Information systems. Computer sciences. Issues of information security
Информационные системы. Информатика. Проблемы информационной безопасности

UDC 004.056.2
https://doi.org/10.32362/2500-316X-2023-11-6-7-15

RESEARCH ARTICLE

Generation of keyboard handwriting during user authentication on mobile devices

Svetlana M. Ivanova,
Zoya V. Ilyichenkova @

MIREA – Russian Technological University, Moscow, 119454 Russia
@ *Corresponding author, e-mail: ilichenkova@mirea.ru*

Abstract

Objectives. This article discusses a new way of generating keyboard handwriting using a touch keyboard for authentication in currently existing mobile systems.

Methods. Due to the insufficient reliability of single password authentication, the proposal is to use it in combination with characteristics which correspond to handwriting on mobile devices. This article demonstrates the possibility of using individual user characteristics in the formulation of keyboard handwriting on devices with touch keyboards. The type of keyboard used affects the characteristics of keyboard handwriting, so this aspect can be used to improve password authentication reliability. The authentication process in the information environment can be supplemented with data on the nature of the impact on a touch keyboard. The use of the built-in 3D Touch function is also of interest. This is available when working on mobile devices and appliances equipped with a touch keyboard. The paper demonstrates that the use of one parameter only is insufficient for accurate authentication. The study proposes a method of determining an acceptable error range for both the touch force and the intermediate interval during authentication. For this purpose, the Laplace function which formulates the interval of each characteristic depending on the required probability of user recognition is used.

Results. Touch force and the intermediate interval are sufficient to obtain the necessary characteristics, in order to formulate a refined user portrait depending on the user's keyboard handwriting. Experimental statistics are given separately for an average sample of three different users depending on touch force. They also provide the results of authentication when using both standard deviations of pressing and the intervals when using the touch keyboard for the iOSXcode platform.

Conclusions. The conclusion relates to the possibility of user authentication by keyboard handwriting, formulated on the basis of both the touch force on the keyboard symbols and intervals between pressing. Using the values of the sample mean and standard deviations allows authentication according to the required recognition probability.

Keywords: authentication, mobile devices, keyboard handwriting, touch force, time interval between character clicks

• **Submitted:** 24.04.2023 • **Revised:** 22.06.2023 • **Accepted:** 04.09.2023

For citation: Ivanova S.M., Ilyichenkova Z.V. Generation of keyboard handwriting during user authentication on mobile devices. *Russ. Technol. J.* 2023;11(6):7–15. https://doi.org/10.32362/2500-316X-2023-11-6-7-15

Financial disclosure: The authors have no a financial or property interest in any material or method mentioned.

The authors declare no conflicts of interest.

НАУЧНАЯ СТАТЬЯ

Формирование клавиатурного почерка при аутентификации на мобильных устройствах

С.М. Иванова,
З.В. Ильиченкова @

МИРЭА – Российский технологический университет, Москва, 119454 Россия
@ *Автор для переписки, e-mail: ilichenkova@mirea.ru*

Резюме

Цели. В статье рассматривается новый способ формирования клавиатурного почерка при использовании сенсорной клавиатуры для аутентификации в существующих на данный момент мобильных системах.

Методы. В силу недостаточной надежности отдельно взятой парольной аутентификации предлагается использовать ее комбинацию с характеристиками, которые соответствуют почерку на мобильных устройствах. В статье продемонстрирована возможность использования индивидуальных характеристик пользователя при формировании клавиатурного почерка на устройствах с сенсорной клавиатурой. Показано, что тип используемой клавиатуры влияет на характеристики клавиатурного почерка, поэтому данный аспект можно использовать для повышения надежности парольной аутентификации. Предлагается дополнить процесс аутентификации в информационной среде данными о характере воздействия на сенсорную клавиатуру. Интерес представляет использование встроенной функции 3D Touch, которая доступна при работе на мобильных устройствах и технике, оснащенной сенсорной клавиатурой. В статье продемонстрировано, что использования только одного параметра недостаточно для точной аутентификации. Предложен способ определения допустимого диапазона погрешности, в который должны укладываться как сила нажатия, так и промежуточный интервал при проведении аутентификации. Для этого используется функция Лапласа, позволяющая сформировать интервал каждой характеристики в зависимости от требуемой вероятности распознавания пользователя.

Результаты. Показано, что силы нажатия и промежуточного интервала достаточно для получения необходимых характеристик, позволяющих сформировать уточненный портрет пользователя по его клавиатурному почерку. Приведены экспериментальные статистические данные отдельно среднего выборки для трех различных пользователей согласно силе нажатия, а также результаты аутентификации при использовании одновременно среднеквадратичных отклонений силы нажатий и интервалов между ними при использовании сенсорной клавиатуры для платформы iOSXcode.

Выводы. Сделан вывод о возможности применения способа аутентификации пользователей по клавиатурному почерку, сформированному на основе одновременно силы нажатий на символы клавиатуры и интервалов между нажатиями. Использование значений среднего выборки и среднеквадратичных отклонений позволяет проводить аутентификацию согласно требуемой вероятности распознавания.

Ключевые слова: аутентификация, мобильное устройство, клавиатурный почерк, сила нажатия, временной интервал между нажатиями

• **Поступила:** 24.04.2023 • **Доработана:** 22.06.2023 • **Принята к опубликованию:** 04.09.2023

Для цитирования: Иванова С.М., Ильиченкова З.В. Формирование клавиатурного почерка при аутентификации на мобильных устройствах. *Russ. Technol. J.* 2023;11(6):7–15. https://doi.org/10.32362/2500-316X-2023-11-6-7-15

Прозрачность финансовой деятельности: Авторы не имеют финансовой заинтересованности в представленных материалах или методах.

Авторы заявляют об отсутствии конфликта интересов.

INTRODUCTION

Authentication systems on mobile devices today are usually based on knowledge possessed by the user (password or graphical authentication) or on the user's biometric characteristics (fingerprint or face authentication) [1, 2]. However, the above methods, as a rule, do not provide the required accuracy[1] and do not have the functionality of customizing the required level of security [3–5]. There may also be situations when it is not possible to use a biometric authentication device. For example, such situations may arise when a person is in non-standard conditions, for example when the user is unable to raise the Smartphone to face level [6, 7]. In this regard, it seems reasonable to use multi-factor authentication using the keyboard handwriting of mobile device users. Since the owner of the device enters text regularly, the handwriting can remain pertinent at all times. Also, if necessary, it allows the use of handwriting not only for authentication.

Keyboard handwriting can be formulated based on the use of user preferences and modern technologies available for these types of gadgets. Such technologies include 3D Touch[2] technology based on determining the touch force on various characters on the touch keyboard [8, 9]. The capabilities of this development can be used on all modern iPhone devices[3] and on most smartphones. 3D Touch makes it possible to personalize the way the user interacts with the device.

Keyboard handwriting generation and recognition systems are usually based on software signal processing [10–12]. Therefore, the method of authentication on mobile devices based on keyboard handwriting, including the use of 3D Touch technology, is relatively inexpensive and well integrated into existing systems.

Biometric handwriting includes the statistical processing of data obtained when a user enters a given phrase [13, 14]. When a user performs password authentication, the phrase entered is usually fixed. However, when the passwords of different users roughly coincide, there is an increased probability of matching the keyboard handwriting, based on the duration of pressing a certain symbol. Studies have shown that the use of keyboard handwriting alone does not guarantee the necessary authentication reliability [15, 16]. Moreover, with the widespread use of mobile devices, the duration of pressing is gradually changing. Thus, this parameter cannot be considered as a determinant [17].

When determining the keyboard handwriting of a user, the following factors should be taken into account: identity of a smartphone or other authentication device, and psychophysical characteristics of the state of the device owner [18, 19]. However, if handwriting statistics are requisite for authentication on a particular device, the first aspect can be neglected [20].

GENERATING INFORMATION ON KEYBOARD HANDWRITING

With the rapid evolution of software in the use of password authentication, factors such as how the user interacts with the touchscreen keyboard should also be taken into consideration.

The following characteristics can be used to generate the keyboard handwriting: input speed and dynamics, frequency of errors, duration of pauses/signal overlapping, and 3D Touch value when working with a touch keyboard.

There are several types of touch keyboards in mobile devices. Most of the time, the user uses the same layout to which he or she is accustomed. However, the keyboard type may sometimes be altered for ease of input. Depending on the type of keyboard, it is not so much the duration of pressing the keys which changes, but rather the interval between significant keys. When entering a password, the spacing also changes, if the user has to switch from a character keyboard to a numeric keyboard. On mobile devices, the duration or the touch force applied upon the character may be different when selecting digits or service characters. This depends on the use of the keyboard, since they can be selected on the basic layout by holding down the finger or by including a special corresponding character set.

The results of the 3D Touch mechanism can be used to gradate the touch force and several levels can be defined according to the value obtained. It is simplest of all to follow the gradation of normal pressure and strong pressure. In the first case, the user is operating the screen of the mobile device in a standard way when performing actions. In the second case, there is a stronger pressure on the characters, leading to a physical impact accompanied by deflection of the glass panel. The 3D Touch mechanism can differentiate between these levels of impact force. In order to determine touch force, Force property of the UITouch object can be used. This function is present in the objects of iPhone version 6 and above and characterizes touch force. The MaximumPossibleForce property characterizes the maximum possible value of the touch force. Using both values, the relative value of the character's touch force can be defined. A value of 1.0 represents the average force defined by the system.

[1] Golubkova V.B., Braginskii A.I. *Issues of theoretical and applied computer science*: textbook. Moscow: MADI; 2018. 72 p. (in Russ.).

[2] *What Is 3D Touch and How It Works*. https://itechguidesad.pages.dev/posts/what-is-3d-touch-and-how-it-works-/. Accessed April 22, 2023.

[3] https://www.apple.com/iphone/. Accessed April 22, 2023.

For increased passphrase security, Latin characters should be used in combination with numbers and service characters. Different mobile devices use different types of keyboards. However, in all devices special characters are placed in a separate keyboard. Sometimes there are also numeric keys on a special tab. It is proposed, therefore, to supplement the touch force applied on the characters with information about the duration of pauses between informational (included in the password) characters which require keyboard switching.

User recognition is a two-stage process. The first stage is required for initial generation of the user's keyboard handwriting. The resulting data is then used in the next stage for authentication. The combination of the two stages makes it possible to conclude that either the user is legitimate or that an intruder has attempted to log on to the system.

In accordance with the above, the proposal is to formulate keyboard handwriting by taking characteristics of the sample mean and standard deviation of the touch force and the intervals between pressing characters. This pair of statistical data is characterized by their heterogeneity which allows for more accurate estimation.

At the first stage, each user enters a passphrase which meets the security requirements several times. In order to increase the representativeness of the sample, additional password requirements can be formulated to include not only generalized rules, but also to define the sequence of typing. For example, the need to switch repeatedly from one character type to another can be included.

Depending on the parameters selected, the required characteristics are calculated character by character and then grouped (Tables 1, 2).

Table 1. Format for character touch force data presentation

Character (x_i)	Sample mean ($\overline{x}$)	Standard deviation (σ_x)
...	...	...

Table 2. Format for presenting data on intervals between pressing characters

Sequential characters (x_i)	Sample mean ($\overline{x}$)	Standard deviation (σ_x)
...	...	...

Calculation of the values of the second and third columns of the tables is carried out by means of the following formulae:

$$\overline{x} = \frac{\sum_{i=1}^{n} x_i}{n}, \quad \sigma_x = \sqrt{\frac{\sum_{i}^{n} \left(x_i - \overline{x}\right)^2}{n-1}},$$

where the variable n shows how many times the passphrase has been repeated.

Since during authentication, the received data x_{n+1} will differ, a possible range of values ($x_{\min}$, $x_{\max}$) needs to be established within which user legitimacy is indicated. The ability to vary the length of the interval depending on the required probability of errors will also be useful. Therefore, when determining the interval boundaries, it seems reasonable to take into account the value of the standard deviation:

$$P\left(x_{\min} < x_{n+1} < x_{\max}\right) = \\ = F\left(\frac{x_{\max} - \overline{x}}{\sigma_x}\right) - F\left(\frac{\overline{x} - x_{\min}}{\sigma_x}\right),$$

where $F(\cdot)$ is the Laplace function and the distribution of the random variable x is normal.

During authentication, errors of the first kind (i.e., a legitimate user is not recognized as such) and of the second kind (an attacker is recognized as a registered user) are possible. In order to reduce errors of the second kind, the value of the probability of erroneous recognition of the user will be reduced.

Since in recognition systems the deviations from the mean value in both directions are equivalent, the probability of hitting the required interval can be written as:

$$P\left(x_{\min} < x_{n+1} < x_{\max}\right) = 2F\left(\frac{\overline{x} - x_{\min}}{\sigma_x}\right).$$

Thus, the values of the acceptable range limits can be adjusted depending on tolerance of errors of the first or second kind.

After formulating the keyboard handwriting, user authentication is performed by entering a password. For a new phrase, the same statistical characteristics are defined and they are checked to to see whether they fall within the specified interval. Depending on the result, a decision about the user's legitimacy is to be made.

EXPERIMENTAL AUTHENTICATION

In order to test the performance of the proposed method of user control, a program to obtain information about the intensity of data input and the force of pressing the characters on the keyboard of the mobile device was written. In this work, the iOSXcode[4] platform was used. Calculations were performed for 10 consecutive inputs performed under the same conditions. For three different users (User1, User2, User3), the corresponding statistical characteristics were calculated for the input data "1@35f1" (Tables 3–5).

[4] Xcode. https://developer.apple.com/xcode/. Accessed April 22, 2023.

Table 3. Character touch force data (User1)

Character	Sample mean	Standard deviation
1	0.4334	0.034916
@	0.4872	0.033796
3	0.558444	0.033623
5	0.539917	0.033619
f	0.492778	0.031256
1	0.479875	0.018871274

Table 4. Character touch force data (User2)

Character	Sample mean	Standard deviation
1	0.35947	0.024012
@	0.460015	0.031145
3	0.501201	0.035001
5	0.54102	0.032115
f	0.402495	0.030598
1	0.483985	0.032012

Table 5. Character touch force data (User3)

Character	Sample mean	Standard deviation
1	0.590235	0.034985
@	0.58098	0.032998
3	0.6001	0.025198
5	0.63101	0.028957
f	0.56398	0.032015
1	0.55356	0.030011

The value 1.0 of the pressing force represents the average force determined by the system.

Figure 1 shows data obtained on the magnitude of the touch force on different characters in the form of a comparison chart for each of the three users. The results were obtained for a user recognition probability equal to 0.95.

According to this data, only for the character "3" do the ranges obtained not overlap. However, a single character sample cannot be considered sufficient. Therefore, it is suggested that s data about the pressing intervals of significant characters be added to the analysis without taking into account the keyboard type switch presses (Tables 6–8).

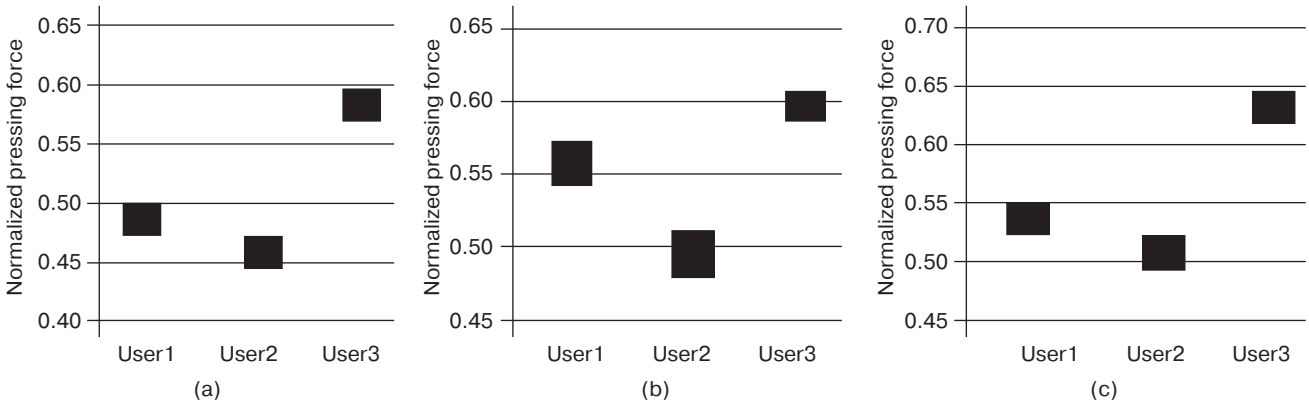

Fig. 1. Permissible touch force ranges: (a) character "@", (b) character "3", (c) character "5"

Table 6. Data on interval between pressing characters (User1)

Sequential characters	Sample mean (10^{-6}, s)	Standard deviation (10^{-6}, s)
1–@	46915.5	143.2862
@–3	47625.13	141.8598
3–5	46764.5	139.9112
5–f	47696.38	133.5322
f–1	46917.25	118.9138

Table 7. Data on interval between pressing characters (User2)

Sequential characters	Sample mean (10^{-6}, s)	Standard deviation (10^{-6}, s)
1–@	59807.5	181.7389
@–3	69081.63	171.6768
3–5	46779.13	158.8777
5–f	69025.38	106.3336
f–1	59943.13	144.3076

Table 8. Data on interval between pressing characters (User3)

Sequential characters	Sample mean (10^{-6}, s)	Standard deviation (10^{-6}, s)
1–@	57835.25	152.0627
@–3	67866.13	150.8391
3–5	45906.38	137.8881
5–f	67908	162.6047
f–1	57937.25	104.8996

Analysis of the data obtained shows that the time interval between pressing the symbols located on the same keyboard does not guarantee the required differentiation of values (Fig. 2c). Switching the keyboard from symbolic to numeric (User2, User3) or selecting numeric or service symbols with the help of increased pressure on the symbols of the main keyboard (User1) enables the required difference in the characteristics of keyboard handwriting (Fig. 2a, 2b) to be attained.

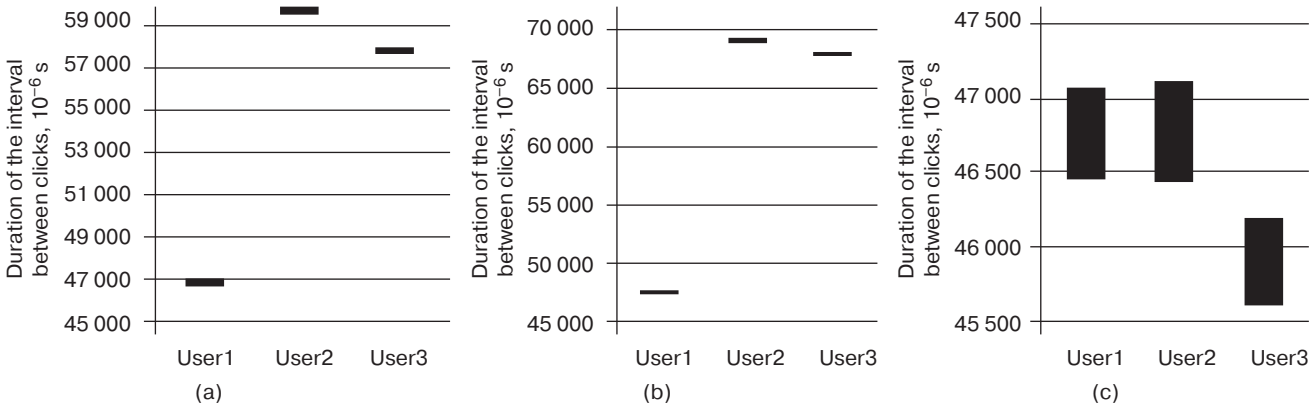

Fig. 2. Permissible ranges for interval between pressing characters (a) "1–@", (b) "@–3", (c) "3–5"

CONCLUSIONS

When using password authentication, the use of additional information about keyboard handwriting, based on the touch force applied on the keys and the duration between successive presses, allows the accuracy of recognition to be increased to the requisite probability. The advantages of the method proposed include the possibility of modifying the parameters to balance between first and second type errors. Obtaining new information in the same format as the original information, allows data to be updated, if necessary.

ACKNOWLEDGMENTS

Authors thank the management of MIREA – Russian Technological University for their assistance in the studies.

Authors' contributions

S.M. Ivanova—development of key goals and objectives; conducting research, including analysis of the specifics of using mobile devices in the formation of the keyboard handwriting; development of mathematical apparatus for data analysis.

Z.V. Ilyichenkova—forming an idea for the article; conducting research, including analyzing the possibility of using a combination of several characteristics to form the keyboard handwriting; processing and analyzing of the statistical data.

All authors—writing the text of the article; approval of the final version of the article; interpretation of the research results; formulation of conclusions.

REFERENCES

1. Ilyichenkova Z.V., Ivanova S.M. Identification of Dynamic Object Parameters. *Nuclear Instruments and Methods in Physics Research. Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*. 2003;502(2–3):535–536. http://doi.org/10.1016/S0168-9002(03)00493-5
2. Khant K.Z., Sosenushkin S. Big data analysis model for the implementation of smart universities. *Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki = Modern Science: Actual Problems of Theory and Practice. Series of "Natural and Technical Sciences*." 2021;8: 72–75 (in Russ.). http://doi.org/10.37882/2223-2966.2021.08.17
3. Ilyichenkova Z.V., Ivanova S.M. Cluster keyboard handwriting. *Procedia Computer Science*. 2021;186: 395–402. https://doi.org/10.1016/j.procs.2021.04.162
4. Gorbukhov N.N., Magomedov Sh.G. Comparison of mobile app builders. In: *KhRONIKI TsIFROVYKh TRANSFORMATsII: Materialy mezhkafedral'nogo kruglogo stola* (*CHRONICLES OF DIGITAL TRANSFORMATIONS. Materials of the Inter-Cathedral Round Table*). V. 4. Volgograd. 2022. P. 44–49 (in Russ.).
5. Nikolsky S.N. The task of automation and evolutionary modeling. *Shkola Nauki = School of Science*. 2022;1(50):3–7 (in Russ.). https://doi.org/10.5281/zenodo.5914537
6. Antonova I.I., Antonova A.A., Shmeleva A.N., Novikov A.A., Nazarenko M.A. System Analysis of Transport-Information Infrastructure Transformation in Modern Cities. In: *2020 International Conference Quality Management, Transport and Information Security, Information Technologies* (*IT&QM&IS*). Yaroslavl, Russia. 2020. P. 154–156. http://dx.doi.org/10.1109/ITQMIS51053.2020.9322902

СПИСОК ЛИТЕРАТУРЫ

1. Ilyichenkova Z.V., Ivanova S.M. Identification of Dynamic Object Parameters. *Nuclear Instruments and Methods in Physics Research. Section A: Accelerators, Spectrometers, Detectors and Associated Equipment*. 2003;502(2–3):535–536. http://doi.org/10.1016/S0168-9002(03)00493-5
2. Кхант К.З., Сосенушкин С.Е. Модель анализа больших данных для внедрения умных университетов. *Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки*. 2021;8:72–75. http://doi.org/10.37882/2223-2966.2021.08.17
3. Ilyichenkova Z.V., Ivanova S.M. Cluster keyboard handwriting. *Procedia Computer Science*. 2021;186: 395–402. https://doi.org/10.1016/j.procs.2021.04.162
4. Горбухов Н.Н., Магомедов Ш.Г. Сравнение конструкторов мобильных приложений. В сб.: *ХРОНИКИ ЦИФРОВЫХ ТРАНСФОРМАЦИЙ: материалы межкафедрального круглого стола*. Выпуск 4. Волгоград. 2022. С. 44–49.
5. Никольский С.Н. Задача автоматизации и эволюционное моделирование. *Школа Науки*. 2022;1(50):3–7. https://doi.org/10.5281/zenodo.5914537
6. Antonova I.I., Antonova A.A., Shmeleva A.N., Novikov A.A., Nazarenko M.A. System Analysis of Transport-Information Infrastructure Transformation in Modern Cities. In: *2020 International Conference Quality Management, Transport and Information Security, Information Technologies* (*IT&QM&IS*). Yaroslavl, Russia. 2020. P. 154–156. http://dx.doi.org/10.1109/ITQMIS51053.2020.9322902
7. Ермакова А.Ю., Лось А.Б. Об оценке рисков при анализе эффективности алгоритмов защиты информации. *Математическое и компьютерное моделирование в экономике, страховании и управлении рисками*. 2022;7:64–70. URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2022/12/21/013.pdf

7. Ermakova A.Y., Los A.B. On risk assessment when analyzing the effectiveness of information protection algorithms. *Matematicheskoe i komp'yuternoe modelirovanie v ekonomike, strakhovanii i upravlenii riskami = Mathematical and Computer Modeling in Economics, Insurance and Risk Management*. 2022;7:64–70 (in Russ.). Available from URL: https://www.sgu.ru/sites/default/files/textdocsfiles/2022/12/21/013.pdf
8. Kuronen T., Eerola T., Lensu L., Kälviäinen H., Häkkinen J. 3D hand movement measurement framework for studying human-computer interaction. In: Arseniev D., Overmeyer L., Kälviäine H., Katalini B. (Eds.). *Cyber-Physical Systems and Control* (*CPS&C 2019*). *Lecture Notes in Networks and Systems.* V. 95. Springer, Cham.; 2019. P. 513–524. http://doi.org/10.1007/978-3-030-34983-7_50
9. Kuronen T., Eerola T., Lensu L., Kälviäinen H. Two-Camera Synchronization and Trajectory Reconstruction for a Touch Screen Usability Experiment. In: Blanc-Talon J., Helbert D., Philips W., Popescu D., Scheunders P. (Eds.). *Advanced Concepts for Intelligent Vision Systems* (*ACIVS 2018*). *Lecture Notes in Computer Science.* V. 11182. Springer, Cham.; 2018. P. 125–136. https://doi.org/10.1007/978-3-030-01449-0_11
10. Stroganov D.V., Sakun B.V., Yartsev M.I. General Principles of Assessment of Staff Skills Building Specialties. *Int. J. Adv. Studies*. 2016;6(4):63–76. https://doi.org/10.12731/2227-930X-2016-4-63-76
11. Volkov A.I., Semin V.G., Semin V.V. Fuzzy sets in the problems of assessing the quality of mobile applications. In: *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies* (*IT&QM&IS*). Yaroslavl, Russia. 2021. P. 355–358. https://doi.org/10.1109/ITQMIS53292.2021.9642873
12. Ivanova S.M., Ilyichenkova Z.V., Antonova A.A. Keyboard handwriting analysis in the learning systems. *Vestnik komp'yuternykh i informatsionnykh tekhnologii = Herald of Computer and Information Echnologies.* 2020;17;6(192):22–30 (in Russ.). https://doi.org/10.14489/vkit.2020.06.pp.022-030
13. Aleshnikova E.A., Chadina Yu.A. The Axiological Approach in Teaching High School Students Reading Comprehension at Russian Language Lessons. *Russkii yazyk v shkole = Russian Language at School*. 2019;80(1):46–49 (in Russ.). https://doi.org/10.30515/0131-6141-2019-80-1-46-49
14. Sarkisova I.O., Laverychev M.A. Analysis of the influence of the location of NFC tags on the occurrence of collisions. *Sovremennaya nauka: aktual'nye problemy teorii i praktiki. Seriya: Estestvennye i tekhnicheskie nauki = Modern Science: Actual Problems of Theory and Practice. Series of "Natural and Technical Sciences*." 2022;8:119–124 (in Russ.). Available from URL: https://elibrary.ru/item.asp?id=49623257
15. Pronin C.B., Maksimychev O.I., Ostroukh A.V., Volosova A.V., Matukhina E.N. Creating quantum circuits for training perceptron neural networks on the principles of Grover's algorithm. In: *2022 Systems of Signals Generating and Processing in the Field of on Board Communications.* Moscow, Russia. 2022. 5 p. https://doi.org/10.1109/IEEECONF53456.2022.9744279
8. Kuronen T., Eerola T., Lensu L., Kälviäinen H., Häkkinen J. 3D hand movement measurement framework for studying human-computer interaction. In: Arseniev D., Overmeyer L. Kälviäine H., Katalini B. (Eds.). *Cyber-Physical Systems and Control* (*CPS&C 2019*). *Lecture Notes in Networks and Systems.* V. 95. Springer, Cham.; 2019. P. 513–524. http://doi.org/10.1007/978-3-030-34983-7_50
9. Kuronen T., Eerola T., Lensu L., Kälviäinen H. Two-Camera Synchronization and Trajectory Reconstruction for a Touch Screen Usability Experiment. In: Blanc-Talon J., Helbert D., Philips W., Popescu D., Scheunders P. (Eds.). *Advanced Concepts for Intelligent Vision Systems. ACIVS 2018. Lecture Notes in Computer Science.* V. 11182. Springer, Cham.; 2018. P. 125–136. https://doi.org/10.1007/978-3-030-01449-0_11
10. Stroganov D.V., Sakun B.V., Yartsev M.I. General Principles of Assessment of Staff Skills Building Specialties. *Int. J. Adv. Studies*. 2016;6(4):63–76. https://doi.org/10.12731/2227-930X-2016-4-63-76
11. Volkov A.I., Semin V.G., Semin V.V. Fuzzy sets in the problems of assessing the quality of mobile applications. In: *2021 International Conference on Quality Management, Transport and Information Security, Information Technologies* (*IT&QM&IS*). Yaroslavl, Russia. 2021. P. 355–358. https://doi.org/10.1109/ITQMIS53292.2021.9642873
12. Иванова С.М., Ильиченкова З.В., Антонова А.А. Анализ клавиатурного почерка в обучающих системах. *Вестник компьютерных и информационных технологий.* 2020;17;6(192):22–30. https://doi.org/10.14489/vkit.2020.06.pp.022-030
13. Алешникова Е.А., Чадина Ю.А. Аксиологизация работы с текстом на уроках русского языка в старшей школе. *Русский язык в школе*. 2019;80(1):46–49. https://doi.org/10.30515/0131-6141-2019-80-1-46-49
14. Саркисова И.О., Лаверычев М.А. Анализ влияния расположения NFC меток на приоритет чтения. *Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки*. 2022;8:119–124. URL: https://elibrary.ru/item.asp?id=49623257
15. Pronin C.B., Maksimychev O.I., Ostroukh A.V., Volosova A.V., Matukhina E.N. Creating quantum circuits for training perceptron neural networks on the principles of Grover's algorithm. In: *2022 Systems of Signals Generating and Processing in the Field of on Board Communications.* Moscow, Russia. 2022. 5 p. https://doi.org/10.1109/IEEECONF53456.2022.9744279
16. Иванова С.М., Ильиченкова З.В., Антонова А.А. Проверка подлинности пользователя при работе в обучающих системах. *Информационные технологии.* 2020;26(11):648–654. https://doi.org/10.17587/it.26.648-654
17. Матюхин Б.Н., Матюхина Е.Н., Чистякова М.А., Морозов Е.А. Математические модели объектов диагноза. *Промышленные АСУ и контроллеры*. 2021;5:29–32. https://doi.org/10.25791/asu.5.2021.1280
18. Каримов М.Т., Никонов В.В. Сравнение производительности моделей сверточных нейронных сетей на графическом процессоре. *Информационные и телекоммуникационные технологии*. 2021;52:42–48.

16. Ivanova S.M., Ilyichenkova Z.V., Antonova A.A. User Authentication in Training Systems. *Informacionnye tekhnologii = Information Technologies*. 2020;26(11): 648–654 (in Russ.). https://doi.org/10.17587/it.26.648-654
17. Matyukhin B.N., Matyukhina E.N., Chistyakova M.A., Morozov E.A. Mathematical models of objects of diagnosis. *Promyshlennye ASU i kontrollery = Industrial Automatic Control Systems and Controllers*. 2021;5: 29–32 (in Russ.). https://doi.org/10.25791/asu.5.2021.1280
18. Karimov M.T., Nikonov V.V. Performance comparison of convolutional neural network models on a GPU. *Informatsionnye i telekommunikatsionnye tekhnologii = Information and Telecommunication Technologies*. 2021;52:42–48 (in Russ.).
19. Savinykh V.P., Gospodinov S.G., Kudzh S.A., Tsvetkov V.Ya., Deshko I.P. Semantics of visual models in space research. *Russ. Technol. J*. 2022;10;2(46):51–58 (in Russ.). https://doi.org/10.32362/2500-316X-2022-10-2-51-58
20. Chekushin A.V., Kotilevets I.D., Ivanova I.A., Chistyakova M.A. Handling hardware interrupts using the ATmega16 microcontroller as an example. *Promyshlennye ASU i kontrollery = Industrial Automatic Control Systems and Controllers*. 2022;1:33–39 (in Russ.). https://doi.org/10.25791/asu.1.2022.1341
19. Савиных В.П., Господинов С.Г., Кудж С.А., Цветков В.Я., Дешко И.П. Семантика визуальных моделей в космических исследованиях. *Russian Technological Journal*. 2022;10;2(46):51–58. https://doi.org/10.32362/2500-316X-2022-10-2-51-58
20. Чекушин А.В., Котилевец И.Д., Иванова И.А., Чистякова М.А. Обработка аппаратных прерываний на примере микроконтроллера ATMEGA16. *Промышленные АСУ и контроллеры*. 2022;1:33–39. http://doi.org/10.25791/asu.1.2022.1341

About the authors

Svetlana M. Ivanova, Cand. Sci. (Eng.), Associate Professor, Department of Digital Data Processing Technologies, Institute for Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: ivanova_s@mirea.ru. Scopus Author ID 36935727700, RSCI SPIN-code 4063-4665, http://orcid.org/0000-0003-3366-3233

Zoya V. Ilyichenkova, Cand. Sci. (Eng.), Associate Professor, Department of Digital Data Processing Technologies, Institute for Cybersecurity and Digital Technologies, MIREA – Russian Technological University (78, Vernadskogo pr., Moscow, 119454 Russia). E-mail: ilichenkova@mirea.ru. Scopus Author ID 6505467030, RSCI SPIN-code 4652-0380, http://orcid.org/0000-0003-2776-5364

Об авторах

Иванова Светлана Михайловна, к.т.н., доцент, кафедра КБ-14 «Цифровые технологии обработки данных» Института кибербезопасности и цифровых технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: ivanova_s@mirea.ru. Scopus Author ID 36935727700, SPIN-код РИНЦ 4063-4665, http://orcid.org/0000-0003-3366-3233

Ильиченкова Зоя Викторовна, к.т.н., доцент, кафедра КБ-14 «Цифровые технологии обработки данных» Института кибербезопасности и цифровых технологий ФГБОУ ВО «МИРЭА – Российский технологический университет» (119454, Россия, Москва, пр-т Вернадского, д. 78). E-mail: ilichenkova@mirea.ru. Scopus Author ID 6505467030, SPIN-код РИНЦ 4652-0380, http://orcid.org/0000-0003-2776-5364

Translated from Russian into English by Lyudmila O. Bychkova
Edited for English language and spelling by Dr. David Mossop