

Научная статья

УДК 004.056.53

<https://doi.org/10.31854/1813-324X-2024-10-6-55-67>

Мягкая биометрия для аутентификации и определения рук на основе использования клавиатуры

Юсеф Мохаммед Абд Аллх Альютум ✉, yousefot49@gmail.com

Андрей Владимирович Красов, krasov.av@sut.ru

Санкт-Петербургский государственный университет телекоммуникаций им. проф. М.А. Бонч-Бруевича, Санкт-Петербург, 193232, Российская Федерация

Аннотация

Актуальность. В настоящее время технологические системы, искусственный интеллект, общедоступность Интернета и проникновение злоумышленников в системы банков, учреждений и социальных сетей стали изучаемой наукой и доступны для всех групп и возрастов. Одна из основных задач – обеспечение системы защиты конфиденциальной информации от хакеров, а также простого доступа к аутентификации и идентификации пользователей. На первый план вышли биометрические системы, в том числе динамика движения мыши и динамика нажатия клавиш, которые выявляют стиль набора и движения мыши у каждого человека. Мягкая биометрия – интересный и недорогой биометрический метод, не требующий дополнительного оборудования. Система идентифицирует человека на основе ввода им информации в специальной графе. Динамика идентификации руки попадает в категорию поведенческой мягкой биометрии, то есть паттерны пользователя отражают индивидуальную программу действий, которой он следует при использовании сайта.

Цель настоящей работы – разработка системы усиленной аутентификации.

Методы исследования. При выполнении работы использовались методы анализа и синтеза, теории алгоритмов, законы кинематики, нейронные сети, динамика нажатия клавиш и мягкая биометрия.

Результаты. Описан метод извлечения динамических характеристик нажатия клавиш. Создана нейронная сеть и определено пороговое значение для выявления типа печатающей руки.

Научная новизна. В отличие от известных способов аутентификации, предлагаемый метод используется для определения печатающей руки на клавиатуре через нейронную сеть с помощью законов кинематики, мягкой биометрии и извлечения динамики нажатия клавиш с целью определения ценности и точности определения типа печатающей руки.

Значимость. Предложенное решение позволяет повысить безопасность аутентификации пользователей, увеличить скорость внедрения и снизить стоимость нового способа верификации. Результаты, полученные в работе, являются положительными и могут быть использованы в ближайшем будущем. В свою очередь, мягкие биометрические измерения зависят от поведенческих паттернов человека, что усложняет фальсификацию пользователя. Имитировать поведение при наборе текста сложно, поскольку оно является баллистическим (полуавтономным), что делает поведенческую информацию ценной, в качестве мягкого и чувствительного биометрического метода.

Ключевые слова: мягкая биометрия, идентификации руки, биометрическая аутентификация, закон растояния и скорости Ньютона


Ссылка для цитирования: Альютум Ю.М.А.А., Красов А.В. Мягкая биометрия для аутентификации и определения рук на основе использования клавиатуры // Труды учебных заведений связи. 2024. Т. 10. № 6. С. 55–67. DOI:10.31854/1813-324X-2024-10-6-55-67. EDN:BGOWBS

Original research

<https://doi.org/10.31854/1813-324X-2024-10-6-55-67>

Soft Biometrics for Authentication and Identification Hand Based on the Use of the Keyboard

 Yousef M.A.A. Alotoum , yousefot49@gmail.com

 Andrey V. Krasov, krasov.av@sut.ru

The Bonch-Bruевич Saint Petersburg State University of Telecommunications,
St. Petersburg, 193232, Russian Federation

Annotation

Relevance. Nowadays, technological systems, artificial intelligence, the general availability of the Internet and penetration into the systems of banks, institutions and social networks have become a studied science and are accessible to all groups and ages. One of the main tasks was to provide a system for protecting confidential information from hackers, as well as easy access to authentication and identification of users. Biometric systems came to the fore, including mouse movement dynamics and keystroke dynamics, which reveal the typing style and mouse movement of each person. Soft biometrics is an interesting and inexpensive biometric method that does not require additional equipment. The system identifies a person based on the input information they enter in a special column. Hand identification dynamics falls into the category of behavioral soft biometrics, that is, the user's patterns reflect the individual program of actions that he follows when using the site.

The goal of this article the purpose of this work is to improve the security level by creating a function that will strengthen the authentication system and improve the iron gate

Research Methods. In carrying out the work, methods of analysis and synthesis, theories of algorithms, laws of kinematics, neural networks, keystroke dynamics and soft biometrics were used.

Results. A method for extracting dynamic characteristics of keystrokes is described. A neural network is created and a threshold value is determined for identifying the type of typing hand.

Scientific novelty. Unlike known authentication methods, the proposed method is used to determine the typing hand on the keyboard through a neural network using the laws of kinematics, soft biometrics and extracting the dynamics of keystrokes in order to determine the value and accuracy of determining the type of typing hand.

Significance. The proposed solution allows to increase the security of user authentication, increase the speed of implementation and reduce the cost. The results obtained in the work are positive and can be used in the near future. In turn, soft biometric measurements depend on human behavioral patterns, which complicates user falsification. It is difficult to imitate typing behavior, since it is ballistic (semi-autonomous), which makes behavioral information valuable as a soft and sensitive biometric method.

Keywords: soft biometrics, hand identification, biometric authentication, Newton's law of distance and speed

For citation: Alotoum Y.M.A.A., Krasov A.V. Soft Biometrics for Authentication and Identification Hand Based on the Use of the Keyboard. *Proceedings of Telecommunication Universities*. 2024;10(6):55–67. (in Russ.) DOI:10.31854/1813-324X-2024-10-6-55-67.EDN:BGOWBS

Введение

В настоящее время технологические системы, искусственный интеллект, легкая доступность Интернета и проникновение злоумышленников в системы банков, учреждений и социальных сетей стали изучаемой наукой и доступны для всех групп и возрастов. Чтобы повысить безопасность персональных данных, исследователи включают метод, используемый для подтверждения личности чело-

века – физические или поведенческие характеристики последнего, именуемый биометрией, в свои системы безопасности [1–3]. Мягкая биометрия представляет собой некоторую информацию о человеке, которая постоянно дополняется и изменяется вместе с поведением человека, например, измерения возраста, роста, веса или биохимические особенности. Жесткая биометрия анализирует постоянные биометрические данные и идентифицирует пользователя по отпечаткам пальцев,

изображению лица и т. д. Жесткая биометрия влечет за собой дополнительные затраты на оборудование и, следовательно, снижает готовность пользователей применять соответствующий механизм проверки. Чтобы решить эту проблему, исследователи предложили использовать определение динамики нажатия клавиш – это поведенческая биометрическая модальность для защиты от несанкционированного доступа к учетной записи. Технология динамики нажатия клавиш применяется в целях аутентификации людей, подчеркивая, что каждый пользователь печатает на клавиатуре характерным образом [4, 5]. Аутентификация пользователей по клавиатурному почерку основывается на анализе особенностей набора текста каждого пользователя. Скорость набора, длительность удержания клавиш, интервалы между нажатиями и другие параметры могут быть частью этих функций. Собирая и анализируя данные, система создает для каждого пользователя индивидуальный «клавиатурный отпечаток», который можно использовать для аутентификации. Клавиатурный почерк трудно подделать, поскольку он зависит от физиологических и поведенческих характеристик пользователя [6]. Поскольку клавиатура является основным средством ввода информации в компьютер, аутентификация на основе динамики нажатия клавиш не требует дополнительных затрат на оборудование.

Необходимо было создать систему, способную самодополняться за счет изменения динамики нажатия клавиш биометрической клавиатуры для определения печатающей руки (одна рука или две), поскольку у каждого человека свой стиль работы на клавиатуре, отличающийся от стиля другого человека с точки зрения скорости, местоположения, движения и интересов человека внутри системы. Эта система позволит существенно сократить количество подобных кибератак [7, 8].

Биометрический метод

Биометрия, в отличие от других методов проверки, опирается на характеристики, присущие каждому человеку [6, 9, 10]. Существует две категории биометрии: физиологическая и поведенческая. В первом случае для подтверждения идентификации используются физические черты тела человека, такие как лицо, отпечатки пальцев, вены или радужная оболочка глаз. Мы рассматриваем приобретенное поведение в поведенческой биометрии. В этом случае мы проверяем человека, наблюдая, как он научился выполнять определенное действие уникальным, стандартизированным способом [11–14]. Современные исследователи, проанализировав данные Джейна Эт Ала (1998), сделали вывод, что биометрическая система должна соответствовать семи различным критериям: универсальность, уникаль-

ность, постоянство, собираемость, производительность, принятие и обход. Уникальность и постоянство – два элемента, которые имеют решающее значение для оценки эффективности. В то время как постоянство связано с необходимостью иметь возможность идентифицировать человека в течение более длительного периода времени, уникальность относится к необходимости различать двух разных людей [1, 15–17].

Основные преимущества биометрии: нет необходимости запоминать пароли или использовать другие элементы / токены, предоставляющие доступ к ресурсам; повышается безопасность; биометрические данные могут использоваться для защиты от некоторых мошеннических атак, например, фишинга [1, 2, 17]. Биометрическая система реализуется посредством аутентификации и идентификации.

Аутентификация – это процедура проверки подлинности пользователя; может быть статической (система проверяет пользователя только один раз в начале сеанса) и непрерывной или активной (система контролирует пользователя на протяжении всего сеанса, чтобы обнаружить любые изменения личности во время этого сеанса [2, 5, 17, 18]).

Идентификация – это процедура установления личности пользователя.

Мягкая биометрия

Биометрические характеристики, которых недостаточно для аутентификации пользователя, такие как рост, пол, кожа, глаза, цвет волос, и которые основаны на различиях черт людей (уникальное представление личности), и эти характеристики доступны всем [15, 19–21]. Мягкая биометрия позволяет уточнить поиск реального пользователя в базе данных, что приводит к сокращению вычислительного времени. Например, если результат «захвата» биометрических данных определяет, что посетитель сайта – мужчина, согласно единице мягкой биометрии, стандартная система биометрической аутентификации может ограничить поле поиска до пользователя-мужчины без учета женщин. Мягкая биометрия для аутентификации позволяет определять эмоциональное состояние (может быть обнаружено на 84 %), пол (на 90 %), одной или двумя руками набран текст на клавиатуре (на 80 %). Наиболее многообещающие результаты аутентификации по мягкой биометрии основаны на классификации уверенности, нерешительности, нервозности, расслабления, печали и усталости с точностью от 77 до 88 %, определении, левша или правша пользователь, и определении возрастной группы. Большинство методов аутентификации пользователя ориентированы на то, когда пользователь инициирует сеанс только во время входа в систему, но также важно его аутентифицировать во

время сеанса, поэтому появляется термин «непрерывная аутентификация» [20, 22–24].

Одна из задач данного исследования – извлечь как можно больше биометрических признаков. В целях повышения точности аутентификации необходимо создать алгоритм, основанный на определении руки, которой пользователь набирает текст на клавиатуре (правой, левой, обеими руками).

Клавиатура qwerty содержит 56 клавиш, которыми можно ввести пароль. В проекте клавиатура разделена на восемь частей, как показано на рисунке 1, и состоит из следующих букв, цифр и символов:

- 1) первая левая часть – **~**, **1**, **2**, **3**, **4**, **5**, а также другие символы при нажатии клавиши Shift (**~**, **!**, **@**, **\$**, **%**);
- 2) первая правая часть – **6**, **7**, **8**, **9**, **0**, **-**, **=**, а также другие символы при нажатии клавиши Shift (**^**, **&**, *****, **(**, **)**, **_**, **+**);
- 3) вторая левая часть – **Tab**, **q**, **w**, **e**, **r**, **t**;
- 4) вторая правая часть – **y**, **u**, **i**, **o**, **p**, **[**, **]**, ****, а также другие символы при нажатии клавиши Shift (**{**, **}**, **|**);
- 5) третья левая часть – **Capslock**, **a**, **s**, **d**, **f**, **g**;

6) третья правая часть – **h**, **j**, **k**, **l**, **;**, **'**, а также другие символы при нажатии клавиши Shift (**:**, **"**);

7) четвертая левая часть – **left_shift**, **z**, **x**, **c**, **v**;

8) четвертая правая часть – **b**, **n**, **m**, **,**, **.**, **/**, **right_shift**, а также другие символы при нажатии клавиши Shift (**<**, **>**, **?**).

Независимо от того, какая задействована рука (правая или левая), скорость набора одной рукой заметно ниже, чем при использовании обеих рук, так как в последнем случае расстояние, которое человек проходит при переключении с одной буквы на другую, короче, чем при наборе одной рукой. Исследователи А. Перейра, Д.Л. Ли, Х. Садишкumar, Ч. Ларош, Д. Оделл и Д. Ремпел опубликовали результаты исследования, проведенного с целью изучения влияния расстояния между клавишами на скорость набора текста, количество допускаемых ошибок, удобство использования, активность мышц предплечья и положение запястья. Исследование было сосредоточено на конструкции традиционной механической клавиатуры, а не на экранной, создаваемой программным обеспечением [16, 25, 26]).

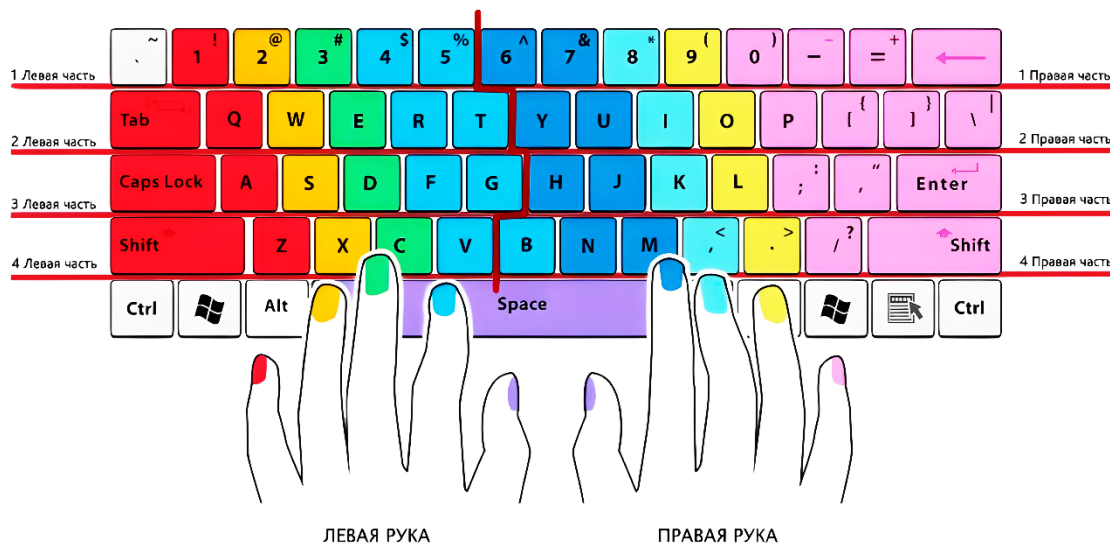


Рис. 1. Части клавиатуры

Fig. 1. Keyboard Parts

На основании исследований А. Перейра и других ученых в 1970-х гг. в работе [18] указано, что на обычное расстояние между клавишами на клавиатуре больше влияет отраслевая практика, чем вопросы эргономики (скорость набора текста, биомеханика, частота ошибок и удобство использования). Исследователи отмечают, что Международная организация по стандартизации (ISO), Американский национальный институт стандартов и Общество человеческого фактора и эргономики (ANSI/HFES) рекомендуют, чтобы горизонтальное и вертикальное межцентровые расстояния (при

взгляде на клавиатуру сверху) составляли 19 мм + / – 1 мм, хотя не все, но большинство конструкций клавиатуры соответствуют этим стандартам.

Взаимосвязь производительности и расстояния между клавишами была рассмотрена в исследованиях А. Перейра и др. исследователей. Так, в Японии исследователи пришли к выводу, что у людей с маленькими пальцами не наблюдается снижение производительности при различном расстоянии между клавишами (диапазон – от 15 до 19,7 мм); в то же время производительность действительно была снижена у людей с большими пальцами, если

расстояние между клавишами составило 16 мм или меньше (исследователи предостерегают от приложения выявленных результатов к населению США или других стран из-за различий в антропометрии рук) [18, 25]. В работе [27] показано, что увеличено время ввода и частота ошибок с использованием цифровых клавиатур при увеличении расстояния с 19 до 21 мм. Обзор литературы 1972 г., в котором рассматривались параметры конструкции клавиатуры того времени, дал основание полагать, что оптимальное расстояние между центрами клавиш составляет 18,1 мм [22]. В работах [28, 29] было выявлено, что при совместном рассмотрении скорости набора текста, частоты ошибок и предпочтений пользователя интервал в 19 мм был лучшим (по сравнению с другими: 14,3; 16,6; 21,4).

Ни в одном из вышеупомянутых исследований не рассматривалось *ключевое* влияние расстояния на биомеханические или физиологические показатели. Понимая, что люди с пальцами меньшей длины скорее всего лучше адаптируются к сокращению расстояния между клавишами, А. Перейра сосредоточил внимание на людях с более длинными пальцами, и в статье [19] автор в первую очередь исследует горизонтальное расстояние между клавишами.

Алгоритм идентификации руки

Каждой цифре, букве или символу на клавиатуре присвоено значение в шестнадцатеричной системе, и соответственно было создано 8 матриц на основе разделения клавиатуры на части (см. рисунок 1).

Американский стандартный код обмена информацией (ASCII, *аббр. от англ.* American Standard Code for Information Interchange) представляет собой стандарт кодирования символов для электронной связи. Коды ASCII представляют текст в компьютерах, телекоммуникационном оборудовании и других устройствах. В связи с техническими ограничениями компьютерных систем на момент его изобретения ASCII имеет всего 128 кодовых точек, из которых только 95 являются печатными символами, что серьезно ограничивает его возможности. Современные компьютерные системы используют Unicode, который имеет миллионы кодовых точек, но первые 128 из них совпадают с набором ASCII [2, 11, 26, 30].

ASCII частично был разработан на основе телеграфного кода. Его первое коммерческое использование было в Teletype Model 33 и Teletype Model 35 в качестве семибитного кода телетайпа, продвигаемого службами передачи данных Bell. Работа над стандартом ASCII началась в мае 1961 г. с первого заседания подкомитета X3.2 Американской ассоциации стандартов (ныне Американский национальный институт стандартов – *сокр.* ANSI). Первое издание стандарта было опубликовано в 1963 г.,

в 1967 г. – было серьезно переработано, последнее обновление произошло в 1986 г. По сравнению с более ранними телеграфными кодами, предлагаемые коды Bellu Piece и ASCII были упорядочены для более удобной сортировки (т. е. расстановки в алфавитном порядке) списков и дополнительных функций для устройств, отличных от телетайпов [22, 26–28].

Первоначально основанный на (современном) английском алфавите ASCII кодирует 128 указанных символов в семибитные целые числа, как показано на рисунке 2.

95 закодированных символов можно распечатать: к ним относятся цифры от 0 до 9, строчные буквы от a до z, прописные буквы от A до Z и символы пунктуации. Кроме того, исходная спецификация ASCII включала 33 непечатаемых управляющих кода, созданных в моделях телетайпов; большинство из них уже устарели, хотя некоторые из них все еще широко используются, например, возврат каретки, перевод строки и коды табуляции [8, 18].

Код ASCII используется для расчета значения характеристики динамики нажатия клавиш. Например, строчная буква e будет представлена в кодировке ASCII как двоичное число 1101001 = шестнадцатеричное 69 (e – девятая буква) = десятичное 105.

Значения символьного кода массива:

- первая левая часть (192, 49, 50, 51, 52, 53);
- первая правая часть (54, 55, 56, 57, 48, 189, 187);
- вторая левая часть (9, 81, 87, 69, 82, 84);
- вторая правая часть (89, 85, 73, 79, 80, 219, 221, 220);
- третья левая часть (20, 65, 83, 68, 70, 71);
- третья правая часть (72, 74, 75, 76, 186, 222);
- четвертая левая часть (16, 90, 88, 67, 86);
- четвертая правая часть (66, 78, 77, 188, 190, 191, 16).

Начальное значение создается для каждого положения кнопки на клавиатуре:

- первая левая часть (1, 2, 3, 4, 5, 6);
- первая правая часть (7, 8, 9, 10, 11, 12, 13);
- вторая левая часть (1, 2, 3, 4, 5, 6);
- вторая правая часть (7, 8, 9, 10, 11, 12, 13, 14);
- третья левая часть (1, 2, 3, 4, 5, 6);
- третья правая часть (7, 8, 9, 10, 11, 12);
- четвертая левая часть (1, 2, 3, 4, 5);
- четвертая правая часть (6, 7, 8, 9, 10, 11, 12).

Однако при случайном и беспорядочном нажатии кнопок клавиатуры (например, кликнуть клавишу «Q», затем – «K», а после – «Z») сложно найти общее расстояние между нажатыми пользователем клавишами. Основываясь на законах кинетической физики, расстояние определяется, как сумма полного движения тела, независимо от направления движения, совершаемого этим телом. Выходит, расстояние является стандартной величиной, а также его можно определить, как длину – путь между

начальной и конечной точками. Т. е. итоговое расстояние можно определить, измерив дистанцию, соединяющую каждую клавишу, использованную

при движении рук / руки от начальной к конечной точки.

Key	Code	Key	Code	Key	Code
backspace	8	e	69	numpad 8	104
tab	9	f	70	numpad 9	105
enter	13	g	71	multiply	106
shift	16	h	72	add	107
ctrl	17	i	73	subtract	109
alt	18	j	74	decimal point	110
pause/break	19	k	75	divide	111
caps lock	20	l	76	f1	112
escape	27	m	77	f2	113
page up	33	n	78	f3	114
page down	34	o	79	f4	115
end	35	p	80	f5	116
home	36	q	81	f6	117
left arrow	37	r	82	f7	118
up arrow	38	s	83	f8	119
right arrow	39	t	84	f9	120
down arrow	40	u	85	f10	121
insert	45	v	86	f11	122
delete	46	w	87	f12	123
0	48	x	88	num lock	144
1	49	y	89	scroll lock	145
2	50	z	90	semi-colon	186
3	51	left window key	91	equal sign	187
4	52	right window key	92	comma	188
5	53	select key	93	dash	189
6	54	numpad 0	96	period	190
7	55	numpad 1	97	forward slash	191
8	56	numpad 2	98	grave accent	192
9	57	numpad 3	99	open bracket	219
a	65	numpad 4	100	back slash	220
b	66	numpad 5	101	close braket	221
c	67	numpad 6	102	single quote	222
d	68	numpad 7	103		

Рис. 2. ASCII коды символов и клавиш

Fig. 2. ASCII Character Codes and Key Codes

Стандартное расстояние между каждой клавишами клавиатуры составляет 19 мм, в связи с чем расстояние, которое проходят руки при вводе пароля, должно рассчитываться от начала до конца слова. Чтобы изначально рассчитать общее пройденное расстояние, необходимо определить полную скорость кликов на клавиши, как показано на рисунке 3.

Скорость в физике делится на стандартную и векторную. *Стандартная* выражает время, необходимое объекту для прохождения определенного

расстояния без указания направления. Это стандартная физическая величина, которая выражается только в количестве. Она бывает двух типов: средняя и мгновенная стандартная скорость. Первая определяется путем деления расстояния на общее время. Вторая характеризует движение в определенный момент времени. *Векторная скорость* выражает скорость, необходимую объекту для перемещения на определенное расстояние и в определенном направлении.

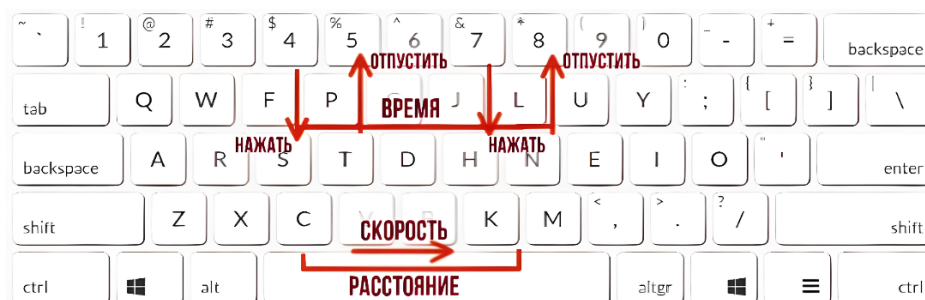


Рис. 3. Расстояние, скорость и время на клавиатуре

Fig. 3. Distance, Speed and Time on Keyboard

В этом исследовании учитывалась средняя стандартная скорость, поскольку объекты перемещаются для определения расстояния и времени без определения направления. Пользователь кладет руки на клавиатуру и начинает нажимать одну клавишу за другой (зависит от длины пароля). Направление нажатых пользователем клавиш не указывается, поскольку клавиатура разделена не на одну строку, а на несколько строк и столбцов, а также из-за средней стандартной скорости, рассчитываемой путем деления пройденного за путь расстояния на общее время, необходимое для прохождения этого пути, расстояние и время.

Стандартную скорость для обеих рук можно выявить, определив расстояние между кнопками при их нажатии и отпуске, чтобы расстояние при использовании обеих рук составляло примерно 19 мм, разделенных на временную метку (*от англ. TimeStamp* – числовое представление текущего времени; уникальный идентификатор, который отмечает точный момент, когда произошло событие или было выполнено определенное действие; рассчитывается с точностью до миллисекунд или быстрее, в зависимости от времени использования устройства, с помощью метода «Date.new» «getTime»). Временная метка используется в различных приложениях, таких как ведение журнала, отладка или измерение временных интервалов.

Получить временную метку можно методом Date().getTime(), который возвращает примитивное значение объекта Date, представляющее собой

количество миллисекунд, прошедших с 1 января 1970 г., 00:00:00 UTC.

Средняя стандартная скорость печати обеими руками определяется следующим образом:

$$a = \frac{19 \text{ mm}}{b}, \tag{1}$$

где a – средняя стандартная скорость для обеих рук; b – временная метка.

Местоположение каждого из нажатия клавиш на клавиатуре определяется путем деления клавиатуры на 8 частей, четыре строки и два столбца в виде матрицы:

$$rk = Key_{z,c}, \tag{2}$$

где rk – расположение клавиш; z – номер матрицы; c – расположение кнопки в матрице.

Высчитывается расположение всех букв, которые были введены в качестве пароля. Получается значение, равное абсолютной величине вычитания расстояния первой буквы от второй буквы подряд:

$$ark = |rk_{i,1} - rk_{i+1}|, \tag{3}$$

где ark – все расположение клавиш; i – расположение кнопки в матрице.

Пройденное обеими руками расстояние (рисунок 4), рассчитывается по формуле:

$$P_{\text{two hand}} = \sum rt * \sum b, \tag{4}$$

где rt – расположение кнопки в матрице.

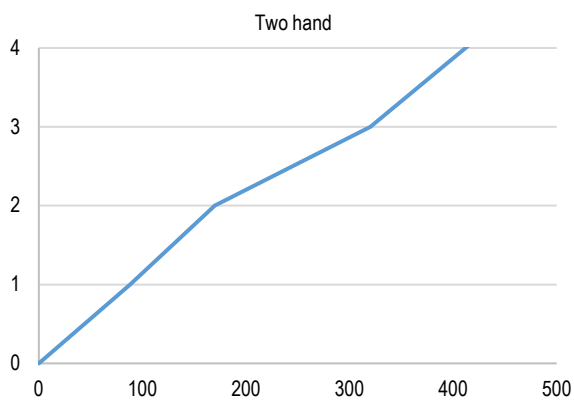


Рис. 4. Диаграмма расстояния, пройденного обеими руками

Fig. 4. Diagram of Distance Traveled by Both Hands

Средняя стандартная скорость печати одной рукой определяется следующим образом:

$$co = \frac{19 \text{ mm} * rk_{i,1}}{b} \quad (5)$$

Расположение клавиш (расстояния между буквами соответствует 19 мм), нажатых одной рукой, которые были введены в качестве пароля, рассчитывается следующим образом:

$$rk_{\text{one hand}} = 19 \text{ mm} * rk_i \quad (6)$$

Пройденное одной рукой расстояние (рисунок 5) определяется по выражению (7).

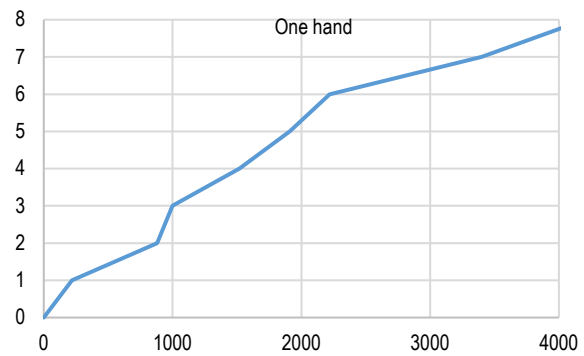


Рис. 5. Диаграмма расстояния, пройденного одной рукой

Fig. 5. Diagram of the Distance Traveled with one Hand

$$P_{\text{one hand}} = \sum co * \sum b \quad (7)$$

Во время введения пароля одной или двумя руками, образуется сложная сеть клавиш, включающая систему параметров: точки клика, скорость, расстояние и время (рисунок 6). Чтобы узнать, как пользователь вводит пароль (одной или двумя руками), вычисляется общая скорость и расстояние от начальной до конечной точки.

Вычислить расположения букв при наборе обеими руками можно следующим образом:

$$ras = \frac{\sum rth}{k} \quad (8)$$

где rth – расстояние, пройденное при наборе текста двумя руками; k – количество временных меток.

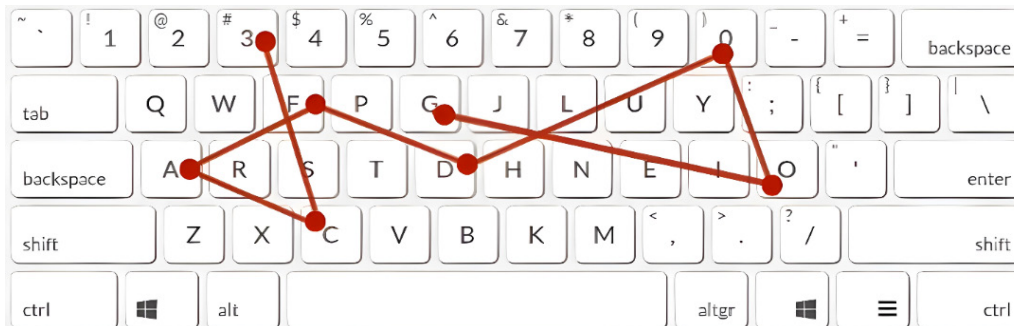


Рис. 6. Сеть клавиш клавиатуры

Fig. 6. Keyboard Button Grid

Общее расстояние, пройденное при наборе текста двумя руками (между буквами – также 19 мм), определяется как:

$$rth = \sum 19 \text{ mm} * k \quad (9)$$

Таким образом, скорость прохождения дистанции при наборе текста двумя руками можно представить в следующем виде:

$$ste = |rth - ras| \quad (10)$$

где ste – скорость печати двумя руками.

Расположения букв при наборе пароля одной рукой вычисляется по формуле:

$$lon = \frac{\sum ro}{k} \quad (11)$$

где lon – расположение одной руки; ro – расстояние, пройденное при наборе текста одной рукой.

Точное значение или фиксированное расстояние, пройденного одной рукой (ФКР), можно рассчитать по выражению:

$$\text{ФКР} = k * 10 \quad (12)$$

Скорость прохождения расстояния при вводе пароля одной рукой определяется как:

$$cpdo = \left| \frac{roh_{i,1}}{\sqrt{\sum b} - \Phi КР} \right|, \quad (13)$$

где *roh* – расстояние, пройденное одной рукой.

Скорость преодоления расстояния от одной клавиши до другой двумя руками выше, чем скорость преодоления этого же расстояния одной рукой.

Соответственно, ориентируясь на затраченное время, можно определить одну или две руки человек использует.

Рабочая среда

Жизненный цикл системы идентификации руки при наборе текста на клавиатуре делится на два этапа: *обучение* (рисунок 7а) и *тестирование* (рисунок 7б).

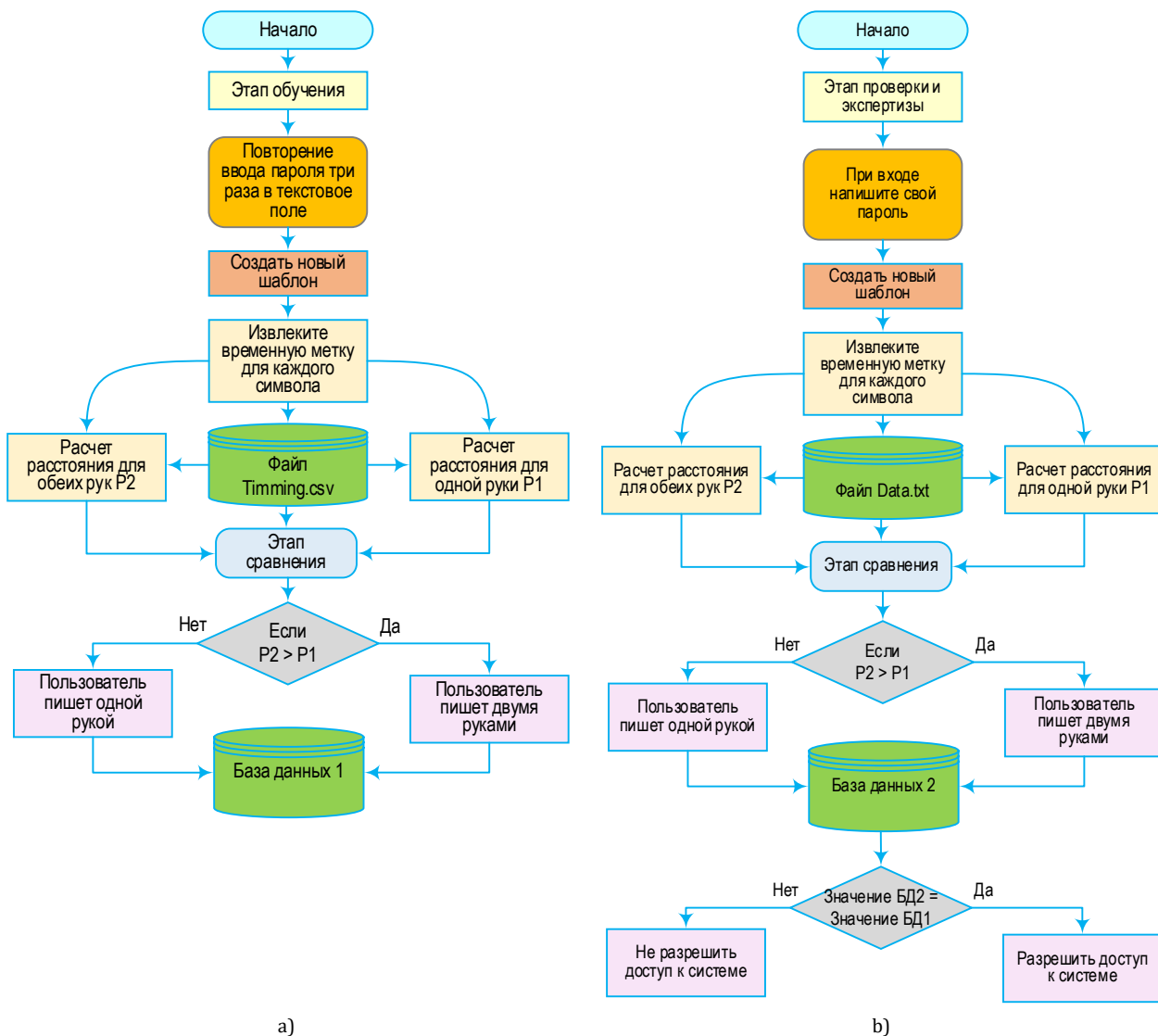


Рис. 7. Тренировка по определению почерка на этапе обучения (а) и тестирования (б)

Fig. 7. Handwriting Recognition Training at the Training Stage (a) and Testing Stage (b)

На этапе обучения пользователь трижды вводит пароль в текстовое поле и использует один и тот же метод написания одной или двумя руками во всех полях. После этого для пользователя создается специальная форма для извлечения функции нажатия клавиши и временная метка нажатия и отпускания клавиш. Функции нажатия клавиш и временная метка сохраняются в файле под названием Timing,

после чего эти функции извлекаются из файла. Затем рассчитывается расстояние, пройденное одной и двумя руками, представленное сетью кнопок клавиатуры, которые были нажаты для ввода пароля в трех полях. После этого происходит этап сравнения. Если скорость прохождения дистанции двумя руками больше скорости провозждения дистанции

одной рукой, то человек печатает двумя руками, а если меньше, то – одной.

На этапе тестирования пользователь вводит пароль во время входа в систему, и использует один и тот же метод написания одной или двумя руками. После этого для пользователя создается специальная форма для извлечения функции нажатия клавиш и временная метка нажатия и отпускания клавиш. Функции нажатия клавиш и временная метка сохраняются в файле под названием «Data», после чего эти функции извлекаются и рассчитывается расстояние, пройденное одной и двумя руками в сети клавиш клавиатуры, представленной кнопками, которые были нажаты для ввода пароля. В базе данных сохраняется информация о том, что расстояние, пройденное в системе клавиш двумя руками, больше, чем пройденное одной рукой. После этого происходит этап сравнения и констатация факта набора текста двумя руками или одной рукой. Далее наступает финальный этап сравнения, где, если значение, хранящееся в базе данных на этапе обучения, равно такому же значению, хранящемуся в базе данных на этапе тестирования, пользователю разрешен вход в систему, в противном случае – нет.

Заключение

В настоящее время происходит революция развития в области искусственного интеллекта и робототехники, а благодаря доступности и простоте использования Интернета область хакерства также стала преподаваемой в университетах. Таким образом, увеличивается опасность стать жертвой взлома и кражи данных.

Текущие области аутентификации и безопасности более уязвимы для взлома из-за разнообразия методов. В такие системы входят: система распознавания лиц, система отпечатков пальцев и т. д., где хакер может создать бота или программу, которая способна клонировать лицо пользователя или отпечаток пальца. Чтобы противостоять различным методам сетевого вторжения, необходимо создать систему, способную самодополняться так, чтобы координаты рабочей среды становились переменными. Для этого в исследовании был предложен способ определения стиля пользования клавиатуры одного человека.

Динамическое определение рук в настоящее время является удобной системой благодаря таким качествам, как низкая стоимость внедрения, нена-

вязчивое и основано исключительно на информации о том, как человек использует клавиатуру в процессе набора текста. В статье была исследована динамика набора текста на клавиатуре для аутентификации и идентификации пользователя. Кроме того, была разработана новая модель адаптивной статистики, которая позволяет корректировать пороговое значение в ответ на различия в показателях ввода пользователем пароля. Сначала были извлечены динамические характеристики нажатия клавиш и временная метка каждого нажатия клавиши, после чего они были отредактированы. Этот процесс повторен три раза для обучения и извлечения соответствующего порогового значения. Помимо расчета частоты ложных отклонений и приемов, для определения общего сформированного расстояния использовались кинематические уравнения.

В исследовании приняли участие 50 человек разного возраста. Были сделаны выводы, что использование законов кинематики со стилем почерка является более точным и строгим, чем другие способы определения стиля набора текста на основе динамики нажатия клавиш, поскольку оно берет среднее значение всего набора данных (рабочая зона при использовании одной руки, умноженное максимум на 10 м/с и при использовании обеих рук), полученного в ходе обучения, и сравнивает их друг с другом, а также выдает небольшой процент ложных ошибок.

В ходе исследования было рассмотрено множество различных биометрических методов, которые хранили бы данные системы и пользователей. Вероятность несанкционированного входа в учетную запись пользователя составляет 25 %. Из приведенной статистики можно сделать вывод, что качество классических биометрических систем недостаточно надежно. Кроме того, используемые в настоящее время системы очень дороги и требуют дополнительных времени и усилий для внедрения дополнительного оснащения, например, сканеры отпечатков пальцев, глаз и лица. В пике применяемым процедурам аутентификации был разработан алгоритм, полагающийся только на клавиатуру устройства, а не на внешние системы. Разработанная система аутентификации обеспечивает повышение безопасности до 15 % за счет предотвращения несанкционированного доступа, не требует от пользователя выполнения других внешних процедур для завершения процесса входа в систему и не вызывает затруднений при использовании.

Список источников

1. Андрианов В.И., Красов А.В., Липатников В.А. Инновационное управление рисками информационной безопасности: учебное пособие. СПб.: СПбГУТ, 2012. 396 с. EDN:QSMDNH
2. Яковлев В.А., Скачкова В.В. Автоматизация выбора графического материала для систем аутентификации пользователей на основе графического пароля // Проблемы информационной безопасности. Компьютерные системы. 2015. № 1. С. 64–73. EDN:TWHDDF

3. Миняев А.А., Красов А.В., Сахаров Д.В. Метод оценки эффективности системы защиты информации территориально-распределенных информационных систем персональных данных // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2020. № 1. С. 29–33. DOI:10.46418/2079-8199_2020_1_5. EDN:ULHTJK
4. Бирих Э.В., Груздев А.С., Камалова А.О., Сахаров Д.В. Выбор инструментов динамического анализа безопасности web-приложений для задач цифровой экономики // Защита информации. Инсайд. 2024. № 1(115). С. 42–46. EDN:RLNHWK
5. Kaixin W., Hongri L., Bailing W., Shujie H., Jia S. User Authentication and Identification Model Based on Mouse Dynamics // Proceedings of the 6th International Conference on Information Engineering (ICIE '17, Dalian Liaoning, China, 17–18 August 2017). New York: Association for Computing Machinery, 2017. Article No. 18. DOI:10.1145/3078564.3078581
6. Blaganesh P., Soniya A. A Survey of Authentication Based on Mouse Behaviours // International Journal of Advanced Information Science and Technology. 2014. Vol 3. Iss. 2. PP. 42–45. DOI:10.15693/ijaist/2014.v3i2.42-45
7. Shen C., Cai Z., Guan X. Continuous Authentication for Mouse Dynamics: A Pattern-Growth Approach // Proceedings of the International Conference on Dependable Systems and Networks (DSN 2012, Boston, USA, 25–28 June 2012). IEEE, 2012. DOI:10.1109/DSN.2012.6263955
8. Mondal S., Bours P. Continuous authentication using mouse dynamics // Proceedings of the International Conference of the BIOSIG Special Interest Group (BIOSIG, Darmstadt, Germany, 05–06 September 2013). IEEE, 2013.
9. Hinbarji Z., Albatal R., Gurrin C. Dynamic User Authentication Based on Mouse Movements Curves // Proceedings of the International Conference on Multimedia Modeling (MMM 2015, Sydney, Australia, 5–7 January 2015). Lecture Notes in Computer Science. Vol. 8936. Cham: Springer, 2015. PP. 111–122. DOI:10.1007/978-3-319-14442-9_10
10. Kasprowski P., Borowska Z., Harezlak K. Biometric Identification Based on Keystroke Dynamics // Sensors. 2022. Vol. 22. Iss. 9. P. 3158. DOI:10.3390/s22093158
11. Janakiraman R., Sim T. Keystroke Dynamics in a General Setting // Proceedings of the International Conference on Biometrics (ICB 2007, Seoul, Republic of Korea, 27–29 August 2007). Lecture Notes in Computer Science. Vol. 4642. Berlin, Heidelberg: Springer, 2007. DOI:10.1007/978-3-540-74549-5_62
12. Tsimperidis I., Arampatzis A. The Keyboard Knows About You Revealing User Characteristics via Keystroke Dynamics // International Journal of Technoethics. 2020. Vol. 11. Iss. 2. DOI:10.4018/IJT.2020070103
13. Idrus S.Z.S., Cherrier E., Rosenberger C., Mondal S., Bours P. Keystroke dynamics performance enhancement with soft biometrics // Proceedings of the International Conference on Identity, Security and Behavior Analysis (ISBA 2015, Hong Kong, China, 23–25 March 2015). IEEE, 2015. DOI:10.1109/ISBA.2015.7126345
14. Gaikwad J., Kulkarni B., Phadol N., Sarukte S. User Authentication using Keystroke Dynamics // Global Research and Development Journal for Engineering. 2018. Vol. 3. Iss. 6. PP. 58–66.
15. Hassan S.I., Selim M.M., Zayed H.H. User Authentication with Adaptive Keystroke Dynamics // International Journal of Computer Science Issues. 2013. Vol. 10. Iss. 4. No 2. PP. 127–134.
16. Bours P. Continuous keystroke dynamics A different perspective towards biometric evaluation // Information Security Technical Report. 2012. Vol. 17. Iss. 1-2. PP. 36–43. DOI:10.1016/j.istr.2012.02.001
17. Mondal S., Bours P. Combining keystroke and mouse dynamics for continuous user authentication and identification // Proceedings of the International Conference on Identity, Security and Behavior Analysis (ISBA, Sendai, Japan, 29 February – 02 March 2016). IEEE, 2016. DOI:10.1109/ISBA.2016.7477228
18. Idrus S.Z.S., Cherrier E., Rosenberger C., Bours P. Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords // Computers & Security. 2014. Vol. 45. PP. 147–155. DOI:10.1016/j.cose.2014.05.008
19. Голованов А.Л. Разработка системы аутентификации по клавиатурному почерку на основе свободных текстов // В книге: Математическое и компьютерное моделирование. сборник материалов XI Международной научной конференции, посвященной памяти В.А. Романькова (Омск, Российская Федерация, 15 марта 2024). Омск: Омский государственный университет им. Ф.М. Достоевского, 2024. С. 236–237. EDN:AAOOFW
20. Сатыбалдиева М.М. Исследование систем для идентификации пользователя на основе анализа клавиатурного почерка // Научный аспект. 2024. Т. 14. № 5. С. 1897–1903. EDN:DENDWJ
21. Ямали Д.Д. Революция в аутентификации через клавиатурный почерк // Научно-исследовательский центр "Technical Innovations". 2024. № 23. С. 114–119. EDN:NLCXWH
22. Polous K.I. Comparative analysis of biometric authentication methods Общество // Молодежь. Общество. Современная наука, техника и инновации. 2021. № 20. С. 61–63. EDN:MRRBLY
23. Семенова О.С., Фадеева К.Н. Биометрическая аутентификация и её типы // III Всероссийская научно-практическая конференция с международным участием «Цифровые технологии и инновации в развитии науки и образования» (Чебоксары, Российская Федерация, 07 апреля 2023). Чебоксары: Чувашский государственный педагогический университет им. И.Я. Яковлева, 2023. С. 186–190. EDN:ILSOXW
24. Ларионов М.Ю. Перспективы развития биометрической идентификации и аутентификации личности // Инновации. Наука. Образование. 2021. № 42. С. 897–902. EDN:QEIXUB
25. Красов А.В., Альотум Ю., Ушаков И.А., Максимов В.В., Архипов А.В. Аутентификация и идентификация пользователя с использованием биометрической динамики нажатия клавиш на основе «манхэттенского и евклидовского расстояния» // Вестник Санкт-Петербургского государственного университета технологии и дизайна. Серия 1: Естественные и технические науки. 2023. № 4. С. 49–56. DOI:10.46418/2079-8199_2023_4_10. EDN:ZBXUBO
26. Yousef M.A.A.A. Biometric and behavioral authentication and soft biometrics using keystroke and mouse dynamics // XII Международная научно-техническая и научно-методическая конференция «Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО 2023, Санкт-Петербург, Российская Федерация, 28 февраля – 01 марта 2023). В 4 т. СПб.: СПбГУТ, 2023. С. 70–75. EDN:QTKUGV

27. Шахин Г. Биометрия во встраиваемых системах // E-Scio. 2020. № 6(45). С. 314–320. EDN:ZYRDPR
28. Ермишева Ю.Д., Омелченко Т.А. Отдельные результаты применения программного средства аутентификации по клавиатурному почерку // НБИ технологии. 2023. Т. 17. № 1. С. 11–16. DOI:10.15688/NBIT.jvolsu.2023.1.2. EDN:EXXQQO
29. Бацких А.В., Дровникова И.Г., Рогозин Е.А. К вопросу использования новой информационной технологии, связанной с дополнительной аутентификацией субъектов доступа по клавиатурному почерку, в системах защиты информации от несанкционированного доступа на объектах информатизации органов внутренних дел // Вестник Воронежского института МВД России. 2020. № 2. С. 21–33. EDN:DDVYPU
30. Пашенко Д.В., Бальзанникова Е.А. Непрерывная идентификация пользователя по клавиатурному почерку с использованием представления на основе контекста состояний // XXI век: итоги прошлого и проблемы настоящего плюс. 2020. Т. 9. № 3(51). С. 74–79. DOI:10.46548/21vek-2020-0952-0012. EDN:MAJRDT

References

1. Andrianov V.I., Krasov A.V., Lipatnikov V.A. *Innovative Information Security Risk Management*. St. Petersburg: SPbSUT Publ.; 2012. 396 p. (in Russ.) EDN:Q5MDNH
2. Yakovlev V.A., Skachkova V.V. Automatic Selection of Graphical Materials for Authentication System Based on a Graphical Password. *Information Security Problems. Computer Systems*. 2015;1:64–73. (in Russ.) EDN:TWHDDF
3. Minyaev A.A., Krasov A.V., Sakharov D.V. The Efficiency Evaluation Method of Distributed ISPD Protection System. *Vestnik of St. Petersburg State University of Technology and Design*. 2020;1:29–33. (in Russ.) DOI:10.46418/2079-8199_2020_1_5. EDN:ULHTJK
4. Birikh E.V., Gruzdev A.S., Kamalova A.O., Sakharov D.V. Selection of tools for dynamic analysis of web application security for digital economy tasks. *Zashita informacii. Inside*. 2024;1(115):42–46. (in Russ.) EDN:RLNHWK
5. Kaixin W., Hongri L., Bailing W., Shujie H., Jia S. User Authentication and Identification Model Based on Mouse Dynamics. *Proceedings of the 6th International Conference on Information Engineering, ICIE '17, 17–18 August 2017, Dalian Liaoning, China*. New York: Association for Computing Machinery; 2017. Article No. 18. DOI:10.1145/3078564.3078581
6. Blaganesh P., Soniya A. A Survey of Authentication Based on Mouse Behaviours. *International Journal of Advanced Information Science and Technology*. 2014;3(2):42–45. DOI:10.15693/ijaist/2014.v3i2.42-45
7. Shen C., Cai Z., Guan X. Continuous Authentication for Mouse Dynamics: A Pattern-Growth Approach. *Proceedings of the International Conference on Dependable Systems and Networks, DSN 2012, 25–28 June 2012, Boston, USA*. IEEE; 2012. DOI:10.1109/DSN.2012.6263955
8. Mondal S., Bours P. Continuous authentication using mouse dynamics. *Proceedings of the International Conference of the BIOSIG Special Interest Group, BIOSIG, 05–06 September 2013, Darmstadt, Germany*. IEEE; 2013.
9. Hinbarji Z., Albatat R., Gurrin C. Dynamic User Authentication Based on Mouse Movements Curves. *Proceedings of the International Conference on Multimedia Modeling, MMM 2015, 5–7 January 2015, Sydney, Australia. Lecture Notes in Computer Science, vol.8936*. Cham: Springer; 2015. p.111–122. DOI:10.1007/978-3-319-14442-9_10
10. Kasprowski P., Borowska Z., Harezlak K. Biometric Identification Based on Keystroke Dynamics. *Sensors*. 2022;22(9): 3158. DOI:10.3390/s22093158
11. Janakiraman R., Sim T. Keystroke Dynamics in a General Setting. *Proceedings of the International Conference on Biometrics, ICB 2007, 27–29 August 2007, Seoul, Republic of Korea. Lecture Notes in Computer Science, vol. 4642*. Berlin, Heidelberg: Springer; 2007. DOI:10.1007/978-3-540-74549-5_62
12. Tsimperidis I., Arampatzis A. The Keyboard Knows About You Revealing User Characteristics via Keystroke Dynamics. *International Journal of Technoethics*. 2020;11(2). DOI:10.4018/IJT.2020070103
13. Idrus S.Z.S., Cherrier E., Rosenberger C., Mondal S., Bours P. Keystroke dynamics performance enhancement with soft biometrics. *Proceedings of the International Conference on Identity, Security and Behavior Analysis, ISBA 2015, 23–25 March 2015, Hong Kong, China*. IEEE; 2015. DOI:10.1109/ISBA.2015.7126345
14. Gaikwad J., Kulkarni B., Phadol N., Sarukte S. User Authentication using Keystroke Dynamics. *Global Research and Development Journal for Engineering*. 2018;3(6):58–66.
15. Hassan S.I., Selim M.M., Zayed H.H. User Authentication with Adaptive Keystroke Dynamics. *International Journal of Computer Science Issues*. 2013;10(4):127–134.
16. Bours P. Continuous keystroke dynamics A different perspective towards biometric evaluation. *Information Security Technical Report*. 2012;17(1-2):36–43. DOI:10.1016/j.istr.2012.02.001
17. Mondal S., Bours P. Combining keystroke and mouse dynamics for continuous user authentication and identification. *Proceedings of the International Conference on Identity, Security and Behavior Analysis, ISBA, 29 February – 02 March 2016, Sendai, Japan*. IEEE; 2016. DOI:10.1109/ISBA.2016.7477228
18. Idrus S.Z.S., Cherrier E., Rosenberger C., Bours P. Soft biometrics for keystroke dynamics: Profiling individuals while typing passwords. *Computers & Security*. 2014;45:147–155. DOI:10.1016/j.cose.2014.05.008
19. Golovanov A.L. Development of an authentication system based on keyboard handwriting based on free texts. In: *Mathematical and Computer Modeling. Collection of Materials of the XI International Scientific Conference Dedicated to the Memory of V.A. Romankov, 15 March 2024, Omsk, Russian Federation*. Omsk: Dostoevsky Omsk State University Publ.; 2024. p.236–237. (in Russ.) EDN:AAOOFW
20. Satybaldieva M.M. Research of systems for user identification based on the analysis of keyboard handwriting. *Scientific Aspect*. 2024;14(5):1897–1903. (in Russ.) EDN:DENDWJ
21. Yamali D.D. Revolution in authentication through keyboard handwriting. *Research Center "Technical Innovations"*. 2024;23:114–119. (in Russ.) EDN:NLCXWH


22. Polous K.I. Comparative analysis of biometric authentication methods Society. *Youth. Society. Modern Science, Technology and Innovation*. 2021;20:61–63. EDN:MRRBLY
23. Semenova O.S., Fadeeva K.N. Biometric authentication and its types. *Proceedings of the IIIrd All-Russian Scientific and Practical Conference with International Participation on Digital Technologies and Innovations in the Development of Science and Education, 07 April 2023, Cheboksary, Russian Federation*. Cheboksary: I. Yakovlev Chuvash State Pedagogical University Publ.; 2023. p.186–190. (in Russ.) EDN:ILSOXW
24. Larionov M.Yu. Prospects for the development of biometric identification and authentication of personality. *Innovations. Science. Education*. 2021;42:897–902. (in Russ.) EDN:QEIXXB
25. Krasov A.V., Alyotum Yu., Ushakov I.A., Maksimov V.V., Arkhipov A.V. User authentication and identification using biometric keystroke dynamics based on the “Manhattan and Euclidean distance”. *Vestnik of St. Petersburg State University of Technology and Design. Series 1: Natural and Technical Sciences*. 2023;4:49–56. (in Russ.) DOI:10.46418/2079-8199_2023_4_10. EDN:ZBXUBO
26. Yousef M.A.A.A. Biometric and behavioral authentication and soft biometrics using keystroke and mouse dynamics // Proceedings of the XIIth International Conference on Infotelecommunications in Science and Education, 28 February – 01 March 2022, St. Petersburg, Russian Federation. St. Petersburg: The Bonch-Bruevich Saint-Petersburg State University of Telecommunications Publ.; 2023. p. 70–75. (in Russ.) EDN:QTKUGV
27. Shahin G. Biometrics in embedded systems. *E-Scio*. 2020;6(45):314–320. (in Russ.) EDN:ZYRDPR
28. Ermisheva Yu.D., Omelchenko T.A. Separate results of the application of the software authentication tool by keystroke dynamics. *NBI Technologies*. 2023;17(1):11–16. (in Russ.) DOI:10.15688/NBIT.jvolsu.2023.1.2. EDN:EXXQQO
29. Batskikh A.V., Drovnikova I.G., Rogozin E.A. On the issue of using a new information technology related to additional authentication of access subjects using keyboard handwriting in information protection systems against unauthorized access at information objects of internal affairs bodies. *The Bulletin of Voronezh Institute of the Ministry of Internal Affairs of Russia*. 2020;2:21–33. (in Russ.) EDN:DDVYPU
30. Pashchenko D.V., Balzannikova E.A. Continuous keystroke dynamics user identification using state context representation. *XXI Century: Resumes of the Past and Challenges of the Present plus*. 2020;9(3(51)):74–79. (in Russ.) DOI:10.46548/21vek-2020-0952-0012. EDN:MAJRDT

Статья поступила в редакцию 04.06.2024; одобрена после рецензирования 23.09.2024; принята к публикации 07.10.2024.


The article was submitted 04.06.2024; approved after reviewing 23.09.2024; accepted for publication 07.10.2024.

Информация об авторах:

АЛЬОТУМ
Юсеф Мохаммед Абд Алх

аспирант кафедры защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций
им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0009-0000-8684-7664>

КРАСОВ
Андрей Владимирович

кандидат технических наук, доцент, заведующий кафедрой защищенных систем связи Санкт-Петербургского государственного университета телекоммуникаций им. проф. М.А. Бонч-Бруевича
 <https://orcid.org/0000-0002-9076-6055>

Авторы сообщают об отсутствии конфликтов интересов.

The authors declare no conflicts of interests.