УДК 621.384.3

Шрамко В. Ю.
Бондаренко О. В.
Сачанюк-Кавецька Н. В.

Практична реалізація удосконаленого методу аутентифікації користувачів WEB–ресурсу з використанням клавіатурного почерку

Вінницький національний технічний університет

Анотація. В даній доповіді розглядається можливий варіант практичної реалізації удосконаленого методу аутентифікації суб'єктів з використанням клавіатурного почерку. Подано схему блоку аутентифікації користувачів Web-ресурсів та особливості використання сторінки запису почерку.

Ключові слова: аутентифікація, клавіатурний почерк, блок аутентифікації,біометричні характеристики

Abstract. In this report, a possible version of the practical implementation of the advanced method of authentication of subjects using the keyboard handwriting is considered. The scheme of the block of authentication of users of Web-resources and the features of the use of handwriting page are presented.

Keywords: authentication, keyboard handwriting, authentication block, biometric characteristics

З розвитком новітніх технологій проблема інформаціної безпеки набуває все більшої актуальності [1]. Традиційні методи аутентифікації, що базуються на використанні карток, електронних ключів чи інших переносних ідентифікаторів, а також паролів і кодів доступу мають суттєві недоліки. Головним недоліком таких методів є неоднозначність ідентифікованої особи, з використанням атрибутивних розпізнавальних характеристик.

Останнім часом, все більшої популярності набуває біометрика у галузі інформаційної безпеки [2], як форма управління ідентифікаторами доступу та контролю доступу. Як самостійна наука, біометрія виникла в кінці 19-го століття в роботах Ф. Гальтона, який зробив великий внесок у створення кореляційного та регресійного аналізу, та К. Пірсона — засновника найбільшої біометричної школи. Біометричні системи можуть працювати в двох режимах: веріфікації, завдання якої звірити відповідність вимірюваної біометричної характеристики записаному шаблону заявленого індивідуума, та ідентифікації, при якій вимірюється біометрична характеристика, що буде порівнюватися з базою раніше записаних шаблонів усіх «відомих» об'єктів.

Біометричні дані можна розподілити на два основні 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, тоб-то побудовані на особливостях, які характерні для підсвідомих рухів у процесі відтворення якої-небудь дії (за почерком, за клавіатурним почерком, за голосом тощо) [3] .

Огляд особливостей методу аутентифікації операторів за клавіатурним почерком дозволяє виділити чотири основні математичні підрахунки підходу до вирішення задачі розпізнавання клавіатурного почерку [4]:

– статистичний (при реєстрації користувачів в системи відбувається збір статистики у вигляді обчислюваних параметрів особливостей динаміки роботи на клавіатурі. Після чого проводиться усереднення динамічних даних. В режимі аутентифікації користувач знову вводить ключову фразу, яка порівнюється з отриманим біометричним еталоном. Порівняння здійснюється шляхом обчислення із допомогою обраного критерію міри близькості введеної ключової фрази і біометричного зразка);

– ймовірнісно-статистичний (час натискання клавіш і пауз при наборі тексту на клавіатурі розглядаються як імовірнісні події. Практично доведено, що значення часу утримання і пауз між утриманнями клавіш розподілені за законом, який наближено можна вважати нормальним законом розподілу);

– на базі теорії розпізнавання образів і нечіткої логіки;

– на основі нейромережевих алгоритмів.

Для спрощення використання WEB-ресурсу пропонуємо аутентифікацію проводити за клавіатурним почерком під час введення пароля користувача (статистичний підхід), що заощадити ресурси обладнання. Однак, слід відмітити, що після кожної зміни пароля користувачем потрібно оновлювати параметри почерку.

Схему блоку аутентифікації користувача наведено на рисунку 1.

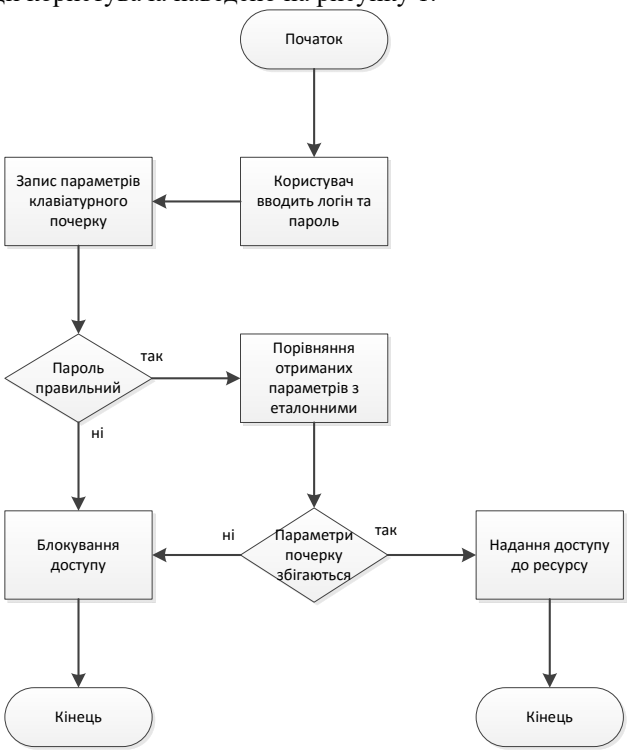

Рисунок 1 – Схема блоку аутентифікації користувача

При авторизації у WEB- додатку під час введення паролю, 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. Окрім блокування доступу можливе виконання додаткових дій. Наприклад, відправлення електронного листа або sms-повідомлення про невдалу спробу аутентифікації. Принцип роботи системи клавіатурного моніторингу WEB-ресурсу аналогічний принципу роботи системи динамічної ідентифікації, за винятком зміни блоку виділення вхідного сигналу. На етапі обробки і перетворення вхідного сигналу в інформаційні системи клавіатурного моніторингу WEB-ресурсу додані фільтри для виділення корисного вхідного сигналу.

В якості фрази для збору параметрів клавіатурного почерку виступає пароль користувача від облікового запису. Тому, для інтеграції алгоритму аутентифікації, необхідно віслідковувати натискання клавіш під час введеня пароля. Для цього до форми входу користувача, а саме до поля введення пароля, потрібно підключити javascript функцію: onkeyup="javascript:keypress('password')".

Код поля з підключеною функцією:

```
<input type="password" class="form-control" onkeyup="javascript:keypress('password')" name="password"
placeholder="Введіть пароль">
```

Коли курсор знаходиться в даному полі, усі натискання будь-яких клавіш фіксуються та обробляються функцією «keypress (d, no)», яка має наступний вигляд:

```
function keypress (d,no)
 {
  var x=document.getElementById(d);
  var t=document.getElementById("demo");
  var evt = event || e; // for trans-browser compatibility
     var charCode = evt.which || evt.keyCode;
  d=new Date();
  curr=d.getTime();
  }
```

Дана функція відслідковує час натискання клавіш та час пауз між ними. Після цього визначається тривалість натискання. За реєстрацією у додатку користувачеві пропонується підняти рівень захисту свого облікового запису методом аутентифікації за клавіатурним почерком (для цього потрібно додати параметри свого почерку).

Для запису свого клавіатурного почерку в систему було розроблено сторінку запису почерку, яка містить шість текстових полів для вводу пароля:

```
<input type="password" onkeyup="javascript:keypress('date1',1)" name="id1"><p id="date1">0</p><br>
<input type="password" onkeyup="javascript:keypress('date2',2)"name="id2"><p id="date2">0</p><br>
<input type="password" onkeyup="javascript:keypress('date3',3)" name="id3"><p id="date3">0</p><br>
<input type="password" onkeyup="javascript:keypress('date4',4)" name="id4"><p id="date4">0</p><br>
<input type="password" onkeyup="javascript:keypress('date5',5)" name="id5"><p id="date5">0</p><br>
<input type="password" onkeyup="javascript:keypress('date6',6)" name="id6"><p id="date6">0</p><br>
```

До кожного з цих полів підключена javascript функція «keypress (d, no)», яка фіксує усі натискання будь-яких клавіш для кожного з полів окремо. Користувачеві необхідно ввести свій пароль в звичних для себе манері та темпі в кожне з шести полів по черзі. Натискання клавіші «backspace» не допускається задля отримання максимально достовірних параметрів. Якщо користувач зробив помилку, йому доведеться оновити сторінку та почати процес запису клавіатурного почерку спочатку. Також додано перевірку на випадок, якщо користувач зробив помилку під час вводу пароля в одне з полів та не помітив цього. Якщо помилки під час введення відсутні – алгоритм проаналізує дані за клавіатурним почерком для кожного з полів та занесе їх в базу даних. При наступній спробі користувача увійти в свій обліковий запис, дані почерку будуть порівнюватись з еталонними. Якщо параметри почерку не співпадають – доступ до додатку блокується.

Аутентифікація за клавіатурним почерком здійснюється з використанням евклідової відстані. Даний метод має досить високу надійність, динамічне визначення допусків, а також адаптивну модель, що підвищує відмовостійкість системи.

Евклідова відстань визначається за формулою:

$$\sqrt{(p_1 - q_1)^2 + (p_2 - q_2)^2 + ... + (p_n - q_n)^2} = \sqrt{\sum_{i=1}^{n} (p_i - q_i)^2} \cdot \quad (1)$$

Після введення пароля користувачем та авторизації у WEB-додатку, за умови наявності клавіатурного почерку користувача у базі даних, запускається процес аутентифікації користувача. Спочатку дані відповідного користувача шукаються в базі, далі перевіряється цілісність та достовірність даних.

Для параметрів почерку визначається евклідова відстань між еталонними та отриманими параметрами. Отриманий результат порівнюється з максимально допустимим відхиленням. Якщо результат не перевищує відхилення – надається доступ до ресурсу, в іншому випадку доступ користувачеві блокується.

Щоб зайти у свій профіль в розробленому WEB-додатку, необхідно на головній сторінці натиснути кнопку «Вхід», після чого відобразиться форма входу існуючого користувача (рис 2).

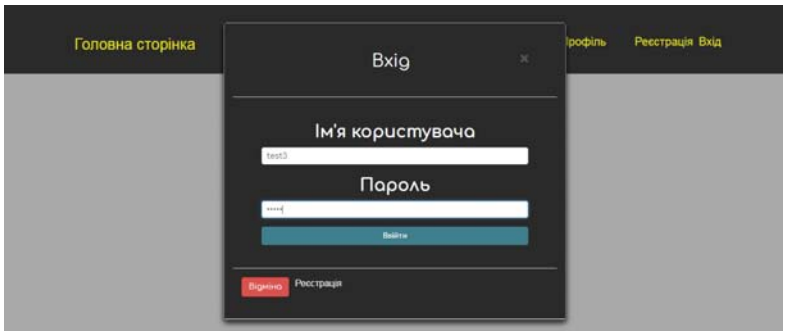

Рисунок 2 – Форма входу користувача

В даній формі наявні два текстових поля, в які потрібно ввести свої ім’я та пароль, після чого натиснути кнопку «Ввійти». Якщо це перша спроба входу користувача в свій обліковий запис, буде відображено повідомлення з пропозицією підвищити рівень захисту облікового запису за допомогою аутентифікації за клавіатурним почерком.

Далі відкриється сторінка облікового запису (рис. 3). На цій сторінці можна подивитись дані за результатами останньої спроби аутентифікації та перейти на сторінку запису клавіатурного почерку (рис. 4), натиснувши відповідне посилання.

Рисунок 3 – Сторінка облікового запису

Рисунок 4 – Сторінка запису клавіатурного почерку

На даній сторінці користувачеві необхідно в кожне поле ввести свій пароль для визначення параметрів клавіатурного почерку, після чого натиснути кнопку «Відправити дані». Якщо користувач зробить помилку та спробує її виправити за допомогою клавіші «backspace», його буде повідомлено про необхідність почати процес запису клавіатурного почерку спочатку. У випадку, коли користувач зробить помилку в одному з полів та не помітить цього, після натискання кнопки «Відправити дані» його буде повідомлено про наявність помилки та необхідність почати процес запису клавіатурного почерку спочатку. Якщо помилки відсутні, користувача буде повідомлено про успішний запис параметрів його почерку в базу даних. У випадку негативного результату аутентифікації (про що користувача буде повідомлено), відкриється головна сторінка, а доступ до облікового запису надано не буде.

СПИСОК ВИКОРИСТАНОЇ ЛІТЕРАТУРИ

1. Данилюк І. І., Карпінець В. В., Приймак А. В., Яремчук Ю. Є., Костюченко О. І. Метод ідентифікації користувача за клавіатурним почерком на основі нейромереж. *Реєстрація зберігання і оброблення даних.* 2018. Том 20, №2. С. 68-77.
2. Гнідець Т.Я. Біометрія: сильні та слабкі сторони. *Науковий вісник Львівського державного університету внутрішніх справ*. 2014. № 2. С. 273–282.
3. 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.
4. Суздальцев А.И., Лобанова В. А., Абашин В. Г. Определение психофизического состояния оперативного персонала по клавиатурному почерку на нефтеперерабатывающих мини–заводах. *Нефтегазовое дело*. 2006. С. 1-6.

Шрамко Володимир Юрійович, студент групи УБ-17мі, факультету менеджменту та інформаційної безпеки
Бондаренко Олександр Володимирович, студент групи УБ-15б, факультету менеджменту та інформаційної безпеки
Науковий керівник: Сачанюк-Кавецька Наталія Василівна, к.т.н., доцент, доцент каф. ВМ Вінницького національного технічного університету, skn1901@gmail.com

Shramko Volodymyr Yuriyovych, student group UB-17m, Faculty of Management and Information Security
Bondarenko Olexander Vladimirovich, student group UB-15b, Faculty of Management and Information Security
Supervisor: Sachaniuk-Kavets'ka Natalia, Candidate of Technical Sciences, Associate Professor, Associate Professor the department of Higher mathematics Vinnysia National Technical University, e-mail: skn1901@gmail.com