УДК 004.056.53
Н. Заверцований, Г. Осухівська, Н. Шаблій
(Тернопільський національний технічний університет імені Івана Пулюя)

МЕТОДИ ПІДВИЩЕННЯ ЕФЕКТИВНОСТІ ЗАХИСТУ КОМП'ЮТЕРНИХ СИСТЕМ З ВИКОРИСТАННЯМ БІОМЕТРИЧНИХ ХАРАКТЕРИСТИК

У сучасному світі стрімкого розвитку інформаційних технологій одним із важливих завдань є забезпечення цілісності конфіденційної інформації. Найефективнішими методами захисту комп'ютерних систем від несанкціонованого доступу є ідентифікація користувачів, яка продовжується подальшою їх автентифікацією, на основі використання біометричних характеристик. В системах захисту використовують динамічні та статичні біометричні методи. Динамічні методи враховують дані про особливості підсвідомих дій особи в процесі відтворення підпису, клавіатурного почерку, голосу і т.п. Статичні методи біометрії ґрунтуються на даних анатомічних особливостей людини, які не змінюються на протязі всього життя або досить тривалого часу. Такими статичними характеристиками є відбитки пальців, форма долоні, зображення обличчя, візерунок райдужної оболонки та сітківки ока й т.ін. [1,2].

Багато науковців проводили дослідження підвищення ефективності різних методів біометричної ідентифікації та автентифікації [1-3], проте зловмисники також знаходять все нові й нові шляхи процедури обходу системи біометричної ідентифікації, які не вимагають використання будь-яких дорогих і високотехнологічних пристроїв [4]. Тому актуальним є розробка та дослідження комбінованих методів захисту комп'ютерних систем з використанням біометричних характеристик.

Серед комбінованих методів можна виокремити такі, які побудовані на одночасному поєднанні: декількох статичних характеристик (відбитків декількох пальців, відбитки пальців і райдужної оболонки ока, райдужної оболонки ока і зображення обличчя людини і т.д.) [2,3]; декількох динамічних характеристик (наприклад, таких як особливості клавіатурного почерку, голосу, динаміки роботи користувача з маніпулятором «миша»); а також біометричних характеристик та USB-ключів; разові паролі та USB-ключі; безконтактні смарт-карти та USB-ключі; гібридні смарт-карти [3]. Але всі ці методи використовують поєднання або тільки статичних, або тільки динамічних біометричних характеристик.

Для підвищення ефективності захисту комп'ютерних систем запропоновано метод, побудований на використанні як статичних, так і динамічних біометричних характеристик, зокрема, поєднання розпізнавання райдужної оболонки ока людини та клавіатурного почерку. Такий комбінований метод ідентифікації та автентифікації користувачів не передбачає використання дорого обладнання, але поряд з тим підвищить ефективність захисту комп'ютерних систем від несанкціонованого доступу.

Література:

1. Чередниченко В.Б. Чередниченко К.Е. Біометричні методи у системах захисту інформації // Системи обробки інформації. – 2012. – Вип. 4 (102). – Т. 1. – С. 145–148.

2. Калініна І.В., Лісовиченко О.І. Комбіновані методи біометричної ідентифікації в задачах захисту від несанкціонованого доступу / Міжвідомчий науково-технічний збірник «Адаптивні системи автоматичного управління». – 2016. – № 2'(29). – С. 42 – 51. – Режим доступу: http://nbuv.gov.ua/UJRN/asau_2016_2_8.

3. Ігнатович А.О. Методи підвищення ефективності компонентів безпеки комп'ютерних систем з використанням маскуючих елементів текстових та біометричних даних: дис. канд.тех.наук: 05.13.05 / Анатолій Олександрович Ігнатович. – Львів, 2016. – 145 с.

4. Chaos Computer Clubs breaks iris recognition system of the Samsung Galaxy S8 [Електронний ресурс] – Режим доступу: https://www.ccc.de/en/updates/2017/iriden.