

*Терещенко Віктор Федорович,*

старший викладач кафедри оперативно-розшукової діяльності Національної академії внутрішніх справ

## **ЗАСТОСУВАННЯ БІОМЕТРИЧНИХ СИСТЕМ АУТЕНТИФІКАЦІЇ ОСОБИ**

Останнім часом при вирішенні питань забезпечення безпеки життєдіяльності суспільства, захищеності особи, підвищення оперативності дій щодо профілактики та припинення злочинної діяльності, значно підвищився інтерес до можливостей цифрової ідентифікації особи. Це перш за все пов'язано з зростанням загроз міжнародного тероризму, проблемами процесів демократизації при переході до інформаційного суспільства, а також збільшенням обсягів торговельних операцій, що здійснюються через глобальні комп'ютерні мережі, зокрема через Інтернет. Необхідність чіткого регулювання доступу особи пов'язана перш за все із природним бажанням кожної людини захистити себе, свої інтереси та інтереси суспільства. Але робота системи контролю доступу особи неможлива без вирішення питання ідентифікації особи. Цифрова ідентифікація особи нерозривно пов'язана також з такими поняттями, як аутентифікація, ідентифікація людини, біометрія, електронний цифровий підпис, біометричний паспорт.

Під ідентифікацією особи розуміють процес встановлення тотожності людини за сукупністю наявних суттєвих ознак шляхом здійснення порівняльного дослідження. Саме у слідчій та судовій практиці широко здійснюється ідентифікація осіб підозрюваних у скоєнні злочину, кримінальних злочинців, невідомих осіб, затриманих правоохоронними органами, невпізнаних трупів та ін.

Біометрія являє собою технологію ідентифікації особи, що будується на використанні фізіологічних параметрів суб'єкта (відбитки пальців, райдужна оболонка ока, геометрія обличчя та ін.).

До основних характерних ознак, за якими може проводитися аутентифікація людини в процесі вирішення питань контролю доступу відносяться:

предмети, які є власністю людини, (особливий розпізнавальний знак, ключ, магнітна картка та ін.);

інформація, якою володіє людина (засекречені дані, пароль, та ін.);

деякі особливості людини (мова, почерк, характерні ознаки певних видів діяльності, та ін.);

деякі фізичні характеристики (відбитки пальців, форма руки, узори кровоносних судин, геометрія обличчя та ін.).

На основі таких ознак створені спеціальні технічні засоби, розроблені методи аутентифікації, які широко застосовуються у судовій практиці. Неможливо обійтися без використання характерних ознак людини і в повсякденній діяльності, при зустрічі незнайомих людей, отриманні повідомлень.

На теперішній час аутентифікація особи та робота системи контролю доступу здійснюється в основному за пред'явленням конкретного документу, магнітної картки, ключа, шифру, та ін. Але це не дає повної впевненості в тому, що пред'явник дійсно має право доступу. А між тим природа створила людей досить різними, кожна людина індивідуальна та неповторна за сукупністю своїх характерних ознак. Застосування ж технічних систем біометричної аутентифікації особи з використанням математичних методів допомагає швидко та ефективно при здійсненні контролю доступу вирішувати питання ідентифікації по частині тіла людини, її фотографії, голосу, підпису, тобто однозначно стверджувати про наявність певної людини (біометрична ідентифікація особи).

Термін «біометрична ідентифікація», як спосіб підтвердження особи, чи приналежності паспорта його власнику шляхом розпізнавання і зіставлення, зафіксованих носіями біометричної інформації біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, та ін.) був започаткований в Україні ще в 2004 році при розробці концепції створення Єдиного державного реєстру фізичних осіб, яка передбачала, в якості основи побудови інформаційного забезпечення цього Реєстру, використання даних біометричної ідентифікації та машинозчитуваної інформації.

Переходячи до огляду застосувань систем біометричної аутентифікації людини, відзначимо, що їх застосування можна умовно розділити на два основні типи: «відкриті» системи (з користувачами, переважно незнайомими з правилами поведінки, тобто з «недисциплінованими» користувачами) і «закриті» системи (з користувачами, від яких вимагається суворе виконання певних правил поведінки).

У відкритих системах, які часто застосовують в банківських та фінансових установах, рівень контролю поведінки користувачів визначається обмеженнями пристроїв захисту. Ці пристрої можуть бути вбудовані в термінали та забезпечувати певні режими одержання контрольованих даних (пристрої для відтворення підпису; механічні обмежувачі положення руки при аутентифікації з геометрії руки,

пристрої обмеження положення пальців – при дактилоскопічній аутентифікації).

Закриті системи характеризуються тим, що доступ до ресурсів для співробітників та інших користувачів є керованим (наприклад доступ до операційної системи ЕОМ), чи може бути винятковим, для спеціально відібраного персоналу (наприклад, до систем управління зброєю).

Широке поширення біометричних систем поки стримується відсутністю стандартів на них. Виробники систем керуються своїми внутрішніми нормативами. Але дослідження та розробки систем тривають. Вони зосереджені на створенні таких версій пристроїв та систем, що характеризуються більш високою пропускнуою здатністю, зниженим рівнем відмов в аутентифікації законних користувачів, меншою вартістю та великими можливостями інтеграції.

Зокрема, застосування безконтактних біометричних технологій дозволяє з високою вірогідністю встановлювати особу за унікальними характеристиками, такими як обличчя та голос людини, здійснювати моніторинг небажаних осіб на підході до об'єкту, біометричну реєстрацію персоналу та відвідувачів об'єкту, біометричну реєстрацію усіх клієнтів при отриманні облікового запису на сайті, захист операцій та доступу зареєстрованих користувачів, забезпечувати автоматичне виявлення шахрайських дій шляхом виявлення потенційно небезпечної поведінки та ін.

Практично всі методи біометричної аутентифікації засновані на наявності характерної сукупності певних індивідуальних ознак у кожній людині. Але важливо зазначити, що існуючі моделі не дозволяють адекватно описати десь біля 5 % населення Землі, крім того, інструментальна похибка методів складає найчастіше десятки відсотків. Так професор антропології Університетського коледжу Лондона Анжела Сесс стверджує, що біометричні сканери, які будуть використовуватися в системі внутрішніх паспортів Великобританії, неможливо застосовувати для ідентифікації людей з деякими фізичними вадами. Наприклад, застосування сканерів сітківки ока буде складним для тих, хто носить окуляри або контактні лінзи, а людина, хвора артритом, не зможе рівно покласти палець на сканер відбитка. «Відсоток тих, для кого неможливо використовувати біометрію, виявляється набагато більшим, ніж передбачалося», – вважає професор [3, с. 54].

Враховуючи усі переваги застосування біометричної аутентифікації, доцільність використання таких систем при вирішенні питань профілактики та припинення злочинної діяльності, опрацювання місць можливого перебування підозрюваних осіб (метро, вокзали та ін.), слід зосередити увагу на необхідності подальшого

дослідження цього питання з метою підвищення ефективності застосування методів цифрової ідентифікації людини та належного захисту її прав та свобод. Важливим також є вирішення питання щодо підвищення можливостей роботи систем біометричної аутентифікації та їх надійності в складних умовах.

#### *Список використаних джерел*

1. Брюхомицкий Ю.А., Казарин М.Н. Тестирование биометрических систем контроля доступа. Россия, г. Таганрог: ТРТУ, 2004. 78 с.
2. Ворона В.А., Тихонов В.А. Системы контроля и управления доступом. Москва: Горячая линия - Телеком, 2010. 272 с.
3. Дубчак О.В., Підгайна К.І., Порівняльний аналіз сучасних біометричних методів аутентифікації. / «Захист інформації в інформаційно-комунікаційних системах». Київ: НАУ, 2010. 87 с.
4. Конеев И.Р., Беляев А.В. Информационная безопасность предприятия. СПб: Петербург. 2003. 733 с.
5. Лакин Г.Ф. «Биометрия». Москва: Высш. Шк., 1990. 352 с.
6. Тихонов В.А., Райх В.В. Информационная безопасность: концептуальные, правовые, организационные и технические аспекты: уч. пособие. Москва: Гелиос АРВ, 2006. 98 с.
7. Wikipedia. USA «Биометрия», [Электронный ресурс] – Режим доступа: URL: <http://ru.wikipedia.org/wiki/Биометрия>. (дата звернення 20.10.2018).