УДК 004.056.52

Медведєва К.В.
Каплун В.А.

ЗАХИСТ ПРОГРАМ З ВИКОРИСТАННЯМ ІДЕНТИФІКАЦІЇ КОРИСТУВАЧА ПО РОБОТІ З МИШЕЮ

Анотація. *Стаття описує основні принципи роботи методів ідентифікації і наведено їх класифікацію. Виявлено основні переваги та недоліки існуючих підходів. Розроблено метод комплексної ідентифікації, запропоновано поєднати пароль з цифровим почерком, задля підсилення надійності системи і збереження зручності для користувачів.*

Ключові слова: *захист програм, ідентифікація користувача, клавіатурний почерк, біометричні методи захисту*

Abstract. *The article describes the basic principles of identification methods and provides their classification. The main advantages and disadvantages of existing approaches are given. The method of complex identification is developed, it is offered to combine the password with digital handwriting, for connection of reliability of system and preservation of convenience for users.*

Keywords: *program protection, user identification, keyboard handwriting, biometric protection methods.*

Вступ

Багато сфер діяльності сучасного суспільства залежать від функціонування інформаційно-комунікаційних систем. У зв'язку з цим гостро постає питання захисту інформації в них. Необхідність вирішення проблем інформаційної безпеки також зумовлена різким зростанням комп'ютерної злочинності, результат діяльності якої призводить до значних матеріальних втрат, незалежно від того чи це вірусна атака, чи несанкціонований доступ до інформації. Найпоширеніший вид порушень конфіденційності інформації – несанкціонований доступ. Дієвим засобом захисту інформації від несанкціонованого доступу є розмежування та управління правами на використання ресурсів інформаційної системи. Один з способів реалізації даного методу є ідентифікація та автентифікація користувачів.

Результати дослідження

Ідентифікація дозволяє суб'єкту (користувачу або процесу, що діє від імені певного користувача) представити власний унікальний ідентифікатор, який виконує роль імені. Тобто під час цього процесу одна з сторін називає себе. Використовуючи автентифікацію, друга сторона переконується, що суб'єкт дійсно той, за кого він себе видає.

Методи однофакторної ідентифікації-автентифікації діляться на 3 великі групи, в залежності від того, що має представити користувач в якості ідентифікатором :

– знання певної інформації, що зберігається в секреті і якою володіє лише особа, яка проходить процедуру ідентифікації, наприклад пароль, персональний ідентифікуючий номер(ПІН), відповіді на питання тощо. Також цей метод ще називають парольною ідентифікацією, за назвою найбільш популярного засобу – паролю;

– володіння деякими фізичними предметами, які може представити особа, яка ідентифікується. Наприклад, електронний ключ, смарт-карта, токен тощо. Цей метод ще називають апаратним;

– біометрія – унікальні характеристики, якими володіє особа, яка ідентифікується. Наприклад, відбитки пальців, малюнок сітківки, термографія долоні, геометрія обличчя, почерк, голос [1].

Двофакторні методи ідентифікації поєднують у собі два або більше однофакторних метода.

При всій різноманітності способів ідентифікації найбільш поширеним залишається парольний захист. Популярність даного методу пояснюється наявністю в нього ряду переваг:

– відносна простота реалізації. Використання парольного способу захисту не вимагає додаткових апаратних засобів;

– звичність. Механізми парольного захисту є звичними для більшості користувачів інформаційних систем та не викликають психологічного відторгнення;

– не вимагає ніяких витрат. Даний метод протидії несанкціонованому доступу реалізовано у

більшості операційних систем та інших сервісах [2].

Основним недоліком парольної ідентифікації є те, що рівень надійності захисту напряму залежить від користувача, точніше від обраного паролю. Відомо, що стійкі паролі є важкими для запам'ятовування. Тому велика кількість користувачів використовує не достатньо надійні ключові слова, які полегшують доступ зловмиснику до інформації.

Суть методу апаратної ідентифікації полягає у використані електронних ключів. Існує два типи пристроїв: смарт-карти та токени. Кожен апаратний ідентифікатор є фізичним пристроєм невеликого розміру. Апаратна ідентифікація має ряд переваг:

– досить висока надійність. У пам'яті токені можуть зберігатись ключі, які важко дізнатись, використовуючи метод «грубої сили»;
– існує багато способів надати захисту додаткової стійкості;
– має додаткові можливості, які дозволяють використовувати електронні ключі для реалізації маркетингової стратегії й оптимізації продажів. Наприклад, створення демо-версії, контроль кількості використовуваних копій програм, надання програм у використання на певний час та продаж програми вроздріб;
– зручність використання. Зазвичай токени виглядають наче флеш-картки або брелоки.

Даний метод ідентифікації має ряд недоліків:

– існує ризик крадіжки, втрати та передачі іншій особі електронного ключа;
– досить висока вартість. Загалом, за останній час, ціна електронних ключів помітно знизилась. Проте для введення в експлуатацію такої системи необхідні вкладення, адже кожного користувача треба забезпечити персональними токенами або смарт-картками;
– перед початком роботи необхідно налаштувати електронний ключ;
– можливість створення копій виготовлення апаратної чи програмної копії ключа зловмисником.

В контексті інформаційної безпеки біометрія – це система методів та засобів для ідентифікації та автентифікації користувача, використовуючи його анатомічні чи поведінкові особливості. Сучасний рівень розвитку комп'ютерних технологій дозволив використовувати подібні ознаки для ідентифікації людини у повсякденному житті. Даний напрямок розвивається дуже активно. Сьогодні використовується вже більше десятка різних біометричних ознак для ідентифікації користувачів.

Методи біометричної ідентифікації за видом ознаки, що використовується поділяються на:

– статичні. Використовують анатомічні характеристики людини. Більшість з них залишаються незмінними протягом життя;
– динамічні. Використовують особливості підсвідомих рухів у процесі виконання будь-якої дії. Наприклад, голос, клавіатурний почерк, робота з мишею тощо.

На сьогоднішній день практичне використання отримали методи статичної біометричної ідентифікації, які використовують у вигляді параметрів анатомічні особливості людини.

Основною перевагою статичних методів біометричної ідентифікації є незалежність результатів ідентифікації від психофізичного стану людини. Ключовим недоліком є висока вартість реалізації даних підходів.

Серед динамічних методів, які використовуються для ідентифікації особи користувача, можна назвати наступні:

– за голосом. В основі підходу лежать унікальні частотні характеристики голосу людини. Саме використовуючи їх, будується цифрова модель;
– за рукописним підписом. Ідентифікація проводить за особистим підписом людини. Перевіряються такі характеристики: графічні параметри, сила натиску на поверхню, швидкість написання. На основі цих характеристиках і будується цифровий код;
– за цифровим почерк(динаміка натискання клавіш та робота з маніпулятором «миша»). Метод аналогічний ідентифікації за почерком.

Перевагою даних методів є відносно низька ціна в порівнянні з способами статичної біометрії. Головним недоліком є те, що при використанні динамічних характеристик на роботу системи захисту впливає психофізичний стан людини.

У кожного методу ідентифікації є свої переваги та недоліки. Тому для підвищення надійності пропонується використовувати багатофакторну ідентифікацію, тобто збільшити кількість ідентифікаційних ознак. Комбінуватися ці параметри можуть у довільному порядку і можуть належати як системам одного класу так і різним. Втім, сьогодні в переважній більшості випадків використовується тільки

одна пара: парольний захист (або PIN-код) і токен. Основною перевагою такої ідентифікації є додаткова стійкість до «злому». Адже втрата апаратного ключа не спричиняє за собою компрометації пароля, оскільки окрім ключа для доступу до комп'ютерної системи потрібний ще і PIN-код до ключа. При організації системи строгої ідентифікації слід використати, як мінімум, двофакторну ідентифікацію.

Пропонується підвищити надійність систем ідентифікації користувачів за допомогою поєднання парольної ідентифікації(як найпоширенішої на сьогоднішній день) і цифровим почерком (особливість та манера введення парольної фрази). Суть даного підходу полягає в такому: для забезпечення захисту від клавіатурних шпигунів парольну фразу користувач вводитиме за допомогою віртуальної клавіатури, використовуючи маніпулятор «миша», тому співставлятиметься відразу два фактори. Основною перевагою даного методу є відсутність необхідності використання додаткового устаткування.

В основу математичного апарату, що використовується при розробці програми ідентифікації за цифровим почерком, покладено оцінювання характеристик числових послідовностей, членами яких є значення певних параметрів оцінювання цифрового почерку.

В якості параметрів оцінювання взято такі: а) величина часу утримування клавіші миші користувачем; б) швидкість набору; в) загальний час набору парольної фрази.

Одиниця вимірювання параметрів – мілісекунди.

Передбачено процес ідентифікації розбити на два етапи: етап налаштування і етап безпосередньо ідентифікації. Крім того, ідентифікація проводитиметься з використанням парольної фрази (і тоді її також необхідно зберігати разом із іншою реєстраційною інформацією про користувача).

В результаті проходження етапу налаштування необхідно отримати файли еталонів. На етапі настроювання користувачу пропонується декілька разів набрати ключову фразу.

Метою розробки є виявлення відмінностей між значеннями обраних параметрів для різних об'єктів (легального і нелегального користувача). Для вирішення питання про випадкове або невипадкове розходження параметрів проводять дві серії експериментів (перша серія – процес налаштування, друга – процес безпосередньої ідентифікації). Для кожної з цих серій підраховуємо середнє значення параметрів та середні квадратичні відхилення. Для виявлення відмінностей між значеннями обраних параметрів для різних об'єктів (легального і нелегального користувача) використаємо критерій Стьюдента і Фішера.

Висновки

Розроблено власний програмний засіб у якому реалізовано метод комплексної ідентифікації. Програму було розроблено у середовищі PyCharm, використовуючи мову Python та бібліотеку Tkinter.

Щодо вибору системи ідентифікації безпосередньо в кожній окремій ситуації, користувач повинен: об'єктивно оцінити співвідношення цінності інформації, що захищається, та вартості програмно-апаратного забезпечення ідентифікації, яке обираєте (включаючи супровід); оцінити зручність у використанні (контактні, безконтактні) та сприйняття обраного підходу користувачами; визначити потрібний рівень захищеності («що» і від «кого» потрібно захищати). Але безперечною порадою є обов'язкове використання комплексної системи ідентифікації, яка поєднує декілька підходів до вирішення задач доступу до інформаційних ресурсів комп'ютерних систем.

Список використаної літератури

1. Брюхомицкий, Ю. А. Биометрические технологии идентификации личности : учебное пособие / Ю. А. Брюхомицкий ; Южный федеральный университет. – Ростов-на-Дону ; Таганрог : Издательство Южного федерального университета, 2017. – 263 с.
2. Цирлов В.Л. Основы информационной безопасности автоматизированных систем. Краткий курс: учебное пособие. – Ростов-на-Дону: Феникс, 2008. – 173 с

Медведєва Катерина Вікторівна – студентка групи 1БС-18б, факультет інформаційних технологій та комп'ютерної інженерії, Вінницький національний технічний університет, м. Вінниця, e-mail: medvedieva.katya@gmail.com

Каплун Валентина Аполінаріївна, ст. викл. кафедри захисту інформації, Вінницький національний технічний університет, Вінниця, valuka8379@gmail.com.

Medvedieva Katherine V.– Department of Information Technology and Computer Engineering , Vinnytsya National Technical University, Vinnytsia.

Valentyna A. Kaplun – Lecturer of the Chair of Safety of Infomation and Communication Systems, NTU, Vinnytsia.