Научная статья
УДК 002.5:004
DOI: 10.14529/ctcr220303

НЕКОТОРЫЕ ПОДХОДЫ К ОЦЕНКЕ ИНФОРМАТИВНОСТИ ПАРАМЕТРОВ ИДЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ ПО КЛАВИАТУРНОМУ ПОЧЕРКУ НА ОСНОВЕ ПОВЕДЕНЧЕСКОЙ БИОМЕТРИИ

***Л.А. Артюшина**, larisa-artusina@yandex.ru*
***Е.А. Троицкая**, troickiyv@mail.ru*
Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия

Аннотация. В отечественных нормативных документах, в частности в Национальном стандарте РФ по защите информации, обозначены три уровня доверия к результатам идентификации, основанные на некоторой степени уверенности в подлинности субъекта доступа, но не содержащей конкретных значений. В статье предложены подходы к качественной оценке информативности параметров идентификации пользователя по клавиатурному почерку на основе поведенческой биометрии. **Цель исследования:** оценка информативности параметров идентификации пользователя по клавиатурному почерку. **Материалы и методы исследования.** Для определения подходов к оценке информативности параметров нами были изучены и проанализированы известные научные результаты и практические решения по проблеме идентификации пользователей в информационно-телекоммуникационных компьютерных системах, размещенные в различных открытых источниках на русском и английском языках. **Основные результаты.** Выделены актуальные на сегодняшний день совокупность параметров, идентифицирующих пользователя по клавиатурному почерку, перечень зашумлений, влияющих на информативность параметров. Рассчитаны средние значения уровней надежности идентификации. Определены основные и дополнительные критерии оценки информативности параметров. В качестве основных критериев оценки надежности идентификации по клавиатурному почерку выделены коэффициенты ложного доступа и ложного отказа в доступе, общая оценка системы. В качестве дополнительных критериев выделены скорость работы, простота использования, стоимость системы. Для основных критериев обозначены показатели, которые мы предлагаем использовать в качестве оценочных характеристик, по которым можно было бы судить о степени достижения критерия: стабильность параметра в различении пользователей друг от друга; количество реализаций параметра, требуемых для обеспечения его стабильности в различении пользователей. Приведены качественные характеристики степени информативности параметров по основным критериям. Определены направления дальнейших исследований. **Заключение.** Представленные в статье перечень параметров и зашумлений, оценка надежности идентификации по критериям и соответствующим им показателям будут полезны разработчикам и исследователям для дальнейшей доработки методов идентификации с целью повышения их надежности.

Ключевые слова: методы идентификации, биометрическая идентификация пользователя, клавиатурный почерк

Для цитирования: Артюшина Л.А., Троицкая Е.А. Некоторые подходы к оценке информативности параметров идентификации пользователя по клавиатурному почерку на основе поведенческой биометрии // Вестник ЮУрГУ. Серия «Компьютерные технологии, управление, радиоэлектроника». 2022. Т. 22, № 3. С. 30–38. DOI: 10.14529/ctcr220303

Original article
DOI: 10.14529/ctcr220303

SOME APPROACHES TO ASSESSING THE INFORMATIVE OF USER IDENTIFICATION PARAMETERS BY KEYBOARD HANDWRITING BASED ON BEHAVIORAL BIOMETRICS

***L.A. Artyushina**, larisa-artusina@yandex.ru*
***E.A. Troitskaya**, troickiyv@mail.ru*
Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia

Abstract. Domestic normative documents, in particular the National Standard of the Russian Federation on Information Protection, outlines three levels of confidence in the results of identification, based on some degree of confidence in the authenticity of the subject of access, but not containing specific values. The article proposes approaches to qualitative assessment of informativeness of user identification parameters by keyboard handwriting on the basis of behavioral biometrics. **Objective of the study.** Evaluation of informativeness of user identification parameters by keyboard handwriting. **Materials and methods of research.** To determine approaches to assessing the informativeness of parameters, we studied and analyzed known scientific results and practical solutions on the problem of user identification in information and telecommunication computer systems, available in various open sources in Russian and English. Main results. We identified the currently relevant set of parameters, identifying the user by the keyboard handwriting; the list of noises affecting the informativeness of the parameters. Average values of identification reliability levels were calculated. The basic and additional criteria for evaluating the informativeness of the parameters were defined. False access and false denial rates and overall system evaluation were selected as basic criteria for evaluating reliability of identification by handwriting. As additional criteria the speed of operation, ease of use, the cost of the system are highlighted. For the main criteria the indicators that we propose to use as evaluation characteristics, which could be used to judge the degree of achievement of the criterion: the stability of the parameter in distinguishing users from each other; the number of implementations of the parameter, required to ensure its stability in distinguishing users. The qualitative characteristics of the degree of informativeness of the parameters on the main criteria are given. The directions for further research are defined. **Conclusion.** The list of parameters and noises presented in the article, the assessment of identification reliability by criteria and corresponding indicators will be useful to developers and researchers for further refinement of identification methods to improve their reliability.

Keywords: identification methods, biometric user identification, keyboard handwriting

For citation: Artyushina L.A., Troitskaya E.A. Some approaches to assessing the informative of user identification parameters by keyboard handwriting based on behavioral biometrics. *Bulletin of the South Ural State University. Ser. Computer Technologies, Automatic Control, Radio Electronics*. 2022;22(3):30–38. (In Russ.) DOI: 10.14529/ctcr220303

Введение

Задаче идентификации пользователя по клавиатурному почерку посвящено большое количество работ. Этот факт обусловлен все возрастающей актуальностью информационно-телекоммуникационных компьютерных систем (ИТКС), отличительной чертой которых является выработка на основе идентификации субъекта, не обязательно являющегося пользователем, оптимальных управляющих воздействий, механизмов выявления нарушителей и построения адекватной системы защиты информации, циркулирующей в ИТКС.

Актуальность поведенческой биометрии обусловлена такими преимуществами, как неотделимость биометрической характеристики от владельца, при этом сохраняется анонимность образов (невозможность установления личности владельца по его биометрическому образу), сложность подделки, простота внедрения и реализации [1–5].

Введем необходимые рабочие определения.

Вслед за работой [6] под ИТКС будем понимать взаимосвязанную совокупность информационных ресурсов, средств вычислительной техники, телекоммуникаций, программного обеспечения, персонала и пользователей.

На основании Национального стандарта РФ по защите информации [7] в рамках тематики статьи под процедурой идентификации будем понимать действия ИКТС по присвоению конкретному субъекту идентификатора доступа и/или по сравнению предъявляемого ИТКС идентификатора с перечнем уже присвоенных идентификаторов.

Идентификатором доступа считать признак субъекта, который используется ИТКС при идентификации и однозначно определяет соотнесенную с ним идентификационную информацию.

Идентификационной информацией будем считать совокупность значений идентификационных атрибутов, которая связана с конкретным субъектом.

Цель работы – оценка информативности параметров идентификации по клавиатурному почерку. Для достижения поставленной цели решались следующие **задачи**:

– анализ достигнутых результатов в области биометрической идентификации по клавиатурному почерку;

– на основе проведенного анализа определение актуальных на сегодняшний день:

o перечня входных параметров (далее параметры) идентификации пользователя по клавиатурному почерку на основе поведенческой биометрии;

o совокупности факторов (зашумлений), влияющих на информативность параметров;

o основных критериев надежности идентификации пользователя ИТКС и соответствующих им показателей;

– уточнить критерии и показатели оценки степени информативности каждого из параметров;

– определить перспективы дальнейших исследований в области оценки информативности параметров идентификации по клавиатурному почерку.

1. Параметры, идентифицирующие пользователя по клавиатурному почерку

Вслед за [8] клавиатурным почерком будем считать набор динамических характеристик работы пользователя на клавиатуре.

Анализ научных публикаций по проблеме идентификации по клавиатурному почерку [1–6, 8–15] позволил нам в качестве возможных входных параметров для методов этой группы указать:

1) количество ошибок при наборе (частота нажатия на клавишу delete);

2) звуковые сигналы, воспроизводимые с помощью клавиатуры при наборе текста пользователем;

3) время нажатия – это период времени, в течение которого клавиша находится в нажатом состоянии;

4) паузы между нажатиями (в некоторых исследованиях «временные задержки при вводе») – это период времени между нажатиями клавиш;

5) наличие факта удержания одной из клавиш;

6) отсутствие факта удержания одной из клавиш;

7) наличие факта удержания одновременно двух клавиш;

8) часто используемые сочетания клавиш – предпочитаемые пользователем комбинации клавиш клавиатуры, ускоряющие его работу с ИТКС;

9) наличие факта использования основной или дополнительной части клавиатуры, клавиш *Shift* или *CapsLook* при вводе заглавных букв;

10) характер нажатий клавиш – одинарный, сдвоенный или строенный;

11) скорость набора – количество набираемых знаков в минуту;

12) общее время набора *ID*;

13) число перекрытий между клавишами (наложение клавиш) происходит тогда, когда одна клавиша еще не отпущена, а другая уже нажимается;

14) степень аритмичности при наборе – характеризует равномерность скорости набора пользователем символов *ID*;

15) силу давления, прилагаемого к клавише;

16) *flight time* (время полета) – период времени между отпусканием одной клавиши и отпусканием другой, находящейся в данный момент в режиме удержания;

17) *Up to Up* – период времени между последовательным отпусканием одной нажатой клавиши и затем другой нажатой клавиши.

18) положение кистей рук относительно клавиатуры;

19) количество случаев использования дополнительных клавиш в единицу времени;

20) скорость движения клавиш при надавливании их пользователем – вычисляется как скорость изменения ёмкости контактной площадки во времени;

21) вибрация клавиши при нажатии на нее;

22) код нажатой клавиши;

23) частота использования функциональных клавиш и комбинаций применительно к одному и тому же классу устройств ввода.

На основе анализа работ [1–6, 8–16] нами также была определена совокупность факторов (зашумлений), влияющих на информативность параметров:

1) эмоциональное состояние;

2) зависимость особенностей работы пользователя от характера выполняемых задач и времени суток;

3) степень покрытия символами, используемыми для идентификации, поля клавиатуры компьютера;

4) возможность набора пользователем идентификационной фразы одной рукой (или одним пальцем) по его желанию или по причине травмы конечности;

5) технические характеристики клавиатуры: форма (прямая, эргономичная и т. д.), степень легкости нажатия на клавишу, расположение клавиш (QWERTY, AZERTY и т. д.);

6) зависимость между стабильностью клавиатурного почерка и уровнем пользователя;

7) нерегулярный характер работы пользователя за компьютером;

8) зависимость точности измерения таймера, захватывающего время, в течение которого произошло событие на клавиатуре, от установленной на компьютере операционной системы и языка программирования.

Проведенный анализ позволил сделать следующие выводы.

1. Признавая факт влияния зашумлений на информативность параметров, исследователи не уделяют изучению этого вопроса должного внимания. Из научных публикаций не ясно, какова взаимосвязь зашумлений и параметров, а также, как именно зашумления влияют на информативность параметров.

2. В силу большого количества для решения задачи идентификации параметры необходимо ранжировать по степени их информативности, т. е. значимости в смысле надежности идентификации в результате измерения значений параметра.

В работах [17] показано, что при наличии пяти анализируемых параметров создание системы идентификации весьма проблематично, а при десяти – практически невозможно. Упорядочивание позволит отсеять наименее информативные параметры, уменьшить размер обучающей выборки и, как следствие, получить максимальное значение целевой функции, характеризующей вероятность принадлежности клавиатурного почерка конкретному пользователю.

В нормативных документах, в частности в Национальном стандарте РФ по защите информации [7], обозначены три уровня доверия к результатам идентификации (низкий, средний, высокий), основанные на некоторой степени уверенности в подлинности субъекта доступа, но не содержащей конкретных значений. Для решения задачи идентификации необходимо иметь конкретные значения нормы этой степени уверенности.

Основываясь на исследованиях [18, 19], мы рассчитали средние значения уровней надежности идентификации (НИ):

– высокий – НИ $\geq$ 90 %;

– средний – 87 % $\leq$ НИ < 90 %;

– низкий – НИ < 87 %.

2. Критерии и показатели оценки информативности параметров идентификации по клавиатурному почерку

В современных исследованиях надежность идентификации пользователя определяется с помощью трех основных критериев [3, 11, 12, 19–21]:

1) FAR-коэффициент ложного доступа, т. е. вероятность допуска незарегистрированного пользователя или «ошибка 2-го рода»;

2) FRR-коэффициент ложного отказа в доступе, «ошибка 1-го рода»;

3) EER (или CER) – общая оценка системы (или средняя интегральная ошибка), описывается при помощи равного уровня ошибок FAR = FRR.

Следует отметить, что в оценке надежности идентификации исследователями и разработчиками в основном используются FAR- и FRR-критерии (в 18 из 25 проанализированных нами работ) и редко (в 3 из 25) ERR-критерий.

Исследователи указывают также на ряд дополнительных критериев, таких как скорость работы, простота использования, стоимость системы и т. д.

Однако, обозначая критерии, исследователи четко не определяют оценочные характеристики, по которым можно было бы судить о степени достижения критерия.

Для того чтобы ранжировать указанные выше параметры по трем основным критериям, мы обозначили соответствующие им показатели. Мы связали с показателем характеристики, по значению которых можно было бы судить о степени достижения критерия.

Основываясь на результатах анализа работ [1–25], для основных критериев в качестве показателей мы выделили:

- стабильность параметра в различении пользователей друг от друга, а именно:
  - для FAR-коэффициента – стабильно малая величина вероятности ложного доступа при наличии различных зашумлений из указанного перечня;
  - FRR-коэффициента – стабильно малая величина вероятности ложного отказа в доступе при наличии различных зашумлений из указанного перечня;
  - EER-коэффициента – стабильно малая величина средней интегральной ошибки при наличии различных зашумлений из указанного перечня;
- количество реализаций параметра, требуемых для обеспечения его стабильности в различении пользователей (КРП).

3. Характеристика степени информативности параметров по FAR-, FRR-, EER-критериям

Основываясь на результатах исследований, представленных в работах [1–25], и выделенных показателях, приведем характеристику степени информативности параметров по критериям.

По FAR-критерию:

- высокая степень – $0{,}01 \le FAR \le 0{,}02$;
- средняя степень – $0{,}02 < FAR \le 0{,}03$;
- низкая степень – $FAR > 0{,}03$.

Допустимая величина ложных срабатываний обуславливается принятым соглашением заинтересованных сторон и характеризуется частотой ложных срабатываний системы (ЧЛСС).

Охарактеризуем степень информативности параметра по FRR-критерию:

- высокая степень – ЧЛСС ≤ 1 %;
- средняя степень – 1 % < ЧЛСС ≤ 3 %;
- низкая степень – ЧЛСС > 3 %.

Охарактеризуем степень информативности параметров по ERR-критерию:

- высокая степень – $0 \le ERR \le 0{,}00372$;
- средняя степень – $0{,}00372 < ERR \le 0{,}14$;
- низкая степень – $EER > 0{,}14$.

Рассмотрим четвертый критерий оценки надежности идентификации пользователя – количество реализаций параметра, требуемых для обеспечения его стабильности в различении пользователей.

В работе [17] показано, что для большинства признаков клавиатурного почерка для надежной идентификации достаточно 26 реализаций параметра. Анализ других исследований, посвященных проблеме идентификации по клавиатурному почерку, показал большой разброс значений КРП, обеспечивающих высокий уровень идентификации. Так, в [13] – 10 реализаций параметра, в [24] – 30, в [17, 25] значения варьируются в пределах от 21 до 24.

Основываясь на этих результатах, дадим характеристику степени информативности параметров по КРП-критерию:

- высокая степень – 24–26 реализаций;
- средняя степень – 16–23 реализации;
- низкая степень – менее 16 реализаций.

Сводная таблица критериев и уровней их достижения представлена ниже.

Характеристики уровней степени информативности параметров клавиатурного почерка (по критериям)
Characteristics of the levels of the degree of informative of the parameters of keyboard handwriting (according to criteria)

№	Название критерия	Характеристика степени информативности параметров по критериям
1	FAR	– высокая степень – $0{,}01 \le FAR \le 0{,}02$; – средняя степень – $0{,}02 < FAR \le 0{,}03$; – низкая степень – $FAR > 0{,}03$
2	FRR	– высокая степень – ЧЛСС ≤ 1 %; – средняя степень – 1 % < ЧЛСС ≤ 3 %; – низкая степень – ЧЛСС > 3 %
3	ERR	– высокая степень – $0 \le ERR \le 0{,}00372$; – средняя степень – $0{,}00372 < ERR \le 0{,}14$; – низкая степень – $EER > 0{,}14$
4	КРП	– высокая степень – 24–26 реализаций; – средняя степень – 16–23 реализации; – низкая степень – менее 16 реализаций

Заключение

Проведенный нами анализ результатов исследований по проблеме идентификации пользователя по клавиатурному почерку показал, что оценка информативности параметров производится по FAR-, FRR-, CER-критериям. Однако показатели степени достижения критерия описаны в нормативных документах в общем виде, без указания конкретного диапазона значений, что, на наш взгляд, позволяет исследователям слишком широко, в смысле надежности идентификации, трактовать полученные ими результаты. В статье представлена попытка решения обозначенной проблемы.

Направления дальнейшего исследования проблемы:

1. В работе представлена совокупность параметров, идентифицирующих пользователя по клавиатурному почерку, и зашумлений, влияющих на их информативность. Очевидно, дальнейшее исследование связано с расширением состава этой совокупности и с ее систематизацией, а также изучением влияния зашумлений на информативность параметров.

2. Вопрос степени достижения FAR- и FRR-критериев изучен достаточно хорошо, для ERR- и КПР-критериев требуются более обстоятельные и глубокие исследования.

Таким образом, исследуемая проблема многоаспектна и не может быть исчерпана настоящей работой. Требуются объединенные усилия ученых различных профилей для рассмотрения как можно большего количества связей и отношений в ней.

Список литературы

1. Сапиев А.З. Идентификация пользователей сети по клавиатурному почерку // Вестник Вологодского государственного университета. Серия: Технические науки. 2020. № 4 (10). С. 45–46.

2. Пащенко Д.В., Бальзанникова Е.А. Метод идентификации пользователя по клавиатурному почерку с использованием модели доверия // XXI век: итоги прошлого и проблемы настоящего плюс. 2021. № 3 (55). С. 96–99. DOI: 10.46548/21vek-2021-1055-0018

3. Казачук М.А. Динамическая аутентификация пользователей на основе анализа работы с клавиатурой компьютера: дис. … канд. физ.-мат. наук: 05.13.11. М.: Моск. гос. ун-т им. М.В. Ломоносова, 2019. 155 с.

4. Исследование системы идентификации и подтверждения легитимности доступа на основе динамических методов биометрической аутентификации / М.М. Путято, А.С. Макарян, Ш.М. Чич, В.К. Маркова // Прикаспийский журнал: управление и высокие технологии. 2020. № 3 (51). С. 83–93. DOI: 10.21672/2074-1707.2020.51.1.083-093

5. Еременко Ю.И., Олюнина Ю.С. Об обработке потока данных с целью выявления скрытых характеристик клавиатурного почерка // Материалы XII Междунар. науч.-практ. конф. «Современные сложные системы управления. HTCS'2017». Липецк: Липецкий гос. техн. ун-т, 2017. Ч. 2. С. 31–36.

6. Модели обеспечения достоверности и доступа информации в информационно-телекоммуникационных системах / М.Ю. Монахов, Ю.М. Монахов, Д.А. Полянский, И.В. Семенова. Владимир: Изд-во ВлГУ, 2015. 208 с.

7. ГОСТ Р 58833–2020. Национальный стандарт Российской Федерации. Защита информации. Идентификация и аутентификация. М.: Стандартинформ, 2020. 32 с.

8. Горохова Е.С. Алгоритмы распознавания компьютерного почерка / под ред. Т.Е. Мамоновой // Сборник трудов XIII Международной научно-практической конференции студентов, аспирантов и молодых учёных. Томск: Нац. исслед. Томский политехн. ун-т, 2016. С. 83–84.

9. Еременко Ю.И., Олюнина Ю.С. Об определении наиболее значимых параметров клавиатурного почерка с помощью регрессионного анализа // Системы управления и информационные технологии. 2018. № 2 (72). С. 28–31.

10. Еременко А.В., Сулавко А.Е. Двухфакторная аутентификация пользователей компьютерных систем на удаленном сервере по клавиатурному почерку // Прикладная информатика. 2015. № 6 (60). С. 48–59.

11. Аверин А.И., Сидоров Д.П. Аутентификация пользователей по клавиатурному почерку. URL: http://journal.mrsu.ru/arts/autentifikaciya-polzovatelej-po-klaviaturnomu-pocherku (дата обращения: 17.06.2022).

12. Аюпова А.Р., Якупов А.Р., Шабалкина А.А. Аутентификация по клавиатурному почерку: выгоды и проблемы использования // Международный научно-исследовательский журнал. 2017. № 12-5 (66). С. 55–58. DOI: 10.23670/IRJ.2017.66.123

13. Васильев В.И., Калямов М.Ф., Калямова Л.Ф. Идентификация пользователей по клавиатурному почерку с применением алгоритма регистрации частых биграмм // Моделирование, оптимизация и информационные технологии. 2018. Т. 6, № 1. С. 399–407.

14. Довгаль В.А. Захват параметров клавиатурного почерка и его особенности / отв. ред. Н.Н. Олейников // Информационные системы и технологии в моделировании и управлении: материалы Всерос. науч.-практ. конф. Симферополь: ООО «Издательство Типография «Ариал», 2017. С. 230–236.

15. Identity Theft, Computers and Behavioral Biometrics / R. Moskovitch, C. Feher, A. Messerman et al. URL: https://www.ise.bgu.ac.il/faculty/liorr/idth.pdf (дата обращения: 01.06.2022).

16. Распознавание психофизиологических состояний пользователей на основе скрытого мониторинга действий в компьютерных системах / В.И. Васильев, А.Е. Сулавко, Р.В. Борисов и др. // Искусственный интеллект и принятие решений. 2017. № 3. С. 21–37.

17. Сулавко А.Е., Еременко А.В. Метод сжатия собственных областей классов образов в пространстве малоинформативных признаков // Искусственный интеллект и принятие решений. 2014. № 2. С. 102–109.

18. Асяев Г.Д., Рагозин А.Н. Определение минимального набора входных данных для корректной аутентификации по клавиатурному почерку с использованием нейронной сети // Вестник УрФО. 2017. № 3 (25). С. 19–23.

19. Шарипов Р.Р., Ситников А.Н. Проблемы при разработке систем распознавания пользователей по клавиатурному почерку // Вестник технологического университета. 2019. Т. 22, № 10. С. 143–147.

20. Брюхомицкий Ю.А., Казарин М.Н. Тестирование биометрических систем контроля доступа // Информационное противодействие угрозам терроризма. 2006. № 8. С. 168–180.

21. Григорьев В.Р., Никитин А.П. Использование статических методов для биометрической идентификации пользователя // Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2012. № 14 (94). С.135–143.

22. Костюченко Е.Ю., Мещеряков Р.В. Распознавания пользователя по клавиатурному почерку на фиксированной парольной фразе в компьютерных системах // Известия ТРТУ. 2003. № 4 (33). С. 177–178.

23. Hidden Authentication of the User Based on Neural Network Analysis of the Dynamic Profile /

A. Sivova, A. Vulfin, K. Mironov, A. Kirillova. URL: http://dx.doi.org/10.25673/32764 (дата обращения: 01.04.2022).

24. Искандарова З.А. Методы повышению надежности идентификации пользователей компьютерных систем по написанию паролей // Энигма. 2020. № 27-3. С. 162–172.

25. Сулавко А.Е., Федотов А.А., Еременко А.В. Распознавание пользователей компьютерных систем по клавиатурному почерку с учетом параметров вибрации и давления на клавиши // Динамика систем, механизмов и машин. 2017. Т. 5, № 4. С. 95–105. DOI: 10.25206/2310-9793-2017-5-4-95-105

References

1. Sapiev A.Z. [Identification of network users by keyboard handwriting]. *Bulletin of Vologda state university. Series technical sciences*. 2020;4(10):45–46. (In Russ.)

2. Pashchenko D.V., Bal′zannikova E.A. [Method of user identification by keyboard handwriting using the trust model]. *XXI century: results of the past and problems of the present plus*. 2021;3(55):96–99. DOI: 10.46548/21vek-2021-1055-0018 (In Russ.)

3. Kazachuk M.A. *Dinamicheskaya autentifikatsiya pol'zovateley na osnove analiza raboty s klaviaturoy komp'yutera: dis. fiz.-mat. nauk* [Dynamic User Authentication Based on Computer Keyboard Operation Analysis. Cand. sci. diss.]. Moscow; 2019. 155 p. (In Russ.)

4. Putyato M.M., Makaryan A.S., Chich Sh.M., Markova V.K. [Research of the system of identification and confirmation of the legitimacy of access based on dynamic methods of biometric authentication]. *Caspian journal: control and high technologies*. 2020;3(51):83–93. (In Russ.) DOI: 10.21672/2074-1707.2020.51.1.083-093 (In Russ.)

5. Yeremenko Yu. I., Olyunina Yu.S. [About data stream processing in order to reveal hidden characteristics of keyboard handwriting]. In: *Materialy XII Mezhdunar. nauch.-prakt. konf. "Sovremennyye slozhnyye sistemy upravleniya. HTCS'2017"* [Materials of the XII International scientific and practical conference "Modern complex control systems. HTCS'2017"]. Lipetsk; 2017. Part 2. P. 31–36. (In Russ.)

6. Monakhov M.Yu., Monakhov Yu.M., Polyanskiy D.A., Semenova I.V. *Modeli obespecheniya dostovernosti i dostupa informatsii v informatsionno-telekommunikatsionnykh sistemakh* [Models for ensuring the reliability and access of information in information and telecommunication systems]. Vladimir: Vladimir St. Univ.; 2015. 208 p. (In Russ.)

7. *GOST R 58833–2020. Natsional'nyy standart Rossiyskoy Federatsii. Zashchita informatsii. Identifikatsiya i autentifikatsiya* [State Standard R 58833–2020. National Standard of the Russian Federation. Information protection. Identification and Authentication]. Moscow: Standartinform Publ.; 2020. 32 p. (In Russ.)

8. Gorokhova E.S. [Computer handwriting recognition algorithms]. In: *Sbornik trudov XIII Mezhdunarodnoy nauchno-prakticheskoy konferentsii studentov, aspirantov i molodykh uchenykh* [Proceedings of the XIII International Scientific-Practical Conference of Students, Graduate Students and Young Scientists]. Tomsk: National Research Tomsk Polytechnic University; 2016. P. 83–84. (In Russ.)

9. Yeremenko Yu.I., Olyunina Yu.S. [On determining the most significant parameters of keyboard handwriting using regression analysis]. *Sistemy upravleniya i informatsionnyye tekhnologii*. 2018;2(72):28–31. (In Russ.)

10. Eremenko A.V., Sulavko A.E. [Two-factor authentication of users of computer systems on a remote server by keyboard handwriting]. *Prikladnaya informatika*. 2015;6(60):48–59. (In Russ.)

11. Averin A.I., Sidorov D.P. *Autentifikatsiya pol'zovateley po klaviaturnomu pocherku* [User authentication by keyboard handwriting]. Available at: http://journal.mrsu.ru/arts/autentifikaciya-polzovatelej-po-klaviaturnomu-pocherku (accessed 17.06.2022). (In Russ.)

12. Ayupova A.R., Yakupov A.R., Shabalkina A.A. Keyboard rhythm authentication: benefits and problems of use. *Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal*. 2017;12-5(66):55–58. DOI: 10.23670/IRJ.2017.66.123 (In Russ.)

13. Vasil′yev V.I., Kalyamov M.F., Kalyamova L.F. [Identification of users by keyboard handwriting using the algorithm for registering frequent bigrams]. *Modelirovaniye, optimizatsiya i informatsionnyye tekhnologii*. 2018;6(1):399–407. (In Russ.)

14. Dovgal' V.A. [Capturing keyboard handwriting parameters and its features]. In: *Informatsionnyye sistemy i tekhnologii v modelirovanii i upravlenii: materialy Vseros. nauch.-prakt. konf.*

[Information systems and technologies in modeling and management: materials of the All-Russian Scientific and Practical Conference]. Simferopol': Arial Publ.; 2017. P. 230–236. (In Russ.)

15. Robert Moskovitch, Clint Feher, Arik Messerman et al. Identity Theft, Computers and Behavioral Biometrics. Available at: https://www.ise.bgu.ac.il/faculty/liorr/idth.pdf (accessed 01.06.2022). (In Russ.)

16. Vasil`ev V.I., Sulavko A.E., Borisov R.V., Zhumazhanova S.S. [Recognition of psychophysiological states of users based on covert monitoring of actions in computer systems]. *Iskusstvennyy intellekt i prinyatiye resheniy*. 2017;(3):21–37. (In Russ.)

17. Sulavko A.E., Eremenko A.V. [A method for compressing eigenregions of image classes in the space of uninformative features]. *Iskusstvennyy intellekt i prinyatiye resheniy*. 2014;(2):102–109. (In Russ.)

18. Asyaev G.D., Ragozin A.N. [Determination of the minimum set of input data for correct authentication by keyboard handwriting using a neural network]. *Vestnik UrFO*. 2017;3(25):19–23. (In Russ.)

19. Sharipov R.R., Sitnikov A.N. [Problems in the development of systems for recognizing users by keyboard handwriting]. *Vestnik tekhnologicheskogo universiteta*. 2019;22(10):143–147. (In Russ.)

20. Bryukhomitskiy Yu.A., Kazarin M.N. [Testing biometric access control systems]. *Informatsionnoye protivodeystviye ugrozam terrorizma*. 2006;(8):168–180. (In Russ.)

21. Grigor`ev V.R. Nikitin A.P. [Using static methods for biometric user identification]. *RSUH / RGGU bulletin. Series: Records management and archive studies. Computer science. Data protection and information security*. 2012;14(94):135–143. (In Russ.)

22. Kostyuchenko E.Yu., Meshcheryakov R.V. [User recognition by keyboard handwriting on a fixed passphrase in computer systems]. *Proceedings of the Taganrog State Radio Engineering University*. 2003;4(33):177–178. (In Russ.)

23. Anastasiya Sivova, Alexey Vulfin, Konstantin Mironov, Anastasiya Kirillova. *Hidden Authentication of the User Based on Neural Network Analysis of the Dynamic Profile*. Available at: http://dx.doi.org/10.25673/32764 (accessed 01.04.2022).

24. Iskandarova Z.A. [Methods for improving the reliability of user identification of computer systems by writing passwords]. *Enigma*. 2020;27-3:162–172. (In Russ.)

25. Sulavko A.E., Fedotov A.A. Eremenko A.V. [Recognition of users of computer systems by keyboard handwriting, taking into account the parameters of vibration and pressure on the keys]. *Dinamika sistem, mekhanizmov i mashin*. 2017;5(4):95–105. DOI: 10.25206/2310-9793-2017-5-4-95-105. (In Russ.)

Информация об авторах

Артюшина Лариса Андреевна, канд. пед. наук, магистр направления «Информационные системы и технологии», доц. кафедры информатики и защиты информации, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; larisa-artusina@yandex.ru.

Троицкая Елена Анатольевна, канд. пед. наук, доц. кафедры информатики и защиты информации, Владимирский государственный университет имени Александра Григорьевича и Николая Григорьевича Столетовых, Владимир, Россия; troickiyv@mail.ru.

Information about the authors

Larisa A. Artyushina, Cand. Sci. (Education), Master's degree in Information Systems and Technologies, Ass. Prof. of the Department of Informatics and Information Protection, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; larisa-artusina@yandex.ru.

Elena A. Troitskaya, Cand. Sci. (Education), Ass. Prof. of the Department of Informatics and Information Protection, Vladimir State University named after Alexander and Nicolay Stoletovs, Vladimir, Russia; troickiyv@mail.ru.

Статья поступила в редакцию 21.06.2022
The article was submitted 21.06.2022