УДК 621.384.3

І. О. Бондаренко
Н. В. Сачанюк-Кавецька

ОСОБЛИВОСТІ АУТЕНТИФІКАЦІЇ КОРИСТУВАЧІВ WEB–РЕСУРСУ З ВИКОРИСТАННЯМ КЛАВІАТУРНОГО ПОЧЕРКУ

Вінницький національний технічний університет

Анотація

В даній доповіді розглядаються особливості використання методу аутентифікації суб'єктів із застосуванням динамічної біометричної характеристики – клавіатурного почерку. Математично описано точність роботи системи моніторингу WEB-ресурсу інтернет провайдера та розглянуто схемо блоку навчання.

Ключові слова: аутентифікація, біометричні характеристики, клавіатурний почерк, блок навчання.

Abstract

This report discusses the peculiarities of the use of authentication methods for subjects with the use of dynamic biometric characteristics - keyboard handwriting. The accuracy of the monitoring system of the WEB-resource of the ISP and the description of the training schemes are described mathematically.

Keywords: authentication, biometric characteristics, keyboard writing, learning unit.

Поширення інформаційних та комунікаційних систем надає все нові можливості для несанкціонованого доступу до інформаційних ресурсів. З погляду безпеки всі види інформації потребують надійного захисту. Однак, управління доступом – ефективний метод комплексного захисту інформації, що регулює використання ресурсів інформаційної системи і включає в себе такий важливий елемент, як аутентифікацію користувача. Слід відмітити, що захисні заходи є ефективнішими, якщо вони вбудовані в інформаційні системи та послуги на етапах формування технічного завдання та проектування.

З появою і розвитком інформаційних технологій актуальною стала проблема інформаційної безпеки, пов'язана із збереженням конфіденційності інформації, що обробляється та зберігається в комп'ютерних системах [1]. До передавання інформації каналами зв'язку ставлять такі вимоги:

- забезпечення конфіденційності інформації;
- забезпечення цілісності інформації;
- аутентичність сторін інформаційного обміну [2].

Методи і системи захисту інформації, що спираються на управління доступом виконують функції: ідентифікації користувачів; впізнання і встановлення достовірності користувача за обліковими даними; допуск до певних умов роботи згідно регламенту. Ідентифікація та аутентифікація застосовуються для обмеження доступу випадкових та незаконних суб'єктів (користувачів, процесів) інформаційних систем до її об'єктів (апаратних, програмних та інформаційних ресурсів). Загальний алгоритм роботи таких систем полягає в тому, щоб отримати від суб'єкта (наприклад, користувача) інформацію, що підтверджує його особу, перевірити її достовірність і потім надати (чи не надати) цьому користувачу можливість роботи із системою. Наявність процедур ідентифікації та автентифікації користувачів є обов'язковою умовою будь-якої захищеної системи, оскільки усі механізми захисту інформації розраховані на роботу іменованими суб'єктами і об'єктами інформаційних систем. Слід відмітити, що сучасні засоби ідентифікації/автентифікації повинні підтримувати концепцію єдиного входу в мережу – вимогу зручності для користувачів.

Існують такі види ідентифікації суб'єктів [3].

1) Парольна ідентифікація, заснована на конфіденційних ідентифікаторах суб'єктів (пароль, таємний ключ, персональний ідентифікатор і т. п.). В цьому випадку при введенні суб'єктом свого пароля підсистема автентифікації порівнює його з паролями, що зберігаються в базі еталонних даних у зашифрованому вигляді. У випадку співпадіння паролів підсистема автентифікації дозволяє доступ

до інформаційних ресурсів. Головна перевага паралельної ідентифікації – простота реалізації й використання пари логін-пароль. Головним недоліком такої ідентифікації є залежність її надійності від користувачів, точніше, від обраних ними паролів (так званий людський фактор).

2) Апаратна ідентифікація, з використанням ключів, токенів або карт, що перебувають в ексклюзивному користуванні суб'єктів ідентифікації. Апаратні ідентифікатори умовно можна розділити на два типи: пасивні (картки з пам'яттю) та активні (інтелектуальні картки). Найбільш розповсюдженими є пасивні картки з магнітною стрічкою, при використанні яких користувач вводить свій ідентифікаційний номер. У разі його співпадіння з електронним варіантом, закодованим у картці, користувач одержує доступ до системи. Інтелектуальні картки мають власний мікропроцесор. Це дозволяє реалізувати різноманітні варіанти парольних методів захисту, наприклад, багаторазові паролі, паролі, що динамічно змінюються. Головною перевагою такої ідентифікації є її досить висока надійність. Однак велика вартість таких пристроїв, їх крадіжка у зареєстрованих користувачів, а також можливість дублювання знижує цікавість до засобів апаратної ідентифікації.

3) Біометрична ідентифікація [4], з використанням унікальних властивостей та ознак людини, забезпечує майже 100% ідентифікацію, вирішуючи проблеми втрати паролів та особистих ідентифікаторів. Біометричних характеристик є два класи:

– статистичні, які ґрунтуються на фізіологічних унікальних характеристиках об'єктів (за відбитком пальця, за термограмою обличчя, за формою долоні, за сітківкою ока, за ДНК, за розташуванням вен на лицьовій стороні долоні і т. ін), що практично не змінюються з часом;

– динамічні, які ґрунтуються на поведінковій характеристиці суб'єктів, тобто побудовані на особливостях, характерних для підсвідомих рухів у процесі відтворення якої-небудь дії (за почерком, за клавіатурним почерком, за голосом і ін.). Головною перевагою біометричних технологій є найвища надійність, а основним недоліком – вартість устаткування. Однак, ці методи не можливо використовувати при ідентифікації процесів чи даних (об'єктів даних), вони тільки починають розвиватися, вимагаються поки складного та дороговартісного обладнання.

4) Ідентифікація за допомогою доведення істинності віддаленого користувача за його місце знаходженням. Даний захисний механізм базується на використанні системи космічної навігації, типу *GPS (Global Positioning System)*. Користувач, який має апаратуру *GPS*, багаторазово надсилає координати заданих супутників, які знаходяться у зоні видимості. Підсистема автентифікації, яка знає орбіти супутників, може із точністю до метра визначити місце знаходження користувача. Висока надійність автентифікації визначається тим, що орбіти супутників піддаються коливанням, передбачити які достатньо важко. Окрім того, координати постійно змінюються, що виключає їх перехоплення. Це найновіший метод ідентифікації, що може бути використаний у випадках, коли авторизований віддалений користувач повинен знаходитись у потрібно місці.

Зосередимося на особливостях використання методу аутентифікації із застосуванням динамічної біометричної характеристики – клавіатурного почерку.

Клавіатурний почерк – манера роботи користувача на клавіатурі. Основними характеристиками є значення часу утримань і пауз між натисканням клавіш. У загальному вигляді процес набору тексту на клавіатурі може бути представлений в вигляді функції [5]:

$$R(t) = \varphi(t) + \psi(t) + \lambda(t), \tag{1}$$

де $\varphi(t)$ – складові, що характеризують інформаційні підсвідомі процеси мислення при наборі тексту,

$\psi(t)$ – складова свідомих процесів мислення,

$\lambda(t)$ – механічні характеристики клавіатури, що впливають на процес набору тексту.

Для порівняння двох зразків клавіатурного почерку між собою найчастіше використовуються наступні характеристики: час утримання клавіші; тривалість паузи між натисканнями; наявність накладень; кількість помилок вводу; натискання системних клавіш.

Точність роботи системи моніторингу WEB-ресурсу інтернет провайдера характеризується двома величинами: помилкою першого роду та помилкою другого роду.

Помилка першого роду (FRR – false rejection rate) – ймовірність відмови авторизованого користувача. Помилка першого роду не настільки критична для системи моніторингу WEB-ресурсу. Значення помилки перебуває в інтервалі від 0,1 до 0,3.

Помилка другого роду (FAR – false acceptance rate) – ймовірність допуску незареєстрованого користувача. Ця величина є визначальною для біометричних систем. При значенні помилки другого роду більшому за 0,5 біометричну систему можна вважати непрацездатною.

Помилки першого і другого роду мають зворотну залежність. При збільшенні помилки першого роду, ймовірність пропуску незареєстрованих користувачів зменшується. У разі збільшення помилки другого роду, ймовірність відмови авторизованому користувачу буде зменшуватися. На рисунку 1 представлені залежності помилок першого і другого роду від коефіцієнта точності .

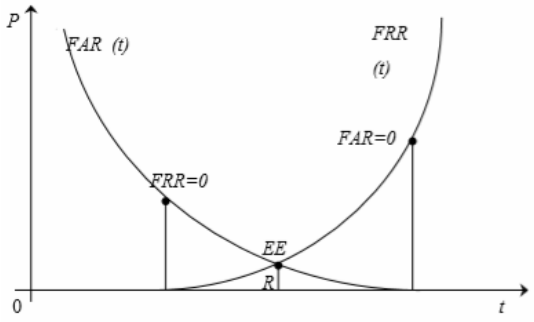

Рисунок 1 – Залежність помилок першого і другого роду

У точці перетину кривих FAR (t) і FRR (t), помилки першого і другого роду рівні. Значення помилки першого або другого роду в цій точці називається рівноймовірною помилкою властивості (EER – equal error rate).

Більшість біометричних систем можуть бути налаштовані певним чином, для досягнення високого або низького рівня безпеки. З одного боку, збільшення рівня безпеки біометричної системи спричинить збільшення помилки першого роду. З іншого – через зменшення рівня інформаційної безпеки біометричної системи можливе збільшення помилки другого роду. Таким чином, система повинна бути налаштована так, щоб ні помилка першого роду, ні помилка другого роду не були достатньо великі. Значення рівноймовірної помилки є оптимальним значенням помилок першого і другого роду.

Система захисту повинна виконувати такі дії: відслідковувати параметри клавіатурного почерку; аналізувати отримані параметри; порівнювати з еталонними параметрами, на основі результату порівняння виконувати відповідні дії. Крім того, необхідно виконувати навчання системи, тобто здійснювати запис еталонних параметрів для кожного користувача. Зрозуміло, що алгоритм має поділятися на два блоки: блок навчання (рис. 2) та блок аутентифікації.

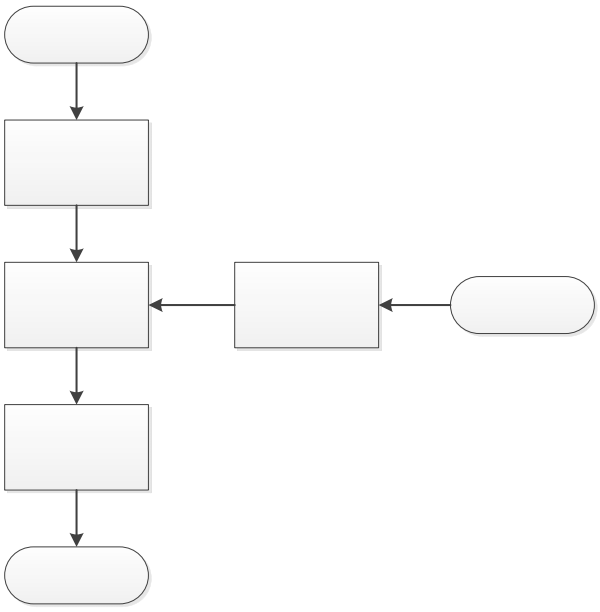

Рисунок 2 – Схема блоку навчання

Система моніторингу WEB-ресурсу роботи користувачів на основі клавіатурного почерку базується на принципах аналізу особливостей динаміки роботи на клавіатурі або руху.

Вхідні дані, представлені у вигляді деяких ненормованих зміщених дискретних значень сигналів, надходять з клавіатури. Після реєстрації користувача потрібне навчання системи. Навчання буде проводитись за кодовою фразою, а саме за паролем користувача. Користувач декілька разів вводить пароль, а система фіксує параметри клавіатурного почерку для кожного введення окремо. Отримані параметри аналізуються та записуються в базу даних. При наступній авторизації у Web-додатку, під час введення паролю користувачем, параметри клавіатурного почерку фіксуються. Якщо логін та пароль правильні, алгоритм аналізує та порівнює отримані дані з еталонними для даного користувача. Якщо параметри співпадають, користувачеві надається доступ до додатку. В іншому випадку доступ блокується.

На першому етапі відбувається обробка вхідних даних, виконується масштабування амплітуд або нормування вхідних сигналів (приведення їх до деякого еталонного значення). Крім цього, здійснюється приведення сигналів до єдиного масштабу часу, дроблення сигналів на окремі фрагменти з подальшим зрушенням фрагментів сигналу до оптимального поєднання з еталонним розташуванням та фільтрацією даних за часом або іншими характеристиками.

На наступному етапі здійснюється обчислення вектора біометричних параметрів (вектора контрольованих параметрів $\overline{V}$).

У режимі навчання, вектори біометричних параметрів $\overline{V}$ надходять в блок правил навчання, який формує біометричний еталон суб'єкта. Динамічні інформаційні образи суб'єкта ідентифікації можуть змінюватись, тому для формування біометричного зразка потрібна деяка кількість прикладів реалізацій одного і того ж образу, які залежать від стабільності динаміки його руху. На практиці виникає ситуація, коли не вдається отримати біометричний еталон через відсутність стабільності динаміки руху. У найпростішому випадку біометричний еталон може формуватися в вигляді двох векторів: $M\left(\overline{V}\right)$- вектора математичних очікувань контрольованих параметрів і $D\left(\overline{V}\right)$- вектора дисперсії цих параметрів.

В режимі аутентифікації вектор контрольованих параметрів $\overline{V}$, отриманий з пред'явленого образу, надходить в блок класифікатора. В основі класифікатора лежить деяке вирішальне правило, яке дозволяє розділяти вхідні вектори на класи властивостей «свій» і властивостей «чужий». Якщо пред'явлений вектор виявляється близький до біометричного еталону, то інформаційна система класифікує його як «свій». Якщо протокол аутентифікації не надто жорсткий, то користувачеві надаються додаткові періодичні спроби аутентифікації.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Русин Б. П., Варецький Я. Ю. Біометрична аутентифікація та криптографічний захист. Львів: Коло, 2010. 287 с.
2. Галатенко В. А. под ред. академика РАН В. Б. Бетелина Основы информационной безопасности: учебное пособие, 4-е изд. Москва: Интернет-Университет Информационных технологий; Бином. Лаборатория знаний, 2008. 205 с.
3. Ахрамович В. М. Ідентифікація й аутентифікація, керування доступом // *Сучас. захист інформації*. 2016. №4. С. 47-51.
4. Сачанюк-Кавецька Н.В. Кодування як засіб захисту інформації у системах контролю доступу з використанням логіко-часових функцій у формі поліномів і біометричних даних суб'єктів. *Реєстрація зберігання і оброблення даних.* 2018. Том 20, №2. С. 60-68.
5. Заяць В.М. Построение и анализ модели дискретной колебательной системы. *Кибернетика и системный анализ*. 2000. С. 161–165.

Бондаренко Ірина Олексіївна – студент групи УБ-15б, факультет менеджменту та інформаційної безпеки, Вінницький національний технічний університет, м.Вінниця

Науковий керівник: ***Сачанюк-Кавецька Наталія Василівна –*** к.т.н., доцент, доцент каф. ВМ Вінницького національного технічного університету, м.Вінниця, e-mail: skn1901@gmail.com

Bondarenko Iryna O. – student of UB-15b group, Department of Management and Information Security, Vinnytsia National Technical University, Vinnytsia

Supervisor: ***Sachaniuk-Kavets'ka Natalia V.*** – Candidate of Technical Sciences, Associate Professor, Associate Professor the department of Higher mathematics Vinnytsia National Technical University, Vinnytsia, e-mail: skn1901@gmail.com