Юрий Е. Козлов, Владимир Л. Евсеев
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: kozlovye@yandex.ru, ORCID 0000-0002-4448-0232
e-mail: VLevseev@fa.ru, ORCID 0000-0003-3283-3106

МУЛЬТИМОДАЛЬНАЯ ТРЕХМЕРНАЯ ДИНАМИЧЕСКАЯ ПОДПИСЬ*

DOI: http://dx.doi.org/10.26583/bit.2017.4.05

Аннотация. Надежная аутентификация в мобильных приложениях является актуальнейшей задачей информационной безопасности современного общества. В настоящее время человека сложно представить без мобильного устройства, подключенного к сети internet. Кроме того, мобильное устройство может хранить большой объем конфиденциальной информации, начиная от личных фотографий, заканчивая инструментами для банковских операций. Использование жеста в воздухе в качестве методики аутентификации впервые было предложено сотрудниками Университета Райса (США) совместно с компанией Моторола в 2009 году. Эта и остальные работы по созданию и усовершенствованию данной методики указаны во введении к статье. К моменту написания статьи, программа, реализующая один из вариантов методики аутентификации при помощи жеста мобильным устройством, доступна к установке для ОС Android. Однако данная программа не получила большого распространения. Возможно, одна из причин этого - недостаточная надежность методики, которая предполагает, как и ее предыдущие аналоги, использование только одного устройства. В данной статье рассмотрена аутентификация с использованием мультимодальной трехмерной динамической подписи (МТДП), выполняемой двумя независимыми мобильными устройствами. Методика аутентификации с помощью МТДП является улучшенным вариантом аутентификации при помощи жеста в воздухе. В основной части статьи рассмотрена работа прототипа системы аутентификации на основе МТДП. Описаны основные алгоритмы, реализованные в прототипе, а так же предварительные результаты, полученные при его использовании. Авторы предполагают использование данной методики в любых мобильных приложениях после введения ряда дополнительных усовершенствований, о которых рассказано в заключении.

Ключевые слова: аутентификация, мобильное устройство, акселерометр, персонализированный жест, подпись

Для цитирования. **КОЗЛОВ, Юрий Е.; ЕВСЕЕВ, Владимир Л.** МУЛЬТИМОДАЛЬНАЯ ТРЕХМЕРНАЯ ДИНАМИЧЕСКАЯ ПОДПИСЬ. Безопасность информационных технологий, [S.l.], v. 24, n. 4, p. 44-51, nov. 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/276>. Дата доступа: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.05.

***Благодарности:** Статья подготовлена по результатам исследований, выполненных за счет бюджетных средств по государственному заданию Финансового университета при Правительстве Российской Федерации 2017 года

Yury E. Kozlov, Vladimir L. Evseev
Financial University under the Government of the Russian Federation (Financial University),
LeningradskyProspekt, 49, Moscow, 125993, Russia
e-mail: kozlovye@yandex.ru, ORCID 0000-0002-4448-0232
e-mail: VLevseev@fa.ru, ORCID 0000-0003-3283-3106

Multimodal three-dimensional dynamic signature

DOI: http://dx.doi.org/10.26583/bit.2017.4.05

Abstract. Reliable authentication in mobile applications is among the most important information security challenges. Today, we can hardly imagine a person who would not own a mobile device

that connects to the Internet. Mobile devices are being used to store largeamounts of confidential information, ranging from personal photos to electronic banking tools. In 2009,colleagues from Rice University together with their collaborators from Motorola, proposed an authentication through in-air gestures. This and subsequent workcontributing tothe development of the method are reviewed in our introduction. At the moment, there exists a version of the gesture-based authentication software available for Android mobile devices. This software has not become widespread yet. One of likely reasons for that is the insufficient reliability of the method, which involvessimilar to its earlier analogsthe use of only one device. Here we discuss the authentication based on the multimodal three-dimensional dynamic signature (MTDS) performed by two independent mobile devices. The MTDS-based authentication technique is an advanced version of in-air gesture authentication. We describe the operation of a prototype of MTDS-based authentication, includingthe main implemented algorithms, as well as some preliminary results oftesting the software. We expect that our method can be used in any mobile application, provided a number of additional improvementsdiscussed in the conclusionare made.

Keywords: authentication, mobile device, accelerometer, personalized gestured, signature

For citation. **KOZLOV, Yury E.; EVSEEV, Vladimir L**. Multimodal three-dimensional dynamic signature. IT Security, [S.l.], v. 24, n. 4, p. 44-51, nov. 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/276>. Date accessed: 29 nov. 2017. doi:http://dx.doi.org/10.26583/bit.2017.4.05.

* ***Acknowledgements:*** The article is based on the results of research carried out at the expense of budget funds of the state task of the Financial University under the Government of the Russian Federation in 2017.

Введение

Аутентификация с использованием биометрических признаков способна обеспечить надежное и естественное решение задачи распознавания личности, при этом все большее исследований посвящены разработкам биометрических систем, основанных наповеденческой (динамической) характеристикечеловекаиучитывающиеособенности, характерныедляподсознательныхдвиженийчеловекавпроцессевоспроизведениякакого-либодействия. Это связано с тем, что неизменяемость и открытость биометрических характеристик, используемых в статических методах, в отличие от динамических, допускают подделку биометрического ключа [1].

Биометрические идентификаторы практически неотторжимы от субъекта и присущи только ему и никому другому, поэтому ими почти невозможно манипулировать. Принципиально важным преимуществом динамических биометрических систем контроля доступа является возможность для личности сохранять в тайне свой биометрический образ, что повышает степень защиты относительно статических биометрических систем контроля доступа [2].

Одной из причин сдерживающих внедрение биометрической аутентификации на практике, является требование соблюдения строгих правил при защите персональных данных, закрепленного в законодательных актах различных стран. Одним из примеров является принятый в 2016 году новый регулирующий акт GlobalDataProtectionRegulation (GDPR), регулирующий защиту персональных данных граждан стран-членов Европейского Союз, в котором биометрические идентификаторы признаны персональными данными, и правила их обработки строго регламентируются[3].

Использование МТДП для аутентификации в мобильных приложениях

Мультимодальная трехмерная динамическая подпись основана на использовании специального жеста для аутентификации. Работы по созданию методик аутентификации при помощи жеста проводились Университетом Райса (США) совместно с компанией Моторола [4,5], а так же Политехническим университетом Мадрида (CeDInt-UPM) (Испания) [6].Кроме того, приложение «InAirSignature», реализующее разблокировку телефона при помощи жеста, доступно для бесплатной установки в операционной системы (ОС) Android.

Появление умных часов и фитнес браслетов позволили значительно повысить надежность методик аутентификации за счет одновременного использования двух независимых устройств одновременно [7]. Поскольку такая аутентификация будет иметь схожесть с рукописной подписью по своим динамическим свойствам (биометрические особенности воспроизведения по скорости и амплитуде), а так же будет содержать два источника данных (мобильное и запястное устройство), можно назвать такой способ - мультимодальная трехмерная динамическая подпись (далееМТДП).

Такая подпись, как и в случае рукописной подписи, потребует выработки специфического функционально-динамического комплекса навыков(ФДК), представляющего собой явление психофизиологической природы, сущность которого составляет система навыков, предназначенных для целевой реализации определенных действий.

МТДП с целью повышения надежности аутентификации предполагает при воспроизведении жеста, регистрацию его двумя устройствами одновременно – мобильным и запястным.

На рисунке 1 представлен пример МТДП, точкой обозначено начало траектории, а стрелкой указывается ее направление.

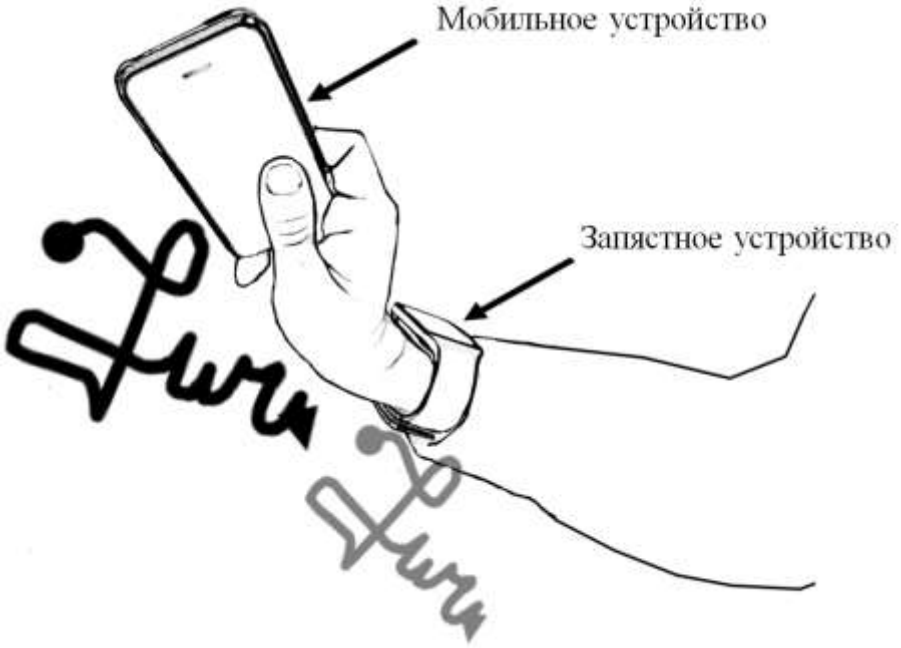

Рисунок 1 -Пример реализации мультимодальной трехмерной динамической подписи с использованием двух устройств
(Fig. 1-Example implementation of multimodal three-dimensional dynamic signature using two devicesЪ

Для «парольного» жеста подойдет любой жест, который человек сможет запомнить и впоследствии воспроизводить.

Процедура выработки эталона для МТДП схожа с процедурой подпись на бумажных документах. Пользователь сам определяет понравившийся ему вариант. И для закрепления навыков и выработки порога срабатывания повторяет его несколько раз (в разработанной реализации используется три попытки). При этом система определят разброс в воспроизведении МТДП и устанавливает порог срабатывания.

Неоспоримым преимуществом МТДП, как системы использующей динамические биометрические признаки, является легкая система смены признака и уточнение его порогов. Кроме того процесс аутентификации легко скрыть, даже используя его в людных местах. Для этого необходимо выбрать в качестве жеста, любой неприметный жест, который не вызовет подозрений. Проведенные предварительные исследования, а так же

исследования, представленные для аналога, показывают, что даже снятый на видео жест тяжел для точного воспроизведения другим человеком [5].

В таблице 1 представлено влияние внешних факторов на МТДП и распространенные системы биометрической аутентификации.

Таблица 1

Методика	**Влияниевнешнихфакторов**			
	Плохаяосвещенность	Шумноеместо	Низкаятемпература	Высокаятемпература
Отпечатокпальца	нет	нет	среднее	среднее
Распознаваниелица	**высокое**	нет	низкое	низкое
Речеваяаутентификация	нет	**высокое**	нет	нет
Радужнаяоболочкаглаза	**высокое**	нет	нет	нет
МТДП	нет	нет	нет	нет

Из таблицы видно, что МТДП имеет лучшую применяемость в шумном месте с плохой освещенностью. Стоит отметить, что в условиях городских улиц это очень частая ситуация.

Работа системы аутентификации на базе МТДП предполагает этап формирования подписи МТДП. На рисунке 2 представлен укрупненный алгоритм работы прототипа системы формирования МТДП, реализованный на базе ОСАндройд.

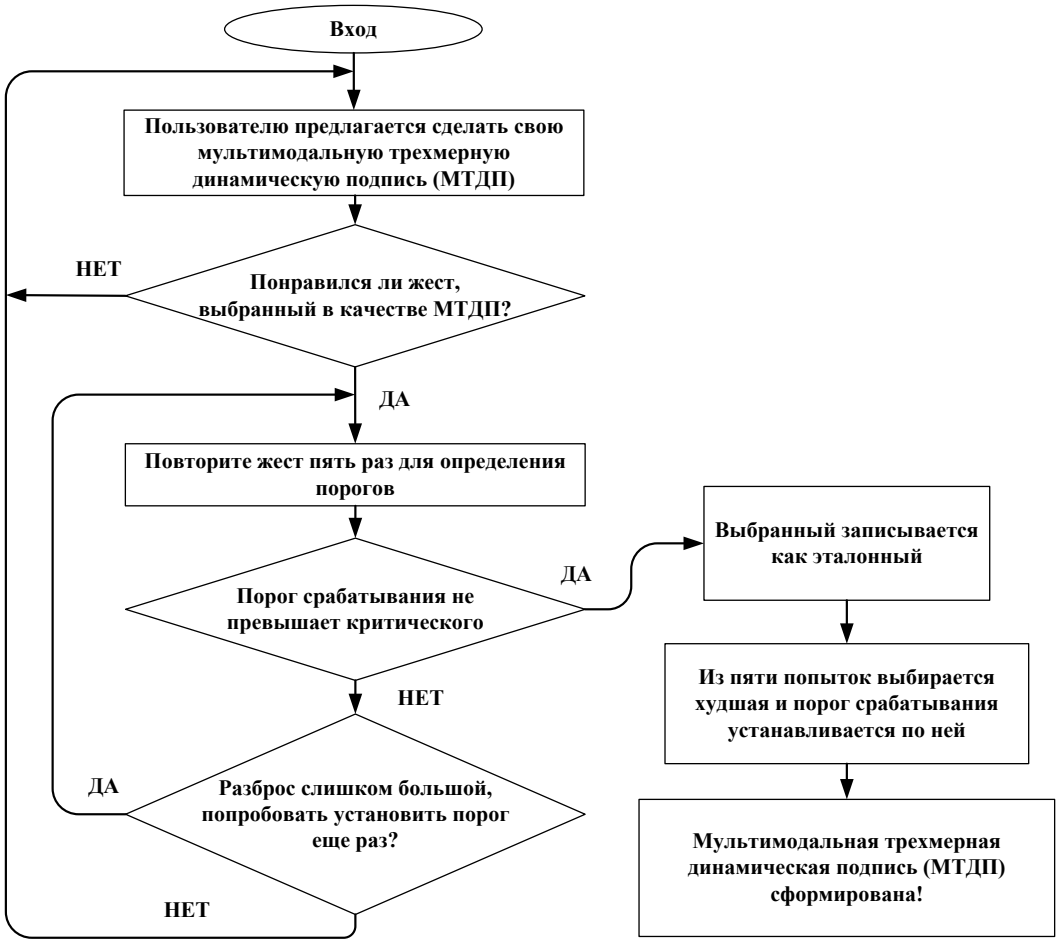

Рисунок 2 - Алгоритм формирования МДТП
(Fig. 2- Algorithm of formation MDTP)

После того, как МТДП сформирована, система готова к работе. Сама процедура аутентификации предполагает использование трех попыток для аутентификации. Если хотя бы одна из трех попыток соответствует шаблону с точностью, не превышающей порога, то аутентификация считается пройденной.

Укрупненный алгоритм процедуры аутентификации, реализованный в прототипе, представлен на рисунке 3.

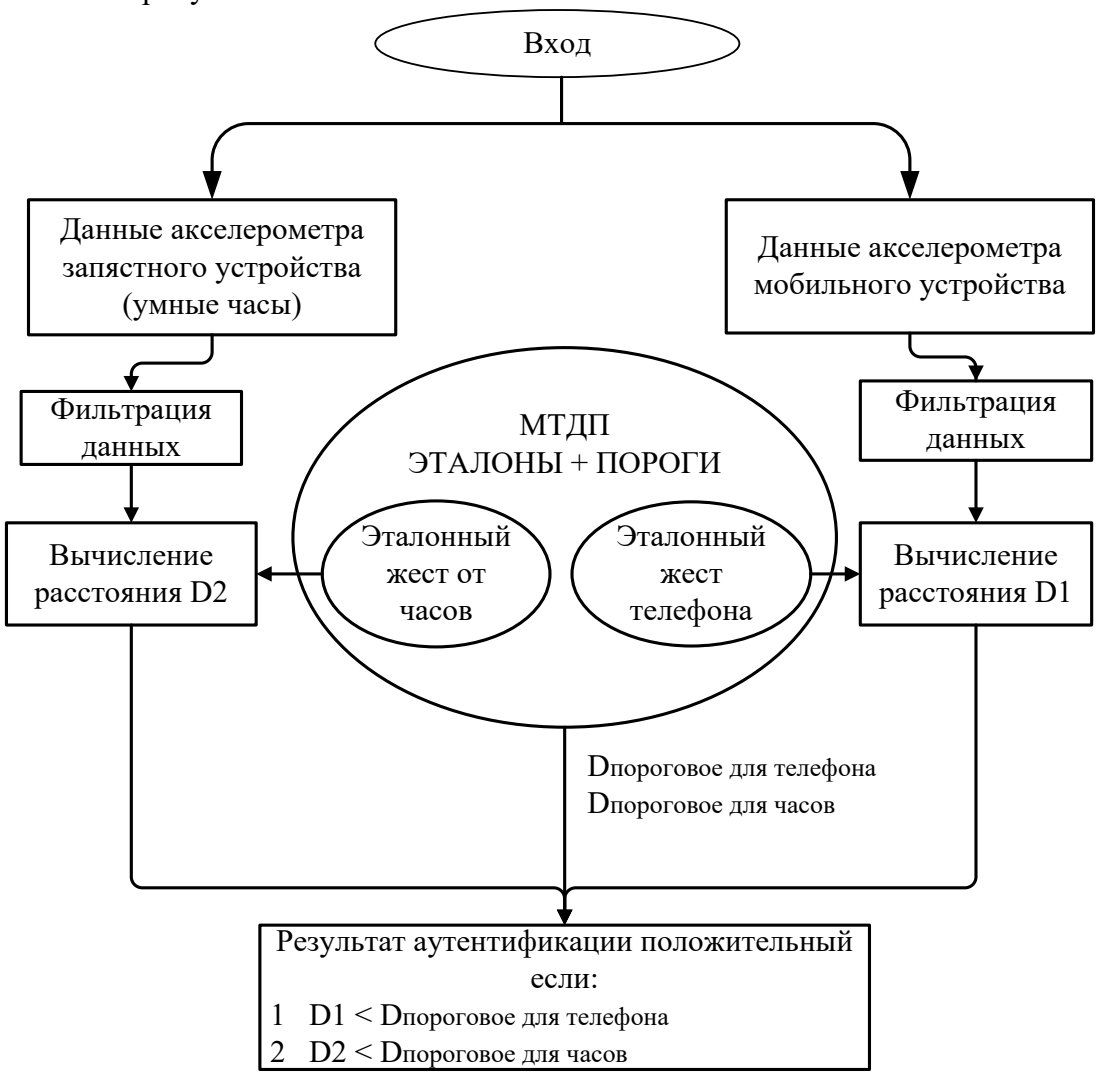

Рисунок 3 -Работа системы аутентификации на базе МТДП
(Fig. 3 - System-based authentication MTDP)

Данные акселерометров устройств участвующие в формировании МТДП и аутентификации являются временными рядами и для нахождения меры близости на всех шагах, где это требуется, используется алгоритм трансформации временного ряда (DTW). Допустим имеется эталон $Q=(q_1,q_2\ldots q_n)$ и воспроизведенный жест $C=(c_1,c_2\ldots c_m)$, суть алгоритма DTW заключается в вычислении минимального пути W по формуле (1) [8]:

$$DTW(Q,C) = min\left\{\frac{\sum_{k=1}^{k} d(w_k)}{K}\right\} \quad (1),$$

где:
K - длина пути,
$d(w_k) =(q_i-c_j)^2$ - элемент пути.

Прототип МТДП был опробован на нескольких современных смартфонах, время, необходимое программе для расчетов и принятия решения об аутентификации, для

пользователя кажется незаметным, это позволяет сделать вывод, что алгоритм с точки зрения производительности выбран правильно.

Создание прототипа системы аутентификации на базе МТДП позволило запланировать эксперимент для того, чтобы получить количественные оценки надежности системы.

В качестве показателей, характеристики которых должен определить эксперимент, являются ошибки первого FRR – вероятность отказа доступа человеку, имеющему доступ и второго рода FAR – вероятность ложного пропуска человека, не имеющего доступ.

Доверительный интервал для предварительной оценки точности ошибок можно определить по следующей формуле (2) [9].

$$p = \frac{n}{g^2+n}\left(\omega + \frac{g^2}{2n} \pm g\sqrt{\frac{\omega(1-\omega)}{n} + \frac{g^2}{4n^2}}\right) \quad (2),$$

Параметр g определяется уровнем доверительной вероятности на основе функции Лапласа. При уровне равном 0.95 параметр g = 1.96.

Предварительные результаты показали, чторост точности за счет использования двух устройств составил примерно 30 %. При этом были проанализированы 1500 попыток аутентификации, проводимой девятью различными людьми.

На рисунке 4 представлен анализ попыток аутентификация для одного из пользователей.

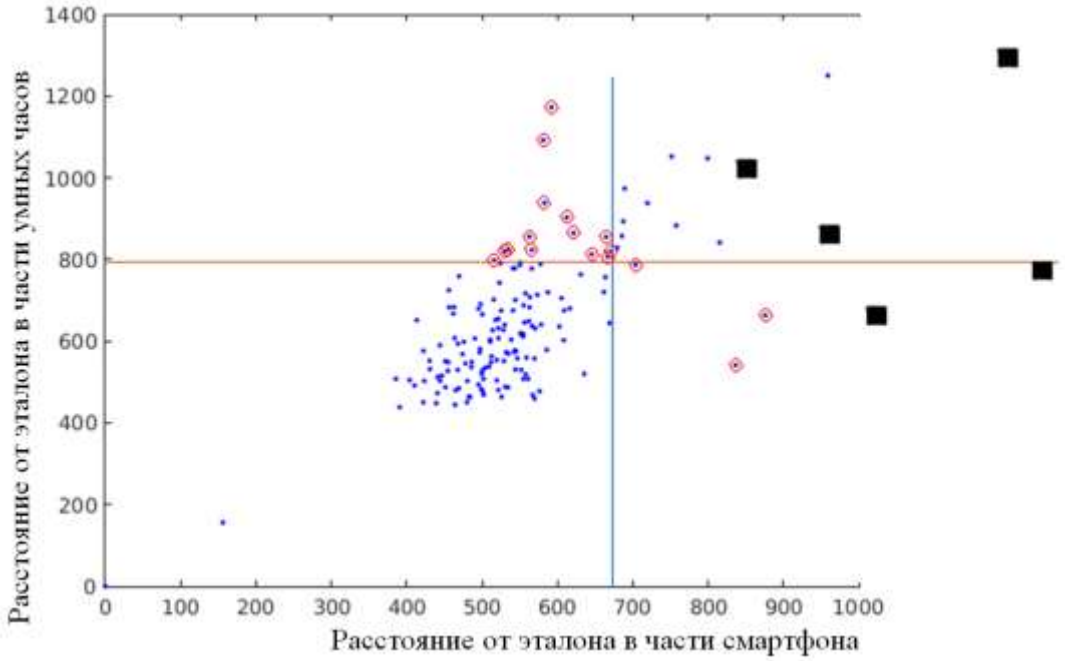

Рисунок4 - Анализ попыток аутентификации
(Fig. 4 - Analysis of authentication attempts)

По оси абсцисс на рисунке 4 отложены, полученные при помощи алгоритма DTW, расстояния между эталонной МТДП и воспроизведенной в части смартфона, а по оси ординат аналогичное расстояние для умных часов. Линии на рисунке - это пороги (уровни, выше которых происходит отсечение) для смартфона (вертикальная линия) и умных часов (горизонтальная линяя). Попытки, отсеченные (не прошедшие аутентификацию) только одним из устройств, обведены кружками. Квадраты на рисунке – попытки воспроизвести жест другим человеком, который видит воспроизведение жеста автором (попытки взлома).

Предварительнаяоценкачастотыошибокпервогоивторогородаможетбытьнайденаисхо дяизанализаошибоканалогов, учетом увеличения точности на 30%, и будет составлять для ошибок первого рода ω_1=0.025 и второго рода и ω_2=0.025 [5,6].

Для получения достоверных данных о надежности системы запланировано не менее 4000 экспериментовопределения вероятности ошибок первого рода и не менее 1000 экспериментовдля определения вероятности ошибок второго рода.

Подставляяэти данные в формулу(2), получаемпредварительныеграницыдоверительныхинтерваловдляошибокпервогоивторогорода: $p_1 \in [0.02; 0.03]$ и$p_2 \in [0.016; 0.036]$. Данныйрасчетявляется прикидочным, посколькусамихоцениваемыхвероятностейпоканет, однакопорядокоценкиточностиэтихзначенийнеизменится.

Основной проблемой МТДП и его предыдущих аналогов, так же как и у систем аутентификации на основе рукописной подписи, является выработка человеком ФДК, необходимого для достаточно точного воспроизведения подписи. Кроме того, сложность самой подписи тоже имеет решающее значение. Так, например, если в качестве МТДП, будет выбран просто круг в воздухе, то надежность такой подписи может быть поставлена под сомнение. В связи с этим МТДП будет дорабатываться системой оценки подписи, которая будет определять надежность, с учетом полученных порогов, а так же давать рекомендации пользователям о возможности ее применения.

Заключение

Система аутентификации личности на основе МТДП, реализованная в мобильных приложениях, обладает перспективами применения в условиях повышенного уровня акустического шума или плохого освещения, а также как вспомогательная методика аутентификации. Надежность системы позволяет использовать ее для всех типов мобильных приложений, где может требоваться аутентификация.

СПИСОК ЛИТЕРАТУРЫ:

1 Брагина Е. К., Соколов С. С. «Современные методы биометрической аутентификации: обзор, анализ и определение перспектив развития». ISSN 1812-9498. Вестник АГТУ. 2016 г. № 1 (61). С. 40-45.
2 ГОСТ Р 52633.0-2006. Национальный стандарт российской федерации защита информации техника защиты информации требования к средствам высоконадежной биометрической аутентификации. М.: Стандартинформ, 2007, 24 с.
3 Regulation (EU) 2016/679 of the european parliament and of the council, 2016. URL:http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (Дата обращения: 05.09.2017 г.).
4 Jiayang L., Zhen W., Lin Z., Jehan W., Venu V. «Wave: Accelerometer-based Personalized Gesture Recognition and its Applications». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09percom.pdf. (Дата обращения: 24.03.2017 г.).
5 Jiayang L., Lin Z., Jehan W., Venu V. «User Evaluation of Lightweight User Authentication with a Single Tri-Axis Accelerometer». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09mobilehci.pdf (Дата обращения: 24.03.2017 г.).
6 JavierGuerra-Casanova, CarmenSánchez-Ávila, GonzaloBailador-delPozo, AlbertodeSantos «ApplicationofLCSAlgorithmtoAuthenticateUserswithinTheirMobilePhoneThroughIn-AirSignatures». URL:https://www.intechopen.com/books/advanced-biometric-technologies/application-of-lcs-algorithm-to-authenticate-users-within-their-mobile-phone-through-in-air-signatur (Датаобращения: 06.09.2017 г.).
7 Козлов Ю.Е., Евсеев В.Л. «Метаматематическая модель мультимодальной жестовой аутентификации при помощи двух независимых мобильных устройств». Безопасность информационных технологий. 2017 г., №1, С. 49-55.
8 Herbst N. R. «Quantifying the Impact of Platform Configuration Space for Elasticity Benchmarking». Karlsruhe Institute of Technology. StudyThesis, 2011, 93 p.
9 Б.Л. ван дер Варден «Математическая статистика». Издательство иностранной литературы. Перевод с немецкого Л.Н. Большева, 1957 г., 435 с.

REFERENCES:

[1] Bragina E. K., Sokolov S. S. Modern methods of biometric authentication: a review, analysis and definition of prospects of development. ISSN 1812-9498. Vestnik AGTU. 2016. № 1 (61). P. 40-45. (in Russian).
[2] GOST R 52633.0-2006 Nacional'nyj standart rossijskoj federacii zashhita informacii tehnika zashhity informacii trebovanija k sredstvam vysokonadezhnoj biometricheskoj autentifikacii. M.: Standartinform, 2007, 24 p. (in Russian).

[3] Regulation (EU) 2016/679 of the european parliament and of the council, 2016. URL:http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf (accessed 05.09.2017).
[4] Jiayang L., Zhen W., Lin Z., Jehan W., Venu V. «Wave: Accelerometer-based Personalized Gesture Recognition and its Applications». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09percom.pdf. (accessed 24.03.2017).
[5] Jiayang L., Lin Z., Jehan W., Venu V. «User Evaluation of Lightweight User Authentication with a Single Tri-Axis Accelerometer». 2009. URL:http://www.ruf.rice.edu/~mobile/publications/liu09mobilehci.pdf (accessed 24.03.2017).
[6] Javier Guerra-Casanova, Carmen Sánchez-Ávila, Gonzalo Bailador-del Pozo, Alberto de Santos «Application of LCS Algorithm to Authenticate Users within Their Mobile Phone Through In-Air Signatures» URL:https://www.intechopen.com/books/advanced-biometric-technologies/application-of-lcs-algorithm-to-authenticate-users-within-their-mobile-phone-through-in-air-signatur (accessed 06.09.2017).
[7] Kozlov Y. E., Evseev V. L. «Metamathematics model multimodal gestural authentication with two independent mobile devices». Bezopasnost' informacionnyh tehnologij. 2017, №1, P. 49-55. (in Russian).
[8] Herbst N. R. «Quantifying the Impact of Platform Configuration Space for Elasticity Benchmarking». Karlsruhe Institute of Technology. Study Thesis, 2011, 93 p.
[9] B.L. van der Varden «Mathematical statistics». Izdatel'stvo inostrannoj literatury. Translated from the German by L. N. Bolsheva 1957, 435 p.(in Russian).

Поступила в редакцию - 01 июля 2017 г. Окончательный вариант – 01 ноября 2017 г.
Received – Jule 01, 2017. The final version – November 01, 2017.