УДК 004.056.53

[1]Є.О. Башков, д-р техн. наук., проф.,
[2]Т.В. Алтухова, канд. техн. наук,
[3]Є.О. Єжова, магістрантка
Донецький національний технічний університет, м. Луцьк, Україна
[1]yevhen.bashkov@donntu.edu.ua
[2]tetiana.altukhova@donntu.edu.ua
[3]yelyzaveta.yezhova@donntu.edu.ua

Розробка методу аутентифікації користувача на основі клавіатурного почерку

В даній науковій роботі виконано дослідження аутентифікації користувача за клавіатурним почерком під час введення парольної фрази. На основі проведеного аналізу та розробки математичної функції розподілу областей «свої» та «чужі» був створений модуль для фільтрації авторського вводу. Для аутентифікації користувача за клавіатурним почерком при введенні парольної фрази необхідно провести розпізнавання за швидкістю та динамікою введення (проміжками між натисканнями клавіш і їх утримання). Тимчасові часові проміжки між натисканнями на клавіатурі та період утримання (натискання) клавіш дозволяють досить однозначно охарактеризувати почерк роботи користувача на клавіатурі, що підтверджується рядом експериментів, проведених під час дослідження особливостей аутентифікації користувача. Окрім того, метод аутентифікації на основі клавіатурного почерку може бути використаний для захисту від шахраїв, які намагаються отримати несанкціонований доступ до системи, та для віддаленої аутентифікації, коли користувачі знаходяться на відстані від сервера.

Отримані результати дослідження та розроблений програмний модуль можуть використовуватися при створенні гібридної системи керування доступом, яка поєднає в собі два методи аутентифікації – парольний та біометричний. Таким чином, довершена система керування буде забезпечувати посилену, в порівняні з класичної парольною аутентифікацією, процедуру аутентифікації.

Метод аутентифікації на основі клавіатурного почерку має великий потенціал для застосування в сфері кібербезпеки та може бути використаний як ефективний інструмент для забезпечення безпеки систем.

Ключові слова: математична модель, аутентифікація, біометрія, біометричні характеристики, клавіатурний почерк

DOI: 10.31474/1996-1588-2023-1-36-61-68

Вступ

За останню чверть століття, завдяки розвитку технологій, більшість людей придбали розумні електронні пристрої й щодня використовують їх для спілкування, пошуку інформації, торгівлі, банківських та інших операцій. Кожен користувач такого пристрою стикається з процесом аутентифікації кілька разів на день.

Традиційні методи, що засновані на використанні електронних ключів, карток, парольних фраз і кодів доступу, після отримання від користувача даних, зіставляють їх з даними в спеціальній захищеній базі даних, і якщо аутентифікація пройшла успішно, виконується авторизація, яка згодом дозволяє користувачеві працювати в системі.

Основною прогалиною цього методу є неможливість виявити заміну аутентифікованих користувачів, що дозволяє зловмисникам отримати доступ до системних ресурсів, обмежених лише привілеями ідентифікованого користувача [1].

Вищезазначене можна виправити, доповнивши систему захисту біометричними методами аутентифікації, які включають ідентифікацію особи за її унікальними фізичними або поведінковими характеристиками. Серед біометричних методів аутентифікації значну увагу приділено методам, заснованих на динамічному клавіатурному (комп'ютерному) почерку людини через їх доступність та необхідність не купувати додаткових пристроїв введення.

Таким чином, **головна мета** даної роботи є розробка та дослідження методу аутентифікації користувачів задля оптимізації захисту інформації з урахуванням аналізу клавіатурного почерку.

Основне завдання дослідження – аналіз сучасних видів аутентифікації користувачів та подальша розробка методу захисту інформації з урахуванням аналізу клавіатурного почерку.

Огляд існуючих методів та систем аутентифікації за клавіатурним почерком

Перед тим, як створювалась математична модель клавіатурного почерку користувача, проведено аналіз вже розроблених систем клавіатурної аутентифікації, що було наведено в різних наукових працях [2-5], де було виявлено, що до параметрів алгоритмів аутентифікації за клавіатурним почерком належить час утримування та швидкість натискання клавіш, швидкість набору парольної фрази, врахування інтервалів між натисканням клавіш та використання додаткового обладнання, як висновок отримана табл. 1.

В роботі [2] описано алгоритм аутентифікації за клавіатурним почерком в якому враховується швидкість набору фрази та нема потреби використовувати додаткове обладнання, проте всі інші параметри не беруться до уваги.

Таблиця 1 – Аналіз алгоритмів аутентифікації за клавіатурним почерком

Наукова робота / Параметри	1	2	3	4
Час утримання клавіш	-	+	+	+
Швидкість натискання	-	+	-	-
Швидкість набору фрази	+	+	+	-
Інтервали між натисканням	-	+	+	+
Психічний стан	+	-	-	-
Використання додаткового обладнання	-	+	-	+
Порівняння отриманих даних	-	-	+	-

В науковій праці [3] наведено алгоритм в якому не зважають на швидкість натискання клавіш [3].

В дослідженні [5] не враховується швидкість натискання клавіш та набору парольної фрази, а також потребує використання додаткового обладнання.

Як видно з вищевикладеного, немає повністю бездоганної системи, тому постає необхідність розробки удосконаленого методу аутентифікації користувача.

Математична модель клавіатурного почерку користувача

Нехай процес набору тексту користувачем описується функцією (1):

$$\vartheta(t) = \alpha(t) + \beta(t) + \gamma(t), \qquad (1)$$

де $\alpha(t)$ – компонента, що характеризує підсвідомі процеси мислення під час набору тексту;

$\beta(t)$ – компонента, що характеризує свідомі процеси мислення;

$\gamma(t)$ – механічні властивості клавіатури, які впливають на процес набору тексту.

Тоді, відповідно до особливостей комп'ютерного почерку, основна задача системи біометричної аутентифікації користувача полягає в тому, щоб виділити та надалі виявити компоненту $\alpha(t)$, що характеризує підсвідомий процес мислення. Це завдання визначає вихідні дані системи ідентифікації після вимірювання тимчасових характеристик клавіатурного почерку користувача.

Для поставленої проблеми необхідно вибрати компоненти $\beta(t)$ та $\gamma(t)$ із вихідної функції $\vartheta(t)$. Оскільки немає способу змоделювати механіку руху людей, що друкують, очевидно, єдиним прийнятним рішенням є проведення збору статистичних даних клавіатурного почерку великої кількості користувачів і побудова емпіричних залежностей $\beta(t)$ та $\gamma(t)$.

Під час введення парольної фрази ймовірність аутентифікації користувача за інтервалом часу між натисканнями клавіш є більш показовою ознакою клавіатурного почерку користувача, ніж час утримання клавіш.

Це тому, що процес, який користувачі часто використовують для введення коротких повідомлень на клавіатурі, є справжнім підсвідомим процесом мислення, який стабільний до тих пір, поки його не порушує мислення вищого свідомого рівня.

Згідно з наведеним, можна прийти до висновку, що не рекомендується використовувати довгі вирази як парольну фразу в системі аутентифікації користувачів, оскільки це призведе до того, що користувачі почнуть вводити текст «з розумом», що призведе до зниження якості їх аутентифікацію.

Отже, можна сказати, що час утримання клавіш найкраще передає властивості $\beta(t)$ функції $\vartheta(t)$. Вилучення компоненти $\beta(t)$ з функції $\vartheta(t)$ досягається введенням кореляційної функції $\Delta(t)$, яка отримана емпірично на основі аналізу наявної статистики. Оскільки характер кореляційної функції $\Delta(t)$ слід вибирати відповідно до того, як довго користувач працює за клавіатурою, необхідно ввести вхідний параметр L, який визначає відповідність між кореляційною функцією і складовою $\beta(t)$ [6].

Аналіз характеристик клавіатурного почерку одного користувача на різних клавіатурах утворюють незначний розкид ймовірності ідентифікації, що дає підстави пояснити це випадковими причинами.

Отже, цей результат дає можливість стверджувати, що механічні особливості

клавіатури практично не впливають на властивості почерку клавіатури користувача, тому $\gamma(t)$ у виразі (1) можна знехтувати. Враховуючи вищевикладене, можна записати функцію $\vartheta(t, L)$ так:

$$\vartheta(t, L) = \alpha(t) + \Delta(t, L). \quad (2)$$

Очевидно, що клавіатурний почерк користувача може змінюватися з часом. Це можна виразити так, що під час виконання і-го процесу ідентифікації отримується ймовірність ідентифікації p_i, яка на деяке значення ξ відрізняється від математичного сподівання ймовірності m_ρ, отриманого під час попередньої операції ідентифікації користувача.

З огляду на це, можна записати рівняння (2) так:

$$\vartheta(t, L) = \big(\alpha(t) + \Delta(t, L)\big)T(t, L), \quad (3)$$

де $T(t, L)$ – функція кореляції, яка враховує залежні від часу зміни параметрів набору тексту користувачем.

Для розв'язання задачі аутентифікації користувача запропонуємо вектор біометричних параметрів:

$$V = \{t_1^{\text{пауза}}, t_2^{\text{пауза}}, \dots, t_{n-1}^{\text{пауза}}, m^{\text{пауза}}, \beta, s, d_1, d_2\}, (4)$$

де $t_{\text{i}}^{\text{пауза}}$ – час між відпусканням і-ої клавіші та натисканні $(\text{i}+1)$-ої;

$m^{\text{пауза}}$ – нормоване математичне сподівання довжини інтервалів;

β – розкид часу між натисканням двох клавіш;

s – швидкість вводу;

y_1, y_2 – параметри зміни часових інтервалів.

Для вирахування довжини паузі між відпусканням і-ої клавіші та натисканні $(\text{i}+1)$-ої $(t_{\text{i}}^{\text{пауза}})$ та часу утримування $(t_{\text{i}}^{\text{утрим}})$ використовуємо виміряні $t_{\text{i}}^{\text{натиск}}$ та $t_{\text{i}}^{\text{відпуск}}$ – час натискання та відпускання і-ої клавіші відповідно.

$$t_{\text{i}}^{\text{утрим}} = t_{\text{i}}^{\text{відпуск}} - t_{\text{i}}^{\text{натиск}}, \ i = 1 \dots n, \quad (5)$$

$$t_{\text{i}}^{\text{пауза}} = t_{\text{i+1}}^{\text{натиск}} - t_{\text{i}}^{\text{відпуск}}, \ i = 1 \dots (n-1), (6)$$

де $t_{\text{i}}^{\text{утрим}}$ – час утримування і-ої клавіші в натиснутому стані;

$t_{\text{i}}^{\text{пауза}}$ – час паузи між відпусканням і-ої клавіші та натисканням $(\text{i}+1)$-ої;

n – довжина ключової фрази в випадку даної роботи – логіна.

Нормоване математичне сподівання $m^{\text{пауза}}$ виглядає так:

$$m^{\text{пауза}} = \frac{\sum_{i=1}^{n-1} t_{\text{i}}^{\text{пауза}}}{t_{max}^{\text{пауза}}}. \quad (7)$$

Розкид часу між натисканням двох клавіш виглядає наступним чином:

$$\beta = \sqrt{\frac{\sum_{i=1}^{n-1} (\frac{t_{\text{i}}^{\text{пауза}}}{t_{max}^{\text{пауза}}} - m^{\text{пауза}})^2}{n-2}}. \quad (8)$$

Швидкість набору користувачем логіна розраховується як:

$$s = \frac{\sum_{i=1}^{n-1} t_{\text{i}}^{\text{пауза}} + \sum_{i=1}^{n} t_{\text{i}}^{\text{утрим}}}{60}. \quad (9)$$

Для того, щоб простежити зміни інтервалів використовуються два параметри y_1 та y_2. Перед початком їх знаходження потрібно вирахувати різницю між часом наступного та поточного інтервалів.

$$dt_i = t_{\text{i+1}}^{\text{пауза}} - t_{\text{i}}^{\text{пауза}}, i = 1 \dots n-1. \quad (10)$$

Відношення числа позитивних різниць до спільного числа різниць (параметр k_1) визначається наступним шляхом: нехай f – кількість різниць dt_i зі знаком плюс, k – кількість різниць. Тоді відношення має вигляд:

$$y_1 = \frac{f}{k} = \frac{f}{n-1}. \quad (11)$$

Відношення числа змін знака в dt_i до загального числа dt_i (параметр y_2) визначається наступним чином: нехай h – кількість змін знака, а g – максимальне число змін знаків. Тоді відношення кількості змін знака dt_i до загальної кількості dt_i:

$$y_2 = \frac{h}{g} = \frac{h}{n-2}. \quad (12)$$

В результаті отримуємо вектор вхідних параметрів V, що використовується для аутентифікації користувача за клавіатурним почерком при зазначеній довжині парольної фрази.

Практична реалізація запропонованої методики

Система клавіатурної аутентифікації функціонує в режимі настроювання та аналізу.

В режимі настроювання визначаються та зберігаються еталонні параметри клавіатурного почерку користувача, в режимі аналізу система порівнює еталонні параметри з введеними, після чого відбувається вибір з двох гіпотез:

- користувач, котрий вводить логін є авторизованим;
- користувач розпізнаний як не є авторизованим.

В режимі настроювання користувач вводить певну L кількість раз ключову фразу, у випадку даної роботи – логін, тобто проводить етап реєстрації (навчання системи). Ці L логінів користувача відповідають L реалізаціям вектора біометричних параметрів $V = \{V_1, V_2, \dots, V_L\}$.

В режимі аналізу відбувається аутентифікація користувача, котрий ввів логін. Процедури аутентифікації користувача, що надав свої біометричні параметри в вигляді вектора V, можна роздивлятись як задачу класифікації вектора V на $(\text{M}+1)$ класів по числу M зареєстрованих в системі користувачів («свої»), та плюс один клас для інших не зареєстрованих («чужі»).

Однак попередньо зареєстровані в системі біометричні параметри користувача можуть використовуватися як параметри класифікатора.

Це дозволяє привести задачу класифікування вектора V на $(\text{M}+1)$ до задачі

класифікувати тільки на два класи: «свої» – вектор $V_{\text{С}}$та «чужі» – вектор $V_{\text{Ч}}$.

Для класифікації користувачів на два класи «свої» (вектор $V_{\text{С}}$) та «чужі» (вектор $V_{\text{Ч}}$) параметричний класифікатор можна реалізувати з використанням лише однієї функції $g(V)$, знак якої визначатиме належність пред'явленого вектора V до одного з двох класів: $V_{\text{С}}$ і $V_{\text{Ч}}$.

Формування функції $g(V)$, розділяє області «свої» і «всі чужі» проводиться з наступних міркувань.

Нехай у загальному випадку область розподілу біометричних параметрів «свого» користувача задана безліччю зразків ω_C, що складається з векторів $L\, V_{Ci}, i = 1 \ldots L$, нормально розподілених в N-мірному просторі ортогональної системи координат, а кожен вектор $V_{Ci}, i = 1 \ldots L$ представлений своїми N компонентами:

$$V_{Ci} = \{v_1, v_2, \ldots, v_j, \ldots, v_N\}, j = 1 \ldots N. \quad (13)$$

Центр розподілу векторів V_{Ci} розташовується в точці $(\xi_1, \xi_2, \ldots, \xi_N)$, яка визначається N математичними сподіваннями $m_{V1} = \xi_1, m_{V2} = \xi_2, m_{V3} = \xi_3, \ldots, m_{VN} = \xi_N$.

Центральні моменти другого порядку розподілу векторів V_{Ci} утворюють квадратну матрицю моментів (коваріаційну матрицю) [7].

$$Q = \|\lambda_{jk}\| = \left\| \begin{pmatrix} \lambda_{11} & \ldots & \lambda_{1N} \\ \ldots & \ldots & \ldots \\ \lambda_{N1} & \ldots & \lambda_{NN} \end{pmatrix} \right\|, \quad (14)$$

де

$$\lambda_{jk} = M(v_j - \xi_j) \cdot (v_k - \xi_j) = \begin{Bmatrix} \sigma_{ij}^2 \text{ при } j = k \\ cov\{v_j, v_k\} \text{ при } j \neq k \end{Bmatrix} j, k = 1..N.$$

Для нормального закону розподілення N-мірних випадкових корельованих величин, що також називають розподіленням Гауса [8], функція щільності розподілення має вигляд:

$$f(v_1, v_2, \ldots, v_N) = \frac{1}{\sqrt{(2\pi)^N \cdot det\|\lambda_{jk}\|}} e^{\left[-\frac{1}{2}\sum_{j=1}^{N}\sum_{k=1}^{N}\lambda_{jk}\cdot(v_j-\xi_j)\cdot(v_k-\xi_j)\right]}, \quad (15)$$

де $det\|\lambda_{jk}\|$ – визначник коваріаційної матриці Q, коефіцієнти Λ_{jk} утворюють матрицю $\lambda = \lambda_{jk}$, зворотну коваріаційної матриці Q.

Для знаходження коефіцієнтів λ_{jk} використовується стандартна формула [9]:

$$\lambda_{jk} = (-1)^{j+k} \cdot \frac{M_{jk}}{det\|\lambda_{jk}\|}, \quad (16)$$

де M_{jk} – мінор визначника λ_{jk}, що отримується з нього шляхом викреслювання j-го рядка та k-го стовпця.

Гіпереліпсоїд розсіювання має рівну щільність розподілення N-мірних випадкових величин, тому його можна отримати з умови [9]:

$$f(v_1, v_2, \ldots, v_N) = const. \quad (17)$$

Вираз, що фігурує в експоненті функції щільності нормального розподілення векторів V_{Ci} є додатньовизначеною квадратичною формою. Поверхня на якій ця квадратична форма постійна:

$$\frac{1}{2} \cdot \sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk} \cdot (v_j - \xi_j) \cdot (v_k - \xi_j) = const. \quad (18)$$

Позначаючи константу у правій частині виразу (18) через k^2, отримаємо:

$$\frac{1}{2} \cdot \sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk} \cdot (v_j - \xi_j) \cdot (v_k - \xi_j) = k^2. \quad (19)$$

Константа k задає коефіцієнт пропорційності між довжинами a_j головних півосей гіпереліпсоїда та відповідними середньоквадратичними відхиленнями σ_j:

$$a_1 = k \cdot a_1, a_2 = k \cdot a_2, \ldots, a_N = k \cdot a_N. \quad (20)$$

Для оптимального розв'язання задачі класифікації з усіх поверхонь рівних щільностей ймовірностей доцільно вибрати ту, яка характеризує розсіювання векторів V_{Ci} щодо точки $(\xi_1, \xi_2, \ldots, \xi_N)$. Ця поверхня відповідає так званому одиничному гіпереліпсоїду, у якого головні півосі рівні відповідним середньоквадратичним відхиленням $\sigma_1, \sigma_2, \ldots, \sigma_N$, тобто для одиничного гіпереліпсоїда $k = 1$, та вираз (20) перетворюється на вид:

$$\frac{1}{2} \cdot \sum_{j=1}^{N}\sum_{k=1}^{N} \Lambda_{jk} \cdot (v_j - \xi_j) \cdot (v_k - \xi_j) = 1. \quad (21)$$

Через обмежену статистику біометричних зразків, що пред'являються на стадії реєстрації «своїм» користувачем, завжди залишається ймовірність того, що зразок, пред'явлений цим же користувачем при аутентифікації, вийде за межі зафіксованого в ідеалі діапазону.

Для зменшення цієї ймовірності додатково задається величина допуску між областями «свої» та «усі чужі» у вигляді коефіцієнта Стьюдента $C[L, (1 - P_1)]$ (критичні значення, якого наведені в додатку Б для різної довірчої ймовірності Р та числа ступенів свободи L), виходячи із заданої помилки першого роду (імовірність Р1 помилкової відмови «своєму» користувачеві) та числа L, пред'явлених на стадії реєстрації зразків [10].

Введення зазначеного допуску до рівняння (21) призводить до його виду:

$$\frac{1}{2} \cdot \sum_{j=1}^{N} \sum_{k=1}^{N} \Lambda_{jk} \cdot (v_j - \xi_j) \cdot (v_k - \xi_j) = \{C[L, (1 - P_1)]\}^2. \quad (22)$$

Ілюстрація методу поділу областей «свої» від області «всі чужі» для двовимірного простору (N =2) показана на рис. 1.

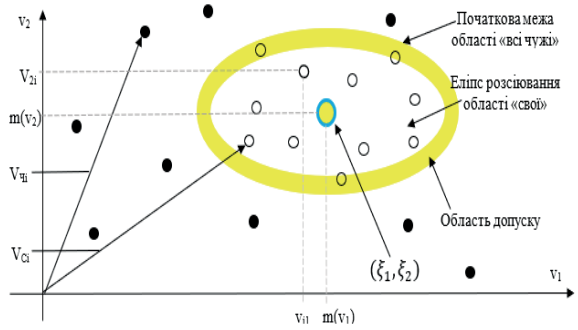


Рисунок 1 – Ілюстрація процесу розподілення

Виходячи з усього вищесказаного, отримуємо, що функції $g(V)$ розділення області «свої» та «всі чужі», використовуючи вираз (122), набуває такого вигляду:

$$g(V) = \frac{1}{2} \cdot \sum_{j=1}^{N} \sum_{k=1}^{N} \Lambda_{jk} \cdot (v_j - \xi_j) \cdot (v_k - \xi_j) = \{C[L, (1 - P_1)]\}^2. \quad (23)$$

Рівняння $g(V) = 0$ у цьому випадку визначатиме шукану поверхню, що розділяє, а знак функції $g(V)$ – приналежність вхідного вектора V до одного з двох класів: «свої» або «чужі» (потрапляння в область «усі чужі»):

$$g(V) < 0, \text{якщо } V \in V_C,$$
$$g(V) > 0, \text{якщо } V \in V_{\text{ч}}.$$

Таким чином, процедура аутентифікації зводиться тепер до перевірки: чи попадає пред'явлений користувачем вектор біометричних параметрів V в область, що описується, виразом (23).

Програмна реалізація системи біометричної аутентифікації за клавіатурним почерком

Аналіз властивостей параметрів клавіатурного почерку користувача проходив у декілька етапів. На першому етапів аналізувався клавіатурний почерк автора даної роботи. Для цього довільну кількість раз вводився логін, який автор використовує вже тривалий термін, зберігаючи кожну спробу вводу.

Введені дані утворили два масиви: перший – інтервали між натисканням клавіш, другий – час утримування клавіш при натиску. Після цього проводився аналіз зібраних параметрів.

На другому етапі аналіз проводився на групі учасників, котрі вводили запропонований автором логін, тобто логін, який вони до цього не знали, для перевірки чи впливає на час вводу попередні навички вводу парольної фрази

Результати проведеного аналізу можна роздивитися на рисунку 2 – для інтервалів між натисканням клавіш та 3 – для часу утримування клавіш при натиску, де різними кольорами вказані зображення 100 варіантів вводу та червоним кольором визначено математичне сподівання.

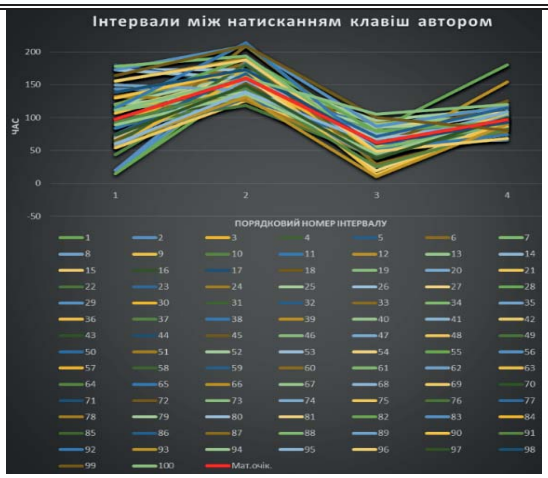


Рисунок 2 – Діаграма часових інтервалів між натисканням клавіш

Клавіатурний почерк характеризує кореляція отриманих даних. Від коефіцієнта кореляції залежать кути нахилу відрізків ламаної лінії діаграми для інтервалів часу між натисканням клавіш автором та часу утримування клавіш автором при натиску.

Оскільки при дослідженні буди побудовані криві вводу для кожної вибірки (100 разів введення логіна), аналізуючи їх можна зробити висновок, що вид ламаної показує характер вводу парольної фрази.

Для кожного учасника були знайдені вибіркові середні всіх інтервалів та часу утримання кожної клавіші.

Рисунок 3 – Діаграма часу утримання клавіш автором

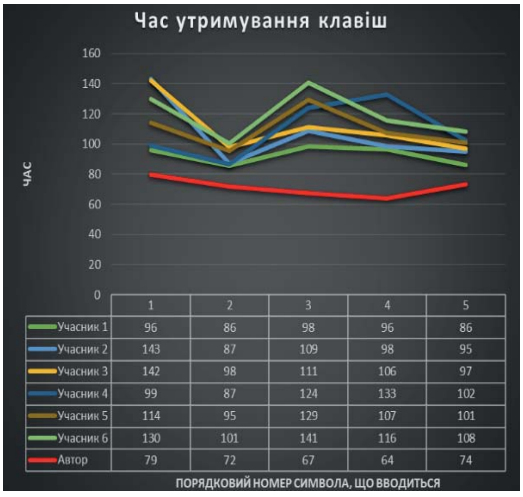
Побудовані діаграми середніх значень для інтервалів між натискання клавіш (рис. 4) та утримання клавіш (рис. 5). На рисунку середні значення автора (еталонні) виділені червоним кольором.

	1	2	3	4
Учасник 1	236	304	148	139
Учасник 2	240	357	181	159
Учасник 3	217	328	174	229
Учасник 4	214	374	295	296
Учасник 5	230	429	354	412
Учасник 6	323	332	457	358
Автор	87	165	98	106

Рисунок 4 – Середні значення часу інтервалів між натисканням клавіш

Як видно з рисунків 4 та 5 отримані дані під час тестування модуля різними учасниками не потрапляють в довірчі інтервали еталонних даних, що дає змогу зробити висновок про те, що клавіатурний почерк кожного користувача є унікальним та непідробним.

Порівнюючи вибіркові дисперсії, приходимо до висновку, що дисперсії практично усіх часових інтервалів для еталонних даних менше ніж дисперсії для «чужих». Це пояснюється тим, що логін, який вводили учасники, був їм не знайомий, для них це довільний набір символів.



	1	2	3	4	5
Учасник 1	96	86	98	96	86
Учасник 2	143	87	109	98	95
Учасник 3	142	98	111	106	97
Учасник 4	99	87	124	133	102
Учасник 5	114	95	129	107	101
Учасник 6	130	101	141	116	108
Автор	79	72	67	64	74

Рисунок 5 – Середні значення часу утримування клавіш

Висновки

Таким чином, за результатами проведеного аналізу можна зробити висновок, що інтервали між натисканням клавіш більш точно показують індивідуальні властивості клавіатурного почерку користувача при введенні логіна.

Для підвищення ефективності аутентифікації слід у вектор біометричних параметрів внести інтервали між натисканням клавіш, нормоване математичне сподівання тривалості цих інтервалів.

Також необхідно внести в вектор параметри, що показують динаміку змін часових інтервалів в процесі набору.

Перспективи подальших досліджень полягають у розробці гібридної системи керування доступом, яка буде поєднувати в собі парольні та біометричні методи аутентифікації. Таким чином, довершена система керування буде забезпечувати посилену, в порівняні з класичної парольною аутентифікацією, процедуру аутентифікації.

Перевагою такої системи є те, що для її використання не потрібно буде закуповувати якесь додаткове обладнання, а також не потрібно значною мірою модифікувати процес аутентифікації.

Недоліком є те, що користувач не може бути під дією психотропних препаратів, алкогольного сп'яніння чи сильно хворий.

Наукова новизна полягає в розробці методу біометричної аутентифікації, шляхом використання клавіатурного почерку, а саме використання унікальних біометричних даних, що дозволило проводити аутентифікацію без необхідності втручання користувача безпосередньо в цей процес.

Практичне значення полягає в авторській розробці методу фільтрації авторського введення від неавторського та програмного модуля реалізації розробленого методу аутентифікації з використанням об'єктно-орієнтованої мови програмування C# на базі використанням інтегрованого середовища розробки Visual Studio.

Список літератури

1. Salem A., Obaidat M. S. A novel security scheme for behavioral authentication systems based on keystroke dynamics. Security and Privacy. 2019. T. 2, № 2. P. 64. URL: https://doi.org/10.1002/spy2.64.
2. Raul N., Shankarmani R., Joshi P. A Comprehensive Review of Keystroke Dynamics-Based Authentication Mechanism. Advances in Intelligent Systems and Computing. Singapore, 2019. P. 149–162. URL: https://doi.org/10.1007/978-981-15-0324-5_13.
3. Tsai C.-J., Shih K.-J. Mining a new biometrics to improve the accuracy of keystroke dynamics-based authentication system on free-text. Applied Soft Computing. 2019. Vol. 80. P. 125–137. URL: https://doi.org/10.1016/j.asoc.2019.03.033.
4. Biometrie authentication using keystroke dynamics / C. Jadhav et al. 2017 International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC), Palladam, Tamilnadu, India, 10–11 February

2017. 2017. URL: https://doi.org/10.1109/i-smac.2017.8058304.
5. Keystroke Biometrics Ongoing Competition / A. Morales et al. IEEE Access. 2016. Vol. 4. P. 7736–7746. URL: https://doi.org/10.1109/access.2016.2626718.
6. Motwani A., Jain R., Sondhi J. A Multimodal Behavioral Biometric Technique for User Identification using Mouse and Keystroke Dynamics. International Journal of Computer Applications. 2015. Vol. 111, no. 8. P. 15–20. URL: https://doi.org/10.5120/19558-1307.
7. Comparison of dynamic biometrie security characteristics against other biometrics / B. Ducray et al. ICC 2017 - 2017 IEEE International Conference on Communications, Paris, France, 21–25 May 2017. 2017. URL: https://doi.org/10.1109/icc.2017.7996938 (date of access: 26.02.2023).
8. Pisani P. H., Lorena A. C. A systematic review on keystroke dynamics. Journal of the Brazilian Computer Society. 2013. Vol. 19, no. 4. P. 573–587. URL: https://doi.org/10.1007/s13173-013-0117-7 (date of access: 26.02.2023).
9. Baig A., Eskeland S. A Generic Privacy-preserving Protocol for Keystroke Dynamics-based Continuous Authentication. 19th International Conference on Security and Cryptography, Lisbon, Portugal, 11–13 July 2022. 2022. URL: https://doi.org/10.5220/0011141400003283.
10. Studying of keystroke dynamics statistical properties for biometrie user authentication / V. Alieksieiev et al. 2018 14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET), Lviv-Slavske, Ukraine, 20–24 February 2018. 2018. URL: https://doi.org/10.1109/tcset.2018.8336264.

References

1. Salem, A., Obaidat, M. S. (2019), "A novel security scheme for behavioral authentication systems based on keystroke dynamics", *Security and Privacy*, 2(2), pp. 64, available at: https://doi.org/10.1002/spy2.64.
2. Raul, N., Shankarmani, R. та Joshi, P. (2019), "A comprehensive review of keystroke dynamics-based authentication mechanism", *Advances in intelligent systems and computing*, available at: https://doi.org/10.1007/978-981-15-0324-5_13.
3. Tsai, C.-J. та Shih, K.-J. (2019), "Mining a new biometrics to improve the accuracy of keystroke dynamics-based authentication system on free-text", *Applied Soft Computing*, Vol. 80. pp. 125–137, available at: https://doi.org/10.1016/j.asoc.2019.03.033.
4. Jadhav, C. et al. (2017), "Biometrie authentication using keystroke dynamics", *International Conference on I-SMAC (IoT in Social, Mobile, Analytics and Cloud) (I-SMAC)*. Palladam, Tamilnadu, India, available at: https://doi.org/10.1109/i-smac.2017.8058304.
5. Morales, A. et al. (2016), "Keystroke Biometrics Ongoing Competition", *IEEE Access*, Vol. 4. pp. 7736–7746, available at: https://doi.org/10.1109/access.2016.2626718.
6. Motwani, A., Jain, R. та Sondhi, J. (2015), "A Multimodal Behavioral Biometric Technique for User Identification using Mouse and Keystroke Dynamics", *International Journal of Computer Applications*, Vol. 111, No. 8, pp. 15–20, available at: https://doi.org/10.5120/19558-1307.
7. Ducray, B. et al. (2017), "Comparison of dynamic biometrie security characteristics against other biometrics", *ICC 2017 - 2017 IEEE International Conference on Communications*. Paris, France, available at: https://doi.org/10.1109/icc.2017.7996938.
8. Pisani, P. H., Lorena, A. C. (2013,) "A systematic review on keystroke dynamics", *Journal of the Brazilian Computer Society*, Vol. 19, No. 4, pp. 573–587, available at: https://doi.org/10.1007/s13173-013-0117-7.
9. Baig, A., Eskeland, S. (2022), "A Generic Privacy-preserving Protocol for Keystroke Dynamics-based Continuous Authentication", *19th International Conference on Security and Cryptography*. Lisbon, Portugal, available at: https://doi.org/10.5220/0011141400003283.
10. Alieksieiev, V. et al. (2018), "Studying of keystroke dynamics statistical properties for biometrie user authentication", *14th International Conference on Advanced Trends in Radioelecrtronics, Telecommunications and Computer Engineering (TCSET)*. Lviv-Slavske, Ukraine, available at: https://doi.org/10.1109/tcset.2018.8336264.

Надійшла до редакції 28.01.2022

[1]Y. BASHKOV, [2]T. ALTUKHOVA, [3]Y. YEZHOVA
Donetsk National Technical University, Lutsk, Ukraine
[1]yevhen.bashkov@donntu.edu.ua
[2]tetiana.altukhova@donntu.edu.ua
[3]yelyzaveta.yezhova@donntu.edu.ua

DEVELOPMENT OF A USER AUTHENTICATION METHOD BASED ON KEYBOARD HANDWRITING

In this research paper, a study of user authentication by keyboard handwriting when entering a passphrase is performed. Based on the analysis and development of a mathematical function for the distribution of "own" and

"foreign" areas, a module for filtering the author's input was created. To authenticate a user by keyboard handwriting when entering a passphrase, it is necessary to recognize the speed and dynamics of input (gaps between keystrokes and their retention). The time intervals between keystrokes and the period of keystroke hold allow us to characterize the user's handwriting on the keyboard quite unambiguously, which is confirmed by a number of experiments conducted during the study of user authentication features. In addition, the authentication method based on keyboard handwriting can be used to protect against fraudsters trying to gain unauthorized access to the system and for remote authentication when users are at a distance from the server.

The results of the study and the developed software module can be used to create a hybrid access control system that combines two authentication methods - password and biometric. Thus, the final control system will provide an enhanced authentication procedure compared to classical password authentication.

The keyboard handwriting authentication method has great potential for use in the field of cybersecurity and can be used as an effective tool to ensure system security.

Keywords: mathematical model, authentication, biometrics, biometric characteristics, keyboard handwriting