

АНАЛІЗ ІСНУЮЧИХ МЕТОДІВ БІОМЕТРИЧНОЇ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА

Ковальчук В.С., ст. гр.. 6151м, д.т.н. Приходько С.Б.
Національний університет кораблебудування імені адмірала Макарова
Україна, Миколаїв
141247@nuos.edu.ua

Анотація. Метою роботи є дослідження та аналіз існуючих методів біометричної ідентифікації користувачів, виявлення їх переваг та недоліків, вибір оптимального методу ідентифікації користувача.

Ключові слова: (Біометрична ідентифікація користувачів, захист інформації, клавіатурний почерк).

Вступна частина. У зв'язку з бурхливим розвитком інформаційних технологій проблема захисту інформації постає все гостріше. Наразі дедалі більше інформації з абсолютно різних сфер життя окремої людини, груп людей або й всього суспільства зберігається і обробляється за допомогою комп'ютерів, при чому досить часто ця інформація не є загальнодоступною, а тому має надійно захищатися від осіб, які не повинні мати до неї доступ, оскільки у разі отримання таких даних невідомими особами можуть бути абсолютно різні наслідки, які нанесуть значних збитків та шкоди «власникам» цих даних. Способи вирішення цієї проблеми будуть розглянуті далі.

Основна частина. «Ідентифікація – це присвоєння суб'єктові, що реалізує доступ до ІС, унікального ім'я, образу або числового значення.»[1] На сьогодні існує декілька способів ідентифікації користувачів, у кожного з яких свої переваги і недоліки. «Аутентифікація полягає в перевірці, чи є даний суб'єкт справді тим, за кого себе видає.»[1] Методи аутентифікації можна розділити на 4 великі групи, наведені у табл. 1.

Таблиця 1

№	Методи аутентифікації	Характеристика методу
1	Методи, засновані на знанні секретної інформації	Класичним прикладом таких методів є парольний захист, коли в якості засобу аутентифікації користувачу пропонується ввести пароль – деяку послідовність символів. Такі методи аутентифікації є найпоширенішими
2	Методи, засновані на використанні унікального предмета	В якості такого предмета можуть бути використані: смарт-карта, токен, електронний ключ тощо.
3	Методи, засновані на використанні біометричних характеристик людини	На практиці частіше використовуються одна або деякі з наступних біометричних характеристик: відбитки пальців; малюнок сітківки або райдужної оболонки ока; термографія долоні; геометрія і термограма обличчя; почерк (підпис); голос
4	Методи, засновані на інформації, асоційованій з користувачем	Наприклад, координати користувача, визначені за допомогою GPS. Цей підхід цілком допустимо використовувати як додатковий елемент захисту.

Розглянемо перераховані методи докладніше.

Парольні системи захисту – основною перевагою ідентифікації за паролем є простота і зручність. Зараз паролі використовуються в операційних системах і багатьох додатках та сервісах. При правильному використанні цей спосіб може забезпечити достатній рівень захищеності, проте за сукупністю характеристик даний метод є найвразливішим. Значна кількість загроз пов'язана з людським фактором, а саме надто легкі паролі, зберігання паролю в доступному для інших місці, передача паролю іншій особі навмисно або під тиском. Також пароль може бути виявлений внаслідок хакерських атак або підбору.

Ідентифікація з використанням унікального предмета. Електронний ідентифікатор є фізичним пристроєм, зазвичай досить невеликих розмірів, а тому його зручно носити з собою. Досить часто використовується для двофакторної аутентифікації (наприклад пароль та електронний ідентифікатор). До недоліків даного методу слід віднести можливість втрати електронного ідентифікатора або заволодіння ним третіми особами.

Біометрична ідентифікація. Методи біометричної ідентифікації поділяються на 2 групи – статичні та динамічні. До статичних методів належить ідентифікація за відбитком пальця, за формою долоні, за розташуванням вен на тильній стороні долоні, за сітківкою ока, за райдужною оболонкою ока, за формою обличчя, за термограмою особи. Перевагою даної групи є досить висока імовірність розпізнавання особи та унікальність перерахованих біометричних ознак, внаслідок чого їх неможливо зімітувати. Недоліки – необхідність у спеціальному обладнанні (сканери відбитків пальців, інфрачервоні або інші специфічні камери) – вартість такого обладнання велика, при чому зі зростанням ціни збільшується і точність ідентифікації.

Динамічні методи ґрунтуються на поведінковій (динамічній) характеристиці людини, тобто враховують особливості, характерні для підсвідомих рухів у процесі відтворення певної дії. Вони включають: рукописний почерк (використовується підпис людини або написання кодового слова, необхідний графічний планшет); голос (поєднання статичних і частотних характеристик голосу, необхідний мікрофон); клавіатурний почерк (для ідентифікації як правило застосовують динаміку набору кодової фрази).

Загалом методи біометричної ідентифікації вигідні тим, що їх неможливо викрасти і підробити, а також вони є унікальними для кожної людини, тому є унікальним ідентифікатором. До недоліків належить необхідність застосовувати специфічне обладнання для зчитування певних характеристик людини.

Клавіатурний почерк – індивідуальна характеристика кожної людини, оскільки кожен має свою індивідуальну швидкість вводу тексту з клавіатури, також кожній людині характерні такі особисті характеристики, як тривалість натискання на клавішу і часовий проміжок між натисканнями різних клавіш. Такі дані досить складно отримати – достатньо виміряти дані часові проміжки, зберегти цю інформацію і відповідно опрацювати, отримавши певну статистику, згідно з якою система і робитиме висновок, чи є дана особа тим користувачем, за якого себе видає.

Ідентифікація за клавіатурним почерком є більш універсальним методом і може досягти більш широкого розповсюдження, оскільки параметри клавіатурного почерку можна визначити не застосовуючи специфічного периферійного обладнання комп'ютера, достатньо звичайної клавіатури, тому даний метод ідентифікації користувача може застосовуватись на будь-якому комп'ютері. Імовірність ідентифікації користувача за допомогою існуючих математичних моделей становить близько 90%, що є досить високим показником. Клавіатурний почерк неможливо підробити,

Висновки. В даній статті розглянуто існуючі методи аутентифікації, виділені їхні переваги і недоліки. Найбільш універсальним методом ідентифікації, не рахуючи парольного є біометричний метод ідентифікації, а саме за клавіатурним почерком, оскільки динаміка набору тексту є унікальною характеристикою кожного користувача, а також для виявлення цих характеристик не потрібно специфічного обладнання, досить звичайного персонального комп'ютера чи ноутбука.

REFERENCES

- [1] Ідентифікація користувача: Освітня публічна бібліотека - <http://po-teme.com.ua/informatika/stati-po-informatike/1588-identifikatsiya-koristuvacha.html>
- [2] Кульчицький О.С.; Грицюк В.В.; Зотова І.Г.; (Ред.). (2016). *Аналіз існуючих підходів при ідентифікації і аутентифікації користувачів в інформаційно-телекомунікаційних системах*, Центр воєнно-стратегічних досліджень Національного університету оборони України імені Івана Черняхівського, Київ.

Koval`chuk V.S., Prihod`ko S.B.

Analysis of existing methods of biometric user identification

Annotation. The purpose of the work is to analyze and explore the existing methods of biometric identification of users, identify their advantages and disadvantages, and choose the optimal method of user identification.

Keywords: (*Biometric user identification, protection of information, keyboard handwriting*).

Ковальчук В.С., Приходько С.Б.

Анализ существующих методов биометрической идентификации пользователя

Аннотация. Целью работы является анализ и исследование существующих методов биометрической идентификации пользователей, выявление их преимуществ и недостатков, выбор оптимального метода идентификации пользователя.

Ключевые слова: (*Биометрическая идентификация пользователей, защита информации, клавиатурный почерк*).