

УДК 004.93

Владислав Олегович Воронько,

*студент Національного аерокосмічного
університету ім. М. Є. Жуковського
«Харківський авіаційний інститут»*

Михайло Віталійович Цуранов,

*старший викладач кафедри комп'ютерних систем, мереж
та кібербезпеки Національного аерокосмічного
університету ім. М. Є. Жуковського
«Харківський авіаційний інститут»*

Біометрична ідентифікація як захист від несанкціонованого доступу

На сьогоднішній день кожна людина зберігає достатньо велику кількість критичної інформації на своєму смартфоні. З кожним роком зберігати конфіденційність все важче, тому що алгоритми і методи зловмисників розвиваються наряду із новітніми технологіями. Задля того, щоб надійно захистити особисті дані системи захисту використовують біометричну ідентифікацію.

Біометрична ідентифікація – засіб підтвердження особи, належності паспорта його власнику шляхом розпізнавання і зіставлення зафіксованих носіями біометричних даних (кольору очей, малюнка сітківки ока, відбитків пальців, геометрії руки, рис обличчя тощо) з особистими даними власника [1]. Біометричні системи ідентифікації досить поширені в системах безпеки.

Незважаючи на високий коефіцієнт надійності більшості методів біометричної ідентифікації, зареєстровано чимало випадків злому. У 2018 році зловмисники розробили 3D-форму голови власника банківського відділення на основі багатьох фотографій із соціальних мереж. Після цього вони створили гіпсову модель цієї форми й даної копії було достатньо для успішної ідентифікації особи. Загальна сума награбованого майна складала близько 2 мільйонів доларів США [2]. Задля захисту від подібного роду атак майже усі системи, котрі використовують ідентифікацію по 3D-формі голови, впроваджують сканування в інфрачервоному діапазоні.

Однією з не вирішених проблем захисту інформації є надійна ідентифікація користувача, який отримує доступ до конфіденційної інформації [3]. Компанія Google навіть опублікувала статтю на цю тему, де попереджувала користувачів класти смартфон дисплеєм донизу, щоб ідентифікація по формі обличчя ненароком не розблокувала телефон [1]. Традиційний парольний захист має ряд недоліків: підбір паролю методом перебору, низька надійність, якщо пароль було розгадано, то уся конфіденційність стає під загрозою. Як альтернатива парольній системі або її доповнення може розглядатися ідентифікація користувачів за біометричними характеристиками. Передовою в цій сфері є компанія Apple, яка першою почала розробляти та використовувати біометричні методи захисту у формі ідентифікації по формі обличчя (FaceID) й по відбитку пальця (TouchID). Біометричне підтвердження, а не проста перевірка пароля, який може бути вкрадений, перехоплений або вгаданий, є ключовим при розширенні Інтернет-торгівлі, створенні нових систем безпеки інформації в корпоративних мережах та системах дистанційного навчання та тестування.

Ідентифікувати людину можливо за ознаками, пов'язаними з її фізіологічними особливостями, які однозначно ідентифікують особу. До таких ознак можна віднести: геометричну будову руки, відбитки пальців, особливості малюнка сітківки ока, райдужну оболонку ока, портрет (наприклад, інфрачервону карту людини), характеристики і особливості мови, рукописний почерк, клавіатурний та комп'ютерний почерк та інші фізіологічні особливості людини, що робить її «особливою».

Методи біометричної ідентифікації діляться на дві великі групи:

- статичні методи, які ґрунтуються на фізіологічних характеристиках людини;
- динамічні методи, які ґрунтуються на особливостях поведінки людини – підсвідомих рухах в процесі виконання якої-небудь дії.

Основною перевагою статичних методів біометричної ідентифікації є їх відносна незалежність від психологічного стану користувача [2].

До сучасних статичних технологій ідентифікації відносять:

- відбиток долоні – в цій системі використовується розташування ліній на долоні людини, повністю аналогічно біометричній технології, що використовує відбитки пальців;

- судинні рисунки — розташування вен в різних частинах тіла людини, включаючи зап'ястя і тильну сторону долоні.

До сучасних динамічних методів відносять:

- ідентифікація особи за особливостями голосу. Досліджувані риси: частота, модуляція і тривалість голосового образу;

- ідентифікація за динамікою рукописного підпису. Досліджувані риси: швидкість, порядок ліній, тиск і зовнішній вигляд підпису;

- ідентифікація за клавіатурним почерком. Досліджувані риси: час затримки та час «польоту».

Биометричні методи не тільки ускладнюють доступ до пристрою, але і у випадку із правопорушником правоохоронним органам. На рахунок цього ведуться дискусії: чи буде згодна фірма надати доступ правоохоронним органам.

З точки зору безпеки найбільш зручним способом являється ідентифікація по термограмі обличчя. Оскільки за допомогою неї можна розблокувати телефон правопорушника навіть при його супротиву.

Список бібліографічних посилань

1. Иванов А. И. Биометрическая идентификация личности по динамике подсознательных движений. Пенза : Изд-во Пенз. гос. ун-та, 2000. 188 с.
2. Голубев Г. А., Габриелян Б. А. Современное состояние и перспективы развития биометрических технологий. *Нейрокомпьютеры. Разработка. Применение*. 2004. № 10. 40 с.
3. Як Google стежить за користувачами. КДБ і не снилося // Економічна правда : сайт. 02.07.2019. URL: <https://www.epravda.com.ua/publications/2019/07/2/649257/> (дата звернення: 24.10.2019).
4. Borodavka V., Tsuranov M. Biometrics: Analysis and multi-criterion selection // 2018 IEEE 9th International Conference on Dependable Systems, Services and Technologies (DESSERT). DOI: <https://doi.org/10.1109/DESSERT.2018.8409152>.

Одержано 25.10.2019