

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



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.

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: ilyichenkova@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.

ВВЕДЕНИЕ

На сегодняшний день системы аутентификации на мобильных устройствах обычно основаны на знании, которым обладает пользователь (парольная или графическая аутентификация), или на его биометрических характеристиках (аутентификация по отпечатку пальца или лицу) [1, 2]. Однако перечисленные способы, как правило, не позволяют достигнуть требуемой точности и не обладают функционалом настройки необходимого уровня безопасности [3–5]. Также возможны ситуации, когда нет возможности использовать устройство биометрической аутентификации. Например, такие ситуации могут возникать при нахождении человека в нестандартных условиях¹, когда нет возможности поднять смартфон до уровня лица [6, 7]. В связи с этим представляется целесообразным использовать многофакторную аутентификацию с использованием клавиатурного почерка пользователей мобильных устройств. Так как владелец устройства вводит текст регулярно, то почерк может все время оставаться актуальным. Также, при необходимости, это позволяет использовать почерк не только для аутентификации.

Клавиатурный почерк может формироваться на основе использования предпочтений пользователя и современных технологий, доступных для гаджетов указанного типа. К таким технологиям относится технология 3D Touch², в основе которой лежит определение силы нажатия на различные знаки сенсорной клавиатуры [8, 9]. Возможности данной разработки могут использоваться на всех современных устройствах iPhone³ и на большинстве смартфонах. 3D Touch дает возможность персонализировать способ взаимодействия пользователя с устройством.

¹ Голубкова В.Б., Брагинский А.И. *Вопросы теоретической и прикладной информатики*: учебное пособие. М.: МАДИ; 2018. 72 с. [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/>. Дата обращения 22.04.2023. / Accessed April 22, 2023.

³ <https://www.apple.com/iphone/>. Дата обращения 22.04.2023. / Accessed April 22, 2023.

Системы формирования и распознавания клавиатурного почерка, как правило, основаны на обработке сигналов программным образом [10–12]. Поэтому способ аутентификации на мобильных устройствах по клавиатурному почерку, основанному, в т.ч. на использовании технологии 3D Touch, является относительно недорогим и хорошо встраиваемым в существующие системы.

Биометрический почерк включает в себя статистическую обработку данных, полученных при вводе пользователем какой-либо фразы [13, 14]. Следует отметить, что при осуществлении парольной аутентификации фраза, вводимая пользователем, как правило, является фиксированной. Однако при примерном совпадении паролей различных пользователей повышается вероятность совпадения клавиатурного почерка, в основе формирования которого лежит длительность нажатия на определенный символ. Как показали исследования, использование только клавиатурного почерка не позволяет гарантировать необходимую достоверность аутентификации [15, 16]. Более того, с повсеместным распространением мобильных устройств длительность нажатия постепенно изменяется, что не позволяет рассматривать этот параметр как определяющий [17].

При установлении клавиатурного почерка пользователя следует принимать во внимание следующие факторы: тождественность смартфона или иного устройства аутентификации, психофизические характеристики состояния владельца устройства в комплексе [18, 19]. Однако если определяются статистические данные почерка для аутентификации на конкретном устройстве, то первый аспект можно не учитывать [20].

ФОРМИРОВАНИЕ ИНФОРМАЦИИ О КЛАВИАТУРНОМ ПОЧЕРКЕ

В условиях быстрого развития программного обеспечения при использовании парольной аутентификации интересным представляется включить в рассмотрение такие факторы, как способ взаимодействия пользователя с сенсорной клавиатурой.

Для формирования клавиатурного почерка могут быть использованы следующие характеристики:

скорость и динамика ввода, частота допущенных ошибок, длительность пауз / наложение сигналов, значение 3D Touch при работе с сенсорной клавиатурой.

В мобильных устройствах существует несколько типов сенсорных клавиатур. Чаще всего пользователь использует одну и ту же раскладку, к которой привык. Однако иногда для удобства ввода тип клавиатуры может меняться. В зависимости от типа клавиатуры меняется не столько длительность нажатия на клавиши, сколько интервал между значащими клавишами. При вводе пароля, интервал также меняется, если пользователю приходится переключаться от символьной клавиатуры к цифровой. На мобильных устройствах длительность или сила нажатия на символ могут быть различными при выборе цифр или служебных знаков в зависимости от использования клавиатуры, т.к. их можно выбирать на основной раскладке, удерживая палец, или включать специальный соответствующий набор знаков.

Использование результатов работы механизма 3D Touch позволяет градуировать силу нажатия и определить несколько уровней в соответствии с полученной величиной. Наиболее простой является следующая градация: обычное нажатие и сильное давление. В первом случае предполагается стандартная работа пользователя с экраном мобильного устройства при выполнении действий. Во втором случае имеет место более сильное давление на символы, что приводит к физическому воздействию, сопровождающемуся прогибом стеклянной панели. Для дифференциации данных уровней силы воздействия предусмотрено использование механизма 3D Touch. Для определения силы нажатия можно использовать свойство Force объекта UITouch, которое присутствует у объектов iPhone версии 6 и выше и характеризует силу касания. Свойство MaximumPossibleForce характеризует максимально возможную величину силы касания. Используя оба значения, можно определять относительное значение силы нажатия на символ. Величина 1.0 представляет среднюю силу, определенную системой.

Для повышения надежности парольной фразы при ее составлении требуется использовать не только символы латинского алфавита, но также цифры и служебные символы. В разных мобильных устройствах используются различные типы клавиатур. Однако во всех устройствах специальные символы вынесены в отдельную клавиатуру. Иногда на специальной вкладке находятся и цифровые клавиши. Поэтому силу нажатия на знаки предлагается дополнить информацией о длительности пауз между информационными (входящими в пароль) символами, требующими переключения клавиатуры.

Процесс распознавания пользователя является двухэтапным. Первый этап требуется для исходного

формирования клавиатурного почерка пользователя. Полученные данные используются на следующем этапе для аутентификации. Сочетание двух этапов позволяет сделать вывод о легитимности пользователя или о попытке войти в систему злоумышленником.

В соответствии с вышеизложенным предлагается формировать клавиатурный почерк, взяв в качестве его характеристик среднее выборки и среднеквадратичное отклонение силы нажатия и интервалов между нажатиями на символы. Эта пара статистических данных характеризуется их разнородностью, что позволяет точнее проводить оценку.

На первом этапе каждый пользователь несколько раз вводит парольную фразу, отвечающую требованиям безопасности. Для повышения репрезентативности выборки можно сформулировать дополнительные требования к паролю, включающие не только обобщенные правила, но и определяющие последовательность набора. Например, можно включить необходимость неоднократного переключения от одного типа символов к другому.

В соответствии с выбранными параметрами требуемые характеристики вычисляются посимвольно и группируются (табл. 1, 2).

Таблица 1. Формат представления данных о силе нажатия на символы

Символ (x_i)	Среднее выборки ($\bar{x}$)	Среднеквадратичное отклонение (σ_x)
...	...	...

Таблица 2. Формат представления данных об интервалах между нажатиями на символы

Последовательные символы (x_i)	Среднее выборки ($\bar{x}$)	Среднеквадратичное отклонение (σ_x)
...	...	...

Вычисление значений второго и третьего столбцов таблиц осуществляется по формулам:

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

где переменная n показывает, сколько раз была повторена парольная фраза.

Так как при аутентификации полученные данные x_{n+1} будут различаться, требуется определить возможный диапазон значений ($x_{\min}$, $x_{\max}$), попадание в который будет свидетельствовать о легитимности пользователя. При этом удобным является наличие возможности варьировать длину интервала в зависимости от требуемой вероятности возникновения

ошибок. Поэтому представляется целесообразным при определении границ интервала учитывать значение среднеквадратичного отклонения:

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

где $\Phi(\cdot)$ – функция Лапласа, а распределение случайной величины x является нормальным.

При аутентификации возможны ошибки первого рода (т.е. легальный пользователь не признается таковым) и второго рода (происходит распознавание злоумышленника как зарегистрированного пользователя). Для снижения ошибок второго рода значение вероятности ошибочного распознавания пользователя будет уменьшаться.

Так как в системах распознавания отклонения от среднего значения в обе стороны равнозначны, то вероятность попадания в требуемый интервал можно записать в виде:

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

Тем самым, значения границ допустимого диапазона можно регулировать в зависимости от допустимости ошибок первого или второго рода.

После формирования клавиатурного почерка аутентификация пользователя происходит посредством ввода пароля. Для новой фразы определяются те же статистические характеристики и проверяется их попадание в заданный интервал. В зависимости от результата принимается решение о легитимности пользователя.

ЭКСПЕРИМЕНТАЛЬНАЯ АУТЕНТИФИКАЦИЯ

Для проверки работоспособности предложенного способа контроля пользователя была написана программа для получения информации об интенсивности ввода данных и силе нажатия на символы клавиатуры мобильного устройства. При работе использовалась платформа iOSXcode⁴. Вычисления производились для 10 последовательных вводов, выполненных в одинаковых условиях. Для трех различных пользователей (Польз1, Польз2, Польз3) были рассчитаны соответствующие статистические характеристики для введенных данных «1@35f1» (табл. 3–5). Величина 1.0 силы нажатия представляет среднюю силу, определенную системой.

⁴ Xcode. <https://developer.apple.com/xcode/>. Дата обращения 22.04.2023. / Accessed April 22, 2023.

Таблица 3. Данные о величине силы нажатия на символы (Польз1)

Символ	Среднее выборки	Среднеквадратичное отклонение
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

Таблица 4. Данные о величине силы нажатия на символы (Польз2)

Символ	Среднее выборки	Среднеквадратичное отклонение
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

Таблица 5. Данные о величине силы нажатия на символы (Польз3)

Символ	Среднее выборки	Среднеквадратичное отклонение
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

Полученные данные о величине силы нажатия на разные символы в виде диаграммы сравнения приведены на рис. 1 для каждого из трех пользователей. Результаты были получены для вероятности распознавания пользователя, равной 0.95.

Согласно этим данным, полученные диапазоны не накладываются друг на друга только для знака «3». Однако выборка по одному символу не может считаться достаточной. Поэтому предлагается добавить к анализу данные, основанные на интервалах между нажатиями значащих символов без учета нажатий переключения типа клавиатуры (табл. 6–8).

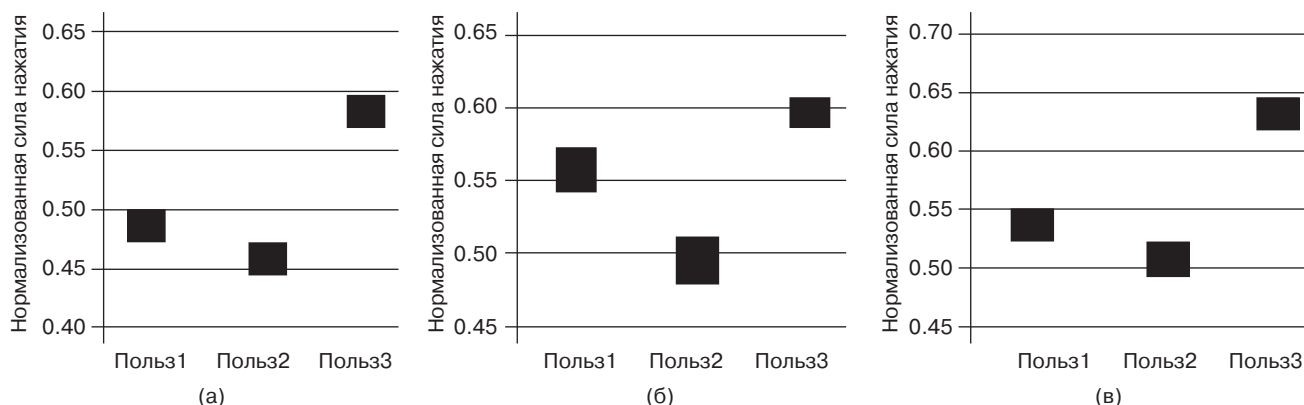


Рис. 1. Допустимые диапазоны силы нажатия:
(а) символ «@», (б) символ «3», (в) символ «5»

Таблица 6. Данные о величине интервала между нажатиями (Польз1)

Последовательные символы	Среднее выборки (10^{-6} , с)	Среднеквадратичное отклонение (10^{-6} , с)
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

Таблица 8. Данные о величине интервала между нажатиями (Польз3)

Последовательные символы	Среднее выборки (10^{-6} , с)	Среднеквадратичное отклонение (10^{-6} , с)
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

Таблица 7. Данные о величине интервала между нажатиями (Польз2)

Последовательные символы	Среднее выборки (10^{-6} , с)	Среднеквадратичное отклонение (10^{-6} , с)
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

Анализ полученных данных показывает, что временной интервал между нажатием символов, расположенных на одной клавиатуре, также не гарантирует требуемой дифференциации значений (рис. 2в), в то время как переключение клавиатуры с символьной на цифровую (Польз2, Польз3) или выбор цифровых или служебных символов с помощью усиленного нажатия на символы основной клавиатуры (Польз1) позволяет добиться необходимой разницы в характеристиках клавиатурного почерка (рис. 2а, б).

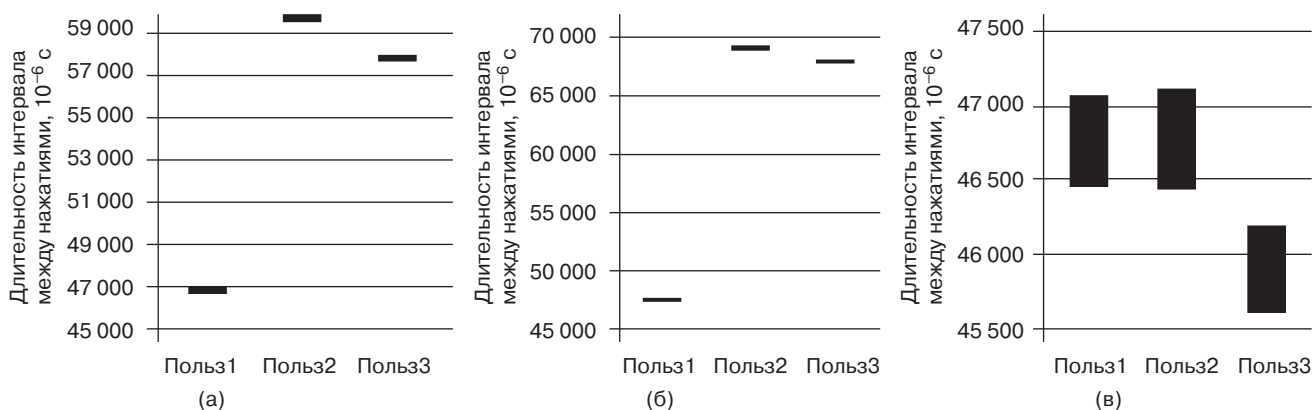


Рис. 2. Допустимые диапазоны интервалов между нажатиями символов
(а) «1-@», (б) «@-3», (в) «3-5»

ЗАКЛЮЧЕНИЕ

При использовании парольной аутентификации применение дополнительной информации о клавиатурном почерке, основанном на силе нажатия на клавиши и длительности между последовательными нажатиями, позволяет повысить точность распознавания согласно требуемой вероятности. К достоинствам предложенного метода относится возможность изменения параметров для соблюдения баланса между ошибками первого и второго рода. Получение новой информации в том же формате, в котором находилась исходная информация, позволяет при необходимости обновлять данные для их актуализации.

БЛАГОДАРНОСТИ

Авторы выражают благодарность руководству «МИРЭА – Российский технологический университет» за оказанную помощь в исследованиях.

ACKNOWLEDGMENTS

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

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](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>

Вклад авторов

С.М. Иванова – развитие ключевых целей и задач; проведение исследований, в т.ч. анализ специфики использования мобильных устройств при формировании клавиатурного почерка; разработка математического аппарата анализа данных.

З.В. Ильиченкова – формирование идеи статьи; проведение исследований, в т.ч. анализ возможности использования комбинации нескольких характеристик для формирования клавиатурного почерка; обработка и анализ статистических данных.

Все авторы – написание текста статьи; утверждение окончательного варианта статьи; интерпретация результатов исследования; формулировка выводов.

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](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>

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>
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., Kälviäinen 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., Чащина 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., Лаврычев 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., Maksimych 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>
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. 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., Kälviäinen 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>

18. Каримов М.Т., Никонов В.В. Сравнение производительности моделей сверточных нейронных сетей на графическом процессоре. *Информационные и телекоммуникационные технологии*. 2021;52:42–48.
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>
15. Pronin C.B., Maksimych 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. 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 kontroly = 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 kontroly = Industrial Automatic Control Systems and Controllers*. 2022;1:33–39 (in Russ.). <https://doi.org/10.25791/asu.1.2022.1341>

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>

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>