INFORMATION SECURITY

DOI: 10.20535/2411-1031.2018.6.2.153487
UDC 004.056.53

VIKTOR YEVETSKYI,
IVAN HORNIICHUK

ANALYSIS OF STABILITY OF THE USER'S KEYBOARD HANDWRITING CHARACTERISTICS IN THE BIOMETRIC AUTHENTICATION SYSTEMS

Consideration is given to the use of biometric characteristics in order to increase the efficiency of user authentication. An identifier that uses biometric characteristics is inextricably linked to the user, and it is virtually impossible to use it unauthorized. As a biometric characteristic it is expedient to use a keyboard handwriting. Keyboard handwriting, or rhythm of typing, displays a way of typing on a keyboard that is specific to a particular user. In addition, it is quite simple to implement and does not require additional hardware costs. Moreover, the use of keyboard writing when entering a password eliminates the main disadvantages of classical password systems and systems based on access cards. The focus of the research was on the sustainability of the time characteristics of the keyboard handwriting of a particular user over a long period of time. To implement the admission of the user to the computer system, an algorithm based on the Heming distance is selected. According to the chosen algorithm an algorithm for forming a vector of biometric characteristics of the user is developed, which includes the duration of holding a specific key and the time between pressing the neighboring keys. An algorithm for forming a user's biometric standard is developed. To analyze the use of keyboard handwriting, software applications that implement the user's access based on keyboard handwriting were developed, as well as a program for collecting time characteristics. Both applications use the developed algorithms. To study the constancy of handwriting time characteristics, an empirical study was conducted. For this purpose, a group of individuals is selected, each of which has a computer input at an adequate level. They all entered the proposed phrase within a year. The obtained statistical data, on the basis of which, the average values and values of the average square deviation of the time characteristics of keyboard handwriting at the various time intervals are calculated. Estimated probability of correct user recognition by its frequency in n independent experiments. As a result of the study, the persistence of user keyboard handwriting as a biometric characteristic for use in computer data protection systems, in particular, authentication systems, was analyzed.

Keywords: authentication, biometric user authentication, biometric characteristics, keyboard handwriting, biometric authentication system.

Problem Statement. Access control systems are used to protect computer data from unauthorized access. When managing access, the authentication and authentication procedures should ensure the correspondence between the user and his identifier, which prevents unauthorized access to information. The most widespread is password authentication thanks to the simplicity of implementation and use. However, this method has a significant disadvantage, which is that password-guessing in the classic password system compromise the entire system.

Authentication systems using a unique object (smart cards, tokens) are equally vulnerable to compromise, in particular by theft or tampering of these items.

To improve the authentication efficiency, it is advisable to use additional features specific to a particular user – its biometric characteristics. Systems that use biometric characteristics of a user are called biometric authentication systems. By biometric characteristics of a person distinguish two separate categories of biometric systems of user authentication of information systems based on biometric characteristics – static and dynamic. The first category of methods involves the

development of biometric authentication systems that analyze the static, invariant characteristics of the person, which include fingerprints, face or hands, DNA, and others. The second category includes biometric systems that analyze the dynamic, behavioral characteristics of the person. They are based on the study of human voice, the dynamics of writing text using a handwritten or keyboard user's handwriting.

Systems that use biometric characteristics of the user are virtually devoid of the drawbacks of traditional authentication systems, since the identifier is inextricably linked to the user and unauthorized use of it is virtually impossible. As a biometric characteristic, it is advisable to use the keyboard user's handwriting [1] - [4].

Analysis of recent researches and publications. Keyboard writing as a biometric characteristic refers to dynamic characteristics that describe subconscious actions that are common to users. Keyboard handwriting or rhythm printing shows the way a user types a text. As the unique information inherent in one or another user, one can note the following most typical features [1], [3]:

- intervals between key presses;
- key hold time;
- number of overlaps between keys;
- degree of arrhythmia of the typing;
- speed of typing;
- the number of errors when typing.

The advantages of systems based on keyboard handwriting are as follows [5], [6]:

- lack of additional hardware for implementation;
- ease of implementation;
- software-based implementation;
- high speed decision-making on the truth of the user;
- an attacker can not log in with a valid password;
- it is impossible to override passwords by the method of brute force.

While the disadvantages of systems are based on keyboard handwriting are next [5]-[10]:

- commercial solutions such as BioPassword® for Enterprise Networks and B-Identified ™ Professional are focused on large computer systems requiring powerful hardware resources and skilled personnel. They are costly because they are geared towards the needs of a large business;
- both commercial and scientific solutions do not provide source code, so it's impossible to test them for undocumented features, and the presence of vulnerable or malicious code;
- there are no studies about the persistence of the user's keyboard typing for a long time. Existing studies do not accentuate this attention. However, without this, it is impossible to make constructive recommendations regarding the effective use of such systems.

The article goal is to analyze the stability of the user's keyboard handwriting characteristics in the biometric authentication systems. It is achieved by solving such individual tasks:

1. Analyze existing approaches, recent research and publications.
2. To analyze the stability of the user's keyboard handwriting characteristics.
3. Evaluate the results and develop recommendations for the creation and updating of the user's biometric standard.

The main material research. In fig. 1 shows a generalized scheme of work of biometric authentication systems [1]. All biometric systems operate in two modes: training and decision making. The main processes of the training mode are the formation of a vector of biometric characteristics and the formation of a user's biometric standard on its basis. The main processes of the decision-making mode are the formation of a vector of biometric characteristics and a decision based on the user's standard and the given vector.

Among the most used decision-making algorithms, the following can be noted [6]:

- algorithm for user recognition based on access control to the domain of reference samples.

– algorithm for making decisions based on the use of neural networks.

The main disadvantages of these algorithms is that [3], [6]:

– the learning process is quite labor intensive;
– to study, a large number of samples of biometric characteristics of users is required.

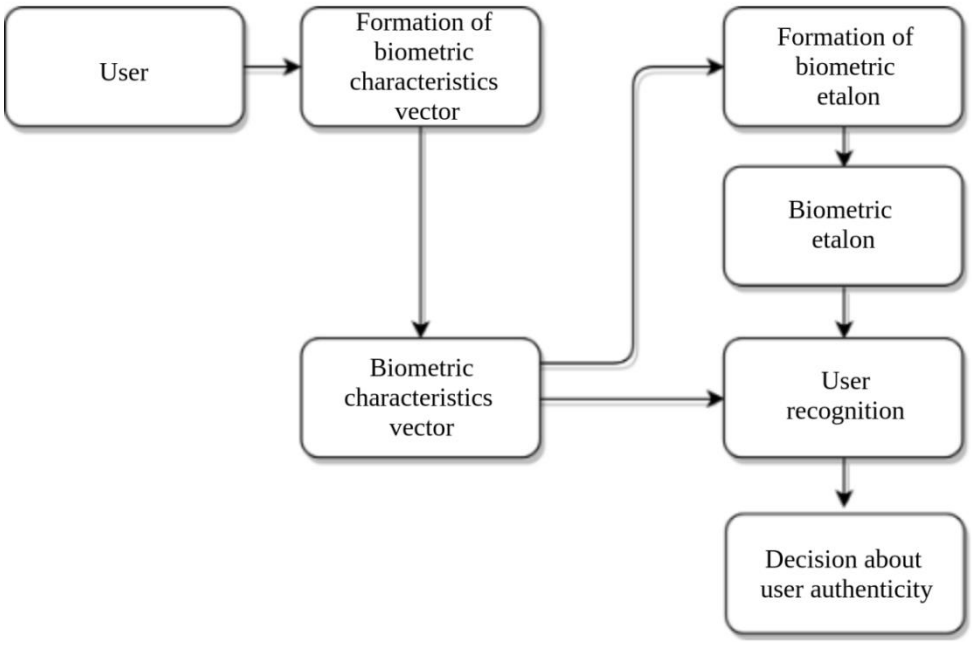

Figure 1 – Generalized scheme of biometric authentication systems

Therefore, to develop a software module, it was decided to use a user recognition algorithm based on the Hamming distance, which is devoid of these drawbacks. Hamming distance is the number of positions in which the corresponding characters of two words of the same length are different [8].

In a more general case, Hamming's distance is applied to rows (vectors) of the same length and serves as a metric of difference (a function that allows determining the distance in a metric space) of objects of the same dimension.

According to the chosen user recognition algorithm, an algorithm for forming a vector of biometric parameters (the time of holding the key for the password and the time between pressing the neighboring keys) is formed. The general view of the vector is the following:

$$v = (t_1, \tau_1, t_2, \tau_2, ..., \tau_{n-1}, t_n)$$

$$t_i = T_i^{up} - T_i^{down}$$

$$\tau_i = T_i^{down} - T_{i-1}^{up}$$

where t_i – hold time of *i* key;

τ_i – the time between pressing the *i* and *(i + 1)* keys;

T^{down} – key press time;

T^{up} – key release time.

The hold time is defined as the time difference between the moment of pressing and releasing the *i*-th key. The interval between clicks corresponds to the difference between the moment of releasing the *i*-th key and pressing the *(i + 1)*-th keys. The general form of the biometric characteristics benchmark for the selected user recognition algorithm is formed. It is formed as confidence intervals for certain time parameters, and the maximum allowable Hamming distance, between the standard and provided during the authentication of the vector time characteristics.

The standard of biometric characteristics has the form:

$$V_e = (\min(t_1), \max(t_1), \min(t_2), \max(t_2), ..., \min(t_N), \max(t_N), E_p),$$

$$\min(t_i) = m(t_i) - T[L,(1-p)]\cdot\sigma(t_i),$$
$$\max(t_i) = m(t_i) + T[L,(1-p)]\cdot\sigma(t_i),$$
$$E_p = m(E_v) + C[L,(1-p)]\cdot\sigma(E_v)$$

where $m(t_i)$ – mathematical expectation of the *i*-th time parameter;

$\sigma(t_i)$ – its mean square deviation;

$m(E_v)$ and $\sigma(E_v)$ – respectively, the mathematical expectation and the mean square deviation for the Hamming distance for each vector;

$T[L,(1-p)]$, $C[L,(1-p)]$ – Student's ratios, with L – degrees of freedom and p – the probability of a *1*-type error.

The decision on the truth of the user is as follows. The user is considered true if [6]:

$$E_v \le E_p,$$

where E_v – Hamming distance from the given vector, to the standard;

E_p – threshold for Hamming's measure for this user.

$$E_v = \sum_{i=1}^{N} e_i,$$
$$E = (e_1, e_2, e_3, ..., e_N),$$
$$e_i = \begin{cases} 0, t_i \in [\min(t_i), \max(t_i)] \\ 1, t_i \notin [\min(t_i), \max(t_i)] \end{cases}$$

where E – Hamming's vector;

e_i – the distance between the corresponding parameters of the given time vector and the user's standard;

t_i – *i*-th time parameter of vector of biometric characteristics.

Thus, the user finds true when the Hamming distance from the given biometric vector to the standard is less than the threshold. When making a decision on the truth of the user formed a Hamming vector whose parameters are units in the case when the time parameter is not included in the confidence interval and zeros if it is included. The Heming distance is the number of units in the Hamming vector. To analyze the use of keyboard handwriting, software applications that implement the user's access based on keyboard handwriting [14], [15], as well as a program for collecting handwriting time characteristics, have been developed.

Analysis of the dependence of the characteristics of the keyboard handwriting on time. To study the constancy of handwriting a group of individuals is selected, all of them have a computer input at an adequate level. All participants introduced the proposed phrase averagely 3 times a week. Thus, the time characteristics of the keyboard handwriting of the group of users for the year were received in the amount of 144 results per user.

The experimental statistical material is obtained - the vectors of the time parameters of the keyboard handwriting of the participants of the study when entering the same text (access password). According to [13], the optimal length of the control phrase is from 8 to 20 characters; for such parameters the authenticity probability is the highest. The length of the text in the study was 15 characters. This means that the dimension of the Hemming's vector will be 29 (15 parameters that reflect the duration of the text key hold; 14 - the duration of intervals between pressing adjacent keys). It is advisable to analyze separately the length of the hold of the keys, and the intervals between their presses. Based on the accumulated material, the average values and mean values of the average square deviation of the time characteristics of keyboard writing for different periods of time (day, week, month, year) are calculated. The calculated values allow us to draw conclusions about the sufficient stability of the time characteristics of the user's keyboard

handwriting over a long period of time. For example, in Fig. 2 shows the dynamics of changing the average key hold duration per week and the average value of the interval between keystrokes a week for a year for each participant in the study.

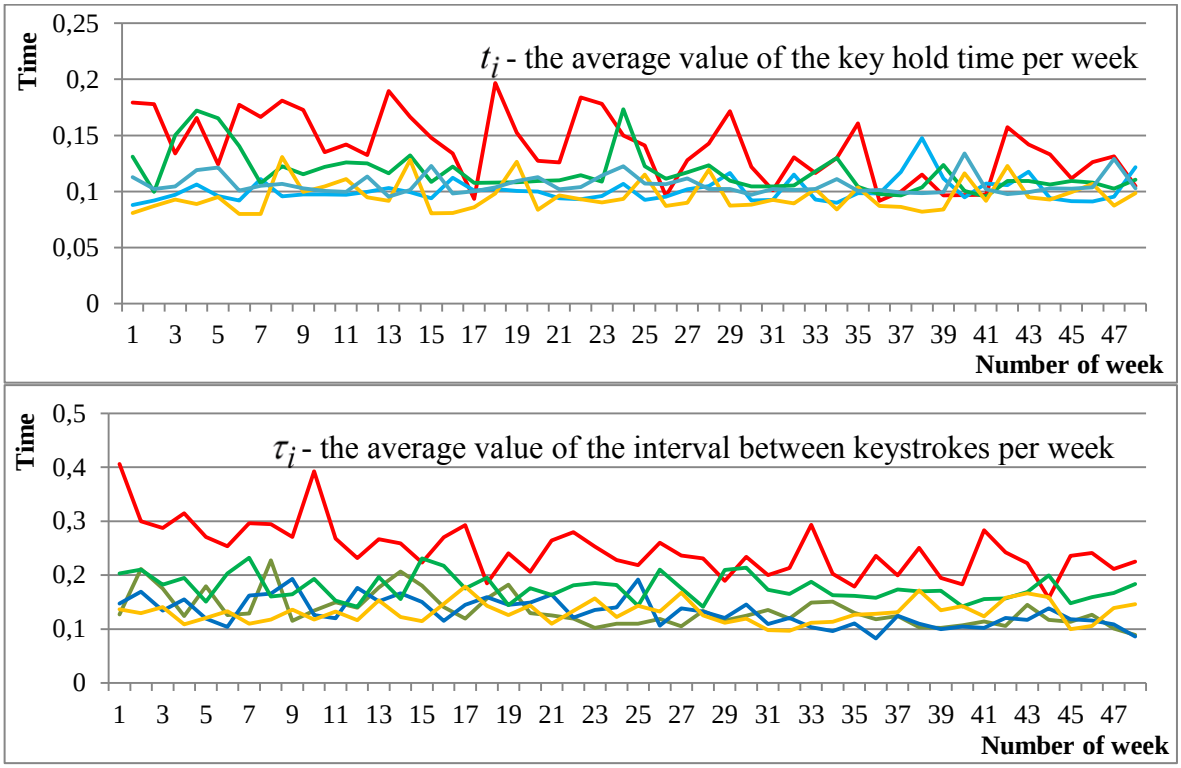

Figure 2 – Dynamics of changes in the average key hold duration per week and the average value of the interval between keystrokes per week for a year for each participant in the study

The data obtained allows us to assume that the duration of key holdings and the intervals between keystrokes received during the year do not have a pronounced trend to increase or vice versa decrease its value.

Research results. Figure 3 shows the dynamics of the change in the value of the Heming distance to the biometric standard of the two participants in the study, for which the threshold value of the Heming distance are significantly different. On the abscissa axis, the number of vector of biometric parameters is deferred (corresponds to the number of the day when the vector was obtained), and the ordinate axis is the value of the Heming measure, which is the number of "no hits" of the time parameter of the vector of biometric characteristics in the confidence interval of the standard. The red color displays the function of changing the value of the Heming measure from time $E_v(t)$, and the blue one - its threshold for the given user E_p.

Each value of Heming's measure, which is more than a threshold, is regarded as a denial of the true user in access to the system. As a result of the received results, the number of errors when entering the password during the year, practically does not increase. After analyzing the same graphs for each participant in the experiment, the number of failures was calculated and the experimental frequency of the correct access to the system for the true user was calculated. Typical values for a user group are shown in the tabl. 1.

Let's evaluate the probability p of the correct user recognition by its frequency in n independent experiments [12]. The average value of the frequency of correct user recognition in a series of 144 experiments is 0.96. Define a 90% confidence interval for probability.

The applicability of the normal distribution law is estimated by the values np and nq [12]. Assuming it is roughly $p \approx p^*$ we obtain:

$$np \approx np^* = 112;$$

$$nq \approx n(1-p^*) = 6;$$

where n – number of experiments;

p* – average admission rate;

q – average frequency of false deny.

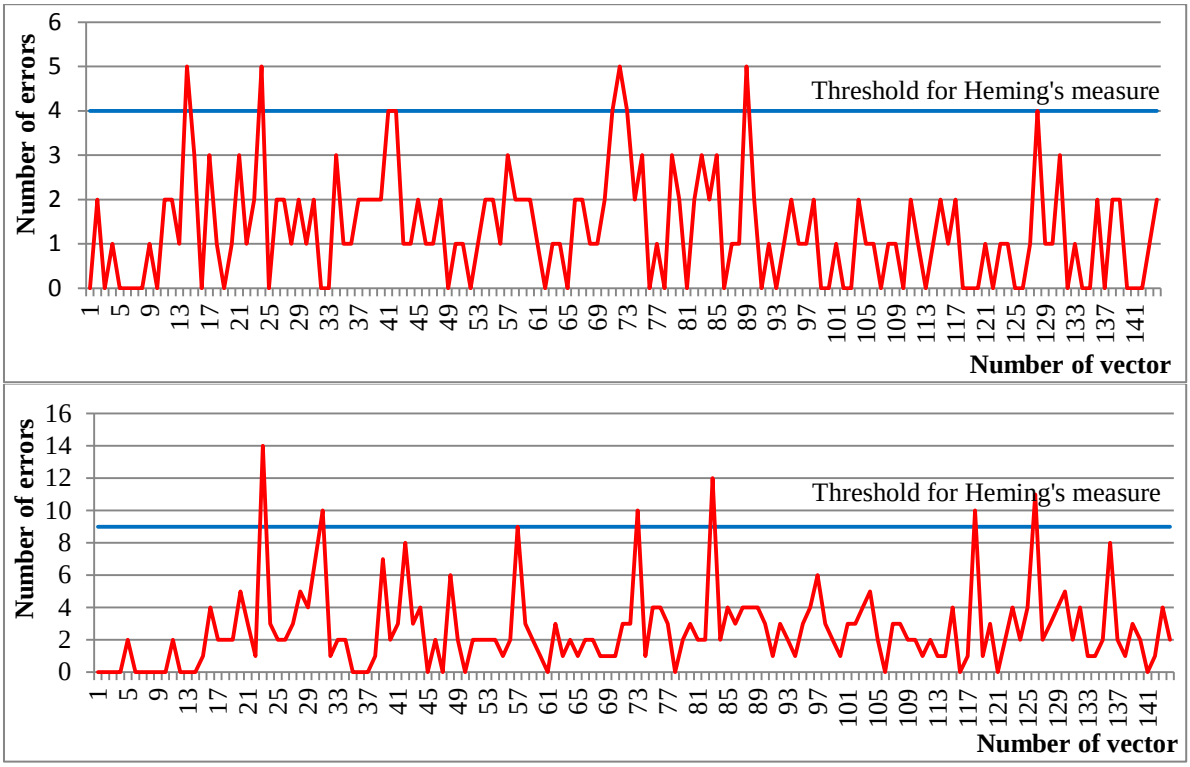

Figure 3 – Dynamics of changing the value of Heming distance to the biometric standard of two participants in the study

Table 1 – The number of failures to access the computer system to the true user

No of paticipant	Number of false authentication failures	Frequency of false deny	Frequency of access permission
1	4	0,027778	0,972222
2	6	0,041667	0,958333
3	4	0,027778	0,972222
4	6	0,041667	0,958333
5	3	0,020833	0,979167

The obtained values give grounds to diminish that the normal distribution law can be applied in this case. For the tables given in [12], for $\beta = 0{,}9$ we find $t_\beta = 1{,}643$. Then we compute p_1 and p_2 by the following formulas:

$$p_1 = \frac{p^* + \frac{1}{2}\frac{t_\beta^2}{n} - t_\beta\sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1 + \frac{t_\beta^2}{n}};$$

$$p_2 = \frac{p^* + \frac{1}{2}\frac{t_\beta^2}{n} + t_\beta\sqrt{\frac{p^*(1-p^*)}{n} + \frac{1}{4}\frac{t_\beta^2}{n^2}}}{1 + \frac{t_\beta^2}{n}};$$

$$p_1 = \frac{0{,}96 + \frac{2{,}7}{288} - 1{,}643\sqrt{\frac{0{,}96*0{,}04}{144} + \frac{2{,}7}{82944}}}{1 + \frac{2{,}7}{144}} = 0{,}969 - 0{,}02 = 0{,}949 \approx 0{,}95;$$

$$p_2 = \frac{0{,}96 + \frac{2{,}7}{288} + 1{,}643\sqrt{\frac{0{,}96*0{,}04}{144} + \frac{2{,}7}{82944}}}{1 + \frac{2{,}7}{144}} = 0{,}969 + 0{,}002 = 0{,}989 \approx 0{,}99$$

Thus, the probability of a correct user recognition at a 90% confidence interval is in the range of 0.95-0.99.

Conclusions and prospects for further research. As a result of the conducted research, the stability of the user's keyboard handwriting characteristics in the biometric authentication systems has been analyzed.

Using the developed software module, experimental statistical data was obtained. They represent the temporal characteristics of the keyboard handwriting of the group of users received during the year, on average three times a week, in a total of 144 timelimit vectores for each participant.

On the basis of the graphs of the change in the average value of time parameters for the year, the absence of their pronounced trend character is established. This means that for users with a sufficient computer input handwriting is quite persistent. Thus there is no need to update the biometric standard of the user more often once a year. On the basis of the experimental statistical material, the range of values of probability of correct user recognition is calculated. It is (0,95-0,99), with a confidence interval of 90%.

Thus, the stability of keyboard handwriting for users with a sufficient computer input over a long period of time is relatively high, which means its high stability as a biometric characteristic. Accordingly, it can be argued that the standard of biometric characteristics for keyboard handwriting is sufficient to update once a year.

REFERENCE

[1] I. Kazantsev, "Analysis of keyboard writing in the processes of authentication, identification and discovery of operator substitution", *Young scientist*, vol. 1, no. 9, pp. 167-169, 2016.

[2] V. Yevetskiy, and I. Horniichuk, "Use of keyboard handwriting in user authentication systems", *Information Technology and Security*, vol. 4, iss. 1, pp. 27-33, 2016.

[3] S. Yengalichev, and S. Semenov, "Biometric authentication based on the analysis of keyboard writing", *Applied electronics*, vol. 11, no. 2, pp. 309-311, 2012.

[4] B. Bukhtiarov, and V. Abashin, "Systems of biometric authentication of the user of the PC by the keyboard handwriting", *Week of science*, vol. 4, no. 1, pp. 172-174, 2013.

[5] A. Kaluzhin, and D. Ruder, "Confirmation of the personality of the user by his keyboard handwriting", *Izvestiya Altay State University*, vol. 1, no. 85, pp. 158-162, 2015. doi:10.14258/izvasu(2015)1.1-28.

[6] V. Grigoriev, and A. Nikitin, "Use of stationary methods for biometric identification of the user", *Bulletin of the RSUU*, vol. 1, no. 94, pp. 135-143, 2012.

[7] V. Yevetskiy, "Evaluating the effectiveness of individual attributes and their aggregates for individual recognition of objects", *Information Technology and Security*, vol. 3, iss. 1, pp. 132-137, 2015.

[8] Hamming distance. [Online]. Available: https://ru.wikipedia.org/wiki/Расстояние_Хэмминга.

[9] I. Sidorkina, and A. Savinov, "Three algorithms for access control to ksiya on the basis of recognition of keyboard operator handwriting", *Herald of Chuvash University*, vol. 1, no. 3, pp. 293-301, 2013.

[10] I. Aguryanov, “Keyboard writing as a means of authentication” [Online]. Available: https://www.securitylab.ru/blog/personal/aguryanov/29985.php.
[11] Authentication Solutions Through Keystroke Dynamics. Info security products guide published from silicon valley. [Online]. Available: http://www.infosecurityproductsguide.com/technology/2007/BioPassword_Authentication_Solutions_Whitepaper_FINAL.pdf.
[12] E. Ventsel, *Theory of probabilities*. Moscow, USSR: Nauka, 1969.
[13] A. Ivanov, *Biometric person identification based on subliminal dynamic movements*. Pensa, Russia: Pensa university, 2000.
[14] V. Yevetskiy, and I. Horniichuk, “Certificate of registration of copyright for a work “Computer program for user authentication by means of keyboard writing”, *State Service of Intellectual Property of Ukraine No.71533*, Apr. 19, 2017.
[15] V. Yevetskiy, and I. Horniichuk, “Certificate of registration of copyright for a work “Computer program for user registration for authoring means of keyboard writing”, *State Service of Intellectual Property of Ukraine No. 71534*, Apr. 19, 2017.

The article was received September 9, 2018.

СПИСОК ВИКОРИСТАННОЇ ЛІТЕРАТУРИ

[1] И. Казанцев, “Анализ клавиатурного почерка в процессах автентификации, идентификации и обнаружения подмены оператора”, *Молодой ученый,* т. 1, № 9, с. 167-169, 2016.
[2] В. Євецький, та І. Горнійчук, “Використання клавіатурного почерку в системах автентифікації користувача”, *Information Technology and Security*, vol. 4, iss. 1, pp. 27-33, 2016.
[3] С. Енгаличев, и С. Семенов, “Биометрическая автентификация на основе анализа клавиатурного почерка”, *Прикладная радиоэлектроника*, т. 11, №. 2, с. 309-311, 2012.
[4] Б. Бухтияров, и В. Абашин, “Системы биометрической автентификации пользователя ПК по клавиатурному почерку”, *Неделя науки*, т. 4, №. 1, с. 172-174, 2013.
[5] А. Калужин, и Д. Рудер, “Подтверждение личности пользователя по его клавиатурному почерку”, *Известия Алтайского государственного университета*. т. 1, №. 85, с. 158-162, 2015.
doi:10.14258/izvasu(2015)1.1-28.
[6] В. Григорьєв, и А. Нікітін, “Использование стастических методов для биометрической идентификации пользователя”, *Вестник РГГУ*, т. 1, № 94, с. 135-143, 2012.
[7] В. Євецький, “Оценка эффективности отдельных признаков и их совокупностей для индивидуального распознавания объектов”, *Information Technology and Security*. vol. 3, iss. 1, pp. 132-137, 2015.
[8] Расстояние Хэмминга [Электронный ресурс]. Доступно: https://ru.wikipedia.org/wiki/Расстояние_Хэмминга.
[9] И. Сидоркина, и А. Савинов, “Три алгоритма управления доступом к ксии на основе распознавания клавиатурного почерка оператора”, *Вестник Чувашского университета*, т. 1, № 3, с. 293-301, 2013.
[10] И. Агур’янов, “Клавиатурный почерк как средство автентификации” [Электронный ресурс]. Доступно: http://www.securitvlab.ru/blog/personal/aeurvanov/29985.php.
[11] Authentication Solutions Through Keystroke Dynamics. Info security products guide published from silicon valley. [Online]. Available: http://www.infosecurityproductsguide.com/technology/2007/BioPassword_Authentication_Solutions_Whitepaper_FINAL.pdf.
[12] Е. Вентцель, *Теория вероятностей*. Москва, СССР: Наука, 1969.
[13] А. Иванов, *Биометрическая идентификация личности по динамике подсознательных движений*. Пенза, Российская Федерация: Пенз. гос. ун-т, 2000.
[14] І. Горнійчук, та В. Євецький, “Свідоцтво про реєстрацію авторського права на твір “Комп'ютерна програма автентифікації користувачів засобами клавіатурного почерку”, *Державна служба інтелектуальної власності України №71533*, Квіт.19, 2017.

[15] І. Горнійчук, та В. Євецький, “Свідоцтво про реєстрацію авторського права на твір “Комп’ютерна програма реєстрації користувачів для авторизації засобами клавіатурного почерку”, *Державна служба інтелектуальної власності України №71534*, Кві.19, 2017.

ВІКТОР ЄВЕЦЬКИЙ,
ІВАН ГОРНІЙЧУК

АНАЛІЗ СТАЛОСТІ ХАРАКТЕРИСТИК КЛАВІАТУРНОГО ПОЧЕРКУ КОРИСТУВАЧА В СИСТЕМАХ БІОМЕТРИЧНОЇ АВТЕНТИФІКАЦІЇ

Розглянуто питання використання біометричних характеристик для підвищення ефективності автентифікації користувача. Ідентифікатор, що використовує біометричні характеристики, нерозривно пов’язаний з користувачем, і скористатися ним несанкціоновано практично неможливо. Як біометричну характеристику доцільно використати клавіатурний почерк. Клавіатурний почерк, або ритм набору тексту, відображає спосіб набору тексту на клавіатурі, властивий тільки конкретному користувачеві. Крім того, він досить простий в реалізації і не вимагає додаткових апаратних витрат. Тим більше, що використання клавіатурного почерку при введенні пароля усуває основні недоліки класичних парольних систем і систем на основі карт доступу. Основна увага при проведенні досліджень була приділена сталості у часі характеристик клавіатурного почерку конкретного користувача протягом тривалого періоду часу. Для реалізації допуску користувача до комп’ютерної системи обрано алгоритм на основі відстані Хемінга. Відповідно до обраного алгоритму розроблено алгоритм формування вектора біометричних характеристик користувача, що включає тривалість утримання конкретної клавіші і час між натисканням сусідніх клавіш. Розроблено алгоритм формування біометричного еталону користувача. Для аналізу використання клавіатурного почерку було розроблено програмні застосунки, що реалізують допуск користувача на основі клавіатурного почерку, а також програма для збору часових характеристик. Обидва застосунки використовують розроблені алгоритми. Для дослідження сталості часових характеристик почерку було проведено емпіричне дослідження. Для цього обрана група осіб, кожен з яких володіє комп’ютерним вводом на достатньому рівні. Всі вони вводили запропоновану фразу протягом року. Отримані статистичні дані, на основі яких, обчислено середні значення і значення середнього квадратичного відхилення часових характеристик клавіатурного почерку за різні проміжки часу. Оцінено ймовірність вірного розпізнання користувача за його частотою в n незалежних дослідах. В результаті проведеного дослідження було проаналізовано сталість комп'ютерного почерку користувача як біометричної характеристики для використання у системах захисту комп'ютерних даних, зокрема, системах автентифікації.

Ключові слова: автентифікація, біометрична автентифікація користувача, біометрирична характеристика, клавіатурний почерк, система біометричної автентифікації.

ВИКТОР ЕВЕЦКИЙ,
ИВАН ГОРНИЙЧУК

АНАЛИЗ ПОСТОЯНСТВА ХАРАКТЕРИСТИК КЛАВИАТУРНОГО ПОЧЕРКА ПОЛЬЗОВАТЕЛЯ В СИСТЕМАХ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ

Рассмотрены вопросы использования биометрических характеристик для повышения эффективности аутентификации пользователя. Идентификатор, использующий биометрические характеристики, неразрывно связан с пользователем, и воспользоваться им несанкционированно практически невозможно. В качестве биометрической характеристики целесообразно использовать клавиатурный почерк. Клавиатурный почерк, или ритм набора текста, отражает способ набора текста на клавиатуре, свойственный только конкретному пользователю. Кроме того, он достаточно прост в реализации и не требует дополнительных

аппаратных затрат. Тем более, что использование клавиатурного почерка при вводе пароля устраняет основные недостатки классических парольных систем и систем на основе карт доступа. Основное внимание при проведении исследований было уделено устойчивости во времени характеристик клавиатурного почерка конкретного пользователя в течение длительного периода времени. Для реализации допуска пользователя к компьютерной системе избран алгоритм на основе расстояния Хемминга. В соответствии с выбранным алгоритмом разработан алгоритм формирования вектора биометрических характеристик пользователя, включающий длительность нажатия конкретной клавиши и время между нажатием соседних клавиш. Разработан алгоритм формирования биометрического эталона пользователя. Для анализа использования клавиатурного почерка были разработаны программные приложения, реализующие допуск пользователя на основе клавиатурного почерка, а также программа для сбора временных характеристик. Оба приложения используют разработанные алгоритмы. Для исследования устойчивости временных характеристик почерка было проведено эмпирическое исследование. Для этого выбрана группа лиц, каждый из которых обладает компьютерным вводом на достаточном уровне. Все они вводили предложенную фразу в течение года. Полученные статистические данные, на основании которых вычислено среднее значение и значение среднего квадратического отклонения временных характеристик клавиатурного почерка за различные промежутки времени. Оценена вероятность верного распознавания пользователя по его частоте в n независимых опытах. В результате проведенного исследования было проанализировано постоянство компьютерного почерка пользователя как биометрической характеристики для использования в системах защиты компьютерных данных, в частности, системах аутентификации.

Ключевые слова: аутентификация, биометрическая аутентификация пользователя, биометрическая характеристика, клавиатурный почерк, система биометрической аутентификации.

Віктор Леонідович Євецький, кандидат технічних наук, доцент, доцент кафедри кібербезпеки та застосування автоматизованих інформаційних систем та технологій, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0002-5364-8076.

E-mail: viktorevetskv@gmail.com.

Іван Вікторович Горнійчук, курсант, Інститут спеціального зв'язку та захисту інформації Національного технічного університету України "Київський політехнічний інститут імені Ігоря Сікорського", Київ, Україна.

ORCID: 0000-0001-6754-4764.

E-mail: horniychuk.ivan@gmail.com.

Виктор Леонидович Евецкий, кандидат технических наук, доцент, доцент кафедры кибербезопасности и применения информационных систем и технологий, Институт специальной связи и защиты информации Национального технического университета Украины «Киевский политехнический институт шимени Игоря Сикорского», Киев, Украина.

Иван Викторович Горнийчук, курсант, Институт специальной связи и защиты информации Национального технического университета Украины "Киевский политехнический институт шимени Игоря Сикорского", Киев, Украина.

Viktor Yevetskyi, candidate of technical sciences, associate professor, associate professor at the cybersecurity and application of information systems and technologies academic department, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.

Ivan Horniichuk, cadet, Institute of special communication and information protection of National technical university of Ukraine "Igor Sikorsky Kyiv polytechnic institute", Kyiv, Ukraine.