Савоста Ірина Іванівна,
старший судовий експерт сектору
дактилоскопічних досліджень відділу
криміналістичних видів досліджень
Запорізького науково-дослідного
експертно-криміналістичного центру
МВС України

ЗАСТОСУВАННЯ ІНФОРМАЦІЙНИХ ТЕХНОЛОГІЙ У ДІЯЛЬНОСТІ ПРАВООХОРОННИХ ОРГАНІВ

Такі виклики сьогодення, як кібертероризм та кіберзлочинність, спричиняють необхідність подальшого розвитку систем захисту інформації у всіх галузях суспільної практики і, зокрема, в діяльності правоохоронних органів. Одним з перспективних напрямів розвитку систем захисту інформації є використання біометричних технологій [1, с. 108].

Використання та удосконалення інформаційних технологій в Україні розвивається ще не в повній мірі. Слід враховувати, що розвиток технології біометричної інформації може впливати на захист від кіберзлочинності та захист інформації у всіх галузях суспільної практики і, зокрема, в діяльності правоохоронних органів.

Варто зазначити, що біометрія вивчає способи вимірювання різних параметрів людини з метою встановлення подібності або різниці між людьми та виділення однієї конкретної людини з множини інших людей.

Системи доступу і захисту інформації, які використовують біометричні технології є найзручнішими для користувачів – не потрібно запам’ятовувати складні паролі, постійно носити з собою смарт-карти або апаратні ключі. Для цього варто лише прикласти до сканера палець або руку, підставити для сканування в інфрачервоному промінні око, обличчя, руку або палець, що-небудь 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.

Біометричні технології захисту інформації використовують різні параметри особи з метою її автентифікації. Існують такі види автентифікації:

– слабка автентифікація відбувається за допомогою пароля називають ще однофакторною або слабкою, оскільки, перехоплення або підбір пароля є справою часу;

– багатофакторна автентифікація здійснюється з використанням двох чи більше факторів;

– посилена автентифікація у відповідності до вимог Європейської директиви PSD2 в платіжних системах використовується так звана посилена автентифікація [2, с. 22], коли для автентифікації використовуються принаймні два різних типи факторів. Типами факторів є: властивість, якою володіє суб'єкт; знання – інформація, яку знає суб'єкт; володіння – річ, якою володіє суб'єкт;

– сувора автентифікація під час якої використовується інформація без розкриття цієї інформації. Як правило, реалізується за допомогою асиметричних криптографічних алгоритмів.

Щодо методів біометричної автентифікації, то вони поділяються на статичні та динамічні.

Статичні методи використовують наступні фізіологічні характеристики людини: відбитки пальців (стійкість, відновлювальність, незмінність), форма долоні (розташування ліній на долоні людини), малюнок вен на долоні чи пальцях руки, малюнок райдужної оболонки ока (ще має назву райдужний код), малюнок кровоносних судин сітківки ока, двовимірне або тривимірне зображення форми обличчя, термографія обличчя, руки або пальця, ДНК (це найдосконаліша на сьогодні біометрична технологія) та інші методи.

Динамічні методи використовують поведінкові характеристики людини при виконанні різних рухів. До цих методів належить автентифікація за рукописним почерком (за підписом), за клавіатурним почерком (швидкість набору, час між натисканням клавіш, кількість пальців, які оператор використовує під час друку [2, с. 23], за голосом (поєднання частотних і статичних характеристик голосу) та інші методики.

Не всі з перечислених методів є в однаковій мірі зручними.

Слід враховувати, що способи розпізнавання за обличчям особи та її голосом мають відчутну перевагу: відеоперехоплення і аудіозапис не вимагають фізичного контакту користувача із системою й ретельного позиціонування перед реєструючим сенсором.

На даний час найбільш широко вживаним є використання систем розпізнавання за відбитками пальців.

Використання біометричних технологій на основі дактилоскопії є дуже популярним. Дактилоскопія («пальцероздивляння»: від грецького «daktylos – палець» та «skopeo – дивлюся») – це розділ криміналістики, що вивчає будову візерунків шкіри внутрішніх поверхонь нігтьових фаланг пальців та долонь для ідентифікації особистості, кримінальної реєстрації та розшуку злочинця. 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).

Підсумовуючи викладене, слід зазначити, що переваги технологій доступу за відбитком пальця полягають у простоті використання, зручності, достатній надійності та економічності. Зазначене дозволяє уникнути недоліків, які характерні окремо кожному алгоритму, і, внаслідок цього підвищити достовірність ідентифікації.

Список використаних джерел

1. Захаров В. П. Використання біометричних технологій в системах захисту інформації правоохоронних органів України / В. П. Захаров, О.І.Зачек // Наукові записки Львівського університету бізнесу та права. - 2013. - Вип. 11. - С. 108-110.

2. Мазниченко Н. І. Посилена ідентифікація і аутентифікація користувача комп'ютерних систем на основі клавіатурного почерку / Н. І. Мазниченко //Актуальные научные исследования в современном мире: матеріали XXII междунар. научн. конф. (26–27 февр. 2017 г., Переяслав-Хмельницкий): сб. научн. тр. – Переяслав-Хмельницкий, 2017. – Вып. 2, ч. 1. – С. 21–26.