ТЕХНИЧЕСКИЕ НАУКИ

TECHNICAL SCIENCES

УДК 004.056.5:004.421
ББК 32.973.26-018.2
Д 58

Довгаль В.А.
Кандидат технических наук, доцент кафедры автоматизированных систем обработки информации и управления инженерно-физического факультета Адыгейского государственного университета, Майкоп, тел. (8772) 593911, e-mail: urmia@mail.ru

Особенности захвата параметров клавиатурного почерка

(Рецензирована)

Аннотация. *Рассматриваются основные аппаратные средства, используемые в процессе захвата параметров клавиатурного почерка, и их особенности, а также основные функции, которые могут быть извлечены в процессе захвата клавиатурного почерка.*

Ключевые слова: *клавиатурный почерк, аппаратное обеспечение для сбора биометрических данных, датчики клавиатурного почерка, биометрическая информация клавиатурного почерка.*

Dovgal V.A.
Candidate of Technical Sciences, Associate Professor of the Department of Automated Systems of Processing Information and Control of Engineering-Physics Faculty, Adyghe State University, Maikop, ph. (8772) 593911, e-mail: urmua@mail.ru

Features of obtaining information on parameters of keystroke dynamics

Abstract. *The paper describes the main hardware which is used in the course of obtaining information on parameters of keystroke dynamics, their features, and basic functions which can be derived in the course of obtaining information on keystroke dynamics.*

Keywords: *keystroke dynamics, the hardware for collection of biometric data, sensors of keystroke dynamics, biometric information of keystroke dynamics.*

Клавиатурный почерк, как новое биометрическое средство проверки подлинности людей с использованием сравнения характеристик ввода ими пароля или свободного текста на клавиатуре, представляет собой алгоритм идентификации состояния мастерства набора с использованием нескольких наборов данных в режиме off-line. Первой фазой обеспечения процесса аутентификации указанным способом набора учетных данных пользователем является фаза захвата сравниваемых характеристик. В зарубежной литературе эта фаза рассматривается как важный элемент процесса биометрической аутентификации.

Фаза захвата имеет место в двух различных важных случаях:

1) регистрация, при которой необходимо собрать несколько образцов пользователя для построения его модели. Процедура регистрации определяется типом системы клавиатурного почерка (набор одной и той же фиксированной строки несколько раз, мониторинг использования компьютерной техники и т.д.), а также количеством требуемых данных;

2) верификация, при которой захватывается единственный образец, из которого извлекаются различные характеристики. Затем они сравниваются с биометрической моделью претендента.

В этой статье будут рассмотрены аппаратные средства, которые могут быть использованы для захвата биометрических данных, а также связанные с этим различные особенности, проявляющиеся в процессе сбора этих данных.

Обязательное аппаратное обеспечение и возможность изменений

Каждая биометрическая методика нуждается в особенном аппаратном обеспечении для сбора биометрических данных. При покупке этого устройства цена, а также количество датчиков могут быть определяющими факторами при выборе биометрической системы, которая

предполагается для использования в инфраструктуре с большим числом пользователей (например, необходимость покупки датчика отпечатков пальцев для каждого компьютера, если предполагается логический контроль доступа для каждой машины). Клавиатурный почерк, вероятно, является биометрической методикой с самым дешевым биометрическим сенсором: используется только простая компьютерная клавиатура, имеющаяся у всех персональных компьютеров и ноутбуков. Стоимость замены клавиатуры в случае ее поломки или необходимости замены достаточно низка.

Для облегчения сравнения биометрических систем можно использовать таблицу 1, в которой представлены основные характеристики для некоторых методик.

Таблица 1

Сравнение цены аппаратного обеспечения различных биометрических методик

Биометрическая методика	нажатие клавиши	отпечаток пальца	лицо	радужная оболочка глаза	вены руки
Сенсор	клавиатура	датчик отпечатков пальцев	камера	инфракрасная камера	камера ближнего инфракрасного диапазона
Цена	очень дешево	нормально	нормально	очень дорого	дорого

Заметим, что клавиатуры различаются между собой по следующим показателям:

- форма (прямая клавиатура, эргономичная клавиатура и т.д.);
- давление (трудность нажатия клавиши);
- расположение клавиш (QWERTY, AZERTY и т.д.).

В некоторых исследованиях используется только цифровая клавиатура компьютера [1, 2]. Следовательно, смена клавиатуры может повлиять на производительность распознавания нажатий клавиш. Эта проблема хорошо известна в биометрическом сообществе и связана с соответствующими согласующими устройствами [3]. Она недостаточно исследована в литературе по клавиатурному почерку.

Наличие только этого датчика (клавиатуры) недостаточно, потому что (когда он классический) единственная информация, которой он обеспечивает – это код нажатой или отпущенной клавиши. Указанные параметры не являются биометрической информацией, они позволяют определить лишь правильность пароля. В то время как цель клавиатурного почерка состоит в установлении личности, которая печатает его.

Для расчета биометрических параметров необходим точный таймер, захватывающий с достаточной точностью время, в течение которого событие произошло на клавиатуре. Этот таймер уже предустановлен в каждом компьютере и каждая операционная система способна использовать его. Следовательно, нет необходимости покупать его. Но у этого таймера есть недостаток – его разрешение может быть различным в зависимости от выбранного языка программирования или операционной системы. Установлено, что более высокая производительность получается с более высокой точностью таймера [4]. Некоторые исследователи также изучили эффект от использования внешних часов вместо установленных внутри компьютера. Например, выявлено, что учет этого таймера важен особенно при сравнении алгоритмов, поскольку он оказывает влияние на производительность [5]. Те же авторы также объясняют, как конфигурировать операционную систему, чтобы получить лучшую производительность. Даже на одном и том же компьютере точность таймера может различаться между разными используемыми языками программирования (кстати, следует помнить, что реализация веб-ориентированного клавиатурного почерка использует интерпретируемые языки программирования – Java или JavaScript, которые, как известно, не имеют точного таймера во всех архитектурах).

Исторически сложилось так, что клавиатурный почерк работает с классической клавиатурой на компьютере, а также избавляет от необходимости покупать специфический датчик. Тем не менее, некоторые исследования были проведены с использованием других видов датчиков, захватывающих дополнительную информацию и улучшающих распознавание. Например, проверена возможность использования датчика давления внутри каждой клавиши клавиа-

туры [6, 7]. В этом случае возможно использование дополнительной информации (силы давления, прилагаемой к клавише), позволяющей более легко различать пользователей. Кроме того, можно использовать клавиатуру, включающую в себя Sudden Motion Sensor (SMS) [8]. Такой датчик (или подобный ему) присутствует в ноутбуках MacBook и используется для обнаружения внезапного движения компьютера для того, чтобы переместить записывающие головки жесткого диска, когда обнаружен риск повреждения привода. Авторы исследования используют движение по оси z, как биометрическую информацию. Эти предварительные исследования показывают, что такая информация является достаточно эффективной.

Еще одним параметром, который может быть проанализирован, являются звуковые сигналы, воспроизводимые с помощью клавиатуры при наборе текста. Некоторые исследователи использовали только звуковые сигналы при вводе пароля и получали косвенным путем время нажатия клавиши, время освобождения клавиши и силу нажатия клавиши только на основании анализа этого сигнала. Установлено, что производительность аналогична классическим системам клавиатурного почерка. Звуковую информацию можно использовать и в дополнение к значениям синхронизации (то есть она является особенностью слияния), которая имеет более высокую производительность, чем только звук, или только как информацию о синхронизации [9].

Поскольку клавиатурный почерк может работать с любой клавиатурой, он также может работать и с любым устройством, обеспечивающим функции клавиатуры или чем-то похожим на клавиатуру. Одно общее устройство, имеющее клавиатуру, которым владеют многие люди – это мобильный телефон, в котором мы также можем использовать клавиатурный почерк. Имеются три вида мобильных телефонов:

1) мобильный телефон с цифровой клавиатурой. В этом случае необходимо нажимать несколько раз на одну и ту же кнопку, чтобы получить алфавитный символ. Имеются исследования, утверждающие, что такой механизм аутентификации на таком мобильном телефоне должен использоваться в паре с другим [10];

2) мобильный телефон со всеми клавишами (буквы и цифры), доступными пальцам. Этот вид клавиатур очень похож на клавиатуру компьютера, следовательно, рассматриваемый механизм аутентификации может быть использован и обычными пользователями таких мобильных телефонов [11];

3) мобильный телефон без клавиатуры, но с сенсорным экраном, наиболее используемый в настоящее время [12]. В таком мобильном телефоне возможен захват информации о различном давлении и положении пальца на клавиатуре.

На рисунке 1 представлена топология различных датчиков клавиатурного почерка, в то время как на рисунке 2 представлены возможности изменений по таймеру.

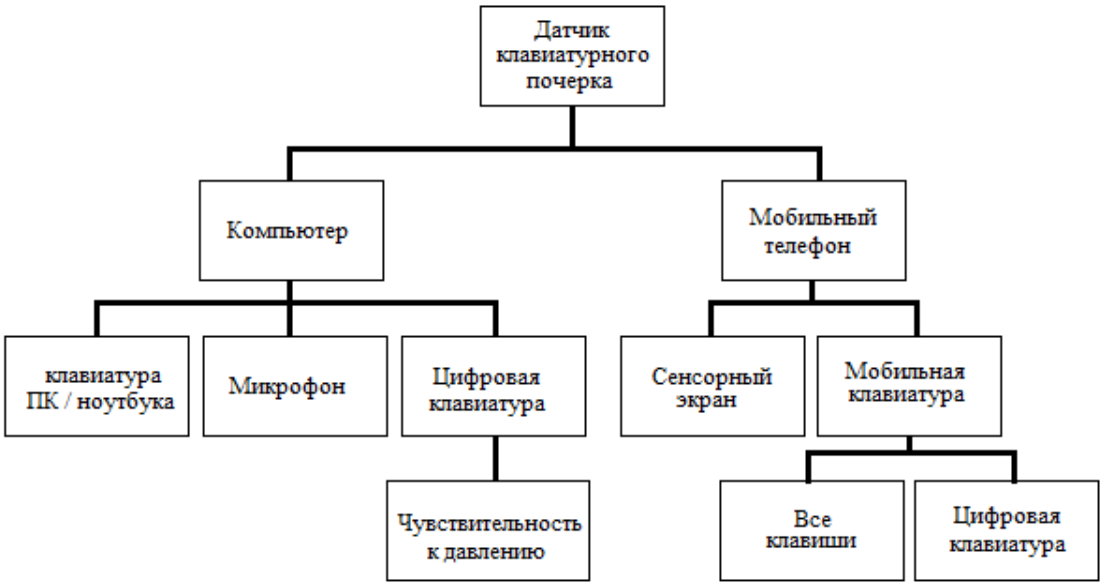

Рис. 1. Топология датчиков клавиатурного почерка

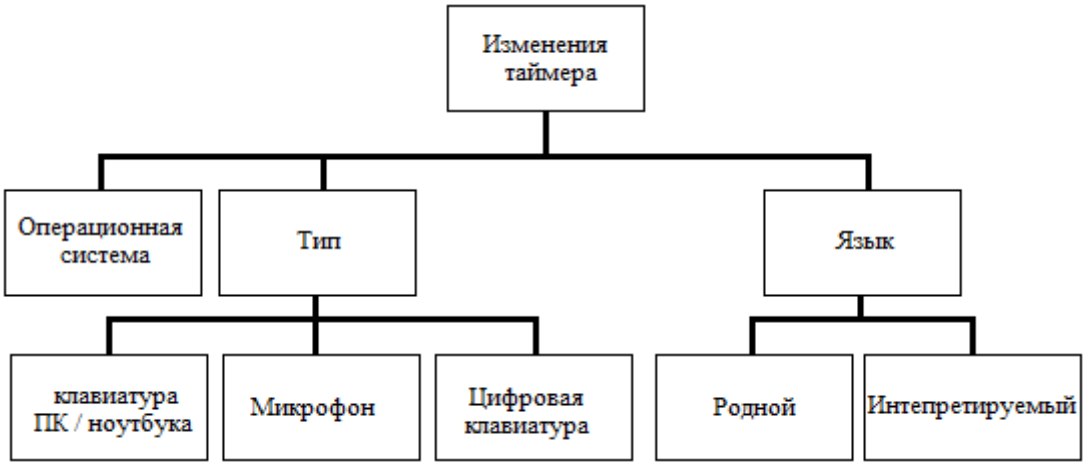

Рис. 2. Топология факторов, которые могут повлиять на точность таймера

Особенности захваченной информации

Как было отмечено выше, процедура клавиатурного почерка в зависимости от типа используемых датчиков захватывает различные виды информации. Несмотря на это, все разнообразие более или менее продвинутых датчиков позволяет определить параметры, которые имеют определенные особенности.

1. Сырые данные – захватываемые во всех исследованиях необработанные данные, представляющие собой события, инициируемые пользователем компьютера и выполняемые им с помощью клавиатуры. Необработанные биометрические данные для клавиатурного почерка – это хронологически упорядоченный список событий: вначале список пуст, но при наступлении события оно добавляется в хвост списка, сопровождаясь следующей информацией:

а) событие, порождаемое действием на клавише [13]. Имеются два разных события:

– нажатие, происходящее при нажатии клавиши;

– отпускание, происходящее при отпускании клавиши.

б) код клавиши, от нажатия которой происходит событие. Мы можем получить символ из этого кода (для того, чтобы проверить, соответствует ли список символов паролю, например). Код клавиши более интересен, чем символ, так как он дает некоторую информацию о месте расположения клавиши на клавиатуре (которая может быть использована некоторыми клавиатурными методами распознавания почерка) и позволяет дифференцировать различные клавиши, дающие тот же символ (который является информацией для критерия распознавания [14]). Этот код клавиши может зависеть от платформы и используемого языка.

в) временная метка, которая кодирует время наступления события. Ее точность оказывает значительное влияние на производительность распознавания. Обычно для Windows предлагается использовать функцию QueryPerormanceCounter с наивысшим приоритетом, имеющуюся в компьютерах с поддержкой Windows, и изменения политики планировщика в FIFO для машин Linux [5]. Метка обычно выражена в миллисекундах, хотя это не является обязательным.

Исходные данные могут быть представлены как (где n – число событий вида $n=2*s$, а s – количество нажатых клавиш, необходимых для печатания текста):

$$\begin{cases} (keycode_i, event_i, time_i), \ \forall i, \ 0 \le i < n, \\ keycode_i \in Z, \\ event_i \in \{PRESS, RELEASE\}, \\ time_i \in N. \end{cases} \quad (1)$$

Некоторые исследователи используют только шесть первых значений времени каждого слова (то есть $s \le 6$) [15]. В зависимости от вида приложения клавиатурного почерка необработанные данные фиксируются в различного рода сценариях: в форме аутентификации

введения логина и пароля, в форме с просьбой ввести заранее определенный или случайный текст, отличный от логина и пароля, или в непрерывном захвате во время использования компьютера.

2. Особенности извлечения. Из этих необработанных данных могут быть извлечены различные функции, но мы приведем лишь чаще всего используемые в литературе.

Наиболее часто извлекаемые характеристики – ***первого порядка*** – локальные, вычисленные путем вычитания значений синхронизации:

а) длительность (*duration*) – промежуток времени, в течение которого клавиша нажата. Для некоторой клавиши i (символ i для удобочитаемости опущен) она вычисляется следующим образом:

$$duration=time\{event=RELEASE\}-time\{event=PRESS\}, \quad (2)$$

где $event$ – событие; $RELEASE$ – освобождение клавиши; $PRESS$ – нажатие.

Тогда мы получим временной вектор (размера набранного текста), также называемый в литературе PR, содержащий длительность каждого нажатия клавиши (в порядке нажатий):

$$\forall i,\ 1\le i\le n,\ \ PR_i=duration_i. \quad (3)$$

б) задержки, которые могут быть различных видов. Задержки вычисляются путем получения разности времени между двумя событиями клавиш. Например, может быть вычислена задержка PP, которая является разностью времени между нажатием каждой клавиши:

$$\forall i,\ 1\le i\le n,\ \ PP_i=time_{i+1}\{event_{i+1}=PRESS\}-time_i\{event_i=PRESS\}. \quad (4)$$

Кроме того, можно получить задержку RR, которая является разностью времени между отпусканием каждой клавиши:

$$\forall i,\ 1\le i\le n,\ \ RR_i=time_{i+1}\{event_{i+1}=RELEASE\}-time_i\{event_i=RELEASE\}. \quad (5)$$

Еще одним видом задержки является RP, которая является разностью времени между отпусканием одной клавиши и нажатием следующей:

$$\forall i,\ 1\le i\le n,\ \ RP_i=time_{i+1}\{event_{i+1}=PRESS\}-time_i\{event_i=RELEASE\}. \quad (6)$$

В большинстве случаев функция слияния работает путем конкатенации вектора длительности с, по крайней мере, одним из векторов задержек (кажется, что в большинстве случаев выбранный вектор задержки PP один, но это не всегда указывается в документах). Возможно использование этих извлеченных признаков с целью повышения скорости распознавания систем клавиатурного почерка [16]. В других работах можно встретить иные виды данных – например, [17]. Главным образом они являются глобальными типами информации:

а) суммарное время набора – время, необходимое для печатания текста на клавиатуре. Указанный параметр может быть использован в качестве дополнительной функции для добавления к векторам признаков или в качестве коэффициента нормализации;

б) среднее время – разница во времени между моментом, когда пользователь вводит символ в середине пароля, и временем начала ввода;

в) коэффициент ошибок, подсчитываемый по количеству нажатий пользователем клавиши *BackSpace*. Клавиша используется пользователем в ходе авторизации при совершении опечатки (это всегда имеет место в непрерывной аутентификации, но почти никогда не бывает в статической аутентификации). Коэффициент дает интересные особенности.

Другая концепция, часто встречающаяся в литературе, – понятие орграфа. Орграф представляет время, необходимое для удара двух клавиш. Функция орграфа D из пароля вычисляется следующим образом:

$$\forall i,\ 1\le i\le n,\ \ D_i=time_{i+1}\{event_{i+1}=RELEASE\}-time_i\{event_i=PRESS\}. \quad (7)$$

Это понятие было распространено на n-графы, где n принимает различные значения. В качестве примера можно назвать триграф [18] или концепцию трудности печатания, основанную на том, что некоторые комбинации клавиш труднее нажать, чем другие [19]. Трудность печатания основывается на расстоянии (на клавиатуре) между двумя последовательными символами (печатания), если несколько клавиш необходимы для создания символа (то есть, использование клавиши Shift).

Некоторые функции – ***второго порядка*** – не извлекаются из необработанных биометрических данных, но извлекаются из функций первого порядка:

- мин/макс. – состоит в получении минимального и максимального значения каждого типа данных (задержка и длительность);
- средн/станд. – состоит в получении среднего значения и его стандартного отклонения каждого типа данных (задержка и длительность);
- наклон – используя наклон биометрического образца, мы заинтересованы в глобальной форме набора текста. Мы ожидаем, что потребители печатают одинаковым способом, даже если скорость может отличаться [20]. Новые функции (*result* – результат) вычисляются следующим образом (*source* – источник):

$$\forall i,\ 1 \le i \le n,\quad result_i = source_{i+1} - source_i; \tag{8}$$

- энтропия – пока изучена только внутри образца [21];
- спектральная информация – к оригинальным извлекаемым признакам применяется дискретное импульсное преобразование [22]. Все операции выполняются с вейвлетными трансформированными данными.

Мы можем представить себе более сложные функции, но окончательные биометрические данные всегда являются одним вектором, состоящим из различных функций. При расчете модели с несколькими образцами механизм выбора функций позволяет удалить не являющиеся информативными признаки.

Таким образом, основной используемой биометрической информацией в клавиатурном почерке являются временные значения (сила давления, движения и т.д.). В настоящей статье показаны основные функции, которые могут быть извлечены в процессе захвата клавиатурного почерка. Производительность процедур проверки значительно зависит от выбранных функций, но чаще всего используется только время задержки и продолжительность.

Примечания:

1. Killourhy K., Maxion R. Keystroke biometrics with number-pad input / IEEE/IFIP International Conference on Dependable Systems & Networks, 2010. DSN'10. P. 201–210.
2. Biometric access control through numerical keyboards based on keystroke dynamics / R.N. Rodrigues, G.F.G. Yared, C.R. Costa, J.B.T. Yabu-Uti, F. Violaro, L.L. Ling // Proceedings of the 2006 International conference on advances in biometrics (ICB'06). Hong Kong, 2006. Vol. 3832. P. 640–646.
3. Ross A., Jain A. Biometric sensor interoperability: A case study in fingerprints / Proc. of International ECCV Workshop on Biometric Authentication (BioAW). Springer, 2004. P. 134–145.
4. Killourhy K., Maxion R. The effect of clock resolution on keystroke dynamics // Proceedings of the 11th International symposium on Recent Advances in Intrusion Detection. Springer, 2008. P. 331–350.
5. Pavaday N., Nugessur S. Investigating & improving the reliability and repeatability of keystroke dynamics timers // International Journal of Network Security & Its Applications (IJNSA), 2010. No. 2 (3). P. 70–85.
6. Design and Evaluation of a Pressure-Based Typing Biometric Authentication System / W. Eltahir, M. Salami, A. Ismail, W. Lai // EURASIP Journal on Information Security. 2008. No 14. Article ID 345047.
7. Grabham N., White N. Use of a novel keypad biometric for enhanced user identity verification / Instrumentation and Measurement Technology Conference Proceedings. 2008. IMTC 2008. IEEE. P. 12–16.
8. Lopatka M., Peetz M. Vibration sensitive keystroke analysis / Proceedings of the 18th Annual Belgian-

References:

1. Killourhy K., Maxion R. Keystroke biometrics with number-pad input / IEEE/IFIP International Conference on Dependable Systems & Networks, 2010. DSN'10. P. 201–210.
2. Biometric access control through numerical keyboards based on keystroke dynamics / R.N. Rodrigues, G.F.G. Yared, C.R. Costa, J.B.T. Yabu-Uti, F. Violaro, L.L. Ling // Proceedings of the 2006 International conference on advances in biometrics (ICB'06). Hong Kong, 2006. Vol. 3832. P. 640–646.
3. Ross A., Jain A. Biometric sensor interoperability: A case study in fingerprints / Proc. of International ECCV Workshop on Biometric Authentication (BioAW). Springer, 2004. P. 134–145.
4. Killourhy K., Maxion R. The effect of clock resolution on keystroke dynamics // Proceedings of the 11th International symposium on Recent Advances in Intrusion Detection. Springer, 2008. P. 331–350.
5. Pavaday N., Nugessur S. Investigating & improving the reliability and repeatability of keystroke dynamics timers // International Journal of Network Security & Its Applications (IJNSA), 2010. No. 2 (3). P. 70–85.
6. Design and Evaluation of a Pressure-Based Typing Biometric Authentication System / W. Eltahir, M. Salami, A. Ismail, W. Lai // EURASIP Journal on Information Security. 2008. No 14. Article ID 345047.
7. Grabham N., White N. Use of a novel keypad biometric for enhanced user identity verification / Instrumentation and Measurement Technology Conference Proceedings. 2008. IMTC 2008. IEEE. P. 12–16.
8. Lopatka M., Peetz M. Vibration sensitive keystroke analysis / Proceedings of the 18th Annual Belgian-

Dutch Conference on Machine Learning. 2009. P. 75–80.

9. Dozono H., Itou S., Nakakuni M. Comparison of the adaptive authentication systems for behavior biometrics using the variations of self organizing maps // International Journal of Computers and Communications. 2007. No. 1 (4). P. 108–116.
10. User authentication using keystroke dynamics for cellular phones / P. Campisi, E. Maiorana, M. Lo Bosco, A. Neri // IET Signal Processing. 2009. No. 3 (4). P. 333–341.
11. Clarke N.L., Furnell S.M. Authenticating mobile phone users using keystroke analysis // International Journal of Information Security. 2007. No. 6. P. 1–14.
12. Паскова А.А., Бутко Р.П. Мобильная работа с корпоративными данными // Символ науки: междунар. науч. журнал. 2016. № 10-2/2016. С. 75–77.
13. Сапиев А.З. О методах аутентификации пользователей на основе анализа компьютерного почерка // Информатика: проблемы, методология, технологии: материалы XVI Междунар. науч.-метод. конф. / под ред. Н.А. Тюкачева. 2016. С. 251–256.
14. User authentication through typing biometrics features / L. Araujo, L.H.R. Sucupira, M. Lizarraga, L. Ling, J. Yabu-Uti // IEEE Transactions on Signal Processing. 2005. No. 53 (2 Pt. 2). P. 851–855.
15. Umphress D., Williams G. Identity verification through keyboard characteristics // Internat. J. Man-Machine Studies.1985. No. 23. P. 263–273.
16. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication / K.S. Balagani, V.V. Phoha, A. Ray, S. Phoha // Pattern Recognition Letters. 2011. No. 32 (7). P. 1070–1080.
17. Ilonen J. Keystroke dynamics, Advanced Topics in Information Processing – Lecture, 2003.
18. Bergadano F., Gunetti D., Picardi C. User authentication through keystroke dynamics, ACM Transactions on Information and System Security (TISSEC). 2002. No. 5 (4). P. 367–397.
19. de Ru W.G., Eloff J.H.P. Enhanced password authentication through fuzzy logic, IEEE Expert: Intelligent Systems and Their Applications. 1997. No. 12. P. 38–45.
20. Modi S.K., Elliott S.J. Kesytroke dynamics verification using spontaneously generated password, IEEE International Carnahan Conferences Security Technology. 2006. P. 116–121.
21. Monrose F., Reiter M., Wetzel S. Password hardening based on keystroke dynamics // International Journal of Information Security. 2002. No. 1 (2). P. 69–83.
22. Chang W. Keystroke biometric system using wavelets // ICB. Springer, 2006. P. 647–653.

Dutch Conference on Machine Learning. 2009. P. 75–80.

9. Dozono H., Itou S., Nakakuni M. Comparison of the adaptive authentication systems for behavior biometrics using the variations of self organizing maps // International Journal of Computers and Communications. 2007. No. 1 (4). P. 108–116.
10. User authentication using keystroke dynamics for cellular phones / P. Campisi, E. Maiorana, M. Lo Bosco, A. Neri // IET Signal Processing. 2009. No. 3 (4). P. 333–341.
11. Clarke N.L., Furnell S.M. Authenticating mobile phone users using keystroke analysis // International Journal of Information Security. 2007. No. 6. P. 1–14.
12. Paskova A.A., Butko R.P. Mobile work with corporate data // The symbol of science: international scientific journal. 2016. No. 10-2/2016. P. 75–77.
13. Sapiev A.Z. On users' authentication methods on the basis of analysis of computer typing // Computer science: problems, methodology, technologies: proceedings of the XVI International scient. and method. conference / ed. by N.A. Tyukachev. 2016. P. 251–256.
14. User authentication through typing biometrics features / L. Araujo, L.H.R. Sucupira, M. Lizarraga, L. Ling, J. Yabu-Uti // IEEE Transactions on Signal Processing. 2005. No. 53 (2 Pt. 2). P. 851–855.
15. Umphress D., Williams G. Identity verification through keyboard characteristics // Internat. J. Man-Machine Studies. 1985. No. 23. P. 263–273.
16. On the discriminability of keystroke feature vectors used in fixed text keystroke authentication / K.S. Balagani, V.V. Phoha, A. Ray, S. Phoha // Pattern Recognition Letters. 2011. No. 32 (7). P. 1070–1080.
17. Ilonen J. Keystroke dynamics, Advanced Topics in Information Processing – Lecture, 2003.
18. Bergadano F., Gunetti D., Picardi C. User authentication through keystroke dynamics, ACM Transactions on Information and System Security (TISSEC). 2002. No. 5 (4). P. 367–397.
19. de Ru W.G., Eloff J.H.P. Enhanced password authentication through fuzzy logic, IEEE Expert: Intelligent Systems and Their Applications. 1997. No. 12. P. 38–45.
20. Modi S.K., Elliott S.J. Kesytroke dynamics verification using spontaneously generated password, IEEE International Carnahan Conferences Security Technology. 2006. P. 116–121.
21. Monrose F., Reiter M., Wetzel S. Password hardening based on keystroke dynamics // International Journal of Information Security. 2002. No. 1 (2). P. 69–83.
22. Chang W. Keystroke biometric system using wavelets // ICB. Springer, 2006. P. 647–653.