для доступу до касових апаратів і для контролю за проведеними транзакціями, що радикально знизило кількість нібито «скасованих» замовлень, та дозволило «Garden Fresh» за 10 місяців зменшити свої витрати на 900 тис. доларів. А згодом, переконавшись у ефективності біометричних технологій, їх поширили й на облік робочого часу. Відповідний проект був успішно реалізований у п'ятьох ресторанах, тому сканери відбитків пальців встановили ще в 120 закладах[1].

Але біометричні системи обліку робочого часу (СОРЧ) застосовуються не тільки у приватних підприємствах, а й у державних установах.

2012 року уряд Гани оголосив про те, що у всіх міністерствах та інших державних організаціях будуть установлені СОРЧ. Очікується, що застосування цих біометричних систем дозволить підвищити ефективність діяльності державних службовців, що у підсумку приведе обсяг виплачуваних їм зарплат у відповідність до результатів їх праці[2].

А в Пакистані біометричні системи контролюють робочий час поліцейських. За допомогою цих систем, як вважає керівництво поліції, підвищується їх трудова дисципліна: значно зменшується кількість запізнень на службу, контролюється відсутність на ній; а також з'являється можливість виявлення так званих «поліцейських-примар», які числяться лише на папері та матеріалізуються тільки під час одержання зарплат.

Раніше аналогічна система була встановлена у Високому суді пакистанської провінції Сінд[3].

В Індії завдяки переходу на біометричний облік робочого часу в Міністерстві внутрішніх справ виявлені службовці-«примари»: зарплату в міністерстві одержували півтори тисячі працівників, а в біометричній системі зареєструвалося на 300 співробітників менше[4].

Отже, контроль за роботою персоналу – одне із найактуальніших завдань у багатьох компаніях, медичних, освітянських і державних установах. Запізнення, затримки на обідній перерві, перекури та ранні відходи з робочих місць завдають чимало труднощів керівництву, а також призводять до зниження ефективності праці, внаслідок чого компанії або установи можуть понести фінансові збитки. Однак усі ці проблемні питання

[1] Михайлов Антон. Биометрические технологии в управлении персоналом / Антон Михайлов // Cnews.ru. – 2011. – 28 декабря. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/HR/articles/articles...

[2] Биометрические системы учтут рабочее время госслужащих в Гане // BIOMETRICS.RU. – 2012. – 15 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические системы проконтролируют пакистанских полицейских // BIOMETRICS.RU. – 2013. – 17 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Биометрия-2010: 50 главных событий года // BIOMETRICS.RU. – 2011. – 13 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

дозволяють вирішити біометричні системи контролю управління доступом, які поєднані з системами обліку робочого часу.

У Росії та Співдружності Незалежних Держав (СНД) біометрична система «BioLink BioTime» вважається розробкою № 1 у галузі біометричних систем СКУД-СОРЧ. П'ятьнадцять років досвіду роботи, 5000 успішних упроваджень та постійне поліпшення якості з урахуванням побажань клієнтів дозволило створити досить надійний продукт на теренах СНД[1].

Більш детальну інформацію можна знайти на порталі «Biolink» за електронною адресою: http://www.biolink.ru.

6.6. Інтелектуальні мережі відеоспостереження

Як було зазначено в четвертому розділі посібника, методи розпізнавання за зображенням лиця особи можуть працювати з двовимірними або з тривимірними зображеннями (так звані 2D- і 3D-фотозображення).

Починаючи з 2006 року, коли була затверджена перша версія проекту поправки до міжнародного стандарту в галузі біометрії (ISO/IEC 19794-5), дедалі більше поширюється комбінований (2D + 3D) метод розпізнавання обличчя. Цей безконтактний метод дозволяє забезпечувати значно більшу вимірюваність використовуваної біометричної характеристики (інакше кажучи, дозволяє досягти збільшення швидкості верифікації, тобто істотно зменшити час проходження контролю) і суттєво підвищити точність ідентифікації особистості.

Під час проведення тестувань було встановлено, що рівень розпізнавання за тривимірною методикою набагато вищий, ніж за двовимірною, і становить понад 90% порівняно з майже 50% у 2D. Пояснюється це тим, що геометричні параметри тривимірного зображення обличчя реально пов'язані з антропометричними характеристиками, які є унікальними для кожної людини, і тому як вимірювальні ознаки набагато надійніші для комп'ютерних алгоритмів порівняно зі звичайними двовимірними фотозображеннями.

Нині відеоспостереження є основою всіх глобальних систем безпеки. Зважаючи на зростаючу потребу в захисті людей та їх майна, а також профілактичний ефект від використання відеосистем безпеки, передові міжнародні компанії здійснюють значні інвестиції у системи відеоспостереження. Нині впровадження таких систем розглядається не тільки як запобіжний засіб, але і як нагальна потреба для забезпечення безпеки в зонах підвищеного ризику.

Значний розвиток інформаційних мереж із достатньо високою пропускною спроможністю та якістю обслуговування за доступними цінами, а також подальший розвиток цифрових технологій передачі відеоданих за допомогою мережі надають унікальну можливість для створення більш ефективних, гнучких і з можливістю розширення систем відеонагляду. Нині системи відеоспостереження використовуються в інтеграції з іншими елементами глобальної системи безпеки такими, як системи контролю за доступом, за можливістю несанкціонованого проникнення, протипожежні системи, датчиками диму або підтоплення. Це, по суті, дає право стверджувати про створення якісно нових систем

[1] BioTime – биометрическая система № 1 в России и СНГ // Biotime.ru. – 2013. – 3 ноября. [Электронный ресурс]. – Режим доступа: http://www.biotime.ru/...

спостереження, контролю й управління ситуаціями, що виникають на об'єктах, які перебувають під наглядом.

Після 2006 року контроль за допомогою зображення обличчя впевнено поліпшує свої позиції у суперництві зі трьома так званими «великими біометриками», особливо під час проведення автоматичного виокремлення та розпізнавання індивідуумів на відстані. Тому ця технологія особливо цікава спецслужбам.

Міжнародна організація цивільної авіації (ICAO) та Міжнародна організація із запровадження стандартів (ISO) запровадили низку додаткових вимог до фотозображень, які використовуються у документах, що дозволило масове запровадження у повсякденне життя систем автоматичного розпізнавання осіб за їх лицем. Ідентифікація людини за рисами її обличчя – один із найдинамічніших напрямів у біометричній індустрії, що посилено розвивається. Поширення мультимедійних технологій, завдяки якому дедалі частіше можна помітити відеокамери на міських вулицях і площах, в аеропортах і вокзалах та інших суспільних місцях, визначають необхідність удосконалення розвитку цього напряму.

Нині безліч потужних компаній у далекому зарубіжжі та навіть у СНД (в основному в Росії), розробляють математичні алгоритми і відеокамери для тривимірного (3D) або комбінованого (2D + 3D) розпізнавання людей за їх обличчям. Багато державних і комерційних споживачів біометричних технологій (різні державні структури, особливо правоохоронні органи, банки, аеропорти, IT-компанії, громадські організації та низка інших установ) зацікавлені у постійному розвитку технологій цього виду біометрики.

Біометричні рішення, що використовують метод біометричної ідентифікації за зображенням лиця особи під час відеоспостереження, нині дедалі ширше використовуються в останніх розробках інтегрованих систем контролю й управління доступом. Вони дають можливість значно зменшити час проведення контролю на пропускних пунктах, що особливо важливо в години пік. Варто зазначити таку особливість, що будь-які комплектуючі пристрої нових систем, які нині розробляються, можуть бути достатньо легко та швидко інтегровані у більшість встановлених раніше систем контролю й управління доступом, котрі вже експлуатуються. Це дає можливість підвищувати ефективність таких систем без заміни всієї системи контролю управління доступом (СКУД). Завдяки достатньо гнучкому налаштуванню останніх систем відеоспостереження можна легко спроектувати та запровадити індивідуальні варіанти дооснащення новою апаратурою як систем безпеки всього об'єкта, що перебуває під охороною, так і його окремих ділянок або приміщень.

Як вже зазначалось, традиційні біометричні рішення в СКУД, які доповнені комплексами відеоспостереження, дозволяють ефективніше контролювати пропуск співробітників і відвідувачів, забезпечувати вищий рівень контролю доступу як до об'єкта, що охороняється, так і до окремих його ділянок, дозволяючи прохід за пред'явленим ідентифікатором тільки одного суб'єкта з певним рівнем допуску. Такі системи контролю управління доступом застосовуються для обмеження доступу на різні об'єкти та установи з одночасним проведенням обліку робочого часу.

Об'єкти й установи, що перебувають під охороною, можуть бути:

– державної власності;

– військового і спеціального призначення, зокрема атомні станції, різні хімічні підприємства та т. д.;

– особливо небезпечні лабораторії та секретні ділянки виробництва;

– будівлі банків, особливо приміщення, де містяться банківські сховища;

– приміщення та взлітні смуги аеропортів, інфраструктура інших транспортних вузлів;

– стадіони, концертні зали, мобільні та стаціонарні виставки, інші місця значного скупчення людей;

– офіси та бізнес-центри;

– фітнес-центри, лікарні, інші медичні заклади;

– освітянські установи різного рівня;

– під'їзди багатоповерхових будинків, приватні будинки та квартири.

Наявність відеоспостереження дозволяє проводити аналіз записів інцидентів, які були зафіксовані, організовувати накопичення статистичної інформації з метою подальшого аналізу для виявлення вразливих місць у системі безпеки та створення банку даних стосовно осіб, які є систематичними порушниками встановленого режиму безпеки[1].

Сучасні системи відеонагляду можуть складатися з сотень відеокамер і виконувати безліч завдань. Наприклад, у міжнародних аеропортах багато підрозділів проводять різні контролюючі або наглядові операції: митний контроль, забезпечення безпеки польотів, прийом і видача багажу, пожежна безпека, контроль за пропуском пасажирів тощо. Кожен із цих підрозділів, як правило, використовує систему відеоспостереження з функціями, що дають можливість відеонагляду за зображеннями місць, що перебувають під контролем, і здійснювати запис отриманих відеокадрів одночасно з декількох камер, які розташовані за різними точками проведення спостереження і які отримують відеозображення з декількох напрямів (ракурсів). Для цього необхідно організувати прийом відеосигналів в один і той же час із декількох ділянок і проводити одночасний їх запис зі всіх точок відеоспостереження. Отже, зважаючи на умови роботи та проведення запису за один і той же проміжок часу значної кількості відеокамер, виникає необхідність постійного пошуку нових схемних рішень для комутування кабелів і розташування матричних відеокомутаторів.

Під час застосування великої системи відеонагляду, яка може налічувати декілька сотень відеокамер, обслуговуючому персоналу практично неможливо забезпечити на належному рівні спостереження за зображенням із кожної відеокамери, тому невелика кількість дійсно важливих кадрів просто може загубитися серед великої кількості відеоінформації. У таких системах необхідно забезпечити автоматизоване виведення зображень на монітори спостереження з відеокамер, які фіксують неординарні події, наприклад, відеокадри відчинення дверей із камери, що зазвичай наглядає за закритими дверима. Тому те, що виводиться в такий час на екрани моніторів, для операторів охорони є негайним сигналом тривоги і дозволяє зосередити основну увагу на цій зоні контролю. Архітектура побудови мережі у такій системі повинна бути достатньо «розумною», щоб гарантувати безперервну роботу кожної відеокамери і наявність безперервного зв'язку з нею. Для виконання цієї умови була розроблена спеціальна мережева база для систем багатофункціонального відеонагляду[2].

Інтелектуальне використання спеціальних інформаційних мереж у системах цифрового відеоспостереження дозволяє:

– забезпечувати значну економію засобів нагляду і, як наслідок, економію коштів;

– домогтися більш високої якості обслуговування та ефективності управління;

– організувати своєчасну й якісну передачу інформації та її отримання без збоїв, досягти високої чіткості зображення на відеокадрах.

---

[1] Современные биометрические системы безопасности // Byte. – 2006. – № 6 (94). – июнь. [Электронный ресурс]. – Режим доступа: http://www.bytemag.ru/articles/ detail…

[2] Новые горизонты CCTV // Secnews.ru. – 2003. – 30 мая. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/articles/...

Перехід на цифрову технологію відеоспостереження уможливило введення низки ключових апаратних рішень (наприклад, таких, як пристрої обробки відеосигналів) безпосередньо в саму мережу систем безпеки відеонагляду, що, своєю чергою, сприяло удосконаленню таких централізованих систем і, у підсумку, підвищенню загального рівня безпеки.

Такі системи дозволили провести автоматизацію низки операцій і, як наслідок, оптимізувати роботу працівників служб безпеки. Тепер у разі подачі сигналу тривоги під час виявлення будь-якого руху в контрольованій зоні система автоматично включає процедуру відеозапису місця такої події, що сприяє підвищенню ефективності рівня безпеки та значній економії коштів.

Тепер користувачі спеціальних інформаційних мереж цифрового відеоспостереження отримали такі можливості:

– проводити одночасний запис, відтворення, архівацію та спостереження за відеозображеннями в режимі реального часу з використанням усіх мережевих можливостей;

– у разі потреби отримати негайний доступ до будь-якого джерела даних (зокрема до відеозображень і звуку в режимі «On-line»), незалежно від місця під'єднання оператора до мережі та від використання водночас цих даних іншим користувачем;

– простоту проведення модернізації за умови подальшого розширення мережі, зокрема можливість заміни всіх апаратних засобів системи на більш сучасні пристрої;

– високу якість роботи системи навіть за умови значного віддалення від джерела даних;

– відстеження роботи та можливість управління будь-якими елементами мережі, а у разі виникнення збою в будь-якому компоненті системи негайно отримати відповідний сигнал про це;

– підвищення ефективності безпеки в самій мережі – заборона доступу до компонентів мережі будь-якого суб'єкта без підтвердження наявності відповідного допуску в нього;

– організація здійснення пошуку в чітко заданих межах ділянки спостереження – задається якась наглядова зона для відеокамери і пошук наявності будь-якого руху проводиться тільки в межах зазначеної зони. Це дозволяє істотно зменшити час, який необхідний для пошуку потрібних кадрів у відзнятому відеоматеріалі;

– здійснення процесу архівації відзнятого матеріалу на спеціальні носії. Як відомо, основна перевага цифрової архівації у тому, що відзнятий відеоматеріал практично можливо зберігати вічно;

– ввімкнення відеозапису за сигналом тривоги, причому дозвіл на запис і його швидкість можуть задаватися за допомогою різних тривожних сигналів за вибором оператора, що дає можливість увімкнути режим запису залежно від активності руху об'єктів у зоні спостереження, а також оцінки ситуації біля пристроїв контролю за доступом, касових терміналів, банкоматів та інфрачервоних модулів;

– здійснення запису та проведення архівації з використанням алгоритму й архітектури SAN (Storage Area Network – «сервер-сховище даних») для одержаних в оцифрованому виді даних, що охоплює також і можливість резервного оперативного зберігання (архівація здійснюється автоматично самою системою, а оператор може працювати як з «онлайновою», так і з архівною інформацією).

Істотним плюсом нової спеціальної інформаційної мережі є те, що вона, використовуючи апаратуру мережевих DVR разом із сучасними кодеками, дозволяє здійснити одночасне об'єднання декількох мереж даних (охоронного телебачення, пожежної тривоги, контролю доступу, телефонного зв'язку тощо) в одну загальну «інформаційну».

Можливість формування лише однієї мережі зумовлює істотне зниження її собівартості як з погляду проведення її монтажу, так і під час подальшого обслуговування[1].

Із 2006–2007 років можна говорити про початок нової ери у відеонагляді – почалось практичне використання перших мережевих рішень відеоаналітики. Вперше в наявних технічних рішеннях високоякісна відеоаналітика була поєднана з можливостями проведення маршрутизації пріоритетного відеосигналу.

Обробка й аналіз відеосигналу вважається найбільш актуальним і перспективним напрямом сучасних досліджень у технології СКУД. Приблизно 10 років тому було вирішено завдання розмежування процесу розпізнавання зображень на два самостійних напрями: перший напрям – доведення відеокадрів до вигляду, за якого можна здійснити процедуру розпізнавання; другий напрям – безпосереднє розпізнання самих зображень у кадрах. Для вирішення цих завдань виникла нагальна потреба в розробці методів і засобів побудови формальних описів зображень – так званих «метрик». Математичні алгоритми методу формального опису зображень використовувались під час створення сучасних систем машинного зору, що дозволяють у реальному часі отримувати тривимірні портрети обличчя людей у вигляді набору сполучень окремих крапок. Нині процес порівняння зображень лиця індивідуума та здійснення аналізу для встановлення їх подібності під час процедури біометричної ідентифікації здійснюється з використанням методу формального опису зображень.

Нині можна говорити про такий напрям досліджень, як комп'ютерний зір. Комп'ютерний зір – це теоретичне обґрунтування та технологія створення пристроїв, які можуть бачити майже так, як людина. Цей напрям динамічно розвивається й удосконалюється, а використання комп'ютерного аналізу дозволяє «витягувати» дедалі більше інформації з оцифрованих відеозображень шляхом відділення корисних сигналів від перешкоджаючих, наприклад: гілки на дереві, що розгойдує вітер, – ця інформація не є цікавою для оператора, а ось людина, яка проходить біля дерева, – є цікавою під час відеоспостереження.

За своєю суттю комп'ютерний зір – це будь-яка форма обробки графічної інформації, яка може бути представлена у вигляді статичного зображення (один кадр), так і змінною у часі послідовністю відеокадрів (зображення в динаміці). Дуже цікавими є алгоритми, які використовують водночас як джерела даних оцифровані відеосигнали від різних камер.

Ефективність охоронних систем сьогодні дедалі більш залежить від достовірності розпізнання в режимі реального часу можливих загроз безпеці об'єкта, який перебуває під охороною. Вона залежить від оцінки поведінки суб'єкта спостереження, що призводить до необхідності багатогодинних переглядів масивів відеоданих, які цікаві для пошуку і виокремлення необхідної інформації. Це вимагає наявності та використання відповідних засобів відеоаналітики, які дозволяли б одночасно використовувати й обробляти сигнали з десятків і навіть сотень відеокамер, які розташовані на території об'єкта, який перебуває під охороною. Нові технології мережевої відеоаналітики мають високопродуктивні аналітичні засоби, які дозволяють практично пристосовуватись до будь-яких розмірів об'єктів, які охороняються, а також і до найскладніших умов відеоспостереження як усередині приміщень, так і поза ними.

Під час використання систем відеоспостереження в режимі реального часу однією з ключових проблем є досягнення високої швидкості обробки кадрів-зображень з умовою

[1] Новые горизонты CCTV // Secnews.ru. – 2003. – 30 мая. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/articles/...

непогіршення якості кінцевого результату. Під час програмної реалізації алгоритмів розмежувань на декілька потоків за поведення цифрової обробки інформації виникають певні труднощі, що призводять до деяких ускладнень під час апаратної реалізації цього процесу в обчислювальних системах. Безпосередньо якість результату залежить від продуктивності використовуваних математичних програм і апаратної платформи, тому високоякісна реалізація універсального алгоритму призводить до значного подорожчання систем відеоспостереження. Більшість розробників програмного забезпечення виходять з цієї ситуації, адаптуючи алгоритми під конкретні завдання та наявні апаратні платформи з метою досягнення потрібної швидкодії, ігноруючи певною мірою вимогу універсальності.

На ринку пропонуються продукти понад 50 компаній, які в інтелектуальних системах відеоспостереження застосовують спеціально розроблені математичні алгоритми. Подальший розвиток таких алгоритмів – це шлях у майбутнє[1].

Стівен Гольдберг, президент та генеральний директор компанії «Vidient Systems Inc», у якій були розроблені перші зразки мережевої інтелектуальної відеоаналітики, висловився так: «Ми здійснюємо новий, вельми сміливий підхід до відеонагляду. Нами створено відкриту платформу для запровадження тонкої відеоаналітики, формування метаданих, інтелектуальної розстановки пріоритетів і маршрутизації скомпресованих потоків високоякісного відеозображення. Тим самим ми сформували нову категорію продуктів – мережевих вирішень інтелектуальної відеоаналітики. Цей підхід, заснований на застосуванні мережі, дозволяє нашим клієнтам забезпечити потрібний доступ обчислювальних потужностей та аналітичного програмного забезпечення до таких місць, де це вкрай необхідно: у внутрішніх приміщеннях, які перебувають під охороною, причому досягаючи віддалених куточків будівль і споруд. Нова платформа відеоспостереження має високий ступінь масштабності та відповідності галузевим стандартам, тому здатна працювати з широким спектром моделей відеокамер охоронного телебачення – від аналогових до найскладніших цифрових пристроїв. Так утворилась єдина система, яка перевищила межу можливостей технологій попереднього покоління. Вона дозволяє прискорити конвергенцію корпоративних IT-систем у бік зростання інвестицій у фізичну безпеку підприємств»[2].

Компанією «Vidient» також була розроблена технологія системи відеоаналітики, яка може обробляти і кодувати велику кількість потоків відеоінформації водночас за допомогою спеціальних алгоритмів обробки відеоаналітичних даних. Нова система добре підходить для застосування в умовах використання значної кількості телекамер відеоспостереження, які об’єднані у мережу та розподілені за всією територією виробничого об’єкта або навіть групи об’єктів, у будь-яких громадських місцях скупчення людей. Система характеризується відкритістю, що дозволяє їй легко адаптуватись у єдине ціле з уже існуючими рішеннями.

«Vidient» сформувала своє нове сімейство продуктів на базі відкритої архітектури, що здатна до розширення і яка дозволяє значно спростити процес інтеграції з іншими системами та пристроями, що використовуються у системах безпеки, такими, наприклад, як засоби контролю доступу, біометрії, радіочастотного розпізнавання, глобального по-

[1] Чижов А. Компьютерное зрение – завтрашний день охранных систем / А. Чижов // Системы безопасности. – 2008. – № 2. [Электронный ресурс]. – Режим доступа: http://www.secuteck.ru/articles2/videonabl/...

[2] Начало новой эры в видеонаблюдении – первые сетевые решения видеоаналитики // Secnews.ru. – 2007. – 23 мая. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/...

зиціонування, оптичного розпізнавання символів. Особливістю цієї розробки компанії є наявність маршрутизатора (тепер уже стара розробка: SmartCatch IVR2400), який одночасно кодує в загальноприйняті формати обміну даними (H.264 або MPEG4) чотири повноформатні відеопотоки, що надходять з аналогових або цифрових IP-камер, і забезпечує таке управління компресією, яке дозволяє автоматично надавати кожному відеопотоку відповідний пріоритет. Практично це означає, що в кожен окремо взятий момент часу пристрій автоматично виділяє для негайної передачі відеокадри, що є з погляду системи найбільш значущими для забезпечення безпеки організації клієнта, причому виокремлює максимально можливу кількість ресурсів мережі для досягнення максимальної пропускної спроможності у цей час.

Сьогодні технічні рішення нової системи відеоаналітики використовуються в багатьох країнах світу, насамперед для організації відеоспостереження в суспільних місцях і крупних транспортних вузлах – таких, наприклад, як міжнародні та внутрішні аеропорти Сан-Франциско, Сан-Дієго, Солт-Лейк-Сіті, Таллахасси, Флориди (США), Хельсінкі (Фінляндія) та багато інших.

«Ринок відеоаналітики знаходиться в стані затишшя перед бурею, – говорить Діліп Саранган (Dilip Sarangan), аналітик-дослідник дослідницько-консалтингової компанії «Frost & Sullivan», яка відстежує розвиток ринку систем і засобів безпеки. Вибухонебезпечний стан ринку пов'язаний із тим, що дедалі сильніше зростає потреба у відеоспостереженні, яке повинно мати випереджальний характер, в усуненні помилок, які виникають унаслідок дії людського чинника, у конвергенції фізичних та електронних систем і підвищенні можливостей масштабування».

Компанія «Frost & Sullivan» прогнозувала, що обсяг ринку відеоаналітики зросте від 60 млн доларів у 2005 році до 400 млн доларів у 2012 році[1].

Використання сучасних систем відеоспостереження створюють нові можливості. Крім систем контролю управління за доступом, їх використання особливо важливе під час організації систем відеонагляду в суспільно-громадських місцях і транспортних вузлах. Останнім часом правоохоронні органи дедалі частіше використовують ці системи для відстеження та документування правопорушень, що скоюються у громадських місцях. Мережеві системи відеоспостереження забезпечують виконання і цього завдання. А застосування функцій міток часу й електронного «водяного знаку» під час шифрування «оригінальних» даних, що передаються, означає, що безпосередньо у процес моніторингу та архівного запису запроваджено процедуру відповідного контролю, яка гарантує достовірність записів. А це означає, що відеоматеріали та кадри зображень можна використовувати як докази в суді[2].

Сьогодні значна частина людства дедалі більше визнає потребу широкого використання заснованих на біометрії систем контролю за доступом та ідентифікації у громадських місцях за допомогою камер відеонагляду осіб, що перебувають у розшуку чи становлять загрозу для суспільства.

Технологія відеоспостереження, яка спочатку була призначена суто для запобігання та виявлення звичайних правопорушень, нині еволюціонує в сторону дедалі більшого використання для захисту від виявів екстремістських і терористичних дій. У світі лунають вибухи, до скоєння яких причетні різні радикально налаштовані політичні та

[1] Начало новой эры в видеонаблюдении – первые сетевые решения видеоаналитики // Secnews.ru. – 2007. – 23 мая. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/...

[2] Новые горизонты CCTV // Secnews.ru. – 2003. – 30 мая. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/articles/...

релігійні угруповання. Крім того, загалом зростає загальна кількість злочинів, що вчиняються у громадських місцях. На цьому тлі зростає використання новітніх систем контролю за доступом і збільшується попит на останні розробки систем інтелектуального відеоспостереження.

Симбіоз таких новітніх технологій, як біометрія, IP-відео та відеоаналітика, радіочастотна ідентифікація (RFID-ідентифікація) з технологіями безпеки став поштовхом для зростання світового ринку засобів безпеки. Із переходом світового ринку систем відеонагляду з аналогової технології на цифрову з'явилися нові широкі можливості для удосконалення вже діючих апаратно-програмних комплексів безпеки та створення нових систем інтелектуального відеоспостереження.

Розвиток інформаційно-комп'ютерних систем на базі формування та використання різних інформаційних мереж – локальних, державних і глобальних (зокрема й Інтернету) – стимулює попит на сучасне спеціалізоване програмне забезпечення та передові технології для масового запровадження систем відеоспостереження.

Спостерігається тенденція до розвитку і поширення інтелектуальних технологій, що забезпечують виявлення та ідентифікацію суб'єктів спостереження у реальному масштабі часу, організацію віддаленого доступу до пристроїв контролю, а також реалізацію таких технологічних рішень, що значно підвищують ефективність роботи оператора за одночасного її полегшення.

Страх перед можливістю вчинення терористичних актів і зростання злочинності у провідних країнах світу змусили уряди цих держав висунути як пріоритетне завдання забезпечення громадсько-суспільної безпеки та захисту законослухняних громадян, що вимагає вкладання чималих коштів у розвиток відповідних технологій. Експерти передбачають, що зближення технологій контролю за доступом з іншими технологіями забезпечення безпеки, насамперед заснованих на використанні технологій біометрії та відеонагляду, зумовить значне зростання попиту на універсальні системи забепечення безпеки, причому, як очікується, починаючи з 2008 року щорічні темпи зростання світового ринку систем безпеки можуть становити приблизно 37%[1].

Під час проведення олімпійських ігор 2008 року в Пекіні використовувалася система відеоспостереження «Smart Surveillance System» (S3) компанії «IBM», основним призначенням якої було стеження за порядком у громадських місцях. Комплекс S3 дозволив отримувати інформацію від найрізноманітніших джерел і видавати попередження про підозрілу поведінку людей або появу підозрілих осіб у недозволених для їх перебування місцях[2].

Великобританія є однією з найбільш передових країн за накопиченим досвідом розробки та використанням систем охоронного телебачення. Відеоспостереження є одним із чинників забезпечення безпеки в Сполученому Королівстві.

Найтиповіші завдання, що актуальні для більшості встановлених систем відеоспостереження, – це контроль скупчень людей, боротьба з крадіжками, забезпечення громадської безпеки, запобігання несанкціонованому проходу. У Великобританії значна частина подібних систем встановлюється і підтримується за рахунок коштів органів державної, регіональної і муніципальної влади. Але і системи охоронного телебачення, що встановлюються приватними компаніями, часто надають істотну допомогу британській поліції

[1] Рынок программного обеспечения для видеонаблюдения: на пути к успеху // Secnews.ru. – 2006. – 18 июля. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/...

[2] В Токио появится трехмерная система видеонаблюдения // Bezpeka.com/ru. – 2008. – 16 января. [Электронный ресурс]. – Режим доступа: http://bezpeka.com/ru/news/...

у розслідуванні злочинів. Згідно з чинним законодавством, компетентним органам забезпечується доступ до знятого приватними системами матеріалу, крім того, встановлення систем відеонагляду, наприклад, у супермаркетах, призводить до значного скорочення випадків крадіжок і зменшує навантаження на поліцію. Тому держава зацікавлена в розвитку приватних систем охоронного телебачення та в їх максимальній ефективності.

Як відомо, Великобританія є країною з найбільшою в світі кількістю відеосистем зовнішнього спостереження за питомою вагою на 1 тисячу населення. Із цієї причини в багатьох інших державах англійський досвід розглядають як «наше майбутнє завтра». Відомості про наявну кількість британських телекамер стеження невпинно зростають. На початок 2007 року їх налічувалося майже 4,2 млн (приблизно 20% від загальної кількості такої апаратури на планеті), або по одній на кожних 14 громадян Сполученого Королівства. Причому йдеться лише про апаратуру, яка встановлена державними органами в громадських місцях, тобто наведені дані не враховують значної кількості приватних камер відеонагляду, що здійснюють спостереження за відвідувачами у будинках, магазинах і офісах компаній. Якщо ж взяти до уваги, що люди постійно переміщуються з місця на місце, то, згідно з неофіційними підрахунками, кожен британець може потрапляти в об'єктив камер стеження в середньому понад триста разів на день[1].

Зважаючи на такий стан запровадження систем відеонагляду, немає нічого дивного у тому, що відділ наукових досліджень Міністерства внутрішніх справ Великобританії випустив настанову під назвою «Керівництво зі складання експлуатаційних вимог до системи охоронного телебачення». Одна з доступних авторам версій цього документа за шифром 4.0 була опублікована ще у 2007 році. У цьому документі детально описано, як зробити вибір типу системи охоронного відеоспостереження, яке відповідало б потребам замовника.

Автори посібника вважають вимоги настанови актуальними для використання і в нашій країні, в зв'язку з чим наведемо низку її основних положень. Відповідно до цього документа, здійснення вибору та встановлення системи має охоплювати чотири ключові рівні, що схематично наведено на малюнку 6.

Мал. 6. Ключові етапи проектування

[1] Киви Берд. Утопия и жизнь / Берд Киви // Компьютерра. – 2007. – № 14. – 12 апреля. [Электронный ресурс]. – Режим доступа: http://offline.computerra.ru/...

Перший рівень полягає у визначенні самої суті вирішуваної проблеми – це може бути безпосередня загроза безпеці об'єкта, якийсь з аспектів громадської безпеки або перше та друге разом. Сформульовану проблему визначають як експлуатаційну вимогу першого рівня. На цьому етапі необхідно однозначно визначити, чи є встановлення системи охоронного телебачення найбільш відповідним рішенням цієї проблеми або існують інші, більш раціональні шляхи її вирішення.

Після усвідомлення повної картини всіх проблем і аспектів, що стосуються вирішення проблеми, необхідно особливу увагу приділити спеціалізованим аспектам, що стосуються виключно охоронного відеонагляду. Саме вони і становлять *другий рівень* експлуатаційних вимог. Надалі їх усвідомлення та перелік допоможе відповідальному за безпеку розмежувати *зони відповідальності* співробітників, зрозуміти всі сторони *процесу експлуатації* системи, розробити *можливі сценарії реагування* на неадекватні ситуації, сформувати оптимальну *конфігурацію системи* охоронного відеонагляду та ухвалити правильні *управлінські* рішення для формування всієї системи безпеки.

Наведений у документі алгоритм визначення експлуатаційних вимог дозволяє потенційному користувачеві системи відеоспостереження отримати структурований список питань, за допомогою якого він зможе остаточно сформулювати вимоги до майбутньої системи загалом для подальшого використання під час вибору та замовлення відповідного програмно-апаратного забезпечення.

Третій рівень – розробка детальної технічної специфікації майбутньої системи відеоспостереження. Зокрема, проводять остаточний вибір моделі відеокамер, підбирають необхідний алгоритм стиснення відеосигналів, визначають потрібну величину обсягу архівної інформації, що повинна архівуватися та зберігатися, здійснюється вибір носіїв для зберігання відзнятого матеріалу.

Четвертий рівень – тестування верифікаційних можливостей системи – проводиться після завершення монтажу та запуску системи. На цьому етапі особливо важливо перевірити, наскільки отриманий результат відповідає запроектованим вимогам і наскільки можливості системи відповідають поставленим завданням.

Перед тим, як зосередитися на технічних характеристиках вибраного для встановлення варіанта системи відеонагляду, необхідно оцінити загалом масштаб загрози або проблеми, яку планують нейтралізувати за допомогою цього заходу. Формулювання та складання осмисленого переліку вимог до безпеки об'єкта загалом названо у настанові *складанням експлуатаційних вимог першого рівня*. Типовий алгоритм цих вимог наведено на мал. 7 і він використовується під час складання пояснювальної записки. У цьому документі замовник повинен сформулювати відповіді на поставлені питання та переконатися у тому, що основні вимоги для досягнення необхідного рівня безпеки проаналізовані правильно, а вибране рішення є оптимальним.

Експлуатаційні вимоги першого рівня *містять такі основні етапи:*

Створення ситуаційного плану (план-схема місцевості чи території об'єкта, де передбачено встановити систему). Першочергове завдання під час визначення експлуатаційних вимог – створення графічної карти-схеми місця, де передбачається запровадження системи та виокремлення на ній зон, які є потенційно небезпечними з погляду забезпечення безпеки.

Водночас здебільшого просто необхідно зазначити на схемі розташування джерел світла, місць майбутнього розміщення камер, їх оглядові поля, виокремити ділянки з поганим освітленням як сонячним, так і штучним, вказати місця, що потрапляють у тінь від дерев і будівель, звернувши особливу увагу на зони, які можуть бути закриті від спостереження листям дерев.

Мал. 7. Складання переліку експлуатаційних вимог (перший рівень)

У документі наведений зразок типового ситуаційного плану, переклад якого, зважаючи на його значний обсяг, у посібнику не наводиться.

Формулювання завдань, які плануються вирішити за допомогою встановлюваної системи відеонагляду. Наступним етапом є визначення кола проблем і завдань, які плануються вирішити за допомогою встановлюваної системи відеоспостереження. Цей етап полягає у визначенні загальної кількості проблем, які можуть виникнути під час забезпечення безпеки на цьому об'єкті. Деякі з них можуть бути загальними (типовими) загрозами, а інші – локальними (специфічними). Найбільш типові завдання, що є актуальними для більшості об'єктів, – це спостереження та контроль можливих місць скупчень людей, забезпечення громадської безпеки, боротьба з крадіжками, припинення несанкціонованого проходу.

Усі потенційно можливі проблеми або загрози повинні бути вказані у плані, що надалі допоможе визначити ступінь можливої загрози та необхідний рівень покриття зон об'єкта оглядовими полями відеокамер. Деякі ділянки (прохідні об'єкта або пункти входу-виходу) можуть вимагати проведення одночасного спостереження з декількох місць. Крім загального спостереження за особами, що проходять пункти пропуску, додатковим завданням є фіксація можливих випадків крадіжок або інших виявів антисоціальної поведінки.

Визначення кола зацікавлених учасників, упровадження відеонагляду. Якщо передбачається встановлення комплексної системи безпеки, яка може зачіпати інтереси різних господарюючих суб'єктів, визначають кількість зацікавлених юридичних осіб і, в разі надання ними згоди, узгоджують деталі експлуатаційних вимог встановлюваної системи відеоспостереження, а за наявності зауваженень відображають їх у ситуаційному плані.

Оцінка можливих загроз. За можливості визначають імовірність виявів можливих небажаних подій, класифікуючи водночас імовірність виникнення майбутніх загроз як низьку, середню або високу. На цьому етапі прагнуть визначити масштаб наслідків у разі, якщо інцидент не буде зафіксований відеокамерою. Чи можуть бути завдані фінансові збитки і чи не виникне загроза безпеці обслуговуючому персоналу та відвідувачам? За можливості необхідно виокремити пріоритетні типи інцидентів, які потрібно буде насамперед фіксувати. Також варто здійснити порівняльну оцінку варіантів використання й інших, більш дешевих способів вирішення проблем, які зможуть запобігти виникненню небажаних інцидентів. Мається на увазі, наприклад, можливість встановлення додаткової огорожі, охоронної сигналізації, поліпшення освітлення небезпечної зони.

Визначення критеріїв ефективності. Визначається ймовірність виявлення інциденту, що у підсумку сприяє можливості його виявлення. Чи можливо у разі виявлення небажаної події запобігти злодійським випадкам або псуванню майна, наскільки реальна ідентифікація на території контрольованого об'єкта будь-якої фізичної особи, що може з'явитися? Наскільки можливе реальне поліпшення керування людським потоком через прохідну, а також припинення у контрольованій зоні будь-якої небажаної діяльності?

Позитивний ефект від запровадження системи визначається тим, як ефективно вона буде функціонувати загалом та наскільки добре відповідатиме експлуатаційним вимогам. Обов'язково необхідно здійснити оцінку того, наскільки у разі виявів будь-яких небажаних подій можливе досягнення позитивного результату. Тобто спробувати визначити ймовірність ефективної та надійної роботи запроваджуваної відеосистеми.

Вибір найбільш ефективного рішення. Після визначення та внесення до ситуаційного плану проблемних зон і потенційних загроз, необхідно здійснити вибір найефективніших способів вирішення можливих проблем. У деяких випадках використання системи відеонагляду може бути тільки частиною комплексу заходів, що запроваджуються, оскільки найліпший результат можливо досягнути тільки у разі проведення низки певних заходів: поліпшення освітленості, встановлення датчиків присутності або охоронної сигналізації. Причому існує вірогідність того, що інколи доцільнішим із погляду економії коштів і досягнення відповідного рівня безпеки провести навіть необхідне архітектурне перепланування.

Проте, на думку британських авторів документа, для *забезпечення фізичної безпеки, попередження протиправних дій та розслідування злочинів* найліпшим вибором є відповідно спроектована система відеоспостереження.

З погляду ефективності обраної конфігурації системи необхідно констатувати, що у випадку, коли злочин доводиться розслідувати після проходження значного терміну з часу його скоєння, то у вибраній системі відеоконтролю були допущені помилки на етапі проектування.

На практиці дуже часто трапляються такі випадки, що злочини, які були зафіксовані відеокамерою, виявляються тільки після передачі в поліцію знятого відеоматеріалу. Водночас часто виявляється, що проведений відеозапис дуже низької якості та, як наслідок, у результаті його перегляду практично мало що можно додатково встановити. Інша доволі поширена помилка проектувальників полягає в неякісній організації процесу архівації, доступу до записаної інформації та її відтворення з архівних матеріалів.

Суттєвим аргументом на користь вибору охоронної системи відеоспостереження є те, що наявність системи на об'єкті повинна мати певне профілактичне значення – злочинець повинен брати цей факт перед здійсненням протиправного діяння.

Якщо в результаті складання експлуатаційних вимог першого рівня було ухвалено рішення про розгортання певного типу системи відеоспостереження, у такому разі приступають до розробки експлуатаційних вимог другого рівня.

Експлуатаційні вимоги другого рівня

Вважається, що мета вимог другого рівня – скласти план дій, який необхідно реалізувати на практиці між ухваленням рішення про розгортання системи відеоспостереження до практичної реалізації цього рішення. Перше та найважливіше питання, на яке потрібно знайти відповідь після ухвалення рішення про розгортання: «За ким або за чим потрібно спостерігати?». За ним відразу ж постає друге: «Чому за цим необхідно спостерігати?».

Застосування відеокамер залежить від мети спостереження для потреб суспільно-громадської безпеки (стеження за скупченням людей або груп людей (натовпом) та їх

пересуванням) і проводиться аж до систем контролю за доступом, коли зняте з близької відстані високоякісне зображення використовується для встановлення особистості. Вибір типу відеокамер насамперед залежить від суті тієї діяльності, за якою передбачається здійснення спостереження.

Для спрощення ситуації та можливості надання рекомендацій для особи, яка розробляє специфікацію системи, використовують співвідношення габаритів людського силуету до розміру екрану монітора, який заплановано використовувати. Існує чотири види спеціально розроблених вимог (категорій) співвідношення зображення фігури та екрана, що використовуються під час вибору розмірів екранів моніторів.

Під час формування експлуатаційних вимог замовникові слід вибрати, який тип категорії найліпше підходить для спостереження за обраним видом людської діяльності. Далі інсталятор системи повинен підібрати таку модель камери, яка б відповідала вимогам обраного типу категорії.

Британські розробники настанови визначають такі існуючі типи категорій співвідношення зображення фігури та розмірів екрана, які обираються залежно від величини розмірів проекцій зображень людських силуетів на екран монітора.

1. Категорія моніторингу та контролю – зображення фігури займає як мінімум 5% від висоти екрана, а картина, що відображається, водночас не переобтяжена «зайвими» об'єктами. За такого рівня деталізації оператор зможе стежити на належному рівні за кількістю, напрямком і швидкістю руху основної маси людей, у лічені секунди визначаючи їх місцеположення.

2. Категорія детектування – фігура займає як мінімум 10% від висоти екрана. Після надходження відповідного сигналу-повідомлення оператор може, перебираючи необхідні зображення з відеокамер стеження, встановити присутність людини в певному місці зони контролю.

3. Категорія розпізнавання – в цьому випадку фігура займає не менше 50% від висоти екрана. Водночас оператор із великою ймовірністю може здійснити процедуру розпізнання особи і зробити попередній висновок щодо того, спостерігав чи не спостерігав його зображення раніше.

4. Категорія ідентифікації – якщо було б можливо повністю помістити зображення людської фігури на екран, то вона займала 120% від висоти використовуваного екрана, причому якість зображення кожного фрагмента загального малюнка фігури суб'єкта має бути достатньою для здійснення процедури комп'ютерного розпізнавання особи.

Мета запровадження цих чотирьох видів категорій – допомогти проектувальнику зробити належний вибір потрібного розміру зображень на екрані для кожної зони контролю, щоб система, яка проектується, відповідала вимогам замовника і були б визначені певні відправні параметри.

Необхідно зазначити, що не існує стовідсоткової гарантії комп'ютерного розпізнавання особистості індивідуума не тільки при висоті зображення фігури менш ніж 50% або 120% від висоти екрана, але й за умови, коли зображення фігури людини може навіть займати понад 120% екрана.

Дуже великий вплив на рівень можливості розпізнання особистості мають такі чинники, як рівень освітленості та кут зйомки об'єкта.

Настанова «Керівництво зі складання експлуатаційних вимог до системи охоронного телебачення» насамперед розроблялась для аналогових систем, тому вона не цілком коректна для цифрових стандартів, які нині є найбільш поширеними. Тому для більшості систем подібна класифікація буде справедливою лише у разі спостереження у реальному

часі з використанням стандартної PAL-камери і PAL-монітора, за звичайного розрішення картини зображення у 576 ТВЛ. Проте ситуація набагато складніша під час використання відео- або телекамери з цифровим виходом і комп'ютерного монітора, коли розрішення зображення, яке отримується, стає абсолютно іншим. У такому випадку під час спроби поділити зображення за необхідним рівнем деталізації є сенс оперувати поняттям кількість «пікселей на ціль».

Ситуація ще більше ускладнюється, якщо ми маємо справу із зображенням, що було заархівоване. Під час запису та архівації до відзнятої інформації можуть застосовуватися різні технології стискання, які в результаті здатні значно знизити якість зображення порівняно з «живою» картиною.

Тобто, це може призвести до такої ситуації, коли фігура, що займає 50% від висоти екрана, легко може бути впізнана під час проведення розпізнавання у реальному масштабі часу, але в разі проглядання збережених у архіві кадрів відеозображень через втрату якості це зробити буде практично неможливо. Тому під час вибору та встановлення системи відеонагляду необхідно звертати особливу увагу на якість відтворених архівних відеозображень так же, як і на якість «живої» картинки. У настанові повідомляється, що в наступних версіях документа британським МВС цьому аспекту приділятиметься значно більше уваги.

Алгоритм підбору експлуатаційних вимог ***другого рівня*** наведений на мал. 8.

Дуже стисло розглянемо основні його етапи.

Визначення проблеми. Мета цього етапу – зібрати інформацію для розробника (інсталятора) щодо місцеположення об'єкта та сформувати перелік вимог до камер спостереження, що будуть використовуватися. Існуючі основні загрози визначені вже на першому рівні формулювання експлуатаційних вимог, а на другому рівні необхідно здійснити їх деталізацію.

Місцеположення або прив'язка до місцевості. Розроблений ситуаційний план розподіляють на окремі зони (директорії або локації), якою може бути така ділянка, де існує ймовірність виникнення будь-якої загрози. Це може бути локальна загроза у відриві від конкретно впливаючого на безпеку чинника, наприклад, місце, де легко можуть бути отримані необхідні високоякісні зображення (прохідна або вхідні двері). Необхідно ухвалити рішення: чи необхідне відслідковування кожного рухомого об'єкта за всією зоною площі, що контролюється.

Водночас необхідно мати детальні відомості щодо існування так званих «мертвих зон» відеокамер і обов'язково зважати на них під час вибору місць розміщення камер спостереження.

Наприклад, на автостоянці можуть бути виокремлені дві директорії: одна для зчитування номерних знаків транспортних засобів, інша – для оглядового моніторингу місця перебування машин безпосередньо на парковці.

Небажані дії. Визначаються типи дій, які зазвичай необхідно контролювати або встановлювати: випадки крадіжок, порушення громадської безпеки, поява скупчення людей, несанкціонований фізичний доступ, неналежна асоціальна поведінка.

Завдання відеоспостереження. Необхідно визначити, який із вищенаведених чотирьох рівнів оглядових категорій проектування зображення фігури на екран найліпше підходить для вирішення проблеми. Можливо, потрібен моніторинг більшої зони, або виокремлення (детектування) людей, що наближаються до будівлі, або розпізнання певних особистостей на ділянці проходу (на прохідній), а можливо виникне необхідність проведення автоматизованої ідентифікації осіб шляхом запровадження системи контролю управління за доступом.

Мал. 8. Складання переліку експлуатаційних вимог до системи відеоспостереження (другий рівень)

Швидкість руху об'єкта спостереження. Інформація про швидкість пересування об'єктів, які потрапили у поле зору відеокамери, критично важлива для вибору оптимальної частоти кадрів.

Лише в поодиноких випадках відзнятий відеоматеріал записується за частоти кадрів «живого відео» (близько 25 кадрів у секунду). Для спостереження за приміщенням або коридором, де люди з'являються рідко, може бути достатньо й одного кадру в секунду, але для запису зображень «пасажиропотоку» на прохідній – і п'яти кадрів у секунду швидше за все буде недостатньо.

Експлуатаційні аспекти. Розглядається процес щоденної експлуатації системи, інакше кажучи, в цьому розділі документа висвітлюють питання стосовно того, що за персонал працює з системою, як він навчений і як він повинен реагувати на різні ситуації (вимагається наявність конкретних планів дій у разі виникнення різних типів нештатних ситуацій), аналіз особливостей місця проведення спостереження тощо.

Значна частина систем охоронного відеоспостереження вимагають наявності операторської – спеціального приміщення, де відбувається моніторинг відеозображень, що надходять із камер відеонагляду. Проте невеликі відеосистеми розроблені переважно на проведення відеозапису, тому записане зображення будь-якого інциденту переглядається тільки як постфактум. У цьому разі низка вищенаведених положень настанови може бути непотрібною, а саме тому під час формування експлуатаційних вимог якраз і повинно бути визначено, чи мусить система бути орієнтована на «живий» моніторинг або тільки на запис для подальшого перегляду.

*Визначення контингенту, яке буде проводити відеоспостереження***.** Це може бути спеціально виокремлений та підготовлений для виконання цієї функції персонал або для роботи можуть залучатися інші співробітники з відривом від виконання своїх основних обов'язків. Деякі системи можуть бути спроектовані та розгорнуті так, що для їх постійного функціонування взагалі не потрібна присутність людини. У разі залучення для організації спостереження певного контингенту осіб слід передбачити необхідність проходження ними спеціального курсу навчання для отримання навичок роботи з системою.

Час проведення спостереження (коли, скільки та як проводити спостереження). Скільки годин на добу й скільки діб на тиждень потрібно проводити безпосередньо «живий» відеонагляд? Чи має сенс здійснення цілодобового моніторингу або досить проводити його тільки впродовж робочого часу підприємства? Наскільки може бути відмінним графік чергувань в операторській у робочі та вихідні дні? Коли необхідне проведення спостереження у режимі реального часу («On-Line») – постійно або тільки під час деяких екстраординарних подій (проведення спортивних або громадських заходів, наприклад, пікетування або інших акцій протесту)?

Місцезнаходження оператора відеонагляду (вибір місця знаходження операторської, звідки проводиться спостереження). На цьому етапі проектування необхідно дати відповідь на питання: з якого фізичного місцеположення повинен стежити оператор за зображеннями, що надходять із відеокамер. Можливо, спостереження доцільніше здійснювати не з операторської, а з офісу спеціальної охоронної компанії? Істотне значення має ергономіка робочого місця оператора. Необхідно однозначно ухвалити рішення з таких питань, як: розміри і форма приміщення операторської, освітленості та наявності вентиляції, фізичної безпеки поста відеонагляду, відстані до об'єкта, що знаходиться під охороною.

Реагування на можливі нестандартні ситуації. Слід розробити чіткий план дій у разі виникнення нештатної ситуації. Необхідно однозначно визначити конкретну особу, яка повинна ухвалювати рішення у разі виникнення потреби у реагуванні, та, за можливості, провести регламентацію алгоритму дій відповідальної особи й оператора/ів/. Наприклад, передбачити порядок дій оператора у разі виникнення нештатної ситуації: чи має він зв'язуватися з охоронним патрулем, менеджером об'єкта, що знаходиться під охороною, з сусіднім постом відеоспостереження або повідомляти спеціальні служби. У деяких випадках цілком достатньо буде зробити відмітку про подію в журналі й утриматися від подальших будь-яких активних дій. На посту відеоспостереження обов'язково має бути встановлена необхідна кількість апаратури зв'язку. Також повинен бути розрахований максимально допустимий час реагування на кожен вид можливих

нештатних подій і розроблена службова інструкція для оператора щодо можливих варіантів його поведінки у разі виникнення таких ситуацій.

Вимоги до обраної системи. Після розробки експлуатаційних вимог за кожною з зазначених у переліку проблем, ґрунтуючись на потребі максимального їх виконання, необхідно здійснити остаточний вибір типу майбутньої системи відеоспостереження, зокрема наявності певної конфігурації апаратно-програмного комплексу.

Наявність сигналізації. Необхідно мати чітку відповідь на питання, які дії повинен проводити системний комплекс після виявлення факту небажаної події? Значна кількість систем володіє функцією автоматичного повідомлення, яка спрацьовує у випадку фіксації тієї чи іншої події. Водночас найбільш ефективним рішенням може бути інтеграція системи відеоспостереження з іншими системами фізичної безпеки, наприклад, охоронною сигналізацією. Одним із варіантів ухваленого комплексного рішення може бути включення (активування) камери відеонагляду після відчинення будь-яких дверей. Альтернативою використання датчиків руху зараз дедалі більше стає так зване «інтелектуальне відеоспостереження», коли функція проведення запису подій вмикається автоматично після виявлення змін у зображеннях відеокадрів, тобто після фіксації наявності будь-якого руху в відеозображенні, що надходить із відеокамери.

На цьому етапі проектування необхідно, відповідно до можливостей розвитку різних варіантів подій, передбачити адекватні способи оповіщення контролюючого персоналу. У деяких випадках це може бути просто однотонний звуковий сигнал, візуальне тривожне оповіщення за допомогою лампочки на пульті, яка починає блимати, текстове повідомлення, що виведене на екран, поява фотозображення на моніторі, а також автоматична передача сигналу тривоги до чергової частини поліції (міліції). У низці випадків це може виявлятися у вигляді видачі команди на початок запису зображень для однієї або групи камер (для економії місця на електронних носіях даних деякі системи не здійснюють постійного запису зображень із відеокамер, проте ця функція може бути задіяна як реакція на певні події). Водночас необхідно зважати на те, що деякі явища або події (такі, наприклад, як мерехтіння світла) можуть постійно активізовувати процедуру запису і за таких випадків записувальний пристрій наповнюватиметься інформацією набагато швидше, ніж передбачалось.

У настанові звертається особлива увага на проведення запису відеозображення та початку його архівації не з часу безпосередньо інциденту, а за деякий час до події. Для реалізації цієї умови необхідно передбачити можливість буферизації даних. Можливе й інше рішення: спочатку застосовувати відеозапис із високою частотою кадрів, а потім видаляти кадри, які не містять корисної інформації.

Окрім цього, як інші автоматизовані дії, бажано застосовувати автоматичне перемикання монітора на ту камеру, яка зафіксувала подію, а також автоматичне проставляння спеціальної відмітки в електронному журналі реєстрації подій.

Монітори. У випадку, якщо було ухвалено рішення про доцільність проведення «живого» моніторингу, слід прийняти рішення про загальну необхідну кількість моніторів та відеокамер, які будуть обслуговуватись одним дисплеєм.

Запис. Визначається термін зберігання відеоінформації, яка буде зафіксована камерами спостереження. Водночас попередньо необхідно визначитись, наскільки якість заархівованої інформації відрізнятиметься від якості «живого» зображення. Також потрібно дати відповідь на такі питання:

– яка необхідна частота кадрів під час проведення запису?

– які інші відомості (наприклад, інформація про час і місце зйомки) повинні бути збережені разом з іншими відеоданими?

На всі ці питання і низку інших обов'язково потрібно дати відповідь на етапі формування експлуатаційних вимог другого рівня. Також достатньо важливим є ухвалення рішення про вибір алгоритму стиснення (стискання) даних.

Експорт/архівація даних. Як уже відомо, система відеонагляду обов'язково повинна володіти функцією запису важливої інформації на постійний носій. У більшості аналогових систем для вилучення інформації було достатнім дістати з архівного сховища відеокасету. А в сучасних цифрових системах потрібно здійснити копіювання даних із внутрішнього вінчестера на CD або DVD-диск (або інший носій) перед тим, як надійде команда на очищення жорсткого диска від старої інформації та початку запису нової. Тому в разі використання цифрових систем відеоспостереження необхідно заздалегідь ухвалити рішення щодо вибору методів копіювання та збереження даних.

Аспекти менеджменту й обслуговування. У цій частині настанови розглядаються аспекти відносин із державними регулювальними органами, а також організаційні питання щодо ремонту та технічного обслуговування системи. Наведено перелік офіційних документів, які необхідні для отримання дозволу на установку системи відеонагляду, а також надано рекомендації про частоту вжиття профілактичних заходів для технічного обслуговування системи.

Вказано на необхідність вибору технічного виконавця для проведення регламентного обслуговування та можливого ремонту системи. Відповіді на ці питання повинні бути передбачені до впровадження системи в експлуатацію.

Британське Міністерство внутрішніх справ наполегливо рекомендує дотримуватися принципу «сім раз відмір та один раз відріж». Переходити до стадії технічної реалізації проекту необхідно тільки після найретельнішого опрацьовування питання обґрунтування вибору системи відеоспостереження, у жодному випадку не довіряти вирішення стратегічних питань іншим компаніям, оскільки інтереси продавця і покупця можуть діаметрально відрізнятися.

Необхідно постійно пам'ятати про головну мету, не передоручати вирішення проблеми іншим юридичним і фізичним особам, детально вникати в технічні деталі – тільки у такому разі вибрана та встановлена система відеоспостереження повинна допомогти у вирішенні поставлених завдань і, безумовно, окупити себе[1].

Оригінал документа є у відкритому доступі в мережі Інтернет за адресою: *www.crimereduction.homeoffice. gov.uk/cctv/cctv047.htm.*

Технології автоматизованого відеоспостереження та розпізнання людей за обличчям постійно розвиваються й удосконалюються. За повідомленням газети «Нью-Йорк Таймс» у США в інтересах департаменту держбезпеки (DHS) за контрактом вартістю понад 5 млн доларів фірмою «Electronic Warfare Associates» створюється система, яка має абревіатуру BOSS («Biometric Optical Surveillance System /BOSS/ at Stand-off Distance» – «Біометрична система для дистанційного оптичного спостереження»).

У стислому вигляді ключові моменти технічного завдання, які покладені на систему BOSS, виглядають так:

1. Служба DHS відповідає за біометричну ідентифікацію людей для визначення того, чи не перебуває зараз особа, яку зафіксовано в зоні спостереження, у федеральному списку осіб, які знаходяться у розшуку або повинні відслідковуватися на законних підставах. Для виконання цього завдання підрозділам DHS потрібна можливість встановлювати особистість людей у прихованому, надійному й оперативному режимі.

[1] Правильная система видеонаблюдения – английский подход // Secnews.ru. – 2008. – 20 марта. [Электронный ресурс]. – Режим доступа: http://www.secnews. ru/articles/…

2. Такі потреби вимагають проведення масового збору, зберігання, передачі та прийому біометричних і біографічних даних людей у реальному масштабі часу (режим On-line). За технічними умовами проекту кінцевий продукт повинен бути портативним і працездатним у широкому спектрі різноманітних умов (мати можливість працювати вночі й удень, у сухому та вологому кліматі, у широкому діапазоні температур повітря).

3. Вихідні дані системи BOSS повинні бути придатними для здійснення пошуку і у великих базах даних (ідентифікація – виявлення одного серед багатьох), і для встановлення однозначної відповідності раніше отриманим і збереженим в архівному масиві біометричним зразкам (верифікація 1 до 1).

4. Програмне забезпечення BOSS повинно формувати біометричний зразок та ідентифікувати особистість людини за тривимірною біометричною сигнатурою лиця особи (3D-метод) на відстані до 100 метрів.

Головним підрядником DHS є фірма військово-промислового комплексу США «Electronic Warfare Associates», яка розташована у штаті Кентуккі. І хоча терміни завершення розробки, які зазначені у контракті (листопад 2012 року), не були виконані, відомо, що роботи з доведення системи BOSS до потрібних кондицій і надалі тривають.

Згідно з наявною інформацією, розроблені алгоритми розпізнавання осіб за формою обличчя працюють чудово з світлинами (фотографіями) типу «для документів», однак у реальних умовах відеоспостереження на вулицях і в інших громадських місцях одержання придатних для ідентифікації відеознімків людини, яка не має бажання «співпрацювати», дуже складно.

Але практично всі експерти з біометрії вважають, що подібні системи «прийшли, щоб залишитися». Загалом, стрімкий прогрес подібних технологій очевидний[1].

А які справи застосування засобів зовнішнього контролю (спостереження) в Україні? Відеокамери вже можно побачити у багатьох громадських місцях обласних центрів. Але чи використовуються в українських системах відеоспостереження сучасні досягнення відеоаналітики? Поки що, на жаль, однозначної позитивної відповіді на це питання не має. Хоча концепція Державної цільової правоохоронної програми передбачає впровадження до 2016 року сучасних високотехнологічних програмно-апаратних засобів для моніторингу, фіксації, передачі інформації про стан громадського порядку та забезпечення швидкого реагування на правопорушення. Цей нормативний акт був розроблений МВС на виконання Указу Президента від 8 червня 2012 № 388 «Про рішення Ради національної безпеки і оборони України від 25 травня 2012 року «Про заходи щодо посилення боротьби з тероризмом в Україні». Прес-служба МВС повідомляла, що під час проведення в Україні фінальної частини чемпіонату Європи 2012 року з футболу системи відеоспостереження, що були встановлені в містах Києві та Донецьку, зарекомендували себе позитивно. Але фінансування з держбюджету на встановлення засобів зовнішнього спостереження на виконання цієї концепції не передбачено. Рекомендовано залучення міжнародної технічної й фінансової допомоги, а також інших джерел, не заборонених законодавством, зокрема за рахунок коштів місцевих бюджетів[2].

Але зважаючи на те, що у розвинутих західних країнах за допомогою сучасних технологій відеоспостереження розкривається значна кількість учинених злочинів у громадських місцях, рано чи пізно у всіх українських містах будуть запроваджені системи відеомоніторингу та відеоконтролю.

---

[1] Технологии биометрической идентификации по лицу могут повысить свою эффективность // DGL.RU. – 2013. – 02 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Правительство утвердило «слежку» за украинцами // Mail.ru. – 2013. – 08 февраля. [Электронный ресурс]. – Режим доступа: http://news.mail.ru/inworld/...

6.7. Біометричні системи захисту інформації від несанкціонованого доступу

Із розвитком комп'ютерних мереж і розширенням сфер автоматизації цінність інформації неухильно зростає. Державні секрети, наукоємні ноу-хау, комерційні, юридичні та лікарські таємниці дедалі частіше довіряють комп'ютеру, який, як правило, підключається до локальної або корпоративної мережі. Популярність глобальної мережі Інтернет, з одного боку, – величезні можливості для електронної комерції, але, з іншого – нагальна потреба в надійних засобах безпеки для захисту корпоративних даних від несанкціонованого доступу ззовні. Нині дедалі більше компаній стикаються з необхідністю запобігати несанкціонованому доступу до своїх систем і можливому витоку даних.

Як показує практика, увага компаній до будь-яких проблем залежить від масштабу загроз та їх впливу на бізнес. Захист персональних даних у цьому плані не є винятком. Загальноприйнято, що чим більше відомостей зберігають і обробляють компанії за допомогою ІТ-технологій, тим вищий рівень ризику, відповідальність і стурбованість менеджменту за збереження даних.

Витоки персональних даних, значна кількість яких зосереджена в інформаційних мережах різних компаній, особливо в установах фінансової сфери, призводять до серйозних фінансових і репутаційних витрат. За даними загальносвітової статистики щодо інцидентів у сфері інформаційної безпеки, приблизно 90% усіх несанкціонованих витоків інформації так чи інакше пов'язано з діями персоналу компаній або установ. Отже, чим більше співробітників володіє доступом до масивів персональних даних, тим вищий ризик витоку[1].

Як свідчить світова практика, практично до кінця 90-х років минулого століття основним засобом персоніфікації користувача у мережі було зазначення його мережевого імені та паролю. В Україні подібний підхід ще й досі широко використовується у багатьох установах та організаціях. Небезпеки, пов'язані з використанням пароля, добре відомі: паролі забувають, зберігають у невідповідному місці, нарешті, їх можно просто вкрасти. Деякі користувачі записують паролі на папері й тримають ці записи безпосередньо на своїх робочих місцях поряд із комп'ютерами. Як свідчить статистика, що ведеться в групах підтримки інформаційних технологій, у багатьох компаніях значна частина дзвінків у цю службу спричинена тим, що клієнти забувають або втрачають паролі доступу.

Відомо, що комп'ютерну систему можна обдурити, увівши вкрадений пароль і логін. Для цього необхідно лише дізнатися про відповідну ідентифікуючу інформацію, якою, з погляду системи безпеки, повинна володіти одна особа. Отже, зловмисник, видаючи себе за співробітника компанії, отримує доступ до всіх ресурсів, які доступні дійсному користувачеві, відповідно до його повноважень і посадових обов'язків. У підсумку можуть статися різні протиправні дії, починаючи від крадіжки інформації та завершуючи виводом із ладу всього інформаційного комплексу відповідної організації або установи.

Розробники старих традиційних пристроїв ідентифікації вже зіткнулися з тим, що стандартні методи організації доступу в інформаційних мережах, які використовувались наприкінці XX століття, здебільшого застаріли. Проблема, зокрема, полягає у тому, що

[1] Ульянов В. Персональные данные на практике остаются беззащитными / В. Ульянов // Cnews.ru. – 2008. – 4 декабря. [Электронный ресурс]. – Режим доступа: http://safe.cnews.ru/reviews/index.shtml?2008/…

методи контролю фізичного доступу до комп'ютерних пристроїв і, відповідно, до інформації з обмеженим доступом, які раніше використовувалися, вже не спроможні забезпечити потрібний рівень захисту. Адже для отримання доступу до сервера зараз зовсім не обов'язково заходити у приміщення, де він знаходиться. Причиною тому є всеосяжна концепція розподілених обчислень, яка використовує технологію клієнт-сервер та Інтернет. Для нейтралізації сучасних проблем крадіжок конфіденційної інформації потрібні такі методи, що використовують найсучасніші досягнення захисту інформації від несанкціонованого доступу безпосередньо у різних комп'ютерних мережах.

Для виходу з ситуації, що виникла, для організації будь-якого доступу до різних інформаційно-комунікаційних мереж і систем необхідно застосовувати методи ідентифікації, які не могли б спрацьовувати без їх носія. Цій вимозі сповна відповідають біометричні характеристики організму людини, які є суто індивідуальними та неповторними. Сучасні біометричні технології дозволяють ідентифікувати особу за фізіологічними і психологічними ознаками.

Головна мета біометричної ідентифікації або аутентифікації полягає у створенні такої системи реєстрації, яка досить рідко відмовляла б у доступі легітимним користувачам і водночас максимально виключала б можливість несанкціонованого входу до комп'ютерних сховищ інформації (баз даних). Порівняно з доступом на основі використання паролів і карток біометричні системи забезпечують набагато надійніший захист: адже складові власного тіла не можна ані забути, ані втратити. Біометричне розпізнавання індивідуума і надання йому права доступу ґрунтується на порівнянні фізіологічних або психологічних особливостей будь-якої особистості з її характеристиками, які були відповідним чином отримані та внесені до бази даних системи[1].

На думку експертів, застосування біометричної ідентифікації забезпечує ефективне та надійне управління організацією доступу співробітників до комп'ютерів, ресурсів корпоративної мережі та інформації, що обробляється за допомогою прикладних програм. Заміна ненадійних паролів безпечною і зручною біометричною ідентифікацією не тільки полегшує роботу персоналу, але й істотно знижує витрати на адміністрування й рівень IT-ризиків.

2008 року компанія «Perimetrix» здійснила дослідження щодо стану інформаційної безпеки (ІБ) у Російській Федерації. Результати цих досліджень є цікавими й для України, оскільки українські компанії, як правило, подібні до російських, а витоки російської та української політики щодо безпеки має одне коріння, хоча і є деякі відмінності, що переважно спричинені відставанням українського законодавства від російського у сфері законодавчої бази про захист персональних даних і станом рівня комп'ютеризації та інформатизації державних і приватних комерційних структур. Оскільки авторами посібника в літературі та ЗМІ майже не знайдено відомостей про загальний стан інформаційної безпеки в Україні, то цифрові показники стану ІБ в Росії за 2008 рік зі значною ймовірністю у загальних рисах відображають і рівень інформаційної безпеки і в Україні.

Згідно з даними компанії «Perimetrix» за 2008 рік, більша частина російських компаній (52%) обробляють у своїх локальних мережах понад 10 тис. записів персональних даних. Приблизно кожна шоста російська компанія (15,3%) обробляє персональні дані понад 1 млн чоловік. Це і державні установи, і великі комерційні компанії. Якщо таке підприємство представлене на фондових ринках, а відомості про витік інформації з нього стануть відомими широкому загалу учасників торгів, акції такої фірми миттєво

[1] Борзенко А. Биометрические технологии / А. Борзенко // Bytemag.ru. – 2001. – № 10. [Электронный ресурс]. – Режим доступа: http://bytemag.ru/...

втратять у ціні: інвестори не стануть чекати завершення розслідування інциденту. Цілком очевидно, що у разі несприятливого результату втрати обчислюються не тільки сумою в грошовому еквіваленті з великою кількістю нулів, – завдається шкода і репутації компанії. Відповідно до теорії, для недопущення витоку інформації доступ до масивів персональних даних варто було б обмежити в основному працівниками служби безпеки установи. Проте здебільшого доступом до конфіденційної інформації володіє значна кількість працівників (57,6%) служб інформаційно-телекомунікаційної (IT) підтримки. Це пов'язано з особливостями як російського, так і українського бізнесу, в якому поки що сфери відповідальності персоналу IT і ІБ підрозділів дуже часто не розмежовані.

Крім того, загрозу витоку даним несуть топ-менеджери (21,9%) й аналітики (18,5%). Перша група, що характеризується переважно значним рівнем недбалості, досить часто отримує у повному обсязі доступ до корпоративних ресурсів, який для уникнення появи конфліктних ситуацій їм надають співробітники, що відповідають за IT-обслуговування. Другій групі, як правило, надається постійний невиправдано високий рівень доступу до всіх корпоративних даних. Але на практиці для виконання значної кількості завдань аналітикам цілком достатньо узагальнювальних і знеособлених статистичних відомостей, а не користування масивами реальних персональних даних.

Необхідно виокремити співробітників кол-центрів і служб технічної підтримки. Ймовірність витоку даних через їх працівників надто висока, оскільки працівники цих підрозділів зазвичай не відзначаються високою лояльністю до організації-працедавця і не завжди достатньо компетентні у сфері безпеки.

Отже, можна зробити висновок, що захищеність персональних даних, а також інформації, що становить комерційну таємницю, у більшості російських та українських організаціях і компаніях все ще перебуває на недостатньому рівні. Загалом дослідження компанії «Perimetrix» показало надзвичайну важливість і зростаючу актуальність проблеми захисту персональних даних[1].

Сьогодні російські й українські компанії обробляють велику кількість персональної та конфіденційної інформації. І, недивлячись на ухвалення законів про захист персональної інформації і в Росії, і в Україні, продовжують існувати випадки неналежної організації доступу до неї, що призводить до існування досить високих ризиків можливості витоку.

Необхідно акцентувати, що біометричні системи організації доступу до масивів даних в основному гарантують захист від інсайдерського витоку інформації (інсайдерами називають тих співробітників, які крадуть і «зливають» конфіденційні відомості, несанкціоновано модифікують і знищують інформацію чи блокують доступ до неї, запускають в мережу різні «троянські» та «черв'ячні» програми, виконують низку інших аналогічних дій, що інколи мають катастрофічні наслідки для власника інформаційної мережі або банку даних).

Фактично інсайдером можна назвати Едварда Сноудена, який використовуючи паролі та логіни своїх колег отримав доступ до інформації, до якої він не мав права доступу за своїми фукціональними обов'язками. Так Е. Сноуден у 2013 році за допомогою журналістів «Washington Post» і «Guardian» розголосив надсекретні відомості щодо програми «Prism», яка використовується в інтересах Агентства національної безпеки (АНБ) /National Security Agency – (NSA)/ і FBI (ФБР).

[1] Ульянов В. Персональные данные на практике остаются беззащитными / В. Ульянов // Cnews.ru – 2008. – 4 декабря. [Электронный ресурс]. – Режим доступа: http://safe.cnews.ru/reviews/index...

Програма «Prism», яка функціонує з 2007 року, є першою у світі розробкою, що використовується для аналізу інформації в глобальних соціальних мережах «Google» і «Facebook». Таємно затверджена судом США програма «Prism» також орієнтована на перехоплення закордонного трафіку зв'язку, що здебільшого проходить через сервери США, навіть за умови відправлення з одного закордонного місця в інше, яке розташоване за межами території США.

Дії суперпрограми «Prism» ґрунтуються на Законі про контроль над діяльністю іноземних розвідок (FISA) й Акті про захист Америки (Protect America Act /PAA/), які дозволяють здійснювати стеження за громадянами іноземних держав за межами США без санкції суду. Щорічне утримання системи «Prism» становить приблизно 20 млрд доларів[1]. Для захисту від перехоплення цією суперпрограмою відомостей необхідно застосовувати вельми потужний криптографічний захист даних.

Основні аспекти біометричних видів захисту інформації і баз даних більш детальніше будуть розглянуті у розділі 14 «Біометричний захист інформації та контроль за доступом у корпоративних мережах до баз даних і електронних пристроїв зберігання даних».

6.8. Застосування біометрії в банках та інших фінансових установах

Банки, кредитні й інші фінансові організації повинні бути для клієнтів символом надійності та довіри. Щоб виправдати ці очікування, фінансові інститути особливу увагу приділяють практичному використанню різних інноваційних досягнень. Коли мовиться про інформаційно-телекомунікаційні рішення у сфері безпеки платежів, зазвичай відразу ж згадують за такі технології, як захищені канали передачі даних, генератори одноразових паролів, різноманітні токени тощо. Але як показує світова практика, нині біометричні технології найактивніше частково вже впроваджені та продовжують запроваджуватися у фінансову сферу, причому в усіх частинах світу.

Із 2005 року, в діяльність різних світових фінансових установ починають втілювати останні досягнення в галузі біометрії для ідентифікації користувачів і персоналу, причому сфера використання технологій біометрики безперервно розширюється, охоплюючи все нові напрями діяльності як офісних працівників, так і в сфері обслуговування клієнтів.

Основні завдання, що вирішуються фінансовими інститутами за допомогою біометричних технологій:

– надійна ідентифікація користувачів різних фінансових сервісів, зокрема онлайнових та мобільних (переважає ідентифікація за відбитками пальців, наразі зростає застосування технологій розпізнавання за малюнком вен на долоні або пальці (в основному в Азії), набуває дедалі більшого поширення ідентифікаційні технології за голосом клієнтів, які звертаються в кол-центри банківських установ);

[1] Prism – глобальная машина наблюдения: как США уничтожают свободу в мире // The Guardian,The Washington Post. – 2013. – 7 и 6 июня. [Электронный ресурс]. – Режим доступа: http://regnum.ru/news/fd-abroad/ukraina/1669976.html

– запобігання шахрайствам і махінаціям із кредитними та дебетовими картками та іншими платіжними інструментами (заміна PIN-коду на розпізнавання за біометричними параметрами, які, як відомо, неможливо викрасти, «підглянути» та дуже складно підробити);

– підвищення якості обслуговування та його комфорту (біометричні банкомати, програми супроводу постійних користувачів або відвідувачів, біометрична ідентифікація користувачів систем «електронної черги»);

– контроль фізичного доступу в будівлі та приміщення банків (до депозитарних скриньок, сейфів і сховищ із можливістю біометричної ідентифікації і співробітника банку, і клієнта-користувача скриньки);

– облік робочого часу співробітників фінансових установ (як правило, інтегрується з контролем фізичного доступу);

– захист інформаційних систем і ресурсів банківських та інших кредитних організацій[1].

За даними порталу «BIOMETRICS.RU», запровадження біометричних систем платежів активно почалося в Європі та США ще на початку 2000-х років. А 2008 року дослідницька компанія «TNS» підготувала доповідь «Нове майбутнє магазину», у якій зазначалося, що 6 із 10 респондентів у світі вірять, що в 2015 році можна буде купувати за допомогою відбитків пальців.

Біометрична система оплати подобалася 41% споживачам, зокрема у Китаї цей відсоток становив 60%, а в Німеччині – 24%[2].

Компанія «Gartner Research» у вересні 2012 р. випустила черговий огляд, у якому досліджено 1900 різних технологій, які застосовуються в 92 сферах людської діяльності, на предмет їх відповідності знаменитому так званому «циклу зрілості» (hype cycle). На думку аналітиків «Gartner», впродовж двох–п’яти років біометричні технології одержать ще більше поширення серед споживачів.

Серед інших експерти «Gartner» виокремили таку перевагу біометричних технологій, як здатність сприяти формуванню «фактично безготівкового світу», в якому будуть переважати електронні транзакції, а не оплата кешем. Серед інших технологій, які допомагають позбутися наявності готівкового обороту, в огляді також згадані комунікації близького поля (Near Field Communication /NFC/) і віддалене управління параметрами мобільних пристроїв, які перебувають у зоні покриття мережі стільникового зв’язку (mobile over the air /OTA/)[3].

Досвід закордонних і вітчизняних фінансових структур, зокрема банківських, дозволяє констатувати, що біометричні технології успішно вирішують і забезпечують головні вимоги до систем ідентифікації та аутентифікації – надійність, безпеку, точність, високу швидкість і зручність для користувачів.

Біометричний ідентифікатор не можна забути або «позичити», а пред’явити легко, швидко та зручно. Під час реєстрації індивідуума створюється цифрова модель (шаблон) його ідентифікатора, що зберігається у відповідній базі даних; у разі наступних звертань до інформаційної системи знову відтворюється шаблон, який порівнюється з вже існуючим взірцем.

---

[1] Банки и финансовые учреждения // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/markets/banking.php...

[2] Биометрическая платежная система начала действовать в Тюмени // Вслух.Ру. – 2012. – 21 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Gartner предрекает биометрическим технологиям светлое будущее // BIOMETRICS.Ru. – 2012. – 21 сентября.

Причому функція отримання шаблону «працює» тільки в одну сторону: відновити з шаблону реальний відбиток пальця неможливо (для баз даних фінансових структур)[1].

Нині велика кількість транзакцій – обмін валют, операції купівлі та продажу, оплата праці й інші реалізуються в комп'ютерних онлайнових системах у вигляді безготівкових розрахунків. Але виникає питання: чи безпечні такі транзакції і чим ризикують користувачі, звертаючись до них?

Такий спосіб безгрошових операцій дуже зручний. Але з проникненням комп'ютерних і веб-технологій у фінансову сферу з'явилися ризики, які пов'язані з можливістю «крадіжки особистості» та всіх безготівкових коштів із рахунків, так звана кіберзлочинність.

Наведемо лише один приклад. У середині 2012 року поки що найбільшу в світі операцію проти кіберзлочинності провели американські спецслужби, що заарештували 24 людини в США та восьми інших країнах. Заарештовані звинувачуються у використанні Інтернету для махінацій із кредитками, банківськими рахунками й особистою інформацією сотень тисяч людей в усьому світі.

Кіберзлочинці викрадали дані не тільки за допомогою шпигунських комп'ютерних програм із персональних комп'ютерів, але й зламували бази даних банків, готелів, торгівельних фірм і перепродували викрадені відомості через мережу.

У Сполучених Штатах Америки було заарештовано 11 осіб, в інших країнах – 13-ть. Крім США, арешти були проведені у Великобританії (шестеро), Боснії (двоє), Болгарії (один), Норвегії (один) і Німеччині (один). Ще двоє були затримані також в Італії й Японії за тимчасовими ордерами. Допити підозрюваних проводилися ще в Австралії, Канаді, Данії та Македонії[2].

Важливість застосування біометрії у діяльності фінансових установ підкреслює той факт, що в 2008 році Міжнародна організація зі стандартизації (International Organization for Standardization – ISO /ICO/) оголосила про випуск спеціального стандарту ISO 19092:2008, що регламентує застосування біометричних технологій у фінансовій сфері та, зокрема, в питаннях забезпечення безпеки під час верифікації й ідентифікації користувачів електронних платежів.

Як відзначають експерти ISO, розвиток комп'ютерно-телекомунікаційних технологій спричинив революцію в системах електронних платежів і зумовив стрімке зростання їх обсягу. Своєю чергою, перехід на електронні платежі дозволяє фінансовій індустрії істотно знизити витрати і суттєво підвищити ефективність своєї діяльності[3].

За оцінкою журналу «Американський економічний огляд», долар, який вкладається в біометричні технології, приносить банкам прибуток у 2,34 долара[4].

За останніми даними, в світі щодня за допомогою електронних платежів скоюються транзакції на мільярди доларів, і, зрозуміло, фінансове співтовариство

---

[1] Почему биометрические решения становятся всё более востребованными в банках? // BioLink. – 2012. – 27 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Операция против киберпреступности на 4-х континентах // Экономические известия. – 2012. – 27 июня. [Электронный ресурс]. – Режим доступа: http://news.eizvestia.com/news_incidents/full/...

[3] Новый стандарт по использованию биометрии в финансовой сфере // BIOMETRICS.Ru. – 2008. – 12 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Биометрические технологии повысили ответственность получателей кредитов // BIOMETRICS.Ru». – 2012. – 16 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/…

та користувачі таких платежів дуже зацікавлені в мінімізації ризиків, які пов'язані з навмисним або випадковим спотворенням оброблюваної інформації, її підміною або знищенням.

Одна з головних нагальних потреб – формування надійної системи аутентифікації та ідентифікації, в зв'язку з чим експерти ISO відзначають важливу роль і подальші значні перспективи біометричних технологій.

У стандарті ISO 19092:2008 описується архітектура застосування біометричних технологій та конкретизуються вимоги безпеки під час їх використання. Стандарт перераховує також основні завдання інтеграції біометричних технологій та електронних платежів і містить рекомендації для практичної реалізації цього процесу в діяльності фінансових і кредитних організацій.

Застосування біометрики для аутентифікації співробітників цих організацій та їх клієнтів розглядається в двох аспектах. Перший із них стосується верифікації користувача (порівняння в режимі «один до одного» з підтвердженням особистості користувача, що надав свої реквізити). Другий аспект зачіпає ідентифікацію користувачів у режимі «один до багатьох», і тут аналізуються та вирішуються такі питання:

– додання юридичної сили реквізитам користувача, які реєструються для його подальшої аутентифікації, у контексті мінімізації існуючих ризиків;

– управління біометричним доступом до інформації і життєвим циклом відповідного облікового запису конкретної фізичної особи на етапах її реєстрації як користувача, збереження відомостей про її повноваження та подальшого проведення операцій передачі, обробки, верифікації та ідентифікації, а у разі завершення клієнтських повноважень – скерування на архівацію або видалення його облікового запису;

– застосування біометрії для розмежування доступу до інформації й управління фізичним доступом;

– застосування технологій інтелектуального відеоспостереження для захисту фінансових організацій і їх клієнтів;

– забезпечення безпеки устаткування, яке використовується для обробки біометричних даних користувача на всіх етапах життєвого циклу його облікового запису.

На думку фахівців, створення та впровадження у діяльність світової фінансової спільноти стандарту ISO 19092:2008 можна розглядати як наступний, але досить важливий крок на шляху розробки і створення нового покоління більш захищених і надійних електронних фінансових транзакцій, на які існує значний попит у нашу еру загальної інформатизації[1].

Використання біометричних ідентифікаторів забезпечує високий рівень імовірності авторизації користувача у банківській інформаційній системі, а у разі виникнення інцидентів набагато легше проводити розслідування, причому висновки яких будуть юридично значимі. Інсайдерські загрози та питання мінімізації можливості таких ризиків традиційно актуальні для керівника служби безпеки будь-якого банку, тому що несанкціонований доступ до конфіденційних ресурсів може призвести до колосальних втрат. Найефективнішим рішенням цієї проблеми також є запровадження системи біометричної ідентифікації співробітників.

Наведемо низку цікавих даних щодо втрат фінансових структур у другій половині першого десятиріччя нового тисячоліття, яким могли б запобігти біометричні технології:

[1] Новый стандарт по использованию биометрии в финансовой сфере // BIOMETRICS.Ru. – 2008. – 12 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

– 929 млн доларів втратили американці через потрапляння паролів платіжних карт до третіх осіб;

– 5 млрд євро – збиток, завданий банку «Societe Generale» його менеджером Жеромом Керв'єлем, який використовував у своїх махінаціях паролі колег;

– 90 млн євро – сума, яку намагався вкрасти в банку «HSBC» Джагміт Чанна за допомогою викрадених паролів[1];

– 53 мільйони злотих на рік втрачає Союз Польських банків через підробку кредитних карт і крадіжок із банківських рахунків[2].

За даними соціологічного дослідження компанії «Unisys», у 2010 році 68% клієнтів у світі хотіли, щоб банки, платіжні системи та державні органи для ідентифікації використовували біометрію замість паролів і карт[3].

«Серцем» будь-якого банку є його корпоративна мережа, яка повинна забезпечувати надійну, безпечну і зручну ідентифікацію користувачів. Разом із масовим переходом до верифікації та ідентифікації користувачів за їх унікальними біометричними параметрами відбуваються не менш актуальні для банків завдання надійного розмежування фізичного доступу в будівлі та приміщення.

Організація проходу та руху співробітників і відвідувачів, додатковий контроль за доступом до сховищ, серверних кімнат, депозитних скриньок, формування відповідних графіків і режимів доступу, контроль за їх дотриманням, інтеграція систем розмежування доступу й обліку робочого часу – всі ці операції здебільшого проводяться з використанням біометричних технологій.

Значна кількість компаній-розробників програмно-апаратних комплексів зробили акцент на розробку алгоритмів і камер для тривимірного (3-D) або комбінованого (2-D + 3-D) розпізнавання обличчя. Технологічні розробки на базі цих методів дозволяють автоматично фіксувати пересування людей, які отримали у встановленому порядку дозвіл доступу на об'єкт, гарантуючи водночас достовірність розпізнавання індивідуумів.

Використання біометричних технологій збільшує ступінь захисту «карткових» турнікетів, зокрема забезпечує надійний захист від підробки, використання викрадених або загублених смарт-карток, а також від передачі їх іншим особам (для отримання доступу недостатньо просто пред'явити картку, необхідно підтвердити достовірність особистості пред'явника його біометричними даними)[4].

Технології біометричної ідентифікації починають активніше використовувати дедалі більше закордонних банків, зокрема російський Ощадбанк, Народний банк Казахстану, ING та інші. Але ще багато банківських установ на теренах СНД доволі скептично ставляться до будь-яких інновацій і змін. На жаль, в Росії (так само і в Україні – *авт*.) досить часто все відбувається за принципом «доки грім не вдарить, мужик не перехреститься». Але, зважаючи на обіг коштів великого банку, «грім» може обійтися критично дорого[5].

---

[1] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрический банкомат появился в Варшаве // Вести ФМ. – 2013. – 27 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] День банковской безопасности в Казахстане: биометрия выходит в лидеры. – 2007. – 26 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[5] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Відповідно до досліджень, проведених американським інститутом «Ponemon» у кооперації з британським центром вивчення громадської думки «Ipsos/MORI», наприкінці 2006 – початку 2007 років, 90% споживачів у Великобританії і приблизно 69% у США однозначно висловилися за розширення сфер використання біометрії. Пріоритетними сферами застосування були визначені діяльність банків, платіжних систем, провайдерів медичних послуг і використання для потреб державних органів.

Ці дані збігаються з тенденціями опитування, яке у другій половині 2006 року провела маркетингова інформаційна група «TNS» і в якому 64% від кількості опитаних позитивно сприймали розміщення біометричної інформації на кредитних картах, а 62% схвально відгукнулися про включення такої інформації до складу відомостей, які розміщені на дебетових картках[1].

Понад дві третини учасників (67%) проведеного у 2008 році фірмою «Unisys» опитування заявили про те, що довіряють дактилоскопічним сканерам, які використовуються банками, урядовими та приватними організаціями у всьому світі. Загалом біометричні рішення є найбільш популярними у жителів Малайзії, Австралії та Великобританії. Опитування споживачів здійснюється паралельно з традиційним дослідженням «Unisys Security Index».

Проведені анкетування довели, що махінації з банківськими картками дуже сильно хвилюють клієнтів банків у всьому світі. Громадяни одинадцяти з тринадцяти країн, в яких проводилося анкетування, назвали шахрайські дії за допомогою банківських карток предметом їх найбільшого занепокоєння. У десяти країнах респонденти вважали, що крадіжка особистих даних є загрозою номер один для них.

Підсумком проведеного опитування стало встановлення закономірності, яка виявилася у тому, що запровадження біометричних методів ідентифікації особистості у діяльність різних комерційних структур відбувається насамперед у тих країнах, де ці технології вже широко використовуються урядовими організаціями[2].

Головною причиною прихильного ставлення людей до впровадження біометричних технологій є прагнення до комфорту. Вирішальним цей чинник визнали 83% респондентів з усієї кількості опитаних.

Використання біометричних рішень під час проведення операцій у банкоматах найбільше поширилось у країнах Азії. Наприклад, Національний банк Оману придбав ридери смарт-карток із сканерами відбитків пальців, що дозволило істотно спростити обслуговування клієнтів, передусім неписьменних, завдяки чому позбулися від черг і наявності значного штату консультантів. Замість введення PIN-коду оманським кардхолдерам тепер досить прикласти палець.

Аналогічні проекти реалізовані або реалізовуються, відповідно, у Пакистані та Індії. Індійський резервний банк розпочав реалізацію на базі біометрії спецпрограми «Залучайся до фінансів» для клієнтів із невеликим рівнем доходу, жителів віддалених сільських районів і соціально незахищених верств населення, більшість із яких не вміють читати і писати. Біометрична можливість підтвердження особистості їм стала в нагоді під час виконання різних фінансових транзакцій[3].

---

[1] Лукашов И. Биометрия выдерживает непрерывный экзамен / И. Лукашов // Secnews.ru. – 2007. – 21 августа. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/ reviews/free/security2007/...

[2] Потребители доверяют сканерам отпечатков пальцев // Компьюлента. – 2008. – 16 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp?group…

[3] Насакин Р. В. Одно касание / Р. В. Насакин // Computerra.ru. – 2007. – 25 июля. [Электронный ресурс]. – Режим доступа: http://www.computerra.ru/focus/...

Наведемо результати низки оглядів і досліджень за 2013 рік щодо довіри користувачів до використання біометричних технологій у банківській сфері та оплати товарів і послуг.

Згідно з опитуванням, проведеним компанією «WorldPay» у червні 2013 року, про готовність розплачуватися за товари й послуги, скануючи біометричні ідентифікатори, заявив кожний другий учасник опитування. За популярністю біометрія суттєво випередила всі інші технології, наприклад, використовувати для розрахунків смартфони готові лише 30% респондентів, для 25% найбільш привабливі онлайнові гаманці, 23% опитуваних прагнули б розплачуватися за допомогою СМС. Найнижчий рейтинг мав спосіб оплати через соціальні мережі – його вважали оптимальним лише 12% респондентів[1].

У квітні 2013 року фірма «Cisco» опублікувала результати опитування споживачів фінансових послуг і професіоналів банківської індустрії, під час якого вивчалося, зокрема ставлення респондентів до застосування біометричних технологій.

Найбільшу стурбованість у споживачів фінансових послуг викликає невирішеність питань захисту їх персональних даних: найважливішими назвали ці питання 83% респондентів. Особливо привабливими клієнти банків вважають біометричні технології. У глобальному масштабі більш 60% опитаних готові надати банкам відомості про свої біометричні ідентифікатори. У США частка прихильників біометрії становить 53%, а найбільше скептично налаштованими виявилися мешканці Японії. У цій країні застосовувати біометричні технології в процесі банківського обслуговування готові лише 33% клієнтів кредитних організацій[2].

Наведемо також підсумки опитувань, які були проведені різними компаніями у 2012–2011 роках.

У четвертому кварталі 2012 року компанія «Javelin Strategy & Research» опублікувала результати проведеного опитування, під час якого вивчалося ставлення клієнтів кредитних організацій до використання біометричних технологій для захисту їх рахунків. Опитування проводилося і серед корпоративних клієнтів банків, і серед фізичних осіб – клієнтів.

70% корпоративних клієнтів кредитних організацій підтвердили свій інтерес до застосування у технологіях безпеки досягнень біометрії. Що ж стосується фізичних клієнтів, то опитування виявило таку закономірність: чим більш «просунутим» у технічному плані є користувач, тем прихильніше ставиться він до біометрії. Забезпечувати безпеку своїх транзакцій за допомогою біометричних технологій загалом та біометричними смарт-картами зокрема бажали б 48% користувачів онлайнового банкінга і 54% тих, хто звертається до послуг мобільного банкінга. Найбільш популярною серед учасників опитування виявилася біометрична ідентифікація за відбитками пальців: її вважають найліпшою для впровадження в банківські системи 35% респондентів. Наче утішаючи розробників інших біометричних технологій, аналітики «Javelin Strategy & Research» вказали на те, що у методів розпізнавання користувачів за їхнім обличчям та голосом у банківській сфері існують довгострокові перспективи[3].

---

[1] Покупатели предпочитают биометрические платежи // BIOMETRICS.Ru. – 2013. – 20 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Клиенты банков выступают за расширение применения биометрических технологий // BIOMETRICS.Ru. – 2013. – 24 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Растет популярность биометрических технологий среди клиентов банков // BIOMETRICS.Ru. – 2012. – 30 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

За оцінкою агентства «Frost & Sullivan», на кінець 2012 року 88,7% продажів біометричних засобів захисту інформації у фінансовому секторі припадало на частку рішень, які використовують технології ідентифікації за відбитками пальців[1].

Наприкінці 2012 року фахівці двох іранських вузів (Тегеранського університету та Університету Ходжі Насира) опублікували результати дослідження, під час якого була проаналізована поширеність біометричних технологій у банках. Автори дослідження з'ясували, що найактивніше до можливостей біометрії звертаються азіатські банки.

Масштаби нового дослідження викликають повагу: його автори загалом вивчили діяльність 121 кредитної організації. Найпопулярнішою біометричною технологією в банках виявилася ідентифікація за відбитками пальців: вона використовувалась у 48% банківських біометричних проектах. Далі з істотним відставанням розташувались технології розпізнавання за малюнком вен на пальці (12,4%), голосом (11,6%), малюнком вен на долоні (9,1%) і райдужною оболонкою очей (7,4%).

Що ж стосується географічних аспектів, то 52% біометричних упроваджень припадали на азійські банки, 32% – на кредитні організації країн Північної та Південної Америки, 9% – на банки Старого Світу.

Найбільшим напрямом застосування розглянутих технологій у кредитних організаціях виявилася біометрична ідентифікація користувачів банкоматів (45% від загальної кількості втілених проектів). Майже кожний четвертий проект пов'язаний із впровадженням у банках біометричних систем контролю доступу; кожна десята кредитна організація з проаналізованих іранськими фахівцями пропонувала проходити біометричну ідентифікацію користувачам інтернет-банкінгу.

Не залишили поза увагою автори дослідження й тему застосування біометрії в іранських банках. 2012 року біометричні рішення були втілені в 21-у кредитну організацію цієї країни, причому більшість рішень стосувалось запроваджень біометричних систем обліку робочого часу[2].

У листопаді 2011 року компанія «Unisys» опублікувала підсумки дослідження «Unisys Security Index», під час якого було опитано понад 1000 американців для з'ясування погляду споживачів на низку проблем безпеки.

Дослідження вказало, що більша частина опитаних американців готова надавати свої біометричні дані, щоб захистити особисту інформацію. Готовність надавати ці дані під час проведення контролю в аеропортах підтримало 59,6% опитуваних, під час проведення фінансових угод із банківськими установами – 56,9% і під час одержання державних виплат й інших послуг (53,0%)[3].

Банк «ANZ», який діє в Австралії і в Новій Зеландії, повідомив про намір запровадити технології біометричної ідентифікації для обслуговування клієнтів. На замовлення «ANZ» було проведено спеціальне соціологічне дослідження серед жителів п'ятого континенту. 75% учасників цього дослідження повідомили, що «будуть щасливі», якщо замість введення незручних і небезпечних PIN-кодів у них з'явиться можливість сканувати відбитки пальців для підтвердження операцій із платіжними картами.

---

[1] «Спецсетьстройбанк» защитил корпоративные информационные ресурсы с помощью биометрических решений // BioLink. – 2012. – 20 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Новое исследование распространенности биометрических технологий в банках // BIOMETRICS.Ru. – 2012. – 19 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Американцы стали еще больше доверять биометрическим технологиям // Xakep.ru. – 2011. – 7 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

67% респондентів не заперечували щодо застосування біометричної ідентифікації за райдужною оболонкою очей[1].

У Франції компанія «Wincor Nixdorf» опублікувала результати опитування 1008 французьких споживачів, під час якого вивчалося ставлення до нових інформаційних технологій (зокрема і біометричних). 69% респондентів заявили, що під час здійснення захищених транзакцій у пунктах оплати платежів вони віддали б перевагу ідентифікації за відбитками пальців, а не PIN-коду.

Зазначимо, що французи так позитивно сприймають не всі інновації. Останнім часом у Франції намагалися поширити технології «комунікацій близького поля» (near field communication /NFC/), однак лише 28% респондентів надали б згоду на підключення своїх мобільних телефонів до функції розрахунків за допомогою NFC[2].

Є цікавими підсумки проведеного у 2012–2013 роках у Франції експерименту щодо застосування біометричних технологій у роздрібній торгівлі. В експерименті брали участь чотири банки («Banque Accord», «BNP Paribas», «Crédit Agricole» і «Crédit Mutuel Arkéa») та дві великі торгівельні мережі («Auchan» і «Leroy Merlin»).

Участь в експерименті взяли понад 900 осіб. Усі вони під час оплати покупок на касі банківськими картками замість PIN-кодів пред'являли: відбиток пальця, який пройшов процедуру попередньої реєстрації (в Ангулемі, департамент Шаранта) або після відповідної реєстрації малюнка вен на пальці (Вільньов-Д'аск, департамент Нор).

Учасниками експерименту було вчинено майже п'ять тисяч біометричних транзакцій, а середній розмір кожної з них становив 58,6 євро, що на 15% більше, ніж під час оплати покупок звичайними банківськими картками.

94% учасників експерименту підтвердили, що вони готові й надалі користуватися біометричними технологіями під час оплати покупок у магазинах. 74% покупців вважали біометричні технології сучасними; 71% учасників експерименту визнали застосування біометрії інновацією; щодо безпеки та зручності біометричних транзакцій висловились 61% і 60% покупців відповідно[3].

Виокремимо повідомлення щодо використання технологій біометричної ідентифікації за голосом у фінансових організаціях.

Фахівці компанії «Opus Research» у своєму огляді зазначали, що використання ідентифікації за голосом не тільки підвищує рівень безпеки банківських систем, але й знижує вартість процедури розпізнавання їх користувачів. За оцінкою авторів огляду, на кінець 2012 року банки налічували приблизно п'ять мільйонів користувачів голосових біометричних систем, а до 2015 року цей показник може сягти 90 млн. Як вважають експерти, головна перевага біометричних технологій полягає в їхній здатності зменшувати час транзакцій і одночасно бути ефективним засобом протидії шахрайству, відмиванню грошей та спробам розкрадання персональних даних[4].

---

[1] Австралийцы активно поддерживают применение биометрических технологий в банковской сфере // BIOMETRICS.Ru. – 2012. – 8 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Французы стали еще больше доверять биометрическим технологиям // BIOMETRICS.Ru. – 2012. – 13 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические технологии в ритейле: итоги французского эксперимента // BIOMETRICS.Ru. – 2013. – 31 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Технологии биометрической идентификации по голосу в финансовых институтах: новые перспективы // BIOMETRICS.Ru. – 2012. – 9 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Спеціалісти «Valid Soft» провели дослідження «Voice Biometrics Authentication Best Practices: Overcoming Obstacles to Adoption» («Кращі приклади застосування голосової біометрії для встановлення особистості: долаючи перешкоди»). Мета дослідження – аналіз поточного стану голосової біометрії на початок 2012 року й оцінка на майбутнє перспектив цього методу.

Автори звіту зазначали, що голосова біометрія може стати частиною багаторівневого процесу розпізнавання для зниження ризиків платіжних онлайн-шахрайств. 2015 року кількість зареєстрованих у фінансових установах голосових «відбитків» сягне понад 25 млн[1].

Як бачимо, у останніх двох прогнозах відрізняється кількість користувачів голосових біометричних систем у 2015 році, але чітко простежується тенденція на зростання застосувань цієї технології.

Наведемо не повний перелік країн і банків, які вже використовують або планують застосовувати біометричні технології у своїй діяльності. Відомо, що 52% біометричних впроваджень припадають на азіатські банки, 32% – на кредитні організації країн Північної та Південної Америки, 9% – на банки Старого Світу.

За алфавітом наведемо низку країн, де банки вже запровадили або впроваджують сучасні технології біометричної ідентифікації (верифікації).

Австралія. Банк «ANZ», який діє в Австралії та Новій Зеландії, повідомив про намір запровадити технології біометричної ідентифікації для обслуговування клієнтів[2].

Аргентина. Банк «Banco Supervielle» є одним із провідних банків Аргентини. Він здійснив біометричну ідентифікацію мільйона пенсіонерів країни. Ідентифікація літніх громадян під час одержання пенсій здійснюється шляхом сканування відбитків пальців у всіх 77 відділеннях «Banco Supervielle». У майбутньому зазначений фінансовий інститут планує провести біометричну ідентифікацію всіх інших своїх клієнтів[3].

Бангладеш. Компанія «Dipon Consultancy Services Ltd» (DCSL). «DCSL» розширює використання біометричних смарт-карт у фінансовому сервісі «Prime Cash». Такими картами планується забезпечити 75% громадян цієї країни, чисельність яких становить 150 млн людей.

За допомогою біометричних смарт-карт користувачі «Prime Cash» можуть швидко здійснювати різні операції: відкривати особові рахунки, оформляти внески та заявки на позики, розплачуватися за раніше виданими кредитами, знімати готівку в банкоматах і переказувати гроші своїм рідним і близьким. На кінець першого півріччя 2013 року майже 200 тисяч бангладешців уже користуються біометричними смарт-картами[4].

Бразилія. «Bradesco Bank» ще у 2010 році обладнав понад півтори тисячі банкоматів сканерами малюнка вен на долоні[5].

---

[1] Новые перспективы голосовой биометрии в финансовой сфере // E-MoneyNews. – 2012. – 15 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Австралийцы активно поддерживают применение биометрических технологий в банковской сфере // BIOMETRICS.Ru. – 2012. – 8 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Аргентинский банк провел биометрическую идентификацию миллиона пенсионеров // BIOMETRICS.Ru. – 2013. – 13 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Биометрические технологии помогут приобщить жителей Бангладеш к финансовым сервисам // BIOMETRICS.Ru. – 2013. – 17 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[5] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

За повідомленням російського біометричного порталу «BIOMETRICS.RU», у 2013 році один із найбільших державних банків Бразилії оголосив про плани встановлення в трьох із половиною тисячах своїх банкоматів сканерів відбитків пальців. Цю роботу буде виконувати бразильське відділення компанії «Diebold», яка поставляє кредитним організаціям обладнання для автоматизації їх діяльності (зокрема й банкомати)[1].

2012 року бразильська компанія «Itautec» оголосила про одержання великого замовлення на оснащення 12 тисяч банкоматів сканерами відбитків пальців. Замовлення надійшло від одного з найбільших комерційних банків, який діє в багатьох країнах Латинської Америки[2].

Діючий у Латинській Америці банк «Banco Azteca» проводить сканування у своїх клієнтів відбитків пальців під час доступу до рахунків, а його інформаційна система щодня здійснює не менш 200 тисяч порівнянь цих ідентифікаторів[3].

Гана. Віце-президент Гани, колишній керівник Банку цієї країни Квесі Аміссах-Артур, оголосив у місцевому парламенті про те, що кредитні організації Гани незабаром почнуть використовувати біометричні технології. Під час свого виступу віце-президент також повідомив, що базою даних, яка була сформована під час біометричної ідентифікації виборців, та, відповідно, їх біометричними ID-картками, має намір скористатися Банк Гани. Доповідач передбачає можливості, що й інші соціальні інститути можуть піти цим шляхом[4].

Індія. В Індії запущений один із наймасштабніших світових проектів «Aadhaar» із присвоєння громадянам унікальних ідентифікаційних номерів на основі сканування їх біометричних параметрів. Відтепер індійці, які зареєструвалися в цьому проекті, за його допомогою зможуть швидше й простіше одержувати виплати від різних державних програм. Зокрема, нововведення стосуватиметься учасників Національної програми стимулювання зайнятості в сільських районах, Суспільної системи розподілу соціальної допомоги серед представників найбідніших верств населення, а також системи грантів на проходження навчання в школах.

Актуальність біометричної ідентифікації учасників цих програм складно переоцінити, тому що більшість жителів Індії не мають будь-яких документів, які б засвідчували їх особистість. А це, своєю чергою, створює умови для махінацій як з боку громадян (повторна реєстрація під іншим прізвищем для одержання ще одного грошового траншу), так і з боку чиновників (привласнення коштів, які випланувались так званим «мертвим душам»). Проходження учасниками згаданих програм біометричної ідентифікації дозволить припинити можливість подібних зловживань і забезпечить дійсну адресність соціальної підтримки[5].

Що ж стосується проекту «Aadhaar» загалом, то планувалось, що до 2014 року ідентифікацію мають пройти 600 млн людей, тобто половина населення Індії.

---

[1] Бразилия: еще одно крупное внедрение биометрических банкоматов // BIOMETRICS.Ru. – 2013. – 26 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] 12 тысяч биометрических банкоматов появятся в Бразилии // BIOMETRICS.Ru. – 2012. – 23 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Банки Ганы станут осуществлять биометрическую идентификацию своих клиентов // BIOMETRICS.Ru. – 2012. – 15 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[5] Крупнейший в мире биометрический проект обрел финансовые функции // BIOMETRICS.Ru. – 2012. – 25 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Нагадаємо, чисельність мешканців країни становить 1,2 млрд осіб і всі вони повинні одержати біометричні посвідчення особистості.

Отже, держава та приватний сектор спільно розбудовують мобільний банкінг. Наслідком цього стало істотне зростання користування банківськими послугами, впорядкування соціальних виплат і підтримка зростання економіки[1].

Резервний банк Індії («Reserve Bank of India» – /RBI/, який виконує функції центрального банку країни) у огляді монетарної політики на кінець 2012 року відзначив необхідність активізувати використання біометричних технологій кредитними організаціями.

Експерти «RBI» запропонували конкретні шляхи інтеграції біометричних технологій у діяльність банків. Найефективнішим способом, як вважаються автори огляду, стане використання можливостей найбільшого у світі біометричного проекту «Aadhaar», у рамках якого індійцям привласнюють унікальні ідентифікаційні номери на основі сканування відбитків їх пальців і райдужної оболонки очей[2].

Платіжна система «Visa» оголосила про початок втілення в Індії нового біометричного проекту «Saral Money». Проект створений для полегшення доступу до сервісів «Visa» десятків мільйонів індійських громадян. Для одержання картки «Visa» досить пред'явити відповідне повідомлення від адміністрації «Aadhaar» і знову відсканувати відбитки пальців. Зробити це буде нескладно, оскільки багато кредитних організацій Індії вже оснащені біометричними банкоматами, в які вбудовані сканерами відбитків пальців.

Після того, як під час автоматичного порівняння підтвердиться збігання цифрових моделей відбитків пальців, які були отримані під час реєстрації в проекті «Saral Money», з моделями цих же ідентифікаторів, що раніше були зареєстровані у базі даних «Aadhaar» для цього індивідуума, його особистість буде вважатися встановленою і ніщо не перешкоджатиме відповідній людині в одержанні картки «Visa».

У рамках біометричного проекту «Saral Money» «Visa» налагодила співпрацю з п'ятьма індійськими кредитними організаціями: «Axis Bank», «HDFC Bank», «ICICI Bank», «Indian Overseas Bank» і «State Bank of India»[3].

«State Bank of India» (SBI), який є найбільшим державним банком Індії за показниками ринкової капіталізації, прибутку та кількості відділень, планує розширити застосування біометричних технологій. Ці технології будуть використовуватися для розмежування доступу співробітників банку до його інформаційних ресурсів.

Біометрична ідентифікація службовців буде здійснюватися за відбитками пальців. Для доступу до центральної банківської інформаційної системи кожному з них потрібно буде відсканувати відбиток пальця, а біометрична система сформує шаблон пред'явленого ідентифікатора та порівняє його з раніше зареєстрованим, якщо шаблони співпадуть, то співробітник зможе ввійти в банківську інформаційну систему й отримати надані йому відповідні повноваження. Сканери відбитків пальців і відповідне програмне

[1] Российских парламентариев заинтересовал индийский опыт использования биометрических технологий // Bankir.ru. – 2011. – 3 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Центральный банк Индии призвал активнее применять биометрические технологии // BIOMETRICS.Ru. – 2012. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Индия: биометрические технологии облегчат доступ к сервисам платежной системы Visa // BIOMETRICS.Ru. – 2012. – 17 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

забезпечення для проведення біометричної ідентифікації буде встановлено у кожному з 21 тисячі відділень SBI[1].

Як повідомила у вересні 2013 року «The Times of India», в Індії всі платіжні термінали та банкомати, що надалі встановлюватимуться, будуть оснащені механізмом біометричної ідентифікації «Aadhaar». Резервний банк Індії пояснив, що готує цю директиву з метою поліпшення безпеки та сприяння фінансової інтеграції з міжнародним ринком.

Індійські банки в 2014 році планують встановити 200 тисяч платіжних терміналів і приблизно 20 тисяч банкоматів, кожний із яких буде оснащений біометричним сканером, причому швидкість передачі біометричних параметрів повинна бути не нижчою стандарту 3g. Усе фінансове навантаження з установлення сканерів і нових ліній передачі даних візьмуть на себе фінансові установи.

Передбачається, що база даних біометричних параметрів буде використовуватися під час відкриття рахунків, прийому внесків і видачі кредитів фізичним особам[2].

Індійський банк «IDBI» відкрив у своєму відділенні в Мумбаї (колишній Бомбей) сейфове сховище, доступ до якого захищає біометрична система. Завдяки використанню біометричних технологій фінансова установа повністю автоматизувала доступ клієнтів до сховища. Сейфове сховище функціонує цілодобово та кожного дня (крім 26 січня, 15 серпня і 2 жовтня, на які в Індії припадають загальнонаціональні свята).

Під час оформлення замовлення на користування банківською коміркою клієнт реєструє свої біометричні ідентифікатори (у випадку «IDBI» – відбитки пальців). За його бажанням цифрова модель зареєстрованих ідентифікаторів може зберігатися або в пам'яті самої біометричної системи, або у чіпі спеціальної картки.

Коли клієнт прагне одержати доступ до сховища та відчинити свою комірку, він знову проходить біометричну ідентифікацію шляхом сканування відбитків пальців. Цифрова модель відсканованого відбитка порівнюється з раніше зареєстрованим, і, якщо вони збіглися, клієнтові надається можливість проходу в сховище.

Річна вартість користування коміркою у сховищі, яке обладнано біометричною системою, залежить від розміру комірки та коливається в межах від 15 до 45 тисяч рупій (від 330 до 990 доларів США)[3].

Іран. В Ірані біометричні рішення використовуються у 21 кредитній організації цієї країни. Більшість використань пов'язане з запровадженням біометричних систем обліку робочого часу[4].

Канада. Канадський кредитний союз «Sunova», відділення якого розташовані у Вінніпезі, у лютому 2011 року застосував біометричну систему контролю за доступом до сейфового сховища. Його клієнти можуть цілодобово користуватися біометричними сейфами, проходячи ідентифікацію за відбитками пальців, причому в сховищі низку послуг їм надає спеціальний робот[5].

---

[1] Крупнейший госбанк Индии расширит применение биометрических технологий // BIOMETRICS.Ru. – 2013. – 27 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Индия: сфера применения биометрических технологий расширится // TAR TASS. – 2013. – 16 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Индийский банк внедрил биометрические технологии // BIOMETRICS.Ru. – 2011. – 27 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Новое исследование распространенности биометрических технологий в банках // BIOMETRICS.Ru. – 2012. – 19 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[5] Индийский банк внедрил биометрические технологии // BIOMETRICS.Ru. – 2011. – 27 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Малаві. У Малаві був проведений цікавий експеримент щодо застосування біометричних технологій у фінансовій сфері. Банки цієї країни зважилися на впровадження досягнень біометрії не випадково. До експерименту підштовхнув той факт, що у жителів цієї південноафриканської держави практично відсутні будь-які документи, що могли б засвідчити особистість громадян (навіть свідоцтва про народження є великою рідкістю, не кажучи вже про паспорти).

Ця обставина досить часто провокує громадян, які бажають одержати кредит, на різні махінації, зокрема на спроби оформити кредити під вигаданим прізвищем, щоб у майбутньому не розплачуватися з банком. Тому біометрична ідентифікація позичальників стала ідеальним рішенням. Малавійські банки вибрали технологію розпізнавання своїх клієнтів за відбитками пальців.

Організатори вказаного експерименту фіксували статистику своєчасності внесення позичальниками-фермерами коштів у рахунок погашення раніше виданих їм кредитів. Учасники експерименту були поділені на дві групи: в одній із них була проведена біометрична ідентифікація позичальників шляхом сканування відбитків їх пальців, а в другій групі робота з позичальниками проводилася за старою схемою. У підсумку 85% позичальників із першої «біометричної» групи повністю та вчасно розплатилися за взяті кредити, тоді як у іншій групі цей показник становив лише 44%, тобто практично виявився майже у два рази нижчим[1].

Нігерія. Голова Центрального банку (ЦБ) Нігерії Санусі Ламідо у серпні 2013 року оголосив, що до 2015 року всі операції, що будуть учинені за допомогою платіжних карт у банкоматах і касових терміналах, повинні супроводжуватися біометричною ідентифікацією користувачів.

Відмова від розрахунків «кешем» – одне з пріоритетних завдань нігерійського ЦБ. Голова цієї фінансової установи вважає, що впровадження системи безготівкових платежів обов'язково повинно супроводжуватися введенням біометричної ідентифікації її користувачів. Це повинно підвищити безпеку нової системи, а у майбутньому суттєво полегшити її застосування та розширення[2].

Нідерланди. Компанія «Albron» запровадила для своїх клієнтів новий біометричний сервіс, який одержав назву «Snel en Simpel Betalen» («Швидкі й прості платежі»). Із другої половини 2012 року клієнти «Albron» можуть не носити з собою готівку, а отримали змогу розплачуватися за спожиті страви у закладах харчування шляхом сканування відбитку пальця або малюнка вен на ньому.

Після біометричної ідентифікації відповідна сума списується з рахунку клієнта, а контролювати стан рахунку користувачі нового сервісу можуть в онлайн режимі або за допомогою щомісячних звітів.

За оцінкою експертів компанії, біометричні платежі здійснюються у два рази швидше, ніж розрахунки з використанням звичайних дебетових і кредитних карт. Водночас безпека платежів гарантується унікальністю біометричних ідентифікаторів і тим фактом, що на відміну від карт ці ідентифікатори клієнтів не можуть бути забутими чи викраденими.

Перед початком масового запровадження новий біометричний проект пройшов тестування за допомогою декількох пілотних проектів, один із яких був успішно здійс-

[1] Биометрические технологии повысили ответственность получателей кредитов // BIOMETRICS.Ru. – 2012. – 16 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] К 2015 году платежные системы в Нигерии станут биометрическими // BIOMETRICS.Ru. – 2013. – 23 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

нений у штаб-квартирі самої компанії «Albron». Загальна чисельність її персоналу становить шість тисяч людей, а кількість центрів обслуговування – одну тисячу одиниць. Сервісом «Albron» почали користуватися державні структури, комерційні фірми, установи охорони здоров'я, готелі, а також організатори численних заходів і прийомів[1].

Польща. Відомий польський кооперативний банк «BPS SA» ще у 2010 році першим у Європі запровадив ідентифікацію власників карток за малюнком вен на пальці[2].

Польський банк «BPH», який входить у групу «GE Capital» і є однієї з найбільших кредитних організацій країни, оголосив про плани широкомасштабного запровадження біометричних технологій. Починаючи з вересня 2012 року всі 287 відділень «BPH» у Польщі та, відповідно, банкомати в них будуть оснащатися сканерами малюнка вен. Загалом банк планує придбати 1800 таких сканерів[3].

Діючий на півдні Польщі «Підкарпатський кооперативний банк», починаючи з кінця 2011 року, почав оснащувати всі 65 своїх банкоматів системами біометричної ідентифікації. Першими нові технології випробували мешканці міста Санок. Ідентифікація клієнтів банку здійснюється за малюнком вен на пальці руки.

Обґрунтовуючи доцільність застосування саме такого методу біометричної ідентифікації, представники банку посилалися на досвід Японії, де можливість сканування малюнка вен на пальці надається більш ніж у 80 тисячах пунктах наявних коштів із карток[4].

Одна з найбільших кредитних організацій Польщі – банк «Getin Noble» має намір розширити сферу застосування біометричних технологій. Ідентифікація клієнтів банку, як і в попередньому повідомленні, буде здійснюватися за малюнком вен на пальці руки. Фінансова установа має наміри з часом запровадити біометрію у всіх своїх відділеннях. У 2013 році ідентифікація за малюнком вен на пальці буде здійснюватися лише в офісах, які будуть відкриватися[5].

У Варшаві на вулиці Плоцькій у другому півріччі 2013 року перший біометричний банкомат встановив банк «BPS» – «Польський кооперативний банк». Вже традиційно для Польщі біометрична ідентифікація здійснюється шляхом аналізу судин пальця. Кількість наявних у «BPS» шаблонів налічує понад 50 тисяч, що, на думку фахівців, є досить переконливим результатом, щоб продовжити впровадження нововведення.

Успішний експеримент кооперативного банку прокладає дорогу для застосування інновації іншим банківським лідерам Польщі, які насамперед очікують поліпшення умов наданих послуг при збільшенні безпеки грошових операцій[6].

---

[1] Внедрение нового биометрического сервиса началось в Нидерландах // BIOMETRICS.Ru. – 2012. – 21 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Один из крупнейших банков Польши перейдет на биометрические технологии // BIOMETRICS.Ru. – 2012. – 24 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Ещё один польский банк внедрит биометрические технологии // BIOMETRICS.Ru. – 2011. – 22 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[5] Биометрические технологии в польских банках: новое внедрение // BIOMETRICS.Ru. – 2013. – 17 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[6] Биометрический банкомат появился в Варшаве // Вести ФМ. – 2013. – 27 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Російська Федерація (РФ). Технології біометричної ідентифікації дедалі більше починають використовувати банки Росії та СНД. Серед них російські «Ощадбанк», «Захсібкомбанк» і «Народний банк Казахстану», які використовують розробку «Biolink Idenium» компанії «Biolink Solutions» (електронна адреса порталу: http://biolink.ru)[1].

2012 року було здійснено успішне впровадження програмних і апаратних засобів біометричної ідентифікації в корпоративній мережі російського Комерційного Банку «Спецмережбудбанк». Ця установа розширює свою мережу, яка налічує понад 130 офісів у Москві та Московської, Калузької, Тульської та Володимирської областях. Банк запровадив технологію ідентифікації за відбитками пальців компанії «Biolink Solutions».

Низка кредитних організацій Росії, зокрема й ті, що входять до ТОР-50 банків РФ, застосовують Рішення «Biolink»[2].

Російський банк «Хоум Кредит» удосконалив технологію виявлення шахрайських заявок для отримання кредитів і налагодив процес оповіщення правоохоронних органів про дії зловмисників. Це дозволило затримати у квітні 2013 року шістьох осіб за підозрою у вчиненні шахрайських дій.

Це стало можливим завдяки запровадженню технології верифікації, яка заснована на біометричній перевірці потенційних позичальників. Робота біометричної системи установи «Хоум Кредит» формується на зіставленні фотознімків позичальника та наданої ним інформації з відомостями бази даних банку, що містить інформацію про більш ніж 10 млн клієнтів.

У березні 2013 року «Хоум Кредит» оптимізував процеси зіставлення фотознімків, для чого сегментував базу даних за регіонами. Завдяки цьому значно збільшилась точність ідентифікації шахраїв[3].

Наприкінці 2011 року ТОВ «Pinmoney» запустило в Тюмені однойменну платіжну систему, яка заснована на ідентифікації клієнтів за допомогою біометричних даних. Щоб розплатитися за допомогою «Pinmoney», користувач прикладає палець до спеціальних сканерів на касах партнерів біометричної платіжної системи: списання з персонального рахунку відбувається практично негайно[4].

Загалом у Росії, як і на теренах Співдружності Незалежних Держав, фінансові ринки відстають від західних у технологічному розвитку. Навіть країни, які розвиваються, краще й успішніше розбудовують свій банкінг, ніж члени СНД.

Сполучені Штати Америки (США)

Діючий у США кредитний союз «Service Credit Union» оголосив про впровадження у свою діяльність біометричної технології – сканування за відбитками пальців. На вересень 2012 року кількість його членів становила приблизно 164 тисячі людей, а чисельність службовців – понад 600. Службовці кредитного союзу під час доступу до різних інформаційних систем і ресурсів мають проходити ідентифікацію за відбитками пальців. Загалом рішення запровадити біометричні технології має не тільки підвищити рівень безпеки, але й пришвидшити обслуговування членів кредитного союзу.

---

[1] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] «Спецсетьстройбанк» защитил корпоративные информационные ресурсы с помощью биометрических решений BioLink // BioLink. – 2012. – 20 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Российский банк освоил биометрические технологии // Банка Хоум Кредит. – 2013. – 25 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Биометрическая платежная система начала действовать в Тюмени // Вслух.Ру. – 2012. – 21 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Про початок використання біометричних технологій у системі інформаційної безпеки оголосив Федеральний кредитний союз Великого Техаса[1].

У Сполучених Штатах Америки досить популярними є платіжні системи розрахунків за відбитками пальців. Алгоритм дії системи простий, але ефективний. Користувачі резервують на своєму банківському рахунку кошти, сканують відбитки пальців, після чого рахунок поєднується з моделлю біометричного ідентифікатора. Під час оплати клієнту потрібно буде ще раз відсканувати відбиток пальця. Після цього новостворена модель ідентифікатора буде порівнюватись з уже наявною в базі даних і за їхнього збігання відповідна сума буде списана з рахунку користувача.

База даних шаблонів біометричних ідентифікаторів надійно захищена за допомогою технологій шифрування, а відомості, що зберігаються в ній, за жодних умов не можуть бути наданими ні правоохоронним органам, ні ритейлерам, ні будь-кому ще[2].

Сінгапур, Малайзія та Філіппіни

«Citibank» почав установлювати в Сінгапурі, Малайзії та Філіппінах біометричні банкомати нового покоління, що одержали назву «Citibank Express». Характерною рисою цих банкоматів є здатність практично повністю замінювати звичайні офіси кредитної організації. Користувачам біометричним банкоматів будуть надані послуги з відкриття рахунків, одержання кредитів, оформлення платіжних карт; передбачена навіть можливість проведення відеоконференцій зі співробітниками банку. «Citibank Express» також наділений можливістю взаємодії з мобільними пристроями: почавши оформлення тієї чи іншої операції на планшеті або смартфоні її можна буде завершити в банкоматі.

Крім зазначених країн, упродовж 2013 року заплановано поширення вказаної технології й на інші азіатські країни, а згодом – на держави інших континентів. На жаль, у публікації не вказано, які саме технології біометричної ідентифікації будуть використовуватися в нових банкоматах[3].

Туреччина. У цій країні ідентифікація у фінансових установах здійснюється переважно за допомогою «Vein»-методу. Як відомо, технологію ідентифікації людини за венами долоні було розроблено компанією «Fujitsu», а технологію безконтактної ідентифікації за малюнком вен на пальці – компанією «Hitachi».

«Isbank», який є найбільшим комерційним банком Туреччини, висловив намір, починаючи з 2012 року, активно використовувати технологію ідентифікації за малюнком вен на пальці під час обслуговування своїх клієнтів.

Раніше «Vein»-технологію почав освоювати інший турецький банк «Ziraat». Але у банкоматах «Ziraat» сканується малюнок вен на долоні[4].

Уганда. Розташований в Уганді «Crane Bank» вирішив запровадити у свою діяльність технології біометричної ідентифікації. Планується, що нова система буде впроваджуватися з 2014 року у відділеннях, які відкриваються, а також у головному офісі «Crane Bank». Сканувати відбитки пальців будуть і клієнти банку, і його співробітники. За допомогою біометричних технологій ця фінансова установа має намір досягти

---

[1] Еще один американский кредитный союз внедрил биометрические технологии // BIOMETRICS.Ru. – 2012. – 17 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрическая платежная система в Горной школе Южной Дакоты // BIOMETRICS.Ru. – 2013. – 27 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Citibank начал устанавливать биометрические банкоматы // BIOMETRICS.Ru. – 2013. – 29 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Еще один турецкий банк внедрит биометрические технологии // BIOMETRICS.Ru. – 2012. – 16 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

амбіційної мети: за рік збільшить кількість своїх відділень до 50, а чисельність клієнтів – до одного мільйона людей.

Зазначимо, що аналогічні рішення використовуються й в інших фінансових інститутах Східної Африки, – наприклад, у Кенійському комерційному банку[1].

Федеративна республіка Німеччина (ФРН)

На кінець 2012 року сканерами відбитків пальців оснащено 10 тисяч робочих місць співробітників мережі «Sparkasse», яка є однією із найбільших фінансових установ ФРН і яка аналогічна російському «Ощадбанку»[2].

Швейцарія. Банк «Pictet & Cie» під час переїзду в новий будинок встановив у ньому біометричну систему контролю доступу. Починаючи з кінця 2010 року, понад дві тисячі співробітників банку щодня проходять ідентифікацію за райдужною оболонкою очей та тривимірною моделлю обличчя[3].

Південно-Африканська Республіка (ПАР)

Голова МВС Південно-Африканський Республіки оголосив наприкінці 2011 року про те, що банкам цієї країни надана можливість проводити біометричну ідентифікацію своїх клієнтів. Банки ПАР мають можливість в онлайн режимі звертатися до Національної ідентифікаційної системи МВС (Home Affairs National Identification System /HANIS/), яка містить відомості про відбитки пальців усіх громадян ПАР віком від 16 років, а також біженців й іноземних резидентів, що перебувають на території республіки.

Прямого доступу до бази даних HANIS у банків немає. Щоб встановити особистість потенційного клієнта, банк пропонує йому відсканувати відбитки пальців і передає отриману інформацію (разом із прізвищем та іменем клієнта) у МВС. Там ці відомості перевіряються за базою даних HANIS, після чого банк одержує позитивну або негативну відповідь на свій запит про те, чи достовірні відомості надав про себе клієнт.

Першим біометричні технології почав використовувати банк «ABSA». Надалі впровадження інновації здійснив «Перший національний банк», а потім до біометричного проекту приєдналися ще три кредитні організації: «Nedbank», «Standard Bank» й «African Bank»[4].

Діючий у Південно-Африканській Республіці банк «Capitec» оголосив про придбання 328 біометричних банкоматів. Ідентифікація клієнтів банку буде здійснюватися за відбитками пальців. «Capitec» визнаний найбільш швидкозростаючим роздрібним банком країни – чисельність його клієнтів становить 4,2 млн чоловік[5].

Японія. Ця країна є батьківщиною «Vein»-технології. На початок 2012 року в банкомати було вбудовано 75 тисяч сканерів малюнка вен на пальці. Відповідно до статистики японського агентства фінансових послуг це становило 46% від загальної кількості банкоматів, які здійснювали розпізнавання за «Vein»-технологією. Тобто, загальна кіль-

[1] Еще один африканский банк выбрал биометрические технологии // BIOMETRICS.Ru. – 2013. – 7 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] «Спецсетьстройбанк» защитил корпоративные информационные ресурсы с помощью биометрических решений // BioLink. – 2012. – 20 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические технологии на защите банковских информационных систем // Bankir.ru. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Банки ЮАР начали осуществлять биометрическую идентификацию своих клиентов // BIOMETRICS.Ru. – 2011. – 14 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[5] Число биометрических банкоматов в ЮАР увеличится // BIOMETRICS.Ru. – 2012. – 30 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

кість сканерів, які використовують технології ідентифікації за малюнком вен на пальці або долоні, становила на початку 2012 року приблизно 167 тисяч[1].

Стисло підіб'ємо підсумок використання технологій біометричної ідентифікації у банківсько-фінансовій сфері. Нині найбільш поширеними є такі технології:

– сканування відбитків пальців за технологією, яка відома під назвою неавтоматизовані системи ідентифікації (non-automated fingerprint identification systems, non-AFIS);

– розпізнавання за рисами обличчя;

– розпізнавання за райдужною оболонкою ока;

– розпізнавання за малюнком вен кисті руки або пальця («Vein»-технології);

– розпізнавання за голосом;

– підтвердження особистості за допомогою його підпису;

– ідентифікація за формою кисті руки.

Нині ніхто не заперечує необхідність упровадження досягнень біометрії у фінансову галузь будь-якої країни. Однак відсутність належної взаємної сумісності різних додатків до використовуваного програмного забезпечення – контролю фізичного доступу, логічного доступу до даних та ідентифікації користувача під час процесу проведення банківських операцій – є досить серйозною перешкодою для більш широкого запровадження біометричних рішень на ринку біометрики. Для подолання цього негативного явища в 2008 році Міжнародна організація зі стандартизації (International Organization for Standardization – ISO /ICO/) оголосила про випуск спеціального стандарту ISO 19092:2008, який регламентує застосування біометричних технологій у фінансовій сфері та, зокрема, в питаннях забезпечення безпеки під час верифікації та ідентифікації користувачів електронних платежів. Однак деякі компанії, що виготовляють біометричні програмно-апаратні комплекси, продовжують використовувати свої наробки, тому можливості обміну даними між програмно-апаратним устаткуванням різних фірм-виробників поки що є обмеженими.

Зазначимо, що в світі зростає популярність розрахунків за покупки за допомогою відбитка пальця. Ще раз підкреслимо, що впровадження біометричних систем платежів активно почалося в США і Європі ще на початку XXI століття. А вже у 2008 році дослідницька компанія «TNS» підготувала доповідь «Нове майбутнє магазину», у якому відзначалося, що 6 із 10 респондентів у світі вірять, що в 2015 році можна буде купувати за допомогою відбитків пальців.

Біометрична система оплати є прийнятною для 41% споживачів, зокрема у Китаї цей відсоток становив 60%, а в Німеччині – 24%[2].

Останніми роками з'являється дедалі більше публікацій про те, що біометричні технології підвищують ефективність системи медичного страхування. 2012 року діюча в США Асоціація індустрії безпеки (Security Industry Association /SIA/) надіслала в комітет американського сенату по фінансах звернення, в якому було вказано на високий потенціал технологій біометричної ідентифікації у боротьбі з протиправними діями в системі медичного страхування.

Відповідно, комітет американського сенату по фінансах надіслав відкритий лист до експертного співтовариства з закликом надати пропозиції щодо шляхів підвищення ефективності двох головних програм медичного страхування, що діють у США: Medicare і Medicaid. У листі констатувалося, що щорічно американська система медичного страху-

[1] Еще один турецкий банк внедрит биометрические технологии // BIOMETRICS.Ru. – 2012. – 16 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрическая платежная система начала действовать в Тюмени // Вслух.Ру. – 2012. – 21 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

вання зазнає багатомільярдних збитків, які спричинені розкраданнями, шахрайськими діями та іншими зловживаннями.

Експерти «SIA» цілком слушно відповіли, що суттєво знизити обсяг саме цих втрат здатні технології ідентифікації власників полісів медичного страхування за їхніми біометричними параметрами, які не можливо «позичити» або викрасти.

У відповіді «SIA» підкреслюється, що застосування біометрії дозволить вирішити і ще більш важливу проблему – гарантувати, що одержувана лікарями медична інформація дійсно стосується цього пацієнта (а, скажемо, не до його однофамільця) і тим самим суттєво знизить імовірність виникнення лікарських помилок.

Крім того, біометрична ідентифікація не дозволить пацієнтам користуватися чужими страховими полісами під час звертання за медичною допомогою. Якщо надання цієї допомоги буде підтверджуватися скануванням відбитків пальців або інших біометричних параметрів, відійдуть в минуле приписки, коли та чи інша медична послуга, вартість якої повинна покриватися страховкою, лише задекларована на папері, а насправді не надається[1].

Останнім часом з'являється дедалі більше повідомлень про переваги платіжних систем, заснованих на технологіях смарт-карт і біометричної ідентифікації. Причому здебільшого у таких смарт-картах додатково реалізують технології «бездротової персональної мережі» (Wireless Personal Area Network /WPAN/) або «комунікацій близького поля» (Near Field Communication /NFC/).

Відмінність між WPAN і NFC полягає в тому, що у першому випадку смарт-картки можуть обмінюватися інформацією з відповідними обладнаннями на відстані до двох метрів, а у другому випадку – потрібно підносити карту до спеціального зчитувача.

Суттєвою перевагою такої платіжної системи є те, що відомості про біометричні ідентифікатори покупців зберігаються у чіпах їхніх смарт-карт, тому не виникає необхідності щодо ведення централізованої бази біометричних даних. Як наслідок, зникають побоювання про можливе викрадення персональних даних із такої бази[2].

Ще кращим рішенням є розробка біометричної ідентифікаційної смарт-карти з вбудованим сканером відбитків пальців. На початку 2012 року грант у 12 мільйонів норвезьких крон від Єврокомісії одержала норвезька фірма «IDEX» та її французький партнер – компанія «UINT».

Уродовж двох років вони зобов'язалися створити смарт-карту, в яку буде інтегрований надзвичайно тонкий сканер відбитків пальців. Це рішення дозволить звести до мінімуму кількість процедур, пов'язаних з обробкою біометричних персональних даних користувача: всі вони будуть виконуватися новою карткою та не будуть нікуди передаватися за межі карти.

Крім того, у смарт-карті буде застосовуватися NFC. Це означає, що власник карти зможе в безконтактному режимі використовувати її в різних платіжних системах (наприклад, для оплати проїзду в суспільному транспорті, вартості паркування, товарів

[1] Биометрические технологии повысят эффективность системы медицинского страхования // BIOMETRICS.Ru. – 2012. – 13 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрические технологии позволят покупателям «Ашана» расплачиваться пальцами // BIOMETRICS.Ru. – 2012. – 24 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

у магазині і т. д.), швидко, легко та безпечно підтверджуючи свої повноваження на проведення відповідної транзакції[1].

Спробуємо заглянути у майбутнє використання нових ІТ-рішень у фінансово-банківської галузі. Це використання технології віртуалізації для створення більш доступного, надійного та захищеного банкомата, а також спрощеної системи управління каналами самообслуговування.

Використання віртуалізації повинно повністю замінити процес впровадження інноваційних рішень. Ця технологія надає можливість використовувати комплексну систему управління та широкий спектр різних послуг, а також сприяє взаємодії величезної кількості інформаційних каналів.

За словами віце-президента компанії «Diebold» ця технологія поєднує переваги так званих хмарних обчислень і є новим словом у сфері банківського роздрібу. Це переломний момент у всій індустрії.

Компанія «Diebold Incorporated» (NYSE: DBD) використала всі переваги технології віртуалізації й створила прототип першого у світі віртуального банкомата. Інноваційна розробка «Diebold» була презентована на виставці-конференції Vmworld 2011 у Лас-Вегасі 29 серпня.

Фірма «Diebold» розробила віртуальний банкомат разом із «Vmware». Суть проекту полягає в комбінації технології самообслуговування та віртуалізації. Ця комбінація допоможе вирішити головні завдання банків: забезпечення високого рівня безпеки та зниження ризику шахрайства, удосконалення операційної ефективності, забезпечення максимальної зручності для користувачів і розширення клієнтської бази.

Завдяки віртуалізації системи самообслуговування банкомат працює без вбудованого комп'ютера і під'єднується до єдиного обчислювального центру. Як наслідок, фізичні компоненти одного сервера здійснюють усі обчислювальні операції багатьох віртуальних банкоматів.

У результаті відбувається консолідація та перерозподіл потоків інформації не тільки у всій мережі самообслуговування, але й в інформаційних каналах, що сприяє більш ефективній їхній взаємодії.

У підсумку формується єдиний безпечний центр даних і підвищується рівень контролю та безпеки IP-адресів. Віртуалізація забезпечує більш ефективну експлуатацію сервера та зумовлює уніфікацію управління банкоматами, що збільшує операційну ефективність, забезпечує більш швидке відновлення після помилок і створює умови для пришвидшеного відновлення програмного забезпечення (ПЗ) і розподілу послуг. Інакше кажучи, віртуалізація зумовлює зниження вартості обслуговування та збільшує період продуктивної експлуатації банкоматів[2].

На думку авторів, слабким місцем у цій технології є канали передачі даних. У повідомленні нічого не говориться про їх захист. А за допомогою каналів передачі під час несанкціонованого доступу можливо заблокувати роботу всієї системи, не кажучи вже про можливість за певних умов крадіжки персональних даних.

Найбільш надійним шляхом для мінімізації банківських ризиків і боротьби з фальсифікацією документів під час одержання кредиту або роботи з депозитним рахунком є мультибіометрична або багатофакторна системи ідентифікації клієнтів банку.

---

[1] Еврокомиссия профинансировала разработку биометрической смарт-карты // BIOMETRICS.Ru. – 2012. – 19 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Виртуальный банкомат оснащен средствами биометрической идентификации // Bankir.ru. – 2011. – 5 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

На теренах СНД одним із надійних рішень є система «Biolink CI» (Client-Identification).

Завдяки запатентованим алгоритмам порівняння біометричних шаблонів, система дозволяє в режимі реального часу здійснювати ідентифікацію за базою клієнтів до 50 млн осіб, використовуючи для ідентифікації особистості один або комбінацію унікальних біометричних параметрів. «Biolink CI» має гнучку модульну структуру, що дозволяє використовувати одну або відразу декілька технологій біометричної ідентифікації.

Ідентифікацію клієнтів у системі можна проводити за такими параметрами або за їх комбінаціями:

– за відбитком пальця;
– за 2 відбитками пальців;
– за геометрією обличчя;
– за райдужною оболонкою ока;
– за малюнком вен;
– за голосом;
– за почерком.

Система дозволяє працювати в режимі дворівневої ідентифікації: на першому етапі ідентифікується особистість клієнта, на другому – співробітник банку проходить біометричну ідентифікацію для підтвердження операції[1].

Розглянемо перспективи застосування біометричних технологій у мобільних платежах. У серпні 2013 року компанія «Frost & Sullivan» опублікувала прогноз, присвячений забезпеченню безпеки мобільних платежів.

Жан-Ноель Жорж, який очолює в компанії глобальну програму дослідження ринків інформаційно-ком'ютерних технологій (ІКТ) у фінансовому секторі, вважає, що перший крок на шляху забезпечення безпеки зазначених платежів полягає в захисті безпосередньо самого мобільного пристрою.

«Зараз якраз і настав час для того, щоб застосовувати біометричні технології для захисту мобільних додатків і особливо – платежів, – говорить експерт «Frost & Sullivan». З точки зору «платіжної» безпеки біометрія і надає істотні переваги»[2].

Розвиток мобільних платежів має пришвидшити інтеграцію смартфонів і біометричних технологій. Такий висновок зробили автори прогнозу, опублікованого «Biometrics Research Group» у вересні 2013 року.

Експерти цієї компанії пророкують, що до 2020 року мобільними платежами будуть користуватися 700 млн людей, а обсяг відповідного сегмента фінансового ринку сягне 750 млрд доларів. Ця обставина істотно пришвидшить впровадження у смартфони біометричних технологій, здатних надавати власникам цих пристроїв високий рівень безпеки під час проведення платежів.

Фахівці компанії «Biometrics Research Group» пророкують, що в 2014 році обсяг поставок біометричних смартфонів сягне 90 млн одиниць. 78% від цього числа буде становити частка корпорації «Apple», яка першою вивела на масовий ринок смартфон

[1] Надежная идентификация клиентов – ключевой фактор минимизации рисков мошенничества // BioLink. – 2011. – 27 сентября. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/products/biolink-ci-system/

[2] Биометрические технологии обеспечат надежную защиту мобильных платежей // BIOMETRICS.Ru. – 2013. – 27 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

зі сканером відбитків пальців; «Samsung» через запізнення з виходом на ринок задовільниться 17%; на інших виробників припаде лише 5% ринку біометричних смартфонів[1].

Використання біометричних технологій у фінансовій сфері України стає дедалі більш необхідною й усвідомленою потребою. Щоб електронний бізнес мав тільки позитивний ефект, потенційним учасникам необхідно гарантувати його безпечність.

Застосування останніх досягнень інформаційних технологій у банківській сфері та електронній комерції дає можливість значно розширити перелік послуг, що надаються, залучити нових клієнтів і підвищити конкурентоспроможність банківської установи.

Міжнародна практика свідчить, що основа процвітання електронного бізнесу – створення надійно захищеного, стандартизованого та уніфікованого середовища. Із запровадження стандартів, особливо міжнародних, і починається універсалізація інструментів бізнесу з єдиними механізмами захисту для вирішення різних завдань (авторизація на будь-яких рівнях і компонентах комп'ютерної мережі – операційних систем, систем управління базами даних (СУБД) і окремих програм; захищений внутрішній документообіг у корпоративній мережі, насамперед електронної пошти; організація захищених з'єднань абонентів мережі; авторизований та ієрархічний доступ до мережевих пристроїв і web-вузлів).

В електронній банківській комерції особливо критичним моментом є отримання підтвердження, що кожне комунікаційне з'єднання, транзакція або запит на доступ є легітимним. Відповідно до цього необхідно використовувати надійні методи перевірки ідентичності (аутентифікація або верифікація), а також авторизація (ідентифікація) клієнтів, які намагаються ініціювати електронні транзакції.

В Україні необхідною умовою розвитку електронної комерції та інтернет-банкінгу є запровадження міжнародних біометричних (ISO 19092:2008) і PKI-стандартов. Причому формування систем персонально відкритих ключів PKI необхідно проводити з урахуванням положень документа IdentrusTM LLC. Під час впровадження у будь-якій фінустанові електронної комерції обов'язковою нормою повинно стати виконання вимог стандарту 3-D Secure VISA.

Система PKI Identrus здебільшого вимагає наявності кваліфікованого електронного підпису. За визначенням Європейського Співтовариства, «кваліфікований електронний підпис» – це такий підпис, що вимагає виконання певних вимог забезпечення достовірності, тобто це означає, що спосіб утворення підпису має відповідати технічним вимогам стандартів FIPS 140-1 (Federal Information Processing Standards, U. S.), 140-2 level 2, 3.

За вимогами Європейського Союзу (ЄС), електронний підпис повинен забезпечувати аутентифікацію та цілісність інформації, що передається. У країнах ЄС, США, Канаді та низці інших держав цифровий підпис законодавчо визнаний як еквівалент власного підпису, також на законодавчому рівні затверджені визначення термінів «електронний підпис», «електронні документи».

Усі держави Європейського Співтовариства ухвалили національні законодавчі акти, які повністю відповідають вимогам Директиви Європарламенту і Ради Міністрів ЄС 1999/93/ЄС і рішенню 2000/709/ЄС Комісії Європарламенту та Ради щодо системи

[1] Биометрические технологии в смартфонах и мобильных платежах: битва Apple и Samsung // BIOMETRICS.Ru. – 2013. – 24 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

електронних підписів, яка застосовується в межах Співтовариства. Нині всі положення Директиви 1999/93/ЄС реалізовані у вигляді європейських і міжнародних технічних стандартів (ETSI і RFC). Для подальшого розвитку українського електронного бізнесу необхідно на державному рівні ввести в дію відповідні стандарти ISO, ETSI і RFC, які вже діють в Європейському Союзі[1].

Серед галузей української економіки вітчизняний фінансовий сектор можна вважати найліпше підготовленим до втілення серйозних інформаційно-технологічних проектів. Про це свідчать і показники економічного потенціалу, і існуючий рівень використання інформаційно-комп'ютерних технологій у бізнесі українських банків. Під час ухвалення відповідних законів і стандартів фінансовий сектор України, порівняно з іншими галузями, має непогані стартові позиції для використання сучасних біометричних технологій під час впровадження нових сучасних форм електронної комерції та здійснення фінансових транзакцій.

Переваги інформатизації банківського сектора і з погляду регулювання бізнес-процесів, і щодо змін у сфері роздрібних послуг банків цілком очевидні. Але зі зростанням інформаційних переваг збільшуються і ризики, які загалом знижують ефективність від впровадження послуг електронних розрахунків.

Велика частина цих ризиків визначається зовнішніми для банків обставинами, які призводять до різкого зменшення очікуваного економічного ефекту від розвитку системи електронних послуг. Весь цей комплекс ризиків залежить від вирішення трьох основних проблем: безпеки, проблеми довіри, а також загального рівня розвитку «технологічної культури». Проблема забезпечення безпеки електронного фінансового сектора економіки – фактично це низка технологічних проблем, подолання яких вимагає певного часу і зусиль. Адже йдеться про проблеми безпеки фінансових операцій, які здійснюються в мережах, причому не завжди у закритих мережевих системах. Основними небезпеками в цьому випадку є: несанкціонований доступ до електронної системи, злом її захисту, навмисний або ненавмисний витік конфіденційної інформації, маніпулювання даними, вихід із ладу системи, порушення цілісності інформації[2].

Технічно поки що повністю усунути подібні ризики неможливо, проте правильне поєднання організаційно-контрольних і технологічних процедур із біометричними технологіями дозволить суттєво знизити рівень недовіри тих клієнтів, для яких використання електронних бізнес-послуг є нагальною потребою. Забезпечення інформаційної безпеки у фінансовій сфері можна порівняти з гонкою озброєнь у військових. Це процес, в якому немає і не може бути постійних переможців, оскільки ситуація змінюється надто швидко. І протистоять один одному тут рівні суперники. Тому недооцінювати можливості кібернетичного кримінального світу абсолютно не варто. Експерти стверджують, що в конкурентній боротьбі, яка нині тільки посилюється й у банківському секторі, і на ринку платіжних систем, переможцями вийдуть ті фінансові інститути та кредитні організації, що будуть спроможними першими реалізувати захисні можливості біометричних технологій.

Використання потенціалу біометрії – це переведення бізнес-процесів на якісно вищий рівень, який забезпечує більш високу ефективність і безпеку в поєднанні з оперативністю, надійністю та комфортністю для користувачів (і для зовнішніх клієнтів, і для власних працівників).

---

[1] Бєлов С. Ризикована привабливість / С. Бєлов, С. Мартиненко. [Електронний ресурс]. – Режим доступу: http://www.business.if.ua/themes/business/print-version.asp...

[2] Карачаровский В. Три преграды на пути высокотехнологичных банковских услуг / В. Карачаровский // Cnews.ru. – 2008. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/banks2008/articles/barrier.shtml

6.9. Світова тенденція об'єднання в практичних біометричних системах мультибіометричних і багатофакторних рішень. Основні завдання інтеграції біометричних технологій

Щоб надати біометричним вимірюванням особливий ступінь достовірності та забезпечити необхідну їх точність, потрібно застосувати більше ніж один спосіб ідентифікації або верифікації. У зв'язку з цим і виникла ідея перехресної біометрії (інша назва – мультибіометрія), що використовує комбінацію декількох видів біометричного вимірювання та їх аналізу. У деяких ситуаціях замовник може вважати використання однієї форми біометричної ідентифікації недостатньою.

Часто подібна ситуація виникає під час використання технології ідентифікації за відбитками пальців, оскільки за деякими даними приблизно 10% населення землі мають зношені папілярні візерунки пальців, тобто такі візерунки, які механічно ушкоджені і, як наслідок, непридатні для ідентифікації.

Перехресна біометрія використовує більше ніж один ідентифікуючий параметр для здійснення процедури порівняння з наявними зразками-шаблонами в процесі ідентифікації. Уявімо собі систему, яка використовує одночасно три біометричні технології, – розпізнавання за рисами обличчя, відбитками пальців та голосом. Якщо одна з технологій не дає відповідного результату, система може визначити особистість за двома іншими методами. За низкою повідомлень 1998 року започатковане промислове застосування технологій перехресної біометрії (мультибіометрії).

У біометричних системах ступінь подібності досліджуваного зразка до контрольного виражається через коефіцієнти подібності. Чим більший коефіцієнт, тим вищий ступінь подібності. Ідентифікація вважається такою, що вже відбулася, лише тоді, коли коефіцієнти подібності біометричних параметрів індивідуума, котрий проходить стадію перевірки, перевищують наперед визначене порогове значення. Використання більше ніж одного виду методу біометричної ідентифікації дає можливість у сукупності забезпечити високий рівень значення порогу доступу. Як відомо, адміністратор біометричної системи має право регулювати їх величину. Для об'єктів із високими вимогами до їх безпеки використовують, зазвичай, програмно-апаратні комплекси з трьома видами біометричної ідентифікації, а в місцях, де такі жорсткі заходи є зайвими, – досить і двох. Ця методологія значно знижує ймовірність проникнення в контрольовану системою зону неавторизованих відвідувачів[1].

Важливу роль надійної та ефективної ідентифікації усвідомлюють усі, хто стикається з різними системами розпізнавання індивідуумів, – їх розробники, постачальники, системні інтегратори, замовники і користувачі. Найбільший рівень безпеки та комфорту забезпечує одночасне використання різних біометричних рішень. Нині мультибіометричні рішення стають більш популярними та престижними.

Отже, розробка й застосування мультибіометричних рішень – один із найперспективніших напрямів розвитку галузевого ринку. Мультибіометричні рішення застосовуються, наприклад, в електронних паспортах й ідентифікаційних картках (ID-card) «друго-

[1] Бирман Натан. Перекрёстная биометрия / Натан Бирман // Газета международных новостей по техническим средствам и системам безопасности. – 2006. – 15 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

го покоління», що вже випускаються різними державами, вносять не тільки цифрові фотографії власників цих документів, але й відомості про відбитки їх пальців або будь-які інші біометричні параметри фізичної особи.

Основні переваги мультибіометричної технології:

– підвищення надійності та якості розпізнавання з одночасним зниженням кількості помилок, коли надається доступ незареєстрованій особі або відмовляється у доступі зареєстрованому користувачеві;

– пришвидшення процесу ідентифікації;

– розмаїття ідентифікаційних методів і можливість альтернативного вибору для їх застосування.

Після біометричних паспортів «другого покоління» одним із наймасовіших запроваджень мультибіометрії є проект Міністерства внутрішньої безпеки (МВБ) США з інтеграції в національні ID-карти нових біометричних параметрів. Цей амбіційний проект реалізується відповідно до директиви про національну безпеку HSPD-12 і до спеціальної директиви адміністративно-бюджетного управління США. Згідно з федеральним стандартом обробки інформації 201-2, який містить докладну інформацію про технології обробки біометричних даних для реалізації HSPD-12, національний інститут стандартів і технологій (NIST) Сполучених Штатів Америки випустив інструкцію для федеральних органів.

Цей документ містить специфікацію з використання технології розпізнавання райдужки ока як додаткової опції нової ідентифікаційної системи. В інструкції також викладені технічні особливості щодо всіх задіяних ідентифікаторів і функціонування самої PIV-карти (Personal Identity Verification cards).

Зокрема, детально розписана вимога впровадження стандартизованого та компактного формату райдужної оболонки ока, який повинен забезпечити додаткову точність ідентифікації, а також надані відповідні норми розпізнавання за відбитками пальців і форми обличчя. PIV-карта (верифікація особистості) повинна стати основним інструментом аутентифікації повноважень державних службовців і підрядників для доступу до послуг, мереж та інформаційних систем.

Нова смарт-карта може мати вигляд ламінованої пластикової карти старого зразка, але зберігатиме набагато більше даних, ніж прості установчі дані, адреса й фото. Вбудовані комп'ютерні чіпи повинні зберігати відомості та ресурси, потрібні для виконання мультибіометричної ідентифікації та низку інших рішень. Карта може мати не тільки штрих-код, RFID-мітку (радіочастотну ідентифікацію) та магнітну смужку, але й вбудований процесор даних для сегментування та зберігання інформації, зокрема для автоматичного віддаленого оновлення інформації. На думку фахівців, загалом може знадобитися майже 30 технологічних видів дій, які необхідні для друкування та ламінування такої карти, а також включення до неї всіх зазначених функцій.

Оскільки діяльність МВБ охоплює широкий спектр напрямів – від безпеки кордонів до реагування на надзвичайні ситуації, – тому саме це міністерство може бути «законодавцем моди» у США щодо організації безпечної ідентифікації для установ на всіх рівнях влади та підприємств у промисловості[1].

Ще один приклад використання мультибіометрії. У лютому 2013 року Міністерство оборони США уклало з однієї з каліфорнійських фірм дворічний контракт на

[1] Биометрические идентификационные карты в США обрели второе дыхание // Экспертный центр электронного государства. – 2013. – 23 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

розробку апаратного та програмного забезпечення, призначеного для здійснення біометричної ідентифікації за допомогою смартфонів.

Виконавець повинен буде представити замовникові «біометричний смартфон», який зможе розпізнавати людей за їхнім обличчям, райдужною оболонкою очей, голосом та відбитками пальців. Відстань ідентифікації за обличчям повинна становити два метри, а за райдужною оболонкою очей – метр. Розпізнавати розмовляючого чоловіка засіб мобільної біометричної ідентифікації повинен на відстані, яка є звичайною під час розмови телефоном; для ідентифікації за відбитками пальців людині, особистість якої встановлюється, необхідно буде торкнутися смартфона.

У технічному завданні до контракту особливо підкреслено, що біометричний смартфон повинен мати можливість працювати за яскравого сонячного світла. Також до технічного завдання включений пункт, за яким біометричний смартфон повинен бути наділений здатністю самостійно, без участі користувача, формувати зображення біометричних ідентифікаторів для їхньої подальшої обробки[1].

Крім застосування мультибіометричних технологій для підвищення надійності ідентифікації та верифікації, в один клас із ними прийнято об'єднувати багатофакторні та мультимодальні рішення.

У багатофакторних системах поряд із біометричними використовуються також й інші ідентифікатори (PIN-код, пароль, смарт-картка, токен). У цьому випадку для підтвердження своєї особистості та повноважень користувачеві необхідно пройти біометричну ідентифікацію та пред'явити додатковий ідентифікатор. У мультимодальних системах ідентифікатори одного і того ж типу (наприклад, відбитки пальців) обробляються за допомогою різних математичних алгоритмів. Головна мета цих заходів – підвищення надійності ідентифікації.

Основними завданнями застосування багатофакторних систем є пришвидшення процесу ідентифікації і/або надання можливості розпізнавання без звернення до централізованої бази даних шаблонів ідентифікаторів (наприклад, коли відомості про відбитки пальців вносяться в пам'ять смарт-картки, яку пред'являють під час верифікації, а цифрова модель відбитка, що внесена до пам'яті картки, порівнюється з моделлю знов отриманого ідентифікатора)[2].

Яскравим прикладом реалізації багатофакторної системи є розробка на замовлення Єврокомісії біометричної ідентифікаційної ID-карти з вбудованим сканером відбитків пальців. Це смарт-карта, в яку буде інтегрований надзвичайно тонкий сканер відбитків пальців. Таке рішення дозволить звести до мінімуму кількість процедур, пов'язаних з обробкою біометричних персональних даних користувача: всі вони будуть виконуватися новою карткою та не будуть нікуди передаватися за межі карти[3].

Нині мультибіометричними найчастіше іменують системи, принцип дії яких заснований на паралельному використанні декількох біометричних ідентифікаторів, і, зрозуміло, навіть таке механічне додавання можна вважати кроком уперед. Проте про справжню мультибіометрію можна буде говорити тільки тоді, коли біометрична

---

[1] Пентагон заинтересовался мобильной мультибиометрической идентификацией // Biometrics.RU. – 2013. – 18 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Мультибиометрические технологии // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/multibiometric.php

[3] Еврокомиссия профинансировала разработку биометрической смарт-карты // BIOMETRICS.Ru. – 2012. – 19 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

ідентифікація стане дійсно інтегральною, тобто коли недоліки одних технологій почнуть компенсуватися перевагами інших.

Ілюстрацією тут може слугувати об'єднання технологій ідентифікації за геометрією обличчя особи та відбитками пальців. Камери відеоспостереження «зустрічають» користувача на підході до об'єкта контролю. Засоби ідентифікації за особливостями обличчя окреслюють коло можливих «кандидатів» на розпізнавання і, коли користувач сканує відбиток пальця за допомогою термінала на прохідній, його розпізнавання істотно прискорюється за рахунок наявності вже проведеної «вибірки» даних на індивідуумів із подібним обличчям[1].

Поряд із мультибіометричними, багатофакторними та мультимодальними рішеннями істотного значення набуває й можливість інтеграції останніх розробок біометричних технологій у різні апаратно-прикладні продукти, які вже експлуатуються (в основному, це системи безпеки та контролю за доступом).

Основні завдання цієї інтеграції такі:

– швидке і легке впровадження останніх досягнень технологій біометричної ідентифікації у вже існуючі прикладні продукти та корпоративні системи;

– звільнення розробників та експлуатаційників цих продуктів і систем від необхідності детально проходити вивчення курсу біометрії;

– надання гнучких і зручних засобів для втілення функцій біометричної ідентифікації у розроблювані прикладні рішення (включаючи надання готового графічного інтерфейсу, спеціальна розробка якого вимагає багато зусиль);

– надання та забезпечення можливостей централізованого зберігання й обробки даних про біометричні ідентифікатори користувачів[2].

На нинішньому етапі розвитку цивілізації завдання досягнення та створення відповідних рівнів безпеки і надійності вирішуються за допомогою різних багатофакторних і мультибіометричних технологій ідентифікації. Нині та в майбутньому основним методом біометричної ідентифікації, який поки що набув найбільшого поширення, буде технологія ідентифікації за відбитками пальців. Як правило, цей вид біометричної ідентифікації зараз доповнюється розпізнаванням користувачів за PIN-кодом або за безконтактними картками та їх аналогами, причому дедалі більшого поширення набувають технічні рішення, що засновані на симбіозі цих методів.

Отже, найуспішнішим рішенням є інтеграція біометрії з іншими технологіями ідентифікації, причому тут також можуть бути виокремлені відповідні ступені зрілості. Поки що найпоширеніший варіант – використання досить простої багатофакторної системи, коли повноваження користувача підтверджуються біометричним ідентифікатором і пред'явленням матеріального носія або введенням PIN-коду. Складнішим, але й перспективнішим шляхом є фіксація відомостей щодо біометричного ідентифікатора у смарткартці, пам'ять якої водночас є захищеним сховищем та сховищем іншої доповнювальної аутентифікаційної інформації (електронні сертифікати, ключі шифрування, цифровий підпис тощо)[3].

Засоби інтеграції повинні забезпечувати реалізацію можливостей, що надаються технологіями підтримки різних програмних продуктів і розробками прикладних рішень:

---

[1] Лукашов И. Биометрия в системах контроля и управления доступом: вызовы времени и новые возможности / И. Лукашов // Системы безопасности. – 2008. – 10 июня.

[2] Интеграция // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/integration.php…

[3] Лукашов И. Биометрия в системах контроля и управления доступом: вызовы времени и новые возможности / И. Лукашов // Системы безопасности. – 2008. – 10 июня.

– у найбільш поширених операційних системах (Windows XP, Windows Mobile, інших останніх розробок Windows, Linux);

– на основі популярних платформ і мов програмування (C, C++, NET, Visual Basic);

– відповідно до міжнародних і галузевих стандартів (ISO/IEC, ANSI/NIST, BioAPI)[1].

В останніх розробках систем контролю й управління доступом (СКУД) контроль за доступом поєднаний із обліком робочого часу. Як правило, для постійних співробітників застосовується рішення з використанням біометричних ідентифікаторів, а для ідентифікації відвідувачів практикується видача на час візиту безконтактних карт.

Сьогодні стала нагальною проблема точної ідентифікації індивідуумів у місцях масового скупчення людей, під час проведення звірки документів і контролю перепусток. Насамперед ця проблема стосується безпеки транспортних систем – аеропортів, залізничних вокзалів, морських портів, метрополітену, а також забезпечення санкціонованого доступу під час використання персональних відомостей державних і міждержавних банків даних (паспортно-візових, митних, міграційних і оперативних служб).

Перше завдання, пов'язане з використанням паспортно-візових документів на транспорті під час перетинання державних кордонів, – це перевірка достовірності документа та його відповідності пред'явнику. Біометричні технології створені для того, щоб підвищити надійність та ефективність перевірки документів, а також забезпечити проведення електронного документування (фіксацію) всіх проведених звірок (перевірок).

Останнім часом у світі збільшується кількість учинених терористичних актів на транспортних вузлах. Загрози громадській безпеці, що спричиняються навмисними діями людини, можна поділити на такі дві категорії: загроза, що виникає під час здійснення доступу персоналу в службові приміщення та загроза під час проведення регулювання пасажиропотоку.

Сучасні транспортні термінали, наприклад великі аеропорти, обслуговуються багатотисячною кількістю працівників. Усі вони мають доступ у ті чи інші службові приміщення, водночас багато з таких приміщень є критично важливими з погляду безпеки.

Упровадження біометричних технологій для контролю за доступом у службові приміщення, виходу на летовище і можливого запобігання небажаним діям співробітників транспортного вузла сьогодні здійснено у багатьох аеропортах. Біометрична верифікація як додаток до ідентифікаційних карток, електронних жетонів («токенів») і спеціальних ключів дозволяє виключити можливість обміну картками між співробітниками, мінімізувати ризики, що виникають у разі втрати або крадіжки перепустки, та істотно знизити вплив «людського фактора» як у випадку втоми або недостатньої кваліфікації співробітника служби безпеки, так і у разі навмисного нехтування своїми обов'язками[2].

Прикладом формування мультибіометричної системи СКУД є підписання корпорацією «Unisys» у травні 2008 року контракту з канадським урядом щодо її впровадження у 29 аеропортах країни. В рамках контракту пройшла модернізацію система карткового доступу в режимні зони (Restricted Area Identification Card system – RAIC). Поєднання цієї системи з біометричними технологіями дозволило істотно підвищити безпеку канадських аеропортів і отримати гарантії того, що санкціонований доступ у режимні зони та службові приміщення отримував той службовець, який дійсно має на це право.

---

[1] Вакуленко А. Аэропорты: зона особого внимания / А. Вакуленко, А. Юхин // Мир и безопасность. – 2006. – № 3. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Там же.

Для ідентифікації співробітників аеропортів використовувалось розпізнавання за відбитками пальців і райдужною оболонкою очей. Цифрові шаблони цих ідентифікаторів вносились у пам'ять карток доступу та після проходження процедури ідентифікації порівнювалися з одержаними моделями відбитків пальців або райдужної оболонки.

Мультибіометрична система контролю за доступом практично охопила всіх службовців і працівників аеропортів, тобто приблизно 100 тис. чоловік. Замовником цього проекту було Канадське управління безпеки на повітряному транспорті (Canadian Air Transport Security Authority – CATSA)[1].

Нині під час регулювання пасажиропотоку одним із найважливіших завдань, з якими стикаються служби безпеки аеропортів та інших транспортних вузлів, – це виключення можливості обміну посадковими талонами після реєстрації пасажира на рейс.

У разі проведення наскрізної реєстрації пасажира на декілька рейсів із пересадками ймовірність обміну посадковими талонами зростає. А здійснення процедури повторної звірки паспортів під час посадки на кожний рейс не завжди можливе та інколи нормативно обмежене.

Тому застосування режиму верифікації дозволяє визначити особистість і номер рейсу будь-якого пасажира у потрібний момент, а не тільки під час здійснення процедури посадки на рейс.

Однією з найімовірніших моделей використання біометрики є таке рішення, коли проводиться звірка документів і запис біометричного шаблону в базу даних у момент реєстрації пасажира на рейс, а біометрична верифікація особистості з даними посадкового талона здійснюється безпосередньо під час посадки на рейс. Тобто, до мікрочіпа посадкового талона пасажира вноситься його біометричний шаблон під час реєстрації на рейс, а контроль за відповідністю біометричних параметрів особи і даних талона здійснюється під час посадки на борт літака.

Як відомо, під час перетинання державних кордонів здійснюється звірка достовірності пред'явленого документа та контроль за його належністю пред'явнику. Для цього проводиться звірка біометричного шаблону, який зберігається у пам'яті мікрочіпа електронного паспорта або візи, з біометричними характеристиками власника (подвійна верифікація) або ще додатково здійснюється порівняння двох наданих характеристик із шаблоном, що зберігається в загальнодержавному реєстрі біометричних даних (потрійна верифікація)[2].

Отже, використання комбінованих способів біометричної (мультибіометричної) й апаратної (багатофакторної) аутентифікації суттєво підвищує надійність системи захисту, що підтверджується значною увагою, яку проявляють до впровадження рішень комбінованих технологій провідні світові виробники.

Отже, найбільший ефект надає інтеграція біометрії з іншими технологіями (смарт-картками, RFID-технологією тощо), комплексне застосування біометрії з не менш значимими засобами захисту інформації, постійний розвиток і вдосконалення й наявних, й нових технологій біометричної ідентифікації, підвищення точності розпізнавання користувачів і «доброзичливості» інтерфейсу біометричних засобів – шлях розвитку сучасних біометричних технологій.

[1] Новые подробности о мультибиометрической системе контроля доступа в канадских аэропортах // Biometrics.RU. – 2008. – 30 мая. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Вакуленко А. Аэропорты: зона особого внимания / А. Вакуленко, А. Юхин // Мир и безопасность. – 2006. – № 3. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Для підтвердження актуальності цього висновку наведемо вислів одного з очільників управління юстиції, свободи та безпеки при Європейській комісії Френка Пола: «Ніколи не виникне ситуація, коли світ погодиться мати тільки один біометричний показник».

Великобританія, Європа та США проводять більш прискіпливий контроль за ідентифікацією осіб за допомогою своїх баз даних (БД) шляхом збору і зберігання в БД ідентифікуючих відомостей, отриманих під час використання різних видів біометричної ідентифікації[1].

2007 року був ухвалений стандарт ISO/IEC TR 24722:2007 (Інформаційні технології – Біометрика – Мультимодальні та інші мультибіометричні з'єднання), який був розроблений міжнародним комітетом стандартизації ISO/IEC JTC 1 «Інформаційні технології». Цей стандарт уніфікує розробку технологічних рішень, які реалізують можливість поєднання застосування декількох біометричних ідентифікаторів в одній біометричній системі для підвищення достовірності ідентифікації[2].

Міністерство національної безпеки США (Department of Homeland Security /DHS/) 2012 року розширило список біометричних ідентифікаторів, відомості про яких будуть використовуватися для забезпечення безпеки американських кордонів. До цих ідентифікаторів поряд із відбитками пальців увійшли також оцифровані фотографії осіб і райдужна оболонка очей. Пілотний проект буде реалізований Митною та прикордонною службою (найбільшим агентством, що входять до DHS)[3].

Раніше про свій намір активізувати використання технологій ідентифікації за райдужною оболонкою очей оголосило ФБР. 2013 року Міністерство внутрішньої безпеки (МВБ) США почало реалізацію проекту з інтеграції в національні ID-карти нових біометричних параметрів, зокрема внесення в чіпи цих карт поряд із відомостями про відбитки пальців також цифрових моделей райдужної оболонки ока та геометрії лиця.

Акцентуємо, що незабаром новим трендом повинна стати біометрична ідентифікація у місцях масового скупчення людей, які перебувають у русі.

6.10. Біометричні технології у мобільних пристроях

2011 року британська дослідницька компанія «Goode Intelligence» опублікувала огляд ринку біометричних продуктів і послуг для мобільних пристроїв. Три роки тому автори огляду спрогнозували можливість фінансового буму на цьому ринку: за період 2011–2015 років вони передбачили збільшення розміру ринку з 30 млн доларів до 161 млн.

У своїй роботі експерти визначили низку перспективних напрямів розвитку ринку біометричних продуктів і послуг для мобільних пристроїв.

---

[1] Баллард Марк. Пограничные и миграционные службы готовятся к введению мультибиометрической идентификации / Марк Баллард // Комментатор. – 2007. – 4 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Новий звіт ISO/IEC щодо біометричного злиття для підвищення безпеки. – 2007. – август. [Электронный ресурс]. – Режим доступа: http://www.ukrndnc.org.ua/index.php...

[3] США расширят применение биометрических технологий в пограничном контроле // Biometrics.RU. – 2012. – 19 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Перший напрям – забезпечення захисту від несанкціонованого доступу як до самих мобільних пристроїв, так і функціонуючих у їхньому складі різних додатків і даних, які зберігаються в їхній пам'яті.

Фахівці передбачали, що необхідність ефективного вирішення завдання захисту від несанкціонованого доступу за допомогою біометричних технологій стимулюватиме подальше розширення сфери застосування біометрії у виробництві та використанні мобільних пристроїв.

Другий напрям – поширення мобільної комерції та безконтактних технологій «зв'язку на близькій відстані» (Near Field Communication /NFC/). Із зростанням обсягів мобільних платежів першочерговим є завдання забезпечення їх безпеки, а переваги, що надаються для вирішення цього завдання технологіями біометрії, є досить переконливими.

Не менш важлива інтеграція біометрики з технологіями NFC, які ще недавно видавалися екзотикою, а зараз переживають у своїй еволюції «переламний момент».

Отже, автори огляду знову підтвердили значення біометричних технологій як зручної та безпечної альтернативи паролям і PIN-кодам. Вони вважають, що сканувати відбиток пальця або проходити ідентифікацію за голосом власникам мобільних телефонів набагато комфортніше, ніж постійно згадувати та набирати різні буквенно-цифрові послідовності.

Третім напрямом розвитку «мобільних» біометричних технологій експерти «Goode Intelligence» назвали їхнє використання у складі систем багатофакторної ідентифікації. Це завдання стає особливо актуальним через збільшення хакерських атак, які часто завершуються успіхом.

Четвертий напрям – це застосування мобільних біометричних рішень у діяльності правоохоронних і силових структур, завдяки чому з'являється можливість практично негайно встановлювати особистість тих, до кого ці структури виявляють інтерес, наприклад, ідентифікація підозрілих осіб безпосередньо під час рейду поліцейського (міліцейського) патруля.

Проаналізувавши перспективи розвитку біометричних продуктів і сервісів для мобільних пристроїв, автори огляду особливо перспективними вважали засоби ідентифікації користувачів за відбитками пальців та їх голосами. Загалом, на думку експертів компанії, настав час переосмислити значення різних технологій у вирішенні завдань ідентифікації користувачів мобільних пристроїв та їх подальшої авторизації в різних IT-системах.

Якщо раніше мобільні пристрої в основному домінували в так званому «споживчому» сегменті (тобто застосовувалися приватними особами для вирішення тільки утилітарних завдань – телефонних дзвінків і т. д.), то вже збільшуються масштаби використання мобільних технологій у корпоративному секторі. Інакше кажучи, дедалі більше компаній видають своїм співробітникам мобільні пристрої або дозволяють працівникам користуватися своїми гаджетами в корпоративних системах. Ця тенденція спонукає на значно серйознішому рівні розглядати вищезгадані завдання безпечної та надійної ідентифікації й авторизації.

Саме біометричні технології дозволяють ефективно вирішувати завдання забезпечення безпеки під час дистанційного доступу до IT-систем або відповідних сервісів і проведення мобільних платежів із використанням NFC.

Необхідність застосування біометричних технологій у мобільних пристроях для забезпечення безпеки нині постійно зростає, тому автори огляду порівнюють

ситуацію з океанською хвилею – спочатку повільною та спокійною, але могутньою на своєму гребені[1].

Залишається лише дивуватися передбачливості фахівців із компанії «Goode Intelligence».

Оскільки вперше про інтеграцію мобільних пристроїв Apple (iPhone і iPod) зі сканерами відбитків пальців було оголошено ще у вересні 2010 року, то, втілення у майбутньому технології першого напряму можливо було передбачити, а от реалізація третього та четвертого напрямів у повному обсязі виглядала тоді деякою мірою фантастичною. Хоча інформація про те, що смартфони можуть стати наступною зброєю в арсеналі солдатів армії США, була відома ще в середині 2010 року.

Через півтора року після виходу в світ огляду «Goode Intelligence» з'явилось повідомлення про те, що Пентагон зацікавився мобільною мультибіометричною ідентифікацією за допомогою смартфонів. У лютому 2013 року Міністерство оборони США уклало з однієї з каліфорнійських фірм дворічний контракт на розробку апаратного й програмного забезпечення, призначеного для здійснення мультибіометричної ідентифікації за допомогою смартфонів.

Виконавець повинен представити замовникові «біометричний смартфон», який зможе розпізнавати людей за їхнім обличчям, райдужною оболонкою очей, голосом та відбиткам пальців.

Відстань ідентифікації за обличчям повинна становити два метри, а за райдужною оболонкою очей – метр. Розпізнавати чоловіка, який розмовляє, засіб мобільної біометричної ідентифікації повинен на відстані, яка є звичайною під час розмови телефоном; для ідентифікації за відбитками пальців людини, особистість якої встановлюється, необхідно буде торкнутися смартфона.

У технічному завданні до контракту акцентовано, що біометричний смартфон повинен мати можливість працювати за яскравого сонячного світла. Також до технічного завдання включений пункт, за яким біометричний смартфон повинен бути наділений здатністю самостійно, без участі користувача, формувати зображення біометричних ідентифікаторів для їхньої подальшої обробки.

У своїх коментарях щодо підписання нового контракту експерти вважають, що Пентагон поступово відмовляється від перебуваючих нині в експлуатації мобільних комплексів біометричної ідентифікації HIIDE. Насамперед від цих комплексів біометричні смартфони будуть відрізнятися за вагою, а також за можливостями керування. Висловлюються припущення, що найвірогідніше біометричні смартфони будуть функціонувати на платформі Android[2].

Крім розробки вищезазначених технічно-програмних рішень, необхідно вирішити завдання можливості підзарядки смартфонів у бойових умовах. Для цього вивчаються альтернативні джерела енергії, зокрема використання сонячних зарядних пристроїв і мікропаливних елементів.

Ще одним суттєво важливим чинником є швидкість передачі інформації в зв'язку з тим, що через смартфони планується передавати багато різної інформації – від чата та текстових повідомлень до відео. Але одним із головних питань під час розробки подібних

[1] Рынок биометрических решений для мобильных устройств будет активно развиваться // Biometrics.RU. – 2011. – 4 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Пентагон заинтересовался мобильной мультибиометрической идентификацией // Biometrics.RU. – 2013. – 18 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

пристроїв є шифрування – адже якщо такий смартфон потрапить до рук супротивника, то той не повинен мати змоги ним скористатися[1].

У вересні 2013 року експерти «Biometrics Research Group» зробили прогноз, що до 2020 року мобільними платежами будуть користуватися 700 млн людей, а обсяг відповідного сегмента фінансового ринку сягне 750 млрд доларів. Ця обставина повинна істотно пришвидшити запровадження в смартфонах біометричних рішень, які здатні гарантувати власникам таких пристроїв належний рівень безпеки під час проведення платежів.

За оцінкою авторів прогнозу, три чверті власників смартфонів взагалі не захищають свої пристрої навіть елементарним паролем. Для таких користувачів втілення у мобільні пристрої досягнень біометричних технологій стануть ідеальним рішенням, що обумовить їх вибір. Фахівці «Biometrics Research Group» пророкують, що в 2014 році обсяг продаж біометричних смартфонів може сягти 90 млн. На корпорацію «Apple», яка першою вивела на масовий ринок смартфон зі сканером відбитків пальців, припаде 78% від цього числа, «Samsung» задовольниться 17%, частка інших виробників буде становити лише п'ять відсотків ринку біометричних смартфонів[2].

Однією з найважливіших інновацій «Apple» є реалізація ідентифікації користувачів смартфонів за відбитком пальця. Але сканер відбитків у смартфонах – лише базис, на якому в майбутньому будуть ґрунтуватися нові функції на основі розробки «Touch ID». Поки що реалізовано дві дії: розблокування iphone і авторизація в itunes Store. Але це тимчасове обмеження, «Apple» планує дуже глибоко інтегрувати «Touch ID» в операційну систему.

У компанії дуже відповідально поставилися до виробництва лінз сканера: був вибраний один із найпрозоріших і твердих та досить дорогих матеріалів – сапфір. Лінза в складі сканера має першорядне значення. Якщо використовувати матеріал менш твердий, ніж сапфір, із часом якість сканування буде деградувати. Смартфон постійно зазнає всіляких впливів: пил, бруд, агресивне середовище (піт із рук, волога під час дощу), – усе це згодом дряпає лінзу і призводить до збільшення помилок під час ідентифікації[3].

За прогнозом експертів через 2–3 роки біометричні сканери будуть вбудовані у 30% всіх нових моделей смартфонів, а їх чисельність на ринку зросте більше ніж у п'ять разів.

Такий стан, на думку аналітіків «Gartner», пов'язаний із масовим захопленням офісних співробітників концепцією BYOD (Bring Your Own Device, тобто «принести власний пристрій»). Плюс конюмеризація в сфері IT-технологій, тобто доступ до корпоративних технологічних рішень для виконання робочих завдань співробітниками фірм і установ здійснюється за допомогою особистих пристроїв. Це може бути прив'язкою девайсів до корпоративної мережі, її віддалене використання, зокрема концепція впровадження особистих ноутбуків для роботи за системою BYOC (Bring Your Own Computer). Ідея конюмеризації ґрунтується на зручності використання особистого персоналізованого

[1] У Пентагона даже смартфоны станут биометрическими // Взгляд.ру. – 2011. – 6 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрические технологии в смартфонах и мобильных платежах: битва Apple и Samsung // Biometrics.RU. – 2013. – 24 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Ши Павел. Биометрические технологии в мобильных устройствах: почему Apple опережает конкурентов / Павел Ши // Appleinsider.ru. – 2013. – 5 нобря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

обладнання, і, як наслідок, підвищення ефективності роботи співробітників. Поняття робочого місця зі стаціонарним ком'ютером у приміщенні компанії перейде до персонального смартфона або планшета. Отже, обробка важливих корпоративних даних буде масово здійснюватися на особистих пристроях. Це відбувається тому, що працівникам так працювати краще.

Але така ситуація створює нову проблему. Стандартні системи інформаційної безпеки, що використовують громіздкі паролі та багатоступеневу аутентифікацію особистості до мобільних гаджетів не можуть бути застосовані. Проблема не в технічній частині, а в організаційній – хто ж захоче, щоб на його особистий смартфон системний адміністратор компанії ставив будь-який пароль, який можна у будь-який момент забути. Співробітники цінують зручність роботи з мобільними комунікаторами і тому, як вважають аналітики, у керівництва корпорацій не буде законних методів впливу на ситуацію. Єдиний засіб – в удосконаленні системи безпеки самих пристроїв, для чого біометричні технології підходять ідеально[1].

Компанія «Ericsson» наприкінці 2013 року провела опитування понад 100 тис. людей із 40 країн щодо визначення головного тренду 2014 року серед мобільних пристроїв. 74% респондентів вважають, що біометричні смартфони будуть головним трендом 2014 року[2].

Шведська компанія «Fingerprint Cards AB», яка займається розробкою біометричних електронних компонентів і технологій ідентифікації людських відбитків пальців, стверджує, що в 2014 році відразу декілька виробників смартфонів розмістять у своїх пристроях дактилоскопічні сканери, подібні до тих, що використовуються в iPhone 5S. Серед них будуть «Samsung», «LG», «Huawei» та деякі інші вендори. У корпорації «Samsung» (головного конкурента «Apple») незабаром мають з'явитися один чи два апарата з подібною технологією.

Завдяки сканеру відбитків пальців, який вбудований у кнопку Home на лицевій панелі, iPhone 5s може однозначно ідентифікувати свого власника. Ця функція, яка отримала назву Touch ID, застосовується для безпечного розблокування пристроя, а в майбутньому застосовуватиметься у процесі безпечного здійснення придбань в App Store або інтернет-магазинах[3].

Протягом 2013 року були чутки, що південно-корейський гігант планує встановити у свій флагманський пристрій Galaxy S5 сканер райдужної оболонки ока, але, за інформацією видання «The Korea Herald», фірма поки що вибрала дактилоскопічний сканер, як і в моделі «Apple» iPhone 5s. «Хто захоче підносити телефон до ока для аутентифікації, перебуваючи у кінотеатрі, за рулем авто або у ліжку вночі?» – таку відповідь дало одне з джерел сайту на питання про можливість використання сканера райдужної оболонки ока. Найімовірніше на впровадження сканера райдужки ока у мобільні пристрої потрібно буде два або три роки. Розробники подібних технологій «IriTech» та «Sambon Precision» говорять, що не співпрацюють із «Samsung»[4].

---

[1] Биометрический сканер получит каждый третий смартфон // Яблык.com. – 2014. – 7 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрические смартфоны – главный тренд 2014 года // Газета.Ru. – 2013. – 12 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрическая идентификация по отпечаткам пальцев будет популярна у производителей мобильных устройств // DailyComm. – 2013. – 9 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Samsung меняет модель биометрического сканера в новом смартфоне // DailyComm. – 2014. – 23 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Але у цієї технології є одна суттєва перевага. Такий спосіб ідентифікації має високу точність. Програмний алгоритм розпізнавання за технологією райдужної оболонки ока обраховує понад 2 тисячі крапок, які фіксуються на райдужці людського ока. А під час сканування за папілярними лініями пальця обрахунки здійснюються тільки за розположенням приблизно ста контрольних крапок. Також сканування райдужки виконується за допомогою камери з дуже високим розрішенням із використанням променів інфрачервоного спектра, що допомогає виокремити структуру райдужної оболонки ока. Для зловмисників така система невразлива, оскільки обдурити її за допомогою роздрукованого зображення людської райдужки неможливо.

Нині удосконалення цієї технології продовжується. Компанія «SRI International» розробила унікальний алгоритм, який уможливлює здійснення розпізнання унікального малюнка райдужки за низької освітленості, а також на відстані. Своє рішення для ідентифікації користувачів гаджетів, яке насамперед призначене для використання на споживчому ринку, запропонувала фірма «EyeLock». Досить цікавий варіант – своєрідний чохол для «яблучних» смартфонів iPhone 4 і 4S, який поєднує сканери і відбитків пальців, і райдужної оболонки ока, запропонувала приватна компанія «Aoptics».

Експерти підкреслюють, що однією з головних проблем на шляху використання біометричних датчиків у мобільних гаджетах є питання про недоторканість приватної інформації. Здійснити розпізнання райдужки, на відміну від папілярного узору, можно здалеку, зробивши це зовсім непомітно для людини. Як наслідок, свого часу під тиском громадської думки у Сполучених Штатах Америки відмовились від встановлення таких сканерів у аеропортах[1].

У грудні 2013 року було надруковане повідомлення про те, що корпорація «Apple» на додаток до існуючих своїх патентів отримала патент на технологію розпізнавання лиця особи для iPhone, iPad або iMac. Технологія дозволяє розпізнавати за характерними рисами лиця особи, текстурою шкіри, віддаленістю носа від рота та за іншими відмінностями обличчя. Якщо пристрій буде тримати в руках не його власник, то він не буде виводити повідомлення про e-mail і СМС, які надходять. А також не дозволить проглядати фото, що зберігаються у пам’яті, та заборонить доступ до деяких додатків.

У компанії «Apple» повідомляють, що під час вхідного дзвінка iPhone зможе «відчути», що хтось дивиться на екран. Якщо це не авторизований користувач, то дисплей не включиться.

Поки що невідомо, чи буде «Apple» впроваджувати нову технологію у свої розробки. Але експерти вважають, що патент досить вдало вписується в загальну концепцію розвитку продуктів цієї компанії[2].

Отже, як відомо, 10 вересня 2013 року компанія «Apple» представила нову модель смартфона iPhone 5S, яка оснащена вбудованим сканером відбитків пальців і за допомогою якого проводиться розблокування екрана та авторизація на фірмових сервісах. Дактилоскопічний датчик під назвою Touch ID поки що встановлюється тільки в смартфонах iPhone 5S, але якщо ідея виявиться вдалою, то він з’явиться й у наступних моделях iPhone, а також у планшетах iPad і плеєрах iPod touch.

Цілком зрозуміло, що для користування датчиком доведеться знімати рукавички (інакше сканер просто не зможе «побачити» папілярні візерунки) – це загальновідомий

[1] Биометрические технологии в мобильных устройствах: проблемы и перспективы // B2BLogger.com. – 2014. – 28 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Очередной биометрический патент появился у корпорации Apple // МИР 24. – 2013. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

факт, і тут не допоможуть навіть спеціальні рукавички для роботи з ємнісними екранами. Невтішний факт для Росії й України, де зима триває досить довго і де без рукавичок інколи просто неможливо вийти на вулицю.

У програмі Touch ID закладені добре перевірені способи ідентифікації, які давно використовуються у базах даних правоохоронних органів і криміналістичних лабораторій. Зокрема, папілярні візерунки класифікуються за трьома основними видами – дуговим, петльовим і завитковим, причому під час розпізнавання певним чином ураховуються можливі дефекти. За деякими повідомленнями, система Touch ID сканує зовсім не ті частини пальців, які звичайно залишаються як відбитки на різних поверхнях. Це суттєво ускладнює завдання зловмисників, які будуть намагатися скористатися відбитками, залишеними зокрема й на самому смартфоні. Інформація щодо відбитків пальців шифрується та зберігається у захищеній пам'яті процесора A7, причому, як стверджують розробники, вона доступна тільки для датчика Touch ID, і жодні програми або сервіси «Apple» не можуть звертатися до цих даних або зберігати їх. Особливо важливою рисою є те, що відбитки зберігаються в пам'яті не у вигляді зображень, а у вигляді цифрового шаблону, тому, на відміну від більшості сучасних дактилоскопічних сканерів, система Touch ID буде кожен раз оцифровувати відбиток зображення, що знімається з вашого пальця, порівнюючи його з еталонним шаблоном.

Відомості про відбитки пальців, які зберігаються в iPhone 5S, можуть використовуватися не тільки для розблокування смартфона, але й для авторизації покупок в itunes і App Store, повністю замінюючи введення відповідних паролів. В «Apple» поки що принципово не мають наміру розширювати сферу використання Touch ID, обмеживши її тільки власними сервісами, щоб не ставити під удар безпеку всієї системи.

Як додатковий засіб безпеки під час використання системи Touch ID користувачеві пропонується ввести спеціальний пароль, який буде потрібен для розблокування телефону в разі його перезавантаження або якщо апарат не був розблокований упродовж 48 годин. У цих випадках одержати доступ до iPhone 5S за ідентифікацією візерунків пальця буде неможливо. Як тільки стало відомо про намір «Apple» вмонтувати в новий iPhone сканер відбитків пальців, у багатьох спостерігачів виникли побоювання, що таким способом планують зібрати базу даних «пальчиків» своїх клієнтів, яка буде зберігатися десь на серверах компанії. Але у відеоролику на сайті «Apple» старший президент фірми з апаратного забезпечення Ден Річчіо спеціально наголошує, що дактилоскопічні відомості зберігаються в зашифрованому вигляді у спеціальній безпечній частині процесора A7 і до них має доступ тільки датчик Touch ID. Ця інформація не може бути зчитана за допомогою іншого програмного забезпечення і ніколи не потрапить ні на сервери «Apple», ні в «хмарне» сховище iCloud.

Підсумовуючи вищенаведене, можна стверджувати, що немаючи досвіду експлуатації, iPhone 5S з системою Touch ID, поки що доволі складно однозначно вказувати і на переваги такого смартфона, і на його недоліки. З одного боку, дактилоскопічний датчик спрощує захист апарата від несанкціонованого доступу та робить більш комфортними покупки в iTunes і App Store. З іншого – тепер неможливо використовувати смартфон у рукавичках, а головне, – це обґрунтовані сумніви щодо безпеки транзакцій через Інтернет. Загалом про позитивні та негативні оцінки цього експерименту поки що говорити зарано[1].

[1] Нечай Олег. Биометрический сканер в iPhone 5S: факты и оценки / Олег Нечай // Компьютерра-Онлайн. – 2013. – 13 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

6.11. Використання біометричних технологій у виборчих системах світу

В Україні після кожних виборів лунають звинувачення в використанні нечесних технологій під час проведення цього заходу. Партійні сили різної орієнтації обвинувачують одна одну в махінаціях:

– розкраданні персональних даних виборців;

– організації так званих «карусельних» махінацій, зокрема з незаконним використанням «голосів» громадян, які через різні причини не взяли участь у голосуванні;

– наявності «мертвих душ»;

– «непрозорості» системи підбиття підсумків голосування загалом.

Експерти однозначно стверджують, що коли біометричні технології широко використовуються в понад 100 країнах світу, застосування біометрії є одним із найефективніших і найнадійних засобів для забезпечення прозорості виборів і чесного підбиття підсумків голосування. А це, своєю чергою, буде сприяти підтримці миру й злагоди, які в іншому випадку можуть бути порушені виступами різних політичних партій та їх прихильників, обурених можливим підтасуванням під час підрахунку голосів.

Також для того, щоб успішно організувати виборчий процес, необхідно мати чіткий і точний список виборців, а також єдиний бюлетень, який неможливо підробити.

Біометричні системи, що дозволяють розпізнавати кожну людину за унікальними, характерними тільки їй ідентифікаційними даними, дозволяють реалізувати на практиці принцип «одна людина – один голос». Додатковими перевагами застосування біометрики також є пришвидшення процесу волевиявлення та підрахунку голосів.

Але перед тим, як проводити кампанію з біометричної ідентифікації громадян, які мають право голосу, необхідно створити єдиний державний демографічний реєстр громадян країни. Єдиний демреєстр є основою для видачі та функціонування біометричних документів. Нині подібні реєстри успішно функціонують (і водночас дозволяють ефективно заощаджувати бюджетні кошти) у багатьох державах світу: Швеції, Бельгії, Голландії, Данії, Великобританії, Іспанії, Люксембурзі, Португалії, Франції, Німеччині, Греції, Італії, Фінляндії, Швейцарії, Литві, Латвії, Естонії, Кенії та ще у багатьох інших країнах.

Нагадаємо, що 29 листопада 2012 року Президент України підписав закон України «Про Єдиний державний демографічний реєстр і документи, які підтверджують громадянство України, засвідчують особистість або її спеціальний статус», який офіційно набув чинності.

Закон передбачає створення бази даних українців і осіб без громадянства, а також видачу низки посвідчень з електронним чіпом, які засвідчують особистість власника. На думку експертів і політиків, реформа має для країни та громадян низку переваг, одна з яких – захист персональних даних і можливість ефективної боротьби зі злочинністю та шахрайством[1].

У парламентах деяких країн запроваджені системи біометричної ідентифікації. Наприклад, у парламенті Болгарії введена система голосування, у якій ідентифікація поданого голосу здійснюється за відбитком пальця. У разі незбігання відбитка пальця члена

[1] Биометрические технологии идеальны для обеспечения прозрачности выборов // Багнет. – 2012. – 14 декабря. [Электронный ресурс]. – Режим доступа: http://www.bagnet.org/news/tech/...

парламенту, котрий голосує з наявним взірцем, закладений у пам'ять системи, цей голос не зараховується. Введення такої технології подолало негативну практику, коли один присутній член парламенту голосував за багатьох відсутніх народних обранців[1].

Наведемо неповний перелік країн, де застосовуються або запроваджуються технології біометричної ідентифікації громадян, які мають право голосу на виборах. Це такі країни, як: Бенін, Бразилія, Буркіна-Фасо, Венесуела, Габон, Гана, Гвінея, Грузія, Замбія, Індонезія, Камерун, Кенія, Колумбія, Кот-д'Івуар, Малаві, Малайзія, Малі, Непал, Нігерія, Океанія, Пакистан, Сенегал, Сьєрра-Леоне, Соломонові острови, Танзанія і Занзібар (Занзібар – архіпелаг в Індійському океані, що належить Танзанії), Того, Фіджі, Філіппіни і частково у Південному Судані. Публікації про необхідність запровадження технологій біометричної ідентифікації громадян інколи з'являються і в інших країнах, які не вказані у переліку. Зокрема, вони були опубліковані в Росії та США. А система голосування, яка була розроблена у Росії, пройшла випробування в Еквадорі. У Південно-Африканській Республіці (ПАР) систему біометричної ідентифікації планується запровадити у парламенті.

Наведемо найцікавіші особливості впровадження у виборчі системи низки держав технологій біометричної ідентифікації.

По-перше, необхідно мати актуальний список виборців. У ньому потрібно зафіксувати їх основні персональні дані, цифрові фотографії осіб та інформацію хоча б ще про один біометричний показник. Практично у всіх країнах у вибочих біометричних системах, крім оцифрованих фото, як додатковий біометричний показник використовують відбитки пальців, а лише в деяких – райдужну оболонку ока. Застосування технологій біометрії дозволяє уникнути внесення до реєстру повторних відомостей про одного і того ж виборця – як відомо, біометричні ідентифікатори унікальні для кожної людини, їх не можна «позичити». Акцентуємо, що в списку мають бути перевірені точні та однозначні відомості щодо виборців. Нині у світі використовуються два підходи до реєстрації виборців. Перший – попередня реєстрація виборців без видачі ID-карт. Другий – видача внутрішніх біометричних посвідчень особи, які використовуються як аспорти чи для інших призначень (наприклад, для вирішення податкових і фінансових питань, як водійські посвідчення, під час безпосередньої реєстрації виборців тощо).

Наведемо приклад багатоцільового використання біометричних посвідчень особи. 2010 року в Індонезії був розпочатий проект, за яким 172 млн громадян мали одержати нові біометричні посвідчення особи. Проект оцінюється в 600 млн доларів, а завершити його заплановано до виборів 2014 року. Біометричні посвідчення в Індонезії, що отримали назву Kartu Tanda Penduduk Elektronik (e-KTP), повинні замінити індонезійцям паспорти, посвідчення виборців і платників податків; передбачається, що за допомогою e-KTP громадяни зможуть також одержувати доступ до послуг соціального страхування.

У спеціальних реєстраційних центрах у громадян Індонезії знімають відбитки пальців і райдужної оболонки ока та фотографують обличчя. Особиста інформація зберігається в державних базах даних. Загалом у країні відкрито понад 7 тис. пунктів видачі посвідчень, у яких працює 72 тис. співробітників. Населення Індонезії перевищує 237 млн чоловік, а говорять вони більш ніж на 700 різних мовах[2].

---

[1] Биометрическая система начала действовать в парламенте Болгарии // Novinite.ru. – 2013. – 14 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Индонезия. Биометрические ID-карты получат 172 миллиона человек // Открытые системы. – 2012. – 24 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...; Индонезия. Выпуск биометрических идентификационных карт: новые подробности // BIOMETRICS.RU. – 2013. – 24 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

У стандартному варіанті кожна виборча дільниця повинна бути оснащеною електронними журналами для реєстрації громадян, які проголосували, та лептопами з підключеними до них сканерами відбитків пальців. Перед тим, як одержати виборчий бюлетень, громадянинові потрібно торкнутися сканера та пройти біометричну ідентифікацію, щоб підтвердити той факт, що в день виборів він ще не голосував[1].

За наявності у громадян ID-карт можливий алгоритм дій під час голосування виглядає так. Прийшовши на виборчу дільницю, виборець пред'являє свою карту та сканує відбитки пальців. Біометрична система в автоматичному режимі порівнює відомості про біометричні ідентифікатори, що зберігаються в пам'яті картки, з інформацією про знов відсканові відбитки пальців, і, якщо вони збіглися, особистість виборця вважається підтвердженою і він одержує бюлетень. Під час процесу біометричної ідентифікації виборця можуть брати участь представники різних політичних партій, які контролюють процес голосування на дільницях[2].

Звісно, ще бажана перевірка за загальним реєстром виборців або ведення єдиного в країні електронного журналу осіб, які проголосували, щоб уникнути можливості голосування за іншим місцем проживання. На виборчих дільницях слід передбачити дії у разі виникнення нестандартних ситуацій. Це може бути і відмова електроживлення, і відмова біометричного обладнання.

Розглянемо запровадження біометричної виборчої технології на прикладі Філіппін. У листопаді 2012 року сенат Філіппін (верхня палата парламенту цієї держави Південно-Східної Азії) ухвалив закон про біометричну ідентифікацію виборців (так званий «Білль 1030»). Відповідно до цього закону, громадяни, які мають право голосу, повинні проходити цифрове фотографування, сканувати відбитки пальців і залишати у відділеннях «Comelec» зразки своїх підписів. Завершити біометричну ідентифікацію виборців планується до травня 2016 року, коли на Філіппінах мають відбутися наступні вибори.

У лютому 2013 року Виборча комісія Філіппін оприлюднила кількість громадян, які зареєстрували свої біометричні ідентифікатори. Їх чисельність становила 52 млн людей[3].

Як бачимо, від ухвалення закону про біометричну ідентифікацію виборців у Філіппінах до початку виборів мине трохи більше чотирьох років. Україна, населення якої становить менше 45,5 млн осіб, може запозичити досвід цієї держави Південно-Східної Азії. Загальна кількість громадян, які мають право голосу в нашій країні, згідно з державним реєстром виборців станом на 31 січня 2014 року, становить 36552415 осіб[4].

Детальніше розглянемо ідею запровадження системи біометричної ідентифікації у парламенті Південно-Африканської Республіки (ПАР).

---

[1] Кения: мартовские выборы пройдут с применением биометрических технологий // BIOMETRICS.RU. – 2013. – 25 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Избиратели Малайзии будут проходить биометрическую идентификацию // BIOMETRICS.RU. – 2011. – 13 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Филиппины: биометрическую идентификацию прошли 52 миллиона избирателей // BIOMETRICS.RU. – 2013. – 13 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Відомості про кількість виборців в межах Автономної Республіки Крим, областей, міст Києва та Севастополя, закордонного виборчого округу (відповідно до частини 5 статті 30 Закону України «Про Державний реєстр виборців») // Державний реєстр виборців. – 2014. – 31 січня. [Електронний ресурс]. – Режим доступу: https://www.drv.gov.ua/portal/...

Передбачено, що у новій системі будуть використовуватись дві інноваційні технології. Позначки радіочастотної ідентифікації (RFID) застосовуватимуться для фіксації факту прибуття депутата до зали засідання або на збори парламентського комітету, у якому він перебуває. Це дозволить уникнути черг під час проходу до приміщень парламенту в так званий час пік. Що ж стосується біометричних технологій, то з їхньою допомогою відстежуватиметься час, проведений депутатом на «службі народу» та його участь у процедурі голосування.

Подібний підхід до застосування біометрії є розумним. Якщо носій RFID-мітки (ту ж карту для голосування) депутат-прогульник зможе передати колезі або помічникові, то з біометричними ідентифікаторами цього зробити не вдасться.

Очікується, що ідентифікація парламентаріїв буде здійснюватися за технологією сканування відбитків пальців. Вартість біометричної системи становитиме приблизно 50 тис. доларів США. Її введення заплановане на 2014 рік, після того, як громадяни ПАР виберуть новий склад парламенту[1].

Підсумовуючи вищезазначене, автори вважають, що в Україні настав час для ухвалення рішення щодо запровадження біометричних технологій у виборчу систему та в діяльність Верховної Ради (ВР). Ці інноваційні технології дозволять уникнути різних махінацій під час проведення виборів і зробити їх більш прозорими. Що ж стосується голосування у ВР, то нарешті повністю буде реалізовано на практиці принцип «один депутат – один голос».

[1] Биометрическая система появится в парламенте ЮАР // BIOMETRICS.RU. – 2013. – 5 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розділ 7

МАЙБУТНЄ БІОМЕТРІЇ. СХВАЛЕННЯ ГРОМАДСЬКОЮ ДУМКОЮ ВИКОРИСТАННЯ СУЧАСНИХ ДОСЯГНЕНЬ БІОМЕТРІЇ

Одна з найпопулярніших тем останніх років у галузі технологій безпеки – біометрична ідентифікація.

Років двадцять п'ять–тридцять тому головними споживачами біометричних методів ідентифікації були в основному правоохоронні структури та спецслужби. Але останніми роками біометричні методи ідентифікації і верифікації набули значного поширення у різних системах безпеки та контролю доступу, причому досягнення біометрії дедалі більше використовуються для забезпечення безпеки різних інформаційних мереж і систем, зокрема й баз даних.

Наведемо декілька прикладів практичного втілення найбільш значущих біометричних проектів за останні роки, які реалізуються світовою спільнотою й окремими державами:

– Організація Об'єднаних Націй (UN/ООН), Міжнародна організація цивільної авіації (ICAO/ІКАО), Міжнародна організація зі стандартизації (ISO/ІСО): а) програма машинозчитуваних транспортних документів (електронних або біометричних паспортів), видачу яких повинні були розпочати до 2010 року майже всі країни світу для своїх громадян під час їх виїзду за кордон.

– Країни Шенгенської зони та інші держави-члени Євросоюзу:

а) загальноєвропейська система біометричної ідентифікації за відбитками пальців EURODAC (європейська база даних про відбитки пальців здобувачів статусу біженця й іноземців, які нерегулярно перетинають границі держав Євросоюзу);

б) візова інформаційна система (Visa Information System /VIS/, у якій акумулюються відомості про відбитки пальців здобувачів шенгенських віз);

в) шенгенська інформаційна система нового покоління (Schengen Information System /SIS II/, що містить, зокрема, інформацію про біометричні ідентифікатори осіб, які перебувають у розшуку, пропали безвісті або ж чиє перебування в зоні Шенгена небажане)[1].

г) Великобританія, Португалія, Іспанія – програми видачі внутрішніх біометричних ідентифікаційних карт громадянам цих держав.

– США:

а) програма US VISIT, яка вимагає безумовну біометричну ідентифікацію всіх претендентів на отримання американських віз (з реєстрацією відбитків усіх 10 пальців рук);

[1] Объем мирового биометрического рынка к 2017 году превысит 16 миллиардов долларов // BIOMETRICS.RU. – 2011. – 17 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

б) президентська директива з національної безпекти (HSPD, яка зобов'язує всіх державних службовців і працівників установ, які працюють за державними контрактами, мати біометричні ідентифікаційні картки)[1];

в) Пентагон оголосив про створення найбільшої біометричної «системи систем», що об'єднує всі бази біометричних даних, які раніше відокремлено формувалися різними структурами Міністерства оборони США.

Із 2010 року Європейський союз (ЄС) починає запроваджувати процедуру зняття відбитків пальців гостей (на в'їзді й виїзді) у всіх країнах співтовариства (станом на 01.02.2014 року 28 держав-членів блоку). Отримані дані повинні вноситися до спеціальної електронної бази. Цей захід має сприяти зміцненню безпеки і зменшити потік нелегалів до країн, що входять в ЄС.

Подібна процедура, що охоплює сканування відбитків пальців і райдужної оболонки ока, вже тривалий час використовується на кордонах і в аеропортах США. Процедура збору біометричних даних здійснюється або вводиться практично всіма розвинутими країнами світу щодо осіб, які перетинають державні кордони. Нині такі заходи під час перетинання державних кордонів застосовуються тією чи іншою мірою у 111 країнах світу. На думку представників силових структур, які забезпечують державну безпеку, всі ці процедури контролю мають сприяти захисту прав особистості, протистояти можливим фальсифікаціям паспортно-візових документів, полегшити роботу організацій, які займаються справами іммігрантів і біженців, спростити процедури перетинання кордонів держав або об'єднань держав[2].

Завдяки бурхливому розвиткові біометричних технологій у XXI сторіччі біометрика застосовується не тільки у криміналістичній галузі, а й у найрізноманітніших сферах суспільного життя:

– персоніфікації доступу до операційних систем і локальних обчислювальних мереж, а також під час підтвердження особистості користувачів комп'ютерних програм там, де потрібне здійснення процедури авторизації;

– аутентифікації під час доступу до Web-ресурсів;

– встановленню конкретної фізичної особи в системах контролю за доступом;

– обліку робочого часу персоналу підприємств та установ;

– реєстрації та ідентифікації клієнтів (сейфових депозитаріїв, відвідувачів різних елітних клубів тощо);

– підтвердженні особистості клієнтів під час проведення електронних платежів;

– запровадженні соціальних проектів, які вимагають процедури ідентифікації («електронне урядування», біометричні системи голосування, добродійні акції та ін.);

– під час здійснення процедури ідентифікації або верифікації у різних державних і міжнарожних проектах (оперативній перевірці осіб, контролю під час перетинання державних кордонів, видачі віз тощо).

Основними складовими будь-яких біометричних систем є різні комбінації зі сканувальних пристроїв, спеціалізованих серверів і відповідного програмного забезпечення для виконання конкретних алгоритмів порівняльних дій.

Архітектура рішення у кожному випадку залежить від вимог, які пред'являються до системи з метою досягнення потрібного степеня захищеності інформації, наявної

[1] Массовая идентификация // Biolink.ru. – 2008. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/...

[2] Все государства Евросоюза могут ввести биометрическую идентификацию иностранцев, прибывающих из-за пределов ЕС. – 2008. – 28 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

кількості шаблонів або оригіналів зображень, що зберігаються у базі даних, необхідного числа порівнянь за одиницю часу (швидкодії), пропускної спроможності каналів зв'язку та потрібної централізації адміністрування[1].

Компанія «Strategic Defence Intelligence» у своєму огляді надала прогноз застосування біометричних технологій різними державними структурами у 2014–2024 роках. Фахівці висловили думку, що у вказаному періоді обсяг відповідного сегмента галузевого ринку буде щорічно збільшуватися на 6,88%. Загалом обсяг глобального ринку до 2024 року повинен сягти 56,1 млрд доларів[2].

16,7 млрд доларів – таким буде обсяг світового біометричного ринку в 2019 році за даними компанії «Wintergreen Research». Порівняно з 2012 роком, коли згаданий показник становив 5,2 млрд доларів (дані «Wintergreen Research» – *авт.*), обсяг світового ринок біометрії за сім років зросте більш ніж у три рази. Аналітики компанії вважають, що збільшення використання біометричних систем буде зумовлено прагненням мінімізувати загрози глобальній безпеці, потребою більш ефективної протидії атакам терористів, зменшення рівня злочинності, забезпечення надійного захисту аеропортів та інших транспортних вузлів.

Свій вклад у збільшення застосування біометрії внесуть розширення програм використання біометричних паспортів та ID-карт, необхідність видачі біометричних водійських посвідчень, масового запровадження біометричних систем прикордонного контролю[3].

2013 року компанія «Techsci Research» опублікувала своє дослідження щодо розвитку світового біометричного ринку. Експерти «Techsci Research» перспективи розвитку світової біометрії оцінюють ще більш оптимістично, ніж їх колеги з «Wintergreen Research». Автори дослідження вважають, що до 2018 року обсяг цього ринку зможе сягти 20 млрд доларів.

У публікації виокремлені такі ключові сфери застосування біометрії: суспільна безпека, прикордонний контроль, національні ідентифікаційні документи та біометричні паспорти, захищений доступ до корпоративних мереж і онлайнових ресурсів, банківсько-фінансовий сектор. Як бачимо, перелік основних напрямів-«локомотивів» застосування біометрики в 2014–2019 роках у цих двох дослідженнях збігається.

Що стосується географічних аспектів, то в 2012 році 61% від загального обсягу глобального біометричного ринку припадав на країни Європи та Північної Америки. У технологічному розрізі лідерство продовжує міцно втримувати ідентифікація за відбитками пальців. Але незабаром, на думку авторів прогнозу, дуже швидкими темпами будуть еволюціонувати Vein Recognition Technology – технології розпізнавання користувачів за малюнком вен[4].

У тому ж 2013 році ще одна фірма – «Research and Markets» – надала свій аналіз розвитку світового біометричного ринку. Аналітики спрогнозували, що на початок 2014 року загальний обсяг цього ринку може становити 10,02 млрд доларів.

---

[1] Системы идентификации личности по отпечатку пальца – средства и сферы применения // НТП «САРТ». [Электронный ресурс]. – Режим доступа: http://www.sart.must-ipra.com

[2] Правительственные структуры станут еще активнее использовать биометрические технологии // BIOMETRICS.RU. – 2014. – 22 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Новый оптимистический прогноз развития биометрического рынка // BIOMETRICS.RU. – 2013. – 12 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Мировой биометрический рынок: новый прогноз развития // BIOMETRICS.RU. – 2013. – 25 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Як бачимо, опубліковані дані всіх наведених досліджень передбачають подальше зростання обсягу світового біометричного ринку – розбіжності тільки у його абсолютній величині.

Зростання використання біометричних технологій зумовлене дією трьох важливих чинників. *По-перше*, користувачі більше не можуть миритися з незручністю й обмеженими можливостями, що їм надають паролі й PIN-коди. *По-друге*, неприйнятність та уразливість паролів і PIN-кодів особливо відчувається в умовах зростання активності терористів і хакерів, тому біометричні технології стають органічною частиною систем захисту інформації, розмежування фізичного доступу та забезпечення безпеки фінансових транзакцій. *По-третє*, продовжується реалізація масштабних біометричних проектів (видача біометричних паспортів та ID-карт у багатьох країнах світу, подальший розвиток автоматичного прикордонного контролю та візових систем, здійснення в Індії програми біометричної ідентифікації 1,2 млрд громадян цієї країни).

Реалізація всіх перелічених чинників і сприяє стрімкому подальшому розвитку біометричної галузі[1].

Останнім часом у світому співтоваристві спостерігається зростання інтересу урядових структур різних країн до використання біометричних технологій у програмах створення «електронного уряду» («Е-уряду»). Ця ідея виникла ще в 90-ті роки минулого століття, коли низка розвинутих держав почали здійснювати роботи для її реалізації. Загальновизнаним світовим лідером у сфері розробки і застосування інноваційних технологій «електронного урядування» є Канада.

Ще у 1994 році урядом країни був випущений «Проект надання послуг державними органами за допомогою інформаційних технологій», що отримав умовну міжнародну назву «E-government». Також світовими лідерами в розвитку систем «Е-уряду» є Сінгапур і США. Саме ці три країни мають найбільшу кількість урядових веб-сервісів (систем для здійснення електронних платежів, подачі податкових декларацій, проведення голосувань тощо), що мають ретельно продуманий інтерфейс із погляду зручності для клієнтів.

2000 року керівництво Європейського Союзу поставило завдання створити в Європі одну з конкурентоздатних і динамічних економік світу й оголосило про десятирічний план економічних реформ (так звана «Лісабонська стратегія») та, відповідно, програму дій із формування «Електронної Європи» шляхом використання можливостей «нової економіки» та інформаційних технологій. Із цього часу однією з обов'язкових умов до країни-кандидата на вступ у ЄС є забезпечення стабільного зростання ІТ-інфраструктури в державі.

Нині у більшості розвинутих країн створені багатофункціональні центри надання державних послуг за принципом дії «одного вікна», який є одним із перспективних каналів взаємодії держави і громадян. Такі центри успішно функціонують у Великобританії, Німеччині та Бразилії[2].

Система, в рамках якої реалізується ідея електронного уряду, повинна самостійно ідентифікувати користувача, автоматично визначати перелік послуг, на які він має право, і надавати юридично важливі послуги. Отже, без вирішення питання про аутентифікацію

---

[1] Объем биометрического рынка к 2014 году превысит 10 миллиардов долларов // BIOMETRICS.RU. – 2013. – 1 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Хохлова Н. Мировые «электронные правительства» идут по пути «одного окна» / Н. Хохлова. – 2008. – 14 октября. [Электронный ресурс]. – Режим доступа: http://www.cnews.u/reviews/free/...

користувачів за допомогою біометричних технологій електронний уряд практично сформувати неможливо.

Система «Е-уряд» є програмою надання державних послуг, а використання можливостей Інтернету сприяє розширенню участі громадян в управлінні через використання системи «Електронного голосування», що є інтегральним показником розвитку системи «E-government» і характеризує рівень електронної демократії (E-democracy).

Для економії коштів у державах Євросоюзу реалізація програми «Електронного уряду» об'єднана з практичним впровадженням програм «Електронний паспорт», «Електронна митниця» і «Електронне голосування». Всі ці програми в принципі повинні або використовують загальні ресурси, стандарти, рішення забезпечення інформаційної безпеки, установчі відомості, зокрема і біометричні дані громадян[1].

Як приклад втілення в життя зазначеної тенденції можна навести факт, що за підсумками 2007 року Уряд Російської Федерації надав відповідне доручення на коректування Федеральної цільової програми «Електронна Росія» для її структуризації навколо низки таких значних національних проектів, що вже реалізовувалися: «паспорт нового покоління», «соціальна карта» та інші (протокол засідання Уряду від 13 березня 2008 року № 10, розділ II, пункт 7)[2].

Перші універсальні електронні карти (УЕК), які були випущені обмеженим тиражем, мали з'явитися в пілотних регіонах Російської Федерації (РФ) ще в серпні 2012 року. Якщо у 2010 році на Петербурзькому економічному форумі проект УЕК обговорювався лише з позиції «бути або не бути», то зараз експерти практично одночасно заявили – карти потрібні, а їх можливості фактично безмежні.

Насамперед карта повинна стати універсальним засобом одержання держпослуг у будь-якому регіоні країни. За її допомогою планують виплачувати всі соціальні та пенсійні виплати. У цьому відношенні вона стане аналогом діючої в низці регіонів (наприклад, у Москві) «соціальної карти», тільки з можливістю використання в будь-якій частині Росії.

Крім того, картка повинна стати засобом платежу. Як обіцяв президент ВАТ «УЕК» Микола Ульянов (компанія-оператор проекту, акціонерами якої стали банки «Сбербанк», «Уралсиб» і «Ак Барс»), відповідне законодавче забезпечення має бути невдовзі сформовано. На час публікації інформації у проекті брали участь вісім кредитних організацій, а власник карти мав право вибору банку, з яким йому було зручніше співпрацювати.

Автори проекту передбачають, що незабаром може розпочатися «фантастика». Вони вважають, що технологія дозволить «включити» до карти необмежену кількість послуг, які необхідні громадянам, зокрема такі, як права водія, пенсійне посвідчення і так далі. У перспективі УЕК може стати універсальним документом, який дозволить ідентифікувати громадян. Тобто стати дублером «паперового» паспорта, повністю від якого відмовитися не вдасться через відсутність на території Росії необхідної інфраструктури для сканування карток і передачі даних[3].

---

[1] Мартиненко С. Сучасні програми розвитку Е-Уряду. Аналітичний огляд / С. Мартиненко. – 2005. – березень. [Електронний ресурс]. – Режим доступу: http://www.itsway.kiev.ua/index…

[2] Федеральную целевую программу «Электронная Россия» переориентируют на развитие системы биометрических паспортов // Министерство экономического развития Российской Федерации. – 2008. – 18 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

[3] В универсальные электронные карты россиян могут включить данные об их биометрических идентификаторах // БалтИнфо. – 2012. – 25 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Нині у великих містах світу відбувається революція в міському відеонагляді за громадськими місцями. А у Великобританії вона практично вже відбулася. Сучасне інтелектуальне відеоспостереження ґрунтується на аналізі даних за допомогою складних алгоритмів, які забезпечують розпізнання особистості з доволі високою часткою ймовірності, водночас значною мірою допомагаючи тим, хто займається проблемами безпеки.

Зараз розроблені малогабаритні оптичні прилади великої дальності дії, що забезпечують можливість спостереження на такій відстані, яка раніше була недосяжною для портативних відеопристроїв.

Можливості цих пристроїв підсилені такими рішеннями, які зменшують негативний вплив туману, дощу і світлових бліків, що супроводжують операції відеонагляду на великій відстані. Отримане зображення передається за допомогою спеціальних каналів, які можуть включати мікрохвильові відеолінії з дальністю дії до одного кілометра, що дозволяє знизити потребу в обслуговуючому персоналі[1].

Цифрові технології дозволили створювати тимчасові замкнуті відеотелевізійні системи, які також можна розглядати як частину внутрішньої стратегії безпеки. Такі інтегровані системи дозволяють спрямовувати об'єктиви відеокамер на різні ділянки, що сприяє забезпеченню додаткового перегляду місця події відповідно до потреб, що виникли. Під час здійснення відеозапису проставляється дата запису, а сигнали тривоги та зображення передаються на необхідний монітор і навіть існує можливість передачі на конкретний мобільний телефон.

До сфер людської діяльності, де застосування біометрії особливо набуло масового характеру, вналежить повітряний транспорт, точніше забезпечення безпеки польотів. Аеропорти – найважливіші транспортні вузли, «форпости» внутрішніх і зовнішніх комунікацій. Забезпечення безпеки їх інфраструктури посідає важливе місце у протидії тероризму, міжнародній злочинності, нелегальній міграції. Комплексна безпека пасажирів і вантажів, ефективне регулювання їх потоків, активне використання можливостей, які надають паспортно-візові документи нового покоління з біометричними даними, – це ще не повний перелік завдань, що формують пріоритети у діяльності аеропортів.

Ця діяльність надзвичайно складна та багатоаспектна. Щодня аеропорти обслуговують велику кількість авіапасажирів, а, крім пасажиропотоку, додаткові потоки формують обслуговуючий персонал, співробітники авіакомпаній, екіпажі літаків, а також зустрічаючі або проводжаючі. В аеропортах здійснюється митний огляд і прикордонний контроль, безперебійну роботу транспортних вузлів забезпечують великі та малі інформаційні системи. Для надійної роботи всіх складових багатоаспектної діяльності повітряних портів потрібний надійний контроль за доступом у службові приміщення та режимні зони аеропортів.

Саме тому активне застосування новітніх технологій контролю й управління за доступом в аеропортах є нагальною вимогою часу. Системи біометричної ідентифікації є важливою складовою цих технологій, які масово застосовуються або впроваджуються в аеропортах практично всіх країн світу. Основні завдання, що вирішуються у діяльності аеропортів за допомогою біометрії такі:

– забезпечення комплексної безпеки пасажирів й авіаперевезень;

– підвищення комфортності та пришвидшення обслуговування пасажирів у аеропортах (без зменшення рівня режиму безпеки);

[1] Технические средства защиты от террористических угроз // Ежемесячный информбюллетень. – Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 1. – М.: ВИНИТИ. – С. 23–26.

– розмежування доступу персоналу в службові приміщення та режимні зони аеропортів;

– проведення оперативної ідентифікації пасажирів, персоналу та інших осіб, що перебувають на території аеропорту;

– забезпечення захисту інформації, яка обробляється у корпоративних мережах аеропортів, управляючих компаній, компаній-перевізників;

– облік робочого часу персоналу аеропортів[1].

Наведемо приклад експерименту з застосування біометричних технологій, що проходив у 2013 році на одному з терміналів лондонського аеропорту Хітроу. Для пришвидшення посадки авіапасажирів на борт повітряного судна випробовувалася технологія ідентифікація за рисами обличчя особи.

Алгоритм дії нової біометричної системи досить простий. Під час реєстрації пасажира на стійці авіакомпанії його лице сканується. Повторна біометрична ідентифікація здійснюється під час наближення пасажира до «воріт самообслуговування»: якщо знову отриманий скан особи співпаде з раніше зареєстрованим, перед пасажиром відкривається турнікет і йому дозволяється посадка на борт літака.

Організатори експерименту вважають, що його реалізація пришвидшить процес посадки на борт повітряного судна та дозволить вивільнити час співробітників аеропорту для роботи з тими авіапасажирами, «що потребують додаткової допомоги та уваги».

Під час недавнього опитування трьох тисяч авіапасажирів із 110 країн світу, проведеного Міжнародною асоціацією повітряного транспорту, 77% респондентів заявили, що будуть почувати себе більш комфортно, якщо скористаються в аеропортах перевагами біометричних технологій[2].

На початку 2004 року міжнародна організація цивільної авіації (ІКАО /ICAO/) повідомила, що підтримує заходи авіаційної безпеки, які запроваджуються в США (програма «US-Visit» перевірки всіх іноземних громадян, які перетинають кордони США, за такими біометричними характеристиками, як відбитки пальців і риси обличчя, а також інші заходи забезпечення безпеки повітряних перевезень), але вважає, що гарантоване підвищення рівня безпеки в аеропортах є неможливим без застосування машинозчитуваних біометричних проїзних документів (МЗПД або MRTD).

Широке використання МЗПД, які вдосконалені за допомогою засобів біометричної верифікації та ідентифікації, дозволяє суттєво пришвидшити проходження пасажирів через контрольні пункти в аеропортах, значно підвищити рівень авіаційної безпеки та практично виключити можливість підміни особи. Відповідно до цих вимог, розроблені технічні вимоги щодо наявності біометричної інформації в MRTD, які впроваджуються різними державами.

На тлі зростання обсягу світових пасажирських перевезень і доцільності підтримки оптимального співвідношення між необхідністю спрощення формальностей та забезпеченням належного рівня безпеки – біометричні ідентифікаційні та верифікаційні технології є одним із ключових моментів. Для формування глобального підходу до впровадження біометрії з метою найбільшого сприяння розвитку цивільної авіації суттєвими є такі аспекти:

– вибір видів (типу) біометричних технологій, що мають застосовуватися на державному рівні. На кінцевий вибір впливають декілька чинників, які є різними для кожної

[1] Biolink.ru. – 2008. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/markets/education.php

[2] Новый биометрический эксперимент в аэропорту Хитроу // BIOMETRICS.RU. – 2013. – 28 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

країни. Це не тільки безпека та висока ефективність, які є дуже важливими чинниками, але й такі аспекти, як зручність користувачів, рівень застосування останніх досягнень інформаційних технологій та загальна вартість запланованих до використання систем контролю та безпеки;

– вибір типу біометричної технології залежить від мети застосування та від специфічних конкретних умов у місцях можливого запровадження. Наприклад, так звана пасивна форма нагляду за пасажирами в термінальних приміщеннях аеропорту вимагає використання різних біометричних систем як додатку до автоматизованих систем прикордонного контролю;

– за глобального застосування біометричних технологій у цивільній авіації дуже важливою вимогою є сумісність біометричних баз даних;

– такий аспект, як забезпечення конфіденційності приватного життя громадян суттєво впливає на використання біометрики. Вона стосується таких складових обраних технологій, як процедури взаємообміну персональними даними з відповідними структурами інших країн і приватними компаніями, а також обов'язкове оприлюднення мети використання й термінів зберігання всіх біометричних відомостей та відображення цих положень на законодавчому рівні кожної країни.

22 травня 2003 року була затверджена рекомендація Технічної консультативної групи з машинозчитуваних проїзних документів (TAG/MRTD), яка згодом отримала назву план ІСАО. Ця рекомендація обумовлює:

– вибір технології розпізнавання рис обличчя для подальшого використання в усьому світі для програмно-комп'ютерного підтвердження особистості;

– використання безконтактної інтегральної мікросхеми з мінімальним обсягом пам'яті 32 Кбайт як засобу зберігання в проїзному документі електронних даних, зокрема й біометричних;

– програмування інтегральних схем із використанням команд, які прописані у встановленій логічній структурі даних (ЛСД);

– використання змінної схеми інфраструктури відкритих ключів (PKI) для застосування електронноцифрових підписів для захисту електронних даних від несанкціонованої зміни[1].

Діяльність аеропортів як найважливіших транспортних вузлів тісно пов'язана з регулюванням міграційних потоків, прикордонним і митним контролем. Наведемо перелік основних питань, які вирішуються за допомогою біометрії на транспорті та насамперед на авіатранспорті:

– інтеграція біометричних технологій у комплексні системи безпеки транспортних об'єктів, особливо до систем контролю за доступом в аеропортах;

– вирішенням цієї проблеми є розробка та застосування біометричних ідентифікаційних карток транспортних співробітників, що вимагає формування спеціальної інфраструктури, реалізації завдань із реєстрації, персоналізації, видачі карток і подальшим супроводженням під час експлуатації;

– реєстрація пасажирів і реалізація програм супроводу клієнтів авіакомпаній, які часто подорожують.

Отже, нині біометричні технології ефективно інтегровані до систем паспортно-візових документів нового покоління та в інші системи масового обслуговування авіапасажирів, наприклад, таких, як програми супроводу пасажирів, які часто подорожують,

[1] Биометрия в авиационной безопасности // Системы безопасности. – 2007. – № 3. [Электронный ресурс]. – Режим доступа: http://www.secuteck.ru/articles2/…

що передбачають пришвидшення проходження контролю перед вильотом за допомогою надійної верифікації особистості клієнта за його біометричними параметрами.

Крім того, авіакомпанії й аеропорти експлуатують масштабні інформаційні системи, забезпечення безпечної роботи яких досягається за допомогою використання засобів ідентифікації користувачів і контролю за їх доступом до корпоративних ресурсів[1].

Досвід використання біометричних технологій у забезпеченні безпеки аеропортів у перспективі повинен бути розповсюджений не тільки на всю транспортну галузь, але й на паливно-енергетичний комплекс та низку інших сфер людської діяльності.

Розглянемо детальніше практичне застосування біометричних системних рішень під час організації процедури здійснення контролю авіапасажирів перед польотом та організації контролю за доступом в аеропортах.

Компаніями «Precise Biometrics» і «IER» було розроблено комплексне рішення, що дозволяє істотно пришвидшити процедуру контролю перед вильотом і одночасно досягти ще більшого рівня безпеки. У цьому рішенні були об'єднані біометричні технології ідентифікації за відбитками пальців та нові моделі турнікетів, за допомогою яких контролюють посадку пасажирів на борт повітряного судна. Новинка вперше була представлена на виставці «Passenger Terminal Expo» у квітні 2008 року в Амстердамі. Були продемонстровані два варіанти «біометричних ліній» контролю перед польотом, які мали деяку технологічну відмінність.

Перший варіант розрахований на осіб, які є учасниками програми супроводу пасажирів, які часто подорожують, і мають відповідну картку, в пам'ять якої вже внесені відомості про відбитки пальців або інші біометричні дані.

Для того, щоб засвідчити свою особистість за допомогою біометричної ідентифікації, пасажир повинен скористатися мобільним телефоном, який може підтримувати технологію NFC (Near-Field Communications), та оснащений сканером відбитків пальців. Авіапасажир вставляє картку учасника програми супроводу і каналами NFC відомості про його біометричні ідентифікатори транслюються в SIM-карту мобільного телефону. Далі за допомогою мобільника клієнт сканує відбиток пальця, а програмне забезпечення Precise Match-on-Card, що завантажене в SIM-картку телефона, зіставляє отримані відомості про раніше зареєстрований і знов пред'явлений біометричні ідентифікатори. Якщо ці персональні дані збіглися, авіапасажирові дозволяється посадка на відповідний рейс.

Другий варіант контролю перед вильотом із використанням біометричних технологій виглядає не настільки екзотичним і не вимагає додаткових технічних засобів. Пасажир сканує відбитки пальців під час реєстрації на рейс, а потім знову проходить біометричну ідентифікацію вже безпосередньо перед посадкою на борт літака, що дозволяє пересвідчитися в тому, що на рейс зареєструвалася та на борт повітряного судна піднімається одна й та ж фізична особа. Відомості про відбитки пальців, що використовуються під час проходження процедури контролю, знищуються відразу ж після того, як літак приземлився в пункті призначення[2].

Окрім систем ідентифікації авіапасажирів, авіаційні компанії використовують у своїй повсякденній діяльності біометричні системи, що призначаються для проведення контролю за доступом у службові приміщення, виходу обслуговуючого персоналу

[1] Биометрия на МАКСе: новейшие решения BioLink в составе экспозиции концерна EADS (авиасалон в Жуковском, 21–26 августа). – 2007. – 9 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Интеграция биометрии и технологии NFC ускоряет предполетный контроль в аэропорту // BIOMETRICS.RU. – 2008. – 30 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

на летовище та запобігання можливим небажаним діям співробітників аеропорту. Нині у цій сфері ринок пропонує ефективні й досить надійні біометричні системи.

Управління транспортної безпеки США (TSA) ще в четвертому кварталі 2007 року затвердила список перших п'яти повітряних портів, у яких були протестовані біометричні ідентифікаційні картки транспортного працівника (Transportation Worker Identification Credential – TWIC). У цей список увійшли аеропорти, що розташовані в містах Лос-Анджелес, Нью-Йорк, Нью-Джерсі, Лонг-Біч (штат Каліфорнія), Браунсвілл (штат Техас). Крім того, компанія «Watermark Cruises», яка знаходиться в Аннаполісі (штат Меріленд) і займається організацією туристичних і чартерних рейсів, також провела тестування такої картки.

За словами менеджера програми TWIC Морін Фенгай (Maurine Fanguy) були проведені випробування апаратно-програмного забезпечення, яке дозволяло проводити ідентифікацію власників карток TWIC за паролем і біометричними ознаками. Час ідентифікації утримувача біометричної ідентифікаційної картки становив приблизно три секунди[1].

За відомостями газети «Financial Times», у березні 2008 року тисячі співробітників британських аеропортів стали першими громадянами Сполученого Королівства, яким видали біометричні ідентифікаційні картки. Видача службовцям аеропортів нових ID-карт дало змогу істотно підвищити безпеку цих об'єктів транспортної інфраструктури і ліквідувати вразливість систем безпеки британських аеропортів, що були виявлені наприкінці 2007 року.

У четвертому кварталі 2007 року було встановлено, що попередня перевірка кандидатів на працевлаштування в аеропортах повною мірою не виключала загрозу прийому на роботу «неблагонадійних» осіб. Це, своєю чергою, підвищувало ступінь можливої вразливості цих транспортних вузлів на предмет здійснення терористичного акту. Крім того, аеропортам потрібно запровадження набагато надійнішої й уніфікованої системи безпеки, яку не можна сформувати на базі використовуваних на цих об'єктах звичайних магнітних карток, випуск яких безпосередньо проводять компанії, що забезпечують працевлаштування[2].

2010 року компанії «Sita» і «IHS Jane's» провели спільний вебінар, під час якого були розглянуті основні можливості застосування біометричних технологій в аеропортах. Експерти цих компаній констатували, що головну вигоду від подальшої «експансії» використання інноваційних технологій біометрії в аеропортах отримають авіапасажири. Такими вигодами для авіапасажирів є: зручна реєстрація на рейс, пришвидшене проходження передпольотного контролю, зменшення часу під час посадки на борт літака, безпечна ідентифікація власників багажу. Перевагами технологій біометрії пасажири користуються не тільки під час відправлення в політ, але й в аеропортах прибуття, особливо при виконанні міжнародних авіарейсів: тут час авіапасажирів суттєво заощаджують біометричні системи паспортного та візового контролю.

Із середини 1-го десятиріччя XXI століття набув поширення ще один напрям застосування біометричних технологій, який полягає у встановленні та перевірці особистості авіапасажирів з метою виявлення тих, хто може становити загрозу і для інших авіапасажирів, і для національної безпеки країн, у яку ці особи мають намір прибути. Отже,

[1] Биометрическая идентификационная карта транспортного работника: определены пять пилотных портов для тестирования новинки // BIOMETRICS.RU. – 2007. – 16 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Британия. Служащие британских аэропортов первыми получат биометрические идентификационные карты // BIOMETRICS.RU (по материалам газеты «Financial Times»). – 2007. – 7 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

використання технологій біометрики виявляється корисним і для авіапасажирів, і для урядових структур. Подальшу інтеграцію систем біометричних паспортів, біометричних віз і ризик-менеджменту на транспорті експерти вважають оптимальною комбінацією, а дехто з них називає її навіть «золотим стандартом» використання біометрії, до якого повинні прагнути уряди всіх держав[1].

Симбіоз контролю за пересуванням авіапасажирів в аеропортах із прикордонним контролем засвідчує факт продажу в квітні 2013 року аеропортом Хітроу Прикордонному агентству Британії біометричної системи прикордонного контролю, яку він експлуатував із 2009 року. Нагадаємо, що біометрична система, що функціонує в Хітроу, ідентифікує авіапасажирів за їх обличчям: отримане «живе» фото порівнюється із його оцифрованою фотографією, яка зберігається в чіпі біометричного паспорта або ID-карти, і у разі збігання двох зображень власникові документа дозволяється перетнути кордон.

Раніше в Хітроу діяла біометрична система розпізнавання авіапасажирів за райдужною оболонкою очей, але аеропорт відмовився від її використання через дороге поточне обслуговування обладнання і його моральне старіння[2].

2011 року британський аеропорт Хітроу встановив сканери з можливістю розпізнавання лиця осіб, причому скануючі пристрої працюють і на міжнародних рейсах, і на внутрішніх. Застосування технології розпізнавання за обличчям буде гарантувати, що авіапасажири, які пройшли квитковий контроль, будуть проходити тільки на свої рейси. Так оператори аеропорту мають намір виключити випадки, коли до країни незаконно в'їжджають транзитні пасажири з міжнародних рейсів.

Такі випадки цілком можливі, оскільки під час посадки на низку внутрішніх авіарейсів із Хітроу не проводиться імміграційний контроль, тому міжнародні транзитні пасажири мають теоретичну можливість здійснити незаконний виліт в інші британські міста. За новими умовами транзитні авіапасажири перевіряються після того, як вони отримали посадковий талон. Контроль за пасажирами внутрішніх рейсів здійснюється після їх виходу із залу.

Технологію розпізнавання обличь, особливостю якої є камера з інфрачервоним спалахом, що може працювати в умовах будь-якого освітлення, надала компанія «Aurora Computer Services»[3].

Фінансисти, банкіри, рітейлери й отельєри вбачають неабиякі перспективи застосування біометричної ідентифікації під час роботи з дебетовими та платіжними картками, а понад 87% клієнтів європейських готелів підтримують запровадження біометричних систем у практику готельного бізнесу. Американські банкіри і страхові компанії почали застосовувати біометрію під час роботи зі здобувачами кредитів і вкладниками, а також використовували її при видачі компенсацій потерпілим від ураганів «Ріта» і «Катріна». Біометрична ідентифікація покупців у платіжній системі «Pay by Touch» дозволила на практиці, а не в теорії, впровадити технології персоналізованого маркетингу[4].

---

[1] Биометрические технологии в аэропортах: новые вызовы и новые возможности // BIOMETRICS.RU. – 2010. – 23 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Аэропорт Хитроу продал биометрическую систему пограничного контроля // BIOMETRICS.RU. – 2013. – 30 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Новые биометрические сканеры появятся в крупнейшем аэропорту Британии // СайберСекьюрити. – 2011. – 25 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Биометрический рынок набирает обороты // BIOMETRICS.RU. – 2007. – январь. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Підприємства торгівлі й обслуговування – невід'ємна і важлива складова інфраструктури будь-якого населеного пункту, незалежно від того – мале містечко чи гігантський мегаполіс. Відвідувачі цих установ чекають від них комфорту, якісного та швидкого обслуговування, безпеки, заохочення своєї лояльності. Своєю чергою, керівники торгівельних і обслуговуючих підприємств зацікавлені в ефективній роботі своїх співробітників, надійному розмежуванні доступу в службові приміщення, склади, наявності дієвого захисту корпоративних мереж, без яких неможлива діяльність будь-якого сучасного супермаркету або ресторану.

Основні завдання, що виконуються підприємствами торгівлі й обслуговування за допомогою біометричних технологій:

– облік робочого часу персоналу;

– розмежування фізичного доступу до об'єкта, його споруд і приміщень;

– контроль за доступом до кас і платіжних POS-терміналів;

– захист інформації, що обробляється у корпоративних мережах;

– надання високого рівня сервісу покупцям і клієнтам, що беруть участь у програмах заохочення лояльності;

– полегшення та пришвидшення розрахунків з відвідувачами з одночасним підвищенням рівня захисту їх персональних даних і зниженням транзакційних витрат.

Наведемо низку прикладів уже втілених у життя проектів ідентифікації покупців і співробітників на підприємствах торгівлі та обслуговування:

– біометрична платіжна система «Pay by Touch» – оплата покупок із підтвердженням транзакції за допомогою проведення ідентифікації за відбитком пальця в США (понад трьох мільйонів користувачів ще у 2007 році);

– розмежування доступу барменів і офіціантів до інформаційних терміналів за допомогою інтеграції сканерів відбитків пальців у інформаційну систему «Food Master» – найбільшу мережу піцерій «Andy's Pizza» в Молдавії;

– впровадження біометричної системи обліку робочого часу в торговому домі «ОЛДІ» в Росії (понад 1000 користувачів у мережі територіально розподілених офісів)[1].

Останнім часом у всьому світі спостерігається активізація використання біометричних технологій у різних установах охорони здоров'я. Зростання інтересу до досягнень біометрії цілком зрозуміле: будь-яка лікарня, поліклініка чи госпіталь повинні працювати достатньо точно і надійно, а реалізуванню цих вимог на практиці сприяють засоби біометричної ідентифікації.

Біометрична ідентифікація пацієнтів дозволяє оптимізувати процес лікування і практично не передбачає ймовірність виникнення помилок під час призначення лікування та прийому ліків. Крім того, застосування біометричних засобів для ідентифікації користувачів під час доступу до медичних інформаційних систем слугує достатньо надійним захистом спеціальної медичної інформації та персональних даних пацієнтів і дозволяє вивільнити персонал від непродуктивної та трудомісткої роботи щодо постійного введення логінів і паролів.

Запровадження біометрії у системи контролю фізичного доступу забезпечує раціональну організацію пересувань пацієнтів, співробітників і відвідувачів за територіями установ охорони здоров'я: водночас комфортність і гранична простота ідентифікації представників кожної з цих груп поєднується з надійністю й ефективністю заходів за контролем доступу.

---

[1] Торговля и сервис // Biolink.ru. – 2007. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/markets/retail.php

Наведемо перелік основних завдань, що вирішуються в діяльності установ охорони здоров'я за допомогою біометричних технологій:

– можливість розмежування фізичного доступу в спорудах і приміщеннях медичних центрів;

– організація доступу лікарів і медперсоналу до медичних інформаційних систем (електронні історії хвороб, витяги з них і т. д.) та систем розподілу медикаментів (включаючи препарати, до складу яких входять наркотичні засоби);

– облік робочого часу співробітників з одночасним проведенням автоматизації розрахунку зарплат, нарахування премій за роботу в нічні зміни тощо.

Як приклади реалізованих проектів можна навести:

– інтеграцію засобів біометричної ідентифікації (сканери, комплект розробника) в спеціалізовану інформаційну систему «Thorax» у словенському клінічному центрі Любляни (Web-інтерфейс, протокол HTTPS) і в систему віддаленого доступу «CITRIX» на замовлення транснаціональної медичної і фармацевтичної корпорації «Quintiles»;

– впровадження засобів біометричної ідентифікації (сканерів відбитків пальців) у медичну інформаційну систему міської лікарні № 1 м. Тольятті, Росія – /проект здійснюється з 2002 року/)[1].

У Латвії за допомогою біометричних технологій проходять процедури ведення електронних рецептів, електронних історій хвороб, організації електронного запису до лікаря. Очікується створення єдиного порталу, що буде висвітлювати питання надання електронних послуг у сфері охорони здоров'я, а також ведення автоматизованих регістрів й архівів зберігання медичної інформації[2].

У Москві столична влада планує створити базу даних відбитків пальців пацієнтів поліклінік і лікарень. Використання біометричної технології дозволить спростити існуючу систему запису до лікарів. Пацієнт повинен лише у перший раз прийти до поліклініки з полісом обов'язкового медичного страхування (ОМС) або з універсальною електронною карткою. Спеціальний пристрій зчитає з поліса або з картки штрих-код, після чого до вбудованого у пристрій сканера слід прикласти свій палець і відбиток автоматично збережеться у біометричній системі. Надалі пацієнтові, щоб записатися на прийом до лікаря, не потрібно буде носити з собою жодних документів. Наприкінці 2013 року експериментальний проект повинен був пройти тестування, після чого планувалося ухвалення остаточного рішення щодо його застосування[3].

Ще одним прикладом сучасного активного запровадження систем біометричних технологій є їх широке й активне розповсюдження у дошкільних, шкільних і вищих навчальних закладах. Застосування біометрії дозволяє вирішити такі нагальні потреби освітніх установ:

1. Забезпечення безпеки дітей, школярів, студентів, співробітників і викладачів. Освітні установи дедалі частіше стають об'єктом атак терористів і злочинців, і лише системи контролю за доступом, які дозволяють ідентифікувати відвідувачів за їх унікальними та невідчужуваними ознаками, здатні підвищити безпеку цих установ. Крім того, біометричні системи надають можливість організації розмежування доступу в особливо важливі службові приміщення (комп'ютерні класи, хімічні лабораторії тощо).

---

[1] Здравоохранение // Biolink.ru. – 2007. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/markets/...

[2] Латвия. Проекты в сфере биометрических технологий отнесены к числу приоритетных. – 2008. – 30 сентября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp…

[3] Биометрическая система поможет быстрее записаться на прием к врачу // M24.ru. – 2013. – 26 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

2. Оптимізація навчально-виховного процесу. Коло відповідних завдань надзвичайно широке: від реєстрації відвідування учнями або студентами занять і спрощення видачі книг у бібліотеках (за простою та зручною ідентифікацією за біометричними ознаками) до засвідчення особистості осіб, які складають іспити або які проходять сертифікаційні випробування чи використовують системи дистанційного навчання, а також захисту інформаційних ресурсів і комп'ютерних мереж освітніх установ.

3. Надання додаткового комфортного сервісу (з одночасним зменшенням організаційних витрат) під час надання супутніх послуг. Наприклад, дедалі популярнішою стає біометрична ідентифікація учнів у кафетеріях і їдальнях (із безготівковою оплатою вартості вибраних школярем /студентом/ страв за його рахунком, що поповнюється і контролюється батьками або спонсорами). Аналогічно може бути організований доступ до копіювальних апаратів, лінгафонної техніки та інше, а також SMS-інформування батьків про час прибуття дитини в навчальний заклад або виходу з нього.

Необхідно зважати на специфічні чинники, що зумовлюють доцільність упровадження біометричних технологій у діяльність освітніх установ. Так, через вікові особливості діти та підлітки постійно гублять картки, жетони та інші матеріальні носії, вони забувають паролі, ідентифікаційні номери або легко плутають їх. Отже, під час використання інформаційно-автоматизованих систем, дія яких заснована на використанні таких ідентифікаторів, неминуче виникають експлуатаційні проблеми, не кажучи про витрати на додаткову закупівлю загублених або зіпсованих носіїв.

Під час організації харчування школярів на пільговій або безкоштовній основі їх ідентифікація за прізвищами або відокремлення пільговиків створює в учнів психологічний дискомфорт і часто викликає глузування з боку дітей із більш заможних сімей. У разі переходу на безготівкову оплату харчування за допомогою ідентифікації учнів за біометричними ознаками ці негаразди усуваються (так же як і інші проблеми, що пов'язані з обертанням грошової готівки у дитячому середовищі).

Поширення біометричних технологій не тільки отримують позитивний відгук в абсолютної більшості учнів та їх батьків, але і зумовлюють інші позитивні результати, які інколи навіть заздалегідь не планувалися. Так, наприклад, оснащення шкільних бібліотек засобами біометричної ідентифікації читачів у деяких освітніх закладах США сприяло тому, що учні, які раніше ігнорували бібліотеки, почали активніше відвідувати їх. Збільшення кількості відвідувань було зумовлене можливістю користування новітніми технологічними досягненнями.

Як приклади вже запроваджених проектів можуть слугувати:

– ідентифікація учнів за відбитками пальців у шкільних кафетеріях та їдальнях у США (штати Нью-Джерсі, Огайо, Флорида, Каліфорнія, Орегон, Мен, Аляска);

– біометричні системи контролю доступу в дитячі садки (ідентифікація батьків і обслуговуючого персоналу за відбитками пальців) у Великобританії (графства Абердіншир, Сомерсетшир, Ланкашир, Камбрія);

– облік відвідування занять школярами (ідентифікація за відбитками пальців) в Індії (штати Пенджаб, Гуджарат, Раджастан)[1].

Американський журнал «Educatering Magazine», який висвітлює роботу шкільних їдалень, проаналізував практику застосування біометричних систем у закладах харчування шкіл і коледжей та зробив висновок, що ці системи вигідні з кількох причин. По-перше, безготівкова оплата гарантує, що школярі витратять «обідні» гроші саме на

[1] Образование // Biolink.ru. – 2007. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/markets/...

їжу в їдальнях, а не на чіпси чи шоколадки. По-друге, біометрична ідентифікація учнів дозволяє керівництву кафетеріїв повніше та точніше враховувати смаки своїх юних клієнтів і підлаштовуватися під них, але не на шкоду принципам здорового і збалансованого харчування[1].

В Англії понад 1 млрд 280 тис. учнів середніх і старших класів пройшли біометричну ідентифікацію в 2012–2013 навчальному році. За підрахунками експертів, 40% англійських шкіл і коледжей застосовують технології біометрії.

За словами прес-секретаря Асоціації керівників шкіл і коледжей, найбільш популярною сферою застосування біометрії в навчальних закладах є обслуговування дітей у кафетеріях, їдальнях, а також у бібліотеках.

Біометричні технології вигідні всім сторонам процесу: школярі не можуть загубити відбитки пальців (на відміну від карток, які постійно забуваються або губляться), а обслуговуючий персонал може пришвидшити видачу підручників чи облік вибраних дитиною страв. Біометричні технології дозволяють навчальним закладам зменшити свої витрати[2].

Нині майже всіх власників смартфонів, планшетів та іншої комп'ютерної і цифрової техніки хвилює питання забезпечення безпеки різних персональних даних, тобто унеможливлення скористання сторонніми особами особистими відомостями без відома власника або, що ще гірше, викрадення приватної інформації. Тому дедалі більше компаній оснащують різні пристрої, що випускаються ними, електронною пам'яттю з функцією біометричної аутентифікації користувача. Низка фірм налагодили випуск USB флеш-приводів, що оснащені вбудованою системою аутентифікації власників. Водночас пристрої здатні запам'ятовувати до 10 різних зображень, які використовуються згодом для аутентифікації, що уможливлює верифікацію декількох фізичних осіб, які можуть користуватися цією апаратурою. Для тих, хто хоче ще більшого рівня захисту, може бути активована система, що вимагає введення пароля[3].

В Індії компанія «Lenovo» ще на початку 2007 року почала випускати ноутбуки Y300 і Y500, які були оснащені вбудованою системою біометричної ідентифікації «Veriface». За повідомленням інтернет-видання «SiliconIndia», біометрична система ідентифікує власника ноутбука за рисами його обличчя. Моментальна фотографія перетворюється на цифрове зображення обличчя власника ноутбука, що є паролем для входу в «Windows» або інші прикладні програми. Тобто власникові ноутбука запам'ятовувати та вводити пароль не потрібно. Крім того, якщо програма доступу до ноутбука «вирішить», що до його ресурсів намагається отримати доступ незареєстрований користувач, вона сфотографує зловмисника і збереже фото в своїй пам'яті для того, щоб згодом законний власник зміг з'ясувати, хто намагався отримати доступ до його комп'ютера. Ноутбуки обох моделей забезпечені 1,3-мегапіксельною камерою[4].

Швейцарська телекомунікаційна компанія «Swisscom» закупила в першому кварталі 2008 року другу партію клавіатур із вбудованими в них сканерами відбитків пальців.

---

[1] Биометрические системы в американских школах: новое внедрение // BIOMETRICS.RU. – 2013. – 10 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Более миллиона английских школьников прошли биометрическую идентификацию // BIOMETRICS.RU. – 2014. – 10 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] USB-накопитель от LG: комплекс безопасности // Интернет-сайт за адресою: http://www.drivers.ru. – 2007. – 21 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] В Индии начались продажи ноутбуков, узнающих хозяев в лицо // BIOMETRICS.RU. – 2007. – 9 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Перша партія «біометричних» клавіатур була придбана швейцарською компанією ще наприкінці 2006 року, і згодом, переконавшись у перевагах цього рішення, фірма вирішила розширити кількість користувачів системи біометричної ідентифікації. Це рішення «Swisscom», яка спеціалізується на наданні послуг мобільного зв'язку і чисельність персоналу якої налічує понад 12 тисяч чоловік, ухвалила, оцінивши зручність заміни автоматичним скануванням відбитка пальця старої схеми введення логіна і пароля. Важливу роль відіграла й прийнятна ціна, яка була запропонована за нову партію «біометричних» клавіатур шведським виробником «Precise Biometrics»[1].

Біометрія належить до тих сучасних технологій, темп розвитку яких надзвичайно збільшився після відомих подій 11 вересня 2001 року в США. У третьому тисячолітті нової ери значно зросло фінансування біометричних досліджень, які виконуються і комерційними, і державними структурами. Нині у багатьох країнах світу біометричні пристрої є частиною повсякденного побуту.

Корпорацією «Nokia» був запатентований мобільний дисплей із функціональністю сканера відбитків пальців. Фінською фірмою запантентовано оригінальний сенсорний інтерфейс, який може надавати або забороняти доступ до даних, ґрунтуючись на результатах біометричної перевірки.

Розробка також уможливлює створення користувальницьких профілів, які є надзвичайно корисними у тому разі, коли пристроєм користується декілька осіб. Кожному користувачеві надається доступ тільки до його відомостей або даних, а також до відповідних додатків до програмного забезпечення[2].

Консалтингова фірма «Farpoint Group», що спеціалізується на вивченні ринку безпровідних комунікацій, опублікувала ще в 2007 році доповідь, у якій висвітлила динаміку використання технологій біометричної ідентифікації у мобільному зв'язку. Російський біометричний портал BIOMETRICS.RU з посиланням на матеріали огляду повідомляв, що кількість нових моделей сотових телефонів, які були оснащені сканерами відбитків пальців і представлені покупцям, збільшилась у вказаному році більш ніж у 10 разів.

За оцінками авторів доповіді, ринок сотових телефонів переживав у 2007 році такий же переломний етап, як і ринок ноутбуків у 2005, коли сканери відбитків пальців стали невід'ємним елементом майже всіх останніх моделей портативних комп'ютерів. «Оскільки мобільні телефони містять важливі дані та все частіше починають виступати у ролі електронних гаманців, цілком очевидно, що їх власники прагнуть до того поєднання безпеки та зручності застосування, яке можуть забезпечити біометричні технології, зокрема, сканери відбитків пальців, – констатував голова «Farpoint Group» Крейг Матіас (Craig Mathias), 2007 рік став свого роду «моментом істини» для сканерів відбитків пальців, які з лептонів перейшли до експансії на ринок мобільних телефонів, і зараз ми спостерігаємо зростаюче сприйняття даної технології на цьому ринку».

Головними стимулами експансії біометричних технологій на ринку сотового зв'язку автори доповіді називали розширення застосування мобільного банкінгу та безпровідних платежів[3].

---

[1] Продвинутые телекоммуникационные компании используют биометрию // BIOMETRICS.RU. – 2008. – 25 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Запатентован мобильный дисплей с функциональностью сканера отпечатков пальцев. – 2007. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp…

[3] Биометрическая идентификация в мобильных телефонах // BIOMETRICS.RU (по материалам фирмы Farpoint Group). – 2008. – 8 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Фахівці компанії «Biometrics Research Group» вважають, що розвиток мобільних платежів пришвидшить інтеграцію у смартфони біометричних технологій. Експерти цієї фірми пророкують, що до 2020 року мобільними платежами будуть користуватися 700 млн людей, а обсяг відповідного сегмента фінансового ринку (тобто обсяг мобільних платежів) може сягти 750 млрд доларів. Ця обставина істотно пришвидшить упровадження в смартфони відповідних компонентів біометричних технологій, які зможуть забезпечити високий рівень безпеки під час проведення платежів[1].

У 2014–2015 роках ринок мобільних пристроїв очікує бум впровадження технологій біометричної ідентифікації. За оцінкою аналітиків «Gartner», у 2016 році приблизно третина організацій та установ світу буде використовувати у своїй діяльності мобільні пристрої з засобами біометричної ідентифікації. За даними агентства на початок 2014 року такі технології застосовувались лише у 5% підприємств, організацій і установ.

Дедалі більше людей зараз використовує у своїй виробничій діяльності особисті планшети та смартфони, що для них є дуже зручно, але водночас збільшується ризик витоку службової інформації: мобільний пристрій можно загубити чи десь забути, також його можно викрасти. Крімо того, багато користувачів легковажні у підході до вибору паролів для захисту особистого пристрою, використовуючи стислі та прості паролі.

Щоб захиститися від можливого витоку конфіденційних даних, підприємства та установи починають запроваджувати біометричні засоби аутентифікації. Наприклад, вбудування у планшет співробітника відповідного біометричного засобу з програмним забезпеченням дозволить розблокувати пристрій та розпочати роботу лише у тому випадку, коли працівник буде аутентифікований.

Компанія «Goode Intelligence» прогнозує, що у 2014 році зчитувачі відбитків пальців з'являться в мобільних пристроях «Android» і «Windows Phone», а до 2015 року стануть стандартними для телефонів і планшетів хай-енд класу. 2018 року біометричні сканери будуть складовою більшості мобільних пристроїв.

«Goode Intelligence» вважає, що у 2015 році світовий ринок усіх засобів біометричної аутентифікації за допомогою мобільних пристроїв буде становити понад 161 млн доларів[2].

Наприкінці 2007 року в Японії розпочалося застосування сигаретних автоматів, які оснащувалися системою розпізнавання облич. Пристрої визначали вік покупця за станом шкіри на його обличчі. Від бажаючого придбати сигарети вимагалось подивитися у вбудовану відеокамеру автомата та натиснути відповідну кнопку. Спеціальний комп'ютерний алгоритм аналізує зморшки і провисання шкіри на обличчі клієнта і протягом трьох секунд визначав, чи виповнилося потенційному покупцеві двадцять років. Якщо висновок був негативним, автомат не продавав сигарети. У тому випадку, якщо виникають ускладнення з визначенням віку молодої людини, покупцеві доводилося пред'являти певним чином свої водійські права або інший документ, і лише тоді він міг отримати пачку сигарет. Під час проведених випробувань пристрою на п'яти сотнях добровольців віком від 10 до 69 років було встановлено, що автомат у 90% випадків правильно визначав вік покупця[3].

---

[1] Биометрические технологии в смартфонах и мобильных платежах: битва Apple и Samsung // BIOMETRICS.RU. – 2013. – 24 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрическая революция на мобильном рынке // Телекомблог. – 2014. – 13 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Автоматы по продаже сигарет идентифицируют покупателей по возрасту // Компьюлента. – 2007. – 16 ноября. [Электронный ресурс]. – Режим доступа: http://www.compulenta.ru

За останніми повідомленнями ЗМІ, ідентифікація за біометричними параметрами дедалі більше починає використовуватися для вирішення таких завдань масової ідентифікації, як проведення перепису населення та забезпечення прозорості виборів.

Голосування за допомогою біометричних технологій повинне звести до мінімуму випадки фальсифікації на виборах. Із 1996 року процес голосування у Бразилії проводиться за допомогою електронних урн. Це дозволяє всього за декілька годин обробляти до 90% загальної кількості бюлетенів. Вибори у найбільшій країні Латинської Америки є обов'язковими для всіх виборців, тому традиційно супроводжуються високою явкою, яка сягає приблизно 80%[1].

Із 28 січня 2008 року в нижній палаті філіппінського парламенту була запроваджена процедура «біометричного голосування». Газета «Philippine Daily Inquirer», яка виходить у Манілі, повідомила, що ідентифікація за відбитками пальців стала обов'язковою процедурою перед голосуванням для всіх 240 членів палати представників.

За допомогою біометричної ідентифікації також здійснюється перевірка явки законодавців на кожне засідання палати. Для того, щоб максимально підвищити комфортність цієї процедури, всі робочі місця членів палати представників оснащені сканерами відбитків пальців. Перед тим, як проголосувати «за» або «проти» конкретного законопроекту, що обговорюється у парламенті, кожен член палати представників засвідчує свою особистість скануванням відбитка пальця. Вважається, що «біометричне голосування» дозволило зробити голосування (особливо щодо спірних питань) дійсно персоналізованим, а не номінальним, що, своєю чергою, значно поліпшило роботу парламенту.

На оснащення палати представників системою біометричної ідентифікації законодавців було витрачено понад 360 тис. доларів США[2].

Зробимо історичний екскурс у минуле України. У нашій державі навесні та на початку літа 2008 року розглядалося питання щодо запровадження ідентифікації за відбитками пальців під час реєстрації та голосування у Верховній Раді (відповідний проект постанови був зареєстрований депутатом Григорієм Смітюхом). У пояснювальній записці автор документа пропонував розширити функції електронної системи підрахунку голосів шляхом встановлення на пультах системи «Рада» пристроїв, які дозволили б розпізнавати особистість депутата за відбитком пальця під час реєстрації і проведення голосування. Проектом ухвали також пропонувалося можливість блокування карток для голосування депутатів, які особисто не реєструвалися на початку ранкового та вечірнього пленарних засідань[3].

Як відомо, ця постанова не була ухвалена.

У нашій країні доволі давно порушувалося питання щодо створення Державного реєстру виборців України. За нормативними документами Центральна виборча комісія (ЦВК) зобов'язана була розпочати підготовку до його створення ще навесні 2007 року. Вартість створення Реєстру виборців тоді становила приблизно 74 млн гривень. Це складна система, де повинні використовуватися засоби криптографічного захисту інформації, унікальне мережеве устаткування тощо. Як відомо, Державний реєстр виборців почав діяти з березня 2009 року, але він не використовує біометричні технології.

---

[1] Бразилия создает базу биометрических данных избирателей // Вести.Ru. – 2008. – 29 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp…

[2] В парламенте Филиппин вводится биометрическое голосование // BIOMETRICS.RU. – 2008. – 9 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Партия регионов предлагает идентифицировать депутатов украинской Рады по отпечаткам пальцев // Деловая Неделя. – 2008. – 7 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

На початку 2008 року був опублікований прес-реліз американської компанії «bioMETRX», де повідомлялось, що передбачається облаштування сканерами відбитків пальців поштових скриньок для отримання кореспонденції, оскільки регулярні крадіжки з них – це постійний головний біль для багатьох американців, і, що найгірше, крадіжка пошти досить часто пов'язана із викраденням персональної інформації.

Ще одна проблема, з якою часто стикаються деякі з авіапасажирів, – це крадіжка речей із багажу, який здається на час перельоту, причому значна частина розкрадань відбувається після того, як пасажири здали багаж на стійці реєстрації. Щоб запобігти несанкціонованому доступу до поштових скриньок або вмісту багажних речей, «bioMETRX» розробляв спеціальну систему «smartCASE». Вона дозволяла відкривати валізи та інші подібні «носії» тільки за пред'явленням попередньо зареєстрованого відбитка пальця.

Крім того, продовжується випуск біометричних систем контролю доступу до гаражів або пристроїв відкриття воріт. У прес-релізі також надано інформацію про те, що незабаром у продаж має надійти і термостат, який буде захищений від несанкціонованого доступу за допомогою біометричних технологій[1].

На Олімпійських іграх 2008 року в Пекіні для забезпечення особистої безпеки спортсменів і членів офіційних делегацій доступ у всі житлові комплекси та об'єкти харчування Олімпійського селища здійснювався за допомогою біометричних пристроїв, які проводили контроль доступу за відбитками пальців мешканців селища[2].

А на лондонській Олімпіаді-2012 у всіх будівельників і спеціалістів, які працювали на зведенні об'єктів, були зняті біометричні дані. Підраховано, що через системи розпізнавання лиця і долонь пройшло близько 100 тис. будівельників. Організатори Олімпіади обіцяли, що персональні дані не потраплять до рук інших осіб, а після завершення заходу будуть знищені.

Усього на забезпечення безпеки під час будівництва олімпійських об'єктів у Лондоні було витрачено понад 354 млн фунтів стерлінгів. А під час проведення самої Олімпіади на заходи безпеки планувалось виділити 1,2 млрд фунтів стерлінгів. На 500 акрах Олімпійського парку було встановлено понад 500 тис. камер відеоспостереження. Для проведення заходів із забезпечення безпеки під час Олімпіади-2012 використовувались послуги майже 8 тис. охоронців[3].

Із 2008 року в індійській столиці Делі застосовується біометрична ідентифікація осіб, затриманих на міських вулицях за жебрацтво. Їх скеровують до спеціального центру «Kingsway Camp», де відскановують відбитки пальців й отримують їх цифрове фотозображення.

Якщо згодом та ж особа буде знову затримана за жебрацтво і за підсумками біометричної ідентифікації буде підтверджено наявність факту її попереднього затримання, це буде враховано судом під час визначення міри покарання. За інформацією видання «Times of India» особи, яких у судах визнають винними у професійному жебрацтві, скеровуються на соціальну реабілітацію.

---

[1] «Потребительская» биометрия: что нового появится на рынке в 2008 году // BIOMETRICS.RU. – 2008. – 11 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрическая система контроля доступа обеспечит безопасность участников Олимпийских игр в Пекине // РИА Новости. – 2008. – 7 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Британцы соберут биометрические данные у строителей олимпийских объектов // Лента.Ру. – 2008. – 6 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Серед інших заходів, які проводились для очищення вулиць столиці Індії від професійних жебраків, було також встановлення камер відеонагляду в громадських місцях[1].

Серед повідомлень про застосування біометричних технологій своєю екзотиністю вирізняється публікація про використання для захисту об'єктів і контролю за фізичним доступом принципово нової біометричної системи, що заснована на голосовій ідентифікації собачого гавкоту. Собаки по-різному гавкають або гарчать на знайомих людей і чужинців.

За появи незнайомця на території, яку собака вважає «своєю», як правило, лунає більш гучний і частіший гавкіт, причому ця закономірність характерна всім собакам, незалежно від того, яка порода, стать і «габарити» чотириногого охоронця. На підставі цієї ідеї ізраїльська компанія «Bio-Sense Technologies» розробила і випробувала спеціальні алгоритми, що ідентифікують загрозу за характером гавкоту та гарчання, і на цій основі створила спеціальний біометричний сенсор, який вмонтовується у собачий ошийник і проводить розпізнавання відповідної звукової інформації. Собаку з таким ошийником можна випускати на територію, що охороняється, і сигнали, що будуть свідчити про вторгнення чужинців, надходитимуть із біометричного сенсора на пульт системи контролю за доступом.

Стверджується, що собаки розпізнають загрозу несанкціонованого вторгнення у 20 тис. разів ліпше, ніж охоронці-люди[2].

Дуже цікавими є результати проведення опитувань громадської думки в країнах, де найбільший рівень запровадження досягнень біометричних технологій у повсякденне життя. Насамперед це США та Великобританія. Як засвідчили результати проведених у 2006–2008 роках опитувань громадської думки в цих країнах, ще тоді можна було однозначно стверджувати, що більшість членів суспільства схвалює масове використання досягнень біометрії.

Втішним для розробників і постачальників біометричних технологічних рішень є той факт, що громадська думка тоді не зводила сферу застосування біометрії тільки до запровадження паспортно-візових документів нового покоління. Згідно з даними дослідження, що проводилося американським інститутом «Ponemon» в кооперації з британським центром вивчення громадської думки «Ipsos/MORI» наприкінці 2006 – початку 2007 років, 90% споживачів у Великобританії і приблизно 69% споживачів у США висловлювались за розширення сфер застосування біометрії.

Дослідження проводилося на замовлення компанії «Unisys» і представляло репрезентативне опитування 500 британських споживачів і 1744 осіб у США. Вік респондентів коливався в межах від 18 до 75 років, а рівень річного доходу – від 20 до 201 тис. доларів США. Пріоритетними напрямами застосування біометричних технологій були зазначені: діяльність банків, проведення фінансових транзакцій та застосування у різних платіжних системах, надання медичних послуг і розширення впровадження у діяльність державних органів.

За підсумками третього щорічного опитування компанії «IDC» експертів з інформаційної безпеки, що було здійснено у 2007 році в ста країнах світу (було опитано 4016 респондентів), біометрія впевнено ввійшла до списку ключових технологій, за допомогою яких треба проводити заходи з захисту інформації. Конкретне місце біометрії

---

[1] Применение биометрических технологий поможет эффективнее бороться с нищетой // BIOMETRICS.RU (по материалам газеты «Times of India»). – 2008. – 4 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

[2] Израильтяне хотят повесить биометрические сенсоры на собак // BIOMETRICS.RU. – 2007. – 12 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

у загальному рейтингу перелічених заходів залежало від регіону опитування, але ніде не опускалося нижче другої позиції.

Технології біометричної ідентифікації мають особливу популярність серед авіапасажирів. У цьому плані показовими є результати опитування, проведеного ще восени 2006 року авіакомпанією «Scandinavian Airlines» відразу після запровадження сервісу біометричної ідентифікації пасажирів під час здачі багажу (опитано понад 500 постійних клієнтів, які користуються різними пільгами і преференціями у рамках втілення програми лояльності «EuroBonus»).

Більша частина опитаних (53%) беззастережно підтримала подальше поширення біометрії на авіатранспорті; трохи більше третини (36%) заявили, що для ухвалення остаточного рішення їм потрібна додаткова інформація; проти висловився лише один із кожних десяти опитаних (10%).

Ще більш вражаючими є підсумки дослідження, проведеного компанією «Steria» влітку-восени 2006 року, коли було опитано 5700 пасажирів. 90% респондентів були згодні проходити ідентифікацію за відбитками пальців або райдужною оболонкою очей – за умови, що цей захід слугуватиме підвищенню безпеки перевезень і пришвидшенню проходження контролю перед вильотом.

До отриманих результатів цілком логічно примикає підсумок опитування, що був проведений у 2007 році старійшою в світі Школою готельного бізнесу в Лозанні (Ecole hoteliere de Lausanne – EHL), де взяло участь 300 осіб. 87,3% опитаних клієнтів різних європейських готелів підтвердили, що позитивно ставляться до перспектив застосування біометрії у готельному сервісі.

Серед найперспективніших напрямів використання біометрії найбільше згадувалось «гостьове» обслуговування, контроль за доступом у спортивні заклади при готелях і проведення різних заходів поза готельними стінами на «відкритому повітрі» (прийоми, ланчі тощо)[1].

Восени 2008 року компанія «Unisys» провела чергове соціологічне дослідження у Новій Зеландії. Половина громадян цієї країни була дуже стурбована тим, як забезпечується безпека їх фінансових транзакцій.

На цьому тлі зростає кількість споживачів, бажаючих брати участь у використанні останніх розробок біометричних технологій, які респонденти вважають значно надійнішими порівняно з використанням паролів і PIN-кодів. Загалом за доповнення паролів і PIN-кодів біометричною ідентифікацією тоді висловилось близько 97% новозеландців[2].

За п’ятнадцять останніх років біометрія зробила стрімкий ривок, вийшовши водночас далеко за рамки молодої технології, що функціонувала у порівняно вузькій сфері та обмежувалась лише декількома видами застосувань.

Тепер біометричні технології є цілим спектром зручних, практичних і корисних засобів і технологічних рішень, які використовуються у багатьох галузях і для вирішення значної кількості прикладних завдань. Продовжується домінування «трьох великих біометрик»: сукупна частка засобів ідентифікації за відбитками пальців, за рисами обличчя та райдужною оболонкою очей і надалі становить більше 50% від усього галузевого ринку.

---

[1] Лукашов И. Биометрия выдерживает непрерывный экзамен / И. Лукашов // Cnews.ru. – 2007. – 21 августа. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security2007/...

[2] У новозеландцев популярны технологии идентификации по отпечаткам пальцев // BIOMETRICS.RU. – 2008. – 28 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

За останніми відомостями щодо регіональної структури світового біометричного ринку більша частина його загального обсягу припадає на держави Північної Америки та країни Азійсько-Тихоокеанського регіону. Особливо зростаючий інтерес до біометричних технологій проявляють фінансові та банківські інститути, які вважають біометричні технології найбільш ефективним і безпечним засобом ідентифікації своєї клієнтури, причому і діючої, і потенційної.

Отже, у світі відбувається неухильне розширення меж застосування біометрії у різних галузях і сферах людської діяльності. Це не тільки надання різних послуг державним організаціям, але й різним бізнес-структурам і приватним особам, причому спектр послуг дуже різноманітний: від прикордонного контролю, обліку населення, одержання грошей у банкоматах до підвищення комфортності обслуговування у закладах торгівлі та аеропортах.

Біометричні технології використовуються як з метою контролю за доступом до об’єктів, що охороняються, так і для їх захисту, а також з метою забезпечення інформаційної безпеки. Зростаючий інтерес до запровадження біометричних рішень зумовлено простотою їх застосування, швидкодією проведення різних ідентифікаційних операцій та зручністю використання у повсякденному житті.

У світі країни одна за одною починають ухвалювати закони «Про біометрію», оскільки запровадження досягнень біометрики, якщо і не є магістральним шляхом розвитку інформаційних технологій, але становлять один з її головних пріоритетів. Біометричні технології, які нині вийшли на індустріальний шлях розвитку, починають повертати ті інвестиції, які були вкладені для їх розвитку.

Розділ 8

ПРОБЛЕМИ ЩОДО ЗАСТОСУВАННЯ БІОМЕТРИЧНИХ СИСТЕМ І ПРИСТРОЇВ ДЛЯ АУТЕНТИФІКАЦІЇ ТА ІДЕНТИФІКАЦІЇ

Біометричні ідентифікатори – унікальні для розпізнання особи. Але ступінь надійності аутентифікації суттєво відрізняється у випадках, коли зняття параметрів будь-яких ідентифікаторів індивідуума проводиться під безпосереднім наглядом за процесом сканування спеціально підготовленими для того співробітниками або коли здійснюється контроль процедури дистанційного доступу до мережі без візуального контролю. Необхідно визнати, що у деяких випадках біометричні системи допускають імовірність задовільного розпізнання за виготовленими муляжами.

Найбільша кількість способів виготовлення муляжів існує для біометричних пристроїв, які розпізнають за відбитками пальців, що цілком природньо, оскільки ця технологія була та є найпоширенішою. Загалом виготовити дублікат відбитка пальця доволі легко, причому немає потреби у рідкісних і дорогих матеріалах – цілком достатньо тих, які можна купити в будь-якому магазині. Йдеться про недорогі хакерські технології, що дозволяють «обдурити» монотехнологію ідентифікації за відбитком пальця. Хакерами та фахівцями у біометричній галузі вже було продемонстровано на наукових конференціях і описано в пресі близько півдюжини різних способів (станом на 2007 рік), коли за допомогою різних підручних пристроїв і розповсюджених матеріалів виготовлялись дублікати чужих пальців (муляжі) з характерним малюнком папілярних ліній конкретного індивідуума. Такі копії дозволяли і дозволяють не тільки вводити в оману біометричні пристрої розпізнання за відбитками пальців, але й за бажання залишати скільки завгодно відбитків чужих «пальчиків» на місці злочину[1].

Наприклад, можна виготовити муляж пальця з гелю. Для цього досить отримати будь-яким способом відбиток потрібного пальця «клієнта» (необхідно, щоб в руки до потрібної особи потрапила під будь-яким приводом якась гладенька, найліпше прозора річ (фужер, чарка тощо), заздалегідь ретельно вимита й обтерта, а далі, як говориться – справа техніки). Відсканувавши поверхню і навівши необхідну контрастність, декілька разів видруковують зображення на одному і тому ж місці вибраного носія. А потім лише за 10 хвилин на устаткуванні, який елементарно купується у магазинах, можна виготовити гелевий муляж із необхідним відбитком пальця[2].

Найнадійніший спосіб – зробити зліпок оригіналу пальця за допомогою стоматологічного компаунда і виготовити латексну або пластилінову копію оригіналу. Відома

[1] Берд Киви. Улики под сомнением / Киви Берд // Компьютерра. – 2007. – № 27–28. – 1 августа. [Электронный ресурс]. – Режим доступа: http://offline.computerra.ru/2007/695/327708/

[2] Ковалевский А. С. Биометрия: а ларчик ломом открывался / А. С. Ковалевский. [Электронный ресурс]. – Режим доступа: http://www.magicpc.spb.ru/journal/200510/04/01.php – http://www.magicpc.spb.ru/journal/200510/04/03.php

й велика кількість значно простіших засобів, не настільки надійних, але цілком дієвих. Найпростіший із них – на поверхні скляного «віконечка» сканера обов'язково залишається відбиток пальця особи, котра пройшла процедуру ідентифікації чи верифікації, і є способи його «оживлення», наприклад, шляхом прикладання поліетиленового пакета з холодною водою.

Співробітники німецького комп'ютерного журналу «Computertechnik» провели ґрунтовне дослідження 11 систем біометричної верифікації на базі розпізнавань облич, пальців і райдужної оболонки очей користувачів. Причому журналісти орієнтувалися на найпростіші методи обману систем. Так, систему впізнання обличчя особи вдалося «обійти» за допомогою звичайної фотографії клієнта, або пред'явлення за допомогою екрана ноутбука фотозображення обличчя одного з користувачів системи. А за допомогою цифрового фотодруку ока на якісному кольоровому принтері елементарно вдалося обдурити систему аналізу за райдужною оболонкою. А низка дактилоскопічних систем зреагувала на відбитки пальців, які були отримані за допомогою графітового порошку та липкої стрічки[1].

Ще одна досить істотна вразливість – це проблема архівного зберігання шаблонів або передача (проходження) в електронному вигляді отриманих під час сканування результатів. Адже основна вада біометрії, на думку більшості фахівців, полягає в тому, що біометричні дані можна викрасти після того, як вони були отримані. Як відомо, існує два варіанти архівного зберігання зображень: коли зберігається саме зображення біометричного параметра та коли зберігається тільки якась контрольна сума (цифровий шаблон), котра була вирахувана за параметрами зображення, що було отримане під час сканування. Відповідно, в першому варіанті існує високий ризик можливості так званої «крадіжки особи». Крім того, методи шифрування, що використовуються у біометричній системі, також можуть виявитися ненадійними, в цьому разі ніхто не застрахований від можливого перехоплення даних, причому і механічних, і програмних.

Отже, однією з важливих характеристик програмно-апаратних біометричних комплексів є їх здатність виявлення муляжів і надійний захист від можливого перехоплення біометричних даних.

На практиці це означає, що у першому випадку біометрична система працює в режимі, коли оператор не може візуально проконтролювати процедуру проходження контролю (процесу сканування) конкретною особою, тобто система повинна мати можливість самостійно визначати справжню приналежність запропонованого до сканування джерела біометричних параметрів. Практично це означає, що якісна біометрична технологія має відрізняти біометричну характеристику, яка відсканована у живої людини, від тієї, що одержується за допомогою муляжу. Це означає, що потрібно приймати для проведення процедури ідентифікації або верифікації тільки такі біометричні зображення, що були отримані скануванням частин тіла живої людини.

Існує декілька типів шахрайського використання муляжів у біометричних системах:

– для доступу до конкретного електронного ресурсу або реального об'єкта;

– з метою компрометації конкретної особи, біометричну характеристику якої копіює муляж;

– анулювання операції, учасники якої верифікувались за допомогою віддаленого доступу до біометричної системи.

[1] Ревич Ю. Удар по интерфейсу: сканеры отпечатков пальцев обмануть не сложнее, чем домофон / Ю. Ревич // Новая газета. – 2006. – 16 января. [Электронный ресурс]. – Режим доступа: http://2006.novayagazeta.ru/nomer/...; http://universalkey.boxmail.biz/cgi-bin/ guide…

Нині практично всі розробники та виробники біометричного устаткування заявляють про здатність власних виробів розпізнавати муляжі, проте спеціальні тестування, що проводились і університетськими дослідницькими центрами, і спеціалізованими ІТ-виданнями, свідчать про те, що у деяких випадках це поки що лише реклама. За висновками експертів, низка апаратно-програмних рішень, зокрема й від виробників, що є лідерами у біометричній галузі, у реальних умовах не завжди відрізняють від оригіналу навіть досить грубі підробки: відбитків пальців із силіконового герметика або жувальної гумки, фотозображень особи або райдужної оболонки ока, які пред'являють скануючому пристрою. У зв'язку з цим проблема «муляжної вразливості» біометричних систем є однією з основних чинників, які ускладнюють поширення біометрії. Адже такі поширені види застосування біометрики, як цивільна ідентифікація, міграційний контроль, аутентифікація власників банківських карт вимагають надання певних гарантій із боку виробників.

Для розпізнавання муляжів програмно-апаратний комплекс біометричної системи водночас з одержанням біометричного зразка повинен проводити дії з реєстрації спеціальної додаткової ознаки або низки інших ознак. По суті, система повинна бути налаштована або на визначення достовірності /достеменності/ біометричної характеристики (ознака достовірності /достеменності/) або на визначення муляжу (ознака муляжу), або одночасно на контроль цих двох ознак. Якщо реєструється ознака муляжу та не реєструється ознака достовірності, – система не дає дозволу на продовження роботи з отриманими даними.

Особливо робить вразливою біометричну систему така ситуація, коли виробники, як правило, не зберігають у таємниці технології, за якими визначають муляжі, що у підсумку істотно знижує її стійкість від можливого злому. Крім того, для подолання захисту від муляжів необхідно лише «підробити» ознаку достовірності або позбавитися від ознаки муляжу. Чим більше різних ознак достовірності здатна визначати система, тим більша її стійкість до несанкціонованих операцій із використанням муляжів[1].

Подолання будь-якого, навіть найвитонченішого захисту від муляжів, – це, як показує практика, лише питання часу. Тому постійне вдосконалення способів захисту системи від доступу за допомогою муляжів має бути однією з обов'язкових умов для розробників сучасної біометричної апаратури.

Крім того, можливі варіанти, коли біометрична ідентифікаційна система може просто давати збої. Наприклад, біометрична система пропуску портових робітників, яка була введена в США наприкінці жовтня 2007 року, не могла проводити порівняння відбитка пальця з даними, що були записані на смарт-картці, в двох випадків зі ста. У зв'язку з цим фактом Департамент безпеки на транспорті (TSA), що підпорядковується Департаменту внутрішньої безпеки (DHS) США, вимушений був внести корективи до програми «Ідентифікаційні реквізити транспортних робітників» (TWIC), яка була розроблена для посилення безпеки після подій 11 вересня 2001 року.

Її технічна реалізація містила систему доступу за відбитком пальця і смарт-карткою, у мікрочіп якої попередньо був внесений електронний шаблон відбитка, та ведення журналу доступу[2].

[1] Устойчивость биометрических систем против несанкционированного доступа с использованием муляжей биометрических характеристик // UNISXCAN. – 2005. – 13 декабря. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art535.html

[2] В процессе реализации программы биометрических идентификационных карт транспортных работников в США возникли проблемы // Cnews.ru. – 2007. – 30 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Через низку ускладнень до останнього часу не вдавалось повною мірою використовувати можливості технології розпізнавання людини за райдужною оболонкою ока, хоча й вона рекомендована для масового застосування Міжнародною організацією цивільної авіації (ICAO). Так, блакитний колір очей, сльози та особливо можливість використання контактних лінз є на заваді або навіть унеможливлюють досягнення необхідної точності, що разом із дорогою вартістю обладнання й обслуговування є стримуючим чинником поширення цієї технології.

Ще однією з найістотніших проблем є «прайвесі», тобто дотримання вимоги конфіденційності персональних даних, що буде більш детально розглянуто у спеціальному розділі. Нині є прецеденти несанкціонованого зчитування інформації з біометричних документів і перехоплення електронних даних. Хоча поширеною є думка про те, що підробити біометричні документи майже неможливо. Великобританія свого часу зіштовхнулася з цією проблемою – там хакерами був розшифрований код чіпа, коли близько 3,5 млн паспортів було вже видано громадянам. Хакерська атака звела нанівець багаторічну роботу і, як наслідок, це вплинуло на реалізації головного завдання – протидії тероризму[1].

Систему захисту нідерландських біометричних паспортів, незважаючи на наявність досить сильного криптографічного захисту, також було зламано хакерами[2].

За висновком фахівців супервайзера із захисту даних «European Data Protection Supervisor» (EDPS), які слідкують за інформаційною безпекою офіційних баз даних ЄС, європейська база даних на осіб, які подали заявки на отримання політичного притулку, а також нелегальних мігрантів – «Eurodac» – свого часу також мали певну уразливість. База, окрім анкетних даних, містить відбитки пальців претендентів на отримання політичного притулку та нелегалів. На деяких ділянках системи, а також в організації захисту «Eurodac» було виявлено низку «проблемних місць», які відповідно до доповіді EDPS за листопад 2007 року, були усунені в найкоротші терміни. Але загалом система захисту бази даних «Eurodac» отримала більше позитивних оцінок, ніж негативних[3].

Основна проблема, яку особливо відзначають фахівці, полягає в тому, що як би надійно не були захищені персональні дані, зокрема й біометричні, існує ймовірність того, що вони можуть бути скопійовані та записані на інший чіп. Це настільки точна форма підробки, яку не можна практично встановити жодними методами. Фактично два чіпи – з оригіналом інформації та її копією – неможливо відрізнити один від одного за тими персональними даними, які вони зберігають. Для усвідомлення суті проблеми зазначимо, що два абсолютно однакових паперових документи створити практично не можливо.

Найгіршим є те, що в деяких випадках біометрична інформація може бути скопійована на відстані та, природньо, без жодної згоди з боку її власника. Найзручнішою формою для зберігання біометричної інформації та інших унікальних даних є так звані RFID-мітки. Ця абревіатура розшифровується як «радіочастотна ідентифікація» (radio frequency identification). RFID-мітка – це досить простий і дешевий пристрій без власного джерела живлення, але з невеличкою антеною. Він приймає зовнішній сигнал від зчитувача іформації та під час встановлення з ним контакту, передає оцифровані дані,

---

[1] Интервью: «Введение биометрических паспортов в России» // Эхо Москвы. – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрические удостоверения личности сами по себе не остановят фальсификаций и мошенничества // Cnews.ru. – 2006. – 8 августа. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/...

[3] Европейская БД об эммигрантах содержит уязвимости // Cnews.ru/ news. – 2007. – 15 ноября. [Электронный ресурс]. – Режим доступа: http://safe.cnews.ru/news/line/index...

використовуючи для цього енергію від зовнішнього сигналу, який приймається пристроєм. Так званий RFID-документ досить просто піднести на недалеку відстань від зчитувального пристрою, і система контролю за наявності позитивного результату відкриє доступ.

RFID-мікрочіпи – це інтегральні мікросхеми, що здатні за радіоканалами приймати інформацію у цифровому електронному вигляді та передавати за допомогою тих же каналів результат її обробки.

Визначають так звані «активні» та «пасивні» мікрочіпи. Активні мікрочіпи мають власне джерело живлення – мініатюрний акумулятор, пасивні живляться за допомогою енергії, що надходить із радіохвилями, які випромінює зчитувальний пристрій. У документах застосовуються, як правило, пасивні мікрочіпи[1].

За підсумком проведених досліджень встановлено, що сканування на відстані широко розповсюджених нині RFID-міток дозволяє створювати абсолютно ідентичні їх копії. Скопіювати персональні дані біометричного паспорта, перебуваючи на відстані декількох метрів від його власника, дійсно неможливо, але нідерландські експериментатори змогли зробити це з відстані 30 см, британські 7,5 см – і це, зважаючи на те, що за офіційними повідомленнями інформація з документа повинна зчитуватися з відстані не більше 2 см[2].

Отже, з'являється можливість «клонувати» електронні оригінали документів. Якщо зловмисник може, пройшовши повз людину, просканувати документ із RFID-чіпом, який є у кишені, портфелі (дипломаті), сумочці або у іншому місці, а потім виготовити його абсолютно тотожну електронну копію, для контрольної системи він стане ідентичним клоном власника документа.

RFID-системи, у випадках їх використання без застосування певних заходів захисту, потенційно є надзвичайно вразливими. Сутність проблеми полягає у тому, що будь-який зчитувальний пристрій, що перебуває в межах можливого прийому радіохвиль, які репродуктуються RFID-чіпами, може записати їх у свою пам'ять. Лабораторія RSA (Bedford, Massachusetts, USA) розробила систему блокування випромінювання радіоміток від випадкового зчитувача і, таким чином, вважається, що проблема частково вирішена.

Одним із найефективніших рішень з захисту RFID-чіпів є використання футлярів, які зроблені повністю з металу, – вони забезпечують повне екранування документів з мікрочіпами, що є у середині. Альтернатива металевому футляру – обгортання документа з вмонтованим мікрочіпом гнучкою металевою сіткою. Сітка може бути розміщена в підкладці шкіряного гаманця, портмоне або в будь-якому іншому аксесуарі, що має призначення для зберігання та носіння документів.

Ефективність такої конструкції трохи менша, ніж у металевого футляра, проте є цілком достатньою, щоб у більшості випадків уберегти мікрочіп документа від несанкціонованого зчитування. Такі захисні вироби відомі під брендом GARDE D'INFO (див. www.garde-dinfo.com або www.united-it.ru)[3].

Найпростішим захисним рішенням є обгортання документів простою алюмінієвою фольгою.

---

[1] Как защитить биометрический паспорт? // GARDE D'INFO. – 2008. – 29 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Гуриев В. Восход Европы: электронные паспорта в России / В. Гуриев, Р. Насакин, К. Курбатов // Компьютерра. – 2007. – № 8. – 1 марта. [Электронный ресурс]. – Режим доступа: http://offline.computerra.ru/2007/676/309158/, http://biometrics.ru/document.asp...

[3] Как защитить биометрический паспорт? // GARDE D'INFO. – 2008. – 29 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Учені з Імперського коледжу Лондона й Даремського університету запропонували досить оригінальний варіант боротьби з можливістю підробки документів. Система лазерної ідентифікації поверхні «Laser Surface Authentication» (LSA) сканує найдрібніші нерівності оригіналу документа з паперу, пластика, металу або кераміки, який пред'являється для контролю, та малює своєрідну картину зліпка його поверхні. Отже, силові структури і насамперед правоохоронні органи можуть отримати новий досить дешевий спосіб перевірки дійсності паспортів, особистих посвідчень, кредитних карток, грошових банкнотів, CD і DVD із програмним забезпеченням.

Мікроскопічні неоднорідності на поверхні матеріалу об'єкта, що перевіряється, скануються за допомогою дешевого портативного лазерного сканера. Отримане зображення кодується разом з унікальним серійним номером і вноситься до бази даних. Коли потрібно буде підтвердження достовірності документа, його поверхня буде знову відсканована, а одержана інформація звірена з відомостями, що зберігаються у базі даних[1].

Уряди країн, які запроваджують біометричні системи, повинні ретельно продумувати і зважувати кожен крок щодо впровадження біометричних технологій та створення відповідних державних систем, інакше передумови можливого майбутнього краху цього важливого заходу в боротьбі з тероризмом, нелегальною міграцією і злочинністю, зокрема й міжнародною, будуть, по суті, закладені безпосередньо в саму концепцію цих програм.

Зважаючи на такий факт, що біометричні технології відіграють дедалі важливішу роль у цивільній інфраструктурі, вони повинні ставати більш функціонально гнучкими, сумісними, зручними, надійними, особливо захищеними та мати можливість у разі потреби до модифікації.

На підтвердження цієї тези можна навести такий досить яскравий приклад. Ідентифікацію на основі ДНК нині прийнято вважати одним із наймогутніших інструментів у боротьбі правоохоронних органів зі злочинністю та й загалом під час проведення судових розслідувань. На відміну від дактилоскопії, для ДНК-аналізу розраховані оцінки ймовірності можливих помилок упізнання, і вона є дійсно надто мала. У судовій практиці вже є достатньо прикладів, коли саме ДНК-аналіз допоміг виправити помилки недостовірної ідентифікації за відбитками пальців і реабілітувати несправедливо засуджених або заарештованих людей. Тому навколо цього методу аналізу сформувався ореол якогось абсолютного засобу встановлення істини, під час використання якого нібито ніколи не допускають помилок і який практично має стовідсоткову надійність. У масовій свідомості сформувалася певна думка, що сліди ДНК підробити практично неможливо. Але реальна картина виглядає інакше.

Австралійський учений-біотехнолог Девід Беррімен з Університету Мердока під час проведення експериментів встановив, що знайомому з біотехнологіями зловмисникові ефективно підробити ДНК-сліди, в принципі, зовсім не складно. Стурбований своїм відкриттям дослідник звернувся до відповідних інстанцій, намагаючись попередити про потенційну небезпеку поліцію та судові органи, проте жодної реакції у властей ця новина не викликала. Тоді Д. Беррімен звернувся до тележурналістів, які й відзняли на цю тему матеріал, що був показаний на австралійському телебаченню ще у вересні 2004 року.

Для додання сюжету більшого драматизму цю передачу зробили у вигляді інсценування злочину, коли реальні краплі крові, мимоволі залишені злочинцем на місці

[1] Губайловский В. Трудности и опасности внедрения биометрических паспортов / В. Губайловский // Радио «Свобода». – 2005. – 9 сентября. [Электронный ресурс]. – Режим доступа: http://www.svoboda.org/ll/sci/..., http://biometrics.ru/document.asp...

«вбивства», були експериментатором обприскані із заздалегідь підготовленого флакона з концентрованим розчином чужої ДНК. Після чого відставний поліцейський експерт із ДНК-аналізу провів дослідження зразків, вилучених із місця події, та зробив висновок, в якому однозначно було вказано, що зібрані на місці події зразки крові належали не реальному «вбивцеві», а зовсім іншій людині, ДНК-розчин якої зберігався у флаконі.

Виникає питання, наскільки складно зловмисникові отримати ДНК іншої людини, щоб виготовити спрей із змістом чужої ДНК і «підставити» когось замість себе? Як виявилось, зробити це, по суті, не складніше, ніж отримати чийсь відбиток пальця. Можна дістати склянку зі зразком слини, що залишилася на його краєчку, або недопалок сигарети, або волосок із коренем, що випав із голови. У будь-якому з цих перелічених зразків достатньо молекул ДНК, які за поміщення у так звану машину полімерної ланцюгової реакції (PCR) можуть із великою швидкістю розмножуватись, і в результаті одержують ДНК-молекули в мільярдах або трильйонах копій. Через декілька годин роботи PCR-машини отриманої кількості ДНК-спрею буде досить, щоб наповнити весь об'єм парфумерного флакона. За висновком експертів, цього об'єму цілком достатньо, щоб приховати будь-який компрометуючий ДНК-слід на місці злочину, для чого потрібно лише обприскати місце події виготовленим спреєм із флакона.

Звичайно, можна стверджувати, що PCR-машини є досить дорогими і не можуть бути легкодоступними для злочинців. Проте в цьому випадку не настільки важлива можливість придбання стерильного PCR-апарату, як сам факт можливості виготовлення ДНК-спрею шляхом підбору відповідного режиму процесу розігріву й охолодження. У принципі, позитивний результат можна одержати і за допомогою каструлі на кухні, маючи під рукою теплу та холодну воду і швидкореагуючий термометр. Крім того, добре відомо, що якщо на ринку кримінальних послуг з'являється стійкий попит на будь-яку технологію, то зловмисники успішно освоюють і достатньо складні технологічні процеси.

Фальшивий ДНК-доказ поки що не набув поширення. Але зовсім не тому, що це технічно зробити доволі складно. Як свідчить кримінальна статистика, понад 50% усіх злочинів здійснюють люди, які перебувають у стані алкогольного або наркотичного сп'яніння, а їх часто не турбує не тільки наявність слідів ДНК, але навіть залишення на місці злочину слідів відбитків пальців. Інша ж частина злочинців, навіть якщо вони тверезі й розумні, зазвичай обирають простіші, але не менш ефективніші способи для досягнення своєї мети, ніж труднощі з використанням технології розмноження чужої ДНК.

Проте слід пам'ятати і зважати під час проведення розслідувань на те, що підробка ДНК-доказу абсолютно можлива, але цей факт може відбутися лише в тому випадку, якщо він комусь дійсно потрібен[1].

Отже, можна зробити висновок, що регулярне оновлення технологій захисту біометричних документів, а також використання на їх основі систем повинно стати головним завданням і для розробників, і споживачів, оскільки цілком очевидно, що створення муляжів або апаратно-технологічних рішень, які б дозволяли обходити розроблені процедури контролю за будь-якою ознакою, справа лише часу, грошей і техніки.

Розглянемо існуючі та можливі проблеми, що виникають або можуть виникнути під час використання смартфонів і гаджетів, особливо під час використання у платіжних системах, зокрема для підтвердження покупок на «itunes» і в «App Store».

Улітку 2013 року були розголошені матеріали щодо програми тотального електронного стеження за іноземцями та потенційно всіма громадянами США під назвою

[1] Берд Киви. Улики под сомнением / Киви Берд // Компьютерра. – 2007. – № 27–28. – 1 августа. [Электронный ресурс]. – Режим доступа: http://offline.computerra.ru/2007/695/327708/

«Prism». За програмою «Prism», американські спецслужби NSA і FBI мають доступ до центральних серверів дев'яти провідних Інтернет-компаній: «Microsoft» (з 2007 року), «Yahoo» (2008), «Google», «Facebook», «Paltalk» (усі три з 2009 року), «Youtube» (2010), «AOL», «Skype», (обидві з 2011 року) і «Apple» (2012) для доступу та копіювання аудіо- та відеочатів, фотографій, електронних листів, пересилаючих файлів документів, логінів зв'язку, пошукових алгоритмів, персональних даних учасників соціальних мереж[1].

У вересні того ж року дактилоскопічний сканер Touch ID став одним із найбільш очікуваних функціональних оновлень нової моделі смартфона «Apple» iPhone 5S. Звісно, зважаючи на останні події, пов'язані з програмою «Prism», власників iPhone 5S дуже цікавить механізм захисту перебуваючих у пам'яті пристрою біометричних відбитків пальців. Фахівці «Apple» повідомили, що конфіденційна інформація зберігається в зашифрованому виді безпосередньо в процесорі A7 і не використовується жодними іншими додатками. Вони запевняють, що стороння особа (чи то розробник додатків чи агент ЦРУ) жодним чином не зможе отримати зображення відбитка користувача.

На думку експерта в сфері безпеки Брюса Шнайєра, такий підхід є досить розумним, оскільки у випадку зберігання біометричних відбитків пальців у централізованій базі даних можливий злом централізованої системи, що підключена до Інтернету. Тоді хакерам могла стати доступною відразу величезна база біометричної інформації. Однак Б. Шнайєр практично не сумнівається в можливості злому окремого смартфона, але збитки водночас будуть набагато меншими, ніж за несанкціонованого доступу до загальної бази даних.

Фахівці в сфері безпеки називають й інші проблеми, які виникають під час використання датчиків відбитків пальців. Насамперед це загальна проблема всіх біометричних систем, яка полягає в тому, що, на відміну від паролів або шифрувальних ключів, поки що не існує абсолютно надійного способу зберегти в таємниці характеристики унікальних фізичних об'єктів – чи то відбитки пальців, малюнок райдужки ока або навіть форма вуха. Ця інформація може бути доступною всім зацікавленим особам, а «добути пальчики» є доволі простим завданням. Люди постійно доторкаються руками до величезної кількості предметів, а зняти з речей відбиток пальця є справою техніки. А скомпрометований відбиток пальця неможливо поміняти з такою ж легкістю, як символьний пароль.

Але найбільш обґрунтоване занепокоєння в експертів із безпеки викликає можливість використовувати Touch ID для підтвердження покупок на «itunes» і в «App Store». Оскільки в «Apple» стверджують, що відбитки пальців – точніше, їхні цифрові сигнатури – не залишають корпусу смартфона, то тоді виникає запитання: що ж тоді відсилається через Інтернет для ідентифікації? Перехопивши ці індентифікаційні ключі, можна й без злому системи біометрії одержати доступ до акаунта користувача та, можливо, навіть до самого смартфона через встановлення програм «троянських» псевдооновлень. Отже, поки незалежні фахівці не перевірять захист реальних пристроїв, встановити серйозність загроз неможливо.

Немаючи досвіду практичної експлуатації iPhone 5S із системою Touch ID, складно однозначно вказати і на чесноти цього смартфона, і на його недоліки. З одного боку, дактилоскопічний датчик спрощує захист апарату від несанкціонованого доступу та робить більш комфортними покупки в «itunes» і «App Store». З іншого – виникають

[1] Prism – глобальная машина наблюдения: как США уничтожают свободу в мире // REGNUM. – 2013. – 13 июня. [Электронный ресурс]. – Режим доступа: http://regnum.ru/news/fd-abroad/ukraina/...

обґрунтовані сумніви в безпеці транзакцій через Інтернет. Водночас потрібно брати до уваги інтелектуальну обдарованість хакерів – «романтиків з великої дороги»[1].

Ще один приклад – ідентифікація за обличчям індивідуума. Представники «Google» ще у 2011 році визнали, що система розблокування за допомогою розпізнавання обличчя користувача Face Unlock, що стала одним із найбільш помітних нововведень у четвертій версії операційної системи (ОС) Android, поки що «працює не зовсім так, як було задумано». Face Unlock можна обдурити, «підсунувши» замість лиця власника його фотографію. У «Google» стверджують, що кінцева версія Face Unlock зможе успішно відрізнити живе обличчя від фото[2].

Наведені приклади проблем, що виникають під час використання біометричних смартфонів і гаджетів нічим не відрізняються від загальних проблем біометричних технологій, які існують за дистанційного візуального неконтрольованого підключення до систем контролю за доступом.

Тому ще раз підкреслимо, що однією з важливих характеристик програмно-апаратних біометричних комплексів є їх здатність виявлення муляжів і надійний захист від можливого перехоплення біометричних даних.

[1] Apple touch ID: «за» и «против» сканера отпечатков пальцев в смартфоне // Компьютера-Онлайн. – 2013. – 13 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрическая идентификация в мобильных устройствах: не всё так просто // Версии.com. – 2011. – 25 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

СПЕЦІАЛЬНА ЧАСТИНА

Розділ 9

НАЦІОНАЛЬНА БЕЗПЕКА В XXI СТОЛІТТІ ТА ДЕЯКІ ДОДАТКОВІ ЗАХОДИ ЩОДО ЇЇ ЗАБЕЗПЕЧЕННЯ

Проблема забезпечення адекватної національної безпеки завжди була викликом для урядів усіх країн. Але якщо раніше було потрібно запобігати озброєним вторгненням ворожих сусідів, то в XXI столітті, окрім запобігання цій традиційній небезпеці, виникла необхідність адекватно відповідати на зовсім інші типи загроз.

Характер цих загроз визначають сформовані нині загальносвітові тенденції розвитку. До них належать глобалізація та негативна реакція на неї, активізація недержавних структур із потенціалом, який у деяких випадках дорівнює можливостям низки країн, наявність глобального інформаційного середовища, створеного інтернетом і супутниковими засобами зв'язку. І поки світова спільнота не навчиться належно нейтралізувати такі загрози, будь-який розумний супротивник буде використовувати їх.

Зараз у світі, як стверджував директор національної розвідки США адмірал Майк Макконнелл у доповіді «Глобальні тенденції 2025», що була представлена Національній раді з розвідки Сполучених Штатів Америки, спостерігається не тільки зростання впливу на світову ситуацію групи країн, але й деяких недержавних формувань. До них належать терористичні організації, об'єднання бізнесменів і міжнародні кримінальні угруповування. Їх вплив на стан міжнародної обстановки щороку збільшується і, як не дивно, його стимулює розвиток нових технологій.

Найімовірнішим варіантом майбутніх змін аналітики розвідувального співтовариства, за висловленням їх шефа, вважають перехід «стратегічного суперництва до зон торгівлі, демографії, а також у сферу доступу до природних ресурсів, інвестицій та технологічних нововведень».

Причому боротьба за технологічну перевагу стане ключовим чинником в отриманні домінуючого впливу в майбутньому[1].

Мегатрендом XXI століття став процес глобалізації. Будучи об'єктивним історичним процесом, глобалізація має і позитивні, і негативні наслідки для держав і народів світу. Вона створює нові можливості для розвитку, які пов'язані з використанням переваг міжнародного розподілу праці, виробничої кооперації, передачі технологій, управлінсь-

[1] Иванов В. Мир ожидают серьезные потрясения / В. Иванов // Независимое военное обозрение. – 2008. – 19 декабря. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/wars/2008-12-19/1_world.html

кого й організаційного досвіду, більш ефективної мобілізації ресурсів, зокрема й людських. Розширюються торгово-економічні, фінансові, міждержавні й транскордонні соціальні взаємини. Але глобалізація – це й зростаюча прозорість кордонів для нелегальної імміграції, організованої злочинності, міжнародного тероризму, наркотрафіка, вірусних інфекцій, інформаційної агресії тощо. Глобалізація одночасно і роз'єднує світ, загострюючи відмінності та суперечності, провокуючи водночас безліч конфліктів[1].

Значна кількість загроз для внутрішньої безпеки будь-якої розвиненої держави нині виходить від політично вмотивованих, незадоволених, позбавлених цивільних прав індивідуумів, які підтримують зв'язки з терористичними рухами в інших країнах, основними джерелами фінансування яких є доходи від контрабанди, незаконного відмивання грошей та іншої злочинної діяльності.

Сучасний підхід до національної безпеки містить інтегроване поєднання і політичних, і технологічно передових внутрішніх і глобальних систем безпеки, які загалом повинні бути пристосовані як до міжнародних, так і національних умов і можливостей. Під час розробки доктрини національної безпеки будь-якої розвиненої держави в XXI столітті повинні бути взяті до уваги і глобальні вимоги, і місцеві культурні та соціальні особливості. На думку канцлера ФРН і голови ХДС Ангели Меркель, що була висловлена 3 грудня 2007 року на з'їзді Християнсько-демократичного союзу (ХДС), в сучасних умовах «немає відмінності між зовнішньою та внутрішньою безпекою»[2].

У червні 2013 року були оприлюднені надані колишнім співробітником американського Агентства національної безпеки (АНБ) Едвардом Сноуденом матеріали щодо американської програми Prism. Це суперпрограма, яка використовується для аналізу інформації в глобальних соціальних мережах і яка дозволяє спецслужбам одержувати прямий доступ до серверів майже всіх провідних Інтернет компаній. Секретно затверджена судом програма Prism орієнтована на закордонний трафік зв'язку, який майже завжди проходить через сервери США, навіть за умови знаходження відправника й отримувача за межами кордонів Сполучених Штатів Америки. Викриття Е. Сноудена стало найбільшим витоком інформації про діяльність Агентства національної безпеки (National Security Agency /NSA/) за весь час існування цієї організації[3].

NSA збирає приблизно п'ять мільярдів записів про пересування мобільних телефонів за один день, про що свідчать цілком таємні документи та інтерв'ю з співробітниками американської розвідки. Це допомагає відслідковувати пересування людей та фіксувати їх місцезнаходження. Ці відомості надходять у величезну базу даних, де зберігається інформація як мінімум декілька сотен мільйонів мобільних пристроїв. Спеціальні новітні програмно-комп'ютерні проекти, які були створені для аналізу даних, забезпечили американське розвідтовариство інструментом тотального стеження.

За своїм масштабом і потенційними наслідками для недоторканості приватного життя дії щодо збору й аналізу відомостей про місцезнаходження перевершують усі інші програми стеження АНБ /NSA/. Аналітики можуть вирахувати стільниковий телефон у будь-якому місці світу, відслідкувати його пересування у минулому та встановити таємні зв'язки між людьми, які телефонували на конкретний номер.

---

[1] Глобализация как мегатренд мирового развития // Geopolitica.ru. – 2013. – 29 апреля. [Электронный ресурс]. – Режим доступа: http://oko-planet.su/...

[2] В Германии планируют ввести «онлайн-обыски» // Эксперт-центр. – 2007. – 3 декабря. [Электронный ресурс]. – Режим доступа: http://www.expert.org.ua/statias/...

[3] Prism – глобальная машина наблюдения: как США уничтожают свободу в мире // Regnum.ru. – 2013. – 13 июня. [Электронный ресурс]. – Режим доступа: http://regnum.ru/news/fd-abroad/ukraina/...

Агентство національної безпеки збирає ці відомості в одну базу даних, оскільки його дуже потужні аналітичні засоби, відомі під назвою CO-TRAVELER, дозволяють відшукувати невідомих однодумців відомих об'єктів стеження, слідкуючи за тим, де їх пересування збігаються або перехрещуються. Сучасні математичні методи дозволяють аналітикам NSA фіксувати відносини власників стільникових телефонів, зіставляючи маршрути їх пересування за тривалий час із тисячами й мільйонами інших абонентів стільникового зв'язку, які трапляються їм на шляху. CO-TRAVELER та інші програми вимагають методичного збору та зберігання відомостей про місцеперебування буквально у планетарному масштабі.

Якщо ознайомитись із документами Е. Сноудена, то можливості АНБ щодо визначення місцеперебування просто приголомшують. Вони вказують на те, що агенство може звести нанівець будь-які спроби забезпечити безпеку та таємність зв'язку. Головна риса використовуваних інструметів та, що конкретна ціль їм наперед невідома і вона навіть не знаходиться під підозрою.

Вони працюють із відомостями у сховищі Агентства національної безпеки FASCIA, де зберігаються трильйони записів метаданих, серед яких є і відомості про місцезнаходження, що становлять немалу, але невідому частину[1].

Виникає питання, де можуть знаходитися потужні сховища National Security Agency? Американський експерт Джеймс Бемфорд у 2012 році повідомляв, що американське NSA – спецслужба, що спеціалізується на зборі інформації та зломі захисних кодів, – будує в пустелі в штаті Юта найбільше сховище даних: так званий «Центр даних Юти». Д. Бемфорд у своїй публікації стверджував, що «Центр даних Юти» буде останнім елементом колосального комплексу стеження АНБ.

«У Юті будуть оброблятися не тільки змісти електронних листів, телефонних розмов і пошукових запитів Google, але й інші особисті дані, наприклад, штрафи за неправильне паркування, маршрути подорожей, купівля книг та інші електронні сліди. Центр повинен бути в змозі зберігати й обробляти всі дані, які NSA збирає в усьому світі та у межах США», – повідомляв експерт. За інформацією Д. Бемфорда, сервера в новому центрі займають площу в 8000 кв. м, а сховища даних – 275 000 кв. м. До відома: сьогодні у чіп розміром із ніготь вміщується терабайт даних.

Світовий інтернет-трафік із 2010 до 2015 року зросте в чотири рази та сягне обсягу в 966 ексабайтів (дані фірми «Cisco»). А мільйон ексабайтів – це йоттабайт. За відомостями Д. Бемфорда, NSA зможе зберігати й обробляти декілька йоттабайтів даних (йоттабайт /англ. *yottabyte* – септібайт/ – одиниця виміру кількості інформації, яка дорівнює 10^{24} байтам), тобто сховище дозволяє повністю зберігати глобальний трафік інтернету за декілька років.

За даними Джеймса Бемфорда, восени 2013 року центр, вартість якого становить приблизно 2 млрд доларів, почав працювати та дозволив втілити у життя ідею тотальної обробки практично світового трафіку інформації[2]. Також американський фахівець повідомив, що NSA має всі необхідні технології, щоб за потреби прослухати та записати кожну телефонну розмову, одержати доступ до будь-якої електронно-поштової скриньки, перехопити дані про фінансові транзакції та зламати захист будь-якої закритої бази

[1] Геллман Бартон. АНБ следит за мобильными телефонами по всему миру, об этом говорят документы Сноудена / Бартон Геллман (Barton Gellman), Ашкан Солтани (Ashkan Soltani) // Первоисточник: «The Washington Post», США». – 2013. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://www.inosmi.ru/world/20131205/215422549.html

[2] В будущем за нами будут следить сверхтщательно // Die Welt. – 2012. – 22 августа. [Электронный ресурс]. – Режим доступа: http://www.inopressa.ru/article/22aug2012/welt/cyber.html

даних. Але це ще не все. Ще одна новина полягає у тому, що декілька років тому АНБ зробило «колосальний прорив» у галузі криптографії, і тепер агентство може дешифровувати надзвичайно складні коди за допомогою одного з трьох надпотужних світових суперкомп'ютерів.

Отже, після відкриття архівного сховища восени 2013 року в м. Блаффдейлі (штат Юта) Агентство національної безпеки (National Security Agency) практично повністю реалізувало ідею тотальної обробки електронної інформації, що дозволило їй стати найбільшою та потенційно найагресивнішою утаємниченою спецслужбою в історії людства[1].

Але професор Марк Мануліс, фахівець із прикладної криптографії в Університеті Сюррея вважає, що одним із дієвих та ефективних способів захисту європейських конфіденційних відомостей від перехоплення є широке застосування криптографічних методів захисту даних. За його словами шифрування було спеціально придумано для захисту даних у небезпечних мережах. Якщо електронного листа правильно зашифрувати, то неважливо, за якими мережами воно передається. На його думку, дані повинні шифруватися не тільки в процесі передачі, але й під час зберігання, що дає можливість контролювати їх використання за будь-якого звернення до них.

Що стосується пропозиції А. Меркель створити інтернет в обхід території США, то фахівці зі сфери мережевої безпеки вважають, що ці плани канцлера Німеччини ігнорують реальний стан інформаційних мереж у світі та можуть підірвати надійність і стійкість інформаційно-комунікаційних технологій зв'язку[2].

У XXI сторіччі набули поширення такі терміни, як «мережева війна» та «кібервійна». Мережеві війни (Netwar) є новітньою технологією захоплення простору, відторгнення територій і зміни влади в державах без використання звичайних озброєнь. Вона ведеться з використанням інформаційних технологій, дипломатичних мереж, неурядових організацій, із підключенням ЗМІ, журналістів, блогерів і т. д.

Мережева операція визначається як сукупність дій, спрямованих на формування поведінки нейтральних сил, ворогів і друзів у ситуаціях миру, кризи та війни і здійснюється як до початку гарячої фази (військової операції), так і під час її проведення (щоб за можливості курувати й управляти всіма процесами на території ворога), а особливо – після завершення гарячої фази – для того, щоб у свідомості мас зафіксувати та закріпити результати[3].

Нині інформаційне протиборство дедалі більше переноситься у віртуальний простір. Водночас інформаційно-комунікаційні технології (ІКТ) значно розширюють можливості традиційної інформаційної війни, а саме: розвідувальної діяльності, підтримки наземних операцій, впливу на супротивника та захисту власних сил, ведення радіоелектронної боротьби. З'явилась можливість проведення самостійних операцій у кіберпросторі, завдати удар по критично важливій інфраструктурі ворога.

Це стало можливим через те, що сьогодні більша частина світу перебуває під впливом розвитку ІКТ. Залежність держав від інформаційної інфраструктури надає не тільки певні переваги, але й створює можливості для кібератак і кібертероризму

[1] В штате Юта строится хранилище данных, где будет сохраняться информация о каждом американце // Uipdp.com. – 2012. – 29 марта. [Электронный ресурс]. – Режим доступа: http://www.bezpeka.com/ru/news/...

[2] Европа может обрести свою собственную отдельную часть интернета, если предложения канцлера Ангелы Меркель получат поддержку // BBC. – 2014. – 18 февраля. [Электронный ресурс]. – Режим доступа: http://www.bbc.co.uk/russian/society/...

[3] Коровин Валерий. Сетевые войны: в сторону широких масс / В. Коровин // Евразия. – 2013. – 20 апреля. [Электронный ресурс]. – Режим доступа: http://evrazia.org/article/2349

в інформаційно-комунікаційному просторі розвинутих країн. Кібертероризм є одним із видів негативного використання ІКТ у терористичних цілях. Відомо, що «Аль-Каїда» спеціально вербувала людей, які добре підготовлені в сфері інформаційних технологій, та навчала основам інформатики своїх оперативних працівників.

Інтернет – це потужний інструмент, який дозволяє підбурювати до терористичних актів, вербувати нових членів терористичних груп, поповнювати фінансові фонди та здійснювати атаки на мережеву державну інфраструктуру.

На думку більшості експертів, кібертероризм став різновидом так званого супертероризму, характерною рисою якого є використання або погроза застосування у терористичних цілях найбільш передових озброєнь і технологій, що можуть спричинити масове ураження населення або завдання відчутного економічного або екологічного збитку. Нині кібертероризм має серйозний потенціал руйнування, оскільки багато критичних інфраструктур розвинутих держав зв'язані з зовнішнім світом через комп'ютерні мережі.

У Національній стратегії Сполучених Штатів Америки з забезпечення безпеки кіберпростору 2003 року особливо було підкреслено, що через складність, а часто неможливость визначення джерел загроз у кіберпросторі необхідно зосередитися на головному – запобіганні кібератак проти критично важливої інфраструктури держави, зниженні її вразливості, мінімізації збитків і часу відновлення у випадку вчиненого нападу. Також чітко було зазначено, що уряд має право контрудару в прийнятній формі, якщо США будуть піддані комп'ютерному нападу. Як відповідні дії розглядається застосування кіберозброї або спеціальних шкідливих комп'ютерних кодів (програм-вірусів), спроектованих для атак і виведення з ладу ворожих керуючих комп'ютерних систем. Такою інформаційно-електронною протидією займається спільний центр інформаційних операцій у Стратегічному командуванні Сполучених Штатів Америки. У ньому утворена спеціальна об'єднана оперативна група глобальних мережних операцій, яка координує та спрямовує дії з захисту комп'ютерних мереж і систем Міністерства оборони. Але ця група не тільки захищає, а за відповідним наказом розпочинає атакуючі дії проти ворожих комп'ютерних мереж із метою виконання завдань національної оборони[1].

За відомостями фахівців «Symantec», яка є однією із провідних світових компаній із виробництва програмного забезпечення (ПЗ), програм антивірусної та інформаційної безпеки, Інтернет-співтовариство вийшло на такий рівень віртуальних відносин, коли антивірусні програми стали лише умовним захистом ПЗ, а кіберзлочинці значно випереджають тих, хто розробляє та поширює захисні програми від кібератак. Цей факт підтверджує тезу, що від дій злочинців не захищені не тільки комп'ютери звичайних користувачів, але й стратегічні об'єкти. Наприклад, у США це програмно-комп'ютерні комплекси, що обслуговують НАСА, атомні електростанції, ядерні спецоб'єкти тощо.

За наявними відомостями, у 2012 році урядові структури США були піддані кібернападам 12 млн раз, комп'ютерна мережа іракського уряду отримала кіберудар у 28 млн атак, а інформаційні ресурси Ізраїлю загалом атакувалися 44 млн раз[2].

Загальновідомо, що сфера бізнесу постійно вимагає розробки нових методик, новітніх технологій, впровадження винаходів. Технічна документація, креслення, інші матеріали – нині розробляються та зберігаються на комп'ютерних ресурсах. Таємні держав-

[1] Золотарев Владимир. Психологическая война уже в киберпространстве / В. Золотарев // Военно-промышленный курьер. – 2013. – 24 апреля. [Электронный ресурс]. – Режим доступа: http://vpk-news.ru/articles/15620

[2] Бовал Валерий. Киберпротивостояние-2013: прогнозы экспертов / В. Бовал // Военное обозрение. – 2013. – 21 января. [Электронный ресурс]. – Режим доступа: http://topwar.ru/23154-kiberprotivostoyanie-2013-prognozy-ekspertov.html

ні відомості також зберігаються на закритих електронних ресурсах. Тому поширилося розкрадання таємних відомостей із мереж і баз даних державних установ і компаній різних форм власності. Багато держав фінансують розробки в галузі створення кіберзброї, які стають засобом шпигунства.

Відповідно до звітів ФБР США, щорічні втрати бізнесу країни від економічного та промислового шпигунства становлять майже 100 млрд доларів. Значну частину в загальний обсяг втрат Сполучених Штатів Америки, як жодної іншої країни світу, вносить кібершпіонаж, який є однією з головних складових і економічного, і промислового шпигунства. Така ситуація стала можливою тому, що Америка набагато сильніше, ніж інші держави, залежить від мережевої інфраструктури: тут зосереджено понад 40% обчислювальних ресурсів світу та приблизно 60% інформаційних ресурсів Інтернету. Проведений американськими спеціалістами аналіз свідчить, що в 58% випадків економічне та промислове шпигунство здійснювалося за завданням закордонних компаній, в 22% – в інтересах іноземних урядів і в 20% – приватних і державних закордонних наукових центрів і лабораторій.

За відомостями Американського товариства промислової безпеки при промисловому шпигунстві, найбільшу цінність для конкуруючих компаній становить інформація про наукові дослідження та розробки (49%).

За заявою голови Робочої групи з безпеки в економіці ФРН Бертольда Штоппелькампа, в Німеччині викрадення секретів виробництва (ноу-хау) компаніями інших країн обходиться економіці держави у суму приблизно 20 млрд євро щороку. За даними німецьких дослідників найцікавіші для промислових шпигунів наукові дослідження та конструкторські розробки (16%). Основними заходами незаконного одержання конфіденційної інформації були: вербування співробітників конкуруючих організацій; одержання інформації через дилерів і консультантів; хакерські атаки на комп'ютерні системи; перехоплення електронних повідомлень; крадіжка документів, матеріалів і зразків; прослуховування та перехоплення конфіденційних переговорів.

У Великобританії, за інформацією Управління комп'ютерної безпеки й інформаційної надійності (OCSIA), втрати британських корпорацій у 2012 році через крадіжки конфіденційних даних і різних комерційних таємниць становили майже 9,2 млрд фунтів стерлінгів.

В Японії, за підсумком перевірки 625 підприємств, яку здійснило Міністерство економіки, торгівлі та промисловості, було встановлено, що в 224 з них (35,8%) були випадки витоку інформації внаслідок промислового шпигунства. Основними виявленими методами промислового шпигунства були: копіювання працівниками за грошову винагороду від конкурентів конфіденційних документів, зокрема й електронних баз даних; одержання інформації через співробітників, які були запрошені працювати за сумісництвом у конкуруючі компанії; через бізнес-партнерів – постачальників устаткування та матеріалів[1].

Глобальна війна проти тероризму звернула увагу світової громадськості на боротьбу з загрозами вчинення терористичних актів, жертвами яких є невинне цивільне населення. Зростаюча загроза світовій безпеці, бажання людей мати гарантований особистий захист і поява нових технологій стимулюють розвиток охоронних, зокрема і біометричних систем. Нині спостерігається зростання особливої уваги до систем інтелектуаль-

[1] Кравцов Андрей. Сезон охоты на секреты российского ОПК / А. Кравцов // Независимое военное обозрение. – 2013. – 9 августа. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/nvo/...

ного відеоспостереження, одним із завдань якої стала ідентифікація індивідуума за його відеозображенням у режимі реального часу. Спецслужби насамперед зацікавлені в автоматизації процесу виявлення осіб, які підозрюються у скоєнні будь-яких злочинних діянь або в намірі їх учинення. Технологія відеонагляду, яка спочатку призначалась для контролю й обліку звичайних правопорушень, еволюціонувала в технічні комплекси для захисту від тероризму[1].

Досить значні політичні й економічні збитки національним інтересам завдають мігранти та незаконне контрабандне переміщення товарів через державний кордон. Контрабанда завдає суттєвого удару доходу уряду будь-якої країни, навіть якщо не брати до уваги ту шкоду, яку вона завдає міжнародним відносинам, оскільки контрабандні дії вчиняються з території сусідніх держав, а її маршрути можуть проходити через треті країни. Свого часу колишній британський прем'єр-міністр Т. Блер заявив: Загроза безпеці, перед якою ми стоїмо, не є звичайною. Це виклик зовсім іншого походження порівняно з тим, що ми мали раніше.

Нелегальна економічна імміграція становить серйозну загрозу розвиткові економіки будь-якої країни та забезпеченню зайнятості своєї робочої сили, якщо вона здійснюється безконтрольно. Серед мігрантів є певна частка злочинних елементів, які ухилилися від здійснення правосуддя у власній країні та навряд чи змінять свій спосіб життя після прибуття в іншу державу, де вони також будуть становити загрозу для законності та порядку. Ці кримінальні елементи повинні бути ізольовані або принаймні взяті під нагляд так, щоб ці дії не обмежували права та свободи законослухняного населення. Але під час реалізації цього завдання, що пов'язане з забезпеченням внутрішньої безпеки держави, можна істотно ускладнити повсякденне життя власних громадян, а це може завдати шкоди владі, яка намагається захистити своє населення від злочинних посягань[2].

Нині, коли загрозу національній безпеці більшості країн становлять тероризм, міграція, організована злочинність, розповсюдження зброї, наркотрафік, всезростаюча можливість здійснення терористичних актів за допомогою зброї масового ураження, впровадження досягнень нових технологій разом із розвідувальною діяльністю набуває вирішального значення. Причому можливості систем на основі останніх наукових досягнень повинні слугувати для узагальнення, аналізу, перевірки та доповнення даних агентурної діяльності.

В епоху, коли тероризм став глобальним явищем, а національні можливості прийняття контрзаходів у зв'язку з використанням світових інформаційних комунікацій та електронних фінансових транзакцій, збільшенням вантажоперевезень і пасажиропотоку значно ускладнились, застосування сучасних інформаційно-технологічних досягнень стало ключем до отримання важливих компонентів розвідувальної інформації, яка необхідна для успішного виконання завдань із забезпечення і національної, і глобальної безпеки.

Розгортання майбутньої, по суті, глобальної біометричної паспортної системи та пов'язаною з нею захищеною інфраструктурою обміну даними є суттєвою компонентою серед заходів боротьби з міжнародним тероризмом і складовою структури національної безпеки будь-якої країни світової спільноти.

---

[1] Рынок программного обеспечения для видеонаблюдения: на пути к успеху // Secnews.ru. – 2006. – 18 июля. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/…

[2] Современные средства предотвращения террористических и криминальных угроз // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 10–13.

Сучасна стратегія національної безпеки в обов'язковому порядку повинна містити заходи щодо забезпечення безпеки стратегічно важливих об'єктів, так званої критично важливої національної інфраструктури, до переліку якої входять об'єкти військового і військово-промислового комплексу, атомні й гідрогенеруючі станції, нафтогазопроводи, нафтоперегінні та хімічні заводи – тобто ті об'єкти, які особливо важливі для нормального забезпечення життєдіяльності держави, а аварія або терористичний акт на них може завдати значної шкоди життю та здоров'ю громадянам країни, на території якої сталася надзвичайна подія.

Комплексний облік і управління ризиками безпеки повинне охоплювати забезпечення безпеки держави на різноманітних напрямах (особливо організація інформаційно-технологічної, екологічної та особистої безпеки громадян).

Отже, у XXI столітті необхідне створення такої національної системи безпеки для кожної країни, яка б забезпечувала належний поступальний розвиток і окремо взятої кожної держави, і усієї цивілізації загалом. Тобто національна система безпеки теоретично не повинна завдавати шкоди безпеці інших країн, вона в обов'язковому порядку має брати до уваги та містити елементи глобальної безпеки.

Наведемо приблизний перелік сучасних додаткових заходів із безпеки, що повинні бути в обов'язковому порядку внесені до комплексу заходів національної безпеки держав на додаток до загальноусталених:

1. Електронні контрзаходи. Це складні електронні заходи, які призначені для захисту населення і матеріальних цінностей від можливих застосувань вибухових пристроїв шляхом блокування надходження детонуючого сигналу.

2. Контроль та стеження за використанням каналів зв'язку, зняття важливої з погляду національної безпеки інформації та блокування, за потреби, каналів зв'язку. Це спеціальне устаткування для блокування у разі потреби електронних засобів зв'язку, що охоплюють GSM і стільникові телефони, GPS, супутникові навігаційні сигнали та Інтернет. У разі потреби здійснюється блокування зв'язку і вживаються заходи з протидії ворожому радіоперехопленню.

3. Відкрите і таємне спостереження. Спеціальне обладнання, яке спроектовано для застосування в міській та сільській місцевостях для забезпечення безпеки кордонів і трубопроводів: в цих системах використовуються наземні й щоглові сенсори, авіаційне та супутникове устаткування для отримання відповідних даних. За допомогою радіосигналів ці системи під'єднані до контрольних центрів, вони також мають системи виявлення, розпізнавання об'єктів, обладнані апаратурою для стеження за автомототранспортом і зчитування номерів транспортних засобів.

Під час охорони сухопутних кордонів або трубопроводів повне спостереження може бути забезпечене за допомогою однієї або декількох систем таких, як супутникова система або авіаційна система, які дозволяють фіксувати спроби проникнення в країну в будь-яких інших місцях, крім звичайних прикордонних контрольних пунктів, або виявляти спроби врізки в трубопроводи.

4. Стеження за автотранспортом, фізичними особами й іншими об'єктами. Використовуючи різні технологічні комплекси спостереження, можна стежити за пересуванням автомобілей, фізичних осіб, інших об'єктів, що становлять інтерес, визначати їх місцезнаходження та передавати інформацію до контролюючого центру.

5. Аеропорти та порти. Загальновідомо, що забезпечення нормального функціонування транспортних потоків є найважливішим завданням держави – разом з іншими інфраструктурними галузями транспорт забезпечує базові умови життєдіяльності суспільства. Безперебійна діяльність і стійкий розвиток транспортної галузі є гарантією

цілісності держави, її національної безпеки та поліпшення умов і рівня життя населення. Забезпечення захисту транспортних об'єктів від можливих несанкціонованих дій та незаконного втручання – найважливіше завдання державних органів будь-якої країни.

Організація спостереження на предмет виявлення осіб, які становлять потенційну загрозу життєдіяльності держави, є тільки однією із багатьох проблем забезпечення національної безпеки. Особливу потенційну небезпеку з погляду можливості скоєння терористичних актів становлять місця масового скупчення та пересування людей. Це такі місця, як аеропорти, морські та річкові порти, метро, залізничні або автовокзали. Десятки тисяч людей проходять через ці транспортні вузли, але на практиці неможливо піддати кожного пасажира контролюючому огляду, в зв'язку з чим відповідний контроль і посилене стеження повинно здійснюватися лише за невеликою кількістю дійсно небезпечних і небажаних для нормальної діяльності держави особистостей.

Із початку XXI сторіччя розроблені спеціальні інтелектуальні системи стеження за індивідуумами в громадських місцях, насамперед в аеропортах, вокзалах, метро та портах. Ці системи запрограмовані так, щоб фіксувати підозрілу поведінку та проводять за можливості ідентифікацію персон, поведінка яких є неадекватною, а також контроль за діями осіб, щодо яких здійснюється негласне спостереження.

6. Тимчасове спостереження. Не всі загрози надходять ззовні. Деякі громадяни (дисиденти) країни можуть становити загрозу для законності та порядку, а у деяких випадках для розсіювання несанкціонованих мітингів та інших скупчень людей, які потенційно загрожують громадському порядку, застосовують насильницькі методи з використанням спеціальних сил і засобів. Забезпечення протидії внутрішнім загрозам вимагає проведення тимчасового спостереження та використання відповідних засобів у тих місцях або місцевостях, де застосування систем постійного спостереження та контролю недоцільне. Воно має сенс тільки тоді, коли є відповідна ефективність. Фахівці з безпеки повинні вміти поєднувати тимчасові системи спостереження з стаціонарними місцевими системами безпеки (за їх наявності).

Системи, що використовуються для контролю за пересуванням об'єктів спостереження, повинні бути під'єднані до відповідних телекомунікаційних мереж для надання можливості співробітникам відповідних служб перебувати у постійному контакті з необхідними відомствами як у середині країни, так і за кордоном. Це необхідно для можливості застосування всіх потрібних заходів для вирішення будь-якої нестандартної або кризової ситуації у випадку її виникнення.

Оперативний склад відповідних спецслужб повинен бути добре навченим і мати відповідну кваліфікацію для успішного використання спеціальних систем спостереження під час вжиття заходів із нейтралізації можливих загроз національній безпеці. Владні структури всіх країн повинні робити все для до того, щоб забезпечити безпеку своїх громадян усіма можливими засобами та заходами.

На думку експертів, відповідно до реалій сучасного існування світового співтовариства, альтернативи цьому постулату немає[1].

Поєднання інноваційних технологій, створення державних і міждержавних баз даних, зокрема і з біометричними відомостями, поліпшення обміну інформацією між різними державними та міждержавними органами, що повинні протистояти тероризму, обов'язкова тісна кооперація розвідувальних, поліцейських, військових та інших

[1] Современные средства предотвращения террористических и криминальных угроз // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 10–13.

силових структур та їх спроможність щодо використання сучасних систем у сфері безпеки повинно зумовити відповідні результати у «війні з тероризмом», а в підсумку сприяти досягненню потрібного рівня національної безпеки держав – членів світового співтовариства.

Прикладом такої інноваційної розробки є реалізація на практиці управління науковими дослідженнями Пентагону ДАРПА (Defense Advanced Research Projects Agency /DARPA/) суперпроекту «Знання інформації про тероризм» (Terrorism Information Awareness /TIA/), мета якого полягає у створенні та випробуванні на практиці системи, яка дозволяє на основі великих обсягів не пов'язаної між собою інформації в різних базах даних виявляти осіб, що готуються до спроби вчинення терористичного акту на території США. Складовою цього суперпроекту є низка проектів, які скеровані на розвиток сучасних інформаційних технологій, зокрема й систем автоматичного розпізнання людей на відстані[1].

В інтересах національної безпеки Пентагон використовує та продовжує розвивати низку біометричних проектів. 2008 року армійською комісією «Biometrics Task Force», яка займається координацією біометричних проектів Пентагону, було вивчено 175 пропозицій, а 10 з них були відібрані для реалізації з виділенням необхідних коштів. Серед відібраних опинилися такі проекти, як системи збору, об'єднання й аналізу біометричних даних, алгоритми створення електронних шаблонів і засоби розбудови архітектури біометричних систем[2].

Досягнення та підтримка необхідного рівня національної безпеки держави вимагає постійного вдосконалення заходів, які дозволяють забезпечувати належний рівень. Прикладом такої необхідності може слугувати терористичний напад у 2008 році, що відбувся в індійському місті Мумбай (Бомбей) і який є суттєвим відступом від традиційної попередньої тактики проведення атак терористів.

У Мумбаї добре озброєні та чудово підготовлені бойовики атакували 10 об'єктів у центрі міста з метою знищення насамперед іноземців: американців, англійців, ізраїльтян та інших. Десяток терористів виявилися здатними спричинити своїми діями хаос в одному з найбільших міст світу і, по суті, поставити його на коліна. Цей напад виявив неготовність і надзвичайну вразливість великих міст світу до застосування нової тактики проведення атак терористів.

Міжнародне співтовариство зважило на цю трагедію. Були розроблені спеціальні заходи для попередження та протистояння можливим атакам такого типу, адже історія тероризму вчить, що у випадку, якщо нова тактика демонструє результативність, то всі терористичні структури беруть її на озброєння. Реалізація потрібних превентивних заходів потребує значних сил і коштів, але у випадку ігнорування трагічних уроків світова спільнота може стати свідком нових атак такого виду та масштабу[3].

В умовах глобалізації процесів світового розвитку, міжнародних політичних і економічних відносин, які формують нові загрози і ризики для розвитку суспільства, країни та її громадян, будь-яка держава повинна здійснювати відповідну політику в галузі національної безпеки.

---

[1] В интересах национальной безопасности // Конфидент. – 2003. – № 6. [Электронный ресурс]. – Режим доступа: http://daily.sec.ru/...

[2] Военная биометрия подразумевает интегрированные решения // Secuteck.ru. – 2008. – 16 декабря. [Электронный ресурс]. – Режим доступа: http://secuteck.ru/newstext...

[3] Пять вопросов двум экспертам. Бойня в Мумбае – возможность повторений // Washprofile.org/ru. – 2008. – 13 декабря. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

Стратегія національної безпеки української держави – це офіційно визнана система стратегічних пріоритетів, мети та заходів у внутрішній і зовнішній політиці, що визначає стан національної безпеки та рівень стійкого розвитку держави на довгострокову перспективу. А засоби забезпечення національної безпеки – сучасні технології, а також технічні, програмні, лінгвістичні, правові та інші організаційні засоби, включаючи інформаційні технології та засоби зв'язку, зокрема й телекомунікаційний зв'язок, які використовуються в системі забезпечення національної безпеки для збору, формування, обробки, передачі або прийому інформації про стан будь-якої складової національної безпеки та здійснення заходів з її зміцнення.

За умов глобальної інтеграції та жорсткої міжнародної конкуренції головною ареною зіткнень і боротьби різновекторних національних інтересів стає інформаційний простір. Сучасні інформаційні технології дають змогу досягти реалізації власних інтересів без застосування воєнного інструментарію, послабити або навіть зруйнувати конкуруючу державу-конкурента, не застосовуючи водночас сили, за умови, якщо ця держава не усвідомить реальних та потенційних загроз негативних інформаційних впливів і не створить дієвої системи захисту та протидії цим загрозам.

Інформаційний простір, інформаційні ресурси, інформаційна інфраструктура та інформаційні технології значною мірою визначають рівень і темпи соціально-економічного, науково-технічного та культурного розвитку держави. За сучасних умов інформаційна складова набуває дедалі більшої ваги і стає одним із найважливіших елементів забезпечення національної безпеки України. Інформаційна безпека, з одного боку, є невід'ємною складовою забезпечення національної безпеки, а з іншого – є абсолютно самостійною сферою[1].

Нині між державами, які перебувають на різних рівнях економічного розвитку, загострюються суперечності, що пов'язані з нерівномірністю розвитку внаслідок сучасних глобалізаційних процесів і поглиблення розриву між рівнями добробуту різних країн. Зросла вразливість усіх членів міжнародної спільноти перед лицем нових викликів і загроз. Як наслідок, суттєво збільшилась загроза поширення зброї масового знищення і можливість її потрапляння до рук терористів, спостерігається вдосконалення форм протиправної діяльності в кібернетичній і біологічній галузях, у інших сферах високих технологій.

Дедалі більше поширюються націоналістичні настрої, ксенофобія, сепаратизм і насильницький екстремізм, зокрема під гаслами релігійного радикалізму.

Загострюється світова демографічна ситуація і проблеми навколишнього природнього середовища, зростають загрози, які виникають унаслідок зростання неконтрольованої та незаконної міграції, наркоторгівлі, торгівлі людьми й іншими формами транснаціональної організованої злочинності.

Останнім часом у світі спостерігається невпинне зростання потреби в забезпеченні безпеки і на національному, і на міждержавному рівнях. На цьому тлі ясніше усвідомлюється необхідність використання біометричних систем, які володіють такими незаперечними перевагами, як точність, зручність експлуатації та економія часу користувачів.

Системи біометричної ідентифікації виявляються незамінними під час виконання завдань боротьби з нелегальною імміграцією, підробками і розкраданнями небіометричних ідентифікаційних документів, активністю кримінальних елементів.

---

[1] Проект Доктрини інформаційної безпеки України // Rainbow.gov.ua. – 2009. – 25 травня. – Інтернет-адреса: http://www.rainbow.gov.ua/news/930.html

За повідомленням агентства «Frost & Sullivan», серед найбільш перспективних державних сфер застосування біометричних технологій у найближчі декілька років відзначають транспортну безпеку, прикордонний та імміграційний контроль[1].

Нині дедалі більше експертів вважають, що нанотехнології будуть визначати обриси XXI століття. Але водночас це поняття ще не є звичним для більшості з нас. Із середини 1990-х років воно вживається, як правило, для позначення різних видів маніпуляцій на молекулярному й атомному рівнях. Сьогодні зрозуміло, що розвиток цього технологічного напряму вимагатиме внесення радикальних змін у діяльність із забезпечення національної безпеки держав і спричинить радикальні зміни у військовому мистецтві та військовій справі.

Нанотехнологіями називають міждисциплінарну сферу прикладної та фундаментальної науки та техніки, яка має справу з сукупністю теоретичних обґрунтувань, а також практичних досліджень, синтезу й аналізу, методів виготовлення та використання продуктів, які створюються з наперед заданими молекулярно-атомними структурами шляхом контрольованого маніпулювання окремими молекулами й атомами. Нині у світі не існує єдиного стандарту, який би однозначно дав визначення, що таке нанопродукція та нанотехнологія.

Нанотехнології дозволять створювати нові напівпровідники й оптику, унікальні конструкційні матеріали, мініатюрні датчики виявлення компонентів біологічної зброї та хімічних речовин, а також комп'ютери, які за продуктивністю у кілька разів перевершать існуючі аналоги. Розроблені на базі нанотехнологій мікропроцесори дають можливість створювати унікальні пристрої систем радіоелектронної боротьби, захисту інформації, боротьби з тероризмом і багато чого іншого.

Для збройних сил, і не тільки, суттєве значення буде відігравати зниження ваги, енергоспоживання і вартості обладнання та прилади, які вироблені з використанням досягнень нанотехнологій[2].

[1] Перспективы расширения сфер применения биометрических технологий в государственном секторе стран Северной Америки // BIOMETRICS.RU. – 2009. – 25 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Юферев Сергей. Нанотехнологии на службе военных / С. Юферев // Военное обозрение. – 2013. – 24 января. [Электронный ресурс]. – Режим доступа: http://topwar.ru/...

Розділ 10

ТЕХНОЛОГІЇ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ – НЕВІД'ЄМНА ЧАСТИНА ЗАСОБІВ У БОРОТЬБІ З ТЕРОРИЗМОМ

Як відомо, початок третього тисячоліття характеризується низкою таких загальносвітових тенденцій:

– глобалізацією та негативною реакцією на деякі її наслідки;

– активізацією недержавних структур, потенціал яких може бути зіставимим із державним;

– існуванням поки що «однополярного» світу, яке характеризується істотною військовою перевагою США в сфері сучасних озброєнь і яке змушує їх супротивників уникати прямої військової конфронтації та використовувати так звану «партизанську» тактику ведення військових конфліктів;

– створенням світового інформаційного середовища, транснаціональні можливості якого впливають на ведення котртерористичної боротьби.

Нині фахівці з міжнародних відносин відзначають посилення загострень відносин між християнським та ісламським світами. Той факт, що приблизно кожен сьомий мусульманин говорить про прийнятність проведення терористичних атак стосовно безневинних людей для захисту ісламу та досягнення мети його подальшого поширення, достатньо переконливо показує, наскільки є серйозною загроза для багатьох країн світової спільноти, насамперед для США, держав Євросоюзу, Росії, деяких членів СНД та низки інших країн. Більшість експертів стверджують, що ісламський фундаменталізм – найпотужніша ідеологічна зброя, яка більше впливає на політичні процеси в світі, ніж усі ядерні арсенали Заходу та Сходу, разом взяті[1].

Але положення «Захід проти ісламу» є спрощенням відомої концепції «зіткнення цивілізацій» Семюеля Хантінгтона. Про С. Хантінгтона, який помер у грудні 2008 року, зазвичай згадують, коли західний світ стикається зі світом ісламу. Його відома книга «Зіткнення цивілізацій» була опублікована 1996 року. Американський футуролог вважає, що значних цивілізацій наприкінці XX століття налічувалось приблизно вісім, і всі вони стикаються одна з однією у сучасному світі. На думку С. Хантінгтона, основною визначальною ознакою цивілізації є релігія.

Саме релігійний чинник дозволяє таким країнам, як Китай, США, Індія успішно здійснювати глобальні проекти. Саме релігія додає гостроти війнам «за лініями розлому», тобто у тих місцях, де відбуваються цивілізаційні конфлікти. «Тоді як на глобальному або на макрорівні світової політики основне зіткнення цивілізацій відбувається між Заходом і рештою світу, на локальному, або на мікрорівні, воно відбувається між ісламом

[1] Иванов В. Мощнее, чем атомная бомба / В. Иванов // Независимое военное обозрение. – 2007. – 16 ноября. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/wars/...

та іншими релігіями», – писав Семюель Хантінгтон. І сучасним двигуном цього протистояння, на думку західних експертів, є ісламська цивілізація[1].

Отже, нині боротьба ідеологій змінилася боротьбою релігій і конфесій за перерозподіл світу, за поширення канонів однієї релігії на терени інших. Наприклад, один із лідерів єгипетських мусульман шейх Ахмед аль-Тайєб звернувся в ООН із закликом ввести всесвітню заборону на будь-які образи ісламу. По суті, йдеться про поширення закону про богохульство, який діє у низці мусульманських країн, на цілий світ. Згідно з цим законом, смертною карою караються навіть ненавмисні дії щодо випадкового спалення Корану з іншою макулатурою.

Під заборону підпадають не тільки карикатури та фільми, але й взагалі кожне згадування ісламу в негативному контексті. Водночас ісламісти вважають свої закони всесвітніми, тому видають фетви на вбивство карикатуристів, письменників і навіть цілих знімальних груп. Чужі закони вони не визнають. У них шаріат і джихад.

Ще раз зазначимо, що боротьба ідеологій змінилася боротьбою релігій. Відбувається перерозподіл світу не між державами, а конфесіональними угрупованнями. Сотні тисяч християн виганяють звідти, де вони жили тисячі років, зате чисельність мусульман в Європі збільшується. І вони вже починають вимагати запровадження принципів шаріату в законодавство. А як аргумент дедалі частіше наводять кулі та вибухівку. Джихад і екстремізм вдало маскуються під релігійне збурювання. І багато громадян різних країн готові обмежити власну свободу заради ефемерного спокою. Через кілька десятків років карту світу не можливо буде впізнати[2].

Нині немає жодних підстав вважати, що тероризм може зникнути. В епоху, коли широкомасштабні війни стали дуже небезпечними та надто дорогими, терористичні дії виявились домінуючою формою здійснення насильницьких акцій. Поки в світі є конфлікти, буде існувати і тероризм. Тероризм мутує, а тому вимагає постійного оновлення арсеналу засобів боротьби з ним. Нові загрози, які здебільшого знецінюють накопичений досвід і знання, свідчать про те, що в XXI сторіччі світова спільнота ввійшла в якісно нову епоху терористичних загроз. І всі контртерористичні структури повинні в своїй діяльності зважати на ці нові реалії та для протидії ним розробляти сучасні сценарії і постійно генерувати нові ідеї нейтралізації цих загроз.

Політичні діячі провідних економічних країн вважають, що тероризм і супутні йому явища кидають світовій демократичній спільноті найсерйозніший виклик, котрий потребує адекватної відповіді. Терористичні акції становлять найбільшу загрозу загальноприйнятим демократичним цінностям, основним правам і свободам людини, а також міжнародній безпеці.

За висновками американського експерта у боротьбі з тероризмом Девіда Кілкаллена, що були викладені ним у статті «Нові концептуальні парадигми для розуміння конфліктів 21-го століття», яка була розміщена у 2007 році на інтернет-сайті Державного департаменту США, необхідна розробка нових концептуальних парадигм боротьби з тероризмом із урахуванням нових світових реалій. На його думку, їх розробка є ще не завершеною, проте деякі ідеї отримали практичне втілення, наприклад, положення щодо розгляду більшості існуючих військових конфліктів як широкомасштабної проблеми протидії партизанським методам ведення боротьби, що вимагає насамперед

[1] Минин С. Хантингтон оказался прав / С. Минин // Независимое военное обозрение. – 2009. – 5 августа. [Электронный ресурс]. – Режим доступа: http://religion.ng.ru/politic/...

[2] Мясников Виктор. Это не антиамериканские протесты, это – джихад / В. Мясников // Независимое военное обозрение. – 2012. – 28 сентября. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/wars/...

застосування невоєнних антипартизанських засобів боротьби одночасно з вжиттям заходів для захисту мирного населення, якому загрожує небезпека.

Нинішній феномен міжнародного тероризму полягає в тому, що він переходить від традиційних форм активності до більш різноманітних і значно ширших транснаціональних недержавних військово-терористичних дій. Разом ці дії нагадують деяку форму міжнародного повстанського руху. Зважаючи на цей постулат, Д. Кілкаллен зробив висновок, що людська цивілізація ввійшла в нову епоху конфліктів, які вимагають принципово нових підходів до їх вирішення[1].

Отже, світ переживає період розвитку тероризму. Нині тероризм трансформувався в масовий: головним об'єктом терору стала не тільки владна еліта, але й суспільство; основними засобами залякування – вбивства не конкретних осіб, а невизначеного, якомога ширшого кола ні в чому невинних людей.

Тероризм став системою, яка постійно розвивається. Форми та методи здійснення терористичної діяльності постійно коригуються, відбувається обмін досвідом між терористичними угрупованнями та встановлення зв'язків, зокрема з використанням глобальної комунікаційної мережі Інтернет. Неможливо замовчувати той вплив, який здійснила глобальна мережа Інтернет на міжнародний рух джихаду з погляду організації, стратегії, тактики, способів боротьби, рекрутування та інших аспектів діяльності.

У статті Sh. Drennan і A. Biack, яка була опублікована в журналі «Jane's Intelligence Review», йдеться про становлення мережі Інтернет як центрального елемента сучасного міжнародного джихадського руху, що призвело до зниження значущості організацій та посилення індивідуалізації цього руху. Раніше мережа Інтернет використовувалася виключно групами, які мали власні стратегічні цілі. Нині ж використання Інтернету досягло такого рівня, що стало ключовим механізмом поширення джихаду, тобто створення окремих маленьких груп, які практично не мають жодних прямих контактів між собою, а спілкування відбувається виключно за допомогою Інтернету.

Інтернет значно підвищив можливості терористичного руху. Хоча зміна тероризму в бік «індивідуалізації» організаційної структури не була оформлена якоюсь постановою, рух як єдине ціле адаптував свою стратегію для того, щоб підключитися до цього могутнього інструмента спілкування. На думку авторів наведеної статті, джихадський рух продовжує еволюціонувати і, відповідно до його стратегії, Інтернет більшою мірою повинен стати головним інструментом «атомізації» глобального тероризму. Ідеологи джихаду A. M. al-Suri і M. Rh. al-Hakaymah розглядають Інтернет як ефективний інструмент, який може бути використаний для виконання таких завдань, як рекрутування нових членів, встановлення комунікаційного зв'язку в режимі «On-Line» та розповсюдження стратегічних вказівок і поточних наказів. Колишня необхідність у міцних організаційних зв'язках значною мірою послабилася внаслідок того, що географічно розсереджені індивідууми та їх лідери мають можливість створювати самостійні канали зв'язку за допомогою Інтернету.

Інтернет став могутнім інструментом рекрутування, пропаганди ідей тероризму і форумом радикалізації. У цьому процесі використання Інтернету надає багато можливостей глобальному тероризмові: ідеологи та вербувальники отримали засіб спілкування в режимі реального часу з прихильниками їх ідей. Цей спосіб спілкування забезпечує передачу перспективним рекрутам необхідних інструкцій і ресурсів. Інтернет фактично

[1] Килкаллен Дэвид. Новые концептуальные парадигмы для понимания конфликтов 21-го века / Дэвид Килкаллен. – 2007. [Электронный ресурс]. – Режим доступа: http://usinfo.state.gov/journals/itps/…

реорганізував організаційний процес рекрутування від особистого контакту до індивідуалізованого через онлайнове спілкування. Нині найбільш могутніми методами рекрутування та радикалізації є інтернет-форуми і веб-послання, які скеровують і координують дії потенційних джихадистів-добровольців на підтримку тією або іншою формою насильницького джихаду.

Інтернет не тільки робить вагомий внесок до радикалізації руху і рекрутування нових членів, але й мережа створила покоління джихадистів, які здійснюють віртуальний джихад. Вони збирають і поширюють потенційно корисну для оперативних планувальників інформацію з відкритих джерел, проводять такі «активні заходи», як хакерські атаки та блокування надання інтернет-послуг. Отже, деякі члени онлайнового проджихадистського співтовариства перетворили Інтернет-мережу на власний бойовий простір[1].

Виконавче керівництво глобальної терористичної організації «Аль-Каїда», використовуючи Інтернет, може безпечно виступати з різними заявами і здійснювати комунікаційний зв'язок у мережі без значних фінансових витрат і ризиків оперативної розробки, які виникають під час використання традиційних мас-медійних засобів. Фундаментальним елементом сучасної глобальної терористичної стратегії є децентралізація та індивідуалізація джихаду.

Методи боротьби з так званими «повстанськими» формами тероризму є основними у протидії новим формам транснаціонального тероризму. Ці методи охоплюють, по-перше, заходи щодо захисту та забезпечення безпеки населення, по-друге, заходи щодо політичного та фізичного усунення впливу ідеологів тероризму, завоювання симпатій із боку місцевих жителів, що, зрештою, повинно зумовити встановлення довіри між владними структурами та місцевим населенням.

Усі органи державної влади, насамперед дипломатичні, військові, економічні та розвідувальні відомства, мають діяти спільно, а їх діяльність повинна координуватися на урядовому рівні. Нині серйозною проблемою ще залишається відсутність необхідного рівня координування й обміну закритою інформацією між різними державними структурами, що повинні протистояти тероризму.

Згідно з розсекреченою 2008 року доповіддю «Причини провалів і успіхів терористичних атак» («Underlying Reasons for Success or Failure in Terrorist Attacks») Інституту національної безпеки США (Homeland Security Institute), який є складовою Міністерства національної безпеки (Department of Homeland Security), терористичні структури – це не чітко сформовані утворення. Вони постійно змінюються, адаптуються до дій антитерористичних служб і знаходять нові способи досягнення своєї мети. Переважно терористичні акти здійснюються нестандартними способами: для терористів це можливість не тільки випередити спецслужби, які протидіють ним, але й засіб привернення додаткової уваги громадськості.

На думку авторів доповіді, головною проблемою терористів нині є низький рівень забезпечення таємності під час проведення оперативних заходів. Наслідком таких непрофесійних дій є ситуація, коли головну загрозу терористам несуть не дії спецслужб, а свідомі громадяни, які стають свідками неадекватних дій членів терористичних структур. Проте здебільшого державні структури не виявляють достатньої гнучкості та належно не реагують на повідомлення громадян.

У доповіді особливо акцентується на такому моменті, що для правоохоронних і антитерористичних структур аналіз розвіданих і оперативний обмін інформацією

[1] Использование Интернета в террористических целях // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2009. – № 2. – М.: ВИНИТИ. – С. 3–8.

з іншими відповідними державними органами – дещо нова сфера діяльності. Тому в цій діяльності державних силових структур постійно виникають проблеми, які у результаті й надають відповідні шанси терористам.

Рекомендації доповіді ґрунтуються на аналізі подій восьми проведених у різний час масштабних терактів, зокрема атак на Нью-Йорк і Вашингтон (11 вересня 2001 року), газової атаки в токійському метро (1995 рік), вибухів у лондонському метро (2005 рік), угону авіалайнера «Air France» (1994 рік) і ін. За підсумками здійсненого аналізу особливо викремлено такий аспект, що перед усіма крупними терактами терористи обов'язково проходили спеціальну підготовку. І саме такі дії (наприклад, навчання в школах авіапілотів, активні відвідини стрілецьких тирів тощо) повинні привертати особливу увагу правоохоронних органів.

Підбиваючи стислий підсумок рекомендацій, які наведені у доповіді, можна однозначно стверджувати, що успіх дій проти будь-якої терористичної загрози потребує тісної кооперації та інформаційної взаємодії розвідувальних, поліцейських, військових та інших державних органів, причому не тільки на національному, але й на міжнародному рівні[1].

Адже відомо, що 11 терористів, які були організаторами терористичної атаки 2001 року в США, перебували під наглядом ФБР і розшукувалися американською федеральною владою, проте використання терористами підроблених документів і існуючий бюрократизм під час реєстрації іноземців дали можливість здійснити теракт[2].

Набутий в останні роки досвід свідчить, що ключовим чинником успішної протидії поширенню насильницького екстремізму є готовність урядів різних країн до тісної взаємодії, приділяючи водночас належну увагу організації співпраці з різними національними та міжнародними організаціями, власними громадянами, а також іммігрантами.

Коли уряди взаємодіють один з одним, формують довірливі відносини та добиваються активної та свідомої підтримки з боку більшості населення, забезпечують ефективне державне управління, що ґрунтується на беззастережному дотриманні вимог законів, рівень загрози тероризму значно знижується. Коли ж уряд не має належної підтримки від населення, не може налагодити добросусідських відносин із межуючими державами, а в країні існують територіально нестабільні або конфліктні зони – тероризм отримує підґрунтя для своєї діяльності та стає головним джерелом загроз для такого державного утворення.

Особливо необхідно відзначити такий висновок експертів із протидії тероризму, що військова складова державної влади не виконує в антитерористичній діяльності головної ролі, оскільки важливе значення тут мають можливості невійськового впливу[3].

За висновком Хенка Крамптона, одного з американських теоретиків із питань протидії тероризму, світова спільнота незабаром увійде в нову військову еру, яка вимагатиме проведення швидких і дуже гнучких дій. І позитивний результат залежатиме від можливості швидкої адаптації до нових реалій міжнародної обстановки та негайної розробки відповідних до неї заходів.

Причому необхідно передбачати і відповідно реагувати на можливі зміни в навколишньому середовищі, яке винятково швидко змінюється під впливом сучасних реалій і в якому створюються передумови для появи нових загроз.

---

[1] Теория заговора // Washprofile.org/ru. – 2008. – 13 декабря. [Электронный ресурс]. – Режим доступа: http://www.washprofile...

[2] Попов Ю. Биометрия для безопасности / Ю. Попов, С. Чекунков. – 2005. [Электронный ресурс]. – Режим доступа: http://www.vankb.ru/ru/magazine/...

[3] Стратегическая оценка прогресса в борьбе с террористической угрозой // Госдепартамент США. – 2007. [Электронный ресурс]. – Режим доступа: http://usinfo.state. gov/journals/…

На думку британського генерала Руперта Сміта, говорити тепер про війну в такому аспекті, що вона визначається як відкритий озброєний конфлікт між державами, за участю в них армій із використанням промислового потенціалу, коли результат безпосередньо досягається прямим зіткненням збройних сил, більше не має сенсу. Генерал вважає, що ми живемо в епоху «війн між людьми», коли ефективність використання збройних сил залежить від їх можливості гнучко адаптуватися до наявних політичних умов і готовності до ведення боротьби проти недержавних формувань, які тепер виступають як ворожі сторони.

Будь-які зміни ситуації внаслідок нових за формою екстремістських дій із боку терористичних організацій досить часто вимагають пошуку й ухвалення нових інноваційних рішень, оскільки сучасні терористичні дії, як правило, відзначаються нестандартністю у їх проведенні, що у підсумку досить швидко знівельовує наші знання, які ґрунтуються на минулому досвіді[1].

За висновком ще одного американського фахівця з тероризму Пола Піллара, за останні декілька десятиліть міжнародний тероризм істотно змінився. Він відзначає такі дві головні тенденції сучасного тероризму:

1. По-перше, нині знизилась підтримка терористичних дій на державному рівні. Офіційно дедалі менше держав активно підтримують тероризм. Сьогодні здебільшого терористичні акти плануються та здійснюються різними недержавними угрупованнями.

2. Друга й головна тенденція – підвищення ролі й значення різних релігійних терористичних організацій. Особливо це стосується радикального ісламізму, який кардинально відрізняється від «світських» і «лівих» терористичних угруповувань, що діяли у попередніх десятиліттях.

Нині терористичне підпілля ісламізму продовжує розширюватися, нові осередки виявляють у багатьох країнах. Особливо це стосується процесу вербування нових членів і географії здійснення терористичних актів. Крім того, цей процес стає більш децентралізованим.

В умовах глобального поширення терористичної загрози правоохоронні та антитерористичні сили для протидії цьому негативному явищу повинні спиратися на останні досягнення інноваційних технологій, зокрема інформаційних і біометричних. Збільшення витрат на антитерористичну діяльність найсприятливіше вплинуло на захистні аспекти цієї діяльності такі, як застосування спеціальних систем контролю та спостереження, введення нових паспортно-візових документів і, відповідно, нових біометричних систем і загальнодержавних та наддержавних захищених інфраструктур обміну даними.

У новому столітті міжнародне співтовариство стало свідком низки кроків щодо створення основних частин майбутньої глобальної паспортно-біометричної системи. Упродовж останнього десятиліття уряди багатьох країн активніше застосовують паспортні-візові документи нового покоління з відомостями про біометричні ідентифікатори їх власників для того, щоб гарантувати, що власник документа насправді є тим, за кого себе видає.

Але оборонні заходи не здатні кардинально вирішити проблему, оскільки захисні методи не спроможні гарантувати повної безпеки кожній потенційній цілі терористів. Тому дуже важливо здійснювати випереджувальні наступальні контртерористичні дії, які були спрямовані на виявлення та нейтралізацію терористичних угруповувань. Однак

[1] Килкаллен Дэвид. Новые концептуальные парадигмы для понимания конфликтов 21-го века / Дэвид Килкаллен. – 2007. [Электронный ресурс]. – Режим доступа: http://usinfo.state.gov/journals/itps/…

успіх цих операцій визначається не стільки розмірами бюджетів, скільки об'єктивними труднощами, пов'язаними з виявленням терористичного підпілля та нейтралізацією атак, які ним плануються.

Найефективніший спосіб зниження ризику – проведення такої зовнішньої та внутрішньої політики, яка б змогла зменшити кількість людей, які сповідують «релігію тероризму». Це вимагає проведення такої політики, яка б сприяла поліпшенню відносин християнського світу з мусульманським. Основний шлях до виходу з теперешньої ситуації – у зближенні рівнів розвитку країн заходу і сходу[1].

Через постійне розширення географії міжнародного тероризму занепокоєння більшості країн щодо захисту демократичних цінностей світового співтовариства невпинно зростатиме. Експерти з боротьби з «новою чумою» XXI століття констатують, що темпи поширення терористичних дій нині перевищують темпи розвитку технологій захисту. Необхідна розробка та вжиття таких превентивних заходів, які б не передбачали можливість учинення терористичних актів.

Одним із головних напрямів боротьби з терором експерти вважають подальше вдосконалення систем спостереження та нагляду за переміщеннями територією держави або співтовариства держав іноземців або своїх громадян, які підозрюються в екстремістських діях.

Запровадження таких систем є тим механізмом, який дозволяє спецслужбам своєчасно виявляти потенційних терористів серед іноземних громадян, які прибувають, і перешкоджати їх в'їзду до країни за наявності певних обставин і здійснювати контроль за перебуванням підозрілих осіб на території країни. В зв'язку з цим особлива увага приділяється застосуванню сучасних біометричних технологій, які нині цілком закономірно стали основним ядром заходів щодо контролю за в'їздом-виїздом як своїх, так й іноземних громадян на кордонах багатьох держав або співтовариств держав.

Тенденція протидії тероризму така, що біометрична паспортизація, яка стає всеохоплюючим явищем, може практично виявитись однією з найважливіших захисних систем і для держав, і для окремих громадян від злочинності та тероризму. Ймовірно у майбутньому будуть країни, які не приєднаються до системи єдиної біометричної паспортизації або не спроможні брати участь у цьому проекті з огляду на потребу реалізації необхідних техніко-економічних вимог, що може призвести тільки до більшої їх ізоляції від решти держав світу.

Постійне збільшення кількості біометричних параметрів, що вимірюються й аналізуються, цілком закономірно розширюють коло питань, які вирішуються за допомогою біометрії. Вважається, що в 2010–2020 роках практично все населення всіх розвинутих держав планети буде охоплено біометричними паспортно-візовими документами нового покоління, отримана інформація з яких буде зберігатися в уніфікованих за організацією доступу різних державних базах даних, об'єднаних за допомогою спеціально захищених каналів зв'язку в єдину міжнародну глобальну ідентифікаційну систему.

Вирішальну роль у розвитку біометричних технологій для боротьби з тероризмом і низкою інших негативних явищ (незаконна міграція, транснаціональна злочинність, наркоторгівля тощо) відіграють урядові структури. Для підтвердження цієї тези наведемо перелік низки програм, реалізованих урядовими структурами США в сфері біометрії наприкінці першого десятиріччя третього тисячоліття.

---

[1] Пиллар Пол. Настоящее и будущее глобального террора / Пол Пиллар // Washprofile.org/ru. – 2007. – 20 сентября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/...

Насамперед слід відзначити діяльність систем IDENT й IAFIS, які експлуатуються Міністерством національної безпеки й Міністерством юстиції, відповідно. У першій із систем збираються й аналізуються дані про відбитки всіх 10 пальців рук індивідуумів, запідозрених або викритих у порушенні імміграційного законодавства та прикордонного режиму. Система IDENT пов'язана із системою IAFIS (зараз NGI), яка використовується ФБР і містить відомості про десятки мільйонів відбитків пальців. Взаємодія двох біометричних систем підвищує ефективність кожної з них: наприклад, з'являється можливість з'ясувати, чи не притягувався нелегальний іммігрант до кримінальної відповідальності ще й за злочини, вчинені на території США.

Прикордонне та митне агентство США сформувало й використовує систему USPASS. За її допомогою пришвидшується проходження прикордонного контролю громадянами, які зареєстровані в цій системі: їх особистість надійно та швидко засвідчується за допомогою біометричних технологій.

Національний інститут юстиції Сполучених Штатів Америки вивчає можливості ідентифікації за обличчям для виявлення підозрілих суб'єктів, підвищення безпеки місць масового скупчення людей та захисту співробітників правоохоронних органів.

Управління транспортної безпеки та Берегова охорона продовжують реалізовувати програму TWIC з видачі біометричних ідентифікаційних карт службовцям портів. Ці урядові агентства сподіваються забезпечити ефективний контроль фізичного доступу в режимні зони портів, морських суден та інших об'єктів берегової інфраструктури за допомогою біометричних технологій, активне використання яких передбачено в програмі TWIC.

У Державному департаменті США почала функціонувати система біометричної ідентифікації, яка забезпечує розмежування доступу до інформаційних ресурсів цієї установи. Службовцям зовнішньополітичного відомства США видані смарт-карти, у чіпах яких зберігаються відомості про відбитки пальців службовців. Якщо працівник прагне одержати доступ до службового комп'ютера, йому потрібно відсканувати відбитки своїх пальців. Отриманий у результаті сканування шаблон відбитка порівнюється з таким ж шаблоном, який був внесений у чіп смарт-карти під час реєстрації біометричних ідентифікаторів, і, якщо моделі-шаблони збіглися, надається можливість доступу до комп'ютера[1].

Низка експертів із біометричних технологій цілком обґрунтовано прогнозують, що до 2020 року, а можливо і раніше, реальністю стане не тільки ідентифікація особи, але і можливість зчитування думок і намірів будь-якого індивідуума. Незабаром під час перетинання кордонів держав або під час доступу на особливо захищені об'єкти суб'єкт контролю буде проходити автоматичне психофізіологічне тестування в режимі реального часу впродовж 10 секунд. Тестування буде здійснюватися з метою встановлення потенційної загрози від підконтрольної особи для держави чи об'єкта, що перебуває під охороною. Завдяки такому тестуванню стане можливістю проведення захисту не тільки від вже відомих злочинців і терористів, але й від осіб, які раніше не потрапляли у поле зору правоохоронних структур, але мають злочинні наміри[2].

Отже, завдання чи блок завдань полягає в тому, щоб завершити проведення загальної біометричної паспортизації населення Землі, створити уніфіковану світову систему

[1] Правительственные органы США расширяют использование биометрических технологий // BIOMETRICS.RU. – 2010. – 21 мая. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Минкин В. Биометрия. От идентификации личности к идентификации мыслей / В. Минкин. [Электронный ресурс]. – Режим доступа: http://www.elsys.ru/review5.php

взаємозв'язаних баз даних біометричних параметрів усього людства, завершити розробку технологій, що були б здатні розпізнавати всі нюанси психофізіологічного стану людського організму, які передують насильницьким діям стосовно інших індивідуумів. Це дозволить розгорнути глобальну систему моніторингу, яка буде здатна відслідковувати у громадських місцях психічний та фізіологічний стан будь-якої особи та виявляти тих індивідуумів, які мають наміри вчинення будь-якого правопорушення[1].

У ролі основного рушію застосування біометричних технологій для боротьби з тероризмом виступають Сполучені Штати Америки, які не тільки самі запроваджують ці технології, але й примушують впроваджувати інноваційні досягнення у галузі систем контролю та спостереження інші держави. Країни, які хочуть мати безвізовий режим із США (на січень 2014 року їх чисельність становила 37 держав), зобов'язані забезпечити своїх громадян паспортами, які повинні містити біометричну інформацію у вигляді, придатному для машинного зчитування, але це звільняє візітерів від проведення у місцях контролю процедур біометричної ідентифікації за обличчям і відбитками пальців[2].

Найважливішим елементом контролю людей, які прибувають до Сполучених Штатів Америки, є забезпечення достовірності в'їзних документів їх власникам, оскільки лише за їх допомогою можливо ефективно здійснювати персональний контроль іноземців, які прибувають, а також визначати мету та наміри їх відвідин Америки. США продовжують провадити політику посилення режиму контролю за доступом на свою територію і громадян із дружніх, і «ненадійних» країн. Багаторівнева система спостереження за всіма іноземцями, які прибувають у Сполучені Штати Америки, повинна контролювати їх переміщення на аеровокзалах, залізничних станціях, у морських портах і на вантажних терміналах, на автомобільних дорогах та інших місцях. Відповідно до державної стратегії, діюча система спостереження та контролю повинна постійно удосконалюватися. Американські спеціальні відомства повинні не допустити інфільтрацію бойовиків на територію Америки та їх проникнення у різні елементи її інфраструктури[3].

У зв'язку з цим завданням повинно невпинно розширюватися застосування різних систем контролю й управління доступом. Наприклад, наявність біометричного захисту доступу до керування літаком могла б перешкодити здійсненню планів терористів 11 вересня 2001 року: використання будь-якого дактилоскопічного сканера, який блокував би передачу управління літака іншим особам, крім пілотів, могли б істотно зменшити наслідки тієї терористичної атаки[4].

Після терористичних атак 2001 року США запровадили істотні зміни до законодавства, що регулює порядок допуску іноземців на американську територію. Першою ластівкою стало прийняття, який 2001 року був прийнятий славнозвісний Закон «Патріот» («Patriot Act»).

2002 року президент США підписав закон, який запровадив нові правила відвідин Сполучених Штатів Америки. Він вимагав запровадження нових видів в'їзних документів для іноземних громадян, в яких обов'язково були б присутні в електронному вигляді персональні біометричні дані. З 2004 року в США почала діяти програма «US-VISIT»,

---

[1] Шишминцев М. Электронные помощники стражей правопорядка / М. Шишминцев. – 2006. – 26 мая. [Электронный ресурс]. – Режим доступа: http://www.glavred.info/archive/…

[2] Мюррэй С. Биометрия против терроризма / Сара Мюррэй // Деловая неделя. – 2004. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document. asp...

[3] Иванов В. Антитеррористический «Смерш» США / В. Иванов. – 2007. – 3 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Попов Ю. Биометрия для безопасности / Ю. Попов, С. Чекунков. – 2005. [Электронный ресурс]. – Режим доступа: http://www.vankb.ru/ru/magazine/...

яка передбачала, зокрема, зняття відбитків пальців у всіх іноземців, які прибували до країни (відбитки пальців і фотографія іноземця в електронному вигляді вносились у комп'ютерну базу даних і проходили процедуру перевірки за банками даних щодо виявлення терористів і злочинців). Із жовтня 2004 року всі візи, які видавалися іноземцям американськими консульствами, почали містити біометричну інформацію.

У Сполучених Штатах Америки також був ухвалений закон, який передбачає поетапне введення єдиного для всіх американців типу посвідчення особистості (як відомо, головним особистим документом громадянина США є водійські права, які видаються кожним штатом). Відповідно до цього закону, владні структури всіх штатів повинні видавати водійські права з уніфікованим дизайном і обов'язковим переліком відомостей, що повинні відповідати новим федеральним критеріям безпеки[1].

В американських аеропортах після подій 2001 року значно посилились заходи з безпеки. У салон літака заборонено проносити предмети, які можуть бути використані як холодну зброю, а в останні роки – і рідину. Зараз усі іноземці, які мають намір в'їхати в США, та всі пасажири американських авіакомпаній, навіть і на внутрішніх рейсах, під час придбання квитка в обов'язковому порядку проходять перевірку за банками даних центру виявлення терористів (Terrorist Screening Center), який діє у складі ФБР (FBI). Результати перевірки надходять ініціаторам запитів: прикордонним й імміграційним службам, поліції, митниці та іншим відомствам, котрі на їх основі здійснюють фільтрацію осіб, які перевіряються, з метою виявлення небезпечних візитерів.

Підвищення рівня безпеки стосувалося не тільки аеропортів, але й інших важливих об'єктів інфраструктури Сполучених Штатів Америки. Найбільш показовим є приклад із Капітолієм, де проводяться засідання Конгресу США. До вересня 2001 року без жодних проблем до нього міг потрапити будь-який бажаючий, але після терористичних подій вулиці, які ведуть до Капітолія, були перегороджені, щоб у разі потреби мати змогу не пропустити підозрілі легковики, а вантажні автомобілі в цю зону взагалі не потрапляють. Екскурсії до Капітолію проводяться й надалі, але всі відвідувачі повинні пройти через металодетектор і пред'явити в установленому порядку особисте посвідчення.

Але розробка та застосування біометричних технологій – це тільки частина роботи. Інша не менш значна її частина – організаторська. Наприклад традиційне слабке місце імміграційної безпеки – організацію контролю за тим, щоб іноземці вчасно залишали країну. За інформацією президента компанії «Identix» (одного з найбільших розробників і постачальників сучасних біометричних систем) Джозефа Атіка: «...старі підходи не спрацьовують. Тепер йдеться про створення віртуального кордону, який за ефективністю повинен бути у жодному разі не менш продуктивним, ніж фізичний кордон. Це буде можливо лише у тому випадку, коли будуть запроваджені інноваційні системи, що мають ефективність в ніякому разі не меншу, за ту, що досягається за допомогою звичайних заходів на кордоні»[2].

Тобто, за допомогою біометричних систем повинен контролюватися і в'їзд, і виїзд іноземців та власних громадян із території як окремої країни, так і співтовариств держав. Тому у всіх осіб, які виїзджають з Америки, заплановано знімати відбитки пальців. Цей захід спрямований не тільки на ефективну боротьбу з іноземцями, які прагнуть назавжди залишитися в США, але запроваджується з метою виявлення туристів, які

[1] Террористическая атака, произошедшая 11 сентября 2001 года, фундаментально изменила отношение США к проблеме безопасности // Washprofile.org/ru. – 2007. – 13 сентября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/...

[2] Мюррэй С. Биометрия против терроризма / Сара Мюррэй // Деловая неделя. – 2004. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

порушують установлені законодавчо терміни перебування в Сполучених Штатах Америки. Центр вивчення імміграційних процесів США повідомляє, що в середньому 4–5 мільйона іноземців постійно перебувають у країні з протермінованими візами, а ця цифра становить до 40% загальної кількості нелегальних мігрантів[1].

На практиці швидкій реалізації запланованого заходу заважають суто технікоекономічні проблеми. Це пов'язано з тим, що процедура зняття відбитків пальців потребує певного часу, а пасажирські потоки в 30 найзавантаженіших аеропортах Америки дуже значні. Тому перші десять аеропортів США обладнають системами сканування відбитків пальців упродовж найближчих двох років після того, як новий імміграційний закон буде остаточно ухвалений. А інші двадцять повітряних портів введуть цей захід протягом шести років[2].

У лютому 2013 року Німеччина запропонувала країнам Європейського Союзу (ЄС) запозичити американський досвід використання біометричних технологій у контролі міграційних потоків. На думку глави німецького МВС Ханса-Петера Фрідріха, застосування цього досвіду дозволить поставити надійну перешкоду на шляху незаконних мігрантів, які прагнуть потрапити до європейських країн.

Х.-П. Фрідріх запропонував створити онлайновий реєстр персональних даних іноземців, які претендують на в'їзд до держав ЄС, причому включати до цього реєстру відомості про їхні біометричні ідентифікатори. На думку глави МВС ФРН, такий реєстр допоможе боротьбі зі спробами незаконного в'їзду на територію Євросоюзу терористів і кримінальних елементів[3].

Сучасний світ створює безліч нових можливостей. Проте цими можливостями користуються не тільки законослухняні громадяни, але й численні зловмисники. Тому на сучасному етапі для боротьби з тероризмом, нелегальною міграцією, іншими формами міжнародної злочинності особливе значення набуває можливість однозначної та достовірної ідентифікації фізичних осіб для виявлення суб'єктів, які раніше мали конфлікт із законом або за наявними відомостями мають відношення до відповідних «небезпечних» організацій. Для реалізації можливості достовірної ідентифікації будь-якого індивідуума необхідно виконати завдання не тільки проведення біометричного контролю, але й низку супутніх обов'язкових завдань, наприклад: створення та підтримування в належному стані біометричних баз даних із необхідними відомостями на всіх громадян Землі (в ідеальному випадку), безпечного їх зберігання й організації захищеного доступу до них. Оскільки це завдання поки що далеке від свого рішення у глобальному масштабі, передові держави та їх об'єднання вживають заходи щодо біометричної документалізації своїх громадян, осіб без громадянства, котрі перебувають на території цих країн, а також усіх іноземних громадян, які перетинають кордони цих держав, шляхом запровадження відповідних паспортно-візових документів нового покоління.

Наведемо перелік низки таких програм, що нині реалізуються:

– Програма машинозчитуваних транспортних документів (електронних або біометричних закордонних паспортів), видачу яких під час виїзду своїх громадян за кордон

---

[1] Биометрические технологии эффективны в миграционном контроле // Security News. – 2013. – 30 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Иностранцы будут проходить биометрическую идентификацию и при выезде из США // Turist.ru. – 2013. – 23 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Германия предложила позаимствовать у США опыт использования биометрических технологий // BIOMETRICS.RU. – 2013. – 6 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

повинні запровадити практично всі країни світу. Міжнародні організації, що опікуються цією програмою: Організація Об'єднаних Націй (ООН), Міжнародна організація цивільної авіації (ІКАО /ICAO/), Міжнародна організація з стандартизації (ІСО /ISO/). Планується, що з 2015 року в'їзд на територію США, ЄС та низки інших держав буде здійснюватися тільки за наявності біометричних закордонних паспортів другого покоління.

– Реалізація програми США «US VISIT», що вимагає безумовної біометричної ідентифікації всіх здобувачів американських віз.

– Виконання директиви Президента Сполучених Штатів Америки з національної безпеки HSPD, яка зобов'язує всіх державних службовців і працівників підприємств, що виконують державні контракти, оформляти індивідуальні біометричні ідентифікаційні картки-посвідчення.

– Візова інформаційна система країн Шенгенської угоди (Visa Information System /VIS/, у якій акумулюються відомості про відбитки пальців здобувачів шенгенських віз). Із 2010 року Європейським Союзом (ЄС) запроваджена процедура зняття відбитків пальців гостей у всіх країнах співтовариства (станом на 01.02.2014 року 28 держав-членів блоку).

– Загальноєвропейська система біометричної ідентифікації за відбитками пальців EURODAC (європейська база даних про відбитки пальців здобувачів статусу біженця та іноземців, які нерегулярно перетинають границі держав Євросоюзу).

– Видача внутрішніх біометричних ідентифікаційних документів (ID-cards) громадянам низки європейських держав. Наразі в Європі такі програми реалізують Великобританія, Португалія й Іспанія.

– Введення в Японії з кінця 2007 року процедури безумовної біометричної ідентифікації всіх претендентів на отримання віз.

Нагадаємо основний перелік негативних проблем, вирішенню яких повинна сприяти масова (у перспективі загальна) біометрична ідентифікація:

– боротьба з тероризмом і злочинністю в будь-яких формах (організованою, транскордонною, пов'язаною з викраданнями людей, новими формами работоргівлі (дорослими та дітьми) тощо;

– протидія нелегальній міграції (зокрема й трудовій);

– боротьба з шахрайством у сфері електронної і мобільної комерції – сприяння припиненню «крадіжок особи» (викрадення або привласнення обманним шляхом повноважень законного користувача для розпорядження грошовими коштами), зокрема зловживань із кредитними картками, створення фінансових пірамід за допомогою викрадених документів[1].

Для поліпшення можливостей системи нагляду за переміщенням країною представників інших держав Сполучені Штати Америки продовжують проведення робіт із метою удосконалювання багаторівневої системи спостереження за всіма іноземцями. Згідно з Стратегією, забезпечення внутрішньої безпеки США повинні створити надійну перешкоду на шляху проникнення бойовиків на її територію та їх вкоріненню у різні елементи інфраструктури[2].

У Сполученому Королівстві чисельність співробітників британської контррозвідки МІ-5 досягла розмірів, небачених із часів Другої світової війни. Це відбулося через

[1] Массовая идентификация // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/civil_id.php

[2] Иванов В. Антитеррористический «Смерш» США / В. Иванов // Независимое военное обозрение. – 2007. – 3 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

розширення служб зовнішнього спостереження й аналітичних підрозділів. Нині основною метою діяльності МІ-5 стала протидія терористам «Аль-Каїди». За твердженням британських контррозвідників, межі країни щодня перетинають тисячі молодих людей, які мають міцні зв'язки з формуваннями нині покійного Усами бен Ладена. За заявою генерального директора МІ-5 Джонатана Еванса, яку він зробив 6 січня 2009 року, нині «Аль-Каїда» та низка інших терористичних угруповань є головними ворогами Великобританії і становлять вельми серйозну загрозу для життя її громадян. Тому всі контртерористичні зусилля його відомства будуть скеровані на виявлення осередків терористів-бойовиків і їх моментальну ліквідацію всіма можливими засобами. За відомостями, що оприлюднив генеральний директор МІ-5, в Англії проживають близько 800 тис. вихідців із Пакистану, а безпосередню загрозу для безпеки країни становлять майже 4 тис. громадян мусульманського походження, які тією чи іншою мірою мають можливості для проведення прихованої підготовки для здійснення терористичних акцій на різних об'єктах Сполученого Королівства[1].

Нині розвиток технології відеоспостереження, яка спочатку призначалася лише для фіксування, контролю й обліку звичайних правопорушень у громадських місцях, еволюціонує у бік створення технічних систем контролю для захисту від різних екстремістських виявів, зокрема і терористичних. Синтез технологій контролю за доступом з іншими системами безпеки, особливо з такими, які дозволяють проводити дистанційне розпізнавання відеозображень людей, а також запровадження у низці країн масового відеоспостереження, дозволяє істотно підвищити рівень безпеки в суспільно-громадських місцях та створити в містах насамперед у мегаполісах єдину загальноміську систему відеоспостереження[2].

За повідомленнями британських ЗМІ, для боротьби з тероризмом і низкою інших негативних явищ Федеральне бюро розслідувань (ФБР /FBI/) США розпочало роботи зі створення всесвітньої бази біометричних даних (кодова назва «Server in the Sky»), в яку повинні бути внесені відомості про сотні мільйонів і навіть мільярдів людей. До участі у створенні «Сервера у небі» також залучені спецслужби Великобританії, Канади, Австралії та Нової Зеландії. Інформація про те, що FBI працює над створенням такої бази, стала відома ще в 2007 році, але жодних подробиць тоді не розголошувалось. Представники вказаних країн увійшли до робочої групи, яка отримала назву Міжнародний інформаційний консорціум (International Information Consortium), а американське федеральне бюро розслідувань взяло на себе загальне керівництво проектом.

Офіційний представник ФБР в інтерв'ю британській газеті «The Telegraph» повідомив, що «Server in the Sky», за задумом його творців, повинен забезпечувати обмін біометричними даними між країнами – учасницями проекту, дозволяючи оперативно отримувати відомості про злочинців, інформація щодо яких буде внесена у створювану базу даних. Водночас високопоставлений співробітник американської спецслужби підкреслив, що проект перебуває на стадії розробки (відомості 2008 року – *авт.*)[3].

---

[1] Иванов В. ЦРУ разворачивает операции в Англии / В. Иванов // Независимое военное обозрение. – 2009. – 23 января. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/spforces/2009-01-23/14_cru.html

[2] Рынок программного обеспечения для видеонаблюдения: на пути к успеху // Secnews.ru. – 2006. – 18 июля. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/4408.htm?phrase_id=118009

[3] ФБР привлекает другие страны к формированию гигантской базы биометрических данных // Lenta.Ru. – 2008. – 16 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp?group_id=12&nItemID=2918&sSID=3.8

Влада Сполучених Штатів Америки виділяє величезні суми грошей на потреби Міністерства національної безпеки (МНБ). МНБ США об'єднує понад 20 федеральних установ, а в його роботі задіяно близько 180 тис. службовців.

На програму «US-Visit», в рамках якої відповідні органи США створили і підтримують в актуальному стані банк даних із відбитками пальців і відеозображеннями іноземців, які перетинають кордони Америки, в 2008 фінансовому році було асигновано майже 500 млн доларів, а в 2009 році сума виділених коштів була збільшена на 4,2 млн доларів. На підвищення рівня безпеки на авіатранспорті у 2008 році було спрямовано майже 6 млрд доларів, з яких 128 млн виділялось на модернізацію в аеропортах обладнання для виявлення вибухових речовин[1].

А загалом на розвиток біометричних проектів американська адміністрація Президента Обами в 2009 році може виділити від 750 мільйонів до мільярда доларів[2].

Сполучені Штати Америки продовжують удосконалювати та створювати технології, які дозволили б «вираховувати» потенційних терористів, які мають на меті здійснення терактів. Учені з університету Баффало (University at Buffalo) створили апаратуру, яка за допомогою комп'ютерно-біометричної системи аналізує різкість рухів людини, вираз її обличчя, тембр голосу та низку інших фізіологічних параметрів. На підставі цієї інформації спеціальний програмно-комп'ютерний комплекс визначає, чи перебуває людина, яка перевіряється, у стані, коли вона налаштована на здійснення терористичної атаки або заздалегідь спланованого акту агресії.

Автори розробки зважали на те, що кожна людина індивідуально і по-різному реагує на власні думки та навколишню дійсність. Тому комп'ютерна система отримала таку додаткову функцію: вона може змінити свій вердикт після 20-ти хвилинної співбесіди з підозрюваною особою (людині задаються особливим чином скомпоновані питання, а система «стежить» за тим, як вона на них реагує). Розробники підкреслюють, що система не може гарантувати 100%-го результату. Проте вона може серйозно допомогти прикордонникам або представникам інших служб під час проведення рутинних перевірок: співробітники служб безпеки вибірково перевіряють людей, які «проходять» через аеропорти, залізничні вокзали, місця переходів державного кордону, пропускні пункти стадіонів й інших спортивних споруд тощо.

Як правило, під час вибору суб'єкта для ретельнішого обстеження (проведення огляду, співбесіди та ін.) співробітники спеціальних служб значною мірою поки що керуються інтуїцією. Система контролю за психофізіологічним станом особистості повинна замінити інтуїцію наукою[3].

Прикладом того, що спецслужби та державні структури Сполучених Штатів Америки найбільш зацікавлені у розвитку та впровадженні досягнень біометрії, є списки учасників будь-яких наукових конференцій із питань біометрії, що проводяться у США. Наприклад, серед учасників конференції у Вашингтоні, яка відбулася ще у 2008 року та на якій обговорювали хід і перспективи запровадження біометричних технологій у державному секторі, були присутні представники Пентагону, Держдепартаменту США,

[1] Администрация Буша предлагает увеличить финансирование программы биометрической идентификации иностранцев // ПРАЙМ-ТАСС. – 2008. – 6 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Администрация Обамы может направить на развитие биометрии до миллиарда долларов // BIOMETRICS.RU. – 2009. – 4 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Поймать террориста // Washprofile.org/ru. – 2007. – 8 октября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/...

ФБР, Управління транспортної безпеки, Міністерства національної безпеки, низки інших державних установ і організацій.

На конференції обговорювалися такі питання:

– інтеграція різних біометричних технологій (насамперед створення мультибіометричних технологій ідентифікації за відбитками пальців, обличчям та райдужною оболонкою очей);

– комплексне застосування біометрики та технологій смарт-карток;

– використання біометричних технологій у загальній системі управління ідентифікацією та доступом до інформаційних ресурсів;

– об'єднання можливостей біометрії й інфраструктури відкритих ключів (Public Key Infrastructure – PKI)[1].

Не змешують темпів упровадження біометричних технологій і країни Європейського співтовариства. Збір персональних даних про авіапасажирів, боротьба з пропагандою тероризму в Інтернеті, швидкий обмін інформацією щодо фактів крадіжок вибухівки – ось три основні вимоги для підвищення рівня безпеки в Європі[2].

Свого часу тодішній депутат італійського парламенту Джуліо Калвізі заявив, що у Європейському Союзі існує директива, відповідно до якої всі громадяни країн ЄС повинні пройти процедуру знімання відбитків пальців, які будуть розміщені у мікрочіпах відповідних документів[3].

Але відсутність узгодженої загальносвітової доктрини, яка була б прийнята до виконання всіма членами світової спільноти та забезпечувала єдині підходи і на міждержавному, і внутрішньодержавному рівнях, обмежує ефективність антитерористичних заходів. Необхідне покращення міждержавного та міжвідомчого співробітництва, яке є одним із найважливіших завдань в епоху конфліктних подій XXI століття. Що стосується світової співпраці у галузі біометричних та інформаційних технологій, то за існуючої значної кількості видів біометричних систем і практичних рішень реалізації досягнень інформаційних технологій найважливішим завданням стало досягнення операційної сумісності між різними системами та базами даних, що дуже необхідно для можливості забезпечення їх широкомасштабного використання.

Крім того, необхідно досягти остаточного концептуального узгодження між країнами світу з приводу того, який саме набір обов'язкової біометричної інформації повинен міститися у розміщеному в електронно-біометричному документі або у в'їзній візі. На сучасному етапі боротьби з тероризмом найбільше використовуються такі види біометричного розпізнавання: за обличчям, відбитками пальців і райдужною оболонкою очей або будь-яка їх комбінація. Також необхідно максимально пришвидшити проведення робіт зі стандартизації, уніфікації та сумісності всіх існуючих технологічних рішень. Одним із головних напрямів боротьби з терором США, Великобританія, Федеральна Республіка Німеччина та низка інших провідних світових держав вважають посилення режиму контролю за доступом на свою територію іноземних громадян.

Сполучені Штати Америки разом зі своїми партнерами продовжують розробляти нові технології, що дозволяють «вичислити» потенційних терористів, які мають наміри

[1] На конференции в Вашингтоне обсудят ход и перспективы внедрения биометрических технологий в госсекторе // BIOMETRICS.RU. – 2008. – 7 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Три основные меры по повышению безопасности в Европе // Эксперт-центр». – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://www.expert.org.ua/...

[3] Все итальянцы сдадут отпечатки пальцев // Страна.Ru. – 2008. – 17 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

вчинити терористичні дії. Останнім часом почали надходити відомості про те, що співробітники департаменту національної безпеки (ДНБ) США форсують реалізацію програми, яка повинна визначати ворожі наміри людини за виразом обличчя та низкою інших ознак її поведінки. Суть технології полягає в тому: комп'ютерна система здійснює запис поводження людини під час проведення контрольних дій, фіксує особливості міміки та виразу людського обличчя, тембру голосу і низки інших параметрів. На підставі зібраної інформації вона визначає, в якому психофізіологічному стані перебуває конкретна особистість і чи можливе в цьому стані вчинення акту агресії або терористичної дії.

Планується, що після успішного завершення розробки цієї програми всі чотириста мільйонів чоловік, які щорічно прибувають до Америки, будуть проходити таку перевірку під час в'їзду. За інформацією очільників департаменту національної безпеки, перевірка буде здійснюватися непомітно для тих, хто проходить процедуру митного або прикордонного контролю. За особами, які проходять процедуру обов'язкового контролю під час в'їзду, стежитимуть за допомогою прихованих спеціальних датчиків лазерного й інфрачервоного сканування, аудіо- та відеоспостереження, контролю за рухом очей, а також інших пристроїв, які зможуть оперативно зібрати інформацію щодо виразу обличчя, особливостей ходи, кров'яного тиску, пульсу та режиму потовиділення. А спеціально розроблена комп'ютерна програма миттєво обробить зібрані параметри з поправкою на культурні та расові відмінності. Якщо програма визначить когось із осіб, які проходили перевірку, потенційно небезпечним, співробітники контрольної служби проведуть із ним спеціальну співбесіду, а за її підсумком ухвалять остаточне рішення щодо необхідності затримання того, хто перевіряється. За наявною інформацією взірці такого обладнання мали проходити практичне тестування у 2010 році. В разі позитивного результату планувалось, починаючи з 2012 року, оснащення такою апаратурою всіх пунктів в'їзду до США[1].

Як додаток до вказаної програми Управління транспортної безпеки США готується до впровадження протестованої його фахівцями «системи виявлення авіапасажирів з ворожими намірами», яка розроблена ізраїльською компанією «Suspect Detection Systems». Основою цієї системи, що отримала офіційну назву «Cogito», є комбінація спеціального програмного забезпечення, пристроїв розпізнавання біометричних параметрів фізичних осіб і так званого «детектора брехні». Алгоритм дії «Cogito» такий: кожному клієнтові, котрий привернув увагу, пропонується пройти до спеціальної кабіни, надати необхідні для перевірки документи та відповісти на 15–20 питань, які задаються на вибраній ним мові. Питання генеруються довільно і стосуються декількох цілком природніх для такої ситуації тем: кінцевий пункт і мета поїздки, установчі відомості особи, яка опитується, її професійна діяльність тощо. Процес аналізу відповідей не більше п'яти хвилин, після чого залежно від висновків, виданих системою, пасажира пропускають до стійки реєстрації квитків або скеровують на проходження детальнішої перевірки до співробітників департаменту охорони аеропорту.

Розробники програмного забезпечення для «Cogito» стверджують, що ними були враховані всі позитивні надбання величезного досвіду ізраїльських спецслужб щодо виявлення потенційно небезпечних суб'єктів і встановлення дійсних намірів під час проведення їх опитування.

Під час проведених тестувань електронній системі «Cogito» вдалося «розкрити злочинні наміри» 85% «псевдотерористів», які брали участь у проведенні випробувань,

[1] Программа будет определять преступников по мимике. – 2007. – 9 августа. [Электронный ресурс]. – Режим доступа: http://www.2000.net.ua/it/bezopasnost/...

а лише 8% ні в чому не винних громадян були помилково затримані для проведення додаткової перевірки в зв'язку з можливою причетністю до терористичних дій. Розробники «Cogito», вартість якої оцінюється приблизно в 200 тис. доларів, працюють над підвищенням рівня «гарантованої ефективності» до 90% з одночасним зниженням кількості помилкових рекомендацій до 4%.

Але слід зауважити, що представники «Suspect Detection Systems» вважають, що їх технологічна новинка повинна не замінювати, а лише доповнювати існуючі засоби передпольотньої перевірки авіапасажирів.

Автори «Cogito» висловлюють упевненість у тому, що їхня розробка у комплексному використанні разом з інструментами виявлення зброї та вибухових речовин, що нині існують, дозволить значно знизити ризик проведення терористичних актів на авіаційному транспорті. «Навряд чи кому-небудь вдасться повністю автоматизувати всі принципи, на яких будується робота органів безпеки нашої країни, – говорить колишній глава «Шабака» (відомства внутрішньої безпеки Ізраїлю) та президент компанії «Asero Worldwide» (станом на 2008 рік) Дорон Бергербест-Ейлон. Але якщо хто-небудь зможе створити електронну систему, що буде керуватися принципами та філософією такої роботи, то така система буде справжньою знахідкою для фахівців усього світу, що ведуть боротьбу з тероризмом»[1].

У червні 2013 року були оприлюднені надані колишнім співробітником американського Агентства національної безпеки (АНБ) Едвардом Сноуденом матеріали щодо американської програми Prism. Це суперпрограма, яка використовується для аналізу інформації в глобальних соціальних мережах і яка дозволяє спецслужбам одержувати прямий доступ до серверів майже всіх провідних Інтернет компаній. Викриття Е. Сноудена стало найбільшим витоком інформації про діяльність Агентства національної безпеки (National Security Agency /NSA – АНБ/) за весь час існування цієї організації.

За своїм масштабом і потенційними наслідками для недоторканості приватного життя дії щодо збору й аналізу відомостей про місцезнаходження осіб перевершують усі інші програми стеження АНБ. Аналітики можуть вирахувати стільниковий телефон у будь-якому місці світу, відслідкувати його пересування у минулому та встановити таємні зв'язки між людьми, які телефонували на конкретний номер.

Агентство національної безпеки збирає ці відомості в одну базу даних, оскільки його дуже потужні аналітичні засоби відомі під назвою CO-TRAVELER, дозволяють відшукувати невідомих однодумців об'єктів стеження, слідкуючи за тим, де їх пересування збігаються або перехрещуються. Сучасні математичні методи дозволяють аналітикам NSA фіксувати відносини власників стільникових телефонів, зіставляючи маршрути їх пересування за тривалий час із тисячами й мільйонами інших абонентів стільникового зв'язку, які трапляються їм на шляху. CO-TRAVELER та інші програми вимагають методичного збору та зберігання відомостей про місцеперебування буквально у планетарному масштабі[2].

Американський фахівець Джеймс Бемфорд запевнює, що NSA має всі необхідні технології, щоб за потреби прослухати та записати кожну телефонну розмову, одержати доступ до будь-якої електронно-поштової скриньки, перехопити дані про фінансові

[1] Базаров Р. Счастливого полета! / Р. Базаров. – 2008. – 14 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Геллман Бартон. АНБ следит за мобильными телефонами по всему миру, об этом говорят документы Сноудена / Бартон Геллман (Barton Gellman), Ашкан Солтани (Ashkan Soltani) // The Washington Post, США. – 2013. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://www.inosmi.ru/world/...

транзакції та зломити захист кожної закритої бази даних. Також він повідомляє, що кілька років тому АНБ зробило «колосальний прорив» у галузі криптографії, і тепер агентство може дешифрувати найскладніші коди, а займатися цим буде надзвичайно потужний суперкомп'ютер.

Отже, Агентство національної безпеки (National Security Agency) реалізувало ідею тотальної обробки інформації та стало найбільшою, найтаємнішою й потенційно найагресивнішою спецслужбою в історії людства[1].

У Російській Федерації державна інформаційна система міграційного обліку була створена ще в 2007 році. Вона формується на основі центрального банку даних обліку іноземних громадян, банку даних щодо здійснення іноземними громадянами трудової діяльності, автоматизованих обліків адресно-довідкових підрозділів Федеральної міграційної служби та інших інформаційних систем.

На початку 2013 року прем'єр-міністр РФ Дмитро Медведєв підписав постанову, відповідно до якої інформацію про іноземців із бази біометричних персональних даних передбачається включати в державну інформаційну систему міграційного обліку. Також заплановано відомості про проходження іноземцем обов'язкової державної дактилоскопічної реєстрації та фотографування у випадках, встановлених законодавством РФ, передбачається включати в банк даних і відомості про трудову діяльність іноземних громадян у Росії[2].

Що стосується України, то наша держава – єдина країна Європи, яка ще не видає біометричних паспортів другого покоління. Також у нашій державі недостатній контроль за переміщенням мігрантів, а нелегальна трудова міграція негативно впливає на соціально-економічну ситуацію в Україні. Кількість мігрантів за оцінками експертів нині становить від 5 до 7 млн, а загальна їх чисельність буде тільки зростати. Відсутність контролю над міграційною ситуацією загрожує економічній безпеці України.

Нелегальна міграція створює умови для постійного порушення законів та існування корупції, оскільки нинішнє законодавство не дозволяє створити прозору систему відносин між державними органами і негромадянами країни. Замість того, щоб легально жити та платити податки, мігрантам набагато простіше «домовитися» з представниками влади та купити підроблені документи. Це призводить до постійного відтоку коштів з економіки країни, що виводяться нелегальними працівниками. За підрахунками фахівців вони можуть сягати щорічно 40–45 млрд гривень, водночас держбюджет недоодержує до 2 млрд грн у вигляді податків.

Завідувач відділом проблемно-орієнтованих інформаційних систем Інституту проблем реєстрації інформації НАН України Олександр Матов вважає, що чим швидше демографічний реєстр запрацює в нашій країні, тим швидше буде встановлений контроль за мігрантами та виключене шахрайство з документами.

Демографічний реєстр – це один з інформаційних проектів, за допомогою якого Україна прямує до інформаційного суспільства.

Створення Єдиного демографічного реєстру стане основою для принципово нової міграційної політики, тому що база даних і захищені від підробки біометричними технологіями документи – основні кроки в управлінні міграційними процесами. Міграція –

[1] В штате Юта строится хранилище данных, где будет сохраняться информация о каждом американце // Uipdp.com. – 2012. – 29 марта. [Электронный ресурс]. – Режим доступа: http://www.bezpeka.com/ru/news/...

[2] Россия расширит использование биометрических технологий в миграционном контроле // РИА Новости. – 2013. – 21 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

це природній процес – і саме тому українська держава повинна здійснювати його постійний облік і контроль, для чого демографічний реєстр дуже необхідний[1].

Що стосується сепаратизму, то в умовах політичної нестабільності в Україні головним регіоном можливого конфлікту більшість зарубіжних експертів ще у 2008 році називали Крим. Цей прогноз здійснився на початку 2014 року. Прецендент визнання багатьма членами світової спільноти незалежності Косово, визнання Росією незалежності Абхазії та Південної Осетії, як і слід було очікувати, призвів до пожвавлення сепаратистських настроїв на всіх територіях, де «тліють» етнічні та релігійні конфлікти[2].

Перші мусульманські громади в Україні почали відроджуватися на початку 90-х років минулого століття. Спочатку вони діяли під контролем Духовного управління мусульман Європейської частини СРСР і Сибіру. Громади були зареєстровані у багатьох великих містах української держави – Харкові, Запоріжжі, Дніпропетровську, Миколаєві, Одесі, Сімферополі, Львові та інших.

Але з часом традиційний іслам почав втрачати свої позиції. Крім офіційно зареєстрованих релігійних громад, почали з'являтися товариства, котрі сприяли поширенню ідеології радикально-екстремістських партій «Брати-мусульмани» та «Хізб ут-Тахрір». Ідеї радикального ісламу в Україні свого часу впроваджувалися в Криму. Ваххабітські громади будували мечеті на кошти, які надходили з Саудівської Аравії[3].

«Хізб ут-Тахрір аль-Ісламі» вважається терористичною організацією в 29 країнах, зокрема в низці держав Середньої Азії та в Росії[4].

Сьогодні під час політичної, економічної й енергетичної нестабільності на Євразійському континенті, що посилюється наслідками минулої глобальної фінансової кризи, дедалі гостріше проявляються проблеми терористичного, міграційного, соціального та регіонального характерів. За словами Нурсултана Назарбаєва «Тероризм – це продукт діяльності цілковито певних сил із зовсім конкретною метою. Історично сучасний тероризм має своїм джерелом політичні та економічні причини. Він міцно зв'язаний не тільки із транснаціональною злочинністю, наркотрафіком і контрабандою зброї, але, на жаль, він має ще й геополітичні джерела»[5]. І тому боротьба проти тероризму та супутніх йому явищ залежить від консолідованих зусиль і заходів, які здійснюються членами світової спільноти для подолання цих викликів людству в XXI столітті.

Запровадження біометричних систем та інших інноваційних технологій є складовою загального комплексу заходів міжнародної спільноти у боротьбі проти тероризму, незаконної міграції та транснаціональної злочинності.

---

[1] Эксперты назвали основы эффективной миграционной политики // Багнет. – 2012. – 19 октября. [Электронный ресурс]. – Режим доступа: http://www.bagnet.org/news/...

[2] Regnum: Перспективы войны в Закавказье и Средней Азии // Regnum.ru. – 2008. – 13 июня. [Электронный ресурс]. – Режим доступа: http://www.regnum. ru/news/…

[3] Лизан Иван. Вилайет Крым: к росту исламского радикализма на Украине / Иван Лизан // Odnako.org. – 2013. – 17 июня. [Электронный ресурс]. – Режим доступа: http://oko-planet.su/politik/politikukr/...

[4] СБУ спасла Украину от террористов // Mignews.com. – 2009. – 12 мая. [Электронный ресурс]. – Режим доступа: http://www.mignews.com/news/politic/cis/...

[5] Игнатченко Игорь. Балканизацию Евразии начинают с Казахстана / Игорь Игнатченко // Независимое военное обозрение. – 2011. – 16 декабря. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/wars/...

Розділ 11

ПАСПОРТНО-ВІЗОВІ ДОКУМЕНТИ НОВОГО ПОКОЛІННЯ

Усі держави, що приймають велику кількість осіб, які приїзджають на їхню територію, хотіли б убезпечити себе від будь-яких небажаних елементів. Для підвищення рівня безпеки, однією з складових якої є довіра до документів, котрі засвідчують особу, яка подорожує, світова спільнота зробила висновок, що необхідно використовувати паспортно-візові документи нового покоління (ПВДНП), які ще мають таку назву в засобах масової інформації: машинозчитувальні біометричні проїзні документи (відповідна абревіатура – МЗПД або MRTD).

2002 року 118 країн світу підписали Новоорлеанську угоду про визнання біометрії основною технологією ідентифікації для паспортів і в'їзних віз (тепер її ратифікували приблизно 180 держав). Нині понад 100 країн запровадили біометричні (інша поширена назва – електронні) паспорти[1].

Широке використання ПВДНП, які вдосконалені за допомогою засобів біометричної верифікації та ідентифікації, дозволяє значно зменшити час проходження пасажирів через контрольні пункти в аеропортах, підвищити рівень авіаційної безпеки та посилити захист від можливої підміни особистості. Більшість країн світу переходять до цієї системи для підвищення продуктивності превентивних заходів у боротьбі з тероризмом, незаконною міграцією, транснаціональною злочинністю, незаконною торгівлею зброєю, наркотиками й іншими злочинними діями.

2000 року Європейським Союзом (ЄС) була прийнята «Резолюція з питань безпеки паспортних документів і інших подорожніх документів», якою встановлювалося, що з 1 січня 2005 року в країнах ЄС вводяться загальнообов'язкові мінімальні стандарти безпеки у сфері виробництва паспортних і проїзних документів, що повинні сприяти належному захистові паспортно-візових документів від підробок. Стандарти безпеки для ПВДНП передбачали введення біметричної ідентифікації власників документів.

У вересні 2001 року Радою Безпеки ООН була прийнята резолюція № 1373 щодо боротьби з міжнародним тероризмом, у якій особлива увага була приділена посиленню заходів із запобігання можливостей фальсифікації офіційних документів, підвищенню їх надійності й уніфікації відповідно до розроблених єдиних світових вимог. Міжнародна організація цивільної авіації (International Civil Aviation Organization /ICAO – ІКАО/) опублікувала рекомендації, згідно з якими всі члени цієї структури повинні були до квітня 2010 року налагодити в своїх країнах випуск біометричних (електронних) паспортно-візових документів нового взірця. Відповідно до нових критеріїв безпеки ICAO, звичайні

[1] Кыргызстан. Отставание во внедрении биометрических паспортов сохраняется // ИА K-News. – 2013. – 20 мая. [Электронный ресурс]. – Режим доступа http://www.biometrics.ru/news/...

паперові паспорти були визнані документами, що є недостатньо захищеними від можливостей їх підробок.

Відповідно до цих резолюцій і рекомендацій, Постановою Ради ЄС № 2252/2004 від 13 грудня 2004 року була затверджена Програма «Електронний паспорт» (ePassport). Згідно з ухвалою Єврокомісії K/2006/2909, всі країни-члени ЄС повинні були до 28 червня 2009 року виконати рішення про обов'язковий перехід на видачу нових біометричних закордонних паспортів, причому з наявністю, крім обов'язкового оцифрованого фотозображення, хоча б ще одного суто біометричного параметра[1].

Необхідно зазначити, що в міжнародній біометрії терміни «електронний паспорт» і «паспортна система» сприймаються дещо ширше, ніж у буквальному розумінні цього словосполучення. Термін «ePassport» – наявність будь-якого документа, за допомогою якого можна ідентифікувати громадянина за його біометричними параметрами. Такими ідентифікаційними документами, окрім паспорта, можуть бути посвідчення особи, водійські права, кредитна картка, соціальне посвідчення (у закордонних ЗМІ вживається здебільшого термін «ID-Cards»).

На сьомому Міжнародному конгресі (ID World), що відбувся 18–21 листопада 2008 року в Мілані, комісія Євросоюзу підтвердила рішучість звертатися до суду стосовно країн Єврозони, які не встигнуть організувати процедуру видачі електронних біометричних паспортів до середини 2009 року[2].

На конференції 19–20 липня 2007 року ОБСЄ у Відні було заявлено, що з 1 січня 2015 року в'їзд на територію ЄС і США за паспортами з наклеєними фотографіями буде заборонений. У майбутньому може виникнути ситуація, коли переміщати країнами світової спільноти, не маючи електронно-біометричних документів, буде неможливо.

Євросоюз, США і низка інших країн пришвидшеними темпами здійснили або завершують здійснення переходу на біометричні паспортно-візові документи нового покоління, що є невід'ємною складовою програми боротьби світової спільноти з такими негативними явищами кінця XX – початку XXI століття, як міжнародний тероризм, наркотрафік, організована злочинність і масова незаконна міграція, які, як відомо, не визнають наявності сучасних державних кордонів[3].

Закордонні електронні паспорти, що випускалися з 2005 року до нині, ділять на два види: *першого покоління*, коли в пам'ять мікрочіпа з біометричних показників вносилося тільки оцифроване фотозображення власника документа, і *другого покоління*, коли в мікросхему додатково вноситься хоча б один з інших біометричних ідентифікаторів – відбитки пальців або райдужна оболонка ока. Із липня 2009 року в Євросоюзі обов'язковим доповнюючим біометричним параметром для закордонних паспортів стало електронне зображення папілярного малюнка пальців.

Для підвищення рівня безпеки або, як говорять фахівці, довіри до документів, світова спільнота зробила висновок, що в біометричних паспортах необхідно використовувати електронний носій інформації, завірений цифровим підписом країни, котра випустила документ, без можливості щось у ньому виправити, а також сучасні можливості

---

[1] Латвия. Начинается выдача биометрических паспортов второго поколения // BizNews.lv. – 2008. – 15 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Минкин В. Дактилоскопический паспорт – каждому россиянину! / В. Минкин // Элсис. [Электронный ресурс]. – Режим доступа: http://www.elsys.ru/review1.php

[3] Самсоненко С. Евросоюз ожидает от Украины внедрения электронных документов / С. Самсоненко // From-ua.com. – 2008. – Декабрь. [Электронный ресурс]. – Режим доступа: http://www.from-ua.com/technology/...

захисту від підробок видимої інформації. Всі ці чинники повинні суттєво підвищити рівень надійності нових ідентифікаційних документів. Отже, паспортно-візові документи нового покоління характеризуються насамперед високим ступенем загального захисту від можливих підробок.

Бланки нових посвідчень особистості виготовляються за уніфікованими міжнародними вимогами та стандартами, що пред'являються до машинозчитуваних документів. Відмінними рисами паспортів нового покоління є те, що на титульній обкладинці документа розміщено стилізоване зображення електронного чіпа, а сам документ містить пластикову полікарбонатну сторінку, яка є багатошаровою конструкцією, спресованою за високої температури, в якій розміщена так звана інлента, – лист із спеціального матеріалу, що містить безконтактну мікросхему з антеною. Мікросхема (у західних джерелах має назву RFID-чіп) містить незалежну пам'ять (як правило, для паспортів першого покоління об'ємом у 32 Кб, для паспортів другого покоління – 64 Кб).

Електронному зчитуванню підлягають метричні дані власника та самого документа: прізвище, ім'я і по батькові, дата народження, стать, номер паспорта, дата видачі та завершення терміну дії паспорта (всі відомості, що зазначені на лицьовій сторінці документа), а додатково – оцифрована фотографія (з паспортів першого покоління) або оцифрована фотографія і відбитки двох вказівних пальців кожної руки (з документів другого покоління). Деякі країни ввели ще один біометричний показник (або здійснили заміну) – райдужну оболонку ока[1].

Отже, одним з основних елементів біометричного або електронного документа є RFID-чіп, що складається з мікрочіпа й антени для передачі даних. У пам'яті чіпа зберігається його власний унікальний номер та інша спеціальна інформація – залежно від сфери використання. Коли власник біометричного паспорта потрапляє в зону реєстрації, спеціальний сканер зчитує інформацію з малогабаритної інтегральної схеми. За деякими даними, що трапляються в ЗМІ, за наявності спеціальних зовнішніх умов радіус дії RFID-чіпа може сягати до 100 м, хоча офіційно він не повинен перевищувати 7 см. Електронний чіп, на який записані біометричні відомості, відповідно до заяв офіційних осіб, захищений від можливості несанкціонованого доступу і відповідає всім вимогам підвищеного рівня безпеки[2].

Пластикова сторінка, що містить дані, які візуально перевіряються, сформована також на основі нової технології – «лазерного гравіювання», що дозволяє в буквальному розумінні «випалювати» зображення та записи на полікарбонаті, захищаючи від можливості підробки найважливішу сторінку в паспорті[3].

Крім того, на полікарбонатній сторінці передбачена зона, на яку нанесена інформація в закодованому вигляді стосовно власника для зчитування спеціальними пристроями (оптичне зчитування). Захисту машинозчитуваної сторінки ІСАО приділяє особливу увагу. В її рекомендаціях зазначено, що використання для цієї мети полікарбонату – найнадійніший спосіб захисту документа від підробки. Нанесення на таку сторінку

[1] Биометрический загранпаспорт – новая революция? // Федеральная миграционная служба России. – 2008. – 15 января. [Электронный ресурс]. – Режим доступа: http://fms.gov.ru, http://biometrics.ru/document.asp...

[2] Лукашов И. Биометрия становится индустриальной технологией / И. Лукашов // Cnews.ru. – 2007. – 21 августа. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security2007/...

[3] Биометрический загранпаспорт – новая революция? // Федеральная миграционная служба России. – 2008. – 15 января. [Электронный ресурс]. – Режим доступа: http://fms.gov.ru, http://biometrics.ru/document.asp...

інформації за допомогою технології лазерного гравіювання і перфорації унеможливлює зміну цієї інформації без пошкодження самої сторінки.

Під час транспортування документа до місця видачі майбутньому власникові він захищається спеціальним транспортним кодом, тому в разі його втрати електронні дані просто не зчитуватимуться. Сам багатолистовий закордонний паспорт повинен бути захищений відповідно до вимог технології SHIELDTM – прошитий за всією довжиною корінця ниткою з пунктирним висвітленням під дією ультрафіолетового випромінювання, а сторінки покриті спеціальною дуже тонкою плівкою з нанесеними багаторівневими голографічними захисними елементами[1].

Отже, інформація, що міститься в закордонних паспортах нового покоління, по суті, дублює ту, яка вносилася в старі паспорти з вклеєною фотографією. За винятком відомостей щодо наявності дітей (тепер на неповнолітніх дітей молодших 14 років теж повинен оформлюватися окремий електронний закордонний паспорт) і таких біометричних персональних даних, як електронне зображення відбитків пальців, а в деяких випадках додатково і райдужної оболонки ока. Конфіденційність цих відомостей європейські держави, що ратифікували Конвенцію Ради Європи про захист фізичних осіб при проведенні автоматизованої обробки персональних даних, гарантують.

Розглянемо основні етапи реалізації міжнародним співтовариством програми «електронний паспорт» (ePassport).

1968 року Міжнародна організація цивільної авіації (International Civil Aviation Organization /ICAO – ІКАО/) почала розробку специфікацій всесвітнього Стандарту для машинозчитуваних паспортів. Стандарт ICAO розроблявся для мінімізації часу, потрібного для проходження прикордонних формальностей або передпольотного контролю.

2002 року 118 країн світу підписали Новоорлеанську угоду, яка визнає біометричні параметри особистості одними з обов'язкових елементів для внесення відомостей щодо них у закордонні паспорти та в'їзні візи нового покоління.

22 травня 2003 року була затверджена рекомендація Технічної консультативної групи щодо машинозчитуваних проїзних документів (TAG/MRTD), яка згодом отримала назву «план ІКАО».

Цей документ рекомендує:

– вибір технології розпізнавання рис обличчя та особливості її використання для здійснення автоматичного розпізнання особистості;

– використання безконтактної інтегральної мікросхеми (мікрочіпа) з мінімальним об'ємом пам'яті у 32 Кб як засобу зберігання електронних даних, зокрема й біометричних, у будь-яких проїзних документах;

– проведення операції програмування інтегральних мікросхем із використанням команд, які задаються відповідно до логічної структури даних (ЛСД);

– використання певним чином зміненої схеми інфраструктури відкритих ключів (Public Key Infrastructure /PKI/) для застосування електронноцифрового підпису з метою захисту електронних даних від можливості проведення операцій із несанкціонованих змін[2].

---

[1] Авдеева С. Биометрические паспорта – защита от нелегалов и террористов / С. Авдеева // Караван+Я. – 2008. – 22 мая. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp...; Мальта. Правительство заключило контракт на поставку полной системы электронных паспортов // PR Newswire. – 2008. – 14 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Биометрия в авиационной безопасности // Системы безопасности. – 2007. – № 3. [Электронный ресурс]. – Режим доступа: http://www.secuteck.ru/ articles2/sys_ogr_dost/…

Рішення щодо запровадження паспортів із використанням біометричних технологій було ухвалене на зустрічі міністрів внутрішніх справ країн «Великої вісімки» у травні 2003 року.

11 липня 2005 ICAO затвердив специфікації машинозчитуваного паспорта, що були розроблені разом з Організацією Міжнародних Стандартів (ISO) як всесвітній стандарт для паспорто-візових докуметів нового покоління. У специфікаціях наведені правила, які регламентують процедуру виготовлення стандартизованих паспортних документів із підвищеним рівнем безпеки. Із затвердженням специфікацій як міжнародного стандарту всі члени ICAO (у 2005 році їх налічувалося 188) дали згоду щодо запровадження нової версії електронного паспорта («ePassport»), який повинен повністю відповідати вимогам Стандарту ISO. Термін завершення перехідного періоду був визначений 1 квітня 2010 року. Багато країн перейшли на використання електронних паспортів до 2008 року, але деякі так і не змогли запровадити їх навіть до другого півріччя 2014 року.

Оскільки Україна прагне отримати безвізовий режим із країнами Європейського Союзу (ЄС) і США, детально розглянемо основні дати запровадження паспортно-візових документів нового покоління в ЄС і Сполучених Штатах Америки:

– свого часу ЄС зобов'язав усіх членів співтовариства до вересня 2006 року запровадити цілком сумісні електронні паспорти, які б містили оцифроване зображення обличчя, але у зазначений термін ця вимога низкою держава Євросоюзу не була виконана;

– Сполучені Штати Америки зобов'язали з 26 червня 2005 року всі держави, які мають безвізовий режим доступу на територію США (наприкінці 2008 року їх кількість досягла 34 країн, на 01.03.2014 р. – 37), забезпечити своїх громадян закордонними біометричними паспортами («ePassport»), які б повністю відповідали вимогам стандарту ICAO.

26–27 травня 2005 року на 7-му семінарі Міжнародної Групи Porvoo, що була створена в зв'язку з проектом ЄС «eEurope» (Електронна Європа), представники 18 європейських держав, Японії і США, а також представники Європейської комісії та Об'єднаних Націй сформулювали три головні завдання політики за Е-паспортом («ePassport»):

– розширення використання сертифікатів PKI (Public Key Infrastructure);

– повна сумісність із міжнародними та стандартами Євросоюзу, що повинно забезпечити загальносвітову сумісність програми «ePassport»;

– стандартизація ринку послуг, пов'язаного з запровадженням технологій Е-паспорта, і, як наслідок, обов'язкове забезпечення проведення сертифікації послуг, що надаються.

Відповідні стандарти Євросоюзу затверджені Постановою Ради ЄС від 29.12. 2004 року (Council Regulation /EC/ on standards for security features and biometrics in passports and travel documents issued by Member States, Official Journal L 385, 29/12/2004 P. 0001 – 0006). Основним змістом програм із стандартизації є питання забезпечення безпеки й уніфікації технічних стандартів та імплементація необхідних вимог до національних законодавств країн ЄС[1].

Нині значна кількість держав перейшли або завершують перехід до видачі біометричних посвідчень особистості другого покоління: закордонних і внутрішніх паспортів, водійських посвідчень, посвідчень моряка, соціальних карт, військових квитків тощо. Порівняно з традиційними такі документи дозволяють надійно встановлювати, чи є пред'явник документа його дійсним власником, значно підвищити захищеність

[1] Мартиненко С. Сучасні програми розвитку Е-Уряду / С. Мартиненко. – 2005. – березень. [Електронний ресурс]. – Режим доступу: http://www.itsway.kiev.ua/index...

документів від підробки, автоматизувати роботу співробітників контрольно-пропускних пунктів, пришвидшити і полегшити процедуру перевірки документів.

Необхідно виокремити таку особливість впровадження зовнішніх і внутрішніх біометричних документів: у деяких країнах закордонний біометричний паспорт одночасно є і внутрішнім паспортом, хоча у більшості держав світової спільноти він призначений тільки для зарубіжного використання. У 2008–2009 роках низка держав одночасно із запровадженням закордонного біометричного документа також вводять біометричні посвідчення особи, що призначені тільки для внутрішнього використання. У зв'язку з цим варто нагадати, що в епоху холодної війни двох систем у минулому столітті радянська практика паспортизації-реєстрації населення трактувалася на заході як один із порочних атрибутів тоталітарного суспільства. Тепер же виявилось, що розбіжності в цьому питанні мали суто кон'юктурний та косметичний характер. А постійна і надійна ідентифікація власних громадян за допомогою високотехнологічних методів – це, за запевненнями високопосадовців урядів провідних країн світу, дуже зручна та корисна річ для будь-якої держави і на Сході, і на Заході[1].

Міжнародна організація цивільної авіації (ICAO) та Міжнародна організація з стандартів (ISO) внесли в 2006 році зміни до стандартів, які регламентують запис електронних моделей біометричних показників у мікрочіпи паспортно-візових документів нового покоління, що дало можливість розпочати широке використання систем автоматичного розпізнавання за обличчям.

Але видача біометричних документів населенню – це лише частина, причому не найскладніша, набагато серйознішого та масштабнішого завдання, що виникає перед будь-якою державою через запровадження паспортно-візових документів нового покоління (ПВДНП). Для запровадження у комплексі всієї системи функціонування ПВДНП потрібна реалізація багатьох додаткових і супутніх заходів:

– розробити та ухвалити відповідні закони, національні стандарти;

– створити центр персоналізації паспортів, який заповнює їх графічною й електронною інформацією та засвідчує державним електронним цифровим підписом;

– створити централізовані бази біометричних даних (БД);

– забезпечити відповідний захист персональної інформації у БД;

– впровадити державну систему захищеної передачі біометричних даних;

– реалізувати інфраструктуру інформаційної взаємодії відповідних державних структур;

– розробити та ввести необхідні засоби контролю та криптографічного захисту наявної інформації на всіх етапах запровадження ПВДНП;

– забезпечити проведення робіт, які реалізують функції автоматизованої верифікації та ідентифікації особистості з заданими ймовірними характеристиками.

Експерти з біометричних технологій особливо виокремлюють необхідність забезпечення виконання ще однієї вимоги, невиконання якої може звести нанівець позитивний ефект від запровадження біометричних документів. Йдеться про реалізацію ще однієї достатньо складної умови на рівні національних держав. *Ця складність пов'язана з недопущенням можливості одержання документів нового покоління, куди можуть бути офіційно внесені фальшиві персональні дані. Фахівці зазначають, що біометричні дані, хоча й пов'язують людину з фізичними атрибутами для підтвердження її особистості, дієві настільки, наскільки є ефективним процес перевірки та засвідчення реальної фізич-*

[1] Жажда биометрии. [Электронный ресурс]. – Режим доступа: http://gbop.nm. ru/htm/gbop-8-2.htm

ної особи під час видачі їй біометричних документів, що надалі засвідчуватимуть його особистість. Дуже важливо, щоб сучасні технології не були використані для прикриття осіб, які перебувають у розшуку, за допомогою біометричних посвідчень нового покоління з фальшивими установчими відомостями. Це проблема не виготовлення документів, а організації перевірки достовірності персональних даних, які надаються, і, особливо, документів старого взірця, що засвідчують особу. Слід виключити на державному рівні можливість того, щоб антисоціальні елементи, особливо терористи, змогли створити канали для отримання посвідчень нового покоління з легалізованими фальшивими персональними даними[1].

На щорічній зустрічі міністрів юстиції країн «Великої вісімки» (G8), яка відбулася в Токіо влітку 2008 року, вперше розглядалася проблема злочинів, які пов'язані з ідентифікацією особи. Незважаючи на широке визнання серйозності цієї проблеми, державам G8 необхідно досягти її ліпшого розуміння та необхідної взаємодії, вважають організатори зустрічі. Навіть у тих країнах, де до вирішення цього завдання ставляться з необхідною увагою, існує недостатнє розуміння всієї важливості цієї проблеми і, особливо, оцінок її можливих негативних наслідків[2].

Ця тема обговорювалась і під час дискусії у Європарламенті в січні 2009 року щодо проблем, пов'язаних із переходом країн Шенгенської зони на біометричні паспорти нового покоління. Парламент Євросоюзу наголосив на необхідності посилення заходів безпеки під час здійснення процесу оформлення біометричних паспортів і належної перевірки громадян країн ЄС, які бажають отримати ці документи[3].

Останнім часом світова спільнота приділяє особливу увагу проблемі сумісності біометричних технологій. Біометричні технології повинні бути сумісними, інакше в них не буде жодного сенсу. Необхідно бути впевненим у тому, що всі країни створили сумісні між собою системи. Світ не повинен бути розділений на різні біометричні блоки, оскільки одне із завдань упровадження біометричних технологій полягає саме у спрощенні перетину кордонів. Необхідно прийти до такої системи, з якою всі держави погодяться.

Застосування біометричних технологій стає одним із найважливіших чинників, що визначають успішність і конкурентоспроможність будь-якого суб'єкта суспільного життя, чи то приватна особа, компанія або держава.

Сучасні паспортно-візові документи нового покоління – це не данина черговій міжнародній моді, а один із заходів безпеки та протистояння загальносвітовим проблемам, з якими людство зіткнулося на рубежі XX і XXI століть.

Ще один аспект запровадження ПВДНП – це автоматизація процесу проходження контролю з метою ідентифікації особистості. Автоматизована система паспортного контролю дозволяє не тільки перевіряти інформацію про власника біометричного паспорта за базами даних, але й автоматично звірити зовнішність людини з його фотографією

[1] Биометрия на службе государству // Secuteck.ru. – 2008. – 29 октября. [Электронный ресурс]. – Режим доступа: http://secuteck.ru/newstext...; Месмер Э. Биометрия на службе государству / Э. Месмер // Открытые системы. – 2008. – 6 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...; Митин В. Интервью. Настоящее и будущее российских биометрических паспортов / В. Митин // PC Week/Russian Edition. – 2009. – 28 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] G8 обсуждает проблемы преступлений «против идентификаторов личности» // BIOMETRICS.RU. – 2008. – 18 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Европейский парламент обсудил внедрение биометрических паспортов нового поколения // BIOMETRICS.RU. – 2009. – 15 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

у пред'явленому документі. У березні 2012 року в Євросоюзі оголосили про намір запровадити стандартизовану систему автоматичного паспортного контролю на кордонах Євросоюзу. За даними ЗМІ, практичне застосування вже відбулося в лондонському аеропорті Хітроу, амстердамському Скіпхоле, у Фінляндії та Мадриді[1].

Зробимо невеличкий екскурс в історію впровадження біометричних документів у країнах світової спільноти. Першою країною, яка ввела в обіг біометричні документи, була Малайзія. В середині 2001 року в цій державі вперше у світі були впроваджені ідентифікаційні картки (ID-Cards), які містили в електронному вигляді біометричну інформацію (малюнок папілярного узору пальця), що розміщувався у спеціальній інтегральній мікросхемі (мікрочіпі). Мікрочіп за спеціальною технологією впресовувався у пластик індивідуальної картки.

Ці біометричні ID-Cards, що засвідчували особистість пред'явника, в обов'язковому порядку були видані всьому дорослому населенню Малайзії[2].

Із європейських країн першою у цій сфері була Великобританія. 2002 року уряд Великобританії оголосив, що з часом усі громадяни країни до 2006 року отримають смарт-карти. Але зазначений термін неодноразово переносився. У мікрочіп документа вносять дані про відбитки пальців, райдужної оболонки ока та фотозображення обличчя. Смарт-картки планується використовувати як посвідчення особистості поряд із звичайними паспортами.

Із 2008 року кожен британець, який звертається за новим закордонним паспортом, за наявності бажання може отримати ідентифікаційну карту для внутрішнього користування, причому в реєстр населення Великобританії автоматично будуть внесені його біометричні дані.

Мета цього заходу – унеможливити або максимально ускладнити процес фальсифікації документів, що засвідчують особистість, полегшити для громадян процедуру здійснення банківських операцій, спростити доступ до медичної страховки, в центри зайнятості, бібліотеки та інші організації, а також реалізувати черговий етап ідеї створення «eGovernment» – «електронного уряду». У всіх перелічених випадках пред'явлення для отримання доступу до вказаних послуг, а в перспективі й до низки інших, наявність біометричної ID-картки є обов'язковою[3].

Із 25 листопада 2008 року прикордонним агентством Великобританії (UK Border Agency /UKBA/) розпочато видачу нових пластикових посвідчень особи іноземцям, які мають намір тривалий час залишатися на території держави. У Сполученому Королівстві планується завершити повний перехід на пластикові ID-картки у 2014–2015 роках.

Як відомо, 28 серпня 2006 року Єврокомісія ухвалила законодавче рішення про обов'язкове введення біометричних паспортів з електронним чіпом, в якому розміщене зображення обличчя власника. Із 28 червня 2009 року в чіпи біометричних паспортів, які видаються на теренах Євросоюзу, почали вносити ще й відбитки пальців[4].

---

[1] Россия обзаведётся собственной биометрической системой пограничного контроля // ТАСС-Телеком. – 2012. – 29 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Панкратов А. Паспорт, виза, идентификация: биометрические технологии на службе государства / А. Панкратов // Информационное общество. – 2005. – Вып. № 2. – С. 4–7. [Электронный ресурс]. – Режим доступа: http://emag.iis.ru/arc/infosoc/emag

[3] Биометрические удостоверения личности сами по себе не остановят фальсификаций и мошенничества // Secnews.ru. – 2006. – 28 августа.

[4] Еврокомиссия подала в суд на Бельгию из-за невыполнения обязательств по переходу на биометрические паспорта нового поколения // Укринформ. – 2012. – 22 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news

Одна з переваг біометричного паспорта – можливість вільного пересування територією ЄС кожного європейця, який є його власником, без отримання будь-яких додаткових документів.

У листопаді 2011 року в 25 країнах Шенгенської угоди була запущена інформаційна візова система VIS. За її допомогою планується пришвидшити процес обробки заяв на одержання візи завдяки використанню оцифрованих відбитків пальців і зображення лиця здобувачів віз, а також забезпечити швидкий обмін відомостями про короткострокові візи між усіма країнами Шенгенської зони. Із 2014 року шенгенську візу можна одержати тільки після проходження процедури сканування відбитків пальців особи, яка забажала отримати візу.

На думку представників владних структур ЄС, зняття відбитків пальців має допомогти у боротьбі з практикою «оренди паспортів», яка особливо поширена серед громадян азіатських країн.

У жовтні 2013 року суд Європейського співтовариства у Брюсселі ухвалив, що здача та зберігання відбитків пальців під час одержання біометричного паспорта є порушенням права на особисте життя, але визнав це виправданим заходом для ефективної боротьби з нелегальним проникненням на територію Євросоюзу, шахрайським використанням документів й іншими фальсифікаціями[1].

У липні 2012 року Єврокомісія повідомила про те, що з наступного року в права водія громадян країн – членів ЄС заплановано включати відомості про їхні біометричні ідентифікатори.

Поряд з основними персональними даними водія і його фотографією вони будуть також містити «додаткову інформацію» – відбитки пальців або райдужної оболонки очей[2].

Нині багато західних країн запровадили технології електронних паспортів та систем прикордонної ідентифікації eGate. Але є й деякі винятки.

Наприклад, наприкінці 2012 року Єврокомісія подала скаргу на Бельгію до Суду ЄС за невиконання зобов'язань із видачі біометричних паспортів, які повинні містити відбитки пальців власника.

Таке рішення було ухвалено через те, що Бельгія більш ніж на три роки прострочила терміни, відповідно до яких необхідно було виконати зобов'язання в межах законодавства ЄС щодо введення паспортів із біометричними даними власників.

Як зазначила Єврокомісія, наявність захищених документів для подорожей громадян ЄС є основним чинником функціонування Шенгенської зони – загального європейського простору для вільного й безпечного переміщення[3].

У галузі впровадження біометричних технологій у паспортні документи в європейському співтоваристві лідерство належить Федеративній Республіці Німеччина (ФРН). ФРН першою з європейських країн запровадила видачу закордонних паспортів другого покоління ще у листопаді 2007 року, а 23 липня 2008 року федеральний уряд затвердив нову форму внутрішнього посвідчення особи, видача якого розпочалася з кінця

[1] Суд ЕС признал законным внесение в биометрические паспорта сведений об отпечатках пальцев // РАПСИ. – 2013. – 18 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Водительские права в Евросоюзе станут биометрическими // BIOMETRICS.RU. – 2012. – 9 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Еврокомиссия подала в суд на Бельгию из-за невыполнения обязательств по переходу на биометрические паспорта нового поколения // Укринформ. – 2012. – 22 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

2010 року. Але розміщення відсканованих зображень відбитків пальців у внутрішньому документі є справою добровільною і залежить від бажання власника[1].

Загалом «біометрична паспортна перебудова» у Німеччині розпочалася з 1 листопада 2005 року. Наприкінці 2005 року в німецьких закордонних документах були присутні оцифровані фотографії, що, за словами тодішнього міністра внутрішніх справ ФРН Вольфганга Шойбле, «істотно підвищило рівень безпеки в країні». Нові ж паспорти «другого покоління» з відбитками пальці, як слушно зауважив міністр, дозволили державі «бути на крок попереду злочинних елементів». Контроль за відбитками унеможливить проникнення в країну особи, яка не є власником документа, – прикордонний контроль розпізнає зловмисника за декілька секунд[2].

Процес внесення електронних даних папілярних узорів двох відбитків пальців у німецькі електронні паспорти проходить у заводських умовах з обов'язковим дотриманням процедури підвищеного рівня безпеки – EAC (Extended Access Control – розширений контроль доступу), застосування якої рекомендовано Європейською комісією. Технологія EAC вимагає застосування спеціальних засобів шифрування, що дозволяє забезпечити необхідний захист конфіденційних даних і запобігає можливостям їх несанкціонованого зняття[3].

Згідно з директивою Євросоюзу та МВС Німеччини, відомості про дітей не вносяться до паспортів батьків: кожна дитина повинна отримувати власний закордонний паспорт терміном дії на 6 років. Продовжуватися документ може лише один раз, починаючи з 6-річного віку в ньому передбачена можливість внесення відбитків пальців.

Німеччина є першою країною Європейського Союзу, яка здійснила перехід на повноформатні біометричні закордонні паспорти другого покоління. Що стосується внутрішніх біометричних посвідчень особистості, то запровадження посвідчень із відсканованими зображеннями відбитків пальців полегшить банківські перекази, зробить непотрібними особисті ідентифікаційні номери (PIN) і транзакційні коди (TAN), виключить необхідність щорічного придбання спеціальної програми «Elster» для заповнення податкової декларації, дозволить спростити процедуру здійснення покупок, а також заощадити час, необхідний для оформлення елементарних речей на зразок реєстрації прописки або отримання паркувальної віньєтки.

Нове посвідчення особи (ID-Card) не займає багато місця в портмоне, оскільки ця пластикова картка має такі ж розміри, як і у звичайної кредитної картки. Але з часом і саму кредитку біометрична карта теж може замінити, тому що при забезпеченні деякими додатковими ознаками вона дозволить здійснювати практично всі фінансові операції через Інтернет, включаючи замовлення авіаквитків і відкриття рахунку. Для здійснення процедури ідентифікації в Інтернеті необхідне використання ще одного додаткового мікрочіпа, що буде другою мікросхемою, розміщеною у документі.

Повний набір послуг, який надаватиметься в режимі «On-line» через Всесвітню мережу, буде можливим у тому випадку, якщо в пам'яті мікрочіпа біометричної картки будуть розміщені у добровільному порядку електронне зображення відбитків пальців

---

[1] Германия. Согласованы требования к новому внутреннему паспорту // Немецкая волна. – 2008. – 16 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Взлом биометрического паспорта – дело времени, считают немецкие эксперты // Newsru.com. – 2007. – 9 ноября. [Электронный ресурс]. – Режим доступа: http://www.news.ru.com/world/...

[3] Германия. В биометрических паспортах «второго поколения» будут использоваться новейшие интеллектуальные микросхемы // BIOMETRICS.RU. – 2007. – 7 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

та електронний підпис власника на додаток до обов'язкових персональних даних таких, як дата та місце народження, адреса місця реєстрації проживання, зріст, вага, колір очей і оцифрована фотографія. Оскільки процедура зняття біометричних ідентифікаторів та їх наявність у загальнонімецьких внутрішніх посвідченнях особистості справа добровільна, то хочеш – здавай відбитки пальців і автограф для внесення в ID-картку та на зберігання в спеціальному банку даних, а якщо не маєш бажання – то не здавай. Але в першому випадку власник ID-Card буде мати можливість доступ до віртуальних благ і використовувати внутрішньонімецьке посвідчення особи як ерзац-паспорт під час перетину кордону[1].

США – перша держава в світі, де почали вважати наявність документа з біометричною інформацією щодо власника істотною складовою гарантії безпеки та громадянських свобод, необхідною умовою боротьби з тероризмом. Тому не дивно, що головною рушійною силою запровадження біометричної ідентифікаційної технології у світовій спільноті стали саме Сполучені Штати Америки, де після відомих подій 11 вересня 2001 року був ухвалений федеральний закон, що передбачає введення єдиного для всіх американців взірця внутрішнього посвідчення особи (як відомо, головним особистим документом мешканця США є водійські права, які випускаються та видаються окремо кожним штатом)[2].

Що стосується біометричних паспортів, то після 2006 року всі паспорти, які видаються в США, є біометричними – з даними власника, двовимірною фотографією, цифровим підписом і відбитками пальців у електронному вигляді.

Отже, необхідною умовою для використання систем біометричного контролю є запровадження в повсякденне життя необхідних «електронних» документів – внутрішніх і зовнішніх паспортів, посвідчень особи («ID Cards»), смарт-карток та інших документів із персональною біометричною інформацією, що надає можливість однозначно ідентифікувати особу пред'явника. Слід зауважити, що одночасно з вирішенням цієї проблеми необхідне впровадження комплексу інших державних і міждержавних програм, які дозволять у режимі реального часу отримати віддалений захищений доступ до необхідних баз даних і здійснити процедуру відповідного обміну даними.

На 1 червня 2008 року приблизно 10% службовців федеральних урядових органів США отримали персональні біометричні ідентифікаційні картки (Personal Identity Verification /PIV/ cards), які призначені для верифікації особистості їх власників. Програма видачі біометричних PIV-карт здійснюється відповідно до директиви з національної безпеки (HSPD-12), згідно з якою під час видачі PIV-картки проводиться ретельна перевірка відомостей, що засвідчують особистість кожного службовця. Передбачалось завершити видачу Personal Identity Verification cards до кінця 2007 року, потім він був перенесений на кінець 2008 року[3].

У травні 2013 року, майже через десятиліття після виходу Президентської директиви про національну безпеку США (HSPD-12), Міністерство внутрішньої безпеки (МВБ) нарешті добилося перших реальних результатів із прив'язки посвідчення особи до власника. МВБ розпочало амбіційний проект щодо інтеграції до національних ID-карт

[1] Ободовская Е. Технологическая модернизация за 59 евро / Е. Ободовская // Русская Германия. – 2008. – 5 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

[2] Террористическая атака, произошедшая 11 сентября 2001 года, фундаментально изменила отношение США к проблеме безопасности // Washprofile.org/ru. – 2007. – 13 сентября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

[3] Американские госслужащие получают биометрические идентификационные карты // BIOMETRICS.RU. – 2008. – 6 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

біометричних параметрів: внесенню в них біометричних даних щодо розпізнавання за обличчям, відбитками пальців і райдужною оболонкою ока. PIV-cards із можливістю верифікації особистості повинні стати основним інструментом аутентифікації повноважень для доступу до послуг, мереж і баз даних інформаційних систем.

За інформацією чиновників міністерства до кінця 2013 року підрядник робіт повинен буде замінити 161924 персональних ідентифікаційних карт, які призначені для верифікації особистості (PIV-карти), а до кінця 2014 року – ще 116172 документа. Виконувач робіт також повинен встановити приблизно 300 терміналів системи управління контролю за доступом загалом не менш, ніж для 300 тисяч користувачів. Термінали будуть розташовувати і за межами США[1].

Весною 2007 року влада американського штату Вашингтон і Міністерство національної безпеки США (DHS) домовилися реалізувати пілотний проект біометричних водійських прав. Ці документи планується також використовувати для підтвердження американського громадянства у випадках, коли власник біометричних прав повертатиметься в країну із зарубіжних поїздок.

Як стверджують представники DHS, плата за новий комбінований документ буде не набагато вищою, ніж за звичайні водійські права, які отримували до цього часу жителі штату Вашингтон. Водночас застосування біометричних технологій дозволить забезпечити цим документам практично такий же рівень захисту, як і в американських закордонних паспортах, що, своєю чергою, надасть змогу засвідчувати за допомогою біометричних водійських документів громадянство США, особу власника документа та його місце проживання. Із упровадженням цього проекту Міністерство національної безпеки пов'язує надії на реалізацію на території Сполучених Штатів Америки федеральної програми «Real ID», яка в перспективі передбачає повний перехід на біометричні водійські права та використання цих документів під час проходження процедури прикордонного контролю[2].

Із 15 серпня 2012 року в США почали видавати тимчасові дозволи на роботу молоді із числа нелегальних іммігрантів. Таке рішення було ухвалено в рамках нової міграційної політики, про яку президент Сполучених Штатів Америки Барак Обама оголосив у червні 2012 року, скасувавши водночас депортацію як захід проти нелегалів. Правда, йдеться тільки про молодих людей віком до 30 років, які приїхали в США, коли їм ще не було 16-ти та прожили в країні мінімум 5 років, а також навчалися в школі або відслужили в армії. Є ще одна дуже важлива умова: іммігранти не повинні мати судимостей, зокрема навіть і за дрібні правопорушення[3].

Розглянемо впровадження паспортно-візових документів другого покоління у нашого північного сусіда – Російської Федерації (РФ). Діяльність з впровадження документів із біометричними даними проводиться в Росії з 2005 року.

У січні 2013 року Президент РФ Володимир Путін підписав указ про видачу з 1 липня 2013 року громадянам Росії закордонних паспортів, які містять додаткову біометричну інформацію: зображення папілярних візерунків двох пальців рук. Участь

[1] Биометрические идентификационные карты в США обрели второе дыхание // Экспертный центр электронного государства. – 2013. – 23 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Водительские права станут биометрическими и заменят паспорта? // BIOMETRICS.RU. – 2007. – 20 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

[3] Американские власти проведут биометрическую идентификацию нелегальных гастарбайтеров // Visa4.ru. – 2012. – 16 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

у цьому проекті беруть територіальні органи Федеральної міграційної служби (ФМС) Москви, Московської області, Санкт-Петербурга та Ленінградської області[1].

Заплановано, що громадянам інших територій Росії закордонні біометричні паспорти другого покоління почнуть видавати з 1 січня 2015 року, а у дипломатичних представництвах і консульських установах РФ – у міру їх оснащення відповідними програмно-технічними засобами, але не пізніше 1 січня 2016 року. Згідно із існуючим законопроектом, паспорти з відбитками пальців зможуть одержувати громадяни РФ, яким виповнилось 12 років.

Відбитки будуть зберігатися в електронному носії інформації паспорта і це дозволить забезпечити максимальний рівень захисту документа[2].

Наведемо перелік інших персональних даних, які також вносяться у чіп біометричного закордонного паспорта Росії другого покоління: номер документа, прізвище та ім'я власника, стать, громадянство, дата народження, а також кольорове фото власника паспорта. Підкреслимо, що, відповідно до офіційного сайту ФМС Росії, персональні дані, які отримуються внаслідок сканування папілярних візерунків двох пальців рук громадянина Росії, зберігаються тільки у мікрочіпі паспорта, всі дублікати біометричної інформації після видачі документа знищуються і жодні бази даних створюватися не будуть[3].

У вересні 2013 року на засіданні урядової комісії з використання інформаційних технологій для поліпшення якості життя й умов ведення підприємницької діяльності прем'єр-міністр Росії Дмитро Медведєв заявив, що внутрішні паспорти росіян теж можуть стати біометричними. «Мова йде про заміну старих паперових паспортів на пластикові картки з електронним носієм інформації. Підготовлений проект відповідного федерального закону. Тільки що я затвердив концепцію введення посвідчення особистості та план заходів щодо її реалізації», – сказав на засіданні Д. Медведєв. «Все, що передбачається зробити, розраховане на період до 1 січня 2030 року, але вже сьогодні потрібно максимально відпрацювати організаційну схему і питання міжвідомчої взаємодії, та, що особливо важливо, просто провести нормальну роз'яснювальну роботу з людьми», – додав глава російського уряду[4].

Що стосується нашої держави, то у 2004 році, коли Україна підписала та ратифікувала низку міжнародних угод із боротьби з тероризмом і незаконною міграцією, вона була першою країною з Співдружності Незалежних Держав, яка була найліпше підготовлена на тоді до реалізації програми щодо впровадження біометричного закордонного паспорта першого покоління. Проте тоді масове виробництво цих документів так і не стартувало, хоча фахівці з ЄДАПС на кінець 2004 року змогли розробити паспортний документ нового покоління, який був визнаний ООН і ОБСЄ одним із найзахищеніших у світі на тоді і таким, що повністю відповідав міжнародним вимогам ІСАО.

Абревіатура «ЄДАПС» розшифровується як єдина державна автоматизована паспортна система. В кінці 2007 року це об'єднання включало дев'ять українських підприємств сучасних інформаційних технологій різних форм власності: СП «Голографія»,

[1] Владимир Путин подписал указ о биометрических паспортах нового поколения // РИА Новости. – 2013. – 9 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрические паспорта с отпечатками пальцев: новые подробности // РИА Новости. – 2013. – 2 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] ФМС: внесение сведений об отпечатках пальцев в чипы биометрических паспортов повысит защищенность этих документов // ФМС России. – 2013. – 5 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Внутренние паспорта россиян тоже могут стать биометрическими // Взгляд.ру. – 2013. – 20 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

компанії «VTI» і «Поллі-Сервіс», підприємство «Знак», поліграфічний комбінату «Зоря», «Комерційний індустріальний банк», ДП «Державний центр персоналізації документів», фірма «З-Т» і корпорація «Інком»[1].

Державний проект про запровадження біометричних паспортів першого покоління зміг стартувати в Україні лише з середини 2007 року. Його практична реалізація стала можливою після ухвалення в тому ж році низки законодавчих і нормативно-правових актів: відповідних ухвал Верховної Ради та Кабінету Міністрів, указу Президента України. Новий закордонний паспорт, зразок якого був затверджений усіма основними державними інститутами та схвалений відповідними міжнародними організаціями, був запущений у серійне виробництво з 27 червня 2007 року. Такі закордонні паспорти видаються впродовж 7 років, а запроваджувати на практиці біометричні паспорти другого покоління в Україні поки що не розпочали.

В українському закордонному паспорті першого покоління були реалізовані всі вимоги щодо підвищення захисних функцій документа, які були рекомендовані Міжнародною організацією цивільної авіації (ICAO, Doc 9303/3), і він у повному обсязі відповідав положенням Організації міжнародних стандартів. У цей документ вносяться такі дані: код держави, номер паспорта, прізвище, ім'я, громадянство, дата народження, стать, місце народження, персональний код власника паспорта, дата видачі та найменування органу, що видав паспорт, дата завершення терміну дії паспорта, а також місце для відтворення підпису пред'явника паспорта. Мікрочіп умонтований в останню сторінку обкладинки паспорта.

Головна особливість закордонного українського паспорта з чіпом – машинозчитувальна сторінка, що виготовлена з багатошарового полімерного матеріалу – полікарбонату, на яку наноситься зображення обличчя власника документа, його підпис і основні відомості про нього. Ці ж дані наносяться і на спеціальну машинозчитувану смугу, що розташована на полікарбонатній сторінці. Але є і певна родзинка, своєрідне ноу-хау – дублювання фотографії власника, яку можна побачити тільки під час розгляду сторінки даних проти світла. Зовнішній вигляд кожної зі сторінок паспорта не повторюється, на них зображені державна символіка України та традиційні орнаментні мотиви та композиції, які характерні українській народній творчості кожного регіону.

У новому паспорті серія і номер наносяться шляхом перфорації. Особливість перфораційних отворів – їх конусоподібність. Це отвори, що мають певний кут нахилу та нанесені на спеціальних верстатах. Паспорт має загалом 25 рівнів захисту, що на вісім ступенів перевищує захищеність української гривні у 2007 році. За визнанням фахівців ICAO, це ставить його в один ряд із п'ятьма найліпшими зразками паспортів у світі за рівнем захисту від підробок. За параметром співвідношення «ціна-якість» український «електронний» закордонний паспорт також є одним із найліпших документів у світі[2].

Нині викликає занепокоєння той факт, що Україна, як і 189 інших держав-членів ICAO, свого часу взяла на себе зобов'язання до 1 квітня 2010 року забезпечити перехід на видачу своїм громадянам електронних документів другого покоління, в яких у імплантований чіп серед обов'язкових даних повинна записуватися і суто біометрична інформація про власника. Особливо актуальне своєчасне виконання цієї вимоги в світлі необхідності

[1] «ЕДАПС» и Инком готовы создать в Украине электронное государство // Багнет. – 2007. – 17 октября. [Электронный ресурс]. – Режим доступа: http://www.bagnet.org/news/summaries/ukraine/...

[2] Плаксина С. Невыездной загранпаспорт / С. Плаксина // Эксперт Украина. – 2007. – № 29 (126). – 23 июля. [Электронный ресурс]. – Режим доступа: http://www.expert.ru/printissues/ukraine/…

спрощення візового режиму з Європейськими країнами та США. Адже відомо, що безвізовий режим 37 країн із США став можливим тільки за умови наявності у в'їжджаючих біометричних паспортів другого покоління. І ця вимога до України є однією з головних предумов на переговорах щодо безвізового режиму, що висуває Європейський Союз, оскільки у ЄС є плани щодо створення спрощеного режиму проходження прикордонних постів для осіб із біометричними паспортами[1].

За твердженням наукового директора Інституту євроатлантичного співробітництва Олександра Сушка «Україна – зараз єдина країна Європи, яка ще не видає біометричних паспортів». І останній строк для української держави – 1 січня 2015 року. До цієї дати треба упорядкувати законадовство і налагодити, відповідно до зобов'язань перед ОБСЄ, випуск паспортно-візових документів нового покоління, які б містили у електронному вигляді, крім зображення обличчя, ще і відбитки пальців.

Технології виробництва біометричних паспортів другого покоління й електронних ідентифікаційних карт має консорціум «ЄДАПС». Ця компанія вже виконувала замовлення щодо виготовлення електронних паспортів та відповідних ID-карт для співробітників Інтерполу (INTERPOL)[2].

20 листопада 2012 року парламент України ухвалив закон «Про єдиний державний демографічний реєстр», який передбачає впровадження електронних документів для громадян країни. Метою ухвалення закону є впровадження загальноприйнятої європейської практики з створення й забезпечення функціонування реєстру населення. Воно спрямоване на виконання Україною своїх зобов'язань перед Європейським співтовариством щодо забезпечення в державі обороту документів з електронним носієм інформації.

Законом визначається, що єдиний державний демографічний реєстр – це електронна інформаційно-телекомунікаційна система, призначена для зберігання, обробки та використання інформації про особу. До реєстру мають вносити таку інформацію про особу: прізвище та ім'я, дата народження/смерті, місце народження, стать, дата внесення інформації про особу до реєстру, відомості про батьків, опікунів та інших представників, дані про громадянство або його відсутність, реквізити всіх документів, виданих особі, зразок підпису, фотографія особи.

Відповідно до вимог закону, на біометричну основу мають перевести паспорт громадянина України (він буде виготовлятися у вигляді ID-карти), закордонний паспорт, права водія, а також низку інших документів. У них буде вмонтований чіп із записаними в нього відомостями власника[3].

Відповідно до закону, інформація Єдиного державного демографічного реєстру є конфіденційною, а її нерозголошення гарантується державою.

13 березня 2013 року Кабінет Міністрів України своєю постановою № 185 «Деякі питання виконання закону України «Про Єдиний державний демографічний реєстр

[1] Самсоненко С. Евросоюз ожидает от Украины внедрения электронных документов / С. Самсоненко // From-ua.com. – 2008. – декабрь. [Электронный ресурс]. – Режим доступа: http://www.from-ua.com/technology/; Евросоюз обещает упростить прохождение пограничного контроля для россиян с биометрическими паспортами // RATA-news. – 2009. – 24 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Монина Лиза. Биометрическое окно в Европу / Л. Монина // From-ua.com. – 2012. – 17 сентября. [Электронный ресурс]. – Режим доступа: http://www.from-ua.com/voice/...

[3] Украина. Верховная Рада одобрила введение биометрических паспортов // РИА Новости Украина. – 2012. – 3 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...; Украина. Закон о биометрических паспортах подписан президентом // Lenta.ru. – 2012. – 30 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

і документах, які підтверджують громадянство України, засвідчують особистість або її спеціальний статус» затвердив єдині зразки бланків документів, що засвідчують особистість, підтверджують громадянство України або спеціальний статус.

Незважаючи на цю постанову Кабміну і той факт, що закон набув чинності ще 6 грудня 2012 року, виявилося, що органи влади української держави станом на 01.04.2014 року не готові розпочати видачу документів нового зразка. В історії запровадження біометричних паспортів обох поколінь в Україні це не перший випадок зриву запланованих на державному рівні програм із запровадження біометричних паспортних документів нового зразка. Причому в усіх випадках це сталося внаслідок боротьби за держзамовлення в сфері виробництва документів.

Останній раз така подія трапилася у 2013 році. Державна міграційна служба (ДМС) оголосила, що консорціум «Єдина державна автоматизована паспортна система» (ЄДАПС) виграв конкурс на виробництво біометричних документів. Однак Кабінет міністрів анулював результати конкурсу, визнавши, що його умови були сформовані для перемоги ЄДАПС.

8 липня 2013 року у ДМС визнали, що уряд зажадав вивести з консорціуму виробництво всіх документів суворої підзвітності як тих, що випускалися на тоді, так і майбутніх – біометричних.

Автори посібника не мають наміру описувати всі нюанси боротьби за державне замовлення в сфері виробництва документів, що засвідчують особистість громадянина України. Поки що «заручниками» залишаються пересічні мешканці України, які не можуть отримати закордонні біометричні паспорти і, як наслідок, відтерміновуються терміни на встановлення безвізового режиму з країнами Шенгену.

Про це свідчить схвалення на початку березня 2014 року депутатами Європарламенту законопроекту, згідно з яким громадянинам Молдови, які мають біометричні паспорти другого покоління, надається право на в'їзд до країн Шенгенської зони на строк 90 діб без віз[1].

В. о. міністра закордонних справ України Андрій Дещиця вважає можливим отримати безвізовий режим із Євросоюзом до кінця 2014 року. Але для цього необхідно терміново ухвалити декілька законів і підвідомчих актів, які передбачали введення біометричних паспортів із наявністю в них зображень відбитків пальців у електронному вигляді та відповідний контроль на кордонах[2].

Підсумовуючи тему закордонних електронних або біометричних паспортів, узагальнимо основні переваги цих документів над паспортами старого взірця:

– відповідність світовим стандартам щодо документів, які засвідчують особистість;

– усі особисті дані власника біометричного закордонного паспорта захищені спеціальним підписом і зашифровані криптографічними засобами відповідно до вимог ІСАО, так що підробити такий документ практично неможливо;

– наявність біометричного закордонного паспорта дозволяє проходити паспортний контроль на кордоні набагато швидше, оскільки процедура зчитування інформації спеціальними біометричними сканерами відбувається миттєво. Зараз у багатьох країнах для проходження прикордонного контролю створені спеціальні коридори для громадян різних країн з електронними паспортами, черга в яких рухається дуже швидко;

[1] Депутаты Европарламента разрешили безвизовый въезд гражданам Молдавии с биометрическими паспортами // MOLDOVAinform. – 2014. – 4 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] ЕС может отменить визы для украинцев до конца года // Mail.ru. – 2014. – 20 марта. [Электронный ресурс]. – Режим доступа: http://news.mail.ru/inworld/...

– обкладинки закордонних паспортів виробляються зі спеціального стійкого матеріалу, що дозволяє доволі довго зберігати презентабельний зовнішній вигляд документа;

– виконання безальтернативної вимоги щодо можливості підписання угод про безвізовий режим між країнами;

– можливість запровадження біометричних паспортів із терміном дії до 10 років;

– одна з складових заходів у боротьбі з незаконною міграцією, тероризмом, транснаціональною злочинностю тощо.

Стисло розглянемо існуючу практику видачі віз для в'їзду в США, Великобританію та країни Шенгену.

Ще з 2004 року в Сполучених Штатах Америки почали втілювати в життя програму «US-VISIT», яка передбачала, зокрема, зняття відбитків двох вказівних пальців з рук у всіх іноземних громадян, які прибувають до країни. З жовтня 2004 року у всіх американських візах почали розміщувати біометричну інформацію щодо їх власників. Біометричний контроль став необхідною процедурою для тих, хто в'їжджає на територію Сполучених Штатів Америки, а згодом і для тих, хто виїжджає з неї, а їх біометричні параметри (зокрема і для осіб, яким відмовлено у видачі візи) підлягали обов'язковому внесенню до банку даних інформаційної системи «IDENT», яка створена та підтримується Міністерством національної безпеки (Department of Homeland Security /DHS/).

Із листопада 2007 року всі посольства і консульства США почали здійснювати процедуру зняття відбитків усіх 10 пальців у бажаючих отримати візу. Ця процедура є складовою «Програми уряду Сполучених Штатів зі зняття біометричних даних» і за офіційною версією спрямована на підвищення захищеності американських віз, а також на спрощення процедури в'їзду до Сполучених Штатів Америки власників біометричних віз. У січні 2009 року Департамент національної безпеки США оголосив про завершення загалом модернізації системи біометричної ідентифікації претендентів американських віз. За повідомленнями січневого прес-релізу Міністерства національної безпеки США, на оновлену десятипальцьову технологію біометричного контролю на початок 2009 року завершили перехід «всі основні пункти контролю в'їзду в США.

Як наголошується в прес-релізі Department of Homeland Security, збір інформації про відбитки всіх пальців рук збільшує точність розпізнавання особистості претендента на візу та зменшує ймовірність того, що біометрична система ухвалить помилкове рішення під час здійснення процедури ідентифікації.

Крім того, значно розширилися можливості перевірки претендента за біометричними базами даних, які сформовані ФБР, Міністерством оборони та іншими спеціальними структурами США і які містять інформацію про відбитки пальців, вилучених із місць злочинів або подій. Згадані відомства проводять збір біометричних даних щодо осіб, які становлять загрозу національній безпеці Сполучених Штатів Америки або є «небажаними гостями», і тепер здобувачів віз буде простіше перевірити на можливу причетність до терористичної або іншої незаконної діяльності.

Представники DHS США у цьому прес-релізі також підкреслили, що реалізація програми оновлення системи біометричної ідентифікації претендентів американських віз та її успішна діяльність є результатом ефективної співпраці Департаменту національної безпеки США, американського Державного Департаменту, ФБР і Пентагону[1].

[1] Завершено обновление системы биометрической идентификации соискателей американских виз // BIOMETRICS.RU. – 2009. – 20 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

2009 року директор програми «US-VISIT» Роберт Мокні (Robert Mocny) повідомив, що в рамках програми «US-VISIT» щорічно перевіряється понад 23 млн відбитків.

У Сполучених Штатах Америки діє Програма безвізового в'їзду (US Visa Waiver Program). Скористатися цим правом можуть тільки власники біометричних паспортів, які пройшли попередню процедуру реєстрації в Електронній системі авторизації в'їзду (ESTA). 2012 року Швейцарія стала однією з 37 країн, які беруть участь в американській Програмі безвізового в'їзду. За відомостями швейцарського порталу www.swissinfo.ch, США пред'являють низку умов країнам, які беруть участь у Програмі. По-перше, американська сторона вимагає надавати біометричні дані – відбитки всіх 10-ти пальців і ДНК всіх потенційних візитерів у рамках угоди про запобігання та боротьбу зі злочинами (Agreement to Prevent and Combat Serious Crime /PCSC/). Друга умова – обмінюватися таємною інформацією стосовно терористів і осіб, які підозрюються у терористичних діях. Слід зазначити, що надавати Сполученим Штатам Америки потрібно інформацію не про всіх злочинців, а тільки про тих, які вчинили серйозні правопорушення або засуджені до трьох і більше років позбавлення волі[1].

Загалом із введенням у дію програми «US-VISIT» всі іноземці, які намагаються одержати в'їзну візу або в'їжджають на територію США, а також усі пасажири американських авіакомпаній, зокрема й на внутрішніх рейсах, в обов'язковому порядку проходять перевірку в Центрі виявлення терористів (Terrorist Screening Center), який діє в складі Федерального бюро розслідувань (ФБР /FBI/). Перевірку відомостей щодо тих осіб, які в'їжджають, та авіапасажирів також здійснюють інші спеціальні служби (імміграційна та митна служба, поліція тощо), які виявляють небезпечних і небажаних за їх висновками осіб (персон non-grata – особистостей, що внесені в спеціальні «чорні» списки). Серйозне підвищення рівня безпеки стосувалося не тільки прикордонних пунктів пропуску, аеропортів і морських портів, але й інших важливих об'єктів інфраструктури США[2].

Тайвань із 1 листопада 2012 року став 37-ю і поки що останньою країною, чиї громадяни, які є власниками біометричних паспортів, отримали право безвізового в'їзду до США.

2011 року за програмою US Visa Waiver Program відвідали Америку громадяни інших країн 18,3 млн раз, що становило понад 60% від загальної кількості візитерів[3].

Колекція біометричних даних, зібраних у рамках виконання програми «US-VISIT», налічувала на початок 2008 року відомості про відбитки пальців понад 90 млн осіб, які повинні зберігатися впродовж 70 років. За повідомленням служби внутрішньої безпеки Сполучених Штатів Америки у всьому світі 211 консульств і візових відділів США щорічно розглядають приблизно 7 млн заявок на видачу віз, із яких 5 млн задовольняються, а 2 млн іноземних громадян отримують відмовне рішення. Щорічно кордони США перетинають понад 440 млн чоловік.

За даними DHS, за час дії програми «US VISIT» у 2004–2008 роках були припинені спроби одержання американської візи з боку 2400 громадян закордонних держав, яких відповідні американські органи вважають злочинцями або такими, що становлять

[1] Швейцарские граждане, владеющие биометрическими паспортами, смогут въезжать в США без виз // Visa4.ru. – 2012. – 29 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news...

[2] Шестилетка безопасности. Реформы // Washprofile.org/ru. – 2007. – 13 сентября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

[3] Обладатели тайваньских биометрических паспортов будут въезжать в США без виз // BIOMETRICS.RU. – 2012. – 4 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

загрозу національній безпеці. Зокрема, у лютому 2008 року вдалося «вирахувати» двох осіб, які підозрювались у терористичній діяльності, оскільки відбитки їх пальців раніше були виявлені на саморобному вибуховому пристрої[1].

Візова політика постійно вдосконалюється з метою забезпечення належного рівня безпеки приймаючої країни. У Міністерстві внутрішньої безпеки США (Department of Homeland Security) побоюються, що терористи зможуть проникнути в США під виглядом біженців або скористатися іншими каналами, наприклад, американською безвізовою програмою.

Тому, починаючи з 12 січня 2009 року, особи, які здійснюють поїздки в Сполучені Штати Америки за безвізовою програмою, використовують нову процедуру отримання дозволів на поїздки в режимі on-line. Нова Електронна система дозволів на поїздки (ESTA) вимагає заповнення всіма громадянами країн, що входять в американську безвізову програму, перед посадкою на літак, який відправляється в США, або судно заповнення спеціальної електронної анкети, розміщеної в Інтернеті (https://esta.cbp.dhs.gov/).

Потрібно дати відповіді на питання про кримінальне минуле, інфекційні захворювання, попередні випадки відмови видачі візи або депортації, а також повідомити основні біографічно-документальні відомості: прізвище, ім'я, дату народження та інші паспортні дані. Після першого представлення форми ESTA у наступних випадках можна буде легко вносити за допомогою Інтернету зміни до адреси перебування та маршруту поїздки.

Нова процедура потрібна для визначення того, чи не становить поїздка іноземця до Сполучених Штатів Америки загрозу її правопорядку та безпеці. Офіційні представники американської влади попереджають, що після того, як програма ESTA стане обов'язковою, пасажирам-іноземцям, які не отримали попереднього дозволу, може бути відмовлено у посадці на борт судна. Для захисту персональної інформації, що передається електронною системою дозволів на поїздки, відповідні служби США використовують новітні технології[2].

Усі розвинуті країни світу, зокрема Австралія, Канада, Сполучене Королівство Великобританія, країни Шенгенської зони, Японія та низка інших вже запровадили національні біометричні системи, які є аналогом «US-VISIT». Існуючі нині біометричні візи, що надають право на в'їзд до Британії, почали запроваджуватися ще у 2006 році. Вони в обов'язковому порядку містять оцифровану фотографію та відомості про відбитки пальців власника[3].

За час дії британської системи біометричних віз до початку 2008 року були отримані дані про відбитки пальців понад мільйона осіб. Серед аплікантів, які звернулися за отриманням британської візи у 2006–2007 роках, ще на етапі розгляду поданих документів завдяки біометричній ідентифікації встановлено близько 10 тис. чоловік, які раніше порушували імміграційне законодавство Британії або порядок подачі заяв на отримання притулку в Сполученому Королівстві[4].

---

[1] Гуру информационной безопасности критикует американскую программу US VISIT // BIOMETRICS.RU. – 2008. – 11 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Система биометрических идентификационных карт в Сингапуре охватит новые социальные группы // Государственный департамент США. – 2008. – 19 июня. [Электронный ресурс]. – Режим доступа: http://usinfo.state.gov/xarchives/...

[3] Введение биометрических виз помогло задержать четыре тысячи фальшивых «беженцев» // BIOMETRICS.RU. – 2007. – 27 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Британская система биометрических виз продолжает развиваться // BIOMETRICS.RU. – 2008. – 23 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

За повідомленням сайта об'єднаного директорату двох британських відомств – МВС і Міністерства закордонних справ і справ Співдружності (скорочена назва сайту «Ukvisas»), у базу даних директорату, що безперервно функціонує, кожні тридцять секунд вносяться персональні відомості щодо кожного нового здобувача британської візи – дані про 10 відбитків пальців рук і оцифрована фотографія. До квітня 2008 року система збору біометричних даних претендентів на отримання британських віз охопила 135 держав світу, а в 53 зарубіжних країнах діяли 111 центрів із видачі віз (усього 193 візових центри). З липня 2007 року банк індивідуальних даних претендентів на отримання віз щомісячно збільшується на сто тисяч «десятипальцьових наборів відбитків»[1].

25 червня 2009 року Європейська рада схвалила єдині для всіх країн Шенгенської угоди правила видачі короткострокових віз. Нові правила, які зведені у так званий «Візовий кодекс» (Visa Code), у більшості шенгенських країн набули чинності до середини 2010 року.

У листопаді 2011 року в 25 країнах Шенгенської угоди була запущена «Візова інформаційна система» («Visa-Information system» /VIS/). За її допомогою пришвидшився процес обробки заяв на одержання візи завдяки використанню оцифрованих відбитків пальців і фотографій, а також забезпеченню швидкого обміну даними про короткострокові візи (термін 90 діб) між усіма країнами Шенгенської зони. З цього часу шенгенську візу можна одержати тільки після проходження процедури дактилоскопії та цифрового фотографування.

Як вважають представники ЄС, перевірка здобувачів віз за відбитками пальців дозволила виключити практику «оренди паспортів», яка була дуже поширеною серед громадян азіатських країн. За 2 тисячі євро вони могли «орендувати» паспорт із багаторазовою шенгенською візою та в'їхати з ним до країн шенгенської зони, а потім відправити його поштою дійсному власнику[2].

Запровадження візової інформаційної системи VIS дозволило налагодити швидкісний обмін візовими даними між всіма державами – членами Шенгенської угоди. Крім того, «Visa-Information system» спростила подачу документів на відкриття візи, проходження процедури прикордонного контролю під час в'їзду в зону Шенгенської угоди та підвищила безпеку самого заявника.

За першої подачі клопотання на одержання короткострокової візи з метою збору потрібних біометричних даних (відбитків десяти пальців і фотографії) необхідна особиста явка здобувача візи у посольство або консульство держави, яка є членом Шенгену. За наступної подачі клопотання протягом п'яти років дані заявника, що зберігаються в базі даних системи VIS, можуть бути використані повторно[3].

Станом на 28 вересня 2012 року в базі даних Європейської «Візової інформаційної системи», яка використовується під час оформлення біометричних віз, були накопичені відомості стосовно одного мільйона громадян, які зверталися за дозволом на в'їзд у Шенгенську зону[4].

---

[1] Первые итоги действия британской системы биометрических виз // BIOMETRICS.RU. – 2007. – 20 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Суд ЕС признал законным внесение в биометрические паспорта сведений об отпечатках пальцев // РАПСИ. – 2013. – 18 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Шенгенские визы станут биометрическими для граждан Узбекистана // CA-News. – 2013. – 11 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Шенгенские визы станут для граждан ОАЭ биометрическими // BIOMETRICS.RU. – 2012. – 28 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news...

Із 1 грудня 2012 року в Європейському Союзі з'явилася нова структура, у веденні котрої серед іншого перебувають і візові питання. Назва цього адміністративного органу – «Агентство ЄС з контролю за великомасштабними ІТ-системами». Одним із завдань цього органу є створення так званих «гармонізованих списків документів», які необхідні під час подання заяви на видачу візи. Головна мета цієї установи – формування уніфікованої бази даних, яка дозволить відповідні документи й отримані біометричні візи однозначно закріплювати за конкретною людиною. Діяльність уніфікованої БД розпочалася з 14 січня 2013 року[1].

Нині у кожному з посольств або консульств Євросоюза, де видаються шенгенські візи, використовують декілька видів комп'ютерних систем для проведення перевірки аплікаанта перед видачею йому візи – Інтерполу, власної служби безпеки країни та «Агентства ЄС з контролю за великомасштабними ІТ-системами», в яких може бути файл із відміткою про протиправні дії аплікаанта (людини, яка звернулася з проханням про видачу візи). Як відомо, система Інтерполу поширена у всьому світі, а власні системи всіх шенгенських країн об'єднані в єдину мережу, комп'ютерний центр якої є в Страсбурзі. Тому особа, яка вчинила протизаконні дії у будь-якій країні, автоматично «закриває» собі дорогу у всі держави, що підписали угоду[2].

Оскільки в українських ЗМІ та заявах офіційних осіб доволі жваво висвітлюється питання щодо можливості досягнення угоди з Європейським Союзом про встановлення для громадян України безвізового режиму, то наведемо перелік основних вимог, які необхідно виконати будь-якій державі для отримання можливості безвізового в'їзду до країн ЄС.

За заявою ще у 2008 році віце-президента Єврокомісії Жака Барро, який відповідав за питання юстиції, свободи та безпеки в Євросоюзі, будь-якій державі для отримання безвізового режиму необхідно досягти певного рівня в таких сферах:

– забезпечення безпеки особистих документів від підробок і фальсифікацій (тобто наявність біометричних паспортів другого покоління);

– відповідати світовим стандартам у боротьбі з нелегальною міграцією;

– забезпечення національної безпеки та внутрішнього правопорядоку;

– відсутності проблем у зовнішніх відносинах із членами світової спільноти.

Відповідаючи на запитання про те, чи вимагатиме Єврокомісія (ЄК) введення в Україні паспортів із біометричними даними, віце-президент ЄК відповів, що введення паспортних документів нового покоління серйозно б полегшило підготовку переходу до безвізового режиму[3].

За словами ще одного з високопосадовців Єврокомісії Гюнтера Ферхойгена, питання безвізового режиму між Україною й Європейським Союзом є технічним, а не політичним. Він уточнив, що повна лібералізація візового режиму з Євросоюзом може відбутися тільки тоді, коли певні вимоги безпеки будуть виконані Україною: «... це залежить від того, наскільки швидко Україна зможе виконати європейські стандарти безпеки». Насамперед йдеться про співпрацю у прикордонних пунктах і застосування відповідної системи технічного контролю. Він також зазначив, що Єврокомісія готова надати Україні технічну допомогу для запровадження відповідних технічних стандартів безпеки на кордоні[4].

---

[1] Европа готовится к введению биометрических виз // Travel.ru. – 2012. – 27 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Как получить шенгенскую визу? // From-ua.com. – 2009. [Электронный ресурс]. – Режим доступа: http://www.from-ua.com/travel/...

[3] Евросоюз рассматривает возможность введения безвизового режима для граждан Украины // Сегодня. – 2008. – 30 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document...

[4] Питання безвізового режиму між Україною і ЄС технічне, а не політичне. – 2009. – 16 лютого. [Електронний ресурс]. – Режим доступу: http://www.golosua.com/suspilstvo/...

Розділ 12

ДЕРЖАВНІ ТА МІЖДЕРЖАВНІ БІОМЕТРИЧНІ БАЗИ ДАНИХ, ЩО ІСНУЮТЬ У СВІТІ

Формування національних інформаційно-біометричних систем паспортів і віз, а в перспективі можливо і глобальної міжнародної системи – ці заходи повинні боротися з незаконною міграцією та міжнародною злочинністю, контролювати потоки законної міграції та сприяти боротьбі з тероризмом. Водночас паспортно-візові документи нового покоління дозволяють їхнім власникам перетинати кордони за спрощеними процедурами, а за наявності спеціальних угод між низкою країн – без оформлення візових документів.

Це вимагає створення національних баз даних (БД), що повинні зберігати вичерпну і достовірну персоналізовану біометричну інформацію про громадян своїх країн і візитерів, створення відповідних захищених каналів зв'язку для обміну за домовленостями між державами відповідними даними.

Деякі експерти вважають, що в перспективі може виникнути питання про створення і глобальної міжнародної БД. Такі бази даних і системи управління ними повинні мати безпрецедентні характеристики за загальною кількістю даних, що зберігаються, можливостями швидкісного пошуку та вибору інформації, продуктивністю, масштабністю, керованістю та, що особливо важливо, забезпечувати необхідний рівень захисту і безпечності зберігання персональних відомостей.

Сучасні біометричні технології і бази даних перевершили дактилоскопічні автоматизовані системи, коли замість громіздких поліцейських програмно-обчислювальних комплексів з'явилися нові технічні засоби – комп'ютерно-телекомунікаційні технології, дактилоскопічні сканери, а можливості інформаційно-комп'ютерної техніки дозволили здійснювати ідентифікацію осіб, які перевіряються, у режимі реального часу. З інформаційного погляду нині системи біометричної ідентифікації є другим поколінням систем безпеки, що здійснюють ідентифікацію користувачів[1].

Програмно-апаратні комплекси, на яких розгорнуті або розгортаються такі інформаційні системи (інколи їх ще називають «серверами додатків»), в обов'язковому порядку повинні бути сформовані за уніфікованими принципами з використанням стандартів Міжнародної організації зі стандартизації (International Organization for Standardization /ISO – ICO/) для можливості інтеграції з інформаційними системами інших країн, нехтуючи про необхідність сумісності з наявними базами даних відповідних національних державних структур. В Україні це такі структури, як: Служба безпеки України (СБУ), органи внутрішніх справ (ОВС), Міністерство закордонних справ (МЗС), прикордонна та митна служби й інші.

[1] Минкин В. Биометрия. От идентификации личности к идентификации мыслей / В. Минкин // Элсис. – 2008. [Электронный ресурс]. – Режим доступа: http://www.elsys.ru/review5.php

Великомасштабні інформаційні системи, що нині реалізуються, для зберігання й обробки біометричних даних використовують як інфраструктуру надпотужні комп'ютерно-серверні комплекси та сучасні системи управління базами даних (СУБД), які надають можливість зберігати відомості стосовно сотень мільйонів індивідуумів.

В Україні та країнах СНД існуючі версії СУБД «Oracle» ще з минулого століття використовуються в різних інформаційно-пошукових системах (ІПС) для обліку населення та виборців, у паспортних, кадастрових і реєстрових системах для зберігання й обробки даних.

Версії СУБД «Oracle» характеризуються:

1. Продуктивністю і масштабністю. Онлайновий пошук за базою даних надає можливість організувати роботу з дуже великою кількістю персональних даних і здійснювати необхідні вибірки за секунди або десятки секунд.

2. Високою доступністю. Організація роботи формується так, щоб запити на пошук необхідних відомостей могли надходити у систему цілодобово та безперервно, переважно в режимі «On-line». Для цього система обов'язково повинна мати дублюючий програмно-апаратний комплекс для підтримання можливості безперервного функціонування.

3. Можливістю забезпечення належного рівня безпеки інформації, що зберігається. Персональні відомості, що зберігаються в таких базах даних, повинні бути захищені від несанкціонованого витоку інформації, тому необхідно забезпечити їх надійну секретність і конфіденційність. Для цього застосовуються сучасні стандарти шифрування та забезпечення цілісності даних[1].

В історії людства перше рішення про створення міждержавної бази дактилоскопічних і антропометричних даних для боротьби з тероризмом і міжнародною злочинністю було ухвалено 100 років тому в червні 1914 року на всесвітньому конгресі поліції в Монте-Карло.

В Україні, як і в інших країнах СНД, багато відомств мають свої локальні бази персональних даних: МВС, Державна податкова адміністрація України (ДПАУ), СБУ, прикордонна служба, інші силові структури, Пенсійний фонд тощо. Нині багато з цих баз продовжують функціонувати в неінтегрованому вигляді, причому часто існують розбіжності між наявними даними цих баз. Така ситуація виникла внаслідок того, що немає єдиної максимально достовірної (так званої еталонної) бази ідентифікаційних даних населення України, через що кожна особистість може позиціонуватися в галузевих базах даних по-різному.

За найскромнішими підрахунками загальний обсяг накопичених у комп'ютерних банках даних інформації стосовно громадян будь-якої великої країни вимірюється в терабайтах, зміст якої характеризується високим ступенем дублювання та суперечності.

Вирішення проблеми ідентичності баз даних полягає у створенні інформаційного ресурсу – державного реєстру (регістра) населення, в якому, крім загальноприйнятих основних ідентифікаційних даних громадянина (прізвище, ім'я, по батькові, стать, дата і місце народження тощо), повинні міститися і його персональні біометричні ідентифікатори.

Саме ці параметри дозволяють однозначно встановити або підтвердити особистість громадян, організувати належну інформаційну взаємодію різних відомчих баз

[1] Данилов С. Интеграция биотехнологий с базовыми технологиями ORACLE / С. Данилов // Информационное общество. – 2005. – Вып. 2. – С. 57–65. [Электронный ресурс]. – Режим доступа: http://emag.iis.ru/arc/infosoc/emag...

даних, гарантуючи водночас повну ідентичність оброблюваних даних. Цим шляхом пішли всі розвинені країни світу (США, Великобританія, інші члени ЄС, Японія та багато інших)[1].

Біометричні бази даних (БД) державних структур за своїм призначенням можно розподілити на такі типи БД:

– систем спеціального призначення (спецслужб і правоохоронних структур);

– державних реєстрів населення, за допомогою яких проводиться видача паспортно-візових документів нового покоління (біометричних закордонних паспортів, ID-cards як внутрішніх документів громадян і державних посвідчень різного призначення);

– організації здійснення прикордонного контролю, що в багатьох випадках щільно поєднується з контролем управління за доступом на транспортних вузлах;

– контролю за доступом на режимні об'єкти;

– для організації захисту доступу до таємної та конфіденційної інформації у комп'ютерно-програмних комплексах різних державних установ;

– для надання населенню різних соціальних послуг, проведення виборів, електронне урядування тощо.

Приватні бази даних біометричних систем різного призначення створюються фінансовими організаціями (галузь, де найбільше використовується у приватному секторі біометричні технології) для проведення безпечного банкінгу, інших онлайнових платежів і рітейлу, а також багатьма компаніями з метою організації захисту доступу до конфіденційної інформації та впровадження систем контролю управління за доступом співробітників і відвідувачів, які можуть бути поєднані з автоматизованими системами обліку робочого часу працівників.

У цьому розділі посібника розглядаються біометричні системи та БД, що експлуатуються державними органами і структурами.

У XXI столітті США, Великобританія та інші розвинені світові держави поступово перетворюються на співтовариство, де жителі перебуватимуть під наглядом упродовж усього життя. Такий розвиток подій може виявитися неминучим наслідком всесвітньої боротьби з тероризмом.

Це практично підтверджено в дослідженні, виконаному ще в 2006 році на замовлення уряду Великобританії групою вчених і експертів «Surveillance Studies Network». Автори дослідження характеризують сучасне громадянське суспільство як «суспільство тотального нагляду», де передові технології широко застосовуються для спостереження та фіксації (запису) пересування людей та їх дій. Це стосується міждержавних подорожей, прихованого відеонагляду, аналізу фінансових операцій та купівельних уподобань, контролю телефонних розмов, електронного листування, використання інтернету вдома або на робочому місці. Автори доповіді ще тоді попереджали: у майбутньому контроль стане більш тотальним, причому здебільшого буде практично непомітним для звичайних громадян[2].

Але найбільше підтвердження теза «суспільства тотального нагляду» отримала у функціонуванні Програми «Prism», яка використовується в інтересах Агентства національної безпеки (National Security Agency – /NSA – АНБ/) і Федерального бюро розслідувань (FBI – ФБР) Сполучених Штатів Америки.

---

[1] Гуриев В. Восход Европы: электронные паспорта в России / В. Гуриев, Р. Насакин, К. Курбатов // Компьютерра. – 2007. – № 8. – 1 марта. [Электронный ресурс]. – Режим доступа: http://offline.computerra.ru/...

[2] Британцы под колпаком // GZT.RU. – 2006. – 8 ноября. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/...

Програма «Prism», яка функціонує з 2007 року, є першою у світі розробкою, що використовується для аналізу інформації в глобальних соціальних мережах. Таємно затверджена судом США програма «Prism» орієнтована на перехоплення закордонного трафіку зв'язку, що здебільшого проходить через сервери США, навіть за умови відправлення з одного закордонного місця в інше місце, яке розташоване за межами території США.

Дії суперпрограми «Prism» ґрунтуються на Законі про контроль над діяльністю іноземних розвідок (FISA) та Акті про захист Америки (Protect America Act /PAA/), які дозволяють здійснювати стеження за громадянами іноземних держав за межами США без санкції суду[1].

Узагалі контроль може бути необхідним і бажаним заходом, наприклад, для боротьби з терористами або небезпечними злочинцями, удосконалення систем пільг і компенсацій, охорони здоров'я, організації доступу до суспільних і приватних послуг. Нині дедалі частіше трапляються техногенні та звичайні катастрофи, безвісті зникають люди, врешті хтось когось шукає, тому потрібна ідентифікація людей, а біометричні банки даних надають неоціниму підмогу в такій роботі. У деякому сенсі це не обмеження, а суттєва необхідність.

Уже близько півсторіччя прийнято вважати, що дані в електронному форматі найстислішим способом зберігання інформації порівняно з картотечними й іншими паперовими засобами зберігання будь-яких відомостей. На початку нового тисячоліття біометрії відкрилося таке широке поле застосування тому, що завдяки досягнутим успіхам у галузі інформаційно-комп'ютерно-телекомунікаційних технологій відомості щодо біометричних ідентифікаторів практично на все населення земної кулі доволі легко можуть зберігатися у вигляді автоматизованих банків даних, які реалізовані на базі останніх досягнень у створенні сучасних суперкомп'ютерів і телекомунікаційних каналів доступу до них.

Нагадаємо, що нині одними з найнебезпечніших глобальних ризиків є незаконна міграція, тероризм і міжнародна організована злочинність. Для успішної протидії цим негативним явищам провідні світові держави ухвалюють спеціальні закони, які дозволяють спецслужбам і поліцейським органам створювати інтегровані бази даних (БД) і проводити відеозапис і моніторинг Інтернету та навіть «заглядати» в персональні банківські рахунки[2]. У США небезпідставно вважають, що тільки поєднання інновацій та практичного досвіду зі спільною кооперацією за відповідними напрямами всіх цивільних і правоохоронних структур, зокрема й на міждержавному рівні – у підсумку повинно зумовити більш ефективне ведення «війни з тероризмом».

Суттєвим заходом, який спрямований на боротьбу з зазначеними негативними явищами XXI століття, міжнародним співтовариством визнано використання досягнень сучасних біометричних технологій і, зокрема введення паспортно-візових документів нового покоління (ПВДНП). Із 1 квітня 2010 року вже в 188 країнах світу[3], які є членами Організації Об'єднаних Націй (ООН) і міжнародної організації цивільної авіації

[1] Prism – глобальная машина наблюдения: как США уничтожают свободу в мире // The Guardian, The Washington Post. – 2013. – 6 и 7 июня. [Электронный ресурс]. – Режим доступа: http://regnum.ru/news/fd-abroad/ukraina/...

[2] Cleden D. О разработке корпоративной информационной системы в английской полиции / D. Cleden // Борьба с преступностью за рубежом (по материалам зарубежной печати / пер. из журнала Police). – М.: ВИНИТИ. – 2004.

[3] Азербайджан. Биометрические паспорта будут содержать сведения об отпечатках пальцев их владельцев // ABC.AZ. – 2010. – 11 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

(International Civil Aviation Organization /ICAO – ІКАО/), вживаються заходи з впровадження ПВДНП. Біометричні паспорти та різні види національних біометричних ідентифікаційних карт (ID Cards), які мають комп'ютерний чіп із біометричними даними, перетворюють ці документи в надійне джерело унікальних відомостей для однозначної ідентифікації будь-якої особистості. Все це зумовлює необхідності формування різних баз даних громадян, осіб без громадянства й імігрантів зі всіма існуючими проблемами з зберігання та захисту зібраної інформації, доступу до неї і шляхами її використання.

Перед тим, як розпочати наведення переліку найбільш відомих у світі автоматизованих біометричних систем ідентифікації осіб нагадаємо, що експерти розділяють системи ідентифікації осіб за відбитками пальців на два класи – AFIS (Automatic Fingerprint Identification Systems – автоматична система ідентифікації за відбитками пальців) і Fingerprint. Системи AFIS застосовують правоохоронні органи та інші силові структури. Водночас використовуються зображення всіх 10 відбитків пальців. Системи Fingerprint застосовують різні «несилові» державні та комерційні організації. Власне зображення відбитків пальців у таких ідентифікаційних системах не зберігаються, а в базі даних зберігаються лише оцифровані шаблони (модулі) відбитків пальців[1].

На жаль, інформація щодо біометричних баз даних, що створені або створюються у світовій спільноті, вкрай уривчаста та розпорошена, хоча починаючи з 2007 року спостерігається «бум» публікацій у засобах масової інформації щодо використання біометричних технологій (особливо в інтернет-виданнях), зокрема про створення та запровадження в повсякденне життя найрізноманітніших біометричних систем ідентифікації або верифікації та відповідних банків даних для зберігання в електронному вигляді біометричних параметрів.

З огляду на публікації ЗМІ у XXI столітті авторами посібника проведено систематизацію зібраної інформації у розрізі використання існуючих і створення нових біометричних баз даних у різних державах і співтовариствах світу.

Невеличкий історичний екскурс щодо відомостей про біометричні бази даних розпочнемо зі Сполучених Штатів Америки (США).

Починаючи з кінця 20-х років минулого століття, Федеральне бюро розслідувань (ФБР – FBI) розробляло та випробувало різні автоматизовані системи ідентифікації за відбитками пальців. У підсумку була створена система AFIS (Automated Fingerprint Identification System) – автоматична система ідентифікації за відбитками пальців із банком даних, в якому зберігалися дактилоскопічні відтиски десяти пальців усіх індивідуумів, що були зняті у встановленому порядку. 1989 року в США було ухвалено рішення про перегляд усього дактилоскопічного процесу та розробки нової автоматизованої комп'ютерної системи, яка отримала назву інтегрованої автоматичної системи ідентифікації за відбитками пальців (Integrated AFIS – IAFIS) і основні елементи якої були запроваджені в 1999 році[2].

Після 11 вересня 2001 року американські спецслужби почали вкладати величезні кошти в збір відомостей про громадян різних країн та інтегрування цієї інформації у відповідні бази даних. Головною антитерористичною базою даних уряду США стала БД Terrorist Identities Datamart Environment (TIDE), куди надходить інформація Центрального розвідувального управління (ЦРУ), Федерального бюро розслідувань (ФБР), Агенства

[1] Мясников В. Модернизация ОПК остается несбыточной мечтой / В. Мясников // Независимое военное обозрение. – 2010. – 1 октября. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/realty/...

[2] Пахомов С. Отпечаток пальца вместо пароля / Сергей Пахомов // КомпьютерПресс. – 2004. – № 4. [Электронный ресурс]. – Режим доступа: http://www.compress.ru/Archive/...

національної безпеки (АНБ) і військової розвідки (Defense Intelligence Agency /DIA/) про терористів і осіб, які підозрюються у тероризмі або його пособництві[1].

2010 року експерти компанії «Frost & Sullivan» у своєму огляді «Біометрія в країнах Північної Америки» зробили висновок, що урядові структури США відіграють головну роль у розвитку біометричних технологій та подальшому їхньому поширенні.

На перше місце авторами доповіді були поставлені системи IDENT та IAFIS, які експлуатуються Міністерством національної безпеки (Department of Homeland Security – DHS) та Міністерством юстиції, відповідно. У першій із систем збираються й аналізуються дані про відбитки всіх 10 пальців рук громадян, які були запідозрені або викриті у порушенні імміграційного законодавства й прикордонного режиму; система IDENT пов'язана із системою IAFIS, яка використовується ФБР і має відомості про десятки мільйонів відбитків пальців. Взаємодія двох біометричних систем підвищує ефективність кожної з них: наприклад, з'являється можливість з'ясувати, чи не притягався нелегальний іммігрант до відповідальності й за кримінальні злочини, вчинені на території США.

Митне й прикордонне агентство США сформувало та використовує систему USPASS. За її допомогою пришвидшується проходження прикордонного контролю громадянами, зареєстрованими в цій системі: їх особистість надійно й швидко засвідчує за допомогою біометричних технологій (ідентифікація здійснюється за геометрією кисті руки).

Національний інститут юстиції вивчає можливості ідентифікації за обличчям для встановлення особистості підозрілих суб'єктів у місцях масового скупчення людей для забезпечення безпеки пересічних громадян і ліпшої організації дій співробітників правоохоронних органів під час забезпечення громадського порядку.

Управління транспортної безпеки та берегова охорона продовжують реалізовувати програму TWIC з видачі біометричних ідентифікаційних карт працівникам морських портів. Ці урядові агентства за допомогою біометричних технологій сподіваються забезпечити ефективний контроль за фізичним доступом у режимні зони аеропортів, морських портів, інших об'єктів берегової інфраструктури та на борт кораблів.

У Державному департаменті США почала функціонувати система біометричної ідентифікації, яка забезпечує розмежування доступу до інформаційних ресурсів зовнішньополітичного відомства. Співробітники установи отримали смарт-карти, у чіпи яких внесені відомості про їх відбитки пальців. Для отримання доступу до службового комп'ютера необхідно відсканувати відбитки пальців. Одержана електронна модель відбитків порівнюється з електронним шаблоном, який зберігається у чіпі смарт-карти, і, якщо результат порівняння позитивний, то доступ ідентифікованого працівника до комп'ютера дозволяється[2].

Спеціальна комісія армії США з біометрії (Biometrics Task Force – BTF) з січня 2009 року почала експлуатувати передану автоматичну систему біометричної ідентифікації нового покоління (Next Generation Automated Biometric Identification System – NG-ABIS). Зважаючи на той факт, що основним замовником і експлуатантом системи є Міністерство оборони (Department of Defense – Dod), назва системи була змінена на Dod ABIS.

---

[1] Бороган Ирина. Тотальный контроль: западный опыт / Ирина Бороган // Ежедневный журнал. – 2009. – 1 декабря. [Электронный ресурс]. – Режим доступа: http://www.agentura.ru/press/about/jointprojects/...

[2] Правительственные органы США расширяют использование биометрических технологий // BIOMETRICS.RU. – 2010. – 21 мая. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Зміни відбулися не тільки в термінології. Dod ABIS виконує для різних структур Пентагону функції основного офіційного джерела інформації щодо біометричних ідентифікаторів осіб, які їх цікавлять.

Це стало можливим через суттєве розширення функцій біометричної системи Dod Automated Biometric Identification System порівняно з попередньою, тобто система стала мультибіометричною.

Військовослужбовці й інші співробітники Міністерства оборони можуть звертатися до Dod ABIS з різних частин усього світу; дані, що зберігаються в БД цієї системи, також доступні іншим силовим структурам США.

Ще одна суттєва відмінність Department of Defense Dod Automated Biometric Identification System – підвищення ролі штучного інтелекту. В новій системі кількість випадків, коли для остаточного ухвалення рішення про ідентифікацію потрібна участь експерта, становить менш 50%, тобто більш ніж у половині випадків розпізнавання здійснюється повністю в автоматичному режимі.

Як підсумок – відповіді на запити користувачів надаються швидше, що зумовлює зростання ефективності використання наданих даних[1].

У травні 2011 року корпорація «Northrop Grumman» уклала з Міністерством оборони США контракт на надання послуг із супроводу автоматизованої системи біометричної ідентифікації Dod ABIS. Контракт розрахований на рік, але може протягом чотирьох наступних років щорічно продовжуватися.

У рамках підписаного з Пентагоном контракту корпорація буде надавати послуги із супроводження цієї системи. Комплекс надаваних послуг охоплює управління програмними й апаратними засобами, що входять до Dod ABIS, навчання користувачів поводженню з системою, нагляд за її масштабуванням та інтеграцією з іншими IT-розробками, а також підтримка безперервності функціонування системи і відновлення її працездатності за можливих збоях[2].

У квітні 2013 року російський біометричний портал «Biometrics.RU» повідомив, що Міністерство оборони США має намір змінити контракт із одним з провайдерів, який здійснює супроводження системи Defense Automated Biometric Identification System. Метою змін є розширення спектра послуг із управління цією системою та підключення нових різних технічних сервісів.

Фахівці вважають, що йдеться про застосування мультибіометричних технологій на основі використання мобільних пристроїв[3].

Пентагон дійсно зацікавився можливістю здійснення біометричної ідентифікації за допомогою смартфонів. Він замовив проведення робіт із розробки «біометричного смартфона», за допомогою якого можно розпізнавати людей не тільки за відбитками пальців, але й за їх обличчям, райдужною оболонкою очей та голосом. До технічного завдання окремо включена умова, згідно з якою біометричний смартфон повинен бути наділений здатністю самостійно, без участі користувача гаджета, формувати електронні зображення біометричних ідентифікаторів для подальшої їхньої обробки.

Коментуючи наведену умову нового контракту, експерти висловлюють припущення, що Пентагон поступово відмовляється від мобільних комплексів біометричної

---

[1] Пентагон наращивает применение биометрии // BIOMETRICS.RU. – 2009. – 10 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Пентагон продолжит развивать свою биометрическую систему // BIOMETRICS.RU. – 2011. – 30 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Пентагон расширит применение биометрических технологий // BIOMETRICS.RU. – 2013. – 9 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

ідентифікації за назвою *HIIDE*. Біометричні смартфони мають набагато меншу вагу та розмір, а також ліпшу систему управління[1].

Акцентуємо, що американці за час перебування на теренах Іраку й Афганістану зібрали біометричні ідентифікатори трьох мільйонів мешканців Іраку та значної кількості населення Афганістану. Вся інформація надходить в єдину інформаційну систему DNA Registry, яку веде Міністерство оборони[2].

Міністерство оборони США у 2009 році проводило роботи за проектом Biometrics Operations and Support Services – Unrestricted (BOSS-U) vehicle. Одним із завдань проекту BOSS-U є формування бази біометричних даних терористів, учасників збройних формувань, що беруть участь у будь-яких конфліктах, де задіяні збройні сили Сполучених Штатів Америки, а також громадян іноземних держав, які потенційно можуть розглядатися «як ворожі елементи». Складовою цього банку даних є біометричні ідентифікатори іноземних громадян, які працюють на закордонних військових об'єктах США[3].

Згодом уся інформація з систем DNA Registry і BOSS-U надійшла до бази даних Defense Automated Biometric Identification System. Це відомості щодо зображень відбитків усіх десяти пальців, п'яти знімків обличчя та наявних татуювань на тілі мешканців Іраку й Афганістану, а також громадян інших країн, де розташовані військові бази США[4].

Кожен із видів військових сил Пентагону експлуатують свої біометричні бази даних різного спрямування. За останні роки у засобах масової інформації була опублікована низка відомостей про ведення БД кадрового спрямування. Наприклад, командування з набору громадян на службу у Військово-морські сили (ВМС) США уклало п'ятирічний контракт на створення біометричної інформаційної системи кандидатів до лав ВМС[5].

2010 року Міністерство оборони США створило спеціальне агентство з біометричної ідентифікації. Воно продовжило формування та розвиток гігантської бази даних про біометричні ідентифікатори, яка функціонує в Пентагоні. Одним із завдань агентства є координація діяльності з розробки нових біометричних технологій в інтересах усіх видів збройних сил, розвідувальних і спеціальних служб Сполучених Штатів Америки[6].

2008 року Федеральне бюро розслідувань (ФБР /FBI/) розпочало процес модернізації «Інтегрованої автоматичної системи ідентифікації за відбитками пальців» (Integrated Automated Fingerprint Identification System – IAFIS) у Систему «Ідентифікація нового покоління» (Next Generation Identification system – NGI), суттєвою рисою якої є можливість підтримки ідентифікації особи за декількома біометричними ознаками (за відбитками пальців і долонь, зображенням райдужної оболонки ока, за формою і геометрією обличчя та іншими можливими методами ідентифікації).

---

[1] Пентагон заинтересовался мобильной мультибиометрической идентификацией // BIOMETRICS.RU. – 2013. – 18 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] США составили биометрическую базу данных на три миллиона иракцев // Хабрахабр. – 2011. – 22 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Американские власти стремятся усиливать информационную безопасность // Хакер. – 2009. – 16 июня. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Пентагон подвел итоги конкурса на сопровождение своей биометрической системы // BIOMETRICS.RU. – 2013. – 13 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[5] Биометрические технологии на защите информационной системы флота США // BIOMETRICS.RU. – 2012. – 4 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[6] Биометрия 2010: 50 главных событий года // BIOMETRICS.RU. – 2011. – 13 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

У квітні 2014 року американський «фонд електронних рубежів» опублікував нові документи про БД NGI, які були отримані під час судового процесу проти Федерального бюро розслідувань в зв'язку з утаємниченням інформації про цю розробку.

Згідно з оприлюдненими документами, у 2015 році система «Ідентифікація нового покоління» повинна зберігати 52 млн індивідуальних записів (так званих досьє). У перспективі вона зможе зберігати біометричні відомості третини населення США. ФБР має намір отримати частину інформації з «цивільних джерел», тобто дані стосовно своїх громадян, які, можливо, ніколи не вчиняли злочинів.

NGI створюється на базі IAFIS, яка зберігає відбитки пальців на 100 млн осіб. У FBI біометрична інформація зв'язана з особистим досьє на людину, де зазначаються прізвище та ім'я, домашня адреса, номер посвідчення водія, імміграційний статус, вік, етнічна приналежність та інші персональні відомості. Доступ до бази мають й інші федеральні відомства, а також 18000 тис. регіональних підрозділів правоохоронних органів.

Оприлюднені документи вказують на невпинне зростанн обсягу базу даних. Так, 2012 року в NGI зберігалось 13,6 млн зображень для автоматичного розпізнавання лиця від 7 до 8 млн індивідуумів, улітку 2013 року обсяг БД зріс до 16 млн зображень, а за останньою інформацією система щодня здатна зростати на 55000 нових зображень і опрацьовувати десятки тисяч пошукових запитів за добу.

Відповідно до планів Федерального бюро розслідувань, у 2015 році система «Ідентифікація нового покоління» повинна зрости до 52 млн індивідуальних фотозображень, із яких 46 млн «кримінальних зображень», 4,3 млн «цивільних зображень», приблизно 1 млн фотозображень із неназваних джерел, зокрема з «нових репозиторіїв».

Збір фотографій громадян уже розпочався: у багатьох організаціях та установах США під час оформлення спеціального допуску в кандидатів беруть не тільки відбитки пальців, а і фотографують.

За повідомленнями ЗМІ, у базу даних «Ідентифікація нового покоління» вносять біометричні характеристики всіх співробітників державних і недержавних структур США та низки інших країн, що проходили у встановленому порядку перевірку на наявність кримінального минулого.

Улітку 2014 року заплановано завершити заходи з модернізації NGI (IAFIS). У «Next Generation Identification system», на відміну від IAFIS, кожному запису, незалежно від наявності криміналу, буде наданий універсальний контрольний номер (UCN), і кожний запит буде проганятися за всіма записами в базі. Фактично це означає, що навіть громадянина без кримінального минулого зможуть розпізнати і за певних обставин він може отримати статус підозрюваного за кримінальною справою.

Незалежні дослідження довели, що ймовірність хибних ідентифікувань за фотозображеннями значно зростають у разі збільшення розмірів отриманих вибірок за запитами, а з 52-х мільйонної бази фотозображень одержана вибірка може бути дуже значною. Тобто вірогідність хибного ідентифікування громадянина зростає, а це для нього може спровокувати низку ускладнень[1].

Ще до 2012 року 47 штатів США брали участь у програмі «Ідентифікація і розпізнавання ув'язнених» (Inmate Identification and Recognition System – IRIS), у рамках якої ФБР одержує від різних правоохоронних органів відомості про відбитки пальців і долонь рук громадян зазначеної категорії, а також їх оцифровані фото. А з 2012 року до цих біометричних ідентифікаторів додалися відомості про райдужну оболонку очей.

[1] ФБР увеличит объем новой базы биометрических данных // Хабрахабр. – 2014. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Щоб упоратися із зростаючою кількістю даних, FBI нарощує обчислювальні потужності своїх серверів[1].

База даних NGI, до якої в обов'язковому порядку вносить інформацію про злочинців і терористів, відповідно до технічного завдання, є технологічно сумісною з іншою окремо сформованою за програмою US-VISIT базою біометричних даних IDENT, яка зберігає оцифровані фотографії та дані про відбитки пальців іноземних громадян, які були здобувачами візи на право в'їзду до США.

За експлуатацію БД IDENT відповідає Міністерство національної безпеки США (Department of Homeland Security – DHS). Формування бази даних за програмою US-VISIT було розпочато 2004 року і вона є однією з найбільших біометричних світових систем за кількістю даних щодо фізичних осіб[2]. За період із 2004 до 2009 року за базою даних IDENT було перевірено відомості на понад 100 млн здобувачів, які подали документи на отримання візи до США.

Перший етап робіт, пов'язаний із оновленням усіх дактилоскопічних даних системи «Next Generation Identification», був завершений у 2010 році. Під час експлуатації системи «Ідентифікація нового покоління» особлива увага приділяється збереженню конфіденційності інформації. Біометрична система «Next Generation Identification» й її база даних використовується для боротьби з міжнародним тероризмом. У своїй країні на цьому напрямі ФБР співпрацює з державними департаментами внутрішніх справ, оборони і закордонних справ[3].

У липні 2009 російський біометричний портал «Biometrics.Ru» з посиланням на передачу «CrimeTracker 10» навів цікаву статистику того обсягу робіт, які виконують суперкомп'ютери FBI. За цією статистикою у базі даних IAFIS – NGI були зібрані відбитки пальців понад 60 млн чоловік, зокрема в наявності були 600 000 зразків, власники яких не були ідентифіковані. Всі ідентифіковані зразки зберігаються і в електронних шаблонах, і в оригінальному зображенні. Кожен новий відбиток перевіряється за базою даних за всіма наявними зразками.

Кожну добу система отримує від різних оперативних служб близько 200000 наборів відбитків пальців, які потрібно терміново перевірити. Швидкість прогону кожного зразка – до семи секунд. Зазвичай кожен набір містить папілярні узори десяти пальців, тому кількість відбитків, яка щодобово аналізується, приблизно дорівнює двом мільйонам. А якщо порахувати кількість проведених порівнянь за умовою перевірки відбитку кожного пальця, то загальна чисельність операцій за добу становить приблизно 600 млрд[4].

2007 року стала відомою інформація про те, що FBI працює над створенням глобальної бази біометричних даних, але жодних уточнювальних відомостей не було опубліковано. 2008 року надійшла інформація про те, що США разом із правоохоронними органами Великобританії, Канади, Австралії і Нової Зеландії створили Міжнародний інформаційний консорціум (International Information Consortium) зі створення глобальної

[1] ФБР расширит использование биометрических технологий // BIOMETRICS.RU. – 2012. – 4 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Иванов В. Какой должна быть паспортная система / В. Иванов. – 2004. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://www.mpru.org/proekty/...

[3] Lockheed Martin заключает контракт с ФБР на разработку новой мультибиометрической идентификационной системы // Lenta.Ru. – 2008. – 13 февраля. [Электронный ресурс]. – Режим доступа: http://lenta.ru...

[4] ФБР анализирует 200000 отпечатков пальцев в сутки // Хабрахабр. – 2009. – 28 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

бази біометричних даних (кодова назва «Server in the Sky»), в яку з часом повинні бути внесені відомості щодо сотень мільйонів мешканців Землі, а у майбутньому можливо навіть мільярдів людей.

Офіційний представник ФБР в інтерв'ю британській газеті «The Telegraph» повідомив, що «Server in the Sky», за задумом його творців, повинен забезпечувати обмін біометричними даними між країнами – учасницями проекту, дозволяючи оперативно отримувати відомості про злочинців, інформація щодо яких буде зберігатися у створюваній базі даних[1].

Як відомо, держави США, Австралія, Британія, Канада і Нова Зеландія входять у так звану Конференцію п'яти країн (Five Country Conference – FCC). Учасники FCC мають домовленість про те, що з метою зміцнення безпеки кордонів, боротьби з незаконною міграцією та іншими виявами злочинних дій вони будуть обмінюватися біометричними даними відносно осіб, які становлять інтерес у кримінальному плані[2].

У бюджеті США на 2010 рік було передбачено фінансування нового проекту Інтерполу під назвою «Vennlig». Цей проект передбачає створення міжнародної бази даних для обміну інформацією стосовно терористів. Заплановано, що відомості будуть надсилатися американськими службами безпеки у країни, що співпрацюють з Інтерполом[3].

Водночас не можна не згадати про узагальнений банк даних на вже відомих терористів і підозрюваних у співпраці з терористами осіб, який функціонував ще у 2004 році у Центрі виявлення терористів (Terrorist Screening Center /TSC/)[4].

У ФБР США ведеться спеціальна база слідчих даних Investigative Data Warehouse (IDW). Це закритий системний банк даних усіх зібраних розвідувальних зведень та іншої слідчої інформації, доступ до якого здійснюється за допомогою інформаційної мережі (Web-enabled).

Ця інформаційна система дозволяє відповідно підготовленому й уповноваженому на проведення таких дій персоналу виконувати запити, які прирівнюються до сфери проведення слідчих або розвідувальних дій. Інформація, що накопичується в базі IDW, надходить від усіх урядових установ (агентств) та, що особливо важливо, із зон бойових дій в Іраку й Афганістані. База IDW постійно розширюється та поповнюється. За допомогою спеціальної інформаційної мережі вона забезпечує організацію єдиного доступу спеціальних агентів, розвідувальних аналітиків і співробітників об'єднаних антитерористичних спеціальних сил JTTF (Joint Terrorism Task Forces) до більш ніж 47-ми джерел контртерористичних даних. До таких джерел належать секретна інформація ФБР, конфіденційні відомості інших силових і владних структур, а також відкрита інформація з будь-яких джерел, зокрема засоби масової інформації.

У центрі аналізу терористичних вибухових пристроїв TEDAC (Terrorist Explosive Device Analytical Centre) створена база даних про саморобні вибухові пристрої (СВП /IED/).

---

[1] ФБР привлекает другие страны к формированию гигантской базы биометрических данных // Lenta.Ru. – 2008. – 16 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp

[2] Кузнецов С. Биометрия на службе охраны правопорядка и безопасности / С. Кузнецов // IEEE Computer Society, V. 43. – 2010. – № 2. – февраль. [Электронный ресурс]. – Режим доступа: http://citforum.ru/computer/2010-02/

[3] Новые подробности о британской базе биометрических данных // BIOMETRICS.RU. – 2009. – 29 мая. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Мюррэй С. Биометрия против терроризма / Сара Мюррэй // Деловая неделя. – 2004. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

За допомогою накопиченої інформації, зокрема й біометричної, та проведеними аналітичними дослідженнями центру в 2003–2008 роках було ідентифіковано 56 осіб, які виготовляли вибухові пристрої[1].

Міністерство національної безпеки США (Department of Homeland Security /DHS/) ще у 2006 році розпочало вести єдину базу біометричних даних на порушників міграційного законодавства, в якій накопичуються біометрична, біографічна, проблемно-кримінальна та поточна інформація стосовно іммігрантів.

Берегова охорона (U.S. Coast Guard) DHS реалізовує свій масштабний державний біометричний проект – Transportation Worker Identification Credential (TWIC). TWIC разом із програмою «Біометрія в морі» повинна сприяти боротьбі з порушниками морських кордонів США.

Проект Transportation Worker Identification Credential, що був розпочатий за ініціативою Берегової охорони й Управління з безпеки на транспорті США, передбачає обов'язкову наявність у співробітників аеропортів, портових підприємств, робочих бурових веж і доків, членів екіпажів судів посвідчень особистості у вигляді картки, в мікрочіп якої внесені електронні шаблони їх папілярних узорів пальців. Ця картка повинна використовуватися для підтвердження особистості власника на пунктах перевірки відбитків пальців, де відповідна інформація зчитується з карт за допомогою спеціальних мобільних модулів[2].

Систему TWIC використовує й Управління транспортної безпеки США (TSA) в аеропортах США. За допомогою біометричної ідентифікаційної картки транспортного працівника здійснюють ідентифікацію власників карток TWIC за паролем і біометричними ознаками.

Час ідентифікації власника біометричної ідентифікаційної картки становить приблизно три секунди[3].

Програма «Біометрія в морі», яка реалізовується з листопада 2006 року, дозволяє береговій охороні через супутниковий зв'язок надсилати у цифровому вигляді на перевірку в банк даних Міністерства національної безпеки (DHS) відбитки пальців і фотографії затриманих у морі мігрантів і контрабандистів та впродовж 3–5 хвилин отримувати результати перевірки безпосередньо на судні. База даних DHS станом на листопад 2007 року містила інформацію приблизно на 3,2 млн осіб, яка охоплювала відомості про всі попередні відвідини ними Сполучених Штатів Америки і видані щодо них ордери на затримання або розпорядження про депортацію. Всі зібрані відомості про затриманих вносяться в базу даних Department of Homeland Security США, водночас відбувається або доповнення вже наявних облікових записів, або створення нових записів щодо осіб, які вперше реєструються[4].

Митне та прикордонне агентство США сформувало і використовує систему USPASS. За її допомогою пришвидшується проходження прикордонного контролю громадянами, зареєстрованими в цій системі: їхня особистість надійно і швидко засвід-

[1] Новые средства получения разведданных о террористах // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 3–9.

[2] Биометрия на службе государству // Secuteck.ru. – 2008. – 29 октября. [Электронный ресурс]. – Режим доступа: http://secuteck.ru/newstext.php...

[3] Биометрическая идентификационная карта транспортного работника: определены пять пилотных портов для тестирования новинки // BIOMETRICS.RU. – 2007. – 16 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Биометрические технологии – гарантия безопасности границ // MIGnews. com. – 2007. – 15 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/ document.asp…

чується за допомогою біометричних технологій (ідентифікація здійснюється за геометрією кисті руки)[1].

Із 2008 року в Сполучених Штатах Америки діє біометрична система прикордонного контролю Global Entry. 2012 року ця система діяла в 20 американських аеропортах і налічувала 137 пунктів контролю. Для участі в програмі Global Entry необхідно пройти початкову перевірку в Міністерстві національної безпеки та зареєструвати як біометричні ідентифікатори відбитки пальців.

Користувачі біометричної системи прикордонного контролю долають кордон США менш ніж за хвилину, водночас проходження прикордонного та митного контролю у звичайному порядку потребує набагато більшого часу.

Участь у програмі Global Entry беруть не тільки громадяни США, але також і власники канадських, мексиканських, нідерландських і південнокорейських паспортів. Проект реалізує Німеччина, а інтерес до програми виявили Франція, Сінгапур, Австралія й Нова Зеландія[2].

Понад десятиліття всі державні структури Сполучених Штатів Америки виконують вимоги Президентської директиви щодо національної безпеки США (HSPD-12) з організації безпечного доступу в робочі приміщення установ і комп'ютерно-телекомунікаційні системи, але лише деякі з них належно використовують усі переваги біометричної ідентифікації.

2013 року Міністерство внутрішньої безпеки (МВБ) розпочало проект з інтеграції в національні ID-карти мультибіометричних параметрів для однозначної прив'язки посвідчення особи до її власника. За Директивою адміністративно-бюджетного управління США, яка спрямована на подальше впровадження директиви HSPD-12, так звана PIV-карта (варіант ID-карти), яка здійснює верифікацію особи, стане основним інструментом аутентифікації повноважень для доступу до послуг, мереж та інформаційних систем усіх державних установ.

Новий варіант ID-карти – PIV-карта у вмонтовановому чіпі буде зберігати, відповідно до стандарту 201-2 Національного інституту стандартів і технологій (NIST) США, електронне зображення відбитків пальців, райдужної оболонки ока та форми обличчя.

Виглядати нова смарт-карта буде як ламінована пластикова карта старого зразка, але загалом у чіпі буде розміщено набагато більше в електронному форматі різних даних, зокрема і біометричних.

Ідентифікація буде здійснюватися за відбитками пальців, райдужної оболонки ока та форми лиця особи.

PIV-карта може мати не тільки штрих-код, RFID-позначку (радіочастотна ідентифікація) та магнітну машинозчитувальну стрічку-смужку, але й вбудований додатковий мікропроцесор даних для сегментування та зберігання інформації, зокрема й для автоматичного віддаленого оновлення інформації[3].

---

[1] Украина. Введение биометрических паспортов запланировано на 2012 год // РИА Новости Украина. – 2010. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] США: сфера действия биометрической системы пограничного контроля будет расширена // BIOMETRICS.RU. – 2012. – 27 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...; Граждане Южной Кореи смогут воспользоваться американской биометрической системой пограничного контроля // BIOMETRICS.RU. – 2012. – 2 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические идентификационные карты в США обрели второе дыхание // Экспертный центр электронного государства. – 2013. – 23 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Звісно, крім наведених біометричних систем і баз даних, у США функціонують й інші біометричні системи і БД, але вони за масштабністю проектів набагато менші вищенаведених.

Перейдемо до Сполученого Королівства Великобританія.

Найперше згадаємо систему об'єднаної організації кримінального правосуддя Criminal Justice Organisation (CJO), створення якої дозволило ліквідувати багато міжвідомчих комунікаційних бар'єрів, налагодити швидкісний обмін інформацією, створити ефективну систему розподілення та адресації всього наявного потоку документів. Акцентуємо, що втілення в життя кримінальної системи правосуддя CJO було надзвичайно трудомістким завданням. У процесі розробки пройшли апробацію аж 43 варіанти корпоративної моделі даних, перед тим, як був створений такий уніфікований варіант, який зміг задовольнити всіх суб'єктів кримінального правосуддя[1]. Слід зауважити, що відомостей про використання біометричних ідентифікаторів у системі CJO авторами не знайдено.

Британська поліція сформувала і продовжує наповнювати необхідними даними першу загальнонаціональну базу даних, у якій зберігаються мільйони фотознімків осіб, описи шрамів, татуювань та інших характерних ознак індивідуумів. Початком випробування у пілотному режимі проекту під назвою FIND (Facial Images National Database – національна база даних за обличчями або ж просто «ЗНАЙТИ») вважається листопад 2006 року, а з 2009 року використання загальнонаціональної бази даних «FIND» повинно було поширитись на всю територію Великобританії.

Мета проекту – реалізація у Сполученому Королівстві ідеї автоматизованого розшуку злочинців та осіб, які підозрюються у вчиненні злочинів, за зображеннями, отриманими з камер відеоспостереження[2].

Поліція Великобританії свого часу завершила тестування програмно-апаратного мобільного комплексу, розробленого в рамках програми «Мідас», який перевіряє відбитки пальців за базою даних Ident1. Дослідна експлуатація показала, що в 80% випадків результати перевірки вилучених із місця події відбитків пальців за БД Ident1 надходили до поліцейських патрулів упродовж двох хвилин. Відповідно до програми «Мідас», всі поліцейські підрозділи Британії до 2013 року повинні були отримати мобільні засоби ідентифікації за відбитками пальців[3].

У Сполученому Королівстві Великобританія, крім ідентифікації за відбитками пальців, дуже поширений метод ідентифікації за райдужною оболонкою ока. На основі цього методу діє державна система «IRIS» (Iris Recognition Immigration System). Її тестування проходило ще у 2005 році, а з другого півріччя 2008 року розпочата експлуатація у штатному режимі.

Крім Сполученого Королівства, цей метод ідентифікації активно використовується у Канаді, Нідерландах і Об'єднаних Арабських Еміратах та в інших країнах Близького Сходу, що входять до Ліги арабських держав[4].

---

[1] Cleden D. О разработке корпоративной информационной системы в английской полиции / D. Cleden // Борьба с преступностью за рубежом (по материалам зарубежной печати / пер. из журнала Police). – М.: ВИНИТИ. – 2004. – № 10.

[2] Захаров В. П. Використання біометричних технологій правоохоронними органами у XXI столітті: науково-практичний посібник / В. П. Захаров, В. І. Рудешко. – Львів: ЛьвДУВС, 2009. – С. 313–314.

[3] Вся британская полиция будет оснащена мобильными средствами биометрической идентификации // BIOMETRICS.RU. – 2008. – 27 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Распознавание радужной оболочки глаза на службе безопасности // UNISXCAN. – 2005. – 19 сентября. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/...

В островній державі реалізується програма «Національний сервіс біометричної ідентифікації». В рамках цієї програми заплановано надати нові функціональні можливості системі персональних біометричних даних громадян Великобританії. Для здійснення цього завдання за підсумками проведеного тендеру ще у 2008 році були відібрані компанії IBM і Thales[1].

У перспективі британські урядові структури мають намір об'єднати в одну біометричну систему банки даних підданих Сполученого Королівства та іноземних громадян, які перебувають на території Великобританії[2]. Але термін виконання цього амбітного завдання неодноразово переносився.

Формування національного сховища біометричних ідентифікаційних даних (National Biometric Identity Store – NBIS) покладене на компанію IBM. У NBIS вносяться відомості про відбитки всіх 10 пальців рук тих британців, які звертаються за отриманням ідентифікаційних документів нового покоління: біометричних закордонних паспортів і внутрішніх ID-карт. У базі даних NBIS зберігаються і цифрові моделі-шаблони біометричних ідентифікаторів, і безпосередньо зображення відбитків пальців. Представники МВС і Ідентифікаційної та паспортної служби заявляють, що National Biometric Identity Store функціонує окремо від бази даних про відбитки пальців Ident1, яку експлуатує британська поліція.

2006 року палатою общин Сполученого Королівства Великобританія був схвалений законодавчий акт із впровадження внутрішніх біометричних ідентифікаційних карт громадян Королівства.

Згідно з цим законом, у країні передбачено створення Національного ідентифікаційного регістра (National Identity Register /NIR/), основним завданням якого є формування бази даних щодо кожного з громадян Британії за 49-ма різними параметрами, куди входять відомості про відбитки пальців, ДНК, домашню адресу та телефони. Відповідно до нормативних документів МВС Великобританії, біометричні дані, які вносяться у нове посвідчення особистості, будуть дублюватися у Національному регістрі громадян тільки в крайніх випадках[3].

Із початку 2007 року МВС і Міністерство закордонних справ і в справах Співдружності Сполученого Королівства Великобританія розпочали практичну реалізацію програми видачі британських біометричних віз. У безперервно діючу спільну базу даних цих двох британських відомств кожні тридцять секунд вносяться нові відомості про всі відбитки пальців кожної руки та оцифроване фотозображення все нових здобувачів британських віз.

За перше півріччя функціонування програми видачі британських біометричних віз у інтегрованому банку даних було накопичено близько 500 тисяч «десятипальцьових наборів» претендентів на отримання віз і кількість накопиченої інформації у базі даних стрімко зростає, щомісячно поповнюючись відомостями приблизно на 100 тисяч осіб[4].

---

[1] Британия. Обнародованы шорт-листы компаний, участвующих в проектах биометрических загранпаспортов и ID-карт // BIOMETRICS.RU. – 2008. – 17 сентября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Британия. Иностранцы получают биометрические идентификационные карты // BIOMETRICS.RU. – 2008. – 25 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Британия. В реализации программы биометрических идентификационных карт возникли первые трудности // Аделанта-Инфо. – 2008. – 8 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Первые итоги действия британской системы биометрических виз // BIOMETRICS.RU. – 2007. – 20 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

До липня 2008 року система видачі біометричних віз була запроваджена у дипломатичних представництвах Британії у 133 країнах світу, а в базі даних зберігалась інформація стосовно 2 млн осіб[1].

Ще у 2006 році державна служба охорони здоров'я Сполученого Королівства запланувала витратити 12 млрд фунтів на створення бази даних хвороб усіх пацієнтів: історії хвороб мільйонів громадян повинні були введені до цієї БД незалежно від бажання тих, хто звернувся за медичною допомогою. Уряд заявив, що реалізація цього плану зробить переворот в управлінні охороною здоров'я, але захисники цивільних свобод наполягали на тому, що потрібно спочатку отримати згоду пацієнтів, перед тим, як створювати можливість отримання конфіденційних подробиць їх стану здоров'я, непитаючи водночас на те відповідного дозволу[2].

За повідомленням агентства «United Press International» уряд Британії має намір розпочати збір даних про відбитки пальців усіх дітей віком 11–16 років в обов'язковому порядку. З початку 2008 року цей збір поки що проходить у добровільному порядку – за згодою особи, яка не досягнула 16-річного віку під час оформлення нею закордонного паспорта.

З 2010 року процедура знімання біометричних параметрів у підлітків повинна була стати обов'язковою. Формування бази даних відбитків пальців британських підлітків є складовою програми введення закордонних біометричних паспортів і внутрішніх біометричних ідентифікаційних карт. Планувалось значний обсяг цієї програми виконати до 2011 року[3].

Ще раз нагадаємо, що США, Австралія, Британія, Канада і Нова Зеландія входять у Конференцію п'яти країн (Five Country Conference – FCC). Учасники FCC мають домовленість про те, що для зміцнення безпеки кордонів, боротьби з незаконною міграцією та іншими виявами злочинних дій вони обмінюються біометричними даними стосовно осіб, які становлять інтерес у кримінальному плані. Австралія – одна з країн, яка є учасницею FCC. Тому її біометричні системи та відповідні бази даних подібні до тих, що функціонують у Сполучених Штатах Америки і Великобританії.

Міністерство оборони Австралії експлуатує автоматизовану інформаційну систему біометричної ідентифікації (Automated Biometric Information System – ABIS). ABIS використовується у діяльності розвідувальних служб, а також для біометричної ідентифікації учасників бойових дій. Зазначимо, що ця система є аналогом пентагонівської системи DoD ABIS[4].

Австралійське міністерство з справ імміграції та громадянства (Department of Immigration and Citizenship – DIAC) з 2007 року експлуатує свою біометричну систему. Оскільки навантаження на біометричну систему цього відомства постійно зростає, з 2013 року DIAC розпочало здійснення модернізації своєї інформаційної системи. Крім обновлення програмного забезпечення процесу біометричної ідентифікації за електронними зображеннями відбитків пальців і обличчя, виконавець робіт повинен забезпечити

[1] Лукашов И. Биометрию «привьют» повсеместно / И. Лукашов // Cnews.ru. – 2008. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/ reviews/free/security2008/articles/…

[2] Британцы под колпаком // GZT.RU. – 2006. – 8 ноября. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/digest/...

[3] Правительство Британии планирует приступить к биометрической идентификации подростков // BIOMETRICS.RU. – 2007. – 6 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Министерство обороны Австралии испытает новую биометрическую систему // BIOMETRICS.RU. – 2012. – 26 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

інтегрування своїх продуктів в усі експлуатовані міністерством системи, а також провести навчання персоналу установи.

Оновлюючи та розширюючи свою біометричну систему, DIAC має намір наділити її новими функціями та можливостями. Зокрема, повинна суттєво збільшитися ефективність електронного документообігу, процесів формування звітності й управління біометричною системою загалом, причому особлива увага буде приділена забезпеченню захисту наявної інформації[1].

Державами Шенгенської зони 2009 року була запроваджена в повному обсязі єдина Інформаційна система про видані візи ((Visa Information System – VIS). Ця система стала єдиною базою даних біометричної інформації щодо осіб, які отримали дозвіл на перебування в «країнах Шенгену» або відмову у видачі візи. З часом цей банк даних повинен стати єдиним для всіх держав ЄС. Політичний імпульс для створення БД «VIS» свого часу дала Європейська рада. Європейською комісією був підготовлений проект відповідного регламенту, який у червні 2007 року практично одностайно був прийнятий Європарламентом.

Європейська інформаційна система про видані візи розрахована на зберігання персональних досьє щодо власників віз, у які в обов'язковому порядку повинні бути внесені загальноустановчі дані, фотозображення та інформація про відбитки пальців, а також реєстраційні дані автомобіля, якщо іноземний громадянин перетинає кордон ЄС на особистому транспорті. Запланований на той час мінімальний обсяг зберігання даних на 70 млн осіб.

Доступ до банку даних «VIS», крім поліційських, консульських і міграційних служб країн Євросоюзу, отримають також усі правозастосовні органи держав – членів Європейського Союзу й Європол. Місцем перебування органу управління системи «VIS» обрано Страсбург, фінансування проводиться з бюджету Європейського Союзу[2].

На 28 вересня 2012 року в базі даних Європейської візової інформаційної системи було зібрано відомостей на один мільйон громадян, які зверталися за дозволом на в'їзд у Шенгенську зону[3].

З 1 грудня 2012 року в Європейському Союзі з'явилася нова структура, у веденні котрої серед іншого перебувають і візові питання. Назва цього адміністративного органу – «Агентство ЄС з контролю за великомасштабними ІТ-системами». Головна мета цієї установи – формування уніфікованої бази даних, яка дозволить відповідні документи й отримані біометричні візи однозначно закріплювати за конкретною особою. Діяльність уніфікованої БД розпочалася з 14 січня 2013 року[4].

Країни Європейського Союзу з метою перешкоджання можливості потрапляння нелегалів на свою територію експлуатують інформаційну систему «EURODAK» – європейську базу даних про відбитки пальців здобувачів статусу біженця й іноземців, які перетинають кордони держав Євросоюзу. У БД «Eurodac», крім анкетних даних,

---

[1] Австралия расширит использование биометрических технологий в иммиграционном контроле // BIOMETRICS.RU. – 2012. – 22 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Евросоюз укрепляет визовую систему // Белорусские новости. – 2007. – 25 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp…; Бокарева Н. Не прячьте ваши пальчики. В Европу без дактилоскопии больше не пустят / Н. Бокарева. – 2007. – 27 июля. [Электронный ресурс]. – Режим доступа: http://news.mail.ru/politics/...

[3] Шенгенские визы станут для граждан ОАЭ биометрическими // BIOMETRICS.RU. – 2012. – 28 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Европа готовится к введению биометрических виз // Travel.ru. – 2012. – 27 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/newsz/...

зберігаються відомості про відбитки пальців, проби ДНК та інформація про вчинені фігурантами правопорушення[1].

Експлуатація шенгенської інформаційної системи SIS повинна була розпочатися ще в 2007 році, але реалізація проекту неодноразово відкладалася. Експлуатація другого покоління Шенгенської інформаційної системи (Schengen Information System /SIS II/) розпочалася у повному обсязі з 2013 року.

SIS II – це основа співробітництва країн Шенгенської зони. Друга версія цієї системи відіграє важливу роль у забезпеченні свободи пересування громадян, а також належного контролю в умовах відсутності перевірок на кордонах між країнами – учасницями Шенгену.

Schengen Information System II містить інформацію про людей, які не мають права на в'їзд або перебування в Шенгенській зоні, а також про осіб, які підозрюються у скоєнні протиправних дій та перебувають у розшуку. Крім того, в Шенгенській інформаційній системі також є інформація про осіб, які безвісти зникли, зокрема про неповнолітніх та інших незахищених категорій людей, котрі потребують захисту. В системі SIS II зберігається інформація про так звані «номерні» предмети, наприклад, про автомобілі, водні транспортні засоби, стрілецьку зброю та документи, що були втрачені, викрадені або використовувались для вчинення злочинів[2].

В Європейському Союзі проводилися науково-дослідні роботи з реалізації масштабного європейського проекту «Моніторинг людини та ідентифікація його особистості з застосуванням біодинамічних індикаторів і поведінкового аналізу» (Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis /HUMABIO/), метою якого є об'єднання різних біометричних технологій в єдине ціле для створення ефективної та захищеної уніфікованої глобальної біометричної системи[3].

Із 2009 року за ініціативою Європейської комісії авіакомпаній країн ЄС розпочалася пілотна експлуатація спеціальної бази персональних даних про авіапасажирів. У системі збору і зберігання інформації щодо клієнтів авіакомпаній збираються цифрові фотографії та відбитки пальців усіх претендентів на отримання в'їзних віз до шенгенської зони. Крім біометричних параметрів, система також зберігає анкетні дані пасажирів[4].

Країни Євросоюзу придивляються до американського досвіду використання біометричних технологій за контролем міграційних потоків. Запровадження біометричного контролю за в'їздом–виїздом іноземних громадян на територію ЄС дозволить поставити надійну перешкоду на шляху незаконних мігрантів, які правдами й неправдами прагнуть потрапити до європейських країн.

Деякі високопосадовці Європейського Союзу пропонують створити реєстр персональних даних, зокрема і біометричних ідентифікаторів, іноземців, які претендують на в'їзд до держав союзу. Доступ до реєстру повинен здійснюватися в онлайновому режимі з усіх контрольно-пропускних прикордонних пунктів європейського співтовариства[5].

---

[1] Преступность в контексте миграционных процессов // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 13–22.

[2] SIS II – Шенгенська інформаційна система II. [Електронний ресурс]. – Режим доступу: http://www.mfa.gov.hu/NR/...

[3] Паспорт мыслей: новый вид биометрии? – 2007. – 17 января. [Электронный ресурс]. – Режим доступа: http://www.egovernment.ru/newstext...

[4] Европа попросит приложить руку // Вокруг Света. – 2008. – 29 января. [Электронный ресурс]. – Режим доступа: http://secuteck.ru/newstext...

[5] Германия предложила позаимствовать у США опыт использования биометрических технологий // BIOMETRICS.RU. – 2013. – 26 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Дуже цікавою є інформація про ідентифікаційні системи Ізраїлю – держави, яка постійно веде боротьбу з терористичними загрозами.

У цій країні з 2006 року діє спеціальна система BCMS (Border Control Management System), яка призначена для швидкого розпізнання і відстеження арабських імен, що дає змогу значно пришвидшити процедуру ідентифікації підозрілих осіб під час проведення прикордонного контролю. Система BCMS є, по суті, фонетично орієнтованим високошвидкісним процесор, який підключений до баз даних усіх органів безпеки й уряду для того, щоб порівнювати та зіставляти арабські імена у всіх можливих варіантах їх написання. З 2008 року діє вдосконалений варіант цієї системи, що запровадив ще один рівень пошуку, який ґрунтується на розпізнанні за папілярними узорами пальців[1].

28 листопада 2012 року Кнесет Ізраїлю схвалив проект із створення біометричної бази даних своїх громадян і видачі посвідчень особи «теудат зеут». Із 1 січня 2013 року до грудня 2014 року одержання біометричних документів буде справою суто добровільною, однак після завершення цього строку почнеться централізована заміна документів у всіх громадян країни.

У мікрочіпі посвідчення нового зразка будуть зберігатися в електронному форматі відбитки двох пальців і фотозображення власника. Ця ж інформація буде дублюватися в централізованій базі даних громадян Ізраїлю[2].

До відомостей централізованої біометричної БД громадян країни без постанови суду будуть мати доступ поліція, армія та служби безпеки. А за наявності судової постанови персональні відомості можуть бути надані іншим відомствам, зокрема й іноземним[3].

Міністерство внутрішніх справ Ізраїлю оголосило про заходи з посилення контролю під час в'їзду в країну. Для цього буде створена база біометричних даних іноземних туристів. Кожному відвідувачеві країни будуть видавати спеціальну ідентифікаційну біометричну картку, яку він зобов'язаний носити з собою під час відпочинку. В державі вже функціонує подібна біометрична система стосовно іноземних працівників, які приїжджають у країну за укладеними трудовими контрактами[4].

Один із наймасштабніших у світі проектів біометричної ідентифікації за райдужною оболонкою очей у прикордонному контролі реалізований в Об'єднаних Арабських Еміратах (ОАЕ). На території цієї країни постійно проживають 5,4 млн іноземців, із них 85% – гастарбайтери. Природньо, міграційні потоки в ОАЕ дуже великі та постійно зростають. Система біометричної ідентифікації прикордонного контролю щодня проводить до 14 млрд порівнянь даних щодо зображень райдужок очей.

У перспективі прикордонні банки даних ОАЕ, Йорданії, Катару й Оману повинні об'єднатися з відповідною базою даних Саудівської Аравії[5].

В Об'єднаних Арабських Еміратах сформована всеосяжна база даних про відбитки пальців мешканців країни. Управління з ідентифікації ОАЕ повідомило, що БД

---

[1] Новые средства получения разведданных о террористах // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 3–9.

[2] Израиль. Уже в январе начнётся выдача биометрических удостоверений личности // NEWSru Израиль. – 2012. – 29 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/izrail...

[3] Власти Израиля намерены создать базу биометрических данных // Russia Today. – 2013. – 9 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Израиль подтвердил планы биометрической идентификации иностранцев // Travel.ru. – 2012. – 18 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[5] Ученый из Кембриджа предрекает дальнейшее распространение технологий идентификации по радужной оболочке глаз // BIOMETRICS.RU. – 2008. – 4 сентября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

в електронному вигляді зберігає відомості щодо 103 млн відбитків пальців і понад 15 млн цифрових фотозображень і підписів[1].

У Російській Федерації (РФ) створена багаторівнева взаємопов'язана система автоматизованих баз даних дактилоскопічної інформації (АДІС) «Папілон», яка охоплює всі регіони країни. Окрім Міністерства внутрішніх справ (МВС), користувачами «Папілон» у Росії є підрозділи низки інших відомств, переважно правоохоронних структур: Федеральної служби з контролю обороту наркотиків, Федеральної міграційної служби, Міністерства оборони, Федеральної служби безпеки.

За технологією АДІС «Папілон» створені та розвиваються національні системи автоматизованих дактилоскопічних обліків для потреб поліції Казахстану, Албанії, Нігерії. Постачання систем «Папілон» також здійснювалося до В'єтнаму, Монголії, Польщі, Таджикистану, Туркменістану[2].

Наприкінці 2013 року в Російській Федерації (РФ) мала запрацювати оновлена єдина система контролю, обліку та систематизації дактилоскопічної інформації.

Досягнення біометрики використовуються Федеральною міграційною службою (ФМС) Росії в автоматизованих системах обліку закордонних документів «Паспорт» і Державній інформаційній системі міграційного обліку (російською мовою «ГИСМУ» – Государственная информационная система миграционного учета). Вона формується на базі центрального банку даних про іноземних громадян і обліку видачі документів нового покоління для іммігрантів, які містять біометричні параметри їх власників. Система повинна забезпечити належний облік і контроль за в'їздом, перебуванням і виїздом іноземних громадян із території РФ[3].

Більш детально функціонування дактилоскопічних систем АДІС у Росії було розлянуто в підрозділі 2.5 «Автоматизовані дактилоскопічні ідентифікаційні системи (АДІС)» цього посібника.

Окремо слід згадати про базу МВС РФ «Єдина інформаційно-телекомунікаційна система» (ЄІТКС). За відомостями ЗМІ, ця система інтегрує всі БД місцевого й федерального рівня органів внутрішніх справ у єдину систему, так щоб доступ до них був у кожному районному відділі поліції. ЄІТКС об'єднана з телекомунікаційною системою внутрішніх військ МВС, а також має доступ до «публічних і спеціальних федеральних інформаційно-телекомунікаційних систем»[4].

Інформація щодо існуючих у світі біометричних систем і баз даних була б неповною, якби автори посібника не згадали про найбільші у світі за кількісним обліком своїх громадян соціальні біометричні системи Індії та Пакистану.

В Індії з 2010 року Управління з присвоєння громадянам унікальних ідентифікаційних номерів (UID Authority of India – UIDAI) проводить заходи присвоєння громадянам ідентифікаційних номерів. UIDAI вирішило під час реалізації цього одного з найбі-

[1] Крупнейшая в мире база биометрических данных создана в ОАЭ // BIOMETRICS.RU. – 2012. – 17 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрические модули предприятия «Системы Папилон» // Exponet.ru. – 2006. [Электронный ресурс]. – Режим доступа: http://www.exponet.ru/exhibitions/...

[3] Научный совет Федеральной миграционной службы будет содействовать становлению системы биометрических паспортов // ФМС России. – 2007. – 1 ноября. [Электронный ресурс]. – Режим доступа: http://www.fms.gov.ru..., http://biometrics.ru/; Сирык В. Не ущемлять интересы российских граждан / В. Сирык // Земляки. – 2007. – № 10. – 16 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[4] Бороган Ирина. Тотальный контроль: западный опыт / Ирина Бороган // Ежедневный журнал. – 2009. – 1 декабря. [Эhttp://www.agentura. ru/press/about/...лектронный ресурс]. – Режим доступа: http://www.agentura.ru/press/about/...

льших у світі проектів сканувати та зберігати у БД електронні відомості щодо трьох різних біометричних параметрів кожного мешканця країни.

Рішення про сканування всіх 10 пальців рук, райдужної оболонки обох очей та отримання оцифрованого зображення обличчя кожного громадянина було ухвалено після того, як експерти проаналізували якість чверті мільйона відбитків пальців, зібраних у мешканців різних регіонів Індії. Під час ухвалення рішення брався до уваги той факт, що найбільша база біометричних даних, яка була сформована ФБР у першому десятиріччі XXI століття і яка охоплювала відомості про відбитки пальців на 50 млн чоловік, забезпечувала безпомилкову ідентифікацію в 99 випадках із кожних ста.

Непіддаючи сумніву відомості про 99-відсоткову точність технологій ідентифікації за відбитками пальців, індійські експерти вирішили все ж таки підстрахуватися та використати також дані про райдужну оболонку очей і фотозображення осіб. Необхідність уведення додаткових ідентифікаторів фахівці UID Authority of India пояснили такими міркуваннями.

По-перше, невідомо, як буде поводитися база біометричних даних на 600 млн чоловік порівняно зі своєю 50-мільйонною «сестрою», тому резервні ідентифікатори вводяться з метою забезпечення масштабування нової індійської біометричної бази даних.

По-друге, регіони Індії значно різняться за складом населення і за кліматичними умовами, тому введення додаткових біометричних ідентифікаторів повинні зменшити викликані цими факторами проблеми, якщо вони будуть виявлені під час здійснення такого значного за кількістю біометричних даних проекту[1].

Програма з присвоєння індійським громадянам ідентифікаційних номерів одержала назву «Aadhar» (у перекладі з хінді – «система»). Під час реалізації проекту «Aadhaar» планується надати унікальні 12-чисельні номери понад мільярду індійських громадян, які поки що в більшості не мають жодних документів, які б засвідчували їх особистість.

За твердженням керівника національного проекту UIDAI Нандана Нилекани (Nandan Nilekani): «Індія стане власником найбільшої у світі бази біометричних даних, яка перевершує за своїми розмірами біометричні бази даних ФБР і програми US-VISIT». Американська візова програма US-VISIT на середину 2012 року мала у своєму розпорядженні відомості про 120 млн здобувачів віз. Тоді, як у базі UIDAI всього за два роки її існування було зареєстровано приблизно 200 млн громадян. У підсумку в базі архівних даних заплановано зібрати понад 12 млрд відбитків пальців, 2,4 млрд «сканів» райдужної оболонки ока та 1,2 млрд фотозображень.

Більшість існуючих у світі біометричних баз даних проводять одну перевірку на наявність дублікатів. У проекті «Aadhar» під час внесення даних ця процедура проводиться кожного разу три рази, що практично повністю унеможливлює внесення в базу двох записів про одну людину. «Подібна точність є критично важливою умовою для країни з найвищим рівнем міграції населення, у якій загальний обсяг виплачуваних державою соціальних допомог перевищує 60 мільярдів доларів, – пояснює Ашок Далвай (Ashok Dalwai), заступник генерального директора UID Authority of India».

Через відсутність посвідчень особистості безліч нужденних індійців не мають доступу до програм соціального забезпечення. Водночас у країні налічується безліч

[1] Индия. При присвоении гражданам идентификационных номеров будут использоваться сведения о различных биометрических идентификаторах // BIOMETRICS.RU. – 2010. – 19 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

шахраїв, які наживаються на посередницькій діяльності або одержують незаконну допомогу з використанням фальшивих посвідчень. Нова технологічна програма дозволить припинити ці шахрайські дії[1].

Одночасно з «Aadhar» в Індії формується Національний регістр населення (National Population Register – NPR). Формування NPR здійснюють два відомства – Генеральний регістр і Бюро з перепису населення. Цим проектом заплановано охопити всіх індійських громадян, а щоб не вносити повторно в Національний регістр відомостей про одну й ту ж людину, в кожного з учасників перепису сканують біометричні ідентифікатори. Представники влади заявляють, що «Aadhar» і NPR не дублюють один одного, а, навпаки, обмінюються отриманими під час реалізації кожної з програм відомостями[2].

Резервний банк Індії (Reserve Bank of India – RBI), який виконує функції центрального банку країни, зазначив необхідність активізувати використання біометричних технологій кредитними організаціями. На думку RBI, згадані технології дозволять суттєво підвищити рівень безпеки транзакцій, здійснюваних за допомогою платіжних карт у банкоматах і за допомогою POS-терміналів[3].

Що стосується наявності найбільшого у світі національного біометричного проекту, то у 2009 році суперечку з Індією вів Пакистан. За словами заступника керівника Національного реєстраційного агентства Пакистану (National Database Registration Authority – NADRA) Таріка Малика: «Пакистан випереджає США та Індію в застосуванні технологій біометричної ідентифікації. Багато аспектів життя пакистанських громадян залежать від здатності NADRA ефективно і безпечно їх ідентифікувати»[4].

На початок четвертого кварталу 2012 року 96% дорослих жителів Пакистану пройшли біометричну ідентифікацію. Цю заяву зробив прес-секретар Національного реєстраційного агентства. Після проходження біометричної ідентифікації пакистанці одержують національні ідентифікаційні карти, придатні для комп'ютерної обробки (Computerized National Identity Card – CNIC); у чіпі карти зберігаються основні персональні дані її власника, цифрове фотозображення його обличчя та відомості про відбитки пальців[5].

Узагальнюючи наведене, можна зробити висновок, що на початку другого десятиріччя XXI століття зусилля найрозвинутіших світових держав у галузі біометрії зосереджені на вирішенні двох таких основних завдань:

– створенні таких ідентифікаційних систем правоохоронних і спеціальних структур, для яких можливість взаємообміну з базами даних спеціальних відомств будь-яких країн світу повинно бути невід'ємною складовою роботи;

– запровадженні уніфікованих багатомодельних мультибіометричних технологій ідентифікації людей для потреб різних державних структур, насамперед правоохоронних.

---

[1] Индия: новые подробности о крупнейшем в мире биометрическом проекте // СОФТ@Mail.Ru. – 2012. – 7 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Президент Индии прошла биометрическую идентификацию // BIOMETRICS.RU. – 2012. – 11 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Центральный банк Индии призвал активнее применять биометрические технологии // BIOMETRICS.RU. – 2012. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Пакистан лидирует в применении биометрических технологий // BIOMETRICS.RU. – 2009. – 10 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[5] Пакистан. 96% взрослых граждан прошли биометрическую идентификацию // BIOMETRICS.RU. – 2012. – 5 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Не можна обминути увагою плани Інтерполу. Для підвищення ефективності боротьби зі злочинністю та тероризмом фахівці Міжнародної поліцейської організації вважають за необхідне створення глобальної бази біометричних даних. Планується, що в майбутню глобальну біометричну БД Інтерполу вноситимуться папілярні узори пальців, ДНК і фізіономічні дані осіб, які обґрунтовано підозрюються у злочинній діяльності. Вся ця інформація повинна бути доступною для правоохоронних органів всіх країн-учасниць Інтерполу, а також і для їх прикордонних служб.

У міжнародному поліцейському відомстві ще у 2008 році вважали, що за допомогою сучасної загальносвітової бази даних фотозображень можна буде значно підвищити ефективність боротьби зі злочинністю та міжнародним тероризмом. За оцінкою Інтерполу, щорічно на планеті понад 800 млн осіб сідають на борти літаків, водночас немає будь-якої статистикаи про те, яка кількість пасажирів проходить на авіарейси за підробленими документами або нелегально перетинають кордони держав, некажучи про відомості щодо осіб, які підозрюються у причетності до вчинення злочинів і мандрують з одних країн до інших. Інтерпол має намір лобіювати ухвалення міжнародного закону про дозвіл міграційним органам робити цифрові знімки пасажирів і в режимі реального часу здійснювати їх перевірку за національними та міжнародними кримінальними базами даних[1].

Нині на порядку денному Інтерполу, Європолу та національних правоохоронних органів більшості держав світу є питання про нагальну потребу створення системи уніфікованого доступу й обміну даними між біометричними базами даних усіх країн світової спільноти. Підсумовуючи вищевикладену інформацію, слід зауважити, що темпи впровадження та розвитку будь-яких інформаційних систем визначаються економічною ситуацією в державі. І тут необхідно констатувати, що Україна істотно відстає у застосуванні біометричних технологій від інших країн.

Єдиним досягненням нашої держави є ухвалення 20 листопада 2012 року Закону України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус».

Відповідно до цього Закону, в нашій країні передбачається створення інформаційно-комунікативної системи з базою даних українців і осіб без громадянства, а також видача низки біометричних ідентифікуючих документів з електронним чіпом.

Створення національної системи біометричної верифікації та ідентифікації громадян України, іноземців та осіб без громадянства та запровадження комплексу заходів, пов’язаних із паспортно-візовими документами нового покоління, є одним із заходів, що наближають нашу державу до інноваційного рівня більшості країн світової спільноти.

Нині розгортання національних компонентів біометричних систем і захищеної інфраструктури обміну даними і на державному, і міждержавному рівнях є суттєвою частиною заходів боротьби з міжнародним тероризмом і значною складовою національної безпеки будь-якої розвинутої країни світу. Міжнародні експерти передбачають, що в 2010–2020 роках більшість населення держав світу в тому чи іншому вигляді буде охоплено біометричними паспортно-візовими документами нового покоління, що сприятиме пришвидшеному проходженню через державні кордони подорожуючих та підвищенню безпеки країн і насамперед їх основних транспортних вузлів. Між біометричними базами даних правоохоронних органів більшості держав буде налагоджений уніфікований взаємообмін даними у режимі реального часу за допомогою захищених телекомунікаційних каналів зв’язку.

[1] Интерпол планирует создать глобальную базу биометрических данных авиапассажиров // CyberSecurity.ru. – 2008. – 23 октября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Розділ 13

ОСНОВНІ КРИМІНОГЕННІ ПРОБЛЕМИ СВІТОВОЇ СПІЛЬНОТИ ТА ВИКОРИСТАННЯ СИЛОВИМИ СТРУКТУРАМИ КРАЇН СВІТУ ІНФОРМАЦІЙНО-БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ ДЛЯ ЇХ ВИРІШЕННЯ

Масштабні проекти з використанням біометричних технологій вже реалізували та продовжують їх удосконалювати практично всі розвинені країни світу. До цього їх уряди спонукає потреба забезпечення безпеки. У сучасному світі застосування досягнень біометрії є одним із найважливіших умов ефективної боротьби зі злочинами проти безпеки держави й основ політичного устрою та конституційних прав громадян, а також з іншими видами протиправних дій.

Основні завдання, вирішення яких переважно забезпечуються за допомогою сучасних досягнень біометрії:

1. *У сфері забезпечення безпеки держави:*

– надійне посвідчення будь-якої особистості під час перетину кордону країни за допомогою проведення ідентифікаційних заходів за унікальними біометричними ознаками;

– боротьба з незаконною міграцією, тероризмом, міжнародною організованою злочинністю, наркоторгівлею, злочинами у фінансовій сфері тощо.

2. *У внутрішньодержавній діяльності правоохоронних органів:* достовірна ідентифікація осіб, які підозрюються у вчиненні злочинів, інших категорій кримінальних елементів за їх унікальними біометричними ознаками[1].

Необхідно підкреслити, що в другому десятиріччі XXI століття чітко простежується тенденція використання у державних системах ідентифікації або верифікації застосування мультибіометричних технологій.

Історично склалося так, що першими почали використовувати біометрію правоохоронні органи. Нині державні силові структури більшості країн світу продовжують інтенсифікувати використання біометричних технологій.

Біометрична ідентифікація має беззаперечну істотну перевагу над іншими ідентифікаційними технологіями, яка полягає у тому, що під час застосування мультибіометричних технологій у комплексі з деякими іншими інноваційними рішеннями практично повністю унеможливлюється використання зловмисниками фальшивих документів.

За допомогою біометричної ідентифікації правоохоронні органи та спецслужби провідних світових країн виконують такі завдання:

– проведення однозначної та достовірної ідентифікації за унікальними біометричними параметрами кримінальних елементів та осіб, які підозрюються у вчиненні злочинів;

[1] Biolink.ru. [Электронный ресурс]. – Режим доступа: http://biolink.ru/solutions/markets/...

– оперативне встановлення особистості затриманих під час проведення заходів з охорони громадського порядку, зокрема й при забезпеченні безпеки проведення різних масових заходів;

– посилення паспортно-візового контролю на кордонах для боротьби з нелегальною міграцією;

– запобігання доступу в державні, муніципальні та інші установи осіб, які не мають на це право;

– організація системи контролю за доступом на територію та приміщення різних спецустанов, режимних об'єктів, аеропортів, морських портів і залізничних вокзалів;

– перевірка претендентів на отримання роботи у правоохоронних і силових органах, різних охоронних структурах, осіб, які подали заяви на отримання дозволу на придбання вогнепальної зброї, здобувачів віз тощо;

– ідентифікація громадян, які перебувають у зонах виникнення надзвичайних ситуацій (регіони, що постраждали внаслідок землетрусу, повені, тайфуну, техногенної катастрофи і т. д.) і не мають при собі документів, які засвідчують особистість (наприклад, для запобігання шахрайств, пов'язаних з одержанням допомоги особами, які вже її отримали і повторно звертаються за наданням цієї державної послуги під іншими установчими даними);

– оперативне впізнання недієздатних осіб, а також осіб, що перебувають у безпорадному стані та нездатні повідомити про себе будь-які відомості;

– можливість впізнання виявлених неідентифікованих трупів[1].

Процес глобалізації, який пришвидшився наприкінці минулого сторіччя та серйозно змінив світ, став каталізатором стрімкого розвитку міжнародної організованої злочинності. Це негативне явище прогресує і в XXI столітті. «Прозорість» кордонів, розширення можливостей інтернет-технологій і, відповідно, спрощення обміну інформацією, безпрецедентне зростання обсягів міжнародної торгівлі та інвестицій, і, як наслідок, вільне переміщення бізнесменів і робочої сили призвело до втрати владними структурами будь-якої держави низки специфічних важелів управління, які раніше дозволяли протистояти експансії міжнародного криміналітету.

Згідно зі статистикою, злочинність у світі за останні кілька десятиліть збільшилася в 4 рази, зокрема на території колишнього СРСР і в США – у 8 разів, у Великобританії і Швеції – у 7 разів, у Франції – у 6 разів, у Німеччині – в 4 рази. За даними ООН, злочинність у світі в кінці 90-х років у середньому збільшувалась на 5% в рік, а приріст населения – на 1%. 2001 року на планеті офіційно було зареєстровано близько 450 млн злочинів, а їх фактична кількість може бути втричі більшою. Чим взаємопов'язанішим стає світ, тим він є більш взаємовразливим. Глобалізація соціальних та економічних процесів призвела до глобалізації злочинності, яка стає дедалі більш організованою, транснаціональною і витонченою. Злочинні співтовариства набагато швидше, ніж державні системи різних країн, реагують на розвиток усіх видів комунікацій, на будь-які пом'якшення прикордонного контролю і полегшення пересувань[2].

Транснаціональним злочинним синдикатам за допомогою корупції, шантажу та погроз вдається сповна використовувати для досягнення своєї злочинної мети всі переваги, що дає сучасне суспільство та відкриті ринки демократичних країн. Основний

[1] Силовые структуры и биометрия. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/markets/...

[2] Гуров А. XXI століття проти глобалізації злочинності / А. Гуров, Н. Ковальов, А. Куліков // Всесвітній Антикримінальний і Антитерористичний Форум. – 2006. – 3 листопада. [Електронний ресурс]. – Режим доступу: http://www.waaf.ru/index_ru...

робочий принцип транснаціональних злочинних угруповань полягає у нейтралізації здійснення контролю правоохоронними органами. Території з іноземною юрисдикцією стають безпечними для заняття злочинною діяльністю на теренах інших держав, а існуючі кордони слугують міжнародним злочинцям «огорожею», за якою вони намагаються вберегтися від національного законодавства країн, де вони здійснюють свою злочинну діяльність.

Протистояння державних і організованих злочинних структур триває не одну сотню років. В енциклопедії Міжнародної Організованої Злочинності «The Encyclopedia Of International Organized Crime» наводяться факти про те, що злочинні угруповання існували ще в часи Римської імперії. Вже тоді вони становили велику проблему для держави, оскільки намагалися контролювати найбільш прибуткові сфери економіки.

Майкл Вудівісс (Michael Woodiwiss), автор книги «Організована Злочинність і Американська Міць: Історія» (Organized Crime and American Power: A History), наводить факти про те, що організована злочинність завжди діяла, нехтуючи державними кордонами. В 30-ті роки минулого століття італійські мафіозі їздили до Японії та Китаю за наркотиками, японська «якудза» діяла на території Сполучених Штатів Америки, а члени американських банд ховалися від правосуддя у Китаї та Європі.

Кримінолог Джеффрі Робінсон, автор книги «Злиття: Конгломерація Міжнародної Організованої Злочинності» (The Merger: The Conglomeration of International Organized Crime), стверджує, що злочинність нині не є лише національною проблемою, а перетворилася на проблему всього людства: «Нездатність сучасного суспільства протидіяти організованій злочинності може стати такою ж доленосною проблемою XXI століття, як холодна війна була проблемою століття XX, а колоніалізм – XIX століття». За оцінкою Д. Робінсона, виявлення та нейтралізація груп міжнародної організованої злочинності ускладнюється тим, що ці угруповання використовують законні бізнес-структури для прикриття своєї діяльності. Іноді злочинна організація лише оперує всередині великої корпорації, а інколи – фактично контролює її. Часто буває складно провести межу між злочинною діяльністю «білих комірців» або корпорацій і діями кримінальних співтовариств.

Федеральне бюро розслідувань (ФБР) вважає, що існують три основні види корпорацій, які пов’язані зі злочинною діяльністю: по-перше, це незаконні бізнес-структури, які з самого початку займаються нелегальною діяльністю, наприклад, торгівлею наркотиками; по-друге, це легітимні фірми, що скоюють службові злочини, такі, як «відмивання грошей» і, по-третє, це легально працюючі підприємства, які повністю або частково були створені на доходи, що були отримані внаслідок протиправних дій організованої злочинності. Отже, міжнародна злочинність становить реальну загрозу для фінансових систем і окремих держав, і всього світового товариства. Але це ще не все. Криміналітет здійснює свій вплив на політику. Вважається, що італійські й японські злочинні співтовариства одними із перших почали вкладати «відмиті» гроші та використовувати підконтрольні їм бізнес-структури для підтримки своїх людей у структурах влади. В США мафія традиційно здійснює контроль над впливовими профспілками. Багато південноамериканських наркокартелів спонсорують «своїх» політиків і навіть деякі терористичні структури для організації тиску на владу та захисту свого бізнесу.

Економіст Раджів Нейлор, автор дослідження «Злочинні Доходи: Чорні Ринки, Нелегальні Фінанси і Підпільна Економіка» (Wages of Crime: Black Markets, Illegal Finance, and the Underworld Economy), стверджує, що міжнародна організована злочинність «глобалізувала» свою діяльність унаслідок тих же причин, що і законослухняні транснаціональні корпорації. На думку Р. Нейлора, зростанню незаконної

транснаціональної діяльності сприяли технічні досягнення минулого століття: бурхливий розвиток авіації, телекомунікацій та міжнародної торгівлі. *Злочинні угруповання скористалися зменшенням державного регулювання в економічній діяльності й ослабленням прикордонного контролю*.

Транснаціональні злочинні угруповання швидко знаходять і з максимальною ефективністю використовують існуючі прогалини у державних правових системах для розширення своєї діяльності.

Вони осідають у тих місцях земної кулі, звідки не можуть бути екстрадовані, створюють опорні бази в державах із неефективною правоохоронною діяльністю й відмивають гроші в країнах, де не чітко дотримуються банківської таємниці або немає ефективного контролю за фінансовими структурами[1].

Організована злочинність охоплює такі надприбуткові види протиправної діяльності, як міжнародна торгівля наркотиками, зброєю та людьми. Нині організовані міжнародні злочинні групи отримують свою частку прибутку від нелегальної міграції, чим доводять свою підприємницьку хватку. Часто проникнення на територію інших країн здійснюється за допомогою фальшивих документів, що є серйозним викликом для правоохоронних органів[2].

Нині інформаційні системи автоматичної мультибіометричної ідентифікації більш інтенсивно використовуються для захисту інтересів суспільства і держав (введення паспортно-візових документів нового покоління, протидія тероризму, злочинності у всіх її видах, нелегальній міграції), забезпечення безпеки крупних інфраструктурних і транспортних об’єктів (аеропорти, порти, атомні й гідроелектричні станції тощо), а останнім часом спостерігається пришвидшене впровадження біометричних технологій у системи масового обслуговування (найпоширеніші сфери застосування: програми надання сприяння авіапасажирам, які часто подорожують, забезпечення онлайнових фінансових і платіжних транзакцій).

Наведемо загальновідомі етапи проведення ідентифікації за допомогою біометричних технологій:

– *реєстрація* біометричного/их/ ідентифікатора/ів/ індивідуума – дані про фізіологічну або поведінкову характеристику перетворюють в електронну форму, яка доступна комп’ютерним технологіям, і вносять до пам’яті відповідних біометричних пристроїв або систем;

– *виділення* – з пред’явленого під час проведення контролю ідентифікатора/ів/ виділяють індивідуальні унікальні ознаки, які піддають подальшому програмно-системному аналізу;

– *порівняння* – зіставлення електронних шаблонів знов пред’явленого/их/ та раніше зареєстрованого/их/ ідентифікаторів;

– *ухвалення рішення* – винесення висновку про збіг або незбігання знов пред’явленого/их/ та раніше зареєстрованого/их/ ідентифікаторів.

Висновок про збіг або незбігання ідентифікаторів за необхідності може транслюватися іншим програмно-апаратним складовим використовуваних біометричних систем (контролю за доступом, програмно-апаратним пристроям захисту інформації тощо), які проводять наперед визначені дії на основі отриманої інформації.

---

[1] Процесс глобализации сопровождается бурным развитием международной организованной преступности // Washprofile.org/ru. – 2008. – 30 октября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/...

[2] Преступность в контексте миграционных процессов // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 13–22.

Нагадаємо ще раз, що використання біометричних технологій у діяльності правоохоронних органів і «цивільних» системах має низку принципових відмінностей. Основна відмінність полягає у тому, що «цивільні» системи оперують не безпосередньо біометричними ідентифікаторами (зображеннями відбитків пальців або райдужної оболонки ока, оцифрованих фотографій індивідуумів т. ін.), а їх цифровими шаблонами – моделями, причому зворотнє відновлення реального ідентифікатора з його цифрового шаблону не можливе.

У такий спосіб гарантується захист персональних біометричних даних користувачів і забезпечується суттєве пришвидшення швидкості роботи «цивільних» біометричних систем – цифрові шаблони ідентифікаторів займають значно менший обсяг електронної пам'яті, ніж оригінали електронних зображень біометричних ідентифікаторів. Цей факт є дуже важливим під час обслуговування значної кількості користувачів.

У таблиці 8 наведено порівняльний аналіз застосування біометричних технологій у діяльності правоохоронних органів і системах цивільної ідентифікації. Деякі положення аналізу, що наводиться, характерні тільки для країн СНД, оскільки у США, державах ЄС та інших отримання відбитків пальців і долонь на папері, склі і подібних поверхнях вже не застосовується[1].

Таблиця 7

Порівняльний аналіз застосування біометричних технологій у діяльності правоохоронних органів і системах цивільної ідентифікації

Критерій	Правоохоронна діяльність	Цивільна ідентифікація
Характер реєстрації	Обов'язкова (для певних соціальних груп)	Добровільна (за бажанням користувача)
Використовувані ідентифікатори	Відбитки пальців (як правило, всіх десяти), долонь, фотографій	Відбитки пальців (одного–двох, рідко більше), райдужна оболонка ока, обличчя, малюнок вен, геометрія кисті руки тощо
Спосіб отримання ідентифікаторів	Шляхом електронного сканування або відтиснення відбитків на папері, склі та інших подібних поверхнях (відтисненя – тільки у деяких країнах, зокрема СНД)	Виключно шляхом електронного сканування
Дії з ідентифікаторами	Реальні зображення зберігаються в оцифрованому вигляді або на дактокартах (оброблятися можуть і самі ідентифікатори, і шаблони для пришвидшення швидкодії пошуку)	Обробляються не самі ідентифікатори, а їх цифрові моделі (шаблони)
Можливість отримання оригіналу ідентифікатора з бази даних	Існує	Відсутня: відновити ідентифікатор із його моделі неможливо

[1] Общая характеристика биометрических технологий. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/technology/biometric...

Продовження таблиці 8

Критерій	Правоохоронна діяльність	Цивільна ідентифікація
Обробка ідентифікаторів	Здійснюється в два етапи: спочатку в автоматизованому режимі відбираються подібні до того взірця, що перевіряється; потім відібрані ідентифікатори аналізує та порівнює експерт	Здійснюється автоматично в режимі «один до багатьох» або «один до одного»
Вимоги до кваліфікації персоналу	Необхідне залучення висококваліфікованих фахівців	Мінімальні: достатньо базових навичок роботи з комп'ютером
Кількість транзакцій	Від декількох сотень до сотень тисяч у тиждень (для загальнонаціональних систем)	Десятки тисяч у день (для великих систем)
Кількість стаціонарних пунктів роботи з даними	Від десятків до декількох сотень	Від одиниць до декількох тисяч
Масштаб	Визначається чисельністю представників певних груп, які підлягають обов'язковій реєстрації	Коливається в широких діапазонах – від невеликих систем (десятки або сотні осіб) до реєстрації всього дорослого населення країни
Сфери застосування	Обмежені й охоплюють реєстрацію представників окремих прошарків суспільства з метою боротьби зі злочинністю, тероризмом, нелегальною міграцією	Різноманітні та охоплюють: ідентифікацію виборців, користувачів послуг транспортних підприємств, клієнтів фінансових, соціальних, медичних, культурних, спортивних, розважальних установ і низки інших сфер

Компетентні органи особливо цікавлять можливості прихованої дистанційної ідентифікації людини без її відома. Вирішити це завдання можливо досить просто за допомогою запровадження документів із мікрочіпами радіочастотної ідентифікації. Але в принципі будь-який громадянин зможе контролювати свій документ і блокувати RFID випромінювання чохлом-екраном за відсутності необхідності його використання за призначенням. А за дистанційної ідентифікації суб'єкта за його обличчям і особливостями його рухів така можливість стає реальністю, от чому до цієї технології нині є така підвищена увага.

Нині під час масових заходів фігуранти цих дій дуже часто приховують свої обличчя та форму голови за різними масками та капюшонами, тому зараз посилено ведуться дослідні роботи з можливості дистанційної ідентифікації за особливостями рухів (ходи) та жестів людини.

У липні 2011 року біометричний інститут, що діє в Австралії і Новій Зеландії, опублікував результати чергового щорічного опитування, яке він проводить серед своїх членів. Учасники опитування визначили, що новинкою у галузі в майбутньому стане біометрична ідентифікація користувачів, які перебувають у русі; ще одним найважливішим завданням респонденти вважають розвиток мультибіометричних систем, а також підвищення ефективності інтеграції біометрії та інших інноваційних технологій[1].

[1] Опубликованы результаты очередного опроса по биометрии // BIOMETRICS.RU. – 2011. – 11 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

На замовлення спецслужб у багатьох країнах продовжують інтенсивно виконувати роботи з приведення так званої технології «дистанційного розпізнавання» за обличчям до розряду «зрілих» технологій. Практична реалізація цього завдання з поєднанням низки інших інноваційних технологій дозволить на практиці реалізувати ідею тотального автоматизованого контролю за всіма переміщеннями і контактами громадян, якими цікавляться правоохоронні структури. З середини 1990-х років саме цю модель спецслужби і намагаються у різних варіантах втілити в життя.

Як приклад системи «дистанційного розпізнавання» можно навести відомості про «Біометричну систему для дистанційного оптичного спостереження» («Biometric Optical Surveillance System /BOSS/ at Stand-off Distance»). Біометрична система BOSS розробляється в США на замовлення Департаменту з національної безпеки (Department of Homeland Security /DHS/). У технічному завданні зазначена вимога, що програмне забезпечення системи «дистанційного розпізнавання» має формувати електронний зразок та ідентифікувати особистість фігуранта за тривимірною біометричною сигнатурою обличчя на відстанях до 100 метрів.

Хоча терміни розробки минули ще у 2012 році, роботи з доведення системи BOSS до кондиції продовжували виконуватися і протягом 2013 року. Головним виконавцем робіт є фірма «Electronic Warfare Associates», яка знаходиться в штаті Кентуккі.

Практично всі експерти з біометрії свідчать, що подібні системи «прийшли, щоб залишитися». У деяких ситуаціях вони сьогодні досить ефективно працюють, але в реальних умовах, коли «об'єкт не співробітничає», виникають ускладнення[1].

Останнім часом у різних засобах масової інформації більше з'являється повідомлень про розробку біометричних систем із використанням «глобальних» баз даних на фігурантів. У ці масштабні корпоративні рішення інтегрують усі останні досягнення у сфері технологій біометричної ідентифікації та контролю за радіотелекомунікаційним зв'язком. За повідомленнями британських ЗМІ, в проекті створення всесвітнього банку даних, що отримав кодову назву «Server in the Sky» («Сервер у небі»), окрім ФБР США, беруть участь правоохоронні органи Великобританії, Канади, Австралії та Нової Зеландії. Представники цих країн увійшли до робочої групи, що отримала назву Міжнародний інформаційний консорціум (International Information Consortium), а ФБР взяло на себе загальне керівництво цим проектом. Офіційний представник ФБР в інтерв'ю британській газеті «The Telegraph» у 2008 році заявляв, що «Server in the Sky», відповідно до планів його творців, повинен забезпечувати обмін біометричними даними між країнами – учасницями проекту, дозволяючи оперативно отримувати інформацію про осіб, що становлять оперативний інтерес[2].

Разом із програмою «Server in the Sky» ще одним прикладом «глобальної» бази даних на фігурантів може слугувати мультибіометрична система Department of Defense Automated Biometric Identification System (Dod ABIS), яку експлуатує Міністерство оборони (Department of Defense) США.

Розширені функції Dod ABIS допомагають армійським підрозділам Пентагону, які виконують оперативні завдання в конфліктних місцях земної кулі, ефективно вирішувати завдання ідентифікації. До цих завдань належать встановлення за біометричними

[1] Технологии биометрической идентификации по лицу могут повысить свою эффективность // DGL.RU. – 2013. – 2 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] ФБР привлекает другие страны к формированию гигантской базы биометрических данных // BIOMETRICS.RU. – 2008. – 16 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

ідентифікаторами особистостей фізичних індивідуумів, які були заарештовані або затримані в зонах конфліктів, а також використання біометрики в системах контролю фізичного доступу на американські військові бази за кордоном[1].

Американське ФБР здійснює комплекс заходів, які спрямовані на модернізацію та формування гігантської «системи біометричної ідентифікації нового покоління» (next generation identification system /NGI/). На ці заходи виділено 1 млрд доларів США, а створення мультибіометричної системи NGI у «пілотному режимі» повинно завершитися до 2014 року[2].

У лютому 2008 року дослідницькою корпорацією «RAND» на замовлення Пентагону було проведено дослідження про те, наскільки Сполучені Штати Америки готові протистояти терористичним виявам і насамперед можливим діям ісламських терористів. Головний висновок доповіді «Війна іншими засобами» (War by Other Means) – нині ісламському екстремізму протистояти дуже складно, він і надалі є однією з найсерйозніших загроз безпеці США. І в перспективі ця загроза тільки зростатиме. У доповіді також вказується, що ісламізм, який існує в різних країнах мусульманського світу, під впливом радикальних ідей активніше застосовує насильство та відмову від будь-яких компромісів. Подібні радикальні рухи складно знищити, а їх ідеї, практика дій і організаційна структура мають тенденцію до поширення та копіювання. Основний висновок доповіді: для досягнення успіху в глобальній війні з ісламськими екстремістами Сполучені Штати Америки повинні більшою мірою спиратися не на військових, а на цивільних фахівців. Міжнародна співпраця в цій сфері не просто бажана, а життєво необхідна.

Історія довела, що великомасштабні військові інтервенції (наприклад, Франції в Індокитаї та Алжирі, США у В'єтнамі, СРСР і США в Афганістані та низки інших) найчастіше не досягають успіху. Відповідно до висновків авторів доповіді «Війна іншими засобами» пріоритетами Сполучених Штатів Америки повинні стати підвищення якості національних урядів, зміцнення місцевих сил безпеки та поліпшення інформаційних можливостей. В Іраку й Афганістані керівництвом США свого часу ці принципи належно не були враховані[3].

За висновком експертів із проблем безпеки, однією з найістотніших проблем XXI століття разом із тероризмом є проблема незаконної міграції. Незаконна міграція, як і тероризм, організована злочинність, наркотрафік, нині є однією з серйозних загроз національній безпеці будь-якої держави.

Масштаби міжнародної міграції безперервно зростають. За даними Держдепартаменту США в 2005 році загальна кількість мігрантів становила близько 192 млн, а на початок 2013 року – майже 214 млн чоловік[4].

2012 року кількість безробітних в усьому світі становила 197 млн чоловік. Зазначимо, що за 2008–2012 роки їх кількість збільшилася на 53 млн. За прогнозами Міжнародної організації праці, в 2013 році безробітних стане більше ще на 5 млн осіб, а в 2014-му –

---

[1] Пентагон наращивает применение биометрии // BIOMETRICS.RU (по материалам Специальной комиссии армии США по биометрии). – 2009. – 10 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...; Пентагон продолжит развивать свою биометрическую систему // BIOMETRICS.RU. – 2011. – 30 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] ФБР расширит использование биометрических технологий // BIOMETRICS.RU. – 2012. – 4 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Лекарство от инсургентов // Washprofile.org/ru. – 2008. – 14 февраля. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

[4] Демография мира // Washprofile.org/ru. – 2009. – 12 февраля. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

показник збільшиться ще на 3 млн і має сягти цифри у 205 млн безробітних. Отже, всі ці люди є потенційними мігрантами, будуть прагнути шукати роботу за межами рідної країни. В Україні, за експертними оцінками, перебуває від 5 до 7 млн мігрантів із різними статусами[1].

За даними президента фонду «Міграція XXI вік» В'ячеслава Поставніна (колишнього заступника директора Федеральної міграційної служби), в Росії у 2012 році перебувало понад 10 млн мігрантів (за іншими джерелами – до 13 млн), з яких близько 4 млн знаходились у Москві та Московській області. Загалом у Росії вже майже 8–9% наявного в країні постійного населення – це мігранти. 1 вересня 2012 року в московські школи прийняли 83 тис. першокласників, у них від 4 до 10% (дані різних джерел відрізняються) батьки є мігрантами[2].

Інтернаціоналізація економіки, лібералізація, розвиток транспортних і комунікаційних технологій зумовили посилення мобільності всіх ресурсів людського розвитку: капіталу, товарів, технологій, інформації, людей. Міграція праці перетворилася на невід'ємну складову світової економіки. На початок XXI століття в світі налічувалися 36–42 млн трудових мігрантів, з членами сімей їх кількість сягала 80–97 млн чоловік, а за деякими оцінками – навіть 120 млн. Тенденції сьогодення такі, що кількість трудових мігрантів збільшується й у найближчі роки буде лише невпинно зростати.

Зі зростанням динаміки переміщення трудових ресурсів сучасного світу зростають і розвиваються можливості техніки маніпулювання ними. Маніпулювання мігрантськими ресурсами перетворилося на один із видів сучасного високоприбуткового бізнесу. Проте світовій спільноті у боротьбі з незаконною міграцією протистоять не стільки самі мігранти, як глобальна структурна мережа, в яку входять і працедавці, і кримінальні угруповування, що діють на територіях приймаючих держав, країн джерел міграції та країн транзиту мігрантів, зокрема і в державах колишнього СРСР. Канали незаконної міграції часто збігаються з каналами наркотрафіку та нелегальної торгівлі зброєю. Крім того, нелегальна міграція є поживним середовищем для розвитку тіньової економіки, а осіб, які нелегально перебувають на території країни, легко залучити до діяльності злочинних організацій, оскільки вони практично позбавлені легальних можливостей отримування коштів для існування. За статистичними даними у структурі загальної злочинності багатьох держав світу досить суттєву частку становлять злочини, що вчиняються іноземними громадянами й особами без громадянства[3].

Крім Сполучених Штатів Америки, питаннями імміграційної політики та нелегальної міграції стурбовані всі найбільш розвинені в економічному плані західноєвропейські країни, особливо такі, як Франція, Німеччина, Італія й Іспанія, де одні з найвищих імміграційних коефіцієнтів у Європі. В умовах недостатньої асиміляції наплив іммігрантів уже став для багатьох держав Європейського Союзу «обоюдогострою зброєю», оскільки, з одного боку, приїжджі є для багатьох країн основним джерелом робочої сили, а з іншого – становлять потенційну загрозу суспільній стабільності та національній безпеці[4].

---

[1] Американцы отказались от термина «нелегальный иммигрант» // Багнет. – 2013. – 4 апреля. [Электронный ресурс]. – Режим доступа: http://www.bagnet.org/news/...

[2] Самсонов Александр. «Сирийский сценарий» для России. Угроза национальной безопасности со стороны «новых варваров» / Александр Самсонов // Военное обозрение. – 2012. – 29 сентября. [Электронный ресурс]. – Режим доступа: http://topwar.ru/.html

[3] Куликов В. Влияние миграции на экономическую безопасность / В. Куликов // Всемирный Антикриминальный и Антитеррористический Форум. – 2006. – 3 ноября. [Электронный ресурс]. – Режим доступа: http://www.waaf.ru/index...

[4] Европарламент одобрил новые правила о нелегальных иммигрантах в ЕС // Эксперт-центр. – 2008. – 18 июня. [Электронный ресурс]. – Режим доступа: http://www.expert.org.ua/statias...

В умовах світової фінансової кризи істотно зростають ризики того, що багато трудових мігрантів, залишившись без роботи, стануть злочинцями. Ніхто не може заперечувати той факт, що є прямий зв'язок між негативними наслідками світової кризи й ускладненням соціально-економічної обстановки в багатьох державах. Прагнення працедавців знизити витрати на наймання робочої сили призводить до різкого скорочення зайнятості, зокрема і в тих сферах економіки, де працюють іноземні громадяни. Негативний процес у сфері зайнятості впливає на зростання злочинів майнового характеру, що здійснюються іноземними працівниками.

За повідомленнями директора Федеральної міграційної служби Російської Федерації К. Ромодановського на третій Московській Міжнародній конференції «Світова спільнота проти глобалізації злочинності і тероризму», частка незаконної міграції, що охоплює незаконний перетин кордону, незаконне перебування на території Росії і незаконну трудову діяльність, становила 3% від загального обсягу злочинності, зареєстрованого у РФ за 10 місяців 2006 року, але темпи щорічного зростання таких злочинів становлять 5–7%[1].

За зведеннями московського управління Слідчого комітету при прокуратурі Російської Федерації, кількість злочинів за останні роки тільки сексуального характеру, скоєних приїжджими з інших країн, значно збільшилася. За даними статистики, кількість зґвалтувань у Москві в 2008 році збільшилася майже на 20%, або вдвічі більше, ніж за аналогічний період 2007 року. Водночас 70% таких злочинів учинено приїжджими. Майже 40% від кількості всіх зґвалтувань здійснили громадяни Узбекистану, далі йдуть громадяни Туркменії, Таджикистану та Киргизії. Загалом дві третини від кількості злочинів цієї категорії у Москві здійснюються вихідцями з країн колишнього СРСР.

Ще одним із суттєвих негативних моментів такої ситуації зі злочинністю в середовищі гастарбайтерів є те, що вона спричиняє збільшення екстремістських виявів із боку місцевих неонацистів[2].

Цікаві дані дослідження проведеного корпорацією «RAND», які засвідчили тенденцію, що нелегальні іммігранти, які мають досвід депортації із США, дедалі частіше стають постійними порушниками закону. Здійснений аналіз статистичних даних виявив, що нелегали, котрі у свій час були депортовані й які незаконно повернулися до Сполучених Штатів Америки, набагато частіше порушують закон, ніж інші незаконні іммігранти, що не мають досвіду депортації.

Загалом «хронічні» нелегали здійснюють близько двох третин від загальної кількості злочинів, що скоюються нелегальними мігрантами. 73% «хроніків» заарештовуються протягом року після їх звільнення з-під варти – для інших категорій іммігрантів, які підлягають депортації, цей показник не перевищує 32%. Автори проведеного дослідження зробили висновок, що «хронічні» нелегали становлять найбільшу небезпеку для суспільства – їх найскладніше затримати, оскільки вони мають навички та зв'язки, необхідні для ухилення від арешту, а ще складніше від них позбутися, тому що вони знаходять будь-яку можливість до повернення у країну нелегального перебування після депортації на батьківщину[3].

---

[1] Крамар В. Бороться нужно не с симптомами, а с причинами / В. Крамар // Военно-промышленный курьер. – 2006. – № 40 (156). – 18–24 октября. [Электронный ресурс]. – Режим доступа: http://www.waaf.ru/index_ru.

[2] Беленев Г. Москву ждут погромы, как в Париже? / Г. Беленев // Независимая газета. – 2008. – 21 ноября. [Электронный ресурс]. – Режим доступа: http://www.ng.ru/.html

[3] Круговорот нелегалов // Washprofile.org/ru. – 2008. – 8 сентября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

За повідомленням Центру досліджень імміграції (Center for Immigration Studies), за період із 2005 до 2007 року в США було заарештовано понад 8 тис. злочинців-іммігрантів, які входили до приблизно 700 банд і кримінальних угруповань. У доповіді констатується, що останніми роками спостерігається стрімке поширення злочинних угруповань у Сполучених Штатах Америки. Їх основою є особи, які перебувають у США незаконно. Наприклад, відоме угруповання MS-13 (назва є абревіатурою фрази іспанською мовою – «Сальвадорська мама» – «MS»), що діє практично у всіх штатах США та налічує приблизно 10 тис. бойовиків, за відомостями «Center for Immigration Studies» 60–90% із них – нелегали. 80% арештованих членів іммігрантських банд раніше на території США вчиняли тяжкі злочини (без урахування порушень візового законодавства), а 40% вчиняли такі насильницькі злочини, як вбивства, згвалтування та інші. Переважно подібні угруповування спеціалізуються на рекеті, викраденні, розбоях і грабіжницьких діях, торгівлі наркотиками, проституції та фальсифікації документів.

Серед наймогутніших злочинних співтовариств, створених іммігрантами, Центром досліджень імміграції Сполучених Штатів Америки також вказується «Вірменська Міць» (Armenian Power)[1].

Погроми у Франції в 2005 і в 2007 роках, події в італійському Мілані засвідчили: європейським країнам потрібні жорсткі імміграційні закони, оскільки криміногенність міграційних процесів і пов'язаних із ними явищ викликає особливе занепокоєння. Загрозу внутрішній безпеці становлять випадки, коли мігранти свідомо не хочуть інтегруватися в існуюче національне громадянське суспільство. Класичний приклад – Сполучене Королівство Великобританія. Тут помітно загострилися проблеми у взаєминах мігрантів та офіційних властей. Британці почали помічати кардинальні зміни у внутрішньому вигляді своєї країни. Дедалі частіше в Англії з'являються школи, де діти говорять різними мовами і не бажають засвоювати ази англійської. А ісламська експансія до Англії призвела до того, що більшість білошкірих робочих Англії почали підтримувати ультраправу Британську національну партію (БНП), голосувати за яку раніше вважалося непристойним явищем. Проте дедалі більше корінних мешканців Великобританії віддають свої голоси на виборах на її користь, тому що хочуть зберегти обличчя доброї старої Англії, в якій вони народилися.

Данією проїжджає велика кількість циган, які подорожують зі всім своїм майном, на сучасних автомобілях. Разом із ними «подорожують» і кримінальні методи існування циганського співтовариства: крадіжки, шахрайство, продаж наркотиків тощо. Громадяни Данії вже б'ють тривогу, проте офіційна влада поки що надала тільки інструкції для поліцейських і власних громадян, зміст яких зводиться в основному до попередження про небезпеку спілкування з циганами та циганками.

Влада США давно стурбована припливом нелегалів із Мексики та Китаю. Водночас, за повідомленнями мексиканської влади, близько 78% мексиканців, які прибули до США в період з 2001–2005 роки, потрапили на територію країни нелегально. Напочатку 2008 року кількість нелегальних мігрантів у США становила (залежно від методики підрахунку) від 5 до 20 млн чоловік (найчастіше фігурує цифра в 11–12 млн осіб). Водночас приблизно 7 млн нелегалів було залучено в економічно активну діяльність і вони складали конкуренцію місцевому населенню[2].

[1] Банды иммигрантов // Washprofile.org/ru. – 2008. – 2 октября. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

[2] Овчинский В. Экстремисты: от фашистов до экологов / В. Овчинский // Всемирный Антикриминальный и Антитеррористический Форум. – 2009. – 21 февраля. [Электронный ресурс]. – Режим доступа: http://www.waaf.ru/index_ru.

Наведені приклади наочно підтверджують тезу, що проблема міграції має глобальний характер. Проте позитивного досвіду у вирішенні міграційних проблем у світі дуже мало. Політика приймаючих мігрантів країн формується методом проб і помилок. Навряд чи хоч одна держава може стверджувати, що виробила дієві механізми боротьби з нелегальною імміграцією. Парадоксально, але факт, що основний урок, який можна отримати з накопиченого до цього часу міжнародного досвіду, такий: в умовах сучасного демократичного суспільства, яке сповідує ліберальні традиції, не знайдено дієвого інструменту, що дозволив би звести нанівець нелегальну міграцію.

Нині жодна демократична держава світу не може стверджувати, що виробила посправжньому дієздатні механізми у боротьбі з нелегальною міграцією. Дотепер не знайдено прийнятного вирішення суперечностей, що перебувають на стику таких базових прав суспільства, як право на свободу пересування і забезпечення національних інтересів кожної окремої держави. З одного боку, право на свободу пересування декларується як фундаментальне право кожної людської особистості. З іншого боку – кожна держава має право на захист своїх національних інтересів й охорону кордонів. Зростання рівня нелегальної міграції у світі є наслідком конфронтації цих фундаментальних правових чинників сучасного світового співтовариства.

У всіх економічно розвинених державах світу існують плани заходів щодо протидії нелегальній міграції. Як правило, вони засновані на комплексному підході до вирішення цієї проблеми, особливо у сфері забезпечення безпеки та недопущення терористичної та кримінальної спрямованості міграції. Але реалії свідчать про те, що без об'єднання зусиль усіх членів світової спільноти не можливо нейтралізувати негативні наслідки, що викликані глобалізацією міграційних процесів. Для вирішення цієї загальносвітової проблеми необхідне ухвалення та реалізація комплексу узгоджених заходів на міждержавному рівні та насамперед організація системи міждержавного регулювання зовнішньої трудової міграції та поліпшення інформаційного обміну з цього питання[1].

Американська влада у 2013 році почала реалізацію нових заходів протидії нелегальній міграції. Сенат США підтримав пропозицію Президента Сполучених Штатів Америки про надання нелегалам дозволів на проживання в країні. Відповідно до нової міграційної реформи, заплановано легалізувати приблизно 11 млн мігрантів. Але заради законного статусу нелегалам прийдеться сплатити податки за весь час їх нелегального перебування в Штатах. Також грін-карти будуть видавати тим, хто одержав у США вищу освіту.

Надалі міграційна політика стане більш жорсткою. Насамперед буде посилений контроль на кордонах, щоб уникнути припливу нових нелегальних мігрантів. Крім того, влада більш суворо буде карати роботодавців, які наважаться наймати робітників без документів про їх статус у США[2].

Але кажучи про інтеграцію та глобалізацію світових процесів боротьби з незаконною міграцією і супроводжуючу її злочинність, необхідно визнати, що поки особливих успіхів у цьому напрямі добивається лише кримінал: злочинність усе впевненіше перетинає національні кордони між державами і стає транснаціональною. У довгостроковій перспективі правоохоронні органи можуть успішно боротися з незаконною міграцією

[1] Куликов В. Доклад на конференции в Риге «Миграция, как фактор криминальной и террористической опасности» / В. Куликов // Всемирный Антикриминальный и Антитеррористический Форум. – 2006. – 3 ноября. [Электронный ресурс]. – Режим доступа: http://www.waaf.ru/index_ru.

[2] Америка легализует нелегальных мигрантов // Багнет. – 2013. – 29 января. [Электронный ресурс]. – Режим доступа: http://www.bagnet.org/news/world/...

тільки за умовою реалізації єдиної стратегії боротьби з нею, тобто наявності відповідної міжвідомчої та міждержавної взаємодії зі всіма основними учасниками протидії нелегальним міграційним процесам. Не тільки різні структури безпеки на державному та міждержавному рівнях, але й органи з питань міграції, праці та соціального забезпечення повинні брати в цьому процесі активну участь і у превентивному, і репресивному плані.

До завдань правоохоронних органів належать збір інформації про методи нелегального в'їзду або незаконних проникнень до країн, способи фальсифікації віз і посвідчень на проживання, кількість бажаючих отримати притулок з окремих країн, методи посередництва у нелегальній діяльності, а також збір будь-яких відомостей про діяльність іноземних екстремістських і терористичних організацій, їх взаємозв'язок і участь у процесах нелегальної міграції. В європейських поліцейських установах вважають, що для запобігання терактам і виступам мігрантів у країнах Європейського Союзу на майбутнє конче необхідно розраховувати ймовірність виникнення всіх можливих ситуацій та мати відповідні плани дій на кожний варіант негативного розвитку подій[1].

Оборонна політика посилення прикордонного контролю та введення жорсткого імміграційного контролю повинна поєднуватися з наступальною стратегією, основними завданнями якої є недопущення терористичних актів і боротьба з трансприкордонною злочинністю. У такій динамічній концепції попередження вказаних негативних явищ вирішальну роль відіграє оперативна інформація. Оперативна інформаційна взаємодія між імміграційними, правоохоронними, інформаційними та іншими компетентними органами, які відповідають за боротьбу з тероризмом, незаконною міграцією й організованою міжнародною злочинністю, дозволяє організувати використання оперативної інформації у масштабі реального часу й організувати нейтралізацію на відповідній правовій основі значної кількості злочинних елементів. *Отже, і на національному, і на міжнародному рівнях правоохоронні органи та спецслужби повинні бути охоплені загальносвітовою інформаційною мережею.* Протистояти злочинності щодо нелегального проникнення можна тільки шляхом плідної співпраці країн джерел, транзиту і мети незаконної міграції. Для протидії організованим злочинним структурам відповідним службам необхідний швидкий транскордонний обмін інформацією. Тільки під час організації належного співробітництва на міждержавному рівні можливе виконання національних державних планів протидії незаконній міграції. Для цього є єдиний шлях – залучення до співпраці країн, які ще не охоплені загальносвітовою співпрацею у цьому напрямі.

У рамках загальноєвропейської співпраці правоохоронні органи всіх держав Європи повинні розробити відповідні заходи на базі єдиних стандартів. Використання Шенгенської інформаційної системи «EURODAK» є одним із таких заходів, який стає на перешкоді тому, щоб нелегали вільно могли б потрапляти в будь-яку країну Шенгенської зони. Напочатку 2007 року в «EURODAK» вже була інформація на 800 тис. громадян третіх країн, які хоча б один раз були депортовані з держав-членів Шенгенської зони. Доступ до системи постійно розширюється і, крім Європола і Євроюста, до дактилоскопічного банку даних країн Шенгену вже підключені правоохоронні структури низки європейських держав, які не належать до членів Шенгенської угоди. Планується, що інформаційна система «EURODAK» згодом може стати загальноєвропейською[2].

Разом із системою «EURODAK» країни Шенгенської зони з 2013 року розпочали експлуатацію у повному обсязі другого покоління Шенгенської інформаційної системи

[1] Преступность в контексте миграционных процессов // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 7. – М.: ВИНИТИ. – С. 13–22.

[2] Там же.

(Schengen Information System /SIS II/). SIS II відіграє важливу контролюючу роль в умовах відсутності перевірок на кордонах між країнами – учасницями Шенгену[1].

У Європейському співтоваристві відповідні структури провели реалізацію останньої версії загальноєвропейської програми «Електронні кордони». Головною складовою цієї програми є біометрична система контролю, основою якої є технологія розпізнання за обличчям. До «Електронних кордонів» також входить взаємодія з програмою видачі біометричних віз (система VIS), що акумулює дані про відбитки пальців громадян країн, які не входять до Європейського економічного простору (а це близько 3/4 світового населення), а також із базами даних, що містять відомості про оформлені біометричні ідентифікаційні карти для іноземців, які тимчасово проживають на території ЄС, і мігрантів, які бажають отримати дозвіл на постійне місце проживання на території Євросоюзу.

У січні 2007 року учасники неформальної зустрічі міністрів внутрішніх справ та юстиції країн-членів Євросоюзу в Дрездені ухвалили рішення про зміцнення матеріальної бази об'єднаної європейської прикордонної охорони «Фронтекс»[2].

Заслуговує на особливу увагу інформація про прийняття сенатом США закону щодо сканування відбитків пальців у всіх іноземців, які залишають США. Закон прийнятий не тільки з метою ефективної боротьби з іммігрантами-іноземцями, які прагнуть назавжди залишитися в США, але й із тими туристами, котрі порушують строки перебування в країні.

На практиці швидкій реалізації запланованого заходу заважають суто економічно-технічні проблеми. Це пов'язано з тим, що процедура зняття відбитків пальців потребує певного часу, а пасажирські потоки в 30 найзавантаженіших аеропортах Америки дуже значні. Тому реалізація цього заходу розтягнута на шість років[3].

У всіх найважливіших аеропортах Федеративної Республіки Німеччина мають з'явитися пункти біометричних систем прикордонного контролю. Ці пункти біометричних систем будуть контролювати і в'їзд у країну, і виїзд з неї. Такий підхід дозволить припинити «зникнення» авіапасажирів, які прилетіли в Німеччину, але потім не покинули її. Протягом 2013–2022 років загальна чисельність біометричних пунктів може сягнути 270 одиниць[4].

У СНД програма спільної співпраці у протидії незаконній міграції на 2009–2011 роки передбачала створення максимально сприятливих умов для проведення компетентними органами держав спільних оперативних і профілактичних заходів щодо боротьби з цим негативним явищем, а також завершення процесу підписання угоди між країнами Співдружності про реадмісію. У документі також вказані заходи щодо зближення національних законодавств і підготовки кадрів.

Країни Співдружності регулярно обмінюються інформацією про канали незаконної міграції, існуючі маршрути, організаторів незаконного пересування мігрантів. У проекті Програми зазначені уніфіковані заходи щодо запровадження нових біометричних

---

[1] SIS II – Шенгенська інформаційна система II. [Електронний ресурс]. – Режим доступу: http://www.mfa.gov.hu/NR/rdonlyres/...

[2] Жолквер Н. ЕС создает единый банк биометрических данных / Н. Жолквер // Немецкая волна. – 2007. – 18 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Иностранцы будут проходить биометрическую идентификацию и при выезде из США // Turist.ru. – 2013. – 23 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Германия расширит применение биометрических систем пограничного контроля // BIOMETRICS.RU. – 2013. – 28 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

паспортів. Зацікавленість у набранні чинності цієї програми висловили всі країни Співдружності Незалежних Держав[1].

19 вересня 2008 року на території Білорусії Виконавчий комітет СНД підписав Меморандум про взаєморозуміння та співпрацю з Адміністрацією Міжнародної організації з міграції (МОМ). У Меморандумі визначені основні положення стосовно співпраці між двома організаціями у галузі міграції, зокрема в протидії незаконній міграції і торгівлі людьми. Підписання Меморандуму дозволило використовувати досвід і допомогу МОМ для вдосконалення договірно-правової бази співпраці у галузі міграції між країнами-учасниками СНД, а головне, створило умови для використання можливостей Міжнародної організації з міграції для поліпшення протидії країн СНД незаконній імміграції та негативним явищам, які її супроводжують. Меморандум надав право користуватись досвідом цієї міжнародної організації для всестороннього навчання співробітників компетентних органів і створення базової організації країн СНД із підготовки, перепідготовки та підвищенню кваліфікації кадрів у сфері боротьби з міграцією і протидії торгівлі людьми. Підписаний документ дозволив взаємообмін інформацією між сторонами про різні тенденції, проблеми та протидію міграційним явищам, що повинно сприяти покращенню стану аналітичної роботи та, як наслідок, зумовити появу нових ефективних розробок у сфері сучасної міграційної політики. Міжнародна організація з міграції стимулювала розширення використання біометричних технологій у процесах управління міграцією в країнах СНД[2].

Отже, можна зробити висновок, що нині міжнародною проблемою є не свобода пересування, а національна безпека держав, особливо через проблеми незаконної міграції і, як наслідок, реалізація заходів із підвищення надійності прикордонного контролю. Зараз усі розвинені країни впроваджують виняткові заходи для встановлення контролю за нелегальною міграцією та зміцнення своїх кордонів. У всіх державах ухвалюють закони про безпеку кордонів (наприклад, Закон про безпеку кордонів США, а в Україні – підписаний 5 листопада 2009 року Президентом України закон № 1710-VI «Про прикордонний контроль»). Євросоюз проводить заходи щодо реалізації проекту «Електронних кордонів».

Сьогодні одним із новітніх інструментів інтегрованої системи управління кордонами європейських країн і засобом превентивного реагування на транснаціональну протиправну діяльність є оперативний аналіз стану прикордонних ризиків і кримінальної ситуації на конкретних ділянках кордонів держав. В основу цієї роботи покладені рекомендації експертів із Бельгії, Великобританії, Німеччини, Голландії, Данії, Іспанії, Норвегії, Польщі, Фінляндії, Франції, Швеції, Європейської комісії й Європолу, які втілилися в Загальну інтегровану модель аналізу ризиків держав–членів Євросоюзу (CIRAM), яка в основному варіанті свого часу була прийнята на саміті ЄС у Севільї в 2002 році. Ідея полягала у тому, щоб створити загальноміжнародну систему, яка дозволить здійснювати аналіз реальних ризиків на кордонах, оцінювати ефективність протидії цим ризикам із боку прикордонних служб і надавати рекомендації для проведення більш доцільних і, головне, більш узгоджених дій. Ще п’ятнадцять років тому прикордонники європейських країн були роз’єднані, що дуже негативно впливало на ефективність їх роботи. Нині

[1] Сотрудничество стран СНГ в противодействии незаконной миграции переходит в практическую плоскость // Исполнительный комитет СНГ. – 2008. – 24 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Исполком СНГ и Международная организация по миграции договариваются о взаимодействии // Исполнительный комитет СНГ. – 2008. – 18 сентября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

у режимі реального часу налагоджений взаємообмін інформацією між усіма країнами-членами CIRAM, особливо з державами так званих найбільш міграційних ризиків[1].

Зараз усі держави запроваджують інтегроване управління службою й охороною кордону. Інтегроване управління запровадило багато країн, зокрема Агентство із управління кордонами ЄС (Frontex). Мета інтегрованого управління проста і зрозуміла – забезпечити необхідні умови охорони кордону і створити комфортні умови громадянам для перетинання кордонів[2].

Однією зі складових ефективності застосування технології «Електронних кордонів» є використання в прикордонному контролі досягнень біометрії.

В опублікованій ще у серпні 2007 року на інтернет-порталі Державного департаменту США «Доповідній записці з зміцнення безпеки кордонів і вирішення проблем імміграції в рамках існуючого законодавства» (скорочена назва – «Безпека кордонів») разом із вирішенням низки інших проблем значну увагу приділено практичному використанню останніх досягнень біометрії для контролю за особами, які перетинають державний кордон.

У пункті 4 першого розділу документа «Безпека кордонів» зазначалося, що до кінця 2008 року повинне бути завершене запровадження системи прикордонного біометричного контролю у всіх аеропортах і морських портах США. На початок 2009 року Міністерство внутрішньої безпеки повинне було зробити остаточний вибір варіанту біометричної системи для запровадження найбільш практичного та найменш витратного методу біометричного контролю у місцях перетинання сухопутного кордону[3].

Використання останніх досягнень біометричних технологій на прикордонних контрольно-пропускних пунктах (КПП) Сполучених Штатів Америки дуже необхідне через невпинне збільшення потоку іноземців, які перетинають кордони США. На початок 2009 року, за даними Міністерства внутрішньої безпеки США, у 2008 році було зафіксовано приблизно 46,3 млн перетинів кордону Сполучених Штатів Америки іноземцями (туристами, візитерами, тими, хто перебував у відрядженні і т. д., причому одна і та ж людина могла в'їжджати в США більше одного разу). Це набагато більше, ніж у попередні роки: в 2007 році було здійснено 37 млн відвідин, у 2006-му – 33,6 млн, у 2005-му – 32 млн.

Завдяки використанню американської програми «US-VISIT» у 2008 році приблизно 25,5 тис. чоловік було відмовлено в отриманні американської візи, а ще майже 11,7 тис. осіб були не допущені в США безпосередньо під час перевірки на прикордонних КПП. Причиною недопуску на територію Сполучених Штатів Америки є перебування цих іноземців у так званих «чорних списках», тобто ці особи раніше вчиняли тяжкі або особливо тяжкі злочини (наприклад, вбивство або торгівлю наркотиками), або за наявною інформацією тією чи іншою мірою пов'язані з терористичними структурами, або у минулому порушували американські візові правила.

Із прибулих у 2008 році приблизно 236,8 тис. чоловік не покинули територію США в заявлений час і, що цілком імовірно, більшість із них залишилися у країні як

---

[1] Астахов С. Николай Литвин: «От анализа рисков зависит безопасность страны» / С. Астахов, Н. Литвин // Еженедельник-2000. – № 21 (415). – 2008. – 23–29 мая. [Электронный ресурс]. – Режим доступа: http://www.2000.net.ua/e/57834

[2] Колычев Владимир. 12 секунд на один паспорт / Владимир Колычев // Еженедельник-2000. – 2012. – № 20 (606). – 18–24 мая. [Электронный ресурс]. – Режим доступа: http://2000.net.ua/2000/derzhava/80365

[3] Докладная записка по укреплению безопасности границ и решению проблем иммиграции в рамках существующего законодательства. Распространено Бюро международных информационных программ Государственного департамента США // Washprofile.org/ru. – 2007. – 15 августа. [Электронный ресурс]. – Режим доступа: http://usinfo.state.gov/xarchives/

нелегальні іммігранти. Ще 54,3 тис. відвідувачів виїхали з Сполучених Штатів Америки, порушивши водночас зазначений у в'їзних візах термін перебування[1].

Щоб забезпечити належний контроль та необхідний рівень безпеки під час перетинання кордону, з початку 2009 року на всіх американських прикордонних переходах встановлені автоматизовані системи контролю на базі біометричних технологій. Причому слід зазначити, що спочатку відповідні державні органи не виявляли особливого ентузіазму з приводу застосування біометрії з метою організації прикордонного контролю, але реалізація вдалих проектів у аеропортах і морських портах, а потім і на інших пунктах перетину сухопутного кордону забезпечила належну підтримку з боку федерального уряду для загального прикордонного запровадження біометричних технологій.

Із упровадженням останніх технологічних розробок біометрики пов'язані надії на пришвидшення прикордонного контролю, зменшення черг, що виникають у процесі його здійснення, вивільнення персоналу, який раніше був задіяний у перевірці документів осіб, які перетинають кордон. Крім того, останні досягнення біометричних технологій використовуються для того, щоб максимально збалансувати вимоги з досягнення необхідного рівня безпеки з гарантуванням права недоторканності приватного життя та належним комфортом перетинання кордону.

Більшість аналітиків (наприклад, Ніліма Сагар із агенства «Frost & Sullivan») вважають, що ці позитивні зміни є наслідком реалізації насамперед загальнодержавних програм «US-VISIT» і низки інших заходів відповідно до «Доповідної записки з зміцнення безпеки кордонів і вирішення проблем імміграції в рамках існуючого законодавства» та програми безвізового в'їзду в США «Visa Waver program»[2]. Нагадаємо, що право безвізового в'їзду на американську територію на початок 2014 року отримали громадяни 37-и країн, які є власниками електронних біометричних паспортів другого покоління.

Із жовтня 2004 року до початку 2009 року була завершена практична реалізація основних положень програми «US-VISIT». За цей же час у США суттєво посилились заходи безпеки в аеропортах і морських портах. Конгресом Сполучених Штатів Америки був ухвалений закон, що передбачає поступове введення єдиного для всіх американців внутрішнього посвідчення особи.

Департамент внутрішньої безпеки США має на меті – створити комплексну систему прикордонного контролю й ефективного управління нею. Основу проекту системи становить процедура сканування відбитків пальців і фотографування людей, які в'їжджають до країни. Ретельна перевірка для пошуку відомих властям злочинців і терористів за відповідними державними та міждержавними банками даних проводиться, якщо під час проходження процедури первинного автоматизованого контролю було встановлено, що потрібно проведення додаткової перевірки. В Сполучених Штатах Америки, протягом 2008 року 10-пальцьова процедура прикордонного контролю іноземців була практична введена в дію на всіх пунктах перетину кордону. На думку американських офіційних осіб, запровадження цієї процедури не створює жодних проблем для законослухняних громадян, але значно підвищує рівень безпеки і цивільних осіб, і держави загалом.

Усі відбитки пальців людей, які перетинають кордон, перевіряються за базою даних біометричних слідів, що були вилучені з місць учинення злочинів або терористичних актів. Наявність повного комплекту відбитків пальців індивідуумів підвищує ймовірність

[1] Поездка в Америку // Washprofile.org/ru. – 2008. – 29 декабря. [Электронный ресурс]. – Режим доступа: http://www.washprofile.org/ru/node/...

[2] Новые перспективы биометрии в пограничном контроле // BIOMETRICS.RU. – 2008. – 4 августа. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

встановлення серед 400 млн туристів, які щорічно прибувають у США, причетних до тероризму осіб, порушників міграційного режиму та інших злочинних елементів. Отримані дані перевіряються за банками даних ФБР, Пентагону та Міністерства національної безпеки[1].

Отже, з серпня 2007 року Адміністрація Сполучених Штатів Америки почала втілювати у життя серію реформ, реалізація яких дала змогу зміцнити рівень безпеки кордонів і просунутися у вирішенні проблем незаконної імміграції. Мета реформ полягала у тому, щоб добитися ефективнішої охорони кордонів США, стимулювати введення єдиних загальнофедеральних правил прийому на роботу, спростити процес тимчасового працевлаштування іноземних робочих, удосконалити існуючий імміграційний порядок і допомогти новим іммігрантам адаптуватися до американської культури.

Розглянемо основні завдання, які вирішуються шляхом запровадження біометричного паспортно-візового контролю під час перетину кордонів та насамперед його значення для боротьби з нелегальною міграцією.

Перше завдання, що вирішується за допомогою паспортно-візових документів нового покоління (ПВДНП), – це перевірка достовірності пред'явленого для контролю документа та його відповідність пред'явникові. Наявність документів нового покоління під час проходження прикордонного контролю дає можливість зчитати інформацію про власника документа за лічені секунди шляхом піднесення біометричного документа до зчитувального електронного пристрою. Декілька секунд – і вся інформація щодо власника документа з'являється на екрані комп'ютера. Передруковувати з паспорта персональні дані стосовно особи, яка перевіряється, не має потреби.

Отже, власники нових паспортів отримують перевагу перед власниками документів старого зразка – значно зменшується час проходження паспортно-візового прикордонного контролю.

Зважаючи на високий ступінь надійності використовуваних біометричних технологій, США з 2005 року дозволили безвізовий в'їзд на свою територію громадянам низки країн тільки за наявності біометричних (електронних) паспортів другого покоління, які, як відомо, передбачають серед інших показників обов'язкову наявність в електронному форматі у мікрочіпі відбитків пальців[2].

На практиці Сполучені Штати Америки застосували процедуру неодноразового обов'язкового зняття відбитків пальців для всіх осіб, які прибувають до країни та виїзджають із неї. Процедура сканування пальців відбувається тричі – під час одержання візи, при в'їзді та виїзді з країни[3].

Друге завдання, яке вирішується безпосередньо під час видачі паспортно-візового документа, є перевірка ймовірності факту можливої видачі аналогічного документа громадянинові з такими ж біометричними даними, але під іншими установочними відомостями, а також перевірка біометричних даних громадянина за базами даних оперативних і спеціальних служб[4].

---

[1] Вашингтон схватит иностранцев за пальцы // Независимая газета. – 2007. – 13 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Микрочип как пропуск за границу // ИА Росбалт. – 2008. – 17 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Бокарева Н. Не прячьте ваши пальчики. В Европу без дактилоскопии больше не пустят / Н. Бокарева. – 2007. – 27 июля. [Электронный ресурс]. – Режим доступа: http://news.mail.ru/politics/

[4] Вакуленко А. Аэропорты: зона особого внимания / А. Вакуленко, А. Юхин // Мир и безопасность. – 2006. – № 6. – 1 декабря. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Для громадян більшості європейських і північноамериканських країн, низки держав Азії й Африки документи нового покоління такі, як біометричні паспорти, ідентифікаційні картки, водійські права та інші з екзотики перетворилося на атрибути буденного життя. Нові біометричні системи прикордонного контролю використовують електронні документи та здійснюють процедуру порівняння оцифрованої фотографії та інших біометричних параметрів власника документа, що внесені в мікрочіп, із реальним зображенням обличчя громадянина та його відсканованими відбитками пальців.

Адміністрації транспортної безпеки (TSA) США та британських аеропортів (BBA) проводили розробку сучасної відеосистеми, принцип дії якої ґрунтується на використанні протоколу Інтернету й яка повинна забезпечити реалізацію численних функцій із можливістю подальшого розширення. Планується, що з часом відеосистема зможе обслуговувати тисячі відеопристроїв і мати можливість інтегруватися з вже існуючими підсистемами такими, наприклад, як обробка багажу[1].

Контроль доступу розглядається як ще один критично важливий елемент продовження вдосконалення безпеки, тому адміністрація BBA Aviation вже працює над такою інтегрованою системою, котра буде охоплювати понад 3500 пристроїв для зчитування карт і приблизно 240 тис. працівників, які мають такі картки-перепуски.

Нині у Сполучених Штатах Америки і Великобританії проходять випробування низки технічних зразків контрольних пристроїв на основі останніх досягнень технологій доступу, причому деякі з них перебувають лише на стадіях пробного тестування. Основною особливістю експериментальних зразків є реалізація вимоги поєднання швидкореагуючої та збалансованої технології безпеки і надання сучасного набору інноваційних послуг.

Міністерство національної безпеки США (Department of Homeland Security /DHS/) свого часу видало завдання на розробку нової технології, яка повинна виявляти за особливостями поведінки фізичних осіб, котрі мають на меті скоєння зловмисних дій. У проекті виявлення «можливих ворожих намірів» (Project Hostile Intent /PHI/), що перебував на стадії розробки, передбачалось використовувати симбіоз різних технологій біометричної ідентифікації та відеоспостереження. У системах PHI використовуваються технології аналізу відео- й аудіопотоків, руху очей та вимірювання температури індивідуума, що перевіряються за базою візуально-контрольованих ознак. Пілотні випробування систем Project Hostile Intent мали проводитися у 2010 році в декількох аеропортах і наземних прикордонних пунктах.

У випадку досягнення позитивних результатів за проведеними тестуваннями DHS планував запровадження системи виявлення «можливих ворожих намірів» на всіх прикордонних контрольно-пропускних пунктах Сполучених Штатів Америки[2]. Оскільки інформації про масове запровадження проекту PHI не надходило, то слід вважати, що ця розробка поки що не досягла своєї мети.

Починаючи з 2010 року, у всіх оглядах, матеріалах конференцій і семінарів експерти зазначають, що світовий ринок біометричних систем прикордонного контролю поступально продовжує розвиватися. У другому десятиріччі XXI століття майже всі держави запроваджують паспортно-візові документи нового покоління з біометричними ідентифікаторами їх власників із метою гарантування того, що власник документа насправді

[1] Новые технологии защиты от терроризма на воздушном транспорте // Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2008. – № 9. – М.: ВИНИТИ. – С. 8–11.

[2] Власти США хотят обнаруживать потенциальных террористов, используя биометрию // BIOMETRICS.RU. – 2008. – 17 сентября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

є тим, за кого він себе видає. А на кордонах розвинутих держав встановлюють системи автоматичної ідентифікації особистості за допомогою ПВДНП.

Аналітик «Frost & Sullivan» Кшиштоф Рутковський (Krzysztof Rutkowski) стверджує, що «розширення міжнародного співробітництва в сфері забезпечення безпеки пасажирів підштовхує уряди багатьох країн до впровадження систем електронного документообігу. Своєю чергою, це сприяє підвищенню ефективності процесів в аеропортах і службах прикордонного контролю у всьому світі».

Електронні документи й автоматичні системи ідентифікації особистості дозволяють пасажирам значно пришвидшити час проходження прикордонного контролю. Цей метод виправдав себе як економічно ефективний, тому слід очікувати більшого запровадження подібних технологій в аеропортах у всьому світі.

Нині багато західних країн впровадили технології автоматизованого прикордонного контролю електронних паспортів і систем пришвидшеного проходження подорожуючими процедур контролю[1].

Розглянемо сучасні проекти організації контрольно-пропускного пункту (КПП) в аеропортах і системи забезпечення безпеки на транспортному вузлі.

У червні 2011 року в Сінгапурі на щорічних загальних зборах Міжнародної асоціації повітряного транспорту (ІАТА) був представлений перший проект «Контрольно-пропускного пункту (КПП) майбутнього». Як вважають фахівці ІАТА, проект спрямований на те, щоб збільшати рівень безпеки в аеропортах, водночас суттєво зменшивши черги та незручності для авіапасажирів.

За заявою генерального директора і президента Асоціації Джованні Бісіньяні, світові аеропорти щорічно витрачають загалом до 7,4 млрд доларів США у рік на забезпечення безпеки в авіації, причому в повітряних гаванях пасажирів очікують тривалі черги та суєта.

Прототип діючих поки що КПП був розроблений ще 40 років тому. Тоді головним пріоритетом була необхідність зупинити потенційних терористів, які користувались звичайною вогнепальною зброєю. ІАТА заявляє, що настав час запровадження нової системи, яка повинна відповідати всім сучасним вимогам безпеки аеропортів. Ця система побудована на симбіозі людських ресурсів та інноваційних технологій.

Під час підходу до КПП «Майбутнього» пасажири будуть скеровуватися до одного з трьох його відділень: «Мандрівник», «Норма» і «Посилена безпека». Доступ осіб до відділень КПП буде проводитись за підсумками попередньо здійснених перевірок на підставі отриманих із наданих документів персональної інформації, зокрема і біометричної. Тобто оцінка ступеня загрози, яку може становити особа, котру перевіряють, буде проведена ще до того, як авіапасажир дістанеться до аеропорта.

Передбачається, що особи, які заздалегідь пройшли перевірку своїх даних у відповідних правоохоронних структурах, максимально швидко будуть проходити процедуру перевірки на контрольно-пропускному пункті. Відділення «Норма» буде призначено для проходу пасажирів, які за підсумками проведеної перевірки не мають жодних заперечень із боку відповідних структур. У відділенні «Посилена безпека» буде проводитися додаткова перевірка осіб, які під час попередньої перевірки викликали у представників спеціальних органів певні сумніви.

Водночас огляд на КПП буде проводитися з застосуванням спеціальної нової технології, яка дозволяє громадянам не знімати одяг і взуття, не пред'являти для візуального

[1] Биометрические системы пограничного контроля: новый прогноз // Frost & Sullivan. – 2013. – 10 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

огляду вміст багажу та непроходити процедуру особистого огляду. Також передбачається, що безпосередньо на КПП «Майбутнього» буде здійснюватися митний та імміграційний контроль.

Усі ці заходи дозволять максимально спростити та пришвидшити здійснення процедури передпольотного контролю[1].

У Російській Федерації (РФ) також розроблена своя система забезпечення безпеки на транспорті. Вона складається з п'яти рівнів.

Перший рівень – це територія привокзального комплексу, яка оснащена відеокамерами.

Другий рівень забезпечений спеціальними програмно-апаратними комплексами, які здатні за біометричними параметрами ідентифікувати осіб, які перебувають у розшуку.

Третій рівень – це зона реєстрації пасажирів, де проводяться оперативно-розшукові заходи з метою виявлення потенційно небезпечних осіб.

Загалом процедура роботи трьох перших рівнів виглядає так. Камери проводять відеозйомку пасажиропотоку, комп'ютерна програма обробляє відеокадри і виокремлює індивідуумів, які перебувають у стані підвищеного збудження або агресії. Таких пасажирів на третьому рівні зустрічають співробітники служби безпеки, далі з ними проводить роботу фахівець (профайлер), завдання якого – визначити, чи становить ця людина загрозу для оточуючих.

На четвертому рівні здійснюється паспортний контроль, під час якого спеціальний апаратно-програмний комплекс за паспортом або проїзним квитком здійснює перевірку пасажира за наявними у розпорядженні поліції (міліції) базами даних.

На п'ятому рівні пасажири проходять передпольотний огляд, а його речі просвічуються в спеціальному інтроскопі. Далі пасажир проходить у так звану «стерильну зону».

Подібна система безпеки вже запроваджена в міжнародних і великих регіональних аеропортах Росії, однак у 2012 році система профайлінга діяла тільки в аеропортах «Домодедово» та «Пулково»[2].

Загалом від застосування сучасних біометричних технологій в аеропортах найбільшу вигоду мають отримати авіапасажири. Це такі зручності, як: скорочення часу реєстрації на рейс і проходження контролю, зменшення часу процедури посадки на борт літака шляхом пришвидшеної перевірки багажу.

Перевагами технологій біометрії пасажири користуються не тільки під час вильоту, але і в аеропортах прибуття, особливо при користуванні міжнародними авіарейсами: тут час авіапасажирів суттєво заощаджують сучасні біометричні системи паспортного й візового контролю.

Міжнародна організація цивільної авіації (ІКАО) нині особливу увагу приділяє перспективам розвитку технологій біометричних паспортів та інших документів, які засвідчують особистість громадян і осіб без громадянства під час їх переміщення світом. Для поліпшення захисту ПВДНП вона приділяє посилену увагу інтеграції біометрії з іншими сучасними інформаційними технологіями, зокрема з інфраструктурою відкритих ключів цифрового підпису (каталог таких ключів ІКАО зараз і продовжує формувати).

Міжнародна організація цивільної авіації продовжує узагальнювати досвід використання біометричних документів у автоматичних системах прикордонного контролю.

[1] Биометрия станет еще активнее использоваться в аэропортах // Туринфо. – 2011. – 8 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Владимир Путин ознакомился с действием биометрической системы // РИА Новости. – 2012. – 18 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

ІКАО особливо цікавить вплив біометричних технологій на забезпечення надійності та безпеки під час проведення автоматичних ідентифікаційних процедур і організації зручного проходження процедури прикордонного контролю[1].

Роглянемо географію використання біометричних технологій у прикордонному контролі. Розпочнемо з Сполучених Штатів Америки, оскільки в засобах масової інформації є найбільша кількість повідомлень про застосування в цій країні різних біометричних систем, зокрема й у прикордонному контролі.

Як відомо, США мають безвізовий режим із 36 країнами світу, громадяни яких є власниками біометричних паспортів другого покоління. Причому власники біометричних документів за певних умов можуть скористатися програмами пришвидшеного проходження прикордонного контролю.

У Сполучених Штатах Америки з 2008 року діє програма Global Entry, яка була розроблена митно-прикордонною службою США для спрощення прикордонних процедур під час в'їзду в країну іноземних громадян із низьким рівнем ризику. 2012 року користувачами цієї програми були громадяни Англії, Німеччини, Мексики, Канади, Голландії й Японії. Програмою Global Entry також цікавляться Австралія, Ізраїль, Нова Зеландія, Південна Корея, Сінгапур і Франція.

Процес залучення до програми доволі простий: кандидат (обов'язково власник біометричного документа) заповнює електронну форму, оплачує внесок і висилає заповнений електронний документ на інтернет-адресу Global Entry. В разі позитивного рішення на адресу його електронної пошти надходить попередня згода. Після цього кандидат у представництві проходить співбесіду, реєструє біометричні ідентифікатори (відбитки пальців) і підтверджує місце свого проживання. Після отримання остаточного схвального рішення здобувач стає trusted traveler (пасажиром на довірі) і учасником програми Global Entry[2].

Після прибуття до американського аеропорту учасник програми підходить до інформаційного кіоску, заповнює за допомогою вбудованого в нього сенсорного екрану митну декларацію, пред'являє для зчитування даних свій паспорт і відскановує відбитки пальців, чим швидко та легко підтверджуючи свою особистість.

За оцінкою американських митників, користувачі Global Entry долають кордон США менш ніж за хвилину (за іншими джерелами – за п'ять хвилин), тоді як проходження прикордонного й митного контролю в звичайному порядку вимагає набагато більшого часу.

Загалом 2012 року програма діяла в 20 американських аеропортах і налічувала 137 кіосків[3].

Міністерство національної безпеки США (Department of Homeland Security – DHS) планує розширити список біометричних ідентифікаторів, які будуть використовуватися для забезпечення безпеки американських кордонів. До ідентифікаторів поряд із відбитками пальців також увійдуть оцифровані зображення обличчя та райдужної оболонки очей.

---

[1] Симпозиум по биометрическим паспортам пройдет в Канаде // BIOMETRICS.RU. – 2013. – 15 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Израиль присоединится к американской биометрической системе пограничного контроля // Visa4.ru. – 2012. – 24 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/izrail...

[3] США: сфера действия биометрической системы пограничного контроля будет расширена // BIOMETRICS.RU. – 2012. – 27 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Заплановано провести у 2012–2013 роках пілотне тестування програми Global Entry на предмет використання додаткових біометричних ідентифікаторів[1].

У Сполучених Штатах Америки здійснюються розробки для поліпшення технологій перевірок іноземців під час перетинання кордону. Дослідники Арізонського університету в співробітництві з митною і прикордонною службою США розробили пристрій, який одержав назву «автоматизований віртуальний агент оцінки правди в режимі реального часу» (Automated Virtual Agent for Truth Assessments in Real-Time/AVATAR/) або термінал «AVATAR». Ще одна назва цього робота-термінала – віртуальний прикордонник «Елвіс».

Термінал «AVATAR» аналізує поведінку прибуваючих у Сполучені Штати Америки іноземців і своїх громадян, використовуючи складні алгоритми для визначення «неправдивої поведінки». За твердженням розробників, термінал під час перевірки фіксує будь-які незвичні фізіологічні реакції, за допомогою яких виявляють неадекватну поведінку з боку особи, яку перевіряють. Максимальна точність виявлення неправдивої інформації співробітниками прикордонної і митної служби сягає 54%, водночас у віртуального прикордонника цей показник становить 90%.

Підконтрольні індивідууми можуть спілкуватися з терміналом «AVATAR» не тільки англійською, але й іспанською мовами. Під час проведення співбесіди зображення віртуального прикордонника «Елвіса» перебуває на рівні обличчя особи, яку перевіряють. Сам процес спілкування проходить як співбесіда з реальною людиною.

Фігуранти, які перевіряються, повинні зареєструватися відповідно до запропонованої схеми, пред'являючи для цього свої відбитки пальців. За оцінкою спеціалістів, кожна особа, яку перевіряють, витрачає приблизно п'ять хвилин для того, щоб пройти процес реєстрації. Термінал «AVATAR» уже пройшов випробовування в аеропорту міста Ногалес (штат Арізона) і незабаром може стати звичайним явищем в аеропортах Сполучених Штатів Америки[2].

Розглянемо застосування біометричних технолій на кордонах Шенгенської зони та інших країн Євросоюзу, що не входять до Шенгенського співтовариства.

Особлива система в'їзду-виїзду (Entry-Exit system) має з'явитися з 2013 року на зовнішніх кордонах усіх держав, які є членами Шенгену. За допомогою Entry-Exit system буде проводитись біометричний контроль і реєструватися дані всіх в'їжджаючих і виїзджаючих осіб, що у перспективі дозволить відмовитися від практики проставлення відповідних штампів у паспортах громадян Європейського Союзу[3].

Система в'їзду-виїзду (Entry-Exit system) є частиною проекту ЄС Smart Borders, який у повному обсязі може бути введений не раніше 2018 року[4].

Необхідно зауважити, що практично в усіх міжнародних аеропортах столиць країн Європейського Союзу встановлені автоматичні біометричні системи прикордонного контролю.

---

[1] США расширят применение биометрических технологий в пограничном контроле // BIOMETRICS.RU. – 2012. – 19 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Биометрический робот-пограничник сканирует отпечатки пальцев // NovostiUA.net. – 2012. – 20 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Пограничный контроль на рубежах Шенгена: новые предложения по применению биометрических технологий // Travel@Mail.Ru. – 2012. – 9 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Когда обладатели российских биометрических паспортов смогут пересекать финскую границу в автоматическом режиме? // Фонтанка.FI. – 2012. – 26 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

У 2012–2014 роках російський біометричний портал «Biometrics.RU» у своїх публікаціях наводив інформацію про встановлення або експлуатацію біометричних систем прикордонного контролю в таких державах ЄС: Болгарія (Софія), Сполучене Королівство Великобританія (низка аеропортів, найбільш відомий аеропорт Хітроу), Німеччина (повітряні гавані Франкфурта, Мюнхена, Дюссельдорфа та Гамбурга), Ірландія (Дублін), Іспанія (Мадрид, аеропорт «Барахас»), Нідерланди (Скіпхол), Норвегія (Осло, аеропорт «Гардермуен»), Португалія (Лісабон), Фінляндія (Ге́льсінкі або Хе́льсінкі), Франція (Париж, аеропорти імені Шарля де Голля і Орлі; Марсель), Чехія (Прага, аеропорт Рузін) і Естонія (Таллінн).

Незабаром (орієнтовно протягом 2014 року) автоматичні системи контролю за перетинанням кордону мають запровадити Данія і Латвія. Але цією послугою можуть користуватися тільки пасажири, які мають біометричні паспорти й які є громадянами країн, що не менш 15 років є членами ЄС, Європейського економічного співтовариства або Шенгенської угоди[1].

В аеропортах Австралії та Нової Зеландії з липня 2009 року запроваджені біометричні системи прикордонного контролю, що діють в автоматичному режимі. Аеропорти розташовані в містах: Сідней, Мельбурн, Перт, Брисбен, Аделаїда, Голд-Коста, Кернс, Веллінгтон, Окленд та Крістчерч.

Аналогічні технології використовують авіапорти Аргентини, Болівії, Ізраїлю, Індії, Канади, Кувейту, Мальдів, Нігерії, Об'єднаних Арабських Еміратів, Росії (дослідна експлуатація в аеропортах Шереметьєво, Нового Новгорода та в новому терміналі Пулково), Філіппін і Японії. Звісно, це не повний перелік країн, де аеропорти оснащені біометричними системами контролю. Автори посібника вказали тільки ті держави, щодо яких вони мали інформацію у вигляді публікацій у ЗМІ за декілька останніх років.

У читачів може виникнути питання, чому така увага в цьому розділі приділяється прикордонному контролю в аеропортах? Згідно із дослідженням компанії «Acuity Market Intelligence», нині у повітряних гаванях використовується 95% від загальної кількості діючих біометричних систем прикордонного контролю.

Передбачається, що до 2020 року цей відсоток зменшиться до 80%, а частка біометричних систем контролю в морських портах і пунктах пропуску на суходольному кордоні, відповідно зросте до 20%.

Загалом у 2014–2020 роках швидкість зростання розвитку світового ринку біометричних систем прикордонного контролю в складних відсотках буде становити 20% і в 2020 році річний обсяг продажу цих систем може сягти 1,2 млрд доларів США. Частка Європи в загальному обсязі світового ринку прикордонних біометричних систем буде становити 47%, друге місце посядуть азійські держави з часткою у 22,5%[2].

Російська Федерація (РФ) на початок 2013 року планувала завершити перехід на проведення біометричного контролю на своїх прикордонних КПП[3]. Але за повідомленнями в кінці жовтня 2012 року російського агенства «РІА Новини» очікується,

---

[1] Биометрическая система пограничного контроля начала работу в аэропорту Таллинна // DGL.RU. – 2013. – 2 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Как будет развиваться рынок биометрических систем пограничного контроля? // BIOMETRICS.RU. – 2014. – 3 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрия 2010: 50 главных событий года // BIOMETRICS.RU. – 2011. – 13 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

що всі контрольно-пропускні пункти російського кордону мають обладнати пристроями для зчитування біометричних даних із паспортів лише в 2013–2014 роках[1].

За відомостями російського агентства «ТАСС-Телеком», у Росії розробляється власна автоматична система паспортного контролю на кордоні. Пробна експлуатація дослідного зразка проводилась у терміналі Е міжнародного московського аеропорту Шереметьєво[2]. А протягом 2013–2014 років пункти біометричного контролю з'являться в повітряних гаванях Нижнього Новгорода, Казані, Сочі та нового термінала Пулково. Запланована також модернізація повітряних портів Уфи, Самари та Нижньокамська. Одним із чинників виконання робіт із сучасного облаштування аеропортів Росії є проведення на її території великих міжнародних подій: Всесвітньої студентської літньої Універсіади (2013 р.), Олімпіади-2014, саміт керівників країн ШОС, зустріч лідерів БРІКС (2015 р.) і чемпіонат світу з футболу (2018 р.)[3].

Загалом у Російській Федерації у другому десятиріччі XXI століття створене принципово нове інформаційне середовище, що забезпечує швидкий, практично миттєвий обмін інформацією між різними правоохоронними та силовими структурами. В об'єднаних інформаційних базах зберігаються 120 млн досьє на іноземних громадян, які відвідували РФ. Причому є відомості про їх родичів, найближче оточення, власний автотранспорт, на якому вони перетинали російській кордон[4].

У грудні 2009 року Україна підписала угоду про стратегічне співробітництво з Європолом. Мета цієї угоди – запобігання та протидія будь-яким формам міжнародної злочинності, виявам терористичних загроз, торгівлі людьми, наркотиками й іншими психотропними речовинами. Угодою передбачено взаємообмін оперативною інформацією загального характеру.

Європол – поліцейська служба Європейського Союзу, головний офіс якої розташований у Гаазі (Нідерланди). Основними завданнями цієї організації є координація роботи національних служб у боротьбі з міжнародною організованою злочинністю та поліпшення інформаційного обміну між національними поліцейськими службами. Серед основних напрямів роботи поліцейської організації ЄС – боротьба з тероризмом, нелегальною торгівлею зброєю, наркоторгівлею, дитячою порнографією та відмиванням грошей[5].

Відповідно до концепції Державної цільової правоохоронної програми в Україні проводяться заходи щодо встановлення сучасних систем безпеки, застосування засобів зовнішнього спостереження (контролю) і швидкого реагування на період до 2016 року. Концепція передбачає залучення міжнародної технічної та фінансової

[1] Все пункты пересечения российской границы будут оборудованы средствами работы с биометрическими паспортами // РИА Новости. – 2012. – 31 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Россия обзаведётся собственной биометрической системой пограничного контроля // ТАСС-Телеком. – 2012. – 29 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] В аэропорту Нижнего Новгорода появится оборудование для работы с биометрическими паспортами // БИЗНЕС-ТАСС. – 2013. – 23 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Пограничники СНГ получат базы данных тех, кому запрещен въезд в Россию // Российская газета. – 2013. – 23 января. [Электронный ресурс]. – Режим доступа: http://4vlada.net/vneshnyaya-politika/...

[5] Украина договорилась о стратегическом сотрудничестве с Европолом // Українські новини. – 2009. – 4 декабря. [Электронный ресурс]. – Режим доступа: http://www.proua.com/news/...

допомоги, а також інших джерел, не заборонених законодавством, зокрема – коштів місцевих бюджетів[1].

Станом на квітень 2013 року на 38 українських пунктах прикордонного контролю встановлено обладнання для обслуговування громадян із біометричними паспортами. Загалом створено 449 автоматизованих робочих місць для зчитування інформації з електронних паспортів. Для повного оснащення прикордонних пунктів устаткуванням для зчитування інформації з біометричних закордонних паспортів необхідно виділення 184 млн гривень, а з бюджету України на 2013 рік для цих заходів було надано лише 13,5 млн грн. Міжнародна технічна допомога українському прикордонному відомстві у 2013 році становила приблизно 50 млн грн[2].

20 листопада 2012 року Президент України підписав Закон України «Про Єдиний державний демографічний реєстр та документи, що підтверджують громадянство України, посвідчують особу чи її спеціальний статус» (реєстраційний № 5492-VI). Цим законом передбачено створення бази даних інформаційно-комунікативної системи на українців і осіб без громадянства, а також впровадження низки документів з електронним чіпом. Головні з них: біометричний закордонний паспорт, електронна ідентифікаційна картка, яка згодом повинна замінити нинішній внутрішній паспорт громадянина України.

Проведення паспортної реформи зумовлене виконанням умов щодо встановлення безвізового режиму з країнами Євросоюзу та підписаних українською державою міжнародних угод, спрямованих на боротьбу з тероризмом і нелегальною міграцією. Загалом запровадження біометричних документів на Україні просувається дуже повільно, але слід пам'ятати, що 19–20 липня 2007 року на конференції ОБСЄ у Відні було заявлено, що з 1 січня 2015 року в'їзд на територію ЄС і США за паспортами з наклеєними фотографіями буде заборонений.

Використання державних технологій безпеки доступу не обмежується організацією проведення прикордонного контролю або передпольотного контролю. Нові покоління систем безпеки розробляються для таких місць масового скупчення людей, як залізничні вокзали, морські й річкові порти, метро та об'єкти спортивних змагань, зокрема Олімпійські ігри та чемпіонати світу й Європи з футболу.

2012 року під час Олімпіади в Лондоні відвідувачі спортоб'єктів проходили за так званим «тунелем правди» («tunnel of truth»), де за час проходження здійснювалась перевірка на наявність зброї, вибухових речовин, а за допомогою замкненої телевізійної системи (CCTV) порівнювалися їх відеозображеннями із фотозображеннями злочинців і підозрюваних у злочинній діяльності осіб, які зацікавлювали правоохоронні органи.

Алгоритм дії «tunnel of truth» такий. Квитки або документи, що надавали право присутності на змаганнях, сканувались на предмет виявлення залишкових слідів вибухових речовин або деяких хімікатів. Потім клієнти проходили перед монітором, який використовує власне випромінювання людського тіла для виводу зображення будь-яких предметів, що приховані під одягом, на екран, а вентилятори під час проходу безперервно обдували відвідувачів із метою виявлення щонайменших залишків від вибухових речовин і небезпечних хімічних реагентів. Спеціальні детектори проводили перевірку на наявність нейтронної та гамма-радіації, а також отруйних речовин нервовопаралітичної, шкірнонаривної, кровозаражувальної та задушливої дії.

---

[1] Правительство утвердило «слежку» за украинцами // Mail.ru. – 2013. – 8 февраля. [Электронный ресурс]. – Режим доступа: http://news.mail.ru/inworld/ukraina/global/112/politics/

[2] Пограничники оборудуют границы аппаратурой для биометрических паспортов // Багнет. – 2013. – 4 апреля. [Электронный ресурс]. – Режим доступа: http://www.bagnet.org/news/tech/

Що стосується лондонського метро, то підрозділ британської поліції, що обслуговує метрополітени (Uk's Metropolitan Police Service /MPS/), приєднався до нової системи біометричної ідентифікації, яка за допомогою мобільних технологій дозволяє швидко встановлювати особистість громадян, які зацікавили співробітників правоохоронних органів. MPS стало 25-м поліцейським підрозділом Великобританії, що був підключений до цієї системи.

Нова система використовує технологію ідентифікації за відбитками пальців: поліцейський за допомогою спеціального мобільного обладнання відсканує пальці людини, яка його зацікавила.

Отримані дані передаються в Національне агентство з поліпшення діяльності поліції (National Policing Improvement Agency /NPIA/), де вони перевіряються за загальнонаціональною базою відбитків пальців осіб, які зацікавлювали поліцію (наприклад: особи, котрі перебувають у розшуку).

Якщо здійснена перевірка дала позитивний результат, громадянин перепроваджується у відділення поліції для проведення подальших дій щодо нього; в іншому випадку він відпускається без проведення будь-яких дій стосовно нього, а дані про відскановані відбитки пальців видаляються з пам'яті мобільного обладнання та з бази даних системи біометричної ідентифікації.

Головною перевагою використання мобільного пристрою є суттєве зменшення часу, потрібного для встановлення особистості суб'єкта, який привернув увагу британських «боббі». Якщо раніше на цю процедуру було потрібно не менше години, то зараз ця дія триває не більш двох хвилин[1].

Розглянемо основні сучасні тенденції використання силовими структурами країн світу інформаційно-біометричних технологій.

Першою особливістю й основною рисою сучасності є масове запровадження уніфікованих багатомодельних мультибіометричних технологій ідентифікації людей для потреб спеціальних і правоохоронних органів.

Запровадження мультибіометрії зумовлено досвідом експлуатації ФБР у першому десятиріччі XXI століття бази даних (БД) зображень відбитків пальців 50 млн осіб. Було встановлено, що технологія ідентифікації за папілярними візерунками пальців дозволяє безпомилково ідентифікувати особистість у 99 випадках із кожних ста. А за 100-млн БД кількість помилкових ідентифікацій може становити 1 млн осіб. А це вже неприйнятна цифра для будь-яких силових структур.

Тому було запропоновано проводити перевірку фігурантів за декількома ідентифікаційними ознаками, що за висновками фахівців дозволяє практично здійснювати безпомилкову ідентифікацію осіб, яких перевіряють.

Крім того, невідомо, як будуть себе поводити бази біометричних даних на сотні мільйонів або декілька мільярдів людей. Тому резервні ідентифікатори запроваджуються для забезпечення масштабування нових біометричних БД[2].

Другою особливістю є розробка можливостей ідентифікування на значній відстані за такими біометричними показниками, як особливості ходи, стать та етнічна приналежність. Оскільки під час масових заворушень більшість їх учасників ховають свої обличчя

[1] Биометрические технологии повысят безопасность лондонского метро // BIOMETRICS.RU. – 2012. – 1 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

[2] Индия. При присвоении гражданам идентификационных номеров будут использоваться сведения о различных биометрических идентификаторах // BIOMETRICS.RU. – 2010. – 19 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

за масками і капюшонами, то нагальною потребою є ідентифікація за допомогою особливостей ходи фігурантів.

Учені Національної лабораторії фізики Великобританії (NPL) разом із Центром сучасних комп'ютерних технологій (CAST) і ще декількома британськими науковими закладами розробили систему розпізнавання людини за допомогою її ходи та силуету.

Спеціальна комп'ютерна програма обробляє відеокадри, що надходять із мініатюрних камер прихованого спостереження. У кожному кадрі силует людини відокремлюється від предметів навколишнього пейзажу, всі особливості її рухів фіксуються і перевіряються комп'ютерною програмою за відомостями спеціальної бази даних. Але ця технологія ідентифікації на великій відстані вимагає використання камер прихованого спостереження з дуже високоякісним розрішенням.

Ще однією обов'язковою умовою є наявність попередньо сформованої спеціальної бази даних з електронною інформацією про особливості рухів громадян країни, які зацікавлювали правоохоронні органи[1].

У Сполучених Штатах Америки Центр ідентифікаційних технологій та досліджень (CITeR) вивчає можливості ідентифікування індивідуумів на значній відстані за допомогою таких біометричних показників, як особливості ходи, етнічної приналежності та статі. Спеціалісти організацій та установ CITeR вважають, що технології, які сформовані на використанні цих показників, поки що не забезпечують проведення однозначної ідентифікації конкретної людини, але аналіз таких відомостей може сприяти пришвидшенню встановлення особистості.

Аналіз відеокадрів, що були отримані з відеокамер на відстані, може доповнювати процедуру ідентифікації за іншими біометричними показниками та підвищувати ефективність усього ідентифікаційного процесу. Інформація щодо особливості ходи, етнічної приналежності та статі особи, яка потрапила в зону відеоспостереження, доповнює інші біометричні відомості та допомагає зменшити діапазон можливих збігань і пришвидшує ідентифікацію. Практично біометрична система починає моніторити об'єкт спостереження та проводити збір відомостей про його ходу, зріст, вагу та стать на відстані понад сто метрів.

Розвиток таких видів систем є одним із науково-дослідних проектів, що розробляються в університетах, які входять до CITeR[2].

Також є цікавим європейський проект «Tabula Rasa», роботи з розробки якого проводяться в інституті «Idiap». Для підвищення якості ідентифікації осіб за їх обличчям, які можуть бути замасковані масками та капюшонами, «Idiap» розробляє спеціальне програмне забезпечення, котре передбачає ідентифікацію за кліпанням повік очей людини. Також досліджується можливість проведення розпізнавання за структурою шкіри різних частин обличчя[3].

Нині ще однією особливістю є пропозиція застосування біометричної ідентифікації покупців Sim-карт. Про плани введення біометричної ідентифікації покупців Sim-карт повідомляла Індія, а Нігерія, Пакистан і Саудівська Аравія вже реалізовують програми

---

[1] Новая система биометрической идентификации по походке изобретена в Британии // RT Russian. – 2012. – 25 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Американские специалисты изучают новые возможности биометрических технологий // Новости систем безопасности. – 2014. – 31 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Как повысить эффективность биометрических систем? // ZIV.RU. – 2014. – 24 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

біометричної ідентифікації власників Sim-карт[1]. Як відомо, мобільні телефони активно використовуються різними злочинними та терористичними формуваннями, тому біометрична ідентифікація власників «сімок» повинна згодом припинити цю практику. У Саудівській Аравії мета запровадження біометричних технологій – боротьба з «чорним ринком» продажу Sim-карт[2].

Також цікавим повідомленням є інформація щодо розширення застосування біометричних технологій за допомогою спеціального фонду, створеного Організацією Об'єднаних Націй для боротьби з піратством біля берегів Сомалі та суміжних країн. Передбачається створення бази даних відбитків пальців добропорядних учасників рибальського промислу та забезпечити до неї доступ міжнародних сил, що беруть участь в акціях проти піратів. У цьому випадку затриманим в Індійському океані будь-яким місцевим морякам досить буде пройти біометричну ідентифікацію, щоб довести свою непричетність до дій корсарів XXI століття[3].

Звісно, у межах невеликого за обсягом розділу неможливо повною мірою розкрити тему використання силовими структурами країн світу інформаційно-біометричних технологій для вирішення криміногенних проблем світової спільноти. З'являються нові розробки і тенденції в цій інноваційній галузі.

Автори посібника за своїх можливостей спробували якнайповніше висвітлити основні досягнення, тенденції та проблеми використання силовими структурами у своїй діяльності останніх досягнень біометричних технологій.

[1] Биометрическая идентификация покупателей SIM-карт может быть введена в Индии // BIOMETRICS.RU. – 2013. – 12 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Покупатели SIM-карт в Саудовской Аравии будут проходить биометрическую идентификацию // BIOMETRICS.RU. – 2013. – 19 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические технологии повысят эффективность борьбы с пиратством // BIOMETRICS.RU. – 2013. – 8 мая. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розділ 14

БІОМЕТРИЧНИЙ ЗАХИСТ ІНФОРМАЦІЇ ТА КОНТРОЛЬ ЗА ДОСТУПОМ У КОРПОРАТИВНИХ МЕРЕЖАХ ДО БАЗ ДАНИХ І ЕЛЕКТРОННИХ ПРИСТРОЇВ ЗБЕРІГАННЯ ДАНИХ

На межі XX–XXI століть інформація стала стратегічним ресурсом, завдання забезпечення інформаційної безпеки вийшло на державний рівень. Відбувся стрімкий розвиток інформаційних технологій, значно зросла необхідність одержання своєчасної та достовірної інформації, особливо в режимі реального часу (on-line).

Значущість сфери інформаційної взаємодії постійно зростає. Зміни в цій сфері, що відбулися через появу і розвиток такої технології, як Інтернет, часто порівнюють із змінами епохи початку книгодрукування. З одного боку, зросла роль персональної інформації в економічному, соціальному і культурному житті, але, з іншого боку – стало набагато складніше захистити своє приватне життя і бізнес від стороннього втручання. З'являється можливість одержання інформації незаконним шляхом. Інформація стала стратегічним ресурсом, а інформаційне середовище – сферою бойових дій.

У третьому тисячолітті спочатку в Сполучених Штатах Америки, а потім і в інших країнах розпочалося втілення програм повної інформатизації збройних сил. США першими розробили доктрину досягнення інформаційної переваги та ведення мережево-центричних операцій із використанням для керування військами єдиного інформаційного простору, що функціонує у реальному масштабі часу.

На початку нового тисячоліття комп'ютерна злочинність стала одним із найнебезпечніших видів злочинних посягань і, за оцінками експертів, вона здатна завдати збитки, які, наприклад, набагато перевищують матеріальну шкоду від крадіжок витворів мистецтва у всьому світі.

Наведені факти переконливо свідчать в актуальності проблеми захисту інформації, проте для того, щоб вона була вирішена необхідно визначити об'єкт захисту. Тому цілком природньо, що поняття захисту інформації розглядається як захист об'єктів інформації, які є носіями інформаційних даних та функціонування яких пов'язане з обробкою (створенням і передачею) і зберіганням інформації в електронному форматі, тобто у вигляді електронних документів.

Фахівці виокремлюють чотири типи об'єктів захисту інформації:

– засоби комп'ютерно-телекомунікаційної техніки;

– безпосередньо самі дані, які зберігаються, обробляються і передаються за допомогою засобів комп'ютерно-телекомунікаційної техніки;

– технології обробки даних;

– канали передачі даних.

Отже, гарантувати захищеність інформації можливо тільки у тому разі, коли забезпечений захист кожного з чотирьох видів вказаних об'єктів.

Зусилля розробників засобів захисту інформації були зосереджені в основному на створенні програмного забезпечення, яке реалізовувало ті або інші функції захисту. Але практичний досвід експлуатації таких розробок наочно продемонстрував обмеженість такого підходу і зумовив висновок про необхідність створення апаратно-програмного захисту[1].

В умовах швидкого розвитку глобального інформаційного суспільства і використання інформаційно-комп'ютерних технологій у всіх сферах життя особливого значення набувають проблеми інформаційної безпеки і, як наслідок, захисту інформації. З цією метою запроваджують функціональні та масштабні системи ідентифікації користувачів у інформаційних мережах, операційних системах і різних інших додатках до фірмового програмного забезпечення.

Згідно з визначенням, наведеним у Законі України № 537-V від 9 січня 2007 року «Основні положення розвитку інформаційного суспільства в Україні на 2007–2015 роки», «Інформаційна безпека – стан захищеності життєво важливих інтересів людини, суспільства і держави, при якому запобігається нанесення шкоди через: неповноту, невчасність та невірогідність інформації, що використовується; негативний інформаційний вплив; негативні наслідки застосування інформаційних технологій; несанкціоноване розповсюдження, використання і порушення цілісності, конфіденційності та доступності інформації».

Вирішення проблеми інформаційної безпеки повинне забезпечуватися шляхом:

– створення повнофункціональної інформаційної інфраструктури держави і забезпечення захисту її критичних елементів;

– підвищення рівня координації діяльності державних органів щодо виявлення, оцінки і прогнозування погроз інформаційній безпеці, попередження таких загроз і забезпечення ліквідації їх наслідків, міжнародна співпраця з цих питань;

– вдосконалення нормативно-правової бази для поліпшення забезпечення інформаційної безпеки, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронної діяльності в інформаційній сфері;

– розгортання і розвиток Національної системи конфіденційного зв'язку як сучасної захищеної транспортної основи, що спроможна інтегрувати територіально розподілені інформаційні системи, в яких обробляється конфіденційна інформація[2].

В умовах збільшення загроз, посилення взаємозв'язку комп'ютерно-інформаційних систем і зростаючої цінності даних, що зберігаються на комп'ютерних пристроях, підключених до Інтернету, власники цих даних починають переоцінювати свої методи контролю доступу. Існує необхідність переходу від перевірки правильності введеної разом із логіном інформації до гарантії того, що людина, яка вводить цю інформацію, є повноправним її власником.

Загалом у XXI столітті розвиток біометрії не міг бути таким успішним, якби на її базі не забезпечувався належний рівень безпеки. Нині практично жодна сучасна розробка систем і пристроїв безпеки не обходиться без застосування біометричних технологій. Особливо це стосується сучасного захисту інформаційних баз даних, персоналізації доступу до різних і приватних локально-корпоративних, і державно-відомчих інформаційних

[1] Вопросы защиты информации // Ежемесячный информбюллетень. – Борьба с преступностью за рубежом (по материалам зарубежной печати). – 2009. – № 3. – М.: ВИНИТИ. – С. 22–30.

[2] Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки: затверджено Законом України від 9 січня 2007 року № 537-V. [Електронний ресурс]. – Режим доступу: http://www.customs.gov.ua/dmsu/control/uk/publish/

мереж доступу до інформації, що зберігається на різних електронних носіях, а також контрольованого доступу на територію об'єктів, що охороняються.

Як показують дані статистичних досліджень, одну з суттєвих загроз корпоративним секретам продовжують становити інсайдерські загрози.

Інсайдерами вважаються штатні працівники підприємств або організацій, які навмисно, випадково або помилково перевищують свої повноваження під час роботи з інформацією, наслідком чого є порушення її цілісності, конфіденційності та доступності, тобто це в основному ті співробітники, які крадуть і «зливають» конфіденційні відомості, несанкціоновано модифікують і знищують інформацію, блокують доступ до неї, запускають у мережу різні «троянські» та «черв'ячні» програми, виконують низку інших аналогічних дій, що часом мають катастрофічні наслідки для власника інформаційної мережі або бази даних.

Ця проблема існує давно, змінюються лише можливості інформаційних технологій, а проблема захисту від інсайдерства залишається. Засобами периметрового захисту: міжмережевими екранами, системами виявлення та попередження несанкціонованого доступу, противірусними і протиспамовими і подібними продуктами ринок насичений, більшість організацій і підприємств, які мають можливість їх придбати, вже запровадили такі системи. Біометричні засоби захисту від інсайдерів (відповідна апаратура та технології, які забезпечують сучасний контроль за процесом ідентифікації або верифікації і, як наслідок, наданням права доступу, аналіз контенту та роботи пристроїв вводу-виводу) загалом для ринку СНД, зокрема й українського, недостатньо поширений.

Цілком можна погодитися з авторами книги «Безпечний аутсорсинг» Майклом Пауером і Роландом Тропом, які зробили висновок, що: «В міру зростання цінності даних, які накопичені організаціями і установами, у сторонніх осіб зростає інтерес до їх отримання, привласнення та неналежного використання». Із справедливістю цього висновку неможливо сперечатися, потрібно лише зауважити, що джерелом інформації для «сторонніх осіб» можуть бути не канали зв'язку і не пристрої несанкціонованого з'йому інформації, а працівники установи, в якій планується організація викрадення інформації, що становить певну цінність для замовників.

Повідомлення, що періодично з'являються в пресі, про чергову масштабну крадіжку баз даних із метою подальшого перепродажу цих відомостей на чорному ринку, безумовно, є наслідком не зламу мереж хакерами та несанкціонованого копіювання через Інтернет гігабайтів даних, а наслідком несанкціонованих дій інсайдерів, тобто адміністраторів баз даних або співробітників, які користуючись своїми службовими повноваженнями скопіювали та продали інформацію заради власної вигоди. І це тільки один із варіантів можливих виявів інсайдерської діяльності[1].

Можна виокремити такі дії персоналу, які можуть призвести до небажаних наслідків:

– отримання доступу до інформації, яка не потрібна для безпосереднього виконання своїх службових обов'язків (останній найбільш відомий приклад – копіювання секретних матеріалів АНБ Е. Сноуденом за допомогою паролів, які були надані йому колегами з АНБ);

– подолання існуючої системи захисту;

– неправомірне поводження з довіреною інформацією;

[1] Емелянников М. Защита от инсайдеров – проблема нетехническая / М. Емелянников // CIO-world.ru. – 2008. – 16 февраля. [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/analytics/cybercrime...

– невміння або небажання виконувати свої службові обов'язки професійно і відповідно до посадових інструкцій;

– помилкові дії.

Статистика свідчить, що у минулому десятилітті нашого сторіччя 71% порушень безпеки в компаніях відбувався за участю її власних співробітників, причому 80% із них мали шкідливу і дуже небезпечну звичку обмінюватися паролями[1].

На думку фахівців «SANS Institute» – однієї з провідних організацій у сфері навчання та аналітичних досліджень у питаннях IT-безпеки, – залишається подальша загроза так званих інсайдерських крадіжок даних, коли інформацію викрадають власні співробітники, яким у компанії цілком довіряють. Один із чинників зростання загроз із боку інсайдерів пов'язаний із тим, що вони можуть здійснювати атаку і «зсередини», перебуваючи у локальній мережі організації, і ззовні, використовуючи водночас відомі зловмисникові вразливі місця та паролі[2].

Ліпшим захистом від існуючих загроз інформаційній безпеці є превентивні заходи, а в цьому випадку – запобігання неправомірному доступу до інформаційних ресурсів. Оскільки завжди є ймовірність обходу навіть найвитонченіших превентивних заходів, тому в будь-якій корпоративній мережі повинні бути передбачені незалежні багаторівневі засоби моніторингу доступу, які дозволяють оперативно виявляти факти інсайдерської активності. Крім того, для мінімізації наслідків виявленого інциденту необхідні спеціальні заходи, які б давали змогу швидкого відновлення пошкоджених баз даних та інформаційних систем до фіксації юридично значущої доказової бази для кримінального переслідування зловмисників[3].

Одна з основних причин підвищеного інтересу злочинців до персональної інформації – поступовий перехід сучасного суспільства на безготівковий розрахунок. Тому цінність особистих відомостей зростає. З «віртуалізацією» економіки, розвитком «електронного» бізнесу виникає дедалі більше можливостей для шахрайських дій із використанням чужих персональних даних (identity theft). Отже, постійно зростає попит на такі відомості. Це і призвело до збільшення випадків витоку інформації. Цінність іншої конфіденційної та секретної інформації (державних таємниць, ноу-хау, комерційних таємниць), якщо в середньому і зростає, проте не такими темпами, як у випадку з персональними даними.

Для розробки технічних і організаційно-технічних засобів захисту від витоків надзвичайно важливе здійснення аналізу їх причин. Аналітики «InfoWatch» (відомості 2007 року) підрахували, що умисні інциденти («злочинний намір») становили лише 29%, а ненавмисні (нехтування правилами інформаційної безпеки та недбалість) – 71%. Отже, цілком зрозуміло, що навіть ігноруючи боротьбу з внутрішніми зловмисниками, а тільки шляхом запобігання інцидентам, які обумовлені випадковістю або недбалістю персоналу, можно практично на 3/4 знизити кількість інцидентів витоку інформації, а відтак й відповідні втрати. Для багатьох установ, організацій і фірм тільки виключення можливості ненавмисних витоків практично компенсує всі витрати на запровадження відповідних засобів систем безпеки.

---

[1] Парамонова Н. Проба сканера отпечатков пальцев BioLink U-Match MatchBook / Н. Парамонова. – 2007. – 13 апреля. [Электронный ресурс]. – Режим доступа: http://www.terralab.ru/input/

[2] Кибершпионаж расширяет свои границы // Osp.ru. – 2008. – 31 января. [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/analytics/...

[3] Емелянников М. Защита от инсайдеров – проблема нетехническая / М. Емелянников // CIO-world.ru. – 2008. – 16 февраля. [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/analytics/cybercrime...

Також необхідно акцентувати, що існує значна латентність щодо кількості зафіксованих випадків крадіжок або витоку інформації. Більшість випадків, які стали відомими громадськості, належать до витоку під час передачі даних і перевезення або пересилання носіїв із персональною інформацією. Тобто, широкому загалу факт витоку персональних даних стає відомим лише тоді, коли два або більше суб'єктів починають публічно перекладати відповідальність за інцидент один на одного або ж, коли факти щодо витоку інформації стали відомі стороннім. Але дуже мало оприлюднено випадків витоку даних всередині установ, організацій та фірм. Тобто практично існує практика приховування більшої частини фактів витоку конфіденційної інформації та нерепрезентативності статистики стосовно кількості таких випадків[1].

Упровадження тільки біометричних пристроїв захисту інформації, не кажучи про спеціальні захистні системи, які сформовані на інтеграції біометричних технологій з іншими інноваційними рішеннями, дозволяє набагато зменшити можливість витоку конфіденційної інформації.

Практично в установах і організаціях України дуже мало застосовується симбіоз таких технологій, як біометричний контроль за доступом до відповідних ресурсів, шифрування та процедура класифікації даних, хоча комбінація шифрування, класифікації та постійного моніторингу операцій із конфіденційною інформацією під час організації біометричного контролю за доступом здатна забезпечити відповідний захист, а у разі витоку інформації – полегшує встановлення осіб, які могли вчинити інсайдерські дії.

Останнім часом для технічного вирішення питань інформаційної безпеки дедалі більше використовуються апаратно-програмні засоби на основі біометричних технологій. Особливо слід зазначити реалізацію комплексних рішень на базі сучасних систем ідентифікації й аутентифікації.

Біометричні системи поєднуються з засобами криптографічного захисту, в яких доступ до ключів шифрування надається тільки після вдалого здійснення процедури біометричної ідентифікації (аутентифікації) їх власника. На думку експертів, нині використання систем безпеки на основі симбіозу біометричних технологій із криптографічним шифруванням є одним із найдієвіших способів, якщо не найдієвішим заходом із захисту таємної або конфіденційної інформації.

Питання боротьби з інсайдерами обов'язково повинне розглядатися у контексті реалізації єдиної політики безпеки, яка сьогодні є обов'язковим атрибутом будь-якої установи, підприємства або фірми. На Заході, якщо компанія не пройшла аудиторської перевірки на відповідність міжнародним стандартам щодо захисту персональних даних (HIPAA, SOX та інші), вона не отримує права на оголошення своїх фінансових показників і, як наслідок, рівень довіри до такої компанії – нульовий. На жаль, в Україні такі жорсткі вимоги поки що, як правило, ігноруються. Винятком є компанії, які беруть участь у міжнародній економічній діяльності.

Розглянемо головні причини, які сприяють або призводять до того, що дії порушників систем безпеки дозволяють досягнути їм своєї мети.

Перша причина: чим менша організація, тим менша інформаційна система, що використовується, тому часто функцію забезпечення інформаційної безпеки у такій установі виконують фахівці IT-підрозділу, які, якщо і розуміють потрібність захисних заходів, об'єктивно значно більше турбуються про такі складові цієї безпеки, як цілісність і доступність інформаційних масивів, а не про виконання заходів щодо недопущення ви-

[1] Внутренние IT-угрозы в России 2007–2008: итоги и прогнозы. [Электронный ресурс]. – Режим доступа: http://www.infowatch.ru/threats...

току конфіденційної інформації. Зрозуміло, що ефективна система захисту інформаційних ресурсів завжди є результатом компромісу між вимогами оперативності доступу до ресурсів і забезпечення їх безпеки.

Друга причина: система управління доступом до ресурсів не є достатньо ефективною, тому не забезпечує вирішення поставлених перед нею завдань. Процедура надання доступу до інформаційних масивів документально або не оформлена, або не виконується: наказом не призначені власники «особливих» ресурсів і відповідальні за їх використання, їх адміністрування знеособлене, будь-який адміністратор має або за бажанням може отримати доступ до бази даних. Як наслідок, практично кожний співробітник підприємства без службової необхідності може отримати доступ до будь-якого ресурсу, крім того, часто ціла група користувачів використовує одну і ту ж пару «логін – пароль» для роботи з тою або іншою програмою та електронним банком документів.

Третя причина, на яку часто не зважають, полягає у тому, що працівники фірм можуть бути не поінформовані про відповідальність за неправомірні дії з інформацією, доступ до якої обмежений.

Четверта причина полягає в тому, що інколи персонал просто не має навичків безпечної роботи в інформаційних системах. Можливий варіант, коли з вимогами або правилами інформаційної безпеки співробітників і ознайомили, але цей захід не досяг поставленої мети, оскільки на практиці ніхто не вчив більшість працівників потрібній методиці вибору паролю, щоб його не можно було легко вгадати або підібрати. Особам, які безпосередньо працюють на автоматизованих робочих місцях, у низці випадків не доводилося до відома про так звані правила «гігієни безпеки»: не залишати комп'ютер ввимкненим у разі виходу з кімнати, не записувати й нікому не передавати логіни та паролі, не залишати без нагляду аутентифікаційні пристрої, самостійно не завантажувати з оптичних дисків програмне забезпечення або інформаційні матеріали, не відвідувати «сумнівних» сайтів в Інтернеті, не відкривати додатки до електронних листів від невідомих відправників тощо.

Часто під час проведення навчальних заходів при ознайомленні з новою автоматизованою системою, початку експлуатації нових допоміжних комп'ютерних програм, що запроваджуються на підприємстві, не передбачається навіть коротких показових заходів, які б сприяли підвищенню практичних знань з інформаційної безпеки. В країнах із високим рівнем інформаційних технологій підвищення обізнаності персоналу давно стало однією з необхідних послуг на ринку комп'ютерно-інформаційної безпеки. У нашій державі переконати керівника виділити кошти для проведення навчання користувачів елементарним заходам інформаційної та комп'ютерної безпеки, зазвичай, вдається тільки після настання серйозної події з досить значущими наслідками.

П'ята причина: на підприємстві немає елементарного контролю за діями співробітників в інформаційній мережі або його безсистемне та недосконале ведення. Закономірність полягає у тому, що навіть найліпші заходи не досягнуть мети, якщо їх реалізація не буде систематично контролюватися. За відсутності належної організації виконання вимог інструкцій із безпеки їх просто починають ігнорувати та не виконувати.

Для усунення зазначених причин необхідна практична реалізація цілого комплексу організаційних і технічних рішень. Практичний досвід показує, що зазвичай організаційні рішення надто не змінюються з часом і щодо них існує достатня кількість спеціальної літератури. Тому детальніше розглянемо технічні рішення, що підтримують та забезпечують виконання організаційної складової інформаційної безпеки, а через невпинний розвиток комп'ютерно-інформаційних технологій дуже швидко змінюються. Технічна підтримка організаційних заходів повинна здійснюватися сучасним ефективним комплек-

сом технічних заходів із забезпечення комп'ютерно-інформаційної безпеки, а також обов'язковою реєстрацією практично всіх дій користувачів та контролем за дотриманням існуючих правил з роботи у корпоративній мережі.

Комплекс технічних заходів повинен забезпечувати реалізацію таких трьох груп захисних механізмів:

– управління процесами аутентифікації або ідентифікації та наданими користувачам правами доступу;

– організації блокування будь-яких неприпустимих дій користувачів;

– обов'язкової наявності копій баз даних (резервування інформації).

Організація нагляду за роботою користувачів має максимально знизити можливість їх несанкціонованих дій і містить контроль за:

– виконанням правил (політики) обраних заходів із забезпечення безпеки;

– доступом і використанням тільки суто потрібних для виконання своїх службових обов'язків баз даних і необхідного програмного забезпечення;

– процесом виконання деяких процедур;

– зовнішнім інформаційним взаємообміном осіб, які працюють на автоматизованих робочих місцях;

– додержанням наданих адміністратором мережі конкретному користувачеві електронних прав доступу;

– використанням зовнішніх пристроїв вводу-виводу.

Для успішної реалізації технічних захисних заходів у будь-якій установі або фірмі повинні бути затверджені правила безпеки, які відповідають обраній інформаційній політиці безпеки та які визначають конкретні заходи та порядок їх впровадження і використання[1].

До 11 вересня 2001 року біометричні системи забезпечення безпеки використовувалися тільки для захисту державних і військових секретів, а також найважливішої комерційної інформації. Парольна система ідентифікації, яка використовувалася тривалий час, довела свою повну неспроможність щодо захисту інформаційних систем, де потрібна достовірна ідентифікація користувача. Крім того, більшість паролів, що використовуються, в основному легко підібрати. Існує достатня кількість утиліт, що дозволяють, розпаковувати архіви, які захищені паролями. Якою б складною послідовністю символів не було парольне слово, його комбінацію практично завжди можна вирахувати – це питання тільки часу. Утиліти для підбору паролів здійснюють цю процедуру шляхом перебору слів, які містяться у великих за обсягом слів словниках.

Отже, практичне використання парольних систем створює більше проблем, ніж зручностей: пароль досить легко забути, а збереження секретного коду ще де-небудь суперечить самій концепції парольного захисту. Тут доречно навести вислів Джорджа Скаффа, віце-президента компанії «DigitalPersona» з маркетингу: «У ширшому контексті ідентифікації, адміністрування та загроз безпеці, які створюються нелегітимним використанням ключів для доступу до важливої інформації, використання паролів настільки загрожує національній безпеці Великобританії, що у запровадженні біометрії вбачається єдиний реальний вихід»[2].

---

[1] Емелянников М. Защита от инсайдеров – проблема нетехническая / М. Емелянников // CIO-world.ru. – 2008. – 16 февраля. [Электронный ресурс]. – Режим доступа: http://www.crime-research.ru/analytics/...

[2] Идентификация по отпечаткам пальцев – применения в бизнесе и промышленности // Secnews.ru. – 2006. – 18 декабря. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/foreign/...

Сьогодні біометрика розглядається як технологія, що надає «рівень надбезпеки», а не просто як засіб аутентифікації. Однак із розвитком загальних інформаційних мереж, віддаленого доступу та локальних мереж, які надають користувачам, що перебувають поза зоною дії внутрішніх засобів захисту, можливість доступу для роботи з корпоративними даними – це поняття дедалі більше зміщується у сторону значення первинної ідентифікації користувача.

У корпоративних мережах ідентифікація користувача з використанням систем біометрії, як правило, перший і основний крок для отримання доступу до даних. Біометрія, яка забезпечує доволі широкий набір інструментів для управління доступом, користується особливою популярністю у розробників архітектури безпеки. Вона використовується для формування такої інфраструктури безпеки, яка об'єднує в єдину захисну структуру технології відкритих ключів (PKI), сертифікатів і біометричної ідентифікації. Такі системи захисту забезпечують належний рівень надійності під час створення розгорнутих схем доступу[1].

Фахівці стверджують, що сьогодні одним із найбільш перспективних напрямів є розробка та виробництво *біометричних інтелектуальних систем безпеки.*

Ця технологія заснована на інтеграції досліджень у сферах електроніки, інформатики, медицини та біометрії, і, за прогнозами експертів, ринок продукції за цим напрямом неухильно зростатиме[2].

Зазначимо переваги використання систем безпеки, що застосовують біометричні технології:

– позбавлення користувачів від проблем, що виникають через втрату ключів і карток-посвідчень особистості, а також від необхідності запам'ятовувати ідентифікаційний код і паролі;

– унікальність біометричних характеристик кожної людини практично унеможливлює їх використання третіми особами або значно ускладнює процес підробки;

– «спілкування» користувачів із біометричним сканером відбувається доволі легко і вимагає мінімальних затрат часу;

– завдяки створенню спеціальних програмних і апаратних інтерфейсів процес розпізнання є зрозумілим і доступним людям будь-якого віку і не створює мовних бар'єрів;

– за потреби можна довести авторство тієї або іншої дії кожного звернення до системи шляхом збереження біометричних даних зловмисника[3].

Нині основу сучасних систем інформаційної безпеки створюють засоби ідентифікації або аутентифікації користувачів і управління їх доступом до корпоративних інформаційних ресурсів.

Наведемо вирішувані за допомогою технології ідентифікації (аутентифікації) основні завдання та вимоги до таких біометричних систем:

– однозначність розпізнавання користувача за унікальними, тільки йому одному характерними ознаками;

– неможливість викрадення, втрати, підміни ідентифікаційних ознак або заволодіння ними обманним шляхом;

---

[1] Боровко Р. Мировой рынок средств идентификации / Р. Боровко. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security/...

[2] Общие сведения о биометрии – 2007. – 25 июля. [Электронный ресурс]. – Режим доступа: http://www.biopassport.ru/ru/biometric/about/

[3] Преимущества биометрических систем безопасности. [Электронный ресурс]. – Режим доступа: http://www.npo-inform.com/biomert/preim/

– немає можливості передачі ідентифікаторів і відповідних повноважень іншим особам;

– реалізація принципу «неможливості відмови» користувача від проведення операцій, що були здійснені ним із застосуванням ідентифікаторів, які відповідають переліченим критеріям;

– ефективна інтеграція засобів ідентифікації і управління доступом в інформаційну інфраструктуру компанії зі збереженням безперервності поточних бізнес-процесів;

– зниження навантаження на користувачів, адміністраторів і фахівців із захисту інформації;

– мінімізація витрат, які виникають під час запровадження засобів ідентифікації й управління доступом;

– зменшення кількості відмов у роботі та можливість використання будь-якої за чисельністю користувачів системи контролю та управління доступом[1].

Біометричні рішення з захисту інформації для досягнення більшої ефективності слід застосовувати у комплексі з такими матеріальними ідентифікаційними носіями, як смарт-картки, токени та інші (так звана багатофакторна ідентифікація). У деяких із цих засобів захист ідентифікаційної інформації забезпечується шифруванням, генерацією одноразових паролів, електронним підписом і цифровими сертифікатами. Як правило, сучасна ефективна система біометричної ідентифікації виконує такі функції:

– уніфікації процесів доступу до інформаційних ресурсів на базі єдиного прийнятого для конкретної системи типу ідентифікатора або типів ідентифікаторів;

– захисту інформаційних ресурсів від несанкціонованого доступу або такого доступу, що здійснюється з порушенням встановлених правил (порушення прийнятої політики безпеки);

– автоматизації та централізації управління і контролю за діями користувачів шляхом створювання стосовно них облікових записів і наданням відповідних повноважень під час роботи з операційними системами та різними прикладними продуктами;

– пришвидшення доступу легальних користувачів до ресурсів корпоративної мережі з забезпеченням максимальної простоти та прозорості цього процесу;

– зменшення непродуктивних втрат, що спричинені помилками під час введення логіна та пароля і, як наслідок, блокуванням облікових записів і ін.;

– оптимізації діяльності системних адміністраторів через зменшення кількості звернень, які пов'язані з помилками користувачів під час проведення ідентифікації, аутентифікації та авторизації;

– швидкої реєстрації нових користувачів і можливості оперативної зміни облікових записів щодо співробітників, які перейшли в інший підрозділ, були звільнені або змінили свої функціональні повноваження[2].

Підсумовуючи наведене, можна однозначно стверджувати, що поширена майже скрізь комбінація імені та паролю може бути легко зламана. А генератори одноразових паролів (one time password /OTP/) можуть бути викрадені. Але злочинці не в змозі підробити відбитки пальців або інші біометричні ідентифікатори так легко, як вони підбирають паролі, а користувачі не можуть забути свої біометричні ознаки так, як вони забувають свої паролі. Тобто біометрія, по суті, є поки що єдиною технологією, що усуває всі ці негативні явища.

---

[1] Преимущества биометрических систем безопасности. [Электронный ресурс]. – Режим доступа: http://www.npo-inform.com/biomert/preim/...

[2] Защита информации. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/security.php…

Як вважають аналітики «Biometrics Research Group», біометричні технології мають значний простір для подальшого розвитку – особливо у великих корпоративних структурах. Зараз у них для ідентифікації співробітників застосовуються численні паролі, картки, токени, що призводить до значних витрат, пов'язаних із необхідністю адміністрування всіх цих застарілих засобів ідентифікації та підтримки працездатності відповідних баз даних. Водночас технології на базі біометрики здатні підсилити корпоративну безпеку, виключивши потребу в численних ідентифікаторах, які можуть бути з успіхом замінені на унікальні для кожної людини біометричні характеристики[1].

Біометрія впевнено увійшла до списку ключових технологій захисту інформації. Останніми роками відбулося значне підвищення інтересу до систем біометричної ідентифікації та аутентифікації. В цій галузі проводяться активні розробки й одним із ліпших нині варіантів можна вважати поєднання багатофакторної та мультибіометричної ідентифікації.

Компанія «IBM» у грудні 2011 року випустила свій щорічний список «Наступні п'ять через п'ять» (Five in Five), у якому наведені найбільш очікувані п'ять інновацій у найближчі п'ять років. Друга інновація в цьому списку стосується кібербезпеки – «IBM» стверджує, що до 2016 року людство практично зможе обходитися без паролів для доступу до різних ресурсів. Реєстраційні дані, які вводяться, змінить мультифакторна біометрика. Наприклад, сканування голосу людини зможе замінити паспорт, а відбиток пальця – пароль до електронної пошти. На думку експертів, сканування унікальних біологічних даних індивідуума допоможе вирішити проблеми крадіжок так званих звичайних ідентифікаційних даних[2].

Завдання забезпечення безпеки (і об'єктів, і інформації) з кожним роком стають дедалі більш серйозними та багаторівневими. В сучасних організаціях, незалежно від форм власності, спостерігається зростання кількості співробітників, що мають доступ до різних інформаційних систем, і збільшення найвикористовуваніших інформаційних підсистем.

Тому всі організації й установи, що в тому або іншому вигляді використовують інформаційні технології, стикаються з низкою проблем, які пов'язані з ідентифікацією та контролем доступу до інформаційних ресурсів. Це і збільшення кількості робочих місць адміністрування, і високий ризик можливих помилок адміністрування, а також величезна кількість ідентифікаторів і паролів, що використовуються одним користувачем[3].

Яскравим прикладом прив'язки посвідчення особи до її власника є інтеграція у Сполучених Штатах Америки в національні ID-картки держслужбовців біометричних параметрів. У Штатах через десятиліття після виходу Президентської директиви про національну безпеку (Homeland Security Presidential Directive 12 /HSPD-12/) Міністерство внутрішньої безпеки (МВБ) почало реалізацію амбіційного проекту з інтеграції в ID-cards біометричних параметрів. Базу даних держслужбовців США буде доповнено такими біометричними параметрами: електронні зображення обличчя, відбитків пальців і райдужної оболонки ока.

---

[1] Объем мирового биометрического рынка к 2015 году удвоится // BIOMETRICS.RU. – 2012. – 10 августа. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] IBM уверена в перспективах биометрических технологий // РИА Новости. – 2011. – 20 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Манова М. Конвергенция рынков ИБ, ИТ и технической безопасности набирает обороты / М. Манова // Cnews.ru. – 2008. – 24 октября. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security2008/articles/convergence.shtml.

ID-cards або PIV-карта (верифікація особистості) стане основним інструментом аутентифікації повноважень державного службовця для доступу до спеціальних послуг, мереж та інформаційних систем[1].

Як бачимо, Сполучені Штати Америки за допомогою реалізації одного заходу вирішують декілька проблем. Окрім організації контролю за доступом до службових приміщень або територій МВБ за допомогою PIV-карти, одночасно вирішує проблему організації чітко контрольованого та розподіленого за ієрархією доступу до комп'ютерів на робочих місцях, мереж та інформаційних систем організацій, установ і навіть держави. А запровадивши технологію контролю робочого часу, можна проконтролювати і час, проведений на робочому місці державним службовцем.

Відтак біометрія заощаджує час і гроші, підвищуючи водночас рівень безпеки. Ще на межі другого та третього тисячоліття вважалося, що запровадження біометричної технології триватиме довго – але на кінець першого десятиріччя XXI століття стало зрозуміло, що біометрія міцно увійшла до нашого життя і надалі відіграватиме дедалі важливішу роль.

Останніми роками застосування біометричних технологій стало одним із провідних і найефективніших напрямів у сфері безпеки. Одне з основних завдань у сфері безпеки – захист від несанкціонованого доступу до інформації, а біометричні системи разом з іншими інноваційними технологіями гарантують забезпечення доступу саме того користувача, який має відповідний дозвіл. Нині пристрої сканування різних біометричних ознак людини вбудовуються в різноманітні портативні пристрої: настільні комп'ютери, ноутбуки, планшети, смартфони, мобільні телефони та інші інформаційні пристрої з електронною пам'яттю. Біометричні системи виявилися зручними для використання і з погляду апаратно-технологічної реалізації, і забезпечення відповідного рівня безпеки. Зручні й доволі прості у використанні біометричні системи визначення автентичності власника або користувача дозволяють їм легко отримувати наданий рівень доступу.

Ще раз зазначимо, що однією з найбільших переваг біометричних систем захисту перед іншими методами забезпечення інформаційної безпеки є неможливість передачі користувачем своїх ідентифікаційних параметрів іншим особам. І це дуже важливо, адже у сучасному світі, на жаль, продається практично все, зокрема і доступ до конфіденційної інформації.

Людина, яка передала звичайні ідентифікаційні носії або повідомила пароль зловмисникові, практично нічим не ризикує. Про пароль можна завжди сказати, що його підібрали, а про апаратний ключ або смарт-картку – вкрали. У разі ж використання біометричного захисту подібний «фокус» вже не пройде.

Одним із недоліків біометричних систем захисту інформації є їх вартість. Але конкурентна боротьба на ринку біометричних пристроїв стає дедалі жорсткішою. Тому експерти ринку пророкують зниження з часом цін на всю біометричну продукцію. Ще одним і головним мінусом є можливість «крадіжок» біометричних ідентифікаційних даних. Детально це питання було розглянуто у 8 розділі.

Акцентуємо, що існують варіанти «крадіжок» самих електронних біометричних кодів-характеристик особи. Для того, щоб нівелювати наслідки такої «крадіжки», нині приділяють увагу розробці систем комплексної «наскрізної» мультибіометричної ідентифікації.

[1] Биометрические идентификационные карты в США обрели второе дыхание // Экспертный центр электронного государства. – 2013. – 23 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Як стверджують фахівці, таким новостворюваним системам будуть характерні дві унікальні риси. З одного боку, системи повинні забезпечувати ідентифікацію осіб у всіх місцях перебування на території об'єкта (офісу): від біометричного контролю за доступом на вході до об'єкта (будівлі або приміщення) до розпізнавання за біометричними ознаками під час проведення операції з завантаження операційної системи комп'ютера. З іншого боку, нова система буде проводити мультибіометричний контроль: у її рамках передбачається об'єднати технології ідентифікації за відбитками пальців, райдужної оболонки очей і обличчям (у перспективі можливо і приєднання й інших ідентифікаторів біометрії).

Розробники не приховують свого оптимізму, оцінюючи перспективи мультибіометричної системи «наскрізної» ідентифікації «від дверей до комп'ютера». Вони вважають, що таке комплексне рішення – це справжній подарунок для фахівців з інформаційної безпеки, оскільки воно дозволяє дійсно забезпечити централізоване управління фізичним і логічним доступом і практично виключає можливість наявності похибок під час ідентифікації особистості[1].

Також можливе використання багатофакторного режиму контролю за доступом, який також забезпечує високу надійність і ефективність, коли ідентифікація користувачів під час проходу через турнікет, шлюз і подібні пристрої здійснюється у різних комбінаціях із використанням відбитків пальців, безконтактних проксімити-карток і PIN-коду[2].

З погляду ефективності багатофакторний режим контролю доступу поступається системі «наскрізної» ідентифікації, але за ціною значно виграє.

В найближчі десять років біометрія однозначно буде займати основну позицію в системах безпеки. Біометричні технології згодом об'єднаються зі звичайними. Більшість людських особистих речей, навіть таких, як годинник, окуляри й одяг, будуть наділені можливістю розпізнання особистості власника. Непотрібно жодних паролів, просто відскануйте одну або декілька біометричних ознак і проходьте будь ласка далі. Отже, пристрої біометричної ідентифікації мають повністю замінити парольну практику.

З впровадженням компанією «Apple» біометричного сканера відбитків пальців у новий iPhone 5S розпочалася нова ера оснащення біометричними системами захисту індивідуальних пристроїв-гаджетів (iPhone, iPad, iPod). Усі гаджети згодом мають бути оснащеними біометричними сканерами. І це можна вважати тільки початком біометричної революції.

Незабаром біометричні сканери будуть запроваджені у майже все IT-обладнання та системи Інтернет-світу. Ідентифікація або аутентифікація буде здійснюватися за відбитками пальців, райдужною оболонкою очей, 3D-технологією розпізнавання обличчя та за голосом[3].

У наступні два роки на ринку мобільних пристоїв відбудеться бум технологій біометричної аутентифікації – прогнозують аналітики. Згідно з прогнозом агенства «Gartner», у 2016 році приблизно третина організацій земної кулі буде використовувати в своїй діяльності мобільні пристрої з засобами біометрії.

---

[1] Создается система «сквозной» мультибиометрической идентификации // BIOMETRICS.RU. – 2007. – 4 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Система учета рабочего времени и контроля доступа BioTime на выставке MIPS'2007 // BioLink www.biolink.ru. – 2007. – 13 апреля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[3] Apple как новый лидер биометрической революции // Appleinsider.ru. – 2013. – 23 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/

Зараз дедалі більше людей використовують для роботи особисті планшети та смартфони. Через що значно зростає ризик витоку інформації – мобільні пристрої можуть бути вкрадені, загублені або просто забуті.

Окрім того, багато користувачів використовують прості паролі, які легко можна підібрати. Для того, щоб захиститися від можливого витоку конфіденційної інформації, підприємства й установи незабаром будуть змушені впроваджувати біометричні засоби аутентифікації.

У грудні 2013 року компанія «Ericsson» провела опитування 100000 людей із 40 країн. 74% опитуваних надіються, що в 2014 році смартфони з засобами біометричної аутентифікації почнуть масово виробляти.

А згідно з даними, отриманими восени 2013 року корпорацією «PayPal», більша частина користувачів мобільних пристроїв бажали б замість пароля використовувати засоби біометричної ідентифікації: відбитки пальців (53%) і розпізнання за райдужною оболонкою ока (45%).

У першій половині 2014 року, крім смартфона iPhone 5S (виробник «Apple») і Galaxy S5 («Samsung»), масово гаджети інших фірм зі сканерами біометричних ідентифікаторів не випускалися.

В «Goode Intelligence» прогнозують, що наприкінці 2014 року зчитувачі біометричних показників мають з'явитися в мобільних пристроях Android і Windows Phone, а на початку 2015 року вони повинні стати обов'язковими для телефонів і планшетів хай-енд класу. 2018 року біометричні сканери мають стати невід'ємною складовою більшості мобільних пристроїв.

У компанії «Frost & Sullivan» прогнозують, що в найближчі декілька років під час проведення ідентифікації користувачів лідером у мобільному секторі буде технологія розпізнавання за відбитками пальців[1].

Компанія «PayPal» опублікувала результати свого дослідження, проведеного у вересні–жовтні 2013 року разом із «National Cyber Security Alliance», про безпеку мобільних обладнань. Дослідження довело, що американці фактично нерозлучні зі своїми смартфонами, дедалі частіше використовуючи ці пристрої для проведення грошових операцій. Водночас люди стурбовані безпекою своїх даних, які зберігаються у гаджетах та інших мобільних пристроях.

Більшість американців використовують смартфони для проплати за свої покупки. Приблизно 70% американців висловлюють занепокоєння щодо зберігання відомостей про платіжні операції у звичайних смартфонах. Загалом респонденти почували б себе у більшій безпеці за умови застосування додаткових заходів захисту.

Тому більшість американських користувачів дедалі частіше починають відмовлятися від традиційних паролів. Серед прихильників здіснення перевірок за біометричними методами аутентифікації типи бажаних технологій розподілилися так: сканування відбитків пальців (53%), далі – розпізнання за райдужною оболонкою ока й обличчям[2].

2013 року дуже актуальною темою стало збільшення кількості загроз для мобільних пристроїв. Чисельність зловмисних програм для смартфонів, як і в попередньому році, росла в геометричній прогресії. Найбільший удар завдали Android – на цю платформу було спрямовано приблизно 98,05% всіх відомих мобільних загроз. Однак найбільше

[1] Биометрическая революция на мобильном рынке // Телекомблог. – 2014. – 13 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Американские пользователи смартфонов хотели бы использовать биометрические технологии // Ferra. – 2013. – 14 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

занепокоєння в експертів викликав факт ускладнення мобільних зловмисних програм. Яскравим прикладом цієї тенденції є троян Obad, який з'явився у червні 2013 року, та на сьогоднішній день є найскладнішою багатофункціональною загрозою. Цей троян не тільки добре маскується та виконує безліч шкідливих команд, але також використовує нові методи поширення, наприклад, через мобільні ботнети[1].

Загалом біометричні технології – це принципово новий рівень безпеки об'єктів і конфіденційності інформації і, крім того, безсумнівна зручність для користувачів. Практика доводить, що системи безпеки, які сформовані на основі біометричного методу ідентифікації, мають суттєві переваги перед іншими засобами контролю доступу. А лідерство серед біометричних ідентифікаційних пристроїв поки що достатньо міцно продовжують утримувати пристрої ідентифікації за відбитками пальців.

Незважаючи на те, що біометричні системи самі собою вже забезпечують достатньо високий рівень безпеки, їх дедалі частіше поєднують з іншими технологіями. Найліпшим рішенням фахівці вважають біометричну ідентифікаційну картку з інтегрованим до неї надзвичайно тонким сканером відбитків пальців. Упровадження такого рішення дозволить звести до мінімуму кількість зовнішніх процедур, пов'язаних із обробкою персональних даних користувача, оскільки майже всі основні дії будуть проводитися самою картою, причому біометрична інформація не буде доступна будь-яким зовнішним пристроям.

Таку картку на замовлення Єврокомісії до кінця 2014 року мають розробити норвезька фірма «IDEX» і французька компанія «UINT».

Крім надзвичайно тонкого біометричного сканера, у смарт-карті мають бути застосовані бездротові технології «комунікацій близького поля» (near field communication /NFC/). Це означає, що власник карти зможе в безконтактному режимі використовувати її в різних платіжних системах (наприклад, для оплати проїзду в суспільному транспорті, вартості паркування, товарів у магазині і т. д.), швидко, легко та безпечно підтверджуючи свої повноваження на проведення відповідної транзакції[2].

Нагадаємо, що Сполучені Штати Америки в нових національних ID-картках держслужбовців розміщують в електронному форматі зображення обличчя, відбитків пальців і райдужної оболонки ока. ID-cards або PIV-карта (верифікація особистості) за допомогою проведення мультибіометричної аутентифікації підтверджують особистість власника. У позитивному випадку аутентифікації власник-держслужбовець за допомогою програми забезпечення ієрархії повноважень отримує доступ до спеціальних послуг, мереж та інформаційних систем[3].

Одним із найнадійніших методів захисту безумовно є криптографічний метод захисту, оскільки охороняється безпосередньо сама інформація, а не доступ до неї (наприклад, зашифрований файл не можно прочитати навіть у разі крадіжки носія). Мета криптографії проста: зробити зрозуміле («відкрите») повідомлення цілком незрозумілим («закритим») для тих, хто не має відповідного ключа. Ця мета досягається за допомогою кодування, а те, що отримується у підсумку, називається криптограмою.

---

[1] Борцы с вирусами предсказывают скорое исчезновение интернета // РБК. – 2013. – 11 декабря. [Электронный ресурс]. – Режим доступа: http://top.rbc.ru/society/11/12/2013/...

[2] Еврокомиссия профинансировала разработку биометрической смарт-карты // BIOMETRICS.RU. – 2012. – 19 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Биометрические идентификационные карты в США обрели второе дыхание // Экспертный центр электронного государства. – 2013. – 23 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Дуже цікавою є можлива інтеграція біометричних і криптографічних технологій, тобто доповнення біометричних технологій криптографічними. У доповіді «Біометричне шифрування: позитивна сума технологій» канадських експертів Енн Кавокян і Олексія Стоянова, опублікованому свого часу на сайті інтернет-видання «InterGovWorld», зроблено висновок про те, що інтеграція біометричних і криптографічних технологій створює нові перспективи строгої ідентифікації, забезпечення інформаційної безпеки та захисту персональних даних. Автори доповіді розглядають такі два можливі напрями інтеграції біометрії і криптографії.

З одного боку, інформація щодо біометричних ідентифікаторів містить досить «чутливі» для їх власника дані, які йому конче необхідно надійно захистити, зокрема й за допомогою технологій шифрування. З іншого – тільки застосування біометричного ідентифікатора (відбитка пальця, райдужної оболонки очей або 3D-зображення обличчя особи) як унікального криптографічного ключа, що не піддається підробці або викраденню, дозволяє користувачеві реально контролювати доступ до зашифрованої інформації.

Розвиток цих двох напрямів і дозволяє говорити про «біометричне шифрування», як іменують результати синтезу двох технологій автори доповіді. На їхню думку, «біометричне шифрування водночас забезпечує як конфіденційність персональних даних, так і переваги безпеки»[1].

Нині у світі дедалі активніше розвиваються та запроваджуються комплексні біометрично-криптографічні комп'ютерні технології, скеровані на забезпечення захисту та працездатності таких комплексних і масштабних мережевих застосувань, як електронний банкінг (e-banking), електронна торгівля (e-commerce) і електронний бізнес (e-business).

У світовій спільноті є і поетапно вирішуються завдання розробки, вдосконалення та впровадження таких найважливіших технологій захисту інформації, як:

– нові стандарти електронно-цифрового підпису (ЕЦП);

– масштабована система електронних цифрових сертифікатів із використанням центрів довіри;

– криптографічно захищені корпоративні (віртуальні) комп'ютерні мережі та засоби міжмережевого екранування;

– засоби антивірусного захисту та засоби захисту від несанкціонованого доступу до інформації для неоднорідно розподілених інформаційних систем;

– моніторинг і аудит безпеки мережевих інформаційних ресурсів;

– захищені програмно-апаратні засоби для IP-телефонії;

– засоби захисту мереж мобільного зв'язку та персональних комунікацій;

– засоби біометричної ідентифікації, а також персональних засобів криптографічного захисту інформації та засобів аутентифікації на базі інтелектуальних карт та інших малогабаритних технічних засобів обробки інформації.

Розвиток зазначених перспективних технологій захисту інформації вимагає, з одного боку, застосування нових математичних і криптографічних рішень (наприклад, криптоалгоритмів на основі еліптичних кривих, методів квантової криптографії, фрактальних алгоритмів стискання даних), а, з іншого – істотно залежить від прогресу розвитку світових мікропроцесорних, алгоритмічних, програмних та інших суміжних технічних рішень.

У розробці біометричних технологій ідентифікації доволі добре зарекомендували себе такі компанії, як «Compaq», «Identix», «Veridicom», «Key Tronic», «Miros»,

[1] Биометрия и шифрование: позитивная сумма технологий // BIOMETRICS.RU. – 2007. – 18 июля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

«Visionics», «Microsoft» і інші. Вони використовують такі принципи забезпечення безпеки інформаційних систем:

– законність заходів щодо виявлення та запобігання правопорушенням в інформаційній сфері;

– безперервність реалізації та вдосконалення засобів і методів контролю й захисту інформаційних систем;

– економічна доцільність, тобто проведення аналізу величин можливих збитків і витрат під час створення необхідного рівня безпеки інформації;

– комплексність використання всіх захисних засобів у всіх підрозділах підприємств і установ на всіх етапах інформаційного процесу[1].

В інформаційному співтоваристві біометрія з широким асортиментом інструментарію для управління доступом особливо затребувана сучасними розробниками архітектури безпеки. Біометрика також застосовується для створення такої архітектури безпеки, яка ґрунтується на використанні електронних сертифікатів й інфраструктури відкритих ключів (PKI). Засоби ідентифікації з застосуванням біометричних технологій забезпечують належний рівень надійності під час створення розгорнутих схем доступу. В розвинутих країнах ідентифікація користувача з використанням систем біометрії є основним та обов'язковим кроком для отримання дозволу доступу до будь-яких відомостей у корпоративних мережах[2].

Державна програма США під назвою PRISM охоплювала проведення масових перехоплень розмов телефоном, переписки в Інтернеті та всіх видів діяльності в соціальних мережах і іноземців, і американських громадян. Агентство національної безпеки (АНБ) США може проникати в операційні системи та зчитувати дані зі смартфонів будь-якого виду – від iPhone до Android і Blackberry. Про це повідомила «Deutsche Welle» з посиланням на секретні матеріали розвідки. АНБ може копіювати списки контактів, SMS-повідомлення, записні книжки, а також визначати місцезнаходження власника смартфона[3].

Фахівці, які займаються проблемами забезпечення комп'ютерно-телекомунікаційної безпеки, заявляють про ймовірність вразливості важливих елементів інфраструктури будь-якої розвинутої країни, особливо різних комп'ютерно-інформаційних мереж, зокрема й таких, що керують роботою електростанцій (у т. ч. і атомних), електромереж, транспорту, систем водопостачання, пропускною спроможністю захисних дамб, гребель та інших життєво важливих об'єктів.

Нині негативний інформаційний вплив може відчути будь-яка держава, тобто всі її державні структури й установи, промислові корпорації та цивільне населення країни. Така ситуація потребує створення єдиних органів управління інформаційною протидією. Потрібні органи інформаційної безпеки як в державних структурах і установах, так і в промислових корпораціях. Необхідно, щоб хтось офіційно відповідав за виявлення інформаційних погроз, оцінював уразливість відповідних структур, визначав критичну інформацію, втрата якої може завдати серйозних збитків, оцінював ризик та визначав заходи з нейтралізації інформаційних погроз. Тобто необхідне створення спеціальних

[1] Минаев В. Современные технологии обеспечения информационной безопасности / В. Минаев. – 2008. – 31 января. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Боровко Р. Мировой рынок средств идентификации / Р. Боровко. [Электронный ресурс]. – Режим доступа: http://www.cnews.ru/reviews/free/security/part2/

[3] Разведка США считывает данные с любого смартфона // Четверта влада. – 2013. – 8 сентября. [Электронный ресурс]. – Режим доступа: http://4vlada.net/smi/...

державних органів, які б займалися розробкою заходів із захисту від негативного інформаційного впливу та проведення відповідних контрдій.

У другому десятиріччі XXI століття експерти прогнозують все зростаючу загрозу кіберпротистоянь між розвинутими країнами.

Дедалі більша кількість населення Землі освоює роботу в Інтернеті. Величезний інформаційний ресурс стає доступним кожному бажаючому. Сфера бізнесу вимагає розробки нових методик, новітніх технологій, впровадження винаходів, які розробляються на базі досягнень сучасних ІТ-технологій. Таємні державні матеріали також зберігаються в електронному форматі на різних закритих ресурсах. Комп'ютеризація та інформатизація суспільства має і інший бік: вони призвели до такого негативного явища, як викрадення електронних таємних або конфіденційних відомостей із державних установ і приватних компаній, а в найгіршому варіанті – порушення та навіть блокування роботи управлінських інфраструктур цілих державних галузей.

На думку експертів, під час кібератак особливій загрозі піддаються житлово-комунальна інфраструктура та транспорт. Порушення функціонування інфраструктурних систем може призвести до кризи і навіть можливе знищення державної системи управління в будь-якій країні. Вже не є секретом, що багато держав фінансують розробки в галузі створення кіберзброї, яка здатна стати засобом шпигунства і причиною збоїв роботи в інфраструктурних системах.

Нинішній рівень розвитку технологій надає змогу хакерам підключатися до управління будь-якої атомної станції, нафтогазового об'єкта або транспортного вузла, які мають вихід в інтернет, і перебрати керування ними під свій контроль. У всіх цих випадках значно зростає ймовірність техногенних катастроф.

Деякі країни, найперше Сполучені Штати Америки, Китай, Росія й Ізраїль, вивчають не тільки можливості кібервійн, а вже на практиці випробовують свої наробки. Якими можуть бути ці можливості у повному обсязі та як могли б виглядати основні дії кібервійни? – все це утаємничено. Але ті країни, які першими оволодіють мистецтвом кібервійн, зможуть отримати фундаментальну перевагу над супротивником на початкових стадіях конфлікту. Вивід із ладу комунікаційних систем перед початком активної фази бойових дій – це стандартна військова практика.

Проводячи свою передвиборчу кампанію в липні 2008 року, Барак Обама назвав організацію кібербезпеки одним із найпріоритетніших завдань, що стоять перед Сполученими Штатами Америки. «Ставши президентом, я дам кібербезпеці пріоритет, якого вона і заслуговує в 21-му столітті», – сказав він. У своєму виступі Б. Обама також порівняв кібернетичні загрози з ядерною і біологічною зброєю[1].

Реалії сьогодення такі, що у кібернетичному просторі військові дії ведуться доволі активно. У листопаді 2012 року в повідомленні одного з провідних американських видань була оприлюднена інформація про те, що на комп'ютерну мережу Білого дому була проведена кібератака. Фахівці вважають, що напад провели хакери, які працюють на уряд Китаю. Комп'ютерним злочинцям, за твердженням видання, вдалося одержати доступ до системи військового управління Президента США. До речі, саме через цю мережу керують американським ядерним арсеналом. Адміністрацією президента було надано доручення федеральним агентствам розробити нові програмні продукти для забезпечення належної безпеки урядових мереж.

[1] Пит Уоррен. США и Великобритания готовят ответную атаку против восточных хакеров / Уоррен Пит // Inosmi.ru. – 2009. – 5 июня. [Электронный ресурс]. – Режим доступа: http://www.inosmi.ru/translation/...

Але американці теж готуються до кібервійн. Ще в червні 2011 року Бараком Обамою були підписані документи, що дозволяли військовому відомству США в рамках забезпечення кібернетичної безпеки держави, проводити кібератаки проти супротивників США у разі хакерських нападів й існування загроз інформаційним інфраструктурам найважливіших об'єктів держави.

Можливість подібних дій включена у військову стратегію Сполучених Штатів Америки. У жовтні 2012 року міністр оборони США повідомив, що на розробку невідкладного програмного забезпечення для військових потреб виділено понад 3 млрд доларів, а в ці витрати можуть сягти 120 млрд доларів.

Американські військові експерти вважають, що Китай є найнебезпечнішим об'єктом у кіберпросторі. Вони стверджують, що програмісти розвідувальних структур Піднебесної здійснюють постійні атаки з метою викрадення таємної інформації з американських урядових і комерційних комп'ютерних систем.

Поряд із китайськими найталановитішими комп'ютерними хакерами вважають фахівців Франції, Ізраїлю та Росії. На відміну від своїх китайських колег, вони більшою мірою займаються кіберрозвідкою, а не крадіжкою комерційних секретів для потреб свого вітчизняного бізнесу. Згідно з оприлюдненими даними, у 2012 році в США було зареєстровано понад 160 кібератак на ресурси найважливіших державних об'єктів.

Учасники міжнародного форуму з кіберзахисту, який відбувся у грудні 2012 року, обґрунтовано довели той факт, що однієї з гострих сучасних проблем світових інформаційних технологій є виникнення кібертероризму. Адже будь-яка розробка, що була здійснена фахівцями тієї чи іншої країни для ведення кібервійн, може згодом опинитися в руках терористів, які зможуть використовувати її для досягнення своєї мети[1].

Американська фірма «Mandiant», яка працює в сфері Інтернет-безпеки, на початку 2013 року звинуватила владу Китаю у причетності до масштабної серії кібератак проти урядових закладів, компаній і об'єктів інфраструктури США. Сліди атак ведуть до Шанхаю, де розташована штаб-квартира секретного китайського підрозділу – військової частини 61398 Народно-визвольної армії Китаю.

В центрі уваги 60-сторінкової доповіді, підготовленої фірмою «Mandiant», виявилися два китайські хакерські угруповання – «Реферативна команда» і «Шанхайська група». Серед їхніх жертв виявилися корпоративні комп'ютерні системи компаній та фірм, що представляють 20 секторів господарства Сполучених Штатів Америки – енергетики, ВПК, нафтохімії, автомобілебудування, телекомунікацій, видобувної, аерокосмічної, харчової промисловості та низки інших.

Як стверджують фахівці «Mandiant», у всіх цих американських компаніях китайські хакерські угруповування викрали величезний обсяг даних. Завдані збитки оцінюються в сотні мільярдів доларів.

У лютому 2013 року президент США Барак Обама підписав розпорядження, яке спрямоване на захист державних структур і бізнесу від зростаючих загроз кібератак, насамперед із Китаю.

Розпорядженням санкціонується передача стратегічно важливим компаніям попереджувальної інформації про можливість кіберзагроз. Документ також визначає поняття критично важливої інфраструктури. До неї належать фізичні або віртуальні об'єкти, системи й активи, руйнування яких може завдати значних збитків державній безпеці, національній економіці та системі охорони здоров'я.

[1] Бовал Валерий. Реальная угроза – киберпротивостояние / Валерий Бовал // Военное обозрение. – 2012. – 19 декабря. [Электронный ресурс]. – Режим доступа: http://topwar.ru/...

Б. Обама доручив Національному інституту стандартів і технологій розробити стратегію і шляхи захисту інфраструктури від хакерських атак. Перша версія цього документа повинна бути підготовлена протягом 2013 року[1].

Розкриття Едвардом Сноуденом засекреченої інформації АНБ про тотальну електронну розвідку США та Великобританії за всім світом спровокувало пришвидшення розробок у галузі інформаційної безпеки та реалізації програм захисту і на державному, і на корпоративному рівнях. Особливе значення серед оприлюднених матеріалів має інформація про системи наступальної кіберзброї, які, як виявилося, вже були неодноразово використані американськими, англійськими та ізраїльськими спецслужбами проти інших країн.

Найгучнішим був скандал із виведенням з ладу іранської АЕС спеціально створеним для атаки на об'єкти енергетичної інфраструктури вірусом Stuxnet. Після іранської атомної електростанції атакам були піддані стратегічні об'єкти в інших країнах-конкурентах, у яких розвиток галузі кібербезпеки перебуває на більш високому рівні, ніж в Ірані. Нападу зазнали Управління енергосистемами Пекіна в Китаї, атомна електростанція в Росії та блок керування російським модулем на міжнародній космічній станції (МКС).

За наявною інформацією, розробками ефективних систем протидії загрозам у кіберпросторі з 2013 року зайнялися практично всі держави світу, навіть такі невеликі країни, як Куба та В'єтнам. А наша північна сусідка після Сполучених Штатів Америки та країн НАТО теж оголосила про створення Кіберкомандування, яке повністю буде домінувати в питаннях інформаційної безпеки серед спецслужб Російської Федерації (ФСБ, ФСО, ФСТЕК).

Пріоритетну увагу інформаційній безпеці почали приділяти і комерційні компанії, особливо виробничого типу. За оцінкою Всесвітньої асоціації електронних комунікацій, ринок захисного програмного забезпечення вже з серпня 2013 року показував «вибуховий» ріст, особливо в сфері систем шифрування, де світовий попит буквально за 3 місяці зріс у 2,5 рази[2].

У лютому 2013 року газета «The Guardian» (Великобританія) оприлюднила відомості щодо розробки мультинаціональною компанією «Raytheon» (працює в галузі безпеки) програми «RIOT», яка використовується для збору даних у соціальних мережах. Комп'ютерна програма дозволяє стежити за пересуванням людей та передбачати їхню поведінку в майбутньому за допомогою відомостей, розміщених на веб-сайтах соціальних мереж. Масштабна аналітична система «RIOT» (Rapid Information Overlay Technology), яка розроблена компанією, збирає величезні обсяги інформації про людей на веб-сайтах Facebook, Twitter і Foursquare.

Представники фірми «Raytheon» стверджують, що вони ще нікому не продали розроблений ними софт. Однак фірма визнала, що в 2010 році вона поділилася розробленою технологією з американськими урядовими структурами в рамках загальних зусиль, які вживаються в галузі науково-дослідних і дослідно-конструкторських робіт для надання допомоги під час створення системи національної безпеки, здатної аналізувати «трильйони даних» із кіберпростору.

---

[1] Паниев Юрий. Кибервойну с Америкой ведут китайские хакеры в погонах / Юрий Паниев // Независимая газета. – 2013. – 20 февраля. [Электронный ресурс]. – Режим доступа: http://www.ng.ru/world/...

[2] Тихонов Сергей. Кибервойну с Америкой ведут китайские хакеры в погонах / Сергей Тихонов // Forum.polismi.org. – 2013. – 16 ноября. [Электронный ресурс]. – Режим доступа: http://oko-planet.su/politik/politwar/...

За допомогою системи «RIOT» можна одержати повний «моментальний знімок» приватного життя людини, який серед інших відомостей охоплює інформацію про друзів, місця відвідувань із прив'язкою їх до карти, причому для цього достатньо тричі клікнути мишкою.

«RIOT» здатен представити у вигляді павутинної діаграми (spider diagram) зв'язки та відносини між онлайновими індивідуумами, тобто проаналізувавши дані про те, з ким особа контактувала у мережі Twitter. Крім того, ця суперпрограма здатна «витягати» відомості з порталу Facebook, а також аналізувати інформацію GPS з Foursquare – мобільного додатка, яким користуються понад 25 млн людей для того, щоб повідомляти друзям про своє перебування. Інформація з сервісу Foursquare може бути використана для того, щоб представити в графічній формі десять основних місць, які відвідує фігурант, із вказанням часу їх відвідування.

Джаред Адамс (Jared Adams), який є офіційним представником відділу фірми «Raytheon», що займається розвідувальними й інформаційними системами, так охарактеризував цю розробку: «Програма «RIOT» є системою аналізу великих даних (big data), над створенням якої ми працюємо разом із представниками промисловості, національними лабораторіями та комерційними партнерами для того, щоб перетворити великі масиви даних у корисну інформацію з метою задоволення швидкозмінних потреб нашої національної безпеки».

У грудні 2012 року компанія «Raytheon» одержала патент на основні інноваційні рішення розробки «RIOT».

Урядове управління США за контролем у сфері торгівлі надав цій технології експортну категорію «EAR99», яка надає право на поставку без ліцензії значній кількості покупців[1].

Наведемо відомості дослідження аналітичного центру «Infowatch», згідно з яким у 2012 році було скомпрометовано понад 1,8 млрд записів, зокрема з фінансовими та персональними відомостями.

За інформацією «Infowatch», у ЗМІ було оприлюднено 934 випадки витоку конфіденційних даних, що на 16% перевищує показник 2011 року. Тільки прямі втрати компаній, інформація щодо яких в зв'язку з витоком конфіденційних даних була опублікована у відкритих джерелах, становили понад 37,8 млн доларів.

Проведений аналіз встановив, що відсоток випадкових витоків знижується (в 2012 році їх частка становила лише 38%), а частка зловмисних витоків зростає і сягла 46%. Перше місце за видом витоків, як і раніше, посідають персональні дані – 89,4% (в 2011 році – 92,4%)[2].

Дуже песимістичним є прогноз експертів «Лабораторії Касперського», який присвячений підсумкам 2013 року. Фахівці вважають, що у майбутньому Інтернет у його звичному глобальному розумінні може зникнути, а на його місце прийдуть десятки окремих національних мереж з обмеженим доступом до іноземних ресурсів.

Причинами можливого обмеження доступу до Всесвітньої павутини є щорічне збільшення та посилення якості загроз користувачам віртуального простору. Експерти

[1] Гэллагер Райан (Gallagher Ryan). Оборонная фирма разработала программу, позволяющую следить за людьми в социальных медиа / Райан Гэллагер (Ryan Gallagher) // Оригинал публикации от 10 февраля 2013 г. в газете «The Guardian»: «Software that tracks people on social media created by defence firm» // Inosmi.ru. – 2013. – 13 февраля. [Электронный ресурс]. – Режим доступа: http://www.inosmi.ru/world/...

[2] Сайты незаконно собирают информацию о пользователях (мнение) // Четверта влада. – 2013. – 20 марта. [Электронный ресурс]. – Режим доступа: http://4vlada.net/smi/...

зазначають, що такому висновку сприяли викриття Едварда Сноудена та поява нового типу кіберзлочинців.

2013 рік характеризувався появою кібернайманців – невеликих хакерських груп, які спеціалізуються на проведенні блискавичних атак на замовлення. Ці зловмисники скрупульозно вибирають своїх жертв і з хірургічною точністю завдають удари, а потім вправно «замітають сліди».

Того ж року сформувалася небезпечна тенденція зміщення акцентів у засобах досягнення зловмисниками своєї мети: замість застосування широкого набору шкідливого програмного забезпечення для зараження комп'ютера кіберзлочинці почали дедалі частіше використовувати так званий людський фактор. Про це свідчать, наприклад, збільшення кількості атак типу «watering hole», коли зловмисники навмисно «заражають» часто відвідуваний користувачем веб-ресурс, навіть якщо він і користувач не є їхньою кінцевою метою.

Такий підхід дає злочинцям великі шанси для проникнення в корпоративну мережу за мінімальних затрат. Саме атаки типу «watering hole» дозволили хакерам успішно провести атакуючу кампанію, спрямовану на сайти тибетських і уйгурських активістів[1].

Нині хакерство перетворилося на прибутковий бізнес. Як вважають західні експерти, він особливо поцвітає на теренах колишнього СРСР. За оцінками деяких фахівців, у 2011 році оборот усіх російськомовних хакерів (включаючи зловмисників із України та Прибалтики), становив від одного до трьох мільярдів доларів. Для кібертерористів атаки на чужі комп'ютери є дуже прибутковим бізнесом. Вартість однієї організованої вдалої атаки із викрадення таємної інформації становить 3–12 млн доларів. А кібератака на програмне забезпечення промислового або військового об'єкта коштує замовникам у середньому в 5 разів більше[2].

За повідомленнями ЗМІ, на початку XXI століття російська мережева злочинність утворила свій професійний діловий простір. Різні угруповування об'єдналися у союз. Своїх партнерів вони знаходять через знайомих або за допомогою так званої «циганської» пошти. Російською особливістю можна вважати службу гарантів, яка не має жодного відношення до вірусів. Ці гаранти мають таємні хакерські форуми та мережі, де вони є нейтральними посередниками, схвалюють кримінальні угоди і стежать за тим, щоб ніхто нікого не обманював. За це вони одержують свою частку від вартості хакерських дій, яка може сягати до 40% від обсягу угоди.

Так звані DDoS-атаки, за допомогою яких підприємці-замовники ускладнюють роботу сайтів конкурентів або взагалі їх блокують, є найпоширенішими, а вартість такої послуги становить лише кілька сот євро. За інформацією провідного спеціаліста з вірусів «Kaspersky Lab» Олександра Гостєва: «Оборот російського спам-бізнесу, що займається розсилкою електронних повідомлень, на які не надходили запити від користувачів інтернету, становить від 300 до 400 мільйонів доларів у рік».

Послуги хакерів, ціни вірусів – усе регулює сірий ринок. Троянська програма «Zeus» в оновленій версії коштує приблизно 5 тис. доларів. За ці гроші покупець одержує технічну підтримку, а також оновлення, як тільки проплачений вірус буде виявлений антивірусною програмою.

---

[1] Борцы с вирусами предсказывают скорое исчезновение интернета // РБК. – 2013. – 11 декабря. [Электронный ресурс]. – Режим доступа: http://top.rbc.ru/society/11/12/2013/894134.shtml.

[2] Бовал Валерий. Киберпротивостояние-2013: прогнозы экспертов / Валерий Бовал // Военное обозрение. – 2013. – 21 января. [Электронный ресурс]. – Режим доступа: http://topwar.ru/...html.

Віруси поширюються через браузери та заражені веб-сайти. Від кількості заражених комп'ютерів і країни атаки залежить ціна послуги. Найдорожче – заразити західноєвропейські та американські комп'ютери[1].

Підприємства, установи й організації всіх форм власності можуть організувати свою безпеку, відокремивши особливо важливі частини своєї IT-системи від всесвітньої мережі. Також треба застосовувати тільки вибрані, заздалегідь перевірені та рекомендовані фахівцями комп'ютерні програми. А працівники повинні мати доступ тільки до таких відомостей та додатків, які потрібні їм для роботи. Так радить захищатись від зловмисників засновник «Лабораторії Касперського» Євген Касперський[2].

Сегмент продаж пристроїв інформаційної безпеки стійко зростає: за оцінкою «International Data Corporation» (IDC) до 2015 року він буде в середньому зростати на 27% щорічно[3].

Останнім трендом застосування біометрії є використання біометричних сканерів у різних мобільних пристроях і гаджетах, серед яких iPhone, iPad й iPod. Експерти прогнозують, що в майбутньому біометричні технології масово будуть застосовуватися не тільки в різному комп'ютерному обладнанні, мобільних пристроях та Інтернет-технологіях, а і в різних особистих речах, наприклад, такі, як електронні годинники, окуляри та навіть одяг[4].

Діюча в Британії дослідницька компанія «Goode Intelligence» ще у 2011 році опублікувала огляд ринку біометричних продуктів і послуг для мобільних пристроїв. Експерти «Goode Intelligence» визначили кілька можливих напрямів розвитку проаналізованого ринку.

Перший із цих напрямів – забезпечення захисту від несанкціонованого доступу як до самих мобільних пристроїв, так і функціонуючих у їхньому складі різних додатків і даних, що зберігаються у пам'яті гаджетів. Нині дедалі більша кількість компаній видає своїм співробітникам мобільні пристрої та дозволяє працівникам користуватися своїми гаджетами в корпоративних системах, що вимагає більш безпечної й надійної ідентифікації й авторизації.

Другий напрям – запровадження мобільної комерції та безконтактних технологій «зв'язку на близькій відстані» (Near Field Communication – NFC). Із зростанням обсягів мобільних платежів на перший план виходить завдання забезпечення їх безпеки, а переваги, що надаються у плані безпеки технологіями біометрії, виглядають доволі переконливими. Не менш важлива інтеграція біометрії з технологіями NFC, що ще зовсім недавно видавалося екзотикою, а зараз симбіоз цих технологій починає переживати справжній бум.

Як ще один *(третій)* напрям розвитку «мобільних» біометричних технологій експерти «Goode Intelligence» називають їхнє використання в складі систем багатофакторної ідентифікації.

І останнім, *четвертим* у списку, але не за значенням напрямом є застосування мобільних біометричних рішень у діяльності правоохоронних і силових структур, завдяки

[1] Хакерство как бизнес-модель («Die Zeit», Германия) // Четверта влада. – 2012. – 4 февраля. [Электронный ресурс]. – Режим доступа: http://4vlada.net/politika-i-biznes/

[2] Интернет-преступность: Евгений Касперский не видит защиты от кибервойны // Financial Times Deutschland. – 2012. – 10 февраля. [Электронный ресурс]. – Режим доступа: http://4vlada.net/smi/internet-prestupnost...

[3] Биометрические технологии на защите информации: новые перспективы // CRN/RE. – 2013. – 5 июня. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[4] Apple как новый лидер биометрической революции // Appleinsider.ru. – 2013. – 23 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

чому з'явилась можливість практично негайного встановлення особистості тих осіб, до яких представники цих структур проявили інтерес під час патрулювання або рейдів.

Біометричні технології роблять свій ефективний вклад у вирішення цих завдань, серед яких особливо слід зазначити проведення мобільних платежів та організацію дистанційного доступу до ІТ-систем і програм відповідного сервісу[1].

Акцентуємо, що справжню інформаційну безпеку на державному рівні від витоку будь-яких таємних і конфіденційних даних може гарантувати тільки використання апаратно-програмних рішень і комплектуючих, які були розроблені та вироблені під спеціальним контролем безпосередньо в країні, де вони будуть використовуватись. На користь такого рішення говорить акцентування аналітиків науково-технічного комітету Пентагона на такому факті, що у програмному забезпеченні, яке розроблене в інших країнах, можуть бути спеціальні закладки, передбачена можливість несанкціонованого доступу та інших прихованих шкідливих функцій.

Оскільки основні сучасні операційні системи (ОС) розроблені в США, тому в багатьох країнах, особливо в Китаї та Росії, поставлено питання щодо розробки свого так званого вільного програмного забезпечення (ВПЗ). Вихідний код закордонного програмного забезпечення (ПЗ) не відкритий – то це означає, що програмісти держав-нерозробників ОС не зможуть ефективно підтримувати роботу закордонного програмного забезпечення у випадках виникнення військових дій або інших так званих форс-мажорних міжнародних обставин. Як підсумок, можливий параліч роботи важливих державних структур.

У кожній країні існують свої відмінності у розроблюваних ВПЗ, але більшість із таких операційних систем і програм сформовані на базі ядра Linux. Затрати на розробку ОС вільного програмного забезпечення доволі значні. Китай щорічно виділяє на розробку свого ВПЗ під назвою Red Flag Linux 154 млн доларів, Євросоюз – 65 млн євро, Росія у 2013 році виділила 490 млн рублів.

Крім ОС, на базі Linux стали популярними й окремі вільні програми. Наприклад, серед Інтернет-браузерів однією з найпопулярніших є програма Mozilla Firefox. Вона також належить до класу ВПЗ, тому що в неї відкритий вихідний код і її можна вільно доопрацьовувати під свої потреби.

А в мобільних пристроях є популярний інший вид вільного програмного забезпечення – операційна система Android[2].

Окрім свого вільного програмного забезпечення, для належної інформаційної безпеки на державному рівні необхідно мати і мікросхеми свого виробництва для внесення в електронному вигляді біометричних даних. Лінії виробництва мікрочіпів за технологією 90 нм, які використовуються у паспортно-візових документах нового покоління та інших персональних документах, різних банківських і соціальних картах, SIM-картах і технологій NFC, за даними російської компанії «Ситроникс» (назва російською – авт.) існують у 8 країнах світу. Це Китай, Німеччина, Південна Корея, Росія, США, Тайвань, Франція та Японія[3].

---

[1] Рынок биометрических решений для мобильных устройств будет активно развиваться // BIOMETRICS.RU. – 2011. – 4 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Грамматчиков Алексей. Быть ли «русской Windows»? / Алексей Грамматчиков // From-ua.com. – 2013. – 12 марта. [Электронный ресурс]. – Режим доступа: http://www.from-ua.com/technology/...

[3] Микросхемы для биометричных паспортов будут выпускать в Зеленограде // РИА Новости. – 2012. – 20 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Що ж стосується нашої держави, то українські ІТ-фахівці не вірять у те, що держвідомства країни можна перевести з Microsoft на українське ПЗ з відкритим кодом. На їхню думку, в держави не вистачить на це коштів, а в місцевого ІТ-співтовариства – бажання, а також можливостей. Для запровадження ВПЗ в Україні потрібно, щоб функціонувала розвинута система сервісних компаній, які були б орієнтовані на внутрішню економіку. Експерти вважають, що навіть у випадку створення національного відкритого програмного забезпечення, а ймовірність такого факту дуже низька, то його підтримка не зацікавить українських айтішників. Хто з них захоче вивчати або підтримувати систему, яку більше ніде у світі не будуть використовувати?[1]

За даними Інтерфаксу, в 2013 році в Росії успішно завершена сертифікація операційної системи спеціального призначення (ОССП) Astra Linux Special Edition. Сьогодні ця ОССП – єдина в Росії операційна система, яка сертифікована у всіх трьох державних сертифікаційних установах засобів захисту інформації (ФСБ, Міноборони й ФСТЕК). Вона використовується для обробки інформації обмеженого доступу.

Система Astra Linux Special Edition дозволяє створювати захищені високопродуктивні масштабовані рішення – від невеликих автономних програмно-комп'ютерних комплексів до найскладніших територіально-розподілених автоматизованих систем. Вона виявилася зручною для запровадження у Збройні сили Росії різних військових автоматизованих систем управління.

Ключовою особливістю російської операційної системи є наявність вбудованих засобів захисту інформації, інтегрованих з її основними компонентами. Роботи зі створення й інтеграції засобів захисту інформації проводились і проводяться за наукового супроводу Інституту криптографії, зв'язку й інформатики академії ФСБ Російської Федерації[2].

Підсумовуючи викладене у цьому розділі, слід зазначити, що біометричні технології на високому рівні забезпечують корпоративну безпеку, практично виключивши потребу в численних ідентифікаторах, які з успіхом замінюються на унікальні для кожної людини біометричні характеристики.

Останні досягнення біометрики у все зростаючому обсязі використовуються для забезпечення національної безпеки, створення надійних систем захисту конфіденційної інформації, організації управління доступом співробітників до різного ІТ-устаткування, інформаційно-комунікаційних систем і мереж.

Інсайдерські загрози та питання мінімізації цих ризиків – традиційно актуальні для керівника служби безпеки будь-якої установи, оскільки несанкціонований доступ до конфіденційних ресурсів може призвести до колосальних втрат. Одним із найефективніших рішень цієї проблеми є впровадження в установах будь-яких форм власності систем біометричної ідентифікації співробітників.

Нині біометричні технології широко запроваджуються в різні устаткування, мобільні пристрої та Інтернет-світ. Для підвищення захистних можливостей та поліпшення контролю за доступом проводяться заходи з інтеграції біометрії з іншими інформаційними технологіями, зокрема з такою, як інфраструктура відкритих ключів цифровому підпису (каталог таких ключів ІКАО продовжує активно формувати). Що стосується

[1] Власенко Виктория. Украинским властям не видать собственного Windows / Виктория Власенко // Proit.com.ua. – 2012. – 31 января. [Электронный ресурс]. – Режим доступа: http://proit.com.ua/article/telecom/...

[2] Владыкин Олег. Секретные сети надежно защищены / Олег Владыкин // Независимое военное обозрение. – 2013. – 20 сентября. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/nvoevents/...

впровадження досягнень біометрики в цифровий підпис, то у березні 2013 року компанія «Hitachi» оголосила про створення першої повністю працездатної системи для роботи з цифровими підписами на базі біометричної інформації. Для створення підпису як біометричного ідентифікатора використовується малюнок вен на пальці користувача.

Для забезпечення належного захисту різних інформаційних систем, електронного уряду й електронної комерції важливо будь-якими засобами запобігти можливості «обману» системи, коли зловмисник може видати себе за іншу людину, для чого змінює або підробляє документи. З метою протидії можливим «обманам» контролюючих систем застосовується технологія відкритих ключів Public Key Infrastructure (PKI), яка використовує електронний цифровий підпис. Нова технологія дозволяє застосовувати біометричну інформацію як базу для цифрового підпису в системах із вимогами будь-якої перестроги.

Офіційно ця технологія була представлена на 30-му симпозіумі з криптографії та захисту інформації SCIS 2013, який відбувся у японському місті Кіото 25-го січня 2013 року[1].

Але, за висновками експертів, найліпший захист таємної або конфіденційної інформації може гарантувати тільки симбіоз біометричних технологій із криптографічним шифруванням. Інтеграція біометричних і криптографічних технологій створює нові перспективи строгої ідентифікації, забезпечення інформаційної безпеки та захисту персональних даних. Тобто вже можна говорити про появу нового способу забезпечення інформаційної безпеки – технології біометрично-криптографічного шифрування.

[1] Разработана технология биометрической цифровой подписи // СОФТ@Mail.Ru. – 2013. – 15 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розділ 15

ПРАВОВІ ПРОБЛЕМИ, ЯКІ ВИНИКАЮТЬ ПІД ЧАС ЗАСТОСУВАННЯ БІОМЕТРІЇ

Перед тим, як перейти до суті проблеми, розглянемо поняття терміна «Privacy». Англійське слово «Privacy» не можна перекласти на українську мову таким же однозначно чітким і лаконічним терміном. «Privacy» нашою мовою – це доволі широке поняття, яке поєднує значення таких термінів-висловів, як «приватна сфера», приватність, нерозголошення особистої інформації. Це право на невторгнення в особисте життя. В юриспруденцію цей термін ввели, як вважають, американські юристи С. Уоррен і Л. Брендіс, які ще в 1890 році опублікували статтю «Право на Privacy».

Майже всі держави світу декларують право громадян на захист приватної інформації. Але держава – складна динамічна система, яка не в змозі існувати неволодіючи і невикористовуючи інформацію. Відомий англійський соціолог Е. Гідденс ще в середині 80-х років минулого століття висловив думку, яка стала найбільш актуальною в XXI сторіччі: в своїй основі всі держави – інформаційні суспільства, оскільки державна влада допускає рефлексивний збір, зберігання й управління інформацією, яка необхідна для адміністрування. Тобто інформація необхідна для вирішення внутрішньодержавних завдань та управління суспільством. Наслідком тривалого еволюційного розвитку держав стало створення специфічних інформаційних систем для потреб державного управління[1].

Нині відомості щодо громадян зберігаються у багатьох державних базах даних (БД), відомості з яких використовуваються у повсякденному житті, наприклад: паспортна система, податкові дані, загальнодержавний реєстр виборців, списки органів освіти, соціального та медичного забезпечення, дані бюро технічної інвентаризації, військоматів, акти органів цивільного стану. Крім того, для забезпечення правоохоронної діяльності та безпеки держави функціонують різноманітні БД правоохоронних і спеціальних структур.

За об'єднання інформацій із різних баз даних отримується інформаційний портрет людини – так зване досьє. У новому тисячолітті з'явилась можливість втілення у життя тотального нагляду за людиною, тобто здійснити на практиці реалізацію систем, які в змозі контролювати життя людей від народження до смерті, причому об'єкти спостереження можуть навіть не підозрювати про це.

Після подій 11 вересня 2001 року можливості технологій спостереження за індивідуумами зробили величезний крок у своєму розвитку. Однією з глобальних суперпрограм спостереження є Програма «Prism», що використовується в інтересах Агенства національної безпеки (АНБ) і ФБР США. Дії суперпрограми «Prism» ґрунтуються на Законі про контроль над діяльністю іноземних розвідок (FISA) й Акті про захист Америки

[1] Акопян Диана. Эпоха тотальной электронной слежки / Диана Акопян, Анатолий Еляков // Скепсис. [Электронный ресурс]. – Режим доступа: http://scepsis.net/library/...

/Protect America Act (PAA)/, які дозволяють здійснювати стеження за громадянами іноземних держав за межами США без санкції суду[1].

Необхідно зазначити, що існуючі інформаційно-розвідувальні системи стали універсальними: вони не тільки в автоматичному режимі збирають інформацію, але і проводять її попередній аналіз. Саме так працюють системи глобального стеження типу «Ешелон» (експлуатується англомовними країнами: США, Великобританія, Австралія, Канада і Нова Зеландія) і СОРМ-2 (система оперативно-розшукових заходів), яка функціонує в низці країн на теренах колишнього СРСР.

З 2011 року в ЗМІ з'являється інформація про фактичний початок ведення «воєнних дій» у кібернетичному просторі (кібервійни) та про можливість виявів тероризму в ньому (кібертероризм). У публікаціях зазначається посилення тенденції вирішення низкою країн сучасних військових завдань не стільки шляхом прямої силової дії, а завдяки технологічно-інформаційним перевагам. За оцінками фахівців у галузі військових технологій, більш зростаючу небезпеку становить інтенсивна розробка засобів так званої «інформаційної зброї», на створення якої потрібні не дуже великі фінансові кошти, але які можуть ефективно використовуватися і у мирний, і у військовий час. Разом із можливістю безпосереднього впливу на засоби телекомунікацій, системи управління військами та фінансово-економічні структури, одним із головних об'єктів ураження інформаційною зброєю є світогляд громадян держави, проти якої ведеться «інформаційна» війна[2].

Наведена інформація свідчить про те, що практично людству загрожує масштабне вторгнення у приватне життя будь-якої особи і, якщо не ліквідація, то значне звуження простору всіх понять, що вкладають у термін «Privacy».

Останнім часом у засобах масової інформації регулярно публікуються повідомлення про факти витоків персональних відомостей у різних країнах світу. Так, ще у 2007 році в Британії був зареєстрований один із найгучніших у світовій історії скандал щодо витоку персональної інформації стосовно 25 млн чоловік (10 млн дорослих і 15 млн дітей). За заявою британського МВС (Home Office), витік інформації з королівського казначейства жодним чином не пов'язаний із формуванням національної системи біометричних ідентифікаційних карт. За заявою прес-секретаря МВС, безпеку бази біометричних даних забезпечуватимуть за допомогою спеціальних організаційних і технічних заходів: функціонування бази даних перебуватиме під постійним контролем та аудитом, усі спроби несанкціонованого доступу або використання персональної інформації тут же виявлятимуться та присікатимуться.

Відповідно до акту «Про захист даних» (DPA), ухваленого ще в 1998 році, у Великобританії зібрані біометричні дані мають статус конфіденційної інформації. Неавторизований персонал не має доступу до біометричних даних, тому вважається, що дані не можуть бути використані не за прямим призначенням[3].

Нині нагальною проблемою є використання біометричних баз даних. Доречно навести суть зробленої ще у 2007 році заяви федерального комісара ФРН Петера Шаара, який опікувався проблемами захисту даних і наглядав за порядком зберігання

[1] Prism – глобальная машина наблюдения: как США уничтожают свободу в мире // «The Guardian», «The Washington Post». – 2013. – 6 и 7 июня. [Электронный ресурс]. – Режим доступа: http://regnum.ru/news/...

[2] Ведущие страны разрабатывают информационное оружие // Novopol.ru. – 2008. – 8 февраля. [Электронный ресурс]. – Режим доступа: http://www.crimeresearch.ru/articles/cyberwar/...

[3] Британия. МВД заявляет, что база биометрических данных владельцев идентификационных карт надежно защищена // BIOMETRICS.RU. – 2007. – 22 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

накопичуваної в банках даних інформації про громадян і недопущення незаконних дій із цими відомостями. У своїй заяві федеральний комісар попередив, що в майбутньому, коли дистанційне розпізнання особистості стане зрілою технологією, у жодному випадку не можна допустити, щоб запровадження цієї технології призвело до появи режиму тотального стеження в суспільстві. Комісар висловився за необхідність створення таких юридичних бар'єрів, які за відсутності відповідних судових дозволів перешкоджали об'єднанню відеозаписів, які здійснюються камерами спостереження в суспільно-громадських місцях, з інформацією баз даних, в яких зберігаються фотозображення власників документів, які засвідчують особистість громадян.

Вимога федерального комісара ФРН із захисту даних особливо нині актульна, коли спецслужби США фактично встановили тотальний автоматизований контроль за всіма комунікаційними зв'язками і, як наслідок, переміщеннями громадян. Компетентні органи також фактично реалізували можливість здійснення прихованої дистанційної ідентифікації людини без її відома.

Свого часу знаний експерт із технологій інформаційної безпеки Брюс Шнайєр заявив: «З деякого часу я почав говорити, що всі дебати про впровадження національних електронно-паспортних документів скоро стануть недоречні. В майбутньому вам не доведеться показувати свої документи. Вони і так знатимуть, хто ви є»[1].

Заходи щодо запровадження паспортно-візових документів нового покоління та збереження персональних, зокрема і біометричних даних, мають декілька аспектів: цивільно-гуманітарний, суспільно-політичний і технологічний. Цілком зрозуміло, що в сучасному все більш глобалізованому світі введення ідентифікаційних документів нового покоління створює більш сприятливі умови для переміщення людей, тобто зростання кількості людей, що приїзджають з одних країн до інших. Причому важливою особливістю цієї тенденції є те, що застосування біометричних ідентифікаційних технологій дозволяє контролювати міграційні потоки і, як наслідок, більш ефективно протидіяти нелегальній імміграції, наркотрафіку, різним виявам міжнародного тероризму та транскордонної злочинності.

Водночас не можна цілком ігнорувати той факт, що частина членів громадянського суспільства висловлює протест проти внесення в ідентифікаційні документи їх особистих біометричних та інших персональних даних. У цих умовах дуже потрібна послідовна та переконлива роз'яснювальна робота, яка спрямована на формування позитивної громадської думки з цієї проблеми і яка повинна бути підкріплена відповідними законодавчими актами.

Вихід тільки один – необхідно встановити такі правові норми, які б забезпечили надійний захист і безпеку зберігання персональної інформації і не завдали б шкоди основним правам і свободам громадян[2].

У світі протестів частини громадянського суспільства проти внесення в ідентифікаційні документи їх особистих біометричних та інших персональних даних корисною є інформація про те, що Суд Європейського Союзу в Брюсселі визнав законним внесення в біометричні паспорти відомостей про відбитки пальців.

Свого часу до Суду Євросоюзу звернувся зі скаргою громадянин Німеччини Михаель Шварц щодо відмови влади ФРН видати йому паспорт без проходження про-

[1] Берд К. Проблема дистанции / К. Берд // Компьютерра. – 2007. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

[2] Введение паспортно-визовых документов нового поколения является важным направлением в работе Федеральной миграционной службы РФ // Единая Россия (Edinros.Ru). – 2007. – 7 мая. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

цедури сканування відбитків пальців. У жовтні 2013 року Суд ЄС розглянув звернення і констатував, що вимога надати біометричні дані суперечить основним правам та свободам громадян, становить загрозу для приватного життя і збереження персональних даних, однак досягнення мети підвищення рівня безпеки виправдовує подібні заходи. Паспорта нового типу з даними про відбитки пальців у мікрочіпі дозволяють більш ефективно боротися з нелегальними проникненнями на територію Європейського Союзу, шахрайським використанням документів та іншими фальсифікаціями, зазначив суд[1].

В Україні тільки з другої спроби набув чинності Закон «Про захист персональних даних». Як відомо, ще у січні 2007 року Верховна Рада України ухвалила Закон «Про захист персональних даних», але тодішній Президент не підписав той варіант закону. В червні 2010 року Президентом була підписана нова версія цього документа (Закон від 01.06.2010 № 2297-VI), який набув чинності з 1 січня 2011 року.

Нові положення Закону ставлять поза законом торгівлю приватними базами даних, встановлюють контроль над циркуляцією особистих відомостей громадян і вимагають від організацій забезпечення захисту персональних даних співробітників, клієнтів тощо.

Наведемо роз'яснення Міністерства юстиції України щодо визначень понять персональні дані та бази персональних даних.

Визначення поняття «персональні дані» наведено в абзаці восьмому статті 2 Закону «Про захист персональних даних», відповідно до якого персональними даними є відомості чи сукупність відомостей про фізичну особу, яка ідентифікована або може бути конкретно ідентифікована.

Але законодавством України не встановлено і не може бути встановлено чіткого переліку відомостей про фізичну особу, які належать до персональних даних. Це зроблено для можливості застосування положень Закону до різних ситуацій, що можуть виникнути у майбутньому через можливі зміни у технологічній, соціальній, економічній та інших сферах суспільного життя, зокрема і під час обробки персональних даних в інформаційних (автоматизованих) базах та картотеках персональних даних.

Поняття «база персональних даних» визначене абзацом другим статті 2 Закону, відповідно до якого база персональних даних – іменована сукупність упорядкованих персональних даних в електронній формі та/або у формі картотек персональних даних.

З огляду на це, база персональних даних є упорядкованою сукупністю логічно пов'язаних даних про фізичних осіб, які:

– зберігаються й обробляються за допомогою відповідного програмного забезпечення, що є базою персональних даних в електронній формі;

– зберігаються та обробляються на паперових носіях інформації, що є базою персональних даних у формі картотек.

Картотекою персональних даних є будь-який структурований масив персональних даних на паперових носіях, що є доступним за визначеними критеріями, незалежно від того, чи є такий масив централізованим, децентралізованим або розділеним за функціональними або географічними ознаками.

Такі дані мають бути структурованими за допомогою визначених критеріїв стосовно фізичних осіб, щоб забезпечити легкий пошук і доступ до потрібних персональних даних.

[1] Суд ЕС признал законным внесение в биометрические паспорта сведений об отпечатках пальцев // РАПСИ. – 2013. – 18 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Необхідно особливо наголосити, що з огляду на положення статті 2 Закону, персональні дані одночасно можуть бути упорядкованими і в електронній формі, і в формі картотек[1].

Для забезпечення виконання громадянами, органами державної влади та місцевого самоврядування, підприємствами, установами організаціями незалежно від форми власності вимог Закону України «Про захист персональних даних» 2 червня 2011 року Верховною Радою України було ухвалено Закон України «Про внесення змін до деяких законодавчих актів України щодо посилення відповідальності за порушення законодавства про захист персональних даних», який набрав чинності 1 січня 2012 року.

У разі порушення положень закону «Про персональні дані» винні особи несуть адміністративну, кримінальну, дисциплінарну та іншу встановлену законодавством України відповідальність. Із набуттям чинності Закону «Про захист персональних даних» про безпеку та належне зберігання персональних даних співробітників і клієнтів тепер повинна дбати абсолютно кожна організація на території України.

Але забезпечення належної безпеки персональних даних у повному обсязі дуже трудомістка і, головне, фінансовозатратна справа. А ще слід пам'ятати, що правоохоронні та спеціальні структури відшукують аргументи та підстави з метою втілення у наше життя ідеї так званого «тотального стеження».

28 січня 1981 року була підписана Конвенція про захист осіб у зв'язку з автоматизованою обробкою персональних даних. Це перший міжнародний договір, в якому були зібрані юридично зобов'язуючі норми захисту прав кожної людини щодо недоторканості приватного життя під час обробки персональних даних.

Конвенція стала основою для подальшого розвитку систем захисту персональних даних. Нині Конвенція ратифікована 46 державами світу. Законом України від 6 липня 2010 року Україна ратифікувала Конвенцію Ради Європи про захист осіб у зв'язку з автоматизованою обробкою персональних даних та Додатковий протокол до неї. Цим самим Україна взяла на себе зобов'язання забезпечити дотримання прав і свобод людини, зокрема права на недоторканність приватного життя, передбаченого статтею 8 Конвенції про захист прав людини й основоположних свобод, що також гарантується статтею 32 Конституції України.

Законодавство України у цій сфері постійно вдосконалюється. Одним із прикладів є Закон України від 03.07.2013 № 383-VII «Про внесення змін до деяких законодавчих актів України щодо удосконалення системи захисту персональних даних». Цим законодавчим актом реєстрація баз персональних даних із 1 січня 2014 року замінена процедурою повідомлення володільцями персональних даних Уповноваженого Верховної Ради України з прав людини про обробку персональних даних, які становлять особливий ризик для прав і свобод суб'єктів персональних даних.

Види обробки таких даних, категорії суб'єктів, на яких поширюється вимога щодо повідомлення, визначаються Уповноваженим та оприлюднюються на його офіційному веб-сайті (http://www.ombudsman.gov.ua) у розділі «Захист персональних даних»[2].

Загалом можно зробити висновок, що практично всі інформаційні технології, зокрема і біометричні, мають безпосереднє відношення до недоторканності при-

[1] Деякі питання практичного застосування Закону України «Про захист персональних даних» // Міністерство юстиції України. [Електронний ресурс]. – Режим доступу: http://www.minjust.gov.ua/38266.

[2] Інформація Державної служби України з питань захисту персональних даних // Державна служба України з питань захисту персональних даних. – 2014. –25 квітня. [Електронний ресурс]. – Режим доступу: http://zpd.gov.ua/dszpd/uk/index.

ватного життя та безпеки громадян, у тому числі й до таких сфер, як здоров'я, навчання тощо.

В Україні застосування і використання біометрії, крім закону «Про Єдиний державний демографічний реєстр і документах, які підтверджують громадянство України, засвідчують особистість або її спеціальний статус» (чинний із 6 грудня 2012 року), регулюється законодавством у галузі високих технологій. Загалом це законодавство можна поділити на такі види: законодавство України у сфері функціонування електронних платіжних систем; законодавство щодо інформаційної політики й інформаційної безпеки України та законодавство України у сфері зв'язку й телекомунікації[1].

До впровадження в Україні біометричних технологій мають відношення Закони і нормативні акти України, що встановлюють основні організаційно-правові принципи електронного документообігу та використання електронних документів, правовий статус електронного цифрового підпису (далі – ЕЦП) і порядок його використання юридичними і фізичними особами. У найзагальніших рисах застосування біометрії як складової інформації в Україні регулюються Законами «Про інформацію», «Про захист інформації в інформаційно-телекомунікаційних системах», «Про захист персональних даних», «Про Національну програму інформатизації», «Про концепцію Національної програми інформатизації» і інших законодавчих актів.

У багатьох документах про стан і розвиток інформатизації в Україні констатуються такі положення:

– розвиток нормативно-правової бази інформаційної сфери недостатній (насамперед це можна віднести до використання біометричних технологій – *авт*.);

– основними стратегічними заходами розвитку інформаційного суспільства в нашій державі є такі положення, як захист інформаційних прав громадян, насамперед щодо доступності інформації, захисту персональної інформації про особу, підтримка демократичних інститутів і мінімізації ризиків «інформаційної нерівності»;

– головними напрямами розвитку інформаційного суспільства в Україні визначено формування і впровадження правових, організаційних, науково-технічних, економічних, фінансових, технологічних, методичних умов розвитку інформаційного суспільства України з урахуванням світових тенденцій.

Для підвищення ефективності розвитку інформаційного суспільства в Україні необхідно створити цілісну систему законодавства, яка б була уніфікована з нормами міжнародного права з питань розвитку інформаційного суспільства, зокрема здійснення кодифікування інформаційного законодавства. Підготовка законопроектів повинна проходити з проведенням їх громадських слухань і обговорень. Із урахуванням світових тенденцій особливої уваги вимагає вдосконалення та регламентування нормативно-правової бази щодо забезпечення інформаційної безпеки, розробки стандартів обміну персональними і медичними даними за умови забезпечення недоторканності особистого життя, зокрема захисту інформаційних ресурсів, протидії комп'ютерній злочинності, захисту персональних даних, а також правоохоронній діяльності в інформаційній сфері.

Під час створення інформаційного законодавства слід керуватися загальними засадами Конституції України, а також реалізовувати принципи свободи створення, отримання та розповсюдження інформації; об'єктивності, достовірності, повноти та точності інформації; гармонізації інтересів індивідуума, суспільства і держави в інформаційній діяльності; обов'язковості опублікування інформації, яка має важливе суспільне значення; обмеження доступу до інформації виключно на основі закону; мінімізації негативного

[1] [Електронний ресурс]. – Режим доступу: http://www.crime-research.iatp.org.ua/ind.html.

інформаційного впливу і негативних наслідків функціонування інформаційно-комп'ютерних технологій (ІКТ); недопущення незаконного розповсюдження, використання і порушення цілісності інформації; гармонізації інформаційного законодавства і всієї системи вітчизняного законодавства.

Для реалізації перелічених принципів необхідно підготувати й ухвалити Інформаційний кодекс України, включивши до нього розділи, зокрема про принципи електронної торгівлі, правову охорону прав на зміст комп'ютерних програм, удосконалення захисту прав інтелектуальної власності, зокрема авторського права під час розміщення і використання творів у мережі Інтернет, про охорону баз даних, дистанційне навчання, телемедицину, порядок надання органами державної влади й органами місцевого самоврядування юридичним і фізичним особам інформаційних послуг із використанням мережі Інтернет, збереження комерційної таємниці тощо[1].

Друге десятиріччя XXI століття характеризується ухваленням у багатьох країнах світу змін до законів про захист персональних даних.

У Європі Єврокомісія ще у 2007 році підготувала пакет нових законів щодо захисту персональних даних. Розробники визначили своєю метою створення ефективної зброї для боротьби з «крадіжками особистості». Європейська комісія свого часу заявляла, що закони, які існують у сфері захисту персональних даних, вимагають змін і доповнень, оскільки вони не відповідають реаліям сучасності. І тому національні закони повинні бути зоорієнтовані на захист від «крадіжок особистості» у сфері електронних злочинів[2].

У березні 2014 року Європейський парламент проголосував за великий пакет нових законів, які мають на меті посилення захисту персональних даних мешканців Євросоюзу. Ухвалені законодавчим органом ЄС закони поки що не набрали чинності. Вони повинні отримати схвалення нового складу парламенту після травневих виборів 2014 року, а далі пройти процедуру затвердження Європейською радою.

У новій версії закону з захисту персональних даних особливо слід виокремити положення, відповідно до якого мешканці країн Євросоюзу повинні в обов'язковому порядку надавати згоду щодо обробки своїх персональних даних, за необхідності мати можливість одержання електронної копії зібраної інформації, а в разі потреби – право на знищення всіх зібраних даних (за винятком, коли інформація становить суспільний інтерес – поправка, яка має на меті захист журналістської діяльності).

За висловом комісара Європейського Союзу з юстиції, фундаментальних прав і громадянства Вів'єна Редінга (Viviane Reding): «Сильний захист даних повинен стати торговою маркою Європи. Після шпигунських скандалів щодо США захист інформації – це конкурентна перевага, яка більш важлива, ніж будь-коли»[3].

Що стосується суто біометричних технологій, то Європейським Союзом 2000 року була ухвалена «Резолюція з питань безпеки паспортних документів і інших дорожніх документів». Цим актом із 1 січня 2005 року було запроваджено в країнах ЄС введення загальнообов'язкових мінімальних стандартів безпеки у сфері виробництва паспортних і проїзних документів. Ухвалені положення були спрямовані на захист паспортів

[1] Закон України про Основні засади розвитку інформаційного суспільства в Україні на 2007–2015 роки. – № 537-V. – 2007. – 9 січня. [Електронний ресурс]. – Режим доступу: http://www.customs.gov.ua/dmsu/control/uk/publish/

[2] Европейские законы поставят инсайдеров на колени // SC Magazine Australia. – 2007. – 7 июня. [Электронный ресурс]. – Режим доступа: http://www.infowatch. ru/threats…

[3] Евросоюз принял новые законы по защите персональных данных в Интернете // Хакер. – 2014. – 13 марта. [Электронный ресурс]. – Режим доступа: http://www.xakep.ru/post/...

та інших аналогічних документів від підробок шляхом запровадження біометричної ідентифікації особистості власника документа.

Із накопиченням біометричної та іншої персональної інформації в банках даних усіх країн дедалі актуальнішими стають питання законодавчого захисту персональних відомостей, регламентації порядку їх використання і встановлення єдиних правил, що формулюють основні положення поводження з персональними даними та недопущення витоку конфіденційної інформації, а у випадку настання такої події – ліквідації наслідків витоку та настання відповідальності за свої дії для всіх суб'єктів права.

У вересні 2001 року Радою Безпеки ООН була ухвалена резолюція № 1373 щодо боротьби з міжнародним тероризмом, в якій особлива увага була приділена посиленню заходів із попередження фальсифікації офіційних документів, які засвідчують особистість, підвищенню їх надійності й уніфікації відповідно до обов'язкових для всіх членів світової спільноти єдиних вимог.

Україна ратифікувала міжнародні угоди з питань захисту паспортних документів і протидії міжнародній організованій злочинності, нелегальній міграції тощо. Йдеться про Європейську конвенцію про захист прав і основних свобод людини 1950 року, Конвенцію ООН проти транснаціональної організованої злочинності, Європейську угоду щодо правил, які регламентують пересування громадян держав – членів Ради Європи, а також про Програму реалізації положень Варшавської конференції про загальну боротьбу проти тероризму 2001 року, Нью-Орлеанську угоду 2002 року, Віденську декларацію 2003 року, Рішення ОБСЄ № 7/03 від 2 грудня 2003 року «Безпека проїзних документів» і низка інших.

Відповідно до положень цих документів та інтересів національної безпеки, економічного благополуччя і дотримання прав людини в Україні, недопущення створення умов для обмеження вільного пересування громадян нашої країни під час в'їзду-виїзду до інших держав реальна світова дійсність наполегливо вимагає імплементації в українське законодавство не тільки норм і вимог відповідних міжнародних угод, але і стандартів.

Розглянемо ще одну проблему, яка ніби прямо не стосується застосування біометрії в Україні. Біометричні технології вважаються складовою інформаційних технологій, тому українські проблеми інформатизації стосуються розвитку біометричних технологій у нашій країні. Належному стану інформатизації у нашій державі і, як наслідок, відповідному стану інформаційного законодавства не сприяють часті реформування українських центральних органів виконавчої влади, які реалізують державну політику в сфері інформатизації.

Державний комітет інформатизації України (Держкомінформатизації) діяв із 26 березня 2008 до 5 липня 2010 року. Правонаступником комітету стало Державне агентство з питань науки, інновацій та інформатизації (Держінформнауки) України, що було утворено на базі Держкомінформатизації та Державного комітету з питань науково-технічного та інноваційного розвитку.

Держінформнауки України відповідальний за реалізацію державної політики у сфері наукової, науково-технічної та інноваційної діяльності, інформатизації, формування і використання національних електронних інформаційних ресурсів, створення умов для розвитку інформаційного суспільства.

Але нині провідні науковці нашої країни вважають, що формуванням і реалізацією державної політики у сфері науки, інновацій та інформатизації повинен займатися центральний орган виконавчої влади зі спеціальним статусом, який би підпорядковувався безпосередньо Кабінету Міністрів. Цей орган доцільно утворити на базі Державного агентства з питань науки, інновацій та інформатизації.

Таку позицію у листі на адресу Прем'єр-міністра України Арсенія Яценюка висловили Президент Національної академії наук України Борис Патон, в.о. Президента Національної академії аграрних наук Ярослав Гадзало, Президент Національної академії медичних наук Андрій Сердюк, Президент Національної академії педагогічних наук Василь Кремень, Президент Національної академії правових наук Василь Тацій, Президент Національної академії мистецтв Андрій Чебикін.

Також, на переконання наукового співтовариства, необхідною умовою успішної реорганізації системи державного управління у сфері науки є утворення Національної ради з питань науки і технологій під головуванням Прем'єр-міністра України. Подібний досвід існує у багатьох європейських країнах. Учені вважають, що зазначені інституційні зміни дозволять наблизити систему державного управління у сфері науки до найліпших світових стандартів та підвищити ефективність вітчизняної науки у забезпеченні економічного розвитку України[1].

Але, на жаль, загалом поки що загальний стан інформаційно-комп'ютерних технологій (ІКТ) в Україні тільки погіршується. Так, згідно з опублікованим Всесвітнім економічним форумом (ВЕФ) індексом мережевої готовності-2014, Україна посіла 81 місце, втративши 8 позицій (в 2013 Україна була на 73 позиції).

Подібна динаміка викликає занепокоєння, адже цілком зрозуміло, що позиція в рейтингу – це індикатор ефективності державного регулювання в цій сфері. Неефективне використання наявного потенціалу і неналежна увага до інформаційно-комп'ютерних технологій (ІКТ) – причина того, що Азербайджан, Вірменія, Грузія, Казахстан і Росія випередили Україну за рівнем та динамікою розвитку ІКТ насамперед завдяки зацікавленості урядів країн цією сферою.

Серед країн СНД лідирує Азербайджан, який піднявся у 2014 році на 49-е місце з 56-го. Росія посіла 50-е місце (у 2013 році – 54-е). Очолюють рейтинг-2014, як і торік, Фінляндія, Сінгапур і Швеція. На четвертому місці опинилися Нідерланди, далі – Норвегія.

Нагадаємо, що Всесвітній економічний форум (ВЕФ) – швейцарська неурядова організація, що відома організацією щорічних зустрічей у Давосі. Форум був створений 1971 року. Членами ВЕФ є майже 1000 великих компаній і організацій із різних країн світу.

Індекс мережевої готовності (Networked Readiness Index) вимірює рівень розвитку інформаційно-комп'ютерних технологій за 53 параметрами, об'єднаними в три основні групи: наявність умов для розвитку ІКТ, готовність громадян, ділових кіл і державних органів до використання ІКТ, рівень використання ІКТ у громадському, комерційному і державному секторах[2].

Про значне погіршення ситуації в Україні також свідчать дані аналітичного дослідження, проведеного компанією «IDC» (International Data Corporation, США) спільно з компанією «De Novo». За відомостями фахівців цих компаній у 2013 році ринок інформаційних технологій (ІТ) в Україні зменшився на 8% – до 2,9 млрд доларів порівняно з 3,2 млрд доларів у 2012 році. Крім того, основною причиною падіння є зменшення ринків ІТ-обладнання на 11,3% – до 2,3 млрд доларів.

[1] Президенти Національних академій наук звернулися до Прем'єр-міністра // Сайт Державного агентства з питань науки, інновацій та інформатизації. – 2014. – 30 квітня. [Електронний ресурс]. – Режим доступу: http://dknii.gov.ua/?q=node/1944.

[2] Україна посіла 81-ше місце в світі за рівнем розвитку інформаційно-комунікаційних технологій // УНІАН. – 2014. – 29 квітня. [Електронний ресурс]. – Режим доступу: http://www.unian.ua/science/...html.

А, за прогнозом аналітиків, український ринок інформаційних технологій у 2014 році порівняно з минулим зменшився ще на 25% – до 2,2 млрд доларів.

«IDC» (International Data Corporation, США) – аналітична та консалтингова компанія. Понад 1000 аналітиків «IDC» в 110 країнах вивчають технології, тенденції і можливості галузі на світовому, регіональному та місцевому рівнях. Компанія має представництво в Україні. Компанія «De Novo» спеціалізується на наданні професійних IT-послуг, послуг комерційного дата-центру і хмарних сервісів, володіє власним центром обробки даних[1].

У розвинутих світових країнах відповідні правові норми, що регламентують використання біометричних ідентифікаційних даних, прописані в галузях права, які охороняють приватні права людини, забезпечують конфіденційність персональної інформації і, як наслідок, практичну реалізацію законодавчих актів оперативно-розшукової діяльності. Для стандартизації й уніфікації нормативних актів, що регулюють використання біометричних технологій у світі, розроблені та ухвалені відповідні міжнародні нормативні документи.

Усередині кожної країни та регіону світу існують різні юридичні проблеми та неоднозначне їх сприйняття, які можуть впливати на використання біометрії. Тому необхідно виробити уніфікований підхід до всіх цих проблем і за можливості сформулювати рекомендації, які потрібно стандартизувати у міжнародному масштабі. Загальноміжнародні стандарти в цій сфері будуть особливо важливі під час розгортання великомасштабних міжнародних систем[2].

Для уніфікації та сумісності технологічних і технічних рішень у галузі біометрії, організації обміну відповідною інформацією між правоохоронними органами різних держав, координації міжнародних зусиль, скерованих на боротьбу з тероризмом, нелегальною міграцією й організованою злочинністю, яка все більш стає транснаціональною, відповідними міжнародними організаціями розроблені та ухвалені загальнообов'язкові технологічні стандарти, які будуть розглянуті у наступному розділі.

[1] Український ринок IT у 2014 році скоротиться на 25% // УНІАН. – 2014. – 16 квітня. [Електронний ресурс]. – Режим доступу: http://www.unian.ua/science/...html.

[2] Расс Райан. Введение стандарта на биометрию / Райан Расс // Security Technology & Design. – 2006. – 14 июля. [Электронный ресурс]. – Режим доступа: http://www.secnews.ru/articles/...

Розділ 16

НЕОБХІДНІСТЬ УНІФІКАЦІЇ СТАНДАРТІВ У СФЕРІ БІОМЕТРИЧНИХ ТЕХНОЛОГІЙ

Біометрія вирішує найрізноманітніші завдання. За цих умов особливо важливою стає наявність всеосяжної системи біометричних стандартів, від прийняття і реалізації яких здебільшого залежить масштабність систем біометричної ідентифікації, спроможність до інформаційної взаємодії, забезпечення їх сумісності та надійності.

Цілком слушно виникає питання – що охоплює поняття стандарт?

Стандарт – це документ, що встановлює вимоги, специфікації, керівні принципи або характеристики, відповідно до яких можуть використовуватися матеріали, продукти, процеси та послуги, котрі придатні для цих цілей. *Стандарти – це документовані угоди, що містять технічні умови або інші точні критерії, які зазвичай використовуються як правила, принципи або визначення характеристик для гарантії того, що матеріали, продукти (вироби), процеси та послуги відповідають своєму призначенню.*

Міжнародна організація з стандартизації International Organization for Standardization (ISO /ICO/) є розробником і видавцем міжнародних стандартів. ISO /ICO/ розробила й опублікувала понад 19500 міжнародних стандартів, що стосуються майже всіх аспектів повсякденного життя.

Із наведеної англійською мовою назви бачимо, що є невідповідність між повною офіційною назвою «International Organization for Standardization» і скороченим ISO. Якщо бути абсолютно точним, то абревіатурою організації повинно бути IOS, а не ISO. Але ISO – це не абревіатура. Насправді, слово ISO (ICO) утворено від грецького слова «isos», що означає «однаковий», слугує приставкою «iso» і трапляється в сукупності термінів таких, як «ізометрія» (однаковий вимір або однакові розміри) і «ізономія» (однаковість закону або рівність людей перед законом).

Назва «ISO (ICO)» вживається в усьому світі для позначення Міжнародної організації з стандартизації, щоб уникнути численних варіацій абревіатури, які утворюються від перекладу «International Organization for Standardization» на різні мови членів організації, наприклад: IOS англійською, OIN французькою (від Organisation internationale de normalisation).

Отже, ISO – скорочена форма позначення міжнародної організації в будь-якій країні[1]. У ЗМІ трапляється також назва «International standards organization», яка повністю відповідає абревіатурі ISO.

Міжнародні стандарти ІСО гарантують, що продукти і послуги є безпечними, надійними та якісними. Використання стандартів ІСО надає країнам, що їх застосовують, технологічні, економічні та соціальні переваги. Вони допомагають гармонізувати

[1] Международная Организация по стандартизации (ИСО) // Интерстандарт. [Электронный ресурс]. – Режим доступа: http://www.interstandart.ru/about_iso.htm.

технічні характеристики товарів і послуг, роблять галузь більш ефективною і сприяють усуненню бар'єрів у міжнародній торгівлі. Відповідність міжнародним стандартам допомагає переконати споживачів, що продукти є надійними, ефективними та безпечними для навколишнього середовища. Стандарти ІСО дозволяють оптимізувати операції і поліпшити кінцевий результат.

Стандарти ІСО відображають міжнародний досвід і знання, тому є життєво важливим ресурсом для національних урядових установ світової спільноти під час розробки національних нормативних документів.

Інтегруючи міжнародні стандарти в національні регламенти, урядові установи держав можуть скористатися знаннями і досвідом іноземних фахівців, не звертаючись до них безпосередньо[1].

За оцінками фахівців, в Україні для забезпечення повноцінного електронного урядування, засобів єдиного порталу адміністративних послуг, звітності й так далі, необхідно впровадити понад 3 тис. стандартів. У країні досі не прийнятий весь спектр таких важливих і дуже необхідних стандартів, що визначають та узгоджують формати даних електронних документів, даних в електронних інформаційних ресурсах та електронного цифрового підпису.

У нашій державі кількість стандартів із інформаційних технологій (ІТ) становить приблизно 2% від загальної кількості державних стандартів, тоді як в інших країнах ця частка перевищує 10% (для порівняння – станом на 1998 рік кількість українських стандартів із ІТ становила приблизно 4% від загальної кількості державних стандартів).

Загальна ситуація в Україні відносно створення стандартів у галузі ІТ-сфери залишається незадовільною, масштаб відставання від темпів міжнародної стандартизації зберігається: з кожної десятки ISO/IEC-стандартів діє в кращому випадку два національних українських або СНД (які нині є безнадійно застарілими) стандарти.

Водночас темпи міжнародної стандартизації інформаційних технологій кожен рік підвищуються, тобто розрив у цій галузі між Україною і провідними країнами світу тільки збільшується.

В українській державі дуже гострою є проблема гармонізації стандартів ІТ-сфери з метою виконання таких директив ЄС:

– 95/46/ЄС «Про захист фізичних осіб при обробці персональних даних і про вільне переміщення таких даних»;

– 1999/93/ЄС від 13 грудня 1999 року Європейського парламенту та Ради Європейського Союзу «Про політику ЄС щодо електронних підписів»;

– 2000/31/ЄС від 8 червня 2000 року Європейського парламенту та Ради ЄС «Про деякі правові аспекти інформаційних послуг, зокрема, електронної комерції, на внутрішньому ринку»;

– 2252/2004 «Про стандарти щодо особливостей безпеки та біометрії в паспортах і проїзних документах, виданих державами-членами».

Зважаючи на наведене, для вирішення проблем стандартизації української сфери ІТ потрібно насамперед проведення таких заходів:

– створення єдиної системи стандартизації інформаційних технологій та проведення єдиної послідовної технічної політики;

– необхідність комплексного перегляду, внесення змін або відміни застарілих стандартів ІТ за невідповідності ISO/IEC-аналогам;

---

[1] Стандарты // ISO. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/ru/home/standards/...

– аналіз стандартів інформаційних технологій щодо визначення головних та найбільш перспективних напрямів стандартизації ІТ-сфери для здійснення імплементації міжнародних стандартів у наших реаліях[1].

У XXI столітті одним із напрямів тотальної інформатизації суспільства є використання нових технологій біометричної ідентифікації й аутентифікації особистості людини. Водночас зростає значення уніфікованих біометричних стандартів для забезпечення належної надійності біометричної ідентифікації або аутентифікації, спроможності до інформаційної взаємодії біометричних систем різних країн із метою забезпечення їх сумісності та надійності. Біометричні технології активно розвиваються у всіх країнах, де є відповідний науково-технічний потенціал. Однією з рушійних причин активізації нових розробок біометрики є запровадження у більшості країн світової спільноти відповідних технологій паспортно-візових документів нового покоління і систем автоматичного їх контролю, що орієнтовані на заміну органолептичної ідентифікації людини за її фотографією і зразком підпису в звичайному паспорті на автоматизовану біометричну аутентифікацію або ідентифікацію.

Через те, що паспортно-візові документи нового покоління повинні видаватися в одних країнах, а перевірятися в інших, основні технологічні моменти біометричної аутентифікації або ідентифікації повинні бути стандартизовані системою національних стандартів, які імплементують основні базові положення відповідних міжнародних стандартів. Однією з найістотніших проблем під час підготовки національних проектів стандартів із біометрії є проблема термінології, гармонізації визначень і термінів, які належать до абсолютно різних і раніше не пов'язаних між собою галузей знань. За своєю суттю створюється цілком нова термінологія[2]. Крім того, сама біометрія як наука є достатньо новим технічним напрямом із не чіткою системою англомовних, російськомовних і україномовних термінів, що істотно ускладнює завдання проведення стандартизації у цій галузі людської діяльності.

Розробка і введення в дію стандартів для всіх рівнів життєвого циклу біометрії: від формування шаблону біометричної характеристики до правил використання біометричних систем у певній сфері людської діяльності – вимагає особливої уваги. Активна робота над створенням та вдосконаленням системи міжнародних біометричних стандартів у XXI столітті проводиться постійно. Для підвищення продуктивності праці в червні 2002 року був створений спеціальний орган, який спеціалізується на розробці й ухваленні міжнародних біометричних стандартів – підкомітет SC37 (Subcommittee 37) об'єднаного технічного комітету з інформаційних технологій JTC 1 Міжнародної організації стандартизації ISO (International Organization for Standardization) і Міжнародної електротехнічної комісії (International Electrotechnical Commission /IEC/). У ЗМІ використовуються абревіатури: англійською мовою ISO/IEC JTC1/SC37 «Biometrics», російською – ИСО/МЭК СТК1/ПК37 «Биометрия», а українською – ІСО/МЕК СТК1/ПК37 «Біометрія»[3].

---

[1] Доповідь про стан інформатизації та розвиток інформаційного суспільства в Україні за 2013 рік (розділ 2.11. Стандартизація ІТ-сфери). [Електронний ресурс]. – Режим доступу: http://www.google.com.ua/url...

[2] Иванов А. Проблемы терминологии национального стандарта по требованиям к средствам высоконадежной биометрической аутентификации / А. Иванов, В. Фунтиков, О. Ефимов, В. Герасименко, Ю. Язов // Inside-zi.ru. – 2005. – № 6. – ноябрь–декабрь. [Электронный ресурс]. – Режим доступа: http://www.inside-zi.ru/pages/6_2005/59.html.

[3] Орган по международной стандартизации в области биометрии ИСО/МЭК СТК1/ПК37 «Биометрия». Состояние работ в настоящий момент // Ассоциация автоматической идентификации «UNISXCAN». – 2007. – 19 июля. [Электронный ресурс]. – Режим доступа: http://www.ean.ru/art1/art693.html.

В роботі підкомітету ISO/IEC JTC1/SC37 беруть участь 29 країн, серед яких є й Україна. Ще 12 країн беруть участь у роботі підкомітету як спостерігачі. У підкомітеті «Біометрія» сформовано 6 робочих груп і нині кількість опублікованих стандартів під безпосередньою відповідальністю ISO/IEC JTC 1/SC 37 (number includes updates) становить 94[1].

У роботі міжнародного підкомітету SC37 «Biometrics» об'єднаного технічного комітету з інформаційних технологій брали участь і двоє українських фахівців.

Логотип ISO/IEC і номер стандарту, що наносяться на вироби, вказують на конкретний нормативний документ, за правилами і рекомендаціями якого були виготовлені вироби або за якою термінологічною базою і роз'ясненнями сформована необхідна документація (насамперед це стосується специфічних технологічних галузей (наприклад «біометрія») і ведення бізнесу в них).

У постанові українського уряду від 13 березня 2013 № 185 згадано використання в електронних документах двох форматів біометричних даних – зображення обличчя і відбитків пальців. Це відповідає вимогами ICAO (Doc 9303) і стандартам ISO / IEC 19794-5:2005 та ISO / IEC 19794-4:2005[2].

Наведемо назви і стадії вже розроблених і введених в дію міжнародних біометричних стандартів /з вказанням поправок і доповнень до них/ (див. табл. 7).

Міжнародний каталог стандартів (МКС)

(ISO / IEC JTC 1/SC 37 – Біометрія. Опубліковані стандарти.)

Скопійовано із сайту інтернет-порталу ISO. [Електронний ресурс]. – Режим доступу: http://www.iso.org/iso/ru/home/store/catalogue_tc/catalogue_tc_browse.commid...)

Таблиця 8

Стандарт і / або проект	Стадія	МКС
ISO / IEC 2382-37:2012 Інформаційні технології. Словник. Частина 37. Біометрія	90.92 – Міжнародний стандарт підлягає перегляду	35.020: Інформаційні технології (IT) загалом *Including general aspects of IT equipment.*
ISO / IEC 19784-1:2006 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 1. Специфікації біометричного прикладного програмного інтерфейсу	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19784-1:2006 / Amd 1:2007 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 1. Специфікації біометричного прикладного програмного інтерфейсу. Зміна 1. Специфікація BioGUI	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

[1] Интернет-портал ISO. – 2014. [Электронный ресурс]. – Режим доступа: http://www.iso.org/iso/ru/standards...

[2] Повесьма Дмитрий: Ученые Украины формируют международные стандарты ISO по биометрии / Дмитрий Повесьма // Наш Продукт. – 2013. – 22 апреля. [Электронный ресурс]. – Режим доступа: http://www.edaps.com/news/n2171.

Продовження таблиці 8

Стандарт і / або проект	Стадія	МКС
ISO / IEC 19784-1:2006 / Amd 2:2009 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 1. Специфікації біометричного прикладного програмного інтерфейсу. Зміна 2. BioAPI без оболонки	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc*
ISO / IEC 19784-1:2006 / Amd 3:2010 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 1. Специфікації біометричного прикладного програмного інтерфейсу. Зміна 3. Підтримка взаємообміну сертифікатами та твердженнями безпеки та іншими аспектами безпеки	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19784-2:2007 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 2. Біометричний архівний, функціональний інтерфейс провайдера	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc*
ISO / IEC 19784-2:2007 / Cor 1:2011 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 2. Біометричний архівний, функціональний інтерфейс провайдера. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19784-2:2007 / Cor 2:2013 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 2. Біометричний архівний, функціональний інтерфейс провайдера. Технічна поправка 2	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19784-4:2011 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 4. Сенсорний інтерфейс для провайдера біометричних послуг	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19784-4:2011 / Cor 1:2013 Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 4. Сенсорний інтерфейс для провайдера біометричних послуг. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 19785-1:2006 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 1. Специфікація елемента даних	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19785-1:2006 / Amd 1:2010 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 1. Специфікація елементів даних. Зміна 1. Підтримка для додаткових елементів даних	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19785-2:2006 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 2. Процедури для операції авторитетного органу реєстрації біометричної інформації	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19785-2:2006 / Amd 1:2010 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 2. Процедури для операції авторитетного органу реєстрації біометричної інформації. Зміна 1. Додаткові реєстрації	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19785-3:2007 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 3. Специфікації формату керівника	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19785-3:2007 / Amd 1:2010 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 3. Специфікації формату керівника. Зміна 1. Підтримка для додаткового елемента даних	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19785-4:2010 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 4. Специфікації формату блоку безпеки	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 19785-4:2010 / Cor 1:2013 Інформаційні технології. Структура форматів обміну загальною біометричною інформацією. Частина 4. Специфікації формату блоку безпеки. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-1:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 1. Структура	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-1:2006 Інформаційні технології. Формати обміну біометричними даними. Частина 1. Структура	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-1:2011 / Amd 1:2013 Інформаційні технології. Формати обміну біометричними даними. Частина 1. Структура. Зміна 1. Методологія перевірки відповідності	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-2:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 2. Дані про шаблон відбитка пальця	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-2:2005 Інформаційні технології. Формати обміну біометричними даними. Частина 2. Дані про шаблон відбитка пальця	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-2:2005 / Cor 1:2009 Інформаційні технології. Формати обміну біометричними даними. Частина 2. Дані про шаблон відбитка пальця. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-2:2011 / Amd 1:2013 Conformance testing methodology and clarification of defects	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 19794-2:2005 / Amd 1:2010 Інформаційні технології. Формати обміну біометричними даними. Частина 2. Дані про шаблон відбитка пальця. Зміна 1. Докладний опис положення, напрямку і типу шаблону відбитка пальця	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-3:2006 Інформаційні технології. Формати обміну біометричними даними. Частина 3. Спектральні дані про конфігурацію пальця	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-4:2005 Інформаційні технології. Формати обміну біометричними даними. Частина 4. Дані про зображення пальця	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-4:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 4. Дані про зображення пальця	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-4:2011 / Cor 1:2012 Інформаційні технології. Формати обміну біометричними даними. Частина 4. Дані про зображення пальця. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-4:2005 / Cor 1:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 4. Дані про зображення пальця. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-4:2011 / Amd 1:2013 Інформаційні технології. Формати обміну біометричними даними. Частина 4. Дані про зображення пальця. Зміна 1. Методологія випробувань на відповідність і розпізнавання дефектів	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-5:2005 Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані про зображення особи	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 19794-5:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані про зображення особи	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-5:2005 / Cor 1:2008 Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані про зображення особи. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-5:2005 / Amd 1:2007 Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані про зображення особи. Зміна 1. Умови отримання фотографій із даними про зображення особи	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-5:2011 / Amd 1:2014 Conformance testing methodology and clarification of defects	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-5:2005 / Cor 2:2008 Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані про зображення особи. Технічна поправка 2	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-5:2005 / Amd 2:2009 Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані про зображення особи. Зміна 1. Формат обміну даних при тривимірному зображенні обличчя	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-5:2005 / Cor 3:2013 Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані про зображення особи. Технічна поправка 3	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-6:2005 Інформаційні технології. Формати обміну біометричними даними. Частина 6. Дані про зображення райдужної оболонки	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 19794-6:2011 / Cor 1:2012 Інформаційні технології. Формати обміну біометричними даними. Частина 6. Дані про зображення райдужної оболонки. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-7:2007 Інформаційні технології. Формати обміну біометричними даними. Частина 7. Дані про підписи / дату	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-7:2014 Information technology – Biometric data interchange formats – Part 7: Signature / sign time series data	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-7:2007 / Cor 1:2009 Інформаційні технології. Формати обміну біометричними даними. Частина 7. Дані про підписи / дату. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-8:2006 Інформаційні технології. Формати обміну біометричними даними. Частина 8. Скелетні дані відбитків пальців	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-8:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 8. Скелетні дані відбитків пальців	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-8:2006 / Cor 1:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 8. Скелетні дані відбитків пальців. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-8:2011 / Amd 1:2014 Conformance testing methodology	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-8:2011 / Cor 1:2012 Інформаційні технології. Формати обміну біометричними даними. Частина 8. Скелетні дані відбитків пальців. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 19794-9:2007 Інформаційні технології. Формати обміну біометричними даними. Частина 9. Відеодані про судини	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-9:2011 Інформаційні технології. Формати обміну біометричними даними. Частина 9. Дані васкулярного зображення	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-9:2011 / Cor 1:2012 Інформаційні технології. Формати обміну біометричними даними. Частина 9. Дані васкулярного зображення. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-9:2011 / Amd 1:2013 Інформаційні технології. Формати обміну біометричними даними. Частина 9. Дані васкулярного зображення. Зміна 1. Методологія перевірки відповідності	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-10:2007 Інформаційні технології. Формати обміну біометричними даними. Частина 10. Дані про геометрію руки	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-11:2013 Інформаційні технології. Формати обміну біометричними даними. Частина 11. Оброблені динамічні дані про підписи / позначення	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19794-14:2013 Інформаційні технології. Формати обміну біометричними даними. Частина 14. Дані DNA	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19795-1:2006 Інформаційні технології. Випробування та звіти, що стосуються біометричних характеристик. Частина 1. Принципи і структура	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC TR 19795-3:2007 Інформаційні технології. Випробування та звіти, що стосуються біометричних характеристик. Частина 3. Випробування, специфічні до модальності	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19795-4:2008 Інформаційні технології. Випробування та звіти, що стосуються біометричних характеристик. Частина 4. Тестування взаємодії	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19795-5:2011 Інформаційні технології. Випробування біометричних характеристик і звітність з випробувань. Частина 5. Сценарій управління доступом і схема класифікації	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19795-6:2012 Інформаційні технології. Випробування біометричних характеристик і звітність з випробувань. Частина 6. Методи оцінки функціонування	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 19795-7:2011 Інформаційні технології. Випробування біометричних характеристик і звітність з випробувань. Частина 7. Випробування алгоритмів біометричного порівняння on-card	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 24708:2008 Інформаційні технології. Біометрія. Протокол взаємодії bioAPI	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 24709-1:2007 Інформаційні технології. Перевірка конформності для біометричного прикладного програмного інтерфейсу. Частина 1. Методи і процедури	90.93 – Підтвердження дії міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 24709-2:2007 Інформаційні технології. Перевірка конформності для біометричного прикладного програмного інтерфейсу. Частина 2. Твердження перевірки для провайдерів біометричних послуг	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 24713-1:2008 Інформаційні технології. Біометричні профілі для взаємодії та обміну даними. Частина 1. Огляд біометричних систем і профілів	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 24713-2:2008 Інформаційні технології. Біометричні профілі для взаємодії та обміну даними. Частина 2. Управління фізичним доступом для службовців в аеропортах	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 24713-3:2009 Інформаційні технології. Біометричні профілі для взаємодії та обміну даними. Частина 3. Біометрична перевірка та ідентифікація моряків	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC TR 24714-1:2008 Інформаційні технології. Біометрика. Юридичні та соціологічні міркування щодо застосування. Частина 1. Загальне керівництво	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC TR 24722:2007 Інформаційні технології. Біометрія. Мультимодальне й інше мультибіометричне злиття	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC TR 24741:2007 Інформаційні технології. Навчальна програма з біометрії	90.60 – Розсилка короткого звіту про перегляд	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-1:2009 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 1. Загальна методологія випробувань на конформність	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-1:2009 / Cor 1:2010 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 1. Загальна методологія випробувань на конформність. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 29109-4:2010 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 4. Дані зображення пальців	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-4:2010 / Cor 1:2011 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 4. Дані зображення пальців. Технічна поправка 1	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-5:2014 Information technology – Conformance testing methodology for biometric data interchange formats defined in ISO / IEC 19794 – Part 5: Face image data	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-6:2011 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 6. Дані зображення райдужної оболонки	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-7:2011 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 7. Послідовність даних підпису / дати підписання	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-8:2011 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 8. Дані про відбитки пальців	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29109-9:2011 Інформаційні технології. Методологія випробувань на конформність форматів обміну біометричними даними, зазначеними в ISO / IEC 19794. Частина 9. Дані васкулярного зображення	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Продовження таблиці 8

Стандарт і / або проект	**Стадія**	**МКС**
ISO / IEC 29141:2009 Інформаційні технології. Біометрика. Захоплення відбитків 10 пальців з використанням інтерфейсу біометричного прикладного програмування (BioAPI)	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29159-1:2010 Інформаційні технології. Біометричні дані про калібрування, приростання і злиття. Частина 1. Формат інформації про злиття	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29164:2011 Інформаційні технології. Біометрика. БіоAPI	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC TR 29198:2013 Information technology – Biometrics – Characterization and measurement of difficulty for fingerprint databases for technology evaluation	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC 29794-1:2009 Інформаційні технології. Якість біометричних зразків. Частина 1. Структура	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC TR 29794-4:2010 Інформаційні технології. Якість біометричних зразків. Частина 4. Дані про відбиток пальця	90.92 – Міжнародний стандарт підлягає перегляду	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*
ISO / IEC TR 29794-5:2010 Інформаційні технології. Якість біометричних зразків. Частина 5. Дані про знімок особи	60.60 – Опублікування міжнародного стандарту	35.040: Набори знаків і кодування інформації *Including coding of audio, picture, multimedia and hypermedia information, IT security techniques, encryption, bar coding, electronic signatures, etc.*

Наведемо також перелік українських біометричних стандартів, які введені в дію відповідно до міжнародних стандартів.

Міністерство економічного розвитку і торгівлі України своїм наказом від 28 листопада 2012 року № 1355 прийняло такі національні стандарти України, гармонізовані з міжнародними й європейськими стандартами, з набранням чинності з 01.05.2013 року (див. табл. 9).

Таблиця 9

ДСТУ ISO/IEC 15945:2012	Інформаційні технології. Методи захисту. Специфікація послуг TTP для підтримки застосування цифрових підписів (ISC/IEC 15945:2002, IDT)
ДСТУ ISC/IEC 19794-1:2012	Інформаційні технології. Формати обміну біометричними даними. Частина 1. Структура (ISC/IEC 19794-1:2006, IDT)
ДСТУ ISO/IEC 19795-1:2012	Інформаційні технології. Експлуатаційні випробування та протоколи випробувань у біометрії. Частина 1. Принципи та структура (ISO/IEC 19795-1:2006, IDT)

Витяг з Наказу Міністерства економічного розвитку і торгівлі України від 28 листопада 2012 року № 1355. [Електронний ресурс]. – Режим доступу: http://www.leonorm.com.ua/p/NL_DOC/UA/201201/Nak1355.htm.

Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості на своєму інтернет-порталі навів такий перелік останніх надходжень українських біометричних стандартів за 2013 – квітень 2014 років (див. табл. 10).

Таблиця 10

ДСТУ ISO/IEC 19784-1:2012	Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 1. Специфікація біометричного прикладного програмного інтерфейсу	184	12
ДСТУ ISO/IEC 19784-2:2012	Інформаційні технології. Біометричний прикладний програмний інтерфейс. Частина 2. Інтерфейс постачальника функції біометричного архіву	18	9
ДСТУ ISO/IEC 19785-2:2012	Інформаційні технології. Загальна структура форматів обміну біометричними даними. Частина 2. Процедури роботи реєстраційного органу в сфері біометрії	19	9
ДСТУ ISO/IEC 19785-3:2012	Інформаційні технології. Загальна структура форматів обміну біометричними даними. Частина 3. Специфікація формату провідної організації	74	12
ДСТУ ISO/IEC 19794-1:2012	Інформаційні технології. Формати обміну біометричними даними. Частина 1. Структура	19	7
ДСТУ ISO/IEC 19794-2:2012	Інформаційні технології. Формати обміну біометричними даними. Частина 2. Дані зображення відбитка пальця – контрольні точки	43	12
ДСТУ ISO/IEC 19794-4:2012	Інформаційні технології. Формати обміну біометричними даними. Частина 4. Дані зображення відбитка пальця	24	9
ДСТУ ISO/IEC 19794-5:2012	Інформаційні технології. Формати обміну біометричними даними. Частина 5. Дані зображення обличчя	84	12
ДСТУ ISO/IEC 19795-1:2012	Інформаційні технології. Експлуатаційні випробування та протоколи випробовувань у біометрії. Частина 1. Принципи та структура	56	7

Перелік останніх надходжень за поточний або попередній рік // Український науково-дослідний і навчальний центр проблем стандартизації, сертифікації та якості. [Електронний ресурс]. – Режим доступу: http://www.ukrndnc.org.ua/index.php?option=com_ushop&Itemid=69&y=2013.

Під час ухвалення нових національних стандартів, що регламентують біометричні технології, необхідно враховувати і досвід створення та положення міжнародних стандартів, і стандартів інших країн насамперед американських. *Адже сучасні засоби біометричної ідентифікації тестуються на відповідність і міжнародним, і американським стандартам*. Зокрема, Міжнародна біометрична група «International Biometric Group» (IBG) використовує стандарти Національного інституту стандартизації США («American National Standards Institute» /ANSI/), Міжнародного комітету зі стандартів у галузі інформаційних технологій («InterNational Committee for Information Technology Standards» /INCITS/), який, незважаючи на таку назву, також є американським, Міжнародної організації з стандартизації (ISO) і Міжнародної електротехнічної комісії (IEC)[1].

Наведемо за даними «Global Authentication Service» список визнаних світовим співтовариством біометричних стандартів /без поправок і доповнень до них/ (див. табл. 11).

Таблиця 11

Список визнаних світовим співтовариством біометричних стандартів

ANSI/NIST – American National Standards Institute / National Institute of Standards and Technology Standards

ANSI/NIST-ITL-1	Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information in Traditional Format
ANSI/NIST-ITL-2	Data Format for the Interchange of Fingerprint, Facial & Other Biometric Information in NIEM-conformant XML format

ISO/IEC – International Organization for Standardization / International Electro-Technical Commission Standards

ISO/IEC 19784	Biometric application programming interface (BioAPI)
ISO/IEC 19785	Common Biometric Exchange Formats Framework (CBEFF)
ISO/IEC 19794	Biometric data interchange formats
ISO/IEC 19795	Biometric performance testing and reporting
ISO/IEC 24708	Biometrics – BioAPI Interworking Protocol
ISO/IEC 24709	Conformance testing for the biometric application programming interface (BioAPI)
ISO/IEC 24713	Biometric profiles for interoperability and data interchange
ISO/IEC 24714	Jurisdictional and societal considerations for commercial applications
ISO/IEC 24722	Multimodal and other multibiometric fusion

[1] Международная биометрическая группа начинает новый раунд тестирования средств биометрической идентификации // BIOMETRICS.RU. – 2009. – 12 марта. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

ISO/IEC 24741	Biometrics tutorial
ISO/IEC 29109	Conformance testing methodology for biometric data interchange formats defined in ISO/IEC 19794
ISO/IEC 29141	Tenprint capture using biometric application programming interface (BioAPI)
ISO/IEC 29159	Biometric calibration, augmentation and fusion data
ISO/IEC 29794	Biometric sample quality

INCITS – InterNational Committee for Information Technology Standards

ANSI INCITS 358	The BioAPI Specification
ANSI INCITS 398	Common Biometric Exchange Formats Framework (CBEFF)
ANSI INCITS 434	Tenprint Capture Using BioAPI
ANSI INCITS 442	Biometric Identity Assurance Services (BIAS)
ANSI INCITS 429	Conformance Testing Methodology for ANSI INCITS 358
ANSI INCITS 377	Finger Pattern-Based Format for Data Interchange
ANSI INCITS 378	Finger Minutiae Format for Data Interchange
ANSI INCITS 379	Iris Image Interchange Format
ANSI INCITS 381	Finger Image Format for Data Interchange
ANSI INCITS 385	Face Recognition Format for Data Interchange
ANSI INCITS 395	Signature/Sign Format (for Data Interchange)
ANSI INCITS 396	Hand Geometry Format for Data Interchange
ANSI INCITS 423	Conformance Testing Methodology Standard for Biometric Data Interchange Format Standards
ANSI INCITS 439	Fusion Information Format for Data Interchange
ANSI INCITS 383	Biometric Profile – Interoperability and Data Interchange – Biometrics-Based Verification and Identification of Transportation Workers
ANSI INCITS 394	Application Profile for Interoperability, Data Interchange and Data Integrity of Biometric-Based Personal Identification for Border Management
ANSI INCITS 421	Biometric Profile – Interoperability and Data Interchange – DoD Implementations
ANSI INCITS 422	Application Profile for Commercial Biometric Physical Access Control
ANSI INCITS 409	Biometric Performance Testing and Reporting

Биометрические стандарты. Список признанных мировым сообществом биометрических стандартов // Global Authentication Service. – 2014. [Электронный ресурс]. – Режим доступа: http://gaus24.com/ru/info/biometricstandarts.

У матеріалах ЗМІ останнім часом з’являються публікації щодо різних чинників, які впливають на розвиток біометричного ринку.

Так, у прогнозі компанії «Technavio» виокремлена низка чинників, які у перспективі можуть ускладнювати розвиток світового ринку систем біометричної ідентифікації за відбитками пальців. І до основних чинників експерти фірми віднесли насамперед недостатній рівень стандартизації цього сегмента біометрії та відсутність повної сумісності різних систем ідентифікації за відбитками пальців[1].

Робота з розробки нових біометричних стандартів і з поліпшення існуючих проводиться безперервно. Проводяться міжнародні конференції, сесії, навчальні курси, для розвитку біометричних технологій створюються нові органи.

Так, наприклад, організація розвитку стандартів структурованої інформації (Organization for the Advancement of Structured Information Standards /OASIS/) у січні 2013 року оголосила про створення у своєму складі комітету з біометричних технологій. Головною метою діяльності нового комітету є створення відкритих стандартів, які повинні полегшити використання біометричних технологій у рамках web-сервісів і систем із сервісно-орієнтованою архітектурою загалом[2].

Європейська комісія в березні 2012 року оголосила про початок реалізації проекту з оцінки та тестування систем біометричної ідентифікації (Biometrics Evaluation and Testing /BEAT/).

Проект BEAT повинен насамперед стати відкритою онлайновою платформою для прозорої та незалежної оцінки біометричних систем на основі наявного в галузі досвіду. Крім того, до завдань проекту входить сприяння розробці засобів для виявлення вразливостей біометричних систем та їх усунення, а також надання допомоги в створенні технічної документації щодо перевірки ступеня відповідності конкретних продуктів загальним критеріям оцінки захищеності інформаційних технологій (Common Criteria). Проект BEAT має пришвидшити процес практичного втілення тих або інших теоретичних ідей у прикладні рішення[3].

Роботи з створення і поліпшення біометричних стандартів тривають постійно. З подальшим розвитком біометричних технологій виникає нагальна потреба у стандартизації, оптимізації та гармонізації нових технічних рішень. У міжнародні стандарти втілюється передовий світовий досвід і нові специфічні знання, вони сприяють вирішенню такого актуального завдання, як сумісність технологічного обладнання та інформаційних систем, які розробляються в компаніях і установах різних країн.

Сучасні стандарти є життєво важливим ресурсом світової спільноти, який має на меті уніфікацію передових технологій з одночасним сприянням їх поширенню у світі.

[1] Системы биометрической идентификации по отпечаткам пальцев: новые перспективы // BIOMETRICS.RU. – 2013. – 4 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Авторитетнейший ИТ-консорциум займется стандартизацией биометрических технологий // BIOMETRICS.RU. – 2013. – 10 января. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] В Евросоюзе начался новый проект по тестированию биометрических систем // BIOMETRICS.RU. – 2012. – 12 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розділ 17

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ СЬОГОДЕННЯ

Зараз ми живемо у час, коли світовий розвиток перейшов у постіндустріальну інформаційну епоху. Водночас рушійною силою є інновації.

Інновації – це нововведення. У сучасному світі інновації відіграють визначальну роль у процесах, які зумовлюють перебудову суспільства. Нині збільшується значення інноваційного фактора в усіх сферах діяльності будь-якої держави. Інноваційні технології та рішення сприяють підвищенню обороноздатності країни, зміцненню її національної безпеки.

Сучасні технології біометрії є представниками інноваційних технологій і охоплюють останні досягнення низки високих технологій. Високі технології – це та сфера, яка ґрунтується на високотехнологічних рішеннях і за допомогою яких багато в чому вирішуються питання національної безпеки.

Нині наукову та технічну оснащеність держави експерти визначають спеціальним інтегруючим показником – «технологічним укладом». Поняття технологічного укладу охоплює шість рівнів. Інновації шостого укладу почали реалізовуватися з початку XXI століття і ґрунтуються на інтеграції досягнень біо-, інфо-, нано- та когнітивних технологій[1].

Наприкінці 2014 року в засобах масової інформації України стало модним розмірковувати та тему «гібридної війни». Виникає питання: в чому зміст цього терміна? Однозначного визначення цього поняття поки що не має. В офіційних документах термін «гібридна війна» вперше був застосований у 13 пункті підсумкової декларації саміту НАТО, що відбувся на початку вересня 2014 року на території Шотландії. Тоді вперше на офіційному рівні було заявлено про необхідність підготовки цього блоку до війни нового типу – так званої гібридної війни (hybrid warfare).

Низка експертів у поняття «гібридної війни» включають широкий спектр ворожих намірів і обставин: таких, як кібернетична війна (кібервійна), сценарії асиметричних конфліктів низької інтенсивності, глобальний тероризм, піратство, незаконна міграція, корупція, етнічні та міжконфесійні конфлікти, безпека ресурсів, демографічні виклики, транснаціональна організована злочинність, проблеми глобалізації та поширення зброї масового ураження[2].

У середині другого десятиріччя XXI століття для протидії глобальному тероризму, незаконній міграції, транснаціональній організованій злочинності та кібернетичним

---

[1] В XXI веке нужно умное оружие // Независивое военное обозрение. – 2014. – 31 октября. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/concepts/2014-10-31/2_xxi.html.

[2] Бартош Александр. Гибридные войны в стратегии США и НАТО / А. Бартош // Независивое военное обозрение. – 2014. – 10 октября. [Электронный ресурс]. – Режим доступа: http://nvo.ng.ru/concepts/2014-10-10/1_nato.html}

загрозам значного поширення набуло використання досягнень такої наукової дисципліни, як біометрія або біометрика.

Нині біометрія – це наука, яка використовує унікальні вимірювальні параметри людини для її ідентифікації (на латині identifico – ототожнювання) та верифікації (латинською *verificatia* – підтвердження, *verus* – істинний, *facio* – роблю).

Біометрія – це не сенсація сьогодення. Загалом біометричні технології використовуються понад п'яти десятиліть, але тільки на початку третього тисячоліття нашої ери за допомогою розроблених різноманітних стандартів і тестів ці технології дійсно стали масовими й їх почали широко застосовувати у різних системах безпеки.

Сучасні біометричні системи та бази даних беруть свій початок із дактилоскопічних автоматизованих систем.

Наприкінці XX століття замість громіздких програмно-обчислювальних комплексів почали застосовувати нові технічні розробки на основі комп'ютерно-телекомунікаційних технологій, дактилоскопічних сканерів, що дало змогу здійснювати ідентифікацію осіб, які потребують перевірки, у режимі реального часу.

Нині використання біометричних методів ідентифікації та верифікації стало невід'ємною частиною інформаційних технологій.

Основною перевагою сучасних біометричних систем є можливість швидкої та досить простої ідентифікації або верифікації практично без особливих незручностей для індивідуума.

Після відомих подій 11 вересня 2001 року в Сполучених Штатах Америки масштабні проекти з використанням біометричних технологій почали інтенсивно реалізовувати і на державному, і недержавному рівні більшості країн світу. В умовах глобального поширення терористичної загрози правоохоронні та антитерористичні сили з метою покращення протидії цьому негативному явищу почали у все зростаючому обсязі використовувати останні досягнення інноваційних технологій, зокрема й біометричних.

Нині наукові фахівці та експерти біометричної галузі визначили такі перспективні напрями розвитку світового біометричного ринку:

– використання технологій біометрії у діяльності правоохоронних і силових структур, тобто боротьба з міжнародною організованою злочинністю, тероризмом, наркоторгівлею, незаконною міграцією, злочинами у фінансовій сфері тощо;

– подальша реалізація значної кількості біометричних проектів, які реалізовуються під патронатом державних структур (біометричні паспорти, ID-карти, візи, організація автоматичного контролю доступу за вказаними документами під час перетину державних кордонів);

– інтенсивне впровадження досягнень біометрії у діяльність недержавних структур, зокрема системи контролю й управління фізичним доступом (СКУД), захисту корпоративних інформаційних ресурсів і проведення фінансових транзакцій;

– все зростаюче застосування біометричних технологій до потреб кінцевих користувачів – фізичних осіб і насамперед використання біометричної верифікації у різноманітних мобільних пристроях.

Масштабні проекти з використанням біометричних технологій реалізовують усі розвинуті країни світу. До цього їх уряди спонукає потреба забезпечення державної безпеки. Застосування досягнень біометрії є однією із найважливіших умов ефективної боротьби зі злочинами проти безпеки держави, конституційних прав громадян, а також із низкою інших видів протиправних дій.

Наведемо перелік ключових завдань, вирішення яких здебільшого стало можливим за допомогою використання сучасних досягнень біометрії:

1. У сфері забезпечення безпеки держави:

– надійне посвідчення будь-якої особистості під час перетину кордону країни за допомогою проведення ідентифікаційних заходів за унікальними біометричними ознаками;

– боротьба з незаконною міграцією, тероризмом, міжнародною організованою злочинністю, наркоторгівлею, злочинами у фінансовій сфері тощо.

2. У внутрішньодержавній діяльності силових структур:

– достовірна ідентифікація осіб, які підозрюються у вчиненні злочинів і кримінальних елементів за їх унікальними біометричними ознаками;

– оперативне встановлення особистості затриманих під час проведення заходів із охорони громадського порядку, забезпечення безпеки масових заходів;

– перевірка здобувачів посад у правоохоронних органах і охоронних установах, осіб, бажаючих придбати вогнепальну зброю, інших представників подібних категорій;

– підтвердження особистості громадян, які перебувають у зонах надзвичайних ситуацій (землетруси, повені, потужні буревії, техногенні катастрофи тощо) і котрі не мають при собі документів, які ідентифікують особу;

– встановлення особистості невпізнаних трупів і осіб, які загинули під час збройних конфліктів або природних катаклізмів;

– оперативне розпізнання осіб, які перебувають у безпомічному або безпритомному стані, а також осіб, що не можуть повідомити про себе жодних відомостей;

– попередження можливості відвідин державних, муніципальних та інших установ небажаними особами (доступ яким заборонений);

– організація контролю за доступом у будівлі та приміщення судів, пенітенціарних і інших подібних установ[1];

– захист електронної інформації, що має обмежений доступ.

У XXI сторіччі головною рушійною силою розвитку світової біометрії є мінімізація існуючих загроз глобальній безпеці, необхідність ефективного протистояння атакам терористів, зниження рівня злочинності, забезпечення відповідного захисту аеропортів та інших транспортних об'єктів шляхом організації контрольованого доступу, контроль за доступом до конфіденційної електронної інформації. Для підвищення рівня безпеки, однією з складових якої є довіра до документів, що засвідчують особу, яка подорожує, світова спільнота зробила висновок, що необхідно використовувати паспортно-візові документи нового покоління (ПВДНП).

Сучасні ПВДНП – це не данина міжнародній моді, а один із дієвих заходів у боротьбі з незаконною міграцією, тероризмом і транснаціональною злочинністю.

Нині слід відзначити такі дві основні тенденції застосування біометрії силовими структурами:

– все зростаюче впровадження уніфікованих багатомодельних мультибіометричних технологій ідентифікації індивідуумів для потреб спеціальних державних структур;

– необхідність такої організації діючих ідентифікаційних систем правоохоронних і спеціальних структур, для яких можливість взаємного обміну відомостями з будь-яких баз даних цих відомств різних країн світу стає невід'ємною частиною їх роботи.

Нині розвиток біометричної галузі характеризується конвергенцією різних біометричних технологій, що забезпечує подальше зростання обсягу світового ринку біометрії та надходження інвестицій для розробки нових біометричних систем.

[1] Биометрические решения для бизнеса, общества, государства // Biolink.ru. [Электронный ресурс]. – Режим доступа: http://www.biolink.ru/solutions/markets/law.php

У майбутньому найбільш суттєвих змін у технологіях, що використовуються для забезпечення національної безпеки світових держав світу, очікують від застосування об'єктів і матеріалів, створених за допомогою нанотехнологій.

Нанотехнології (англійською nanotechnologies, німецькою Nanotechnologien f pl, інша назва – наномолекулярні технології) будуть визначати основні риси подальшого майбутнього різних технологій. Вони дозволять створити нові напівпровідники, унікальні конструктивні матеріали, а на їх базі комп'ютери, продуктивність яких на порядок або декілька порядків перевершить сучасні аналоги. Причому пристрої, які будуть розроблені з використанням досягнень наномолекулярних технологій, будуть мати значно менші розміри, вагу, енергоспоживання, що зумовить принципово нові можливості їх застосування та значне зменшення їх вартості.

У середині другого десятиріччя XXI століття технологіями біометричної ідентифікації та аутентифікації (англійською authentication – процедура перевірки істинності або справжності) вже користуються сотні мільйонів людей у різних країнах світу. Значні проекти реалізуються не тільки державними, але й комерційними структурами. Застосування біометричних технологій стало одним із найважливіших чинників, яким визначається успішність і конкурентоспроможність будь-якого суб'єкта суспільного життя – чи то приватна особа, компанія чи держава.

Більшість сучасних біометричних систем використовують такі ідентифікаційні ознаки, як зображення відбитків пальців (дуже рідко долонь), райдужної оболонки ока, геометрії рис обличчя, візерунків малюнків вен руки або пальця, форми вуха. У набагато меншому обсязі поки що застосовують технології ідентифікації за ДНК, електронним підписом і голосом.

Це далеко не повний перелік, який має стійку тенденцію до розширення. Нині у світі найбільш поширеними продовжують залишатися технології розпізнавання за відбитками пальців, райдужної оболонки очей і зображенням обличчя. З цих трьох так званих великих біометрик ідентифікація за папілярним малюнком пальця за використанням перевершує поки що всі інші технології.

Перелічимо основні напрями застосування біометрії у найближчі роки. Експерти відомої компанії «WinterGreen Research» вважають, що у 2015 – 2019 роках буде спостерігатися подальше зростання використання біометричних технологій. На першому плані та надалі буде залишатися протидія тероризму та всім видам злочинності, забезпечення безпеки аеропортів та інших інфраструктурних об'єктів. Для досягнення максимального ефекту в цьому напрямі потрібне глобальне запровадження паспортно-візових документів нового покоління (електронних паспортів, ідентифікаційних карт /ID-card/, сучасних водійських посвідчень тощо) і, як наслідок, масове запровадження систем прикордонного контролю за в'їздом – виїздом індивідуумів.

Другим суттєвим чинником стає використання можливостей засобів біометричної ідентифікації у системах інформаційної безпеки та СКУД. Це пов'язано з невпинним зростанням обробки обсягів інформації в електронному вигляді. Замість небіометричних паролів і PIN-кодів будуть використовуватись суто індивідуальні ознаки кожної людини, тобто його біометричні ідентифікатори.

На думку фахівців «WinterGreen Research», обсяг світового біометричного ринку в 2019 році має сягнути 16,7 млрд доларів проти 5,2 млрд доларів у 2012. Лідерами за темпами зростання мають стати Індія, Мексика та Росія[1].

[1] Объем мирового биометрического рынка продолжит расти // Biometrics.Ru. – 2014. – 28 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Розширення сфер застосування біометрії всі експерти пов'язують насамперед із потребою, яка постійно зростає, державних органів і бізнесу в забезпеченні необхідного рівня безпеки, з уразливістю персональних комп'ютерів й існуючих інформаційних мереж та безупинним зростанням комп'ютерної злочинності.

Для співробітників силових структур найцікавішою є інформація про практичне використання досягнень біометрії для їх потреб. Насамперед це стосується світового досвіду щодо використання біометричних баз даних (БД) в їх практичній роботі.

Загалом біометричні бази даних державних структур за своїм призначенням можна поділити на такі типи БД:

– систем спеціального призначення (спецслужб і правоохоронних структур);

– державних реєстрів населення, за допомогою яких проводиться видача паспортно-візових документів нового покоління (біометричних закордонних паспортів, ідентифікаційних карт /ID cards/ як внутрішніх посвідчень громадян та інших державних документів різного призначення);

– організації здійснення прикордонного контролю, що в багатьох випадках щільно поєднується з контролем управління за доступом на транспортних вузлах;

– контролю за доступом на режимних об'єктах;

– організації захищеного доступу до таємної та конфіденційної інформації у комп'ютерно-програмних комплексах різних державних установ;

– надання населенню різних соціальних послуг, проведення виборів, електронне урядування тощо.

За останні п'ять років у світі з'явилися бази даних із персональними відомостями, зокрема й біометричними, на сотні мільйонів осіб, причому деякі з них у недалекій перспективі можуть сягнути і понад мільярда осіб. Поза конкуренцією за чисельністю зареєстрованих даних є проект присвоєння індійським громадянам ідентифікаційних номерів «Aadhaar» (у перекладі з хінді – «система»). Станом на листопад 2014 року унікальний номер мали понад 700 млн індусів із 1,289 мільярда осіб населення Індії[1].

У підсумку в базі архівних даних на мешканців Індії заплановано зібрати понад 12 млрд зображень відбитків пальців, 2,4 млрд «сканів» райдужної оболонки ока й 1,2 млрд фотозображень[2].

За офіційним повідомленням індійського міністерства іноземних справ, у всі паспорти громадян Індії з січня 2015 року будуть вноситися біометричні відомості з карт «Аадхаар». Під час оформлення паспортів буде здійснюватися перевірка за всіма базами реєстрації злочинів[3].

Планується, що за допомогою проекту «Aadhaar» індійці зможуть користуватися біометричною системою прикордонного контролю та забезпечувати проведення чесних і прозорих виборів. У січні 2015 року індійські громадяни зможуть випробувати автоматичну систему прикордонного контролю у Міжнародному аеропорті Kempegowda в місті Бангалор. А виборча комісія Хайдарабада (четвертого за чисельністю населення міста Індії) має намір використовувати у своїй діяльності біометричні технології. Заплановано

[1] Попова Анна. Индия. Паспорт выдадут только участникам биометрического проекта Aadhaar / А. Попова // Biometrics.RU. – 2014. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Президент Индии прошла биометрическую идентификацию // BIOMETRICS.RU. – 2012. – 11 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Попова Анна. Индия. Паспорт выдадут только участникам биометрического проекта Aadhaar / А. Попова // Biometrics.RU. – 2014. – 19 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

пов'язати облікові відомості громадян, які мають право голосу, з наявними даними про них у базі «Aadhaar». Оскільки біометричні ідентифікатори є унікальними для кожної людини, це дасть можливість не допустити спроби повторного голосування під іншими установчими відомостями, крім того, громадянам, які відмовилися від голосування, не треба хвилюватися, що їх правом скористаються інші особи[1].

На прикладі розвитку індійського проекту «Aadhaar» ми бачимо зростання його багатофункціональності з погляду можливостей прикладного застосування. Спочатку планувався тільки соціальний напрям, який із часом був доповнений можливостями здійснення банківських транзакцій, паспортизації населення, проведення прикордонного контролю та виборчого процесу. Автори посібника передбачають, що згодом буде вирішено і питання криміналістичного використання бази даних «Aadhaar» для встановлення злочинців за їх ідентифікаційними ознаками. Досвід Індії у багатоцільовому використанні однієї мультибіометричної БД повинен бути прикладом для інших країн.

У Сполучених Штатах Америки створені перші у світі бази даних (БД) силових структур із біометричними відомостями на приблизно 100 млн фігурантів. Насамперед йдеться про такі автоматизовані системи біометричної ідентифікації, як:

– система Міністерства національної безпеки (Department of Homeland Security /DHS/) США US-VISIT (програма оформлення віз) із базою даних IDENT, у якій на кінець 2014 року знаходилось понад 120 млн записів[2];

– система Федерального бюро розслідування (ФБР /FBI/) США Next Generation Identification (NGI – ідентифікація нового покоління);

– система Міністерства оборони США Defense Automated Biometric Identification System (Dod ABIS) та низка інших.

Більш детально розглянемо систему розпізнавання осіб ФБР NGI, яка у повному обсязі почала функціонувати наприкінці літа 2014 року. Програма США «Ідентифікація нового покоління» почала функціонувати із 2008 року і за цей час обсяг її фінансування сягнув 1,2 млрд доларів. За офіційною інформацією метою програми є «боротьба з тероризмом і злочинністю за допомогою покращення засобів біометричної ідентифікації, а також опрацювання нових методів аналізу архівної інформації шляхом проведення дослідження, оцінки та застосування перспективних технологій».

Головна особливість NGI полягає в тому, що вона може здійснювати обробку поступаючих біометричних даних в автоматичному режимі. За допомогою системи в автоматичному режимі проходить обробку інформація, яка надходить із розташованих у всій країні відеокамер. Під час розслідування злочинів вона здійснює практично миттєву ідентифікацію осіб, які зафіксовані на відеознімках, за базою даних. Також система дозволяє правоохоронним органам кожного штату здійснювати перевірку осіб, які претендують на відповідальні посади, на можливу причетність до скоєння злочинних дій[3].

Next Generation Identification створювалася на основі системи Integrated Automated Fingerprint Identification System (IAFIS – інтегрована автоматизована система ідентифікації за відбитками пальців), яка мала базу даних із відбитками пальців на приблизно

[1] Биометрический проект облегчит индийцам въезд в страну // Biometrics.RU. – 2014. – 19 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...; Биометрический проект обеспечит честность выборов // Biometrics.RU. – 2014. – 31 октября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Индия: как продвигается крупнейший в мире биометрический проект? // Biometrics.RU. – 2014. – 8 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Новая биометрическая система ФБР введена в эксплуатацию // Biometrics.RU. – 2014. – 17 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

100 млн фігурантів. Система NGI є мультибіометричною, тобто вона використовує для біометричної ідентифікації не тільки відбитки пальців, але і відомості щодо райдужної оболонки очей, характерних рис обличчя та інших біометричних ознак. У FBI США біометрична інформація зв'язана з персональним досьє індивідуума, де зазначаються його установчі відомості (прізвище, ім'я, домашня адреса, номер водійського посвідчення, імміграційний статус, вік, етнічна приналежність тощо). Доступ до бази даних, крім Федерального бюро розслідування, мають й інші федеральні агентства, а також приблизно 18000 регіональних підрозділів правоохоронних органів.

Обсяг бази даних «Ідентифікація нового покоління» у майбутньому може сягти третини населення Америки (до відома: чисельність населення США станом на 16 травня 2014 року становила 317,8 млн). ФБР має наміри отримувати частину інформації з «цивільних джерел», тобто у БД будуть внесені біометричні відомості щодо громадян, які не вчиняли злочинів. Для кожного запису в базу даних, кримінального чи ні, надається універсальний контрольний номер (UCN), а кожен запит буде «проганятися» за всіма існуючими записами бази. Це означає, що будь-який добропорядний громадянин без наявної кримінальної історії може потрапити в статус підозрюваного за матеріалами будь-якої кримінальної справи[1].

У серпні 2014 року Федеральне бюро розслідування (Federal Bureau of Investigation /FBI – ФБР/) повідомило, що перевело у цифровий формат усі справи, що зберігалися в паперовому вигляді в архіві Інформаційної служби кримінальної юстиції (Criminal Justice Information Services /CJIS/ – підрозділ ФБР). Архівні справи, що були оцифровані, поділені на три категорії: кримінальні справи, що були порушені у період із 1970 року до нині; особові справи громадян, які працювали в державних установах або проходили службу в армії; наявні паперові дактилоскопічні відбитки пальців громадян.

За відомостями, що були розміщені на сайті Federal Bureau of Investigation, збір та оцифрування даних проводилися протягом останніх 20 років. За цей час були сформовані докладні досьє (мовою оригіналу «профілі») приблизно на 30 млн американців.

Згідно з заявою керівника відділу біометрії Інформаційної служби кримінальної юстиції, система біометричної ідентифікації Next Generation Identification є тією платформою, яка буде використовуватися американськими спеціальними структурами для отримання біометричної та іншої інформації стосовно громадян США, що підозрюються у вчиненні протиправних дій. NGI дозволяє надавати інформацію за запитами співробітників силових структур за лічені секунди, коли раніше на їх виконання були потрібні години[2].

Нині для боротьби з тероризмом, нелегальною міграцією, іншими формами міжнародної злочинності особливе значення набуває можливість однозначної та достовірної ідентифікації фізичних осіб для виявлення суб'єктів, які раніше мали конфлікт із законом або за наявними відомостями можуть мати відношення до відповідних «небезпечних» організацій.

Для реалізації можливості достовірної ідентифікації будь-якого індивідуума необхідно вирішити завдання не тільки проведення суто біометричного контролю, але й низку супутніх обов'язкових завдань, наприклад: створення і підтримування у належному стані біометричних баз даних із необхідними відомостями на всіх можливих

[1] ФБР увеличит объем новой базы биометрических данных // Biometrics.RU. – 2014. – 18 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Касьянова Любовь. ФБР оцифровало 83 млн. отпечатков пальцев граждан США / Л. Касьянова // Cnews.ru. – 2014. – 26 августа. – [Электронный ресурс]. – Режим доступа: http://uec.cnews.ru/news/top/index.shtml?2014/08/26/583990

фігурантів (в ідеальному випадку на всіх громадян Землі), безпечного їх зберігання й організації захищеного доступу до них. Оскільки це завдання поки що не вирішене у глобальному масштабі, передові держави та їх об'єднання вживають заходів щодо повної біометричної документалізації своїх громадян, осіб без громадянства, котрі перебувають на території цих країн, а також усіх іноземних громадян, які перетинають кордони цих держав, шляхом запровадження відповідних паспортно-візових документів нового покоління, а на базі цих заходів реалізацію комп'ютерного контролю за в'їздом – виїздом індивідуумів із території своїх держав або об'єднань держав.

Експерти вважають, що в 2010–2020 роках практично все населення розвинутих держав планети буде охоплено біометричними паспортно-візовими документами нового покоління (ПВДНП), отримана інформація з яких під час перетину кордону буде зберігатися в уніфікованих за організацією доступу різних державних базах даних, із часом об'єднаних за допомогою спеціально захищених каналів зв'язку в єдину міжнародну глобальну ідентифікаційну систему.

У 2007 році на липневій конференції ОБСЄ у Відні було заявлено, що з 1 січня 2015 року в'їзд на територію ЄС і США за паспортами з наклеєними фотографіями буде заборонений.

Нині програмами машинозчитуваних транспортних документів (електронних або біометричних закордонних паспортів), видачу яких під час виїзду своїх громадян за кордон повинні запровадити практично всі країни світу, опікуються такі міжнародні організації, як Організація Об'єднаних Націй (ООН), Міжнародна організація цивільної авіації (ІКАО /ICAO/), Міжнародна організація з стандартизації (ІСО /ISO/).

Наведемо перелік деяких програм ПВДНП, що вже реалізовані:

1. Програма США «US VISIT», яка вимагає безумовної біометричної ідентифікації всіх здобувачів американських віз.

2. Візова інформаційна система країн Шенгенської угоди (Visa Information System /VIS/), у якій акумулюються відомості про відбитки пальців здобувачів шенгенських віз. Із 2010 року Європейським Союзом (ЄС) запроваджена процедура зняття відбитків пальців прибуваючих іноземців у всіх країнах співтовариства (станом на 01.02.2014 року 28 держав-членів блоку).

3. Загальноєвропейська система EURODAC біометричної ідентифікації за відбитками пальців здобувачів статусу біженця та іноземців, які нерегулярно перетинають границі держав Євросоюзу.

4. Видача внутрішніх біометричних ідентифікаційних документів (ID-cards) громадянам низки європейських держав. Зараз в Європі такі програми реалізовують Великобританія, Німеччина, Португалія та Іспанія.

Нині більшість розвинутих країн світу запровадили процедуру безумовної біометричної ідентифікації всіх претендентів на отримання віз.

Наведемо основні переваги закордонних електронних або біометричних паспортів над паспортами старого взірця:

– відповідність світовим стандартам щодо документів, які засвідчують особистість;

– усі особисті дані власника біометричного закордонного паспорта захищені спеціальним підписом і зашифровані криптографічними засобами відповідно до вимог ІСАО, тому вважається, що підробка такого документа практично неможлива;

– наявність біометричного закордонного паспорта дозволяє проходити паспортний контроль на кордоні набагато швидше, оскільки процедура зчитування інформації та контроль за допомогою спеціальних біометричних сканерів відбувається миттєво.

Зараз у багатьох країнах для проходження прикордонного контролю створені спеціальні коридори для громадян різних країн з електронними паспортами, черга в яких рухається дуже швидко;

– обкладинки закордонних паспортів виробляються зі спеціального стійкого матеріалу, що дозволяє досить довго зберігати презентабельний зовнішній вигляд документа;

– виконання безальтернативної вимоги щодо можливості підписання угод про безвізовий режим між країнами;

– можливість запровадження біометричних паспортів із терміном дії до 10 років;

– наявність електронного документа є однією з складових заходів у боротьбі з незаконною міграцією, тероризмом, транснаціональною злочинністю тощо.

Застосування паспортно-візових документів нового покоління автоматично вимагає розробку і впровадження біометричних систем прикордонного контролю.

Нині міжнародною проблемою стала не свобода пересування, а національна безпека держав, особливо через проблеми незаконної міграції і, як наслідок, реалізація заходів із підвищення надійності прикордонного контролю. Зараз всі розвинені країни впроваджують виняткові заходи для встановлення контролю за нелегальною міграцією та зміцнення своїх кордонів. Більшість світових держав взяли курс на впровадження «методу інтегрованого управління» для посилення охорони кордону.

Збалансування охоронних вимог з одночасним досягненням необхідного рівня безпеки при гарантуванні права недоторканності приватного життя і належного комфорту перетинання кордону можливі тільки в разі використання останніх досягнень біометричних технологій.

Електронні документи й автоматичні системи ідентифікації особистості дозволяють подорожуючим значно зменшити час проходження прикордонного контролю. Нині багато країн запровадили технології автоматизованого прикордонного контролю електронних паспортів і систем пришвидшеного проходження подорожуючими процедур контролю[1].

У сучасних системах прикордонного контролю здійснюється процедура порівняння оцифрованої фотографії та інших біометричних параметрів, записаних у мікрочіп електронного документа, з реальними зображеннями обличчя пред'явника ПВДНП та його відбитками пальців.

Цілком логічно, що автоматизовані системи прикордонного контролю набули найбільшого поширення у великих міжнародних аеропортах. Крім того, використання біометричних технологій в аеропортах дозволяє забезпечити зручну реєстрацію на рейс, пришвидшене проходження всіх форм контролю, зменшення часу під час посадки на борт літака та безпечну ідентифікацію власників багажу. Крім того, під час виконання міжнародних авіарейсів у аеропортах прибуття використання біометричних систем паспортного та візового контролю дозволяє авіапасажирам суттєво заощадити час проходження прикордонного контролю.

Одночасно біометрична перевірка особистості авіапасажирів за базами даних спецслужб дозволяє ідентифікувати осіб, які можуть становити загрозу і для інших авіаційних пасажирів, і для національної безпеки тих держав, до яких вони прибувають.

Отже, використання технологій біометрії є корисним і для авіапасажирів, і для урядових структур країн, до яких вони прямують.

---

[1] Биометрические системы пограничного контроля: новый прогноз // Frost & Sullivan. – 2013. – 10 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

Необхідно зазначити, що в багатьох аеропортах західних країн запроваджені або запроваджуються спеціальні програми ідентифікації особистості мандрівників, які призначені для зменшення часу, необхідного для здійснення посадки авіапасажирів на літаки.

Останнім часом біометричні технології почали дедалі ширше застосовувати у морських або річкових портах і на залізничних вокзалах.

Про важливість використання біометричних технологій в аеропортах і прикордонних пунктах пропуску громадян свідчить повідомлення про відкриття восени 2014 року Центру тестування засобів біометричної ідентифікації в американському штаті Меріленд. Ініціатором створення нової установи є Митна і прикордонна служба США (Customs and Border Protection – CBP). Головним завданням нового Центру є підвищення ефективності засобів біометричної ідентифікації, що використовуються у програмах контролю за в'їздом-виїздом до Сполучених Штатів Америки іноземних громадян. Особлива увага приділяється контролю за терміном перебування та часом виїзду з країни[1].

Сьогодні під час політичної, економічної й енергетичної нестабільності на Євразійському континенті та у всьому світі дедалі гостріше проявляються міграційні та терористичні проблеми. Перелічимо загальносвітові негативні тенденції, які протягом 2014 року стрімко розвивалися.

На Близькому Сході й надалі тривали бойові дії. На Синайському півострові єгипетські армія та поліція мали постійні сутички з місцевими терористами, Лівія охоплена громадянською війною, в Ємені триває боротьба між сунітами та шиїтами, на теренах Іраку і Сирії з'явилася ісламська держава Іраку та Леванту (ІДІЛ), яка проголосила всесвітній джихад. Радикальний джихадизм у повну силу проявив себе у Малі, Чаді, Камеруні, Нігерії та Центральноафриканській Республіці.

Що стосується європейського континенту, то на Україні ведеться громадянська війна. Порушена система безпеки Європи. У низці країн Старого Світу посилились сепаратистські тенденції, ще більше ускладнились суперечності між корінними європейцями та мігрантами[2].

У серпні 2014 року збори керівників держав і урядів країн Європейського Союзу (ЄС), визнали ІДІЛ найголовнішою загрозою європейській безпеці. Особливо керівні органи ЄС стурбувало таке небезпечне явище, як участь громадян Євросоюзу, які сповідують іслам, у збройних формуваннях ісламської держави Іраку та Леванту[3]. Тому стисло розглянемо проблему ісламізації Західної Європи.

За останні 20 років кількість мусульман у Старому Світі зросла на 50%. Нині за поширеністю іслам на європейському континенті є другою релігією після християнства, причому найбільш швидкозростаючою. Кількість мусульман зросла у країнах Західної Європи з 29,6 млн чоловік у 1990 році до 44,1 млн у 2010 році. Мусульманська частка у загальній чисельності населення зросла з 4,1% до 6%. За прогнозом експертів, у 2030 році 8% мешканців Західної Європи будуть сповідати іслам, а в 2100 – кожен четвертий[4].

---

[1] Центр тестирования средств биометрической идентификации откроется в США // Biometrics.RU. – 2014. – 12 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] 10 главных военных событий 2014 года // Армейский вестник. – 2014. – 10 декабря. [Электронный ресурс]. – Режим доступа: http://army-news.ru/2014/12/...

[3] Минеев Александр. Против терроризма, не поступаясь принципами / А. Минеев // Новая газета. – 2015. – 8 января. [Электронный ресурс]. – Режим доступа: http://subscribe.ru/digest/economics/society/...

[4] Чернега Алексей. Сколько в Европе живет мусульман / А. Чернега // Euromag.ru. – 2015. – 14 января. [Электронный ресурс]. – Режим доступа: http://www.euromag.ru/catalogs/stat/40825.html

Доволі складно дати точну оцінку потенціалу рекрутування джихадистів з Європи до зони бойових дій на Близькому Сході. Історично склалося так, що Франція посідає перше місце на європейському континенті за чисельністю мусульманського населення. Послідовники пророка у цій державі мають у користуванні понад 2100 мечетей і становлять 7,5% від 62 млн французів. У 83-мільйонній Німеччині іслам сповідують 5% громадян, у Великобританії приблизно таке ж співвідношення.

За офіційними повідомленнями міністрів МВС і голів спецслужб країн ЄС загальна чисельність рекрутів-джихадистів становить понад 3 тис. Це в основному мешканці Німеччини, Франції, Бельгії, Нідерландів, Данії, Швеції, Сполученого Королівства, меншою мірою Іспанії та Австрії.

Питання «іноземних бойовиків» (європейців, які беруть участь у бойових діях на боці ІДІЛ) стала постійною на щомісячних зустрічах міністрів іноземних справ країн Європейського Союзу.

Наприкінці вересня 2014 року один із високопосадовців Європейського Союзу, який добре знайомий із антитерористичною тематикою і який захотів залишитися невідомим, на одному з брифінгів попередив про неминучість значного теракту в Європі за участю бойовиків, які повернулися з зони бойових дій[1].

Паризький теракт 7 січня 2015 року не був несподіванкою для спецслужб США, Ізраїлю та Великобританії. За інформацією німецької газети «Bild am Sonntag», американське агентство національної безпеки попереджало відповідні європейські служби про те, що теракт у Парижі має стати першим у серії терактів на теренах Західної Європи. Ще у серпні 2014 року американський генерал Майкл Флін попереджав: «Теракти такого роду не повинні бути несподіванкою. Ми станемо свідками й інших терактів». Голова британської MI-5 Ендрю Паркер, своєю чергою, зазначав, що «збільшилась небезпека вчинення теракту з багаточисельними жертвами». Британські спецслужби інформували своїх європейських колег щодо загроз учинення терактів на літаках[2].

На тому ж серпневому засіданні 2014 року очільниками Євросоюзу було дано доручення керівним органам у Брюсселі пришвидшити виконання червневої програми посилення боротьби з тероризмом 2013 року, яка складалася з 22 завдань. До переліку основних заходів увійшли: запровадження другого покоління Шенгенської інформаційної системи (SIS II – у базі даних цієї системи мають перебувати відомості про всіх встановлених злочинців і правопорушників), посилення частоти перевірок на кордонах, обмін інформацією про бойовиків із держав ЄС між компетентними органами цих країн, передача відповідних відомостей Європолу для спільного аналізу.

До переліку невідкладних заходів керівники європейських силових структур намагалися внести на затвердження Європарламентом директиви щодо поіменної реєстрації авіапасажирів (PNR)[3].

У січні 2015 року пленарна сесія Європейського парламенту через три роки знову ухвалила рішення про повернення до обговорення законопроекту, яким вимагається від

---

[1] Минеев Александр. Против терроризма, не поступаясь принципами / А. Минеев // Новая газета. – 2015. – 8 января. [Электронный ресурс]. – Режим доступа: http://subscribe.ru/digest/economics/society/...

[2] «Моссад» и ЦРУ предупреждают Папу Франциска: «Ватикан – следующая цель ИГИЛ» // Inopressa.ru. – 2015. – 15 января. [Электронный ресурс]. – Режим доступа: http://www.inopressa.ru/article/12Jan2015/Giornale/...

[3] Минеев Александр. Против терроризма, не поступаясь принципами / А. Минеев // Новая газета. – 2015. – 8 января. [Электронный ресурс]. – Режим доступа: http://subscribe.ru/digest/economics/society/...

авіакомпаній надання силовим відомствам персональних відомостей щодо пасажирів із зазначенням маршрутів їх пересування (директива PNR)[1].

Міністри внутрішніх справ країн ЄС і США 11 січня 2015 року домовилися про активізацію обміну розвідданими і посилення контролю за кордонами Євросоюзу для поліпшення реагування на існуючі терористичні загрози. Також було ухвалено рішення про отримання офіційного дозволу на проведення контролю за телефонними розмовами, електронною перепискою та уподобаннями в Інтернеті європейських громадян. Отже, Західна Європа стає на американський шлях боротьби з екстремізмом, який вимагає обмежень цивільних свобод[2].

Особливо слід акцентувати на тому, що одним із виконавців теракту 7 січня у Парижі був бойовик ІДІЛу, що мав судимість за статтею тероризм і заборону на в'їзд до США. Цей факт висвітлює значущість проблеми, яка виникла перед французькими чиновниками, розвідкою та поліцією. Найважливіше завдання спецслужб Західної Європи – нейтралізація діяльності бойовиків-ісламістів, які є громадянами країн ЄС.

На думку головного редактора сайту «RéseauVoltaire» Тері Мейсана, напад на Charlie Hebdo – це «французьке 11 вересня». Він вважає, що це була не помста журналістам, а провокування європейської громадянської війни в рамках стратегії «зіткнення цивілізацій». Ті, хто підготував напад, чітко уявляли, що цим нападом вони спричинять розкол між французами-мусульманами і французами-немусульманами[3].

Запровадження біометричних систем та інших інноваційних технологій є складовою загального комплексу заходів міжнародної спільноти у боротьбі проти незаконної міграції, тероризму та транснаціональної злочинності. Про це яскраво свідчить намір влади Німеччини відбирати персональні посвідчення (ID-карти) у громадян ФРН, які бажають приєднатися до бойовиків «Ісламської держави»[4].

Для упорядкування міграції біометричні показники запроваджені у такі міжнародні ідентифікаційні документи:

– закордонний, дипломатичний і службовий паспорти, посвідчення моряка;

– національні електронні картки (ID-cards);

– візи для в'їзду до країни або транзитного проїзду через її територію;

– посвідчення біженця, що видається іноземцю, згідно з яким він може перебувати на території держави та здійснювати процедури в'їзду-виїзду.

Проведення біометричної ідентифікації біженців дозволяють ефективно вирішувати їх проблеми. Наприклад, Управління Верховного комісара Організації Об'єднаних Націй у справах біженців (УВКБ) з весни 2014 року проводить біометричну ідентифікацію біженців у Йорданії, Лівані та Туреччині. Біометрична ідентифікація виключає випадки повторної реєстрації одного і того ж біженця за різними установчими даними і, як наслідок, можливі махінації під час отримання гуманітарної допомоги. Крім боротьби з зловживаннями, використання біометричної системи дозволяє забезпечити точний облік

[1] Евродепутаты спорят о мерах против терроризма // Ru.euronews.com. – 2015. – 12 января. [Электронный ресурс]. – Режим доступа: http://ru.euronews.com/...

[2] Макаренко Георгий. Свобода или безопасность: пойдет ли ЕС по пути США в борьбе с террором / Г. Макаренко, О. Макаров // РБК. – 2015. –12 января. [Электронный ресурс]. – Режим доступа: http://top.rbc.ru/politics/...

[3] Четверикова Ольга. Расстрел Charlie Hebdo: трагический урок Европе / Ольга Четверикова // Военно-политическая аналитика. – 2015. –10 января. [Электронный ресурс]. – Режим доступа: http://vpoanalytics.com/...

[4] Макаренко Георгий. Свобода или безопасность: пойдет ли ЕС по пути США в борьбе с террором / Г. Макаренко, О. Макаров // РБК. – 2015. –12 января. [Электронный ресурс]. – Режим доступа: http://top.rbc.ru/politics/...

біженців. Достовірний облік дозволяє ефективно планувати потреби біженців у продовольчих та інших товарах першої необхідності[1].

Понад півстоліття прийнято вважати, що дані в електронному форматі є найстислішим способом зберігання інформації порівняно з картотечними та іншими паперовими засобами зберігання будь-яких відомостей. Але у новому тисячолітті з кожним роком зростає загроза несанкціонованого впливу на електронні інформаційні ресурси, бази даних і обробку інформації з обмеженим доступом. Фактично світ вступив у нову техногенну епоху, яка характеризується такими негативними явищами, як кібернетична злочинність, кібернетичний тероризм, а останні декілька років – вже і кібернетичні війни.

У першому десятилітті третього тисячоліття нашої ери спочатку в Сполучених Штатах Америки, а потім і в інших країнах почалося втілення в життя програм повної інформатизації збройних сил. США першими розробили доктрину досягнення інформаційної переваги та ведення мережевоцентричних операцій із використанням для керування військами єдиного інформаційного простору, що функціонує у реальному масштабі часу. Тепер в Америці розробляють стратегії ведення війн у віртуальному просторі.

Кібернетичні атаки стали звичним явищем у сучасному світі. І, крім хакерів, які діють самостійно або об'єднавшись у співтовариства, останнім часом дедалі більше кібератак вчиняють спеціальні підрозділи збройних сил і національних спецслужб багатьох держав. Підрозділи для вирішення проблем, пов'язаних із комп'ютерними загрозами, вже функціонують у США, Великобританії, Китаї, Північній Кореї, Ірані, Росії та низці інших країн[2].

Однозначно можно стверджувати, що розробками ефективних систем кібернападу і протидії загрозам у віртуальному просторі з 2013 року зайнялися більшість держав світу. Наприклад, США за останні роки почав виділяти значні кошти на розробку систем кібернетичної зброї та захисту від неї. За повідомленнями інформаційного агентства Bloomberg спеціалізованому підрозділу United States Cyber Command, штаб квартира якого знаходиться на території військової бази Форт-Мід (штат Меріленд), у 2013 році було виділено 3,94 млрд доларів, а у 2014 році вже 4,65 млрд доларів. За відомостями цього ж агентства, штат US Cyber Command має становити 5000 осіб[3].

Не відстає від США і Китай. За деякими відомостями, чисельність китайських кіберпідрозділів може сягати 6000 тис. осіб. Кібервійська – наукомісткий вид військ, тому головна його складова – це добре підготовлені кадри. До штату військ інформаційних операцій разом із програмістами вводять також висококваліфіковані математики, інженери, криптографи, зв'язкові, перекладачі та інші допоміжні фахівці. Ступінь напруги у віртуальному просторі зростає, експерти стверджують, що інформаційні атаки сьогодні використовуються для вирішення військових і політичних завдань. Підтвердженням такого висновку є виявлення у листопаді 2014 року вірусу Regin. Фахівці вважають, що розробка

[1] Сирийские беженцы в Турции проходят биометрическую идентификацию // Biometrics.RU. – 2014. – 5 сентября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Гринуолд Гленн. Новое крупное расширение «подразделения кибербезопасности» в Пентагоне предпринято вовсе не ради обороны / Г. Гринуолд // Inopressa.ru. – 2013. – 29 января. [Электронный ресурс]. – Режим доступа: http://inopressa.ru/article/; Флоранский Александр. В Британии создана Команда быстрого реагирования для борьбы с киберугрозами / А. Флоранский // Best of Security. – 2014. – 10 апреля. [Электронный ресурс]. – Режим доступа: http://bos.dn.ua/viewnews.php?nid=1045; Военное подразделение по борьбе с хакерами будет учреждено в ракетных войсках РФ // Securitylab.ru. – 2014. – 18 июня. [Электронный ресурс]. – Режим доступа: http://www.securitylab.ru/news/460357.php

[3] Иран и кибервойны // Око планеты. – 2014. – 22 декабря. [Электронный ресурс]. – Режим доступа: http://oko-planet.su/politik/politwar/265225-iran-i-kibervoyny.htm.

цієї шкідливої програми зайняла багато місяців або навіть років. На думку аналітиків, за розробкою Regin повинна стояти держава, оскільки тільки вона володіє таким обсягом ресурсів, який потрібен для створення вірусу подібного рівня складності. Але найвідомішим прикладом хакерської атаки є використання вірусу Stuxnet для кібернападу на іранську атомну електростанцію в Бушері та на ядерну програму Ірану. У підсумку на значний час було паралізовано роботу декількох тисяч центрифуг, які використовувались для збагачення урану[1].

Дуже важливим питанням безпеки держави є спроможність захисту від атак у кібернетичному просторі. Розглянемо це питання на прикладі Сполучених Штатів Америки, оскільки Америка є однією з найбільш комп'ютеризованих країн світу.

Питання кібернетичної безпеки США особливо стало актуальним після проведення низки комп'ютерних атак на інформаційні системи великих банківських установ, торгових мереж і приватних компаній. А 12 січня 2015 року хакери, які згідно з їхньою заявою діяли як прихильники «Ісламської держави», зламали аккаунт Центрального командування Збройних сил США в Twitter-е та канал відеохостингу Youtube. На Twitter-аккаунті @CENTCOM з'явився напис «Кіберхаліфат», лозунги халіфату та погрози на адресу Сполучених Штатів Америки. В Інтернет-мережі хакери виклали викрадений список американських генералів із вказанням їх адрес та інших установчих даних.

Після цих подій президент США подав у Конгрес законопроект із метою посилення захисту американських комп'ютерних мереж і невідкладних заходів із нейтралізації кібернетичних загроз. Під час виступу в Міністерстві національної безпеки США 13 січня Барак Обама заявив, що «Тільки вчора кібератаці були піддані сторінки військових Twitter-а і YouTube-а. Суттєвих негативних наслідків це не мало, оскільки, наскільки нам відомо, витоку конфіденційної інформації не було. Слідство триває. І треба пам'ятати, що загроза кібератак – актуальна проблема, яка потребує негайного вирішення»[2].

Особливої уваги заслуговує думка Едварда Сноудена щодо акцентів дій у кібернетичному протистоянні: «Власний захист США від атак в інтернет-мережі набагато важливіший, ніж можливість проводити атаки на відповідні об'єкти закордонних держав. Тому що, коли ми говоримо про інтернет і технічний сектор, то тут ми можемо набагато більше втратити, ніж будь-яка інша країна. Якби ворог не націлювався на наші електростанції, а радше атакував би магістральний маршрутизатор, тобто ту основу, яка з'єднує всі зв'язки в інтернеті, це мало б величезний вплив на суспільство і цим діям не було б що протиставити, Сполучені Штати не змогли б надати достойну відсіч»[3].

Що стосується можливості кібернетичного тероризму, то учасники міжнародного форуму з кіберзахисту, який відбувся у грудні 2012 року, обґрунтовано довели той факт, що однією з гострих сучасних проблем світових інформаційних технологій є виникнення кібертероризму. Адже будь-яка розробка, що була здійснена фахівцями будь-якої країни для ведення кібервійни, може згодом опинитися в руках терористів, які зможуть використати її для досягнення своєї мети[4].

---

[1] За организацией хакерских атак стоят спецслужбы ведущих государств // Око планеты. – 2014. – 5 декабря. [Электронный ресурс]. – Режим доступа: http://oko-planet.su/politik/politwar/...

[2] Белый дом принимает меры по борьбе с киберугрозой // Ru.euronews. – 2015. – 14 января. [Электронный ресурс]. – Режим доступа: http://ru.euronews.com/2015/01/14/...

[3] Эдвард Сноуден: США могут потерять в кибервойнах больше, чем любая другая страна // Око планеты. – 2015. – 10 января. [Электронный ресурс]. – Режим доступа: http://oko-planet.su/politik/politiklist/...

[4] Бовал Валерий. Реальная угроза – киберпротивостояние / Валерий Бовал // Военное обозрение. – 2012. – 19 декабря. [Электронный ресурс]. – Режим доступа: http://topwar.ru/22244-realnaya-ugroza-kiberprotivostoyanie.html.

Останні досягнення біометричних технологій у все зростаючому обсязі продовжують використовувати для забезпечення національної безпеки, створення нових надійних систем із захисту конфіденційної інформації, організації управління доступом співробітників до різного IT-устаткування, інформаційно-комунікаційних систем і мереж. Упровадження біометричних технологій у пристрої захисту інформації, розробка спеціальних захисних систем, які побудовані на інтеграції біометричних технологій з іншими інноваційними рішеннями, дозволяє набагато зменшити можливість витоку конфіденційної інформації. Нині біометричні технології дедалі ширше використовуються у різних устаткуваннях, мобільних пристроях та організації доступу до Інтернет-мережі. Для підвищення захисних можливостей та поліпшення контролю за доступом проводяться заходи з інтеграції біометрії з іншими інформаційними технологіями, зокрема з такою, як інфраструктура відкритих ключів цифровому підпису (каталог таких ключів ІКАО продовжує активно формувати).

Що стосується впровадження досягнень біометрії безпосередньо у технології цифрового підпису, то ще у березні 2013 року компанія «Hitachi» оголосила про створення першої повністю працездатної системи для роботи з цифровими підписами на базі біометричних даних. Для створення оцифрованого підпису як біометричного ідентифікатора використовувався малюнок вен на пальці користувача[1].

Компанії, які займаються питаннями інформаційної безпеки, попереджають, що розрив між засобами боротьби з загрозами інформаційній безпеці та новими формами проведення дій кібернетичних атак продовжує збільшуватися.

Для фінансових установ, особливо банків, дуже важливо мінімізувати ризики несанкціонованого витоку інформації, зокрема й від інсайдерських дій. Тому нині фінансова галузь зробила безпеку одним із своїх головних пріоритетів. Загроза цілісності банківської системи і та ключова роль, яка відводиться фінансовим ринкам у безпеці країн, вимагає розробки сучасної захисної стратегії та впровадження наступного покоління пристроїв і нового програмного забезпечення для формування надійного інформаційного захисту. Із метою розробки нових захисних рішень Комісія з цінних паперів і бірж США створила Центр аналізу й обміну інформацією щодо фінансових послуг (Financial Services Information Sharing and Analysis Center)[2].

Біометрія дає можливість подальшої оптимізації інформаційної безпеки фінансових структур, особливо під час здійснення розрахунків клієнтів за допомогою мобільних пристроїв або платіжних карт.

Використання біометричних ідентифікаторів разом із відповідним програмним забезпеченням дозволяє створювати довгі та складні паролі доступу до інформаційних ресурсів. Але користувачам запам'ятовувати їх не обов'язково – практично це виглядає як авторизація за допомогою будь-якого біометричного показника. Відбитком пальця, скануванням райдужної оболонки ока, малюнком вен пальця або долоні можливо замінити паролі не тільки до входу в операційну систему, але і доступ до відповідного програмного забезпечення (наприклад, до банківської інформаційної системи або термінала, електронної пошти, онлайнових ресурсів тощо).

У грудні 2014 року міжнародна платіжна система MasterCard Worldwide проінформувала про успішне завершення пілотного проекту з впровадження нових біометричних платіжних карт у Норвегії.

---

[1] Разработана технология биометрической цифровой подписи // СОФТ@Mail.Ru. – 2013. – 15 марта. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Поднять мосты, закрыть крепостные ворота // Inopressa.ru. – 2014. – 12 сентября. [Электронный ресурс]. – Режим доступа: http://inosmi.ru/world/...

Родзинкою цього впровадження є використання у кожній карті вбудованого надтонкого сканера відбитків пальців. Ця новація не вимагає створення спеціальних біометричних баз даних клієнтів і дозволяє використовувати навіть старе обладнання систем контролю за доступом, але з новим програмним забезпеченням[1].

Рішення такого типу поки що на біометричному ринку ще не стало трендом, але зважаючи на зростання загроз безпеці системам контролю та управління доступом (СКУД) і все зростаючий тиск зі сторони правозахисників щодо контролю за використанням персональних відомостей громадян, карти з вбудованими надтонкими зчитувачами біометричних ідентифікаторів є одним із найліпших варіантів, якщо не найоптимальнішим варіантом організації системи контролю за доступом. Біометричні ідентифікатори – унікальна річ для розпізнавання особи. Але під час використання монотехнологій біометричної ідентифікації існує ймовірність хибного ідентифікування за виготовленими муляжами. Найбільша кількість способів виготовлення муляжів існує для біометричних пристроїв, які розпізнають особу за відбитками пальців, що цілком зрозуміло, оскільки ця технологія була та залишається найпоширенішою.

Останньою новиною у виготовленні муляжів відбитків пальців є повідомлення щодо можливості відтворення індивідуальних шкірних візерунків пальців за якісною фотографією рук людини та, відповідно, можливості здійснення хибного ідентифікування. Про це на конференції Chaos Communication Congress (CCC) у Гамбурзі повідомив відомий під ніком (англ. *nick* – прізвисько) Starbug німецький хакер Ян Кріслер. Він заявив, що скопіював відбиток пальця міністра оборони Німеччини Урсули фон дер Ляйен, використавши для цього знімки, що були отримані під час прес-конференції за допомогою звичайного фотоапарата.

Я. Кріслер висловив жартівливе припущення, що, дізнавшись про таку можливість, політики у майбутньому почнуть з'являтися на публіці тільки у рукавичках.

На думку експертів, досягнення хакера Starbug не ставить біометричну форму захисту під загрозу, а лише вказує на наявність суттєвого недоліку. Тому використання монобіометричних даних повинно підкріплюватися доповнюючими рівнями захисту[2].

Надійні системи захисту використовують, як правило, мультибіометричні та багатофакторні технології ідентифікації або їх симбіоз.

Нині головною проблемою всіх існуючих систем доступу й електронних баз даних залишається можливість викрадення ідентифікуючих відомостей або пристроїв для проведення несанкціонованого доступу до масиву еталонних записів.

Тому особливо слабким місцем використання біометричних технологій є можливість перехоплення ідентифікаційної інформації в електронному вигляді під час її передачі від сканера до бази даних. Упровадження карток із вбудованими сканерами відбитків пальців запобігають витоку безпосередньо самої інформації щодо параметрів біометричного ідентифікатора, але не перехопленню самого електронного пакета сигналів до устаткування, яке керує наданням дозволу на доступ.

На думку експертів, найліпшим захистом від несанкціонованого доступу може бути запровадження рішень, що засновані на технології біометрично-криптографічного шифрування. Симбіоз біометричних і криптографічних технологій створює нові перспективи строгої ідентифікації, забезпечення інформаційної безпеки та захисту персональних даних.

---

[1] Биометрические платежные карты: Норвегия, Британия, далее – везде? // Biometrics.RU. – 2014. – 09 декабря. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Хакеры научились воспроизводить отпечатки пальцев с фотографий // Eterra Digest. – 2015. – 15 января. [Электронный ресурс]. – Режим доступа: http://eterra.info/mosaic/...

У липні 2014 року Біометричний інститут, який діє на теренах Європи, Австралії та Нової Зеландії, оприлюднив підсумки опитування, що було проведено серед експертів і членів цієї організації. Головною і багатообіцяючою тенденцією 2014–2015 років у біометричній галузі більшість опитуваних визнало інтеграцію біометричних технологій у мобільні пристрої. Використання біометрії у системах прикордонного контролю посіло друге місце (нагадаємо, що раніше цей тренд декілька років поспіль посідав перше місце), а третє місце посіло застосування біометричних технологій у мобільних платіжних системах у мобільних транзакціях[1].

До цих висновків необхідно додати, що біометрія і надалі буде дедалі більше застосовуватися у різних системах контролю за будь-якою формою доступу, все зростаюча кількість держав почнуть використовувати біометричну ідентифікацію у забезпеченні ефективності процесів голосування. Ще однією істотною тенденцією стає дедалі ширше застосування досягнень біометричних технологій у споживчій електроніці та забезпеченні безпеки житла. Будуть і надалі посилено розвиватися системи, що використовують можливості мультибіометричної та багатофакторної ідентифікації.

Свого часу Уінстон Черчилль (сер Ві́нстон Леонард Спенсер-Че́рчиль /англ. Winston Leonard Spencer-Churchill/ – прем'єр-міністр Великої Британії у роки Другої світової війни) зазначив: «Імперії майбутнього – це імперії інтелекту». Відомий американський філософ Елвін Тоффлер (англ. Alvin Toffler) у праці «Метаморфози влади» (1990 р.) стверджував, що основним чинником сучасної «революції влади» є знання, тобто нині знання більше не є простим додатком до влади грошей і військової моці, а стало їх суттю. Цим можно пояснити той факт, що в світовому просторі дедалі сильніше розгортається битва за контроль над інформацією та засобами комунікацій[2].

Із початку XXI сторіччя в низці навчальних закладів США, Великобританії, Канади та інших країн розпочато викладання курсу біометрії. У американському Університеті Західної Вірджинії (West Virginia University – WVU) викладання цієї дисципліни ведеться ще з 2001 року.

Курс біометрії має міждисциплінарний характер і охоплює обчислювальну й електронну техніку, біологію та статистику. Після завершення університету студенти, які засвоїли курс біометрії, отримують, як правило, дипломи з технічних наук і обчислювальної техніки. На базі West Virginia University діє науковий Центр із досліджень у сфері технологій ідентифікації (Center for Identification Technology Research /CITeR/). У його роботі ще у 2009 році брали участь понад 20 комерційних компаній і федеральних агентств[3].

У розвинутих країнах світової спільноти для представників силових структур дедалі актуальнішим стає завдання ефективного практичного застосування інформаційних технологій. Найважливішою є підготовка кваліфікованого персоналу, що міг би у повному обсязі використовувати широкий і різноманітний потенціал інформаційних технологій, зокрема й біометричних.

---

[1] Интеграция биометрических технологий и мобильных устройств признана главным трендом развития отрасли // Biometrics.RU. – 2014. – 15 июля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Буренок Василий. Современная система вооружения должна включать средства защиты сознания / В. Буренок // Око планеты. – 2014. – 31 июля. [Электронный ресурс]. – Режим доступа: http://oko-planet.su/politik/politwar/...

[3] Университет Западной Вирджинии готовит специалистов по биометрии // BIOMETRICS.RU. – 2009. – 26 февраля. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp...

Нині дуже стрімкий розвиток біометрії вимагає відповідної якісної підготовки персоналу, який обслуговує біометричні системи і пристрої. Ця вимога особливо стосується співробітників силових структур, оскільки більшість із них не має спеціальної технічної освіти. Біометрія посідає дедалі важливіше місце у нашому повсякденному житті. Нині біометричні системи практично зробили непотрібним необхідність запиту будь-яких фізичних документів або ключів-паролів: фактично нагляд за індивідуумом може здійснюватися не тільки без його дозволу, але і без його відома – за потреби компетентні органи за допомогою симбіозу біометричних та інших інформаційних технологій можуть відслідковувати кожен його крок.

В Україні майже не має узагальнюючих видань щодо історії, розвитку і використання сучасних досягнень біометрії на державній мові. Здійснений авторами посібника інформаційний пошук в Інтернеті виявив, що більшість Інтернет-публікацій українською мовою стосуються запровадження в Україні біометричних паспортів і можливості вирішення питання безвізового режиму з Європейським співтовариством. У невеликій кількості трапляються публікації щодо ролі біометричних технологій у захисті інформації. Останньою новиною щодо впровадження біометричних документів є повідомлення Державної міграційної служби (ДМС) про приймання заяв на їх оформлення з 12 січня 2015 року. Біометричні закордонні паспорти будуть видаватися на 10 років. Для їх видачі до кінця січня 2015 року в підрозділах ДМС повинні додатково встановити 573 автоматизованих робочих місця (терміналів) для видачі біометричних закордонних паспортів[1].

Для правоохоронців цікавою є інформація про появу проекту Закону України «Про національну поліцію». У першій частині статті 14 «Використання досягнень науки та техніки, сучасних технологій та інформаційних систем» зазначено, що «Національна поліція у своїй діяльності використовує досягнення науки та техніки, інформаційні системи, системи зв'язку та передачі даних, а також інформаційно-телекомунікаційну інфраструктуру».

У четвертій частині цієї статті наголошується, що «Міністерство внутрішніх справ України забезпечує Національну поліцію можливістю користування мережею Інтернет, автоматизованими системами, інтегрованими базами даних, у тому числі міжнародними»[2].

Біометричні технології не перебувають у статичному положенні – вони невпинно розвиваються. Реальність сьогодення така, що відомості про використання силовими структурами країн світу інформаційно-біометричних технологій для вирішення криміногенних проблем світової спільноти дуже швидко застарівають.

Нині низка нових методик біометричної ідентифікації або аутентифікації перебувають на ранніх стадіях розвитку, зокрема: швидкісна ДНК-ідентифікація, встановлення особистості за особливостями ходи та запаху тіла, ідентифікація за формою вуха та навіть прогнозування намірів дій за біоелектричними мозковими хвилями.

Автори посібника спробували якнайповніше висвітлити основні досягнення, тенденції та проблеми використання силовими структурами останніх досягнень біометричних технологій. Практичний інтерес для правоохоронних органів України становить можливість використання вже існуючих біометричних баз даних Європолу, Інтерполу та прикордонних служб суміжних держав.

[1] Біометричний закордонний паспорт буде видаватися на 10 років // УНІАН. – 2015. – 9 січня. [Електронний ресурс]. – Режим доступу: http://www.unian.ua/society/...

[2] Закон України про національну поліцію. – 2015. – 1 січня. – [Електронний ресурс]. – Режим доступу: http://www.3republic.org.ua/docs/...

ПІСЛЯМОВА

Минуло п’ять років після видання посібника «Використання біометричних технологій правоохоронними органами у XXI столітті». Необхідно зазначити, що посібник відображав повний спектр застосування біометричних технологій у повсякденному житті на той час, а не тільки у діяльності силових структур світового співтовариства. За той період, що минув від часу написання посібника, біометрія зробила величезний крок у своєму розвитку.

Нині біометричні технології найактивніше впроваджуються в тих сферах людської діяльності, де на першому плані є питання безпеки. Це прикордонно-імміграційний контроль, національна оборона, робота органів внутрішніх справ, безпека аеропортів, інших великих транспортних об’єктів, діяльність спецслужб, урядових установ, освітянських і медичних закладів, безпечне функціонування фінансово-банківської галузі, захист конфіденційних відомостей, а також споживча електроніка та інше.

Автори другого видання вважають, що оновленому змісту викладеного матеріалу більш буде відповідати нова назва посібника «Біометричні технології в XXI столітті та їх використання правоохоронними органами».

Основні характерні риси біометричних проектів середини другого десятиліття XXI сторіччя такі:

1. У світі з’явилися біометричні бази даних (БД) із персональними відомостями на сотні мільйонів осіб, а у перспективі й на понад мільярд фігурантів. Це індійська програма з присвоєння громадянам країни ідентифікаційних номерів, котра відома за назвою Aadhaar і яка має охопити все населення Індії, офіційна чисельність якого становить на 1 квітня 2014 року 1,289 млрд осіб.

На початку 2014 року унікальні ідентифікаційні номери на основі сканування відбитків пальців і радужної оболонки ока вже отримали приблизно 600 млн індійців, що становить половину мешканців країни.

Зі слів представника Національного реєстраційного агентства Пакистану (National Database Registration Authority – NADRA), у цій країні на початок четвертого кварталу 2012 року 96% дорослих мешканців (кількість населення майже 185 млн осіб) пройшли біометричну ідентифікацію для отримання національних ідентифікаційних біометричних карт, придатних для комп’ютерної обробки (Computerized National Identity Card – CNIC).

Виникає питання, чому ці проекти посідають таке чільне місце. Це пов’язано з тим, що до проектів Aadhaar і NADRA не було досвіду експлуатації таких великих за кількістю фігурантів біометричних БД.

2. У Сполучених Штатах Америки створені перші у світі бази даних силових структур із біометричними відомостями приблизно 100 млн фігурантів, а надалі передбачається і більша чисельність облікованих осіб. Насамперед йдеться про такі автоматизовані системи біометричної ідентифікації:

– система Міністерства оборони США Defense Automated Biometric Identification System – (Dod ABIS);

– система Федерального бюро розслідування Next Generation Identification (NGI). База даних NGI, до якої вносять інформацію про злочинців і терористів, відповідно до технічного завдання, є технологічно сумісною з іншою окремо сформованою за програмою US-VISIT базою біометричних даних IDENT, яка зберігає оцифровані фотографії та дані про відбитки пальців іноземних громадян, які були здобувачами віз на право в'їзду до США;

– система Міністерства національної безпеки США (Department of Homeland Security /DHS/) US-VISIT. Формування бази даних IDENT за програмою US-VISIT було розпочато ще 2004 року і вона є однією з найбільших біометричних світових систем за кількістю даних щодо громадян різних країн;

– глобальна база біометричних даних Міжнародного інформаційного консорціуму (International Information Consortium) за назвою «Server in the Sky». Інформації про цю БД майже не має у відкритих джерелах, відомо що правоохоронні органи США, Великобританії, Канади, Австралії та Нової Зеландії мають внести у цю БД відомості щодо сотень мільйонів мешканців Землі. Нагадаємо, що США, Австралія, Британія, Канада та Нова Зеландія входять у Конференцію п'яти країн (Five Country Conference – FCC). Учасники FCC мають домовленість про те, що для зміцнення безпеки кордонів, боротьби з незаконною міграцією та іншими виявами злочинних дій вони обмінюються біометричними даними стосовно осіб, які становлять інтерес у кримінальному плані.

Щодо загального розвитку біометрії, то необхідно виокремити такі ключові сегменти сучасного світового біометричного ринку:

3. Суспільно-державний (паспортно-візові документи нового покоління, електронні системи прикордонного контролю, дистанційна електронна ідентифікація, «електронний уряд» тощо).

4. Комерційний (корпоративна та інформаційна безпека, фінансові транзакції та ін.).

У контексті еволюції цих двох секторів ринку проводяться інтенсивні дослідження щодо розвитку основних прикладних сфер застосування біометрії – ідентифікації й верифікації особи, особливо в системах відеоспостереження, контролю фізичного доступу та захисту інформації.

Необхідно виокремити таку тенденцію, що за останні п'ять років суттєво збільшилась кількість застосувань біометричних технологій у різних мобільних пристроях – смартфонах, планшетах тощо. Застосування останніх досягнень біометрії у гаджетах та інших мобільних пристроях дозволяє говорити про початок ери так званої мобільної комерції, тобто з метою підвищення безпеки здійснення електронних фінансових транзакцій та інших операцій у різних платіжних системах комерційних установ і організацій за допомогою мобільних пристроїв із вбудованими біометричними сканерами.

5. Нині цілком очевидною необхідністю є потреба точної та швидкої ідентифікації або аутентифікації індивідуумів у місцях масового скупчення людей і під час проведення контролю перепусток і перевірки документів. Насамперед ця проблема стосується безпеки транспортних систем – аеропортів, вокзалів, морських портів, метрополітену тощо. Звичайних паспортного і фейс-контролю (зорового контролю за допомогою обличчя) є недостатньо. Всі надії тепер пов'язані з використанням біометричних технологій, що дозволяють швидко здійснювати процедуру порівняльного контролю наданого документа на предмет його відповідності пред'явникові за великого напливу індивідуумів, які проходять через точку контролю.

Що стосується тенденцій застосування біометрії правоохоронними та іншими силовими структурами у другому десятиріччі XXI століття, то вони сконцентровані на виконанні таких двох основних завдань:

– створенні таких ідентифікаційних систем правоохоронних і спеціальних структур, для яких *можливість взаємообміну* з базами даних цих відомств будь-яких країн світу є невід'ємною складовою їхньої роботи;

– запровадженні *уніфікованих багатомодельних мультибіометричних технологій* ідентифікації індивідуумів для потреб різних спеціальних державних структур.

Що стосується головної рушійної сили розвитку світової біометрії, то впродовж усього нового тисячоліття нею була і залишається потреба ефективної протидії терористичним загрозам. Загалом збільшення потреб у застосуванні біометричних систем зумовлено прагненням мінімізування існуючих загроз глобальній безпеці, необхідністю ефективного протистояння атакам терористів, зниженню рівня злочинності, забезпеченню надійного захисту аеропортів та інших транспортних об'єктів. Свою частку в поширення технологій біометрики у світі мають внести необхідність подальшого розвитку систем біометричних паспортів і ID-карт, випуск біометричних водійських посвідчень, потреба впровадження суцільного автоматизованого прикордонного контролю за допомогою біометричних показників.

Для підвищення рівня безпеки, однією з складових якої є довіра до документів, які засвідчують особу, яка подорожує, світова спільнота зробила висновок, що необхідно використовувати паспортно-візові документи нового покоління (ПВДНП). Сучасні ПВДНП – це не данина черговій міжнародній моді, а один із заходів у боротьбі з незаконною міграцією, тероризмом і транснаціональною злочинністю.

На нинішньому етапі розвитку цивілізації завдання досягнення та створення відповідних рівнів безпеки і надійності вирішуються за допомогою різних багатофакторних і мультибіометричних технологій ідентифікації. Впродовж останніх п'яти років відбувалось інтенсивне впровадження біометрії у системи контролю фізичного доступу та захисту корпоративних інформаційних ресурсів.

Як відомо, системи контролю й управління доступом (СКУД) відіграють особливу роль у системах безпеки, оскільки контроль доступу є фундаментальною складовою будь-якої технології забезпечення безпеки. Нині можна констатувати, що біометрія за останні десять років перетворилась на невід'ємну частину і важливий чинник еволюції ринку СКУД.

Нові технології організації доступу і захисту інформації, що використовують біометричні технології, є не тільки найнадійнішими, але і найзручнішими для користувачів – зникла необхідність запам'ятовувати складні паролі та постійно носити з собою смарт-карти або апаратні ключі.

Ще однією з важливих тенденцій сучасного розвитку біометричної галузі є конвергенція різних біометричних технологій – тільки вона здатна забезпечити подальше зростання обсягу світового ринку біометрії та прибутковість інвестицій у створення різних біометричних систем.

За дослідженням компанії «MarketsandMarkets», яке було опубліковане у квітні 2014 року, обсяг біометричного глобального ринку 2020 року може сягти 23,54 млрд доларів. Цей висновок є найоптимістичнішим із усіх прогнозів, які були доступні авторам і щодо яких відомості наводились у посібнику.

Експерти «MarketsandMarkets» прогнозують, що біометричні технології і надалі будуть мати найбільше застосування в діяльності державних структур, а також у банківській і фінансовій сфері.

Біометрика й надалі буде дедалі більше застосовуватися у системах контролю за доступом, зокрема в різних освітянських і медичних закладах, біометричними все частіше будуть ставати ідентифікаційні карти, різні документи, системи голосування. Нова

істотна тенденція – широке застосування досягнень біометрії у споживчій електроніці та забезпеченні безпеки житла.

На думку аналітиків компанії «MarketsandMarkets», три «великі біометрики»: технології ідентифікації за папілярним малюнком пальців, обличчям та райдужкою – в найближчі 6 років і надалі лідируватимуть[1].

За останні декілька років технологія ідентифікації осіб за обличчям у загальних громадських місцях отримала виклик у вигляді закриття контурів лиця капюшонами і масками.

Американський центр ідентифікаційних технологій та досліджень (Center for Identification Technology Research /CITeR/) вивчає можливості ідентифікування індивідуумів на значній відстані за допомогою таких біометричних показників, як особливості ходи, етнічної приналежності та статі. Інформація щодо цих показників, яка попадає в зону спостереження відеокамер, доповнює інші біометричні відомості та допомагає звузити діапазон можливих ідентифікаційних збігань, що у підсумку пришвидшує ідентифікацію.

Європейський інститут «Idiap» у рамках проекту «Tabula Rasa» проводить дослідні роботи з метою підвищення якості ідентифікації осіб за їх обличчям у разі використання лицьових масок і капюшонів. «Idiap» розробляє спеціальне програмне забезпечення, яке передбачає можливість ідентифікації за кліпанням повік очей людини. Також досліджуються можливості проведення розпізнання за структурою шкіри різних частин обличчя.

У лютому 2014 року надійшло повідомлення про придбання компанією «HID Global» фірми «Lumidigm». Остання компанія відома тим, що має наробки в мультиспектральній технології формування зображень, яка дозволяє вирішувати пролеми традиційної біометричної ідентифікації, за яких точність зчитування зменшується у випадках несприятливих умов навколишнього середовища, тобто коли шкіра перебуває у поганому стані внаслідок уражень поверхні пальців або обличчя. Об'єднання компаній дозволяє використати можливості мультиспектральної технології формування зображень у процесах отримання облікових даних і аутентифікації, розпізнавання жестів та інших особливостей руху індивідуумів. З'являється можливість реалізації ідеї багатофакторної аутентифікації за допомогою єдиного інтегрованого пристрою[2].

2014 року альянс компаній FIDO (Fast IDentity Online) проводить масштабне тестування нового протоколу проведення платежів із біометричним підтвердженням здіснення транзакції. Технологія отримала назву Touch ID, а стороннім розробникам не буде повідомлятися код API (Application Programming Interface) для роботи з нею.

У протоколі, що просувається альянсом FIDO, біометрична аутентифікація виконується нетривіальним способом. Відбитки пальців взагалі ніде не зберігаються. Замість цього папілярний візерунок використовується для генерування криптографічного ключа безпосередньо під час сканування. Далі він об'єднується з іншим ключем, який є унікальним для кожного пристрою. На базі цього сполучення формується новий ключ, який бере участь у платіжній транзакції.

Публічну діяльність FIDO почало проводити лише з лютого 2013 року, але за цей час його членами стали понад сто великих компаній, зокрема таких, як «Microsoft»,

[1] Каким будет мировой биометрический рынок через шесть лет? // BIOMETRICS.RU. – 2014. – 30 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] Ещё одно слияние на биометрическом рынке // Mskit.ru. – 2014. – 14 февраля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

«Google», «Lenovo», «Infineon», «LG» і «Mastercard». Apple має намір просувати альтернативну технологію Touch ID своїми силами[1].

Згідно з прогнозом компанії «Goode Intelligence», три мільярда чотириста мільйонів людей будуть використовувати біометричні технології в своїх мобільних пристроях у 2018 році. Автори огляду вважають, що у 2014–2015 роках оснащення мобільних пристроїв біометричними сканерами стане стандартом для високотехнологічних планшетів і смартфонів, а з 2018 року ця тенденція має поширитися на весь ринок мобільних пристроїв[2].

Розвиток будь-яких біометричних систем неможливий без прогресу комп'ютерних технологій. Тому наведемо низку прогнозів авторитетних аналітиків із «Futuretimeline.net» на 2014 рік.

На думку експертів із «Futuretimeline.net», незабаром можуть з'явитися у продажу пристрої на мемристорах. На відміну від звичайних модулів комп'ютерної пам'яті, мемристори функціонують на атомному рівні, тому модулі пам'яті на мемристорах мають дуже велику швидкодію, яка набагато перевершує цей показник звичайних електронних аналогів. Цей факт означає, що суттєво має зрости швидкодія нових комп'ютерних пристроїв. А зважаючи на те, що терабайтні карти пам'яті вже стали реальністю, то можливості нових комп'ютерів набагато зростуть, що суттєво вплине на можливості біометричних систем майбутнього. Проведення ідентифікації суб'єктів контролю або пошуку практично буде блискавичною[3].

Але найбільші зміни у діяльності з забезпечення національної безпеки будь-яких держав світу мають внести використання останніх досягнень нанотехнологій. Більшість наукових експертів висловлюють думку, що нанотехнології будуть визначати основні риси подальшого майбутнього у XXI столітті.

Нанотехнології дозволять створити нові напівпровідники й оптику, унікальні конструкційні матеріали, а на їх базі мініатюрні датчики виявлення компонентів біологічної зброї та хімічних речовин, а головне комп'ютери, продуктивність яких на порядок або декілька порядків перевершать сучасні аналоги. Причому значно зменшаться розміри, вага, енергоспоживання та вартість пристроїв, приладів і обладнання, розроблених із використанням нанотехнологій.

Деякі російські вчені висловлюють думку, що використання нанотехнологій з часом можуть дати значно більший ефект, ніж усі космічні й атомні проекти СРСР, разом узяті[4].

Що стосується України, на думку авторів посібника, крім запровадження паспортних документів другого покоління, ще одними з головних чинників розвитку біометричного ринку в нашій країні слугують потреби в ефективних засобах забезпечення контролю за доступом, інформаційної безпеки й організації сучасного прикордонного контролю.

---

[1] Васильков Андрей. Будущее мобильных биометрических платежей: проблемы и решения / Андрей Васильков // Компьютерра-Онлайн. – 2014. – 7 апреля. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[2] На мобильных технологиях биометрические компании заработают восемь миллиардов долларов // BIOMETRICS.RU. – 2013. – 6 ноября. [Электронный ресурс]. – Режим доступа: http://www.biometrics.ru/news/...

[3] Василькевич К. Заглянем чуть дальше / К. Василькевич // Еженедельник-2000. – 2013. – Вып. № 3 (638). – 18–24 января. [Электронный ресурс]. – Режим доступа: http://2000.net.ua/2000/derzhava/realii/87273

[4] Юферев С. Нанотехнологии на службе военных / Сергей Юферев // Военное обозрение. – 2013. – 24 января. [Электронный ресурс]. – Режим доступа: http://topwar.ru/23354-nanotehnologii-na-sluzhbe-voennyh.html

Але найбільшим біометричним ринком у нашій державі в майбутньому має стати держзамовлення на виготовлення біометричних закордонних паспортів другого покоління та систем автоматизованого контролю перетину кордону за паспортно-візовими документами нового покоління (ПВДНП). У нашій країні гостро постало питання щодо створення у повному обсязі всієї структури державних інформаційних систем ПВДНП і подальшого їх розвитку.

Якщо ж говорити про біометричну сегментацію ринку, то найбільш популярними є і будуть у майбутньому біометричні системи, які використовують технології сканування за відбитками пальців.

Головними чинниками, що перешкоджають поширенню біометричних систем в Україні, є слабка поінформованість осіб, які ухвалюють рішення про використання біометричних технологій, а також порівняно висока ціна біометричних систем і пристроїв.

Автори посібника своє основне завдання вбачають в ознайомленні читачів із основними відомостями щодо прикладного використання досягнень сучасних біометричних технологій і насамперед у світлі потреб правоохоронних органів, спецслужб та інших силових структур. Зокрема використання біометричних можливостей вже існуючих баз даних Європолу, Інтерполу та прикордонних служб суміжних держав на практиці повинно сприяти зростанню розкриттю злочинів в Україні.

Автори також вважають, що зважаючи на той факт, що фінансово-банківська галузь в Україні є найпрогресивнішою з погляду впровадження інформаційних технологій, тому працівникам цієї сфери, а особливо менеджерам, що відповідають за впровадження інноваційних технологій та стан безпеки, буде корисно ознайомитися з матеріалами посібника, особливо з розділом «Застосування біометрії в банках та інших фінансових установах». У світі зараз відбувається бум запровадження біометричних технологій у фінансово-банківські установи.

СПИСОК СКОРОЧЕНЬ І АБРЕВІАТУР

Абревіатури і терміни латиницею

Aadhar – програма з присвоєння індійським громадянам ідентифікаційних номерів (у перекладі з хінді – «система»)

***ABIS* (Automated Biometric Identification System)** – автоматична система біометричної ідентифікації

***AFIS* (Automated Fingerprint Identification System)** – автоматична система ідентифікації за відбитками пальців

***AMT* (Active Management Technology)** – технологія активного управління в інформаційних технологіях

***ANSI* (American National Standards Institute)** – Національний інститут стандартизації США

API – інтерфейс прикладного програмування чи інтерфейс програмування додатків

***APRA-E* (Advanced Research Projects Agency – Energy)** – управління з перспективних досліджень у галузі енергетики (США)

***AVATAR* (Automated Virtual Agent for Truth Assessments in Real – Time)** – автоматизований віртуальний агент оцінки правди в режимі реального часу (інша назва цього робота-термінала – віртуальний прикордонник «Елвіс»)

***BAT* (Biometrics Automated Toolset)** – набір біометричних автоматичних вимірів

BBA Aviation – британська компанія, що займається забезпеченням безпеки авіаперельотів і обслуговуванням літаків та авіасистем

***BEAT* (Biometrics Evaluation and Testing)** – проект оцінки та тестування систем біометричної ідентифікації

***BCMS* (Border Control Management System)** – система управління та контролю за перетином кордону, яка використовується поліцією та спецслужбами Ізраїлю. Основним призначенням системи є швидке розпізнання та відстеження арабських імен

BioAPI – група з понад 90 організацій, метою якої є заохочення і сприяння впровадженню біометричних технологій шляхом розвитку галузевих інтерфейсів прикладного програмування (*API*)

***BFC* (Biometric Fusion Center)** – центр обробки біометричних даних Міністерства оборони США

***BOSS* – Biometric Optical Surveillance System (*BOSS*) at Stand-off Distance** – біометрична система для дистанційного оптичного спостереження

***BOSS*-U (Biometrics Operations and Support Services – Unrestricted)** – апаратно-програмні засоби проведення біометричної ідентифікації

***BSI* – (Biometric Services International)** – компанія

***BTF* (Biometrics Task Force)** – спеціальна комісія армії США з біометрії

***BYOD* (Bring Your Own Device)** – перекладається як «принести власний пристрій»

***CAGR* (Compound Annual Growth Rate)** – термін, який означає середньорічний темп зростання з урахуванням складного відсотка (складні відсотки /compound interest/ – спосіб обчислення відсотка приросту з урахуванням вже накопичених відсотків)

Call-центр – центр обслуговування вхідних та вихідних дзвінків

CAST – Центр сучасних комп'ютерних технологій

***CATSA* (Canadian Air Transport Security Authority)** – управління безпеки повітряного транспорту Канади

***CBEFF* (Common Biometric Exchange Formats Framework)** – стандарт для узагальнення системи форматів обміну біометричними даними

***CCD* (Charge-Coupled Device)** – прилад або матриця елементів із зарядним зв'язком

***CCTV* (Closed-Circuit Television)** – телевізійна система закритої трансляції

***CD* (Compact Disc**) – переносний оптичний диск для збереження цифрової інформації

CERN – європейський центр ядерних досліджень

***CHILD* (Children's Identification and Location Database)** – база даних з ідентифікації та визначення місцезнаходження зниклих або викрадених дітей

***CIRAM* (Common Integrated Risk Analysis Model)** – загальна інтегрована модель аналізу ризиків держав-членів ЄС, яка була розроблена у 2002 році

***CITeR* (Center for Identification Technology Research)** – центр досліджень у сфері технологій біометричної ідентифікації. Діє в американському Університеті Західної Вірджинії (*West Virginia University – WVU*)

***CJO* (Criminal Justice Organisation)** – система кримінального правосуддя

CMOS (Complementary metal-oxide-semiconductor) – матриця елементів потрібної розподільчої здатності

***CNIC* (Computerized National Identity Card)** – комп'ютерні національні ідентифікаційні карти

***CPS* (Central Picture System)** – єдина державна система цифрових фотозображень бельгійської поліції

***CSIA* (Cyber Security Industry Alliance)** – альянс компаній, які працюють на американському ринку інформаційної безпеки (*ІБ*)

***DARPA* (Defense Advanced Research Projects Agency)** – управління з перспективних досліджень та розробок Міністерства оборони США

***DHS* (Department of Homeland Security)** – Департамент з національної безпеки

***DIA* (Defense Intelligence Agency)** – військова розвідка США

***DIAC* (Department of Immigration and Citizenship)** – австралійське міністерство з справ імміграції та громадянства

DNK-samples – генетичні зразки

***DoD ABIS* (Department of Defense Automated Biometric Identification System)** – автоматична система біометричної ідентифікації Міністерства оборони США

***DPA* (Data Protection Act)** – Акт щодо захисту даних, прийнятий у Великобританії в 1998 році

***DVD* (Digital Versatile Disc)** – оптичний диск для збереження цифрової інформації, який має значно більший обсяг порівняно зі звичайними компакт-дисками

***DVR* (Digital Video Recorder)** – цифровий відеореєстратор, призначений для запису, зберігання та відтворення відеосигналів

***EAC* (Extended Access Control)** – розширений контроль доступу, що є складовою дотримання процедури підвищеного рівня безпеки

***EDPS* (European Data Protection Supervisor)** – європейський супервайзер із захисту даних

Egate – персональна електронна картка або інший електронний документ, який засвідчує особистість, для системи пришвидшеного проходження контролю

E-government – електронний уряд. Проект надання послуг державними органами за допомогою інформаційних технологій

***EHL* (Ecole Hôtelière de Lausanne)** – школа готельного бізнесу в Лозанні

***ESTA* (Electronic System for Travel Authorization)** – електронна система дозволів на поїздки у США

***ETSI* (European Telecommunications Standards Institute)** – європейський інститут телекомунікаційних стандартів

***EUBAM* (European Union Border Assistance Mission)** – місія Європейського союзу з прикордонної допомоги

***Eurodac* (євродак)** – загальноєвропейська система біометричної ідентифікації за відбитками пальців осіб, які подали заявки на отримання політичного притулку, та нелегальних іммігрантів (євродактилоскопія)

E-voting – електронне голосування

FaceIt – технологія розпізнавання облич, що автоматично виокремлюються в кадрах відеозйомки камер спостереження, з метою їх подальшого пошуку в базах даних різних категорій осіб

***FAR* (False Acceptence Rate)** – процентний поріг, який визначає ймовірність того, що одна людина може бути прийнята за іншу

***FBI* (ФБР)** – Федеральне бюро розслідувань США

***FCC* (Five Country Conference – *FCC*)** – Конференція п'яти країн

***FIDO* (Fast IDentity Online)** – альянс технологічних компаній, які займаються пошуком надійного стандарту аутентифікації

***FIND* (Facial Images National Database)** – національна база даних Великобританії за обличчям

***FISA* (Foreign Intelligence Surveillance Act)** – Закон США про контроль за діями іноземних розвідувальних служб

***FRR* (False Rejection Rate)** – імовірність помилкового нерозпізнавання людини біометричною системою

***FRVT* (Face Recognition Vendor Test)** – тестування постачальників систем для розпізнавання осіб за обличчям

***FSC* (Fingerprint Smart Card)** – біометрична картка з відбитками пальців

***FTE* (Failure to Enroll)** – вимірність біометричної характеристики. Визначає процентне відношення людей, які не змогли пройти реєстрацію (система не змогла сформувати їхні біометричні шаблони), до середнього часу розпізнавання (recognition time)

***GNIB* (Garda National Immigration Bureau)** – Національне імміграційне бюро Ірландії

***GPS* (Global Positioning System)** – супутникова система навігації

***GSM* (Global System for Mobile communications)** – глобальний цифровий стандарт для мобільного зв'язку

***HANIS* (Home Affairs National Identification System)** – Національна ідентифікаційна система МВС Південно-Африканської Республіки

***HIIDE* (Handheld Interagency Identity Detection Equipment)** – пересувний термінал мультибіометричної ідентифікації, який підтримує розпізнання за основними

біометричними ознаками: відбитками пальців, райдужною оболонкою ока й обличчям (головний недолік – наявність громіздкої камери)

***HIPAA* (Health Insurance Portability and Accountability Act)** – закон про забезпечення передачі та можливості обліку даних у системах медичного страхування США

Home Office – Міністерство внутрішніх справ Великобританії

***HSI* (Homeland Security Institute)** – Інститут національної безпеки США

***HSPD* (Homeland Security Presidential Directive)** – директива президента США з національної безпеки

***HUMABIO* (Human Monitoring and Authentication using Biodynamic Indicators and Behavioural Analysis)** – європейський проект «Моніторинг людини та ідентифікація її особистості із застосуванням біодинамічних індикаторів і поведінкового аналізу»

***IAFIS* (Integrated Automated Fingerprint Identification System)** – інтегрована автоматизована система ідентифікації за відбитками пальців

***IARPA* (Intelligence Advanced Research Projects Activity)** – організація, що займається дослідженнями, пов'язаними з державною безпекою США

IATA – Міжнародна асоціація повітряного транспорту

***IBG* (International Biometric Group)** – Міжнародна біометрична група

IBM – транснаціональна корпорація, один із найбільших у світі виробників обчислювальної техніки, периферійного обладнання та програмного забезпечення

IButton – клас електронних приладів із двопровідним протоколом обміну інформацією (має вигляд таблетки)

***ICA* (Immigration and Checkpoints Authority)** – імміграційне і прикордонне агентство Сінгапуру

***ICAO* (International Civil Aviation Organization)** – Міжнародна організація цивільної авіації (ІКАО)

***ICMPD* (International Centre for Migration Policy Development)** – Міжнародний центр розвитку міграційних процесів із штаб-квартирою у Відні

ID-Card – ідентифікаційна карта

IDENT – інформаційна система, що створена відповідно до функціонування системи керування імміграційним та прикордонним контролем США *US-VISIT*

***IDW* (Investigative Data Warehouse)** – спеціальна база даних ФБР для використання в антитерористичних розслідуваннях

***IEC* (International Electrotechnical Commission)** – Міжнародна електротехнічна комісія (*МЕК*)

***IED* (Improvised Explosive Device)** – саморобний вибуховий пристрій (*СВП*)

***INCITS* (InterNational Committee for Information Technology Standards)** – Міжнародний комітет зі стандартів у сфері інформаційних технологій, який представляє інтереси США в *ISO*

***INIS* (Irish Naturalisation and Immigration Service)** – служба натуралізації та імміграції Ірландії

***INSPASS* (INS Passenger Accelerated Service System)** – тип верифікаційних систем служби імміграції та натуралізації США, які встановлюються в аеропортах для полегшення процедури реєстрації пасажирів, які часто користуються авіапослугами

IP – означає «Інтернет-протокол». Термін IP-протокол вказує на стандартний набір правил і процедур, які дозволяють обмінюватися даними через мережу з пакетною комутацією

***IPS* (Identity and Passport Service)** – ідентифікаційна і паспортна служба Великобританії

***IRIS* (Iris Recognition Immigration System)** – автоматична система біометричної ідентифікації за райдужною оболонкою ока Великобританії

***ISO /ICO/* – (International Organization for Standardization)** – Міжнародна організація зі стандартизації

***IT* (Information Technology)** – інформаційні технології; в низці випадків трапляється вживання у значенні інформаційно-телекомунікаційних технологій

***JTC № 1* (ISO / IEC Joint Technical Committee 1, ISO / IEC JTC 1)** – об'єднаний технічний комітет № *1 ICO / МЕК* – підрозділ Міжнародної організації із стандартизації (англ. *International Organization for Standardization, ISO*) і Міжнародної ефектротехнічної комісії (*МЕК*, англ. *International Electrotechnical Commission, IEC*), який займається всіма питаннями, пов'язаними зі стандартами в галузі інформаційних технологій

***JTTF* (Joint Terrorism Task Force)** – об'єднані антитерористичні спецпідрозділи США

***KBA* (Knowledge-Based Authentication**) – технологія «авторизації за знанням» для захисту персональних даних

***LSA* (Laser Surface Authentication)** – система лазерної ідентифікації поверхні

***MEMS* (MicroElectroMechanical Systems)** – технології, прилади та методи, що об'єднують мікроелектромеханічні компоненти

***MNIC* (Multipurpose National Identity Card)** – багатоцільова національна ідентифікаційна картка (Індія)

***MRTD* (Machine Readable Travel Document)** – машинозчитуваний проїзний документ

***MPS* (Uk's Metropolitan Police Service)** – підрозділ британської поліції, що обслуговує метрополітени

***NAB* (National Australia Bank)** – Національний банк Австралії

***NAC* (Network Access Control)** – контроль доступу до IT-мережі

***NADRA* (National Database Registration Authority)** – національне реєстраційне агентство Пакистану

***NBIS* (National Biometric Identity Store)** – національне сховище біометричних ідентифікаційних даних Великобританії

***NCTC* (National Counterterrorism Center)** – Національний антитерористичний центр США

***NFC* (Near Field Communication)** – технологія безпровідного високочастотного зв'язку малого радіусу дії

***NG-ABIS* (Next Generation Automated Biometric Identification System)** – автоматична система біометричної ідентифікації нового покоління

***NGI* (Next Generation Identification)** – ідентифікація нового покоління

***NIST* (National Institute of Standards and Technology)** – Національний інститут стандартів і технологій США

***NIR* (National Identity Register)** – Національний ідентифікаційний реєстр

***Non-AFIS* (non-automated fingerprint identification systems)** – неавтоматизовані системи ідентифікації

***NPIA* (National Policing Improvement Agency)** – Національне агентство з модернізації поліції (Великобританія)

***NPL* (National Physical Laboratory)** – національна фізична лабораторія

***NPR* (National Population Register)** – Національний регістр населення Індії

***NSA* (National Security Agency)** – агентство національної безпеки (АНБ)

OASIS **(Organization for the Advancement of Structured Information Standards)** – глобальний консорціум, який управляє розробкою, конвергенцією і прийняттям промислових стандартів електронної комерції в рамках міжнародного інформаційного співтовариства; в ЗМІ фігурує також як організація розвитку стандартів структурованої інформації

On-line – режим роботи в реальному часі

OTA **(mobile over the air)** – мережа стільникового зв'язку

OTP **(one time password)** – генератор одноразових паролів

PAA **(Protect America Act)** – Акт про захист Америки

PAL – формат передачі телевізійного сигналу, означає зміну фази. *PAL* є стандартним форматом мовлення в Європі, Австралії та деяких частинах Азії

PCR **(Polymerase Chain Reaction)** – полімеразна ланцюгова реакція (*ПЛР*)

PHI **(Project Hostile Intent)** – проект Міністерства національної безпеки США з виявлення «можливих ворожих намірів»

PIN **(Personal Identification Number)** – унікальний персональний ідентифікаційний номер

PIV-cards **(Personal Identity Verification cards)** – персональні біометричні ідентифікаційні картки, призначені для підтвердження особи їх власників

PKI **(Public Key Infrastructure)** – інфраструктура відкритих ключів

RAIC **(Restricted Area Identification Card system)** – система карткового доступу в режимні зони

RAND **(Research ANd Development)** – стратегічний дослідницький центр США. Некомерційна організація, яка проводить досліження в галузі національної безпеки

RBI **(Reserve Bank of India)** – резервний банк Індії

RFC **(Request for Comments)** – це пронумерований документ, який містить технічні специфікації і стандарти (в перекладі з англійської «Запит коментарів»)

RFID **(Radio Frequency IDentification)** – технологія радіочастотної ідентифікації

RIOT **(Rapid Information Overlay Technology)** – масштабна аналітична суперсистема для збору даних у соціальних мережах

SAN **(Storage Area Network)** – мережа зберігання даних

SANS **(похідна від SysAdmin, Audit, Networking, and Security)** – інститут комп'ютерної безпеки в США

SC37 **(Subcommittee 37)** – підкомітет об'єднаного технічного комітету з інформаційних технологій *JTC 1* Міжнародної організації стандартизації *ISO* (International Organization for Standardization) і Міжнародної електротехнічної комісії (International Electrotechnical Commission /*IEC*/)

SDK-продукти **(Software Development Kit)** – набір засобів для розробки, який дозволяє фахівцям із програмного забезпечення створювати прикладні програми для певної технології або платформи

SHIELDTM – дуже тонка плівка з нанесеними багаторівневими голографічними захисними елементами

SIGNOBJ – об'єкт електронного підпису разом із додатковими персональними даними

SIM-картка – ідентифікаційний модуль абонента, що використовується у мобільному зв'язку

SITA – швейцарська транснаціональна інформаційна організація, яка надає телекомунікаційні та IT-послуги в авіаційній галузі

SIS **(Schengen Information System)** – шенгенська інформаційна система

***SOX* (Sarbanes-Oxley Act, Sarbanes–Oxley, Sarbox або SOX)** – закон Сарбейнза-Окслі 2002 року, який визначає вимоги до захисту та зберігання даних у фінансовому секторі США

***SRT* (Secure Registered Traveler)** – процедура безпечної реєстрації пасажирів у аеропортах

***SSS* (Social Security System)** – система соціального забезпечення Філіппін

***TAG/MRTD* (Technical Advisory Group on Machine Readable Travel + Documents)** – технічна консультативна група щодо машинозчитуваних проїзних документів

***TAN* (Transaction Authentication Number)** – ідентифікаційний код транзакції

***TEDAC* (Terrorist Explosive Device Analytical Centre)** – центр аналізу терористичних вибухових пристроїв *TNS* – маркетингова інформаційна група США

Template – шаблон; числовий образ відбитка пальця

***TIA* (Terrorism Information Awareness)** – проект «Знання інформації про тероризм»

***TIDE* (Terrorist Identities Datamart Environment)** – база даних уряду США на відомих або підозрюваних у міжнародному тероризмі осіб

Touch-memor – контактна пам'ять (від англ. *touch memory* іноді трапляється англ. *contact memory* або англ. *iButton*) – клас електронних пристроїв, які поміщаються в стандартний металевий корпус (зазвичай має вигляд «таблетки»)

***Touchpad-e* – тачпа́д** – се́нсорна пане́ль (вказівний пристрій для введення), яка зазвичай застосовується в ноутбуках (використовується для керування курсором через переміщення пальця поверхнею пристрою)

***TSA* (Transportation Security Administration)** – управління транспортної безпеки США

***TSC* (Terrorist Screening Center)** – центр виявлення терористів при ФБР

***TSE* (Tribunal Superior Eleitoral)** – вищий виборчий трибунал Бразилії

***TWIC* (Transportation Worker Identification Credential)** – державний проект берегової охорони США, який регламентує допуск у порти, літаки або кораблі тільки за наявності біометричної ідентифікаційної картки працівника на транспорті

***UCN* (Universal Control Number)** – універсальний контрольний номер *FBI*

***UIDAI* (UID Authority of India)** – Управління з присвоєння громадянам унікальних ідентифікаційних номерів Індії

***UKBA* (UK Border Agency)** – прикордонна служба Великобританії

UN – Організація Об'єднаних Націй

***USB* (Universal Serial Bus)** – послідовний інтерфейс передачі даних для середньота низькошвидкісних периферійних пристроїв

***USMEPCOM* (U.S. Military Entrance Processing Command)** – підрозділ Міністерства оборони США з обліку призовників до збройних сил країни

USPASS – система митного і прикордонного агентства США (використовує ідентифікацію осіб за геометрією кисті руки для пришвидшення прикордонного контролю)

US-VISIT – візова програма США з метою збору біометричної та біографічної інформації іноземців під час їх в'їзду та виїзду

Vennlig – міжнародна база даних Інтерполу для обміну інформацією про терористів

VIP-клієнти – клієнти-високопосадовці з фінансового, політичного або соціокультурного погляду

***VIS* (Visa Information System)** – інформаційна система обліку іноземців, яким було видано візи до держав-членів Шенгенської зони

***VPN* (Virtual Private Network)** – віртуальна приватна мережа

***VRT* (Vein Recognition Technology)** – аутентифікація за венозним малюнком руки

***WVU* (West Virginia University)** – університет Західної Вірджинії

***WPAN* (Wireless Personal Area Network)** – технологія «бездротової персональної мережі»

Абревіатури і терміни кирилицею

АДІС – автоматизована дактилоскопічна інформаційна система

АЕС – атомна електостанція

АІС – автоматизована інформаційна система

АН – Академія наук

АНБ – Агентство національної безпеки (*NSA – National Security Agency*)

АС – автоматизована система

АСПК – автоматизована система прикордонного контролю

АТ – акціонерне товариство

АТР – Азійсько-Тихоокеанський регіон

БД – база даних

БНП – Британська національна партія

ВЕФ – Всесвітній економічний форум

ВІНІТІ – Всеросійський інститут наукової і технічної інформації

ВІС – організація «Всесвітнє інформаційне суспільство»

ВІТ – відділ інформаційних технологій ряду УМВСУ в регіонах

ВНДІ – Всеросійський науково-дослідний інститут

ВНДІСЕ – Всеросійський (або Всесоюзний) науково-дослідний інститут судових експертиз

ВПК – військово-промисловий комплекс

ВПЗ – вільне програмне забезпечення

ВПС – військово-повітряні сили

ВТО – Всесвітня торгова організація

ГІАЦ – Головний інформаційно-аналітичний центр МВС Росії

ГУВС – Головне управління внутрішніх справ

ГУМ – Головне управління міліції

ДАРПА (DARPA) – Управління з перспективних досліджень та розробок Міністерства оборони США

ДАС – державна автоматизована система

ДДГІРФО – Державний департамент у справах громадянства, імміграції і реєстрації фізичних осіб

ДІС – державна інформаційна система України

ДІТ – Департамент інформаційних технологій МВС України

ДМС – Державна міграційна служба

ДНБ – Департамент національної безпеки

ДНДІ – Державний науково-дослідний інститут

ДНДЦ – Державний науково-дослідний центр

ДНК – дезоксирибонуклеїнова кислота – високополімерне природне з'єднання, що міститься в ядрах клітин живих організмів та є носієм генетичної інформації

ДПАУ – Державна податкова адміністрація України

ДПС – державна прикордонна служба України

ДПС міліції – дорожньо-патрульна служба міліції

ДСТСЗІ – Департамент спеціальних телекомунікаційних систем та захисту інформації СБ України

ДСТУ – державний стандарт України

ЕЕГ – електроенцефалографія

ЕКГ – електрокардіограма

ЕОМ – електронно-обчислювальна машина

ЕЦП – електронно-цифровий підпис

Європол – європейське поліцейське управління із штаб-квартирою у м. Гаага (Нідерланди)

ЄДАПС – єдина державна автоматизована паспортна система України

ЄІТКС – єдина інформаційно-телекомунікаційна система ОВС

ЄК – Європейська комісія

ЄС – Європейський Союз

ЗАТ – закрите акціонерне товариство

ЗКЗІ – засоби криптографічного захисту інформації

ЗМІ – засоби масової інформації

ІБ – інформаційна безпека

ІБ – інформаційна база (друге значення)

ІБД – інтегрована база даних

***ІКАО – ICAO* (International Civil Aviation Organization)** – Міжнародна організація цивільної авіації

ІКТ – інформаційно-комп'ютерні технології, ще одне значення – інформаційно-комунікаційні технології

Інтерпол – Міжнародна організація кримінальної поліції

ІПІ – Інститут проблем інформатики

ІПС – інформаційно-пошукова система

ІСО (ISO) – Міжнародна організація стандартизації

ІЦ – інформаційний центр

КМ (Кабмін) – Кабінет Міністрів

КМУ – Кабінет Міністрів України

КПП – контрольно-пропускний пункт

ЛАД – Ліга арабських держав

ЛСД – логічна структура даних

ЛьвДУВС – Львівський державний університет внутрішніх справ

МВБ – Міністерство внутрішньої безпеки США

МВС – Міністерство внутрішніх справ

МЗПД (MRTD) – машинозчитуваний проїзний документ

МЗС – Міністерство закордонних справ

МІБ – Міждержавний інформаційний банк

МНБ – Міністерство національної безпеки

МНС – Міністерство надзвичайних ситуацій

МО – Міністерство оборони

МОМ – Міжнародна організація з міграції

МПА – Міжпарламентська асамблея

МЮ (Мін'юст) – Міністерство юстиції

НАВСУ – Національна академія внутрішніх справ України
НАН – Національна академія наук
НБУ – Національний банк України
НВО – науково-виробниче об'єднання
НДІ – науково-дослідний інститут
НДІК – науково-дослідний інститут криміналістики
НДІСЕ – науково-дослідний інститут судових експертиз
НКВС – народний комісаріат внутрішніх справ
НКЮ – народний комісаріат юстиції
НПІ – Національна програма інформатизації
НСМЕП – Національна система масових електронних платежів
НСД – несанкціонований доступ
НТВ – науково-технічне відділення
ОАЕ – Об'єднані Арабські Емірати
ОБСЄ – Організація з безпеки і співробітництва в Європі
ОВС – органи внутрішніх справ
ОДПУ – Об'єднане державне політичне управління
ООН (UN) – Організація Об'єднаних Націй
ОС – операційна система
ОССП – операційна система спеціального призначення
ПАР – Південно-Африканська Республіка
ПВДНП – паспортно-візові документи нового покоління
ПЗ – програмне забезпечення
ПК – персональний комп'ютер
Прайвесі – дотримання вимог конфіденційності персональних даних
ПТК – програмно-технічний комплекс
РІФ – реєстр інформаційного фонду
РРФСР – Російська Радянська Федеративна Соціалістична Республіка
РСЗ – Регіональна співдружність зв'язку
РФ – Російська Федерація
РФЦСЕ – Російський федеральний центр судових експертиз
СБУ – Служба безпеки України
СКУД – система контролю і керування доступом
СМС /SMS/ **(Short Message Service)** – послуга обміну (передачі і прийому) короткими текстовими повідомленнями в телекомунікаційних мережах
СНД – Співдружність Незалежних Держав
СОРМ – система оперативно-розшукових заходів
СОРЧ – системи обліку робочого часу
СОТ – системи охоронного телебачення
СПІ – системи передачі інформації
СРСР – Союз Радянських Соціалістичних Республік
СУБД – система управління базами даних
США – Сполучені Штати Америки
ТВН – термовакуумне напилення
ТВЛ – телевізійні лінії, що формують зображення
ТЗ – технічне завдання
ТІО – тотальна інформаційна обізнаність
ТОВ – товариство з обмеженою відповідальністю

УВКБ ООН – Управління Верховного комісара Організації Об'єднаних Націй у справах біженців

УВС – управління внутрішніх справ

УВСТ – управління внутрішніх справ на транспорті

УІТ – управління інформаційних технологій ряду УМВСУ в регіонах

УРСР – Українська Радянська Соціалістична Республіка

ФБР (FBI) – Федеральне бюро розслідувань США

ФМС – Федеральна міграційна служба Росії

ФРН – Федеральна Республіка Німеччина

Фронтекс – об'єднана європейська прикордонна охорона

ФСБ – Федеральна служба безпеки Росії

ФСО – Федеральна служба охорони Росії

ФСТ – Федеральна служба по тарифам Росії

ФСТЕК – Федеральна служба з технічного й експортного контролю Росії

ХДС – Християнсько-демократичний союз

ЦБ – центральний банк

ЦВК – Центральна виборча комісія

ЦМТ – центр мовних технологій

ЦНДІСЕ – Центральний науково-дослідний інститут судових експертиз

ЦСД – центральне сховище даних

ЧК – (рос. – чрезвычайная комиссия) надзвичайна комісія

Шабак – відомство внутрішньої безпеки Ізраїлю

ЮНІСКАН – асоціація автоматичної ідентифікації

ГЛОСАРІЙ*

Атака – спроба зловмисника обійти систему захисту інформаційної технології та незаконно скористатися її ресурсами.

Атака шляхом підбору – атака на аутентифікаційну систему шляхом випадкового або спрямованого підбору її секретних компонент (паролі, ключі, біометричні паролі, біометричні ключі).

Аудит біометричної інформації – реєстрація, зберігання й обробка результатів біометричної аутентифікації за достатньо тривалий інтервал часу для виявлення спроб атак на біометричні фрагменти системи захисту.

Аутентифікація – процес доказу і перевірки достовірності заявленого елементом інформаційної технології свого імені в рамках заздалегідь визначеного протоколу.

Біометрія – наукова дисципліна, що вивчає способи вимірювання різних параметрів індивідуума для встановлення подібності/відмінності між людьми та виокремлення однієї конкретної фізичної особи з безлічі інших людей.

Біометрична аутентифікація – процес доказу та перевірки достовірності заявленого користувачем свого імені через пред'явлення ним власного біометричного образу шляхом проведення перетворень цього образу відповідно до заздалегідь визначеного протоколу аутентифікації.

Біометрична ідентифікація – процес створення моделі, що описує з заданими значеннями помилок першого і другого роду сукупність біометричних образів конкретної особистості в рамках заданого способу спостереження біометричних образів і в рамках заданого способу вимірювання контрольованих біометричних параметрів.

Біометрична система – технічна система, яка побудована на вимірюванні біометричних параметрів особистості, що здатна за спеціальними алгоритмами розпізнавати конкретний індивідуум.

Біометричний пароль – пароль або парольна фраза, яка відтворюється особою рукописним способом, за допомогою голосу або через використання свого клавіатурного почерку.

Біометричний параметр – параметр особистості, який легко піддається вимірюванню, має достатню стабільність на прогнозований період можливих у майбутньому вимірювань, та який істотно відрізняється від аналогічних парамет-

* Глоссарий терминов // Biometrics.ru. [Электронный ресурс]. – Режим доступа: http://biometrics.ru/document.asp?group_id=10&url=Глоссарий&sSID=3.6.

рів безлічі інших людей. Біометричні параметри отримують прямим вимірюванням характерних елементів біометричного образу або шляхом математичних перетворень цього образу.

Біометричний еталон – дані про найстабільнішу частину контрольованих біометричних параметрів і їх допустимих відхилень, що зберігаються в біометричній системі для подальшого порівняння з ними біометричних образів, що знов пред'являються. Вид еталона визначається за прийнятим у системі основним існуючим (так званим «вирішальним») правилом.

Біометричний образ – образ особистості, що безпосередньо спостерігається системою без використання будь-яких операцій для його попередьої обробки та масштабування.

Біометричний ключ – ключ, що використовується для криптографічних перетворень та одержується зі стабільної частини вимірюваних біометричних параметрів особистості.

Біометричний криптографічний процесор – універсальна програма, що має гарантовану стійкість до злому і яка здатна коректно виконувати під керуванням тільки свого користувача різноманітні криптографічні операції, зокрема:

– безліч загальноприйнятих операцій із віддаленої криптографічної антентифікації;

– адаптуватися до конфігурації використовуваного обчислювального середовища;

– виправляти деякі помилки користувача;

– надійно зберігати його секрети;

– з великою ймовірністю розпізнавати різні варіанти біометричних параметрів свого конкретного користувача.

Вагові коефіцієнти нейрона (нейровага) – вагові коефіцієнти, що вимірюють вхідні дані нейрона, підбираються або обчислюються під час налаштування нейрона.

Віртуальні монети – монети-файли, в існуванні та достовірності яких можна переконатися достовірним способом, проте отримати їх у володіння можна тільки за допомогою строго визначених процедур, наприклад, після суворо регламентованої послідовності дій їх реального власника.

Взірець (приклад) – реалізація одного з можливих варіантів біометричного образу або так званого вектора контрольованих біометричних параметрів, який є тотожний цьому образу.

Вчитель – користувач біометричної системи, що пред'являє їй взірці-приклади різних варіантів своїх біометричних образів, наприклад, у вигляді багатократного рукописного запису парольного слова.

Дефект нейронної мережі (дефект учня) – потенційне некомпенсоване зниження якості роботи нейронної мережі, обумовлене такими чинниками, як нічим не виправдана відсутність або наявність уведення додаткових нелінійних елементів, нічим не виправдане зменшення кількості нашарувань мережі, кількості нейронів у одному нашаруванні мережі, кількості зв'язків одного нейрона з іншими.

Дефекти вчителя біометричної системи – нездатність користувачів під час «навчання» біометричної системи пред'явити приклади можливих підробок образів, які належать до множини образів «Всі чужі», небажання користувачів пред'являти системі значну кількість взірців своїх біометричних образів.

Дефекти підручника – наявність у векторі контрольованих біометричних параметрів конкретної особистості параметрів із сильною кореляцією, присутність невдалих взірців біометричних образів у навчальній вибірці, що призводить до значних помилок під час обчислення статистичних показників.

Дефекти методики навчання – поступове забування образів первинних взірців, що використовувались для «навчання» системи, або витіснення їх з пам'яті останніми невдалими зразками, які використовувались для навчальної процедури, технічні обмеження можливостей відстеження за впливами малих змін значень вагових коефіцієнтів нейронів на кінцевий результат «навчання» системи.

Динамічний біометричний образ – це такий взірець, який користувач, що вибрав його для проходження процедури аутентифікації, може змінювати за своїм бажанням, наприклад, змінивши відтворюване рукописне слово-пароль.

Динамічний біометричний параметр – отримується з динамічного біометричного образу, який користувач, що вибрав його для проходження процедури аутентифікації, може змінювати за власним бажанням, наприклад, змінивши відтворюване рукописне слово-пароль.

Електронні гроші – електронні аналоги грошей, чекових книжок, цінних паперів, які випущені в обіг банком та забезпечені активами банку емітента.

Електронні монети – файли, які створені банком і які мають вартість, що є кратною прийнятій одиниці оплати (аналог звичайних монет). Достовірність електронних монет загальнодоступна для перевірки, наприклад, шляхом перевірки електронного цифрового підпису банку, що їх випустив. Процедура оплати проводиться шляхом пересилки файла електронної монети від покупця до продавця. Покупець не має змоги повторно скористатися вже використаним ним файлом електронної монети.

Електронний цифровий підпис (ЕЦП) – дані, що приписуються до інформації, або криптографічне перетворення інформації, яке дозволяє одержувачеві інформації переконатися в її цілісності та достовірності джерела інформації, а відправникові – захистити інформацію від можливої підробки, наприклад, одержувачем інформації.

Зловмисник – стороння особа (нелегальний користувач), що намагається видати свої біометричні параметри за чужі, або намагається обійти фрагменти біометричного захисту шляхом модифікації програмного забезпечення, або підробляючи графічні або звукові файли біометричних образів легального користувача.

Ідентифікація – процес синтезу моделі досліджуваного об'єкта, яка здатна описувати його з заданою точністю за умови існування низки технічних обмежень.

Ідентифікація у вузькому розумінні – деталізація (уточнення) значень параметрів заздалегідь заданої моделі з наперед відомою структурою, з точно заданим числом параметрів, які обліковуються, на вибраному класі сигналів і за однозначно визначених технічних обмежень.

Ідентифікація у широкому розумінні – процес синтезу моделі досліджуваного об'єкта, яка здатна описувати його з заданою точністю, причому процес охоплює:

– вибір математичного опису моделі;

– вибір структури моделі;

– вибір числа параметрів, що враховуються в моделі;

– вибір тестових дій;

– визначення існуючих технічних обмежень.

Ключ – послідовність символів, яка генерується, зберігається, використовується та знищується відповідно до криптографічних вимог і застосовується як керуюча інформація в криптографічних перетвореннях таких, як шифрування або дешифрування, обчислення криптографічного чека цілісності, генерації та перевірки електронного цифрового підпису.

Коефіцієнти лінійного прогнозу – коефіцієнти лінійного цифрового фільтра (рекурсивного або нерекурсивного), який спеціально налаштований (синтезований) для апроксимації звукових хвиль при збудженні цифрового фільтра вхідними імпульсами, що надходять із частотою, яка дорівнює періоду основного тону.

Конфіденційність – властивість інформації, яка потребує під час її передачі, обробки і зберігання приховувати її смисловий зміст, і яка робить доступним зміст інформації тільки авторизованим користувачам, апаратним об'єктам і процесам.

Користувач – легальний користувач біометричної системи або будь-якої інформаційної технології.

Криптографія – наукова дисципліна, яка вивчає принципи, засоби та методи перетворення інформації для утаємничення її інформаційного змісту, запобігання її несанкціонованої зміни та неавторизованого використання.

Криптографічний автомат користувача – програма автоматичного шифрування або дешифрування файлів даних тільки конкретного банку, де у користувача знаходиться його особистий рахунок. Криптографічний автомат користувача створюється конкретним банком і налаштовується на біометричні параметри тільки конкретного користувача, що дає змогу користувачеві спростити роботу з банком і відмовитися від потенційно небезпечної операції зберігання особистих ключів на звичайних носіях інформації. Поняття «криптографічний автомат користувача» – це окремий випадок значно ширшого поняття – «біометричного криптографічного процесора».

Методика навчання – визначена послідовність пред'явлення взірців (образів) системі або мережі, спосіб підбору або обчислення вагових коефіцієнтів і параметрів нелінійних перетворень елементів системи або мережі, встановлена послідовність навчання різних фрагментів системи або мережі.

Міра наближеності до біометричного еталона – відстань від центру біометричного еталона, що утворюється, наприклад, при математичному очікуванні значень контрольованих біометричних параметрів зареєстрованого легального користувача. Бажана, але не обов'язкова, позитивна визначеність міри для

більшості прикладів взірців, які мають допустимі відхилення (зона допустимого відхилення) від біометричного еталона.

Множина «Всі чужі» – чисельність біометричних образів або значень біометричних параметрів, що утворюються великою кількістю зловмисників, кожен з яких намагається обійти біометричний фрагмент аутентифікації шляхом відтворення біометричного образу легального користувача.

Множина «Свій» – чисельність біометричних образів або значень біометричних параметрів, що пред'являються (надаються) раніше зареєстрованим легальним користувачем.

Множина «Чужий» – чисельність біометричних образів або значень біометричних параметрів, що пред'являються (надаються) зловмисником, який намагається обійти біометричний фрагмент аутентифікації шляхом відтворення біометричного образу легального користувача.

Муляж – імітація статичного біометричного образу, наприклад, виготовлення дубліката папілярного узору пальця.

Навчання – процес пред'явлення набору взірців біометричних образів або біометричних параметрів, який дає змогу створити в тій або іншій формі біометричний еталон особистості, що дозволяє з заданою похибкою описати стабільну частину взірців біометричних образів або біометричних параметрів та їх допустимі варіації.

Навчальна вибірка – декілька прикладів взірців біометричних образів, які належать одній особистості та не піддавалися будь-якій попередній обробці, сортуванню, відбору.

Невдалий приклад взірця – біометричний образ користувача, ймовірність появи якого серед взірців навчальної поточної вибірки дуже мала. Синонім у статистичному аналізі даних – «груба помилка».

Нейрон – елемент керуючого (вирішуючого) алгоритму (правила) або мережі, який ухвалює кінцеве рішення та здатний оцінювати межу допустимого відхилення між контрольним фрагментом біометричного еталона і пред'явленим для зрівняння аналогічним фрагментом вектора біометричних параметрів.

Оцінка якості навчання – рівні значення ймовірності появи помилок першого і другого роду, які виникають під час ухвалення системою рішення, а також певні значення стандарту нормального закону, що відповідають значенням однакових імовірностей появи помилок першого і другого роду.

Пароль – випадкова послідовність символів, яка запам'ятовується користувачем, що становить його таємницю та використовується ним у процесі аутентифікації.

Парольна фраза – фраза, яка запам'ятовується користувачем та складається з декількох випадкових слів, що узгоджені між собою відповідно до правил мови користувача.

Період основного тону – період першої форманти звукового фрагмента, який є еквівалентом інтервалу часу між вхідними дельта-імпульсами, що збуджують лінійний сповіщувач.

Персептрон – окремий випадок реалізації керуючого алгоритму (нейрона) у варіанті вагового суматора з можливістю регулювання вхідної ваги і постійного

зміщення, який також має вихідну монотонну нелінійність із двома пологими ділянками насичення.

Підручник – група, що складається з декількох векторів виміряних біометричних параметрів, які приведені до єдиного масштабу та отримані з взірців (прикладів) біометричних образів однієї конкретної особистості.

Підсвідомі рухи – добре відпрацьовані особистістю швидкоплинні рухи, що виконуються індивідуумом автоматично на підсвідомому рівні без попередньо усвідомленого аналізу виконуваних рухів тіла.

Помилка першого роду – помилка біометричної системи, що прийняла зареєстрованого легального користувача за зловмисника.

Помилка другого роду – помилка біометричної системи, що прийняла зловмисника, який підробив чужий біометричний образ, за легального користувача.

Протокол аутентифікації – заздалегідь визначена послідовність дій процедури аутентифікації, де співучасниками є користувачі, програмно-апаратні процеси або технічні пристрої.

Статичний біометричний образ – біометричний образ особистості, котрий надається їй від народження і який вона не може змінити за своїм бажанням, наприклад, – папілярний узор пальців людини.

Статичний біометричний параметр – параметр, що отримується як наслідок обробки статичного біометричного образу.

Точка рівноймовірних помилок – особлива точка налаштування порогів спрацювання системи або пристрою, в якій імовірність настання помилок першого і другого роду збігаються.

Учень – нейронна мережа біометричної системи в сукупності з пристроями автоматичного навчання, яка перебуває в режимі навчання або в режимі тестування якості навчання.

Фонема – звуковий аналог відповідної букви алфавіту.

Форманта – амплітуда однієї з кратних гармонійних складових голосового звукового фрагмента. Форманти мають номери, і їх частоти кратні частоті першої форманти або частоті імпульсів основного голосового тону.

Функція збудження нейрона – нелінійна монотонна функція, яка має дві яскраво виражених ділянки насичення, і яка знімається (підключається) до виходу лінійної частини нейрона, наприклад, суматора.

Хеш-функція (хешування) даних – математичне перетворення даних, що дозволяє провести стискання інформації до меншого об’єму. Розрізняють ключове і безключове хешування. Обчислення хеш-функції є односпрямованим криптографічним перетворенням без колізій, що не дозволяє відновлювати початкові дані.

Цілісність – властивість інформації, що дозволяє зберігати незмінність інформації або встановити факт її спотворення.

НАВЧАЛЬНЕ ВИДАННЯ

Захаров Василь Павлович,
Рудешко Вадим Іванович

БІОМЕТРИЧНІ ТЕХНОЛОГІЇ В XXI СТОЛІТТІ ТА ЇХ ВИКОРИСТАННЯ ПРАВООХОРОННИМИ ОРГАНАМИ

Посібник

Редагування *Г. А. Романова*

Макетування *Н. М. Лесь*

Друк *Н. Я. Ганущак*

Здано до набору 26.06.2014 р. Підписано до друку 23.01.2015 р.
Формат 60×84/8. Папір офсетний. Умовн. друк. арк. 57,2.
Тираж 100 прим. Зам. № 81-14.

Львівський державний університет внутрішніх справ
Україна, 79007, м. Львів, вул. Городоцька, 26.

Свідоцтво про внесення суб'єкта видавничої справи до державного реєстру
видавців, виготівників і розповсюджувачів видавничої продукції.
ДК № 2541 від 26 червня 2006 р.