Юрий Е. Козлов
Финансовый университет при Правительстве Российской Федерации (Финансовый университет),
Ленинградский проспект, 49, Москва, 125993, Россия
e-mail: kozlovye@yandex.ru, https://orcid.org/0000-0002-4448-0232

ПОДХОДЫ К ОПРЕДЕЛЕНИЮ НАДЕЖНОСТИ МУЛЬТИМОДАЛЬНОЙ ТРЕХМЕРНОЙ ДИНАМИЧЕСКОЙ ПОДПИСИ

DOI: http://dx.doi.org/10.26583/bit.2018.1.07

Аннотация. Рынок современных мобильных приложений предъявляет все более жесткие требования к надежности систем аутентификации. В статье рассматривается аутентификация с использованием мультимодальной трехмерной динамической подписи (МТДП), которая может использоваться в качестве основного или дополнительного средства аутентификации пользователей в мобильных приложениях. В ее основе лежит использование жеста в воздухе, выполняемого двумя независимыми мобильными устройствами в качестве идентификатора. Методика использования МТДП имеет ряд преимуществ по сравнению с используемыми в настоящее время биометрическими методиками, такими как отпечаток пальца, аутентификация по форме лица или речевая аутентификация. Она позволяет быстро сменить жест, который служит идентификатором, а также скрывать саму процедуру аутентификации, используя жесты, не привлекающие внимание. Несмотря на преимущества, использование МТДП имеет ряд ограничений, прежде всего — это необходимость выработки человеком функционально динамического комплекса (ФДК). Он необходим для повторения аутентифицирующего жеста с достаточной точностью. Для корректного формирования МТДП необходима система, реализующая оценку надежности жеста, а также его допустимые вариации. Подходы к решению данной задачи описаны в данной статье с разделением их по способам их реализации. Два подхода могут быть реализованы только с использованием сервера, как центра обработки МТДП, а один может быть реализован с использованием вычислительных ресурсов смартфона. В заключительной части статьи приведены данные опробования одной из методик на макете, реализующем аутентификацию при помощи МТДП.

Ключевые слова: аутентификация, мобильное устройство, акселерометр, персонализированный жест, подпись в воздухе, аутентификация жестом.
Для цитирования. ***КОЗЛОВ, Юрий Е.*** *ПОДХОДЫ К ОПРЕДЕЛЕНИЮ НАДЕЖНОСТИ МУЛЬТИМОДАЛЬНОЙ ТРЕХМЕРНОЙ ДИНАМИЧЕСКОЙ ПОДПИСИ. Безопасность информационных технологий, [S.l.], v. 25, n. 1, p. 74-80, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1095>. Дата доступа: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.07.*

Yury E. Kozlov
Financial University under the Government of the Russian Federation (Financial University),
Leningradsky Prospekt, 49, Moscow, 125993 (ГСП-3), Russia
e-mail: kozlovye@yandex.ru, https://orcid.org/0000-0002-4448-0232

Approaches to determining the reliability of a multimodal three-dimensional dynamic signature

DOI: http://dx.doi.org/10.26583/bit.2018.1.07

Abstract. The market of modern mobile applications has increasingly strict requirements for the authentication system reliability. This article examines an authentication method using a multimodal three-dimensional dynamic signature (MTDS), that can be used both as a main and

additional method of user authentication in mobile applications. It is based on the use of gesture in the air performed by two independent mobile devices as an identifier.
The MTDS method has certain advantages over currently used biometric methods, including fingerprint authentication, face recognition and voice recognition. A multimodal three-dimensional dynamic signature allows quickly changing an authentication gesture, as well as concealing the authentication procedure using gestures that do not attract attention. Despite all its advantages, the MTDS method has certain limitations, the main one is building functionally dynamic complex (FDC) skills required for accurate repeating an authentication gesture.
To correctly create MTDS need to have a system for assessing the reliability of gestures. Approaches to the solution of this task are grouped in this article according to methods of their implementation. Two of the approaches can be implemented only with the use of a server as a centralized MTDS processing center and one approach can be implemented using smartphone's own computing resources. The final part of the article provides data of testing one of these methods on a template performing the MTDS authentication.
Keywords: authentication, mobile device, accelerometer, personalized gestured, in-air signature, handwaving authentication.
For citation. ***KOZLOV, Yury E.*** *Approaches to determining the reliability of a multimodal three-dimensional dynamic signature. IT Security (Russia), [S.l.], v. 25, n. 1, p. 74-80, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1095>. Date accessed: 15 feb. 2018. doi:http://dx.doi.org/10.26583/bit.2018.1.07.*

ВВЕДЕНИЕ

Развитие информационных технологий и тренд мобильности привели к тому, что современное мобильное устройство – смартфон/планшет или иной «гаджет» зачастую используется в качестве мобильного офиса, центра развлечений и инструмента для потребления Интернет-контента. Использование биометрических методик аутентификации в мобильных приложениях повышает информационную безопасность. Это связано с таким свойством биометрии как неотторжимость биометрического признака. Однако возросло количество сообщений о краже и фальсификации биометрических признаков [1, 2]. Это, прежде всего, связано с тем, что в подавляющее большинство этих признаков, таких как отпечаток пальца, радужная оболочка глаза и речь не могут быть скрыты. Кроме того, методики аутентификации при помощи данных признаков тоже не являются секретом.

Противодействие подделкам биометрических признаков идет в двух направлениях – разработка новых методик защиты биометрических параметров [3-5], а также разработка новых методик. Например, делаются попытки сделать систему, делающую традиционные биометрические признаки модифицируемыми и сменяемыми [6]. Среди работ по поиску легко модифицируемых и сменяемых биометрических признаков стоит выделить аутентификацию при помощи жеста [7-9]. Мультимодальная трехмерная динамическая подпись (МТДП) является одной из таких методик и может быть использована как основное, так и резервное средство. МТДП имеет ряд преимуществ перед традиционными биометрическими методиками, используемыми в мобильных приложениях, таких как отпечаток пальца, распознавание по радужной оболочки глаза, распознавание лица, а также распознавание речевых характеристик. Это, прежде всего, возможность скрытой аутентификации и быстрой смены признака. Однако МТДП имеет ряд недостатков, главным из которых является необходимость запоминания жеста, служащего биометрическим признаком, или если говорить научным языком - выработка при этом функционально-динамического комплекса навыков (ФДК). Одним из средств, которые могут помочь в этом пользователю, является создание системы классификации жестов. Такая система позволит выдавать пользователю оценку надежности жеста и рекомендации по его использованию.

Варианты реализации аутентификация при помощи МТДП

Методика МТДП основана на использовании специального жеста для аутентификации, который регистрируется акселерометрами двух устройств – смартфона и умных часов. Данные акселерометра от умных часов по bluetooth попадают в смартфон. Дальнейшие вычисления могут идти в смартфоне или передаваться на сервер.

Фактически МТДП представляет собой «эталоны» и «пороги». Эталоны - это данные акселерометров умных часов и смартфона, полученные во время жеста, который пользователь выбирает как свою мультимодальную трехмерную подпись. «Пороги» - это максимально возможный разброс значений акселерометров, при превышении которых аутентификация будет считаться не пройденной.

Данные акселерометров устройств, участвующих в формировании МТДП и аутентификации, являются временными рядами и для нахождения меры схожести использование хорошо зарекомендовавшего себя алгоритма DTW (алгоритм трансформации временной шкалы) для сравнения жеста с эталоном [10, 11]. Суть алгоритма в вычислении нелинейного отображения одного временного ряда в другой с помощью минимизации расстояний между ними.

Допустим имеется эталон $Q = q_1,q_2,\ldots,q_n$ и воспроизведенный жест $C = c_1,c_2,\ldots,c_m$, тогда с помощью алгоритма DTW по формуле (1) можно определить кратчайший путь W [12]:

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

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

В ходе исследования жестов в качестве идентификаторов использовались два макета - МТДП1 и МТДП2. Макет МТДП1 предполагал выработку двух порогов для смартфона и часов по формулам (2). Под порогом срабатывания подразумевается значение, при превышении которого, аутентификация считается не пройденной:

$$\begin{gathered} P_s = DTW(X_s,X_{se}) + DTW(Y_s,Y_{se}) + DTW(Z_s,Z_{se}) \\ P_w = DTW(X_w,X_{we}) + DTW(Y_w,Y_{we}) + DTW(Z_w,Z_{we}), \end{gathered} \quad (2)$$

где P_s и P_w – соответственно меры схожести жеста с эталоном смартфона и жеста с эталоном умных часов; X_s, Y_s, Z_s – значения ускорений по трем осям, полученные от смартфона; X_w,Y_w, Z_w - значения ускорений по трем осям, полученные от умных часов; X_{se}, Y_{se}, Z_{se}, X_{we},Y_{we}, Z_{we} - значения ускорений, хранящиеся в качестве эталона, для трех осей смартфона и трех осей умных часов.

Для второго макета пороги вырабатываются для каждой координаты отдельно (3):

$$\begin{gathered} P_{sx} = DTW(X_s,X_{se});\ P_{sy} = DTW(Y_s,Y_{se});P_{sz} = DTW(Z_s,Z_{se}) \\ P_{wx} = DTW(X_w,X_{we});\ P_{wy} = DTW(Y_w,Y_{we});\ P_{wz} = DTW(Z_w,Z_{we}), \end{gathered} \quad (3)$$

где P_{sx}, P_{sy}, P_{sz} - меры схожести жеста с эталоном смартфона, P_{wx}, P_{wy}, P_{wz} - меры схожести жеста с эталоном умных часов.

Решение об успешной аутентификации A=1 принимается в случае, если меры схожести между воспроизведенным жестом и эталонами смартфона и умных часов не превышают установленных порогов – формулы (4) и (5) для первого и второго макетов, соответственно:

$$A = (P_s \le P_{se}) \cap (P_w \le P_{we}), \quad (4)$$

$$A = (P_{sx} \le P_{sxe}) \cap (P_{sy} \le P_{sye}) \cap (P_{sz} \le P_{sze}) \cap$$

$$\cap (P_{wx} \leq P_{wxe}) \cap (P_{wy} \leq P_{wye}) \cap (P_{wz} \leq P_{wze}), \quad (5)$$

где P_{se}, P_{sxe}, P_{sye}, P_{sze} - пороги для смартфона, P_{we}, P_{wxe}, P_{wye}, P_{wze} - пороги для умных часов.

Пороги для двух вышеуказанных макетов формируются следующим образом:

- пользователь придумывает жест и принимает решение о том, что он будет эталоном;
- выбранный жест пользователь воспроизводит пять раз. Для каждого раза вычисляются меры схожести по формулам (2) или (3);
- наибольшие меры схожести из пяти попыток выбираются в качестве порогов.

При этом могут возникнуть следующие негативные сценарии формирования МТДП:

- если жесты очень похожи и пороги были установлены слишком жестко, то в реальных условиях возможно большое количество ошибок первого рода - недопуск своего;
- если был выбран слишком простой жест или жесты слишком различались, то пороги будут установлены слишком мягко - это повысит вероятность ошибки второго рода - допуск чужого (иной жест будет принят за подлинный) и ошибка третьего рода – подделка (спуфинг) МТДП.

Оба сценария будут ставить под угрозу информационную безопасность мобильного приложения в случае выбора МТДП в качестве средства аутентификации.

Задачи системы оценки МТДП

Первой и очевидной задачей системы оценки МТДП является определение максимального порога, исходя из характеристик жеста – чем проще жест, тем жестче должен быть установлен порог. Это необходимо для того, чтобы ошибки третьего и второго рода для всех видов жестов была в допустимых пределах.

Исходя из назначения мобильного приложения, система оценки МТДП может решать еще одну задачу – выдавать рекомендацию к применению. Так, например, для входа в банковские приложения стоит рекомендовать более сложные жесты, а для разблокировки смартфона можно использовать более простые. Отсюда вытекает еще одна задача – система не должна пропускать слишком простые жесты. Например, когда пользователь вместо жеста будет держать телефон на одном месте.

Важно отметить, что, поскольку МТДП предполагает жесткую связку смартфона и умных часов, то системе оценки достаточно работать только с показаниями смартфона – оценивая только жест, зарегистрированный им. Далее в статье все оценки будут предполагать оценку данных только смартфона.

Прежде чем искать пути реализации системы оценки МТДП стоит определить диапазон работы этой системы. Одной из самых очевидных характеристик, позволяющих провести такой анализ, является сумма значений временных рядов МТДП.

В таблице 1 представлены результаты суммирования всех значений временных рядов (какими являются показания акселерометра по трем осям), выполненные по формуле (6) для различных жестов:

$$M = \sum_1^i |x_i| + |y_i| + |z_i|, \quad (6)$$

где M – сумма всех значений ускорений по трем осям, i – количество значений во временном ряду, x_i, y_i, z_i – показания акселерометра для осей x, y и z. При этом влияние гравитации убрано согласно рекомендациям разработчиков ОС Android.

Таблица 1. Результаты суммирования временных рядов МТДП для разных жестов.

Жест	Сумма значений M
Круг	250 - 350
Квадрат	300 - 450
Крест	1300 - 1700
Тряска смартфона	3000 - 5000

Время воспроизведения всех указанных жестов примерно равно 1 с. Предельная же сумма значений с учетом максимального значения ускорения равного 39 м/с^2 и частоте работы акселерометра 1600 Гц равна 187200 за одну секунду.

Так как система оценки МТДП должна быть доступна широкому кругу пользователей, то представляется целесообразным, свести задачу системы к отнесению выбранного жеста к одному из четырех классов:

- высокая надежность;
- средняя надежность;
- низкая надежность;
- недопустимая МТДП.

При этом внутренний алгоритм может использовать более широкий диапазон классов для реализации более тонкой настройки.

Подходы к реализации системы оценки МТДП

Можно выделить три наиболее подходящих методики решения задачи классификации МТДП:

1) использование метода KNN – k - ближайших соседей;
2) использование нейронной сети;
3) ранжирование надежности в зависимости от M (суммы модулей ускорений).

Методика KNN–k - ближайших соседей широко используется для анализа рукописных подписей [13]. Она предполагает создание базы МТДП ранжированных по классам от высокой надежности до недопустимой МТДП. При создании подписи происходит вычисление меры схожести к каждому объекту в базе. В качестве меры схожести также может быть использован алгоритм DTW (7):

$$Q_j = \sum_{i=1}^{n} \frac{1}{DTW(x,a_i)}, \quad (7)$$

где Q_j – классы МТДП, x – воспроизведенный жест, a_i - объекты класса.

Вторая методика – использование нейронной сети также используется для анализа рукописной подписи [14]. Для использования данной технологии, как и для метода k-ближайших соседей, должен быть использован сервер, как центр обработки МТДП.

Для создания классификатора МТДП могут использоваться нейронные сети хорошо себя зарекомендовавшие в распознавании рукописных подписей:

1)персептроны, ГОСТ Р 52633.5-2011, и их модификации;
2)нечеткий экстрактор;
3)сети квадратичных форм.

Методика KNN – k - ближайших соседей и использование нейронной сети не могут использовать вычислительные ресурсы только смартфона, однако такая реализация МТДП может потребоваться, например, для разблокировки смартфона.

Методика ранжирования надежности в зависимости от суммы модулей всех значений ускорений – M для своей работы может использовать ресурсы только

смартфона. Суть ее в классификации МТДП в зависимости от M. Кроме того следует ввести ограничение на максимально возможный порог P_{max}. Так как от величины M должна зависеть величина порога, можно устанавливать P_{max} в зависимости от M (8):

$$P_{max} = \frac{M}{M+\Delta}, \quad (8)$$

где Δ - значение, которое может быть рассчитано экспериментально и будет ограничивать P_{max}. Пример ограничения по P_{max} показан кривой на рисунке 1.

Жесты, имеющие слишком маленькое значение M, либо слишком большой разброс $P>P_{max}$, стоит признать недопустимыми. Для остальных жестов эмпирически могут быть подобраны значения M, при превышении которых жест будет попадать в классы высокой, средней или низкой надежности.

На рисунке 1 представлены результаты опробования макета МТДП1 на группе из пяти человек.

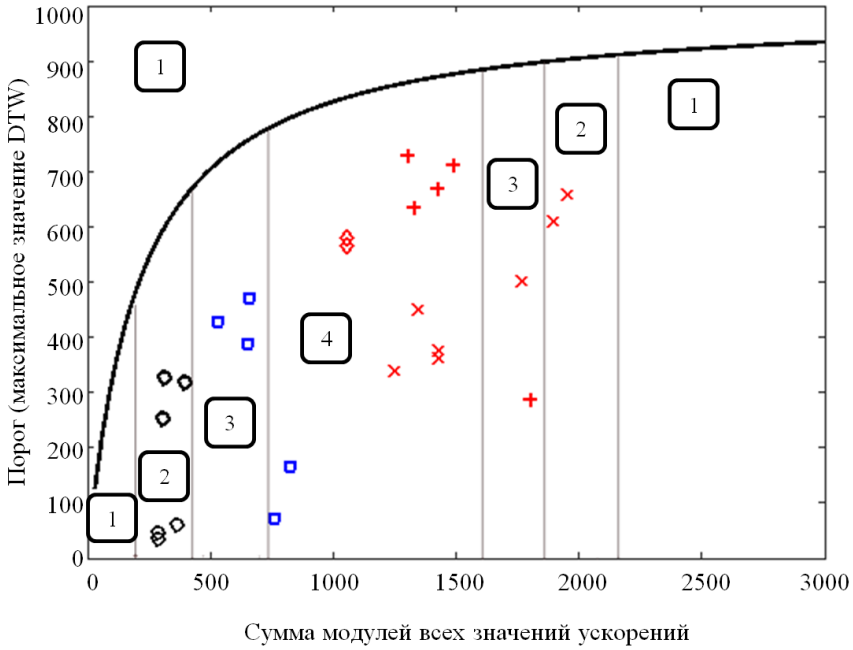

Рис. 1. Результаты опробования макета МТДП1)
(Fig. 1. Results of testing the layout of MTDP1)

На рисунке 1 кроме ограничения, заданного по формуле (8), показаны зоны, ранжированные по величине M:

1 - зона недопустимых жестов;
2 - зона жестов с низкой надежностью;
3 - зона жестов со средней надежностью;
4 - зона жестов с высокой надежностью.

Для каждого представленного на рисунке 1 жеста были проведены проверки воспроизводимости и не менее пяти попыток взлома (спуфинга), когда жест выполнялся другим человеком.

Заключение

Несмотря на участившиеся сообщения о возможностях подделки и кражи биометрических признаков, использование биометрии в системах верификации и аутентификации продолжит расти. Новые технологии будут применяться и в смежных областях деятельности человека, например, бумажном документообороте [15]. Система аутентификации личности на основе МТДП может получить распространение в мобильных приложениях за счет ее преимуществ перед ныне используемыми

биометрическими технологиями, такими как возможность скрытной аутентификации и быстрая смена идентификатора. Реализация системы оценки жеста позволит сделать его удобным для использования и повысить его характеристики с точки зрения надежности.

СПИСОК ЛИТЕРАТУРЫ:

1 Abhishek K., Yogi A. «A minutiae Count Based Method for Fake Fingerprint Detection» Procedia Computer Science. – 2015. – Т. 58. – P. 447-452.
2 Chingovska I. Trustworthy Biometric Verification under Spoofing Attacks. – 2016.
3 Козлачков С.Б., Дворянкин С.В., Бонч-Бруевич А.М. «Проблемы и перспективы защиты акустической речевой информации». Специальная техника. – 2016. – №. 6. – С. 15-21.
4 Galbally J., Gomez-Barrero M. «A review of iris anti-spoofing». Biometrics and Forensics (IWBF), 2016 4th International Workshop on. – IEEE, 2016. – P. 1-6.
5 Sinha V.K., Gupta A. «Enhancing Iris Security by Detection of Fake Iris». National Conference Gyan Jyoti–National Conference MITE. – 2016. – P. 1-22.
6 Patel V. M., Ratha N. K., Chellappa R. Cancelable biometrics: A review IEEE Signal Processing Magazine. – 2015. – Т. 32. – №. 5. – P. 54-65.
7 Wang Z., Shen C., Chen Y. Handwaving Authentication: Unlocking Your Smartwatch Through Handwaving Biometrics. Chinese Conference on Biometric Recognition. – Springer, Cham, 2017. – P. 545-553.
8 Casanova J. G. et al. A real-time in-air signature biometric technique using a mobile device embedding an accelerometer. International Conference on Networked Digital Technologies. – Springer, Berlin, Heidelberg, 2010. – P. 497-503.
9 Козлов Ю.Е., Евсеев В.Л. «Мультимодальная трехмерная динамическая подпись». Безопасность информационных технологий. – 2017 г., № 4, С. 44-51.
10 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.
11 Bailador G. et al. «Analysis of pattern recognition techniques for in-air signature biometrics». Pattern Recognition. – 2011. – Т. 44. – №. 10. – P. 2468-2478.
12 Salvador S., Chan P. «Toward accurate dynamic time warping in linear time and space». Intelligent Data Analysis. – 2007. – Т. 11. – №. 5. – P. 561-580.
13 Kaur J., Sharma R. «A comparison of artificial neural network and k-nearest neighbor classifiers in the off-line signature verification». International Journal. – 2017. – Т. 8. – №. 7. P. 380-383.
14 Ложников П.С. и др. «Экспериментальная оценка надежности верификации подписи сетями квадратичных форм, нечеткими экстракторами и персептронами». Информационно-управляющие системы. – 2016. – №. 5 (84). С. 73-85.
15 Алюшин А.М., Дворянкин С.В. «Использование речевых технологий для защиты документооборота». Безопасность информационных технологий. – 2017. № 2. С. 6-15.

REFERENCES:

[1] Abhishek K., Yogi A. «A minutiae Count Based Method for Fake Fingerprint Detection». Procedia Computer Science. – 2015. – Т. 58. – P. 447-452.
[2] Chingovska I. Trustworthy Biometric Verification under Spoofing Attacks. – 2016.
[3] Kozlachkov S.B., Dvorjankin S.V., Bonch-Bruevich A.M. «Problems and prospects of protection of acoustic speech information". Special equipment. – 2016. – №. 6. – P. 15-21. (in Russian)
[4] Galbally J., Gomez-Barrero M. «A review of iris anti-spoofing». Biometrics and Forensics (IWBF), 2016 4th International Workshop on. – IEEE, 2016. – P. 1-6.
[5] Sinha V. K., Gupta A. «Enhancing Iris Security by Detection of Fake Iris». National Conference Gyan Jyoti – National Conference MITE. – 2016. – P. 1-22.
[6] Patel V. M., Ratha N. K., Chellappa R. Cancelable biometrics: A review. IEEE Signal Processing Magazine. – 2015. – T. 32. – №. 5. – P. 54-65.
[7] Wang Z., Shen C., Chen Y. Handwaving Authentication: Unlocking Your Smartwatch Through Handwaving Biometrics. Chinese Conference on Biometric Recognition. – Springer, Cham, 2017. – P. 545-553.
[8] Casanova J. G. et al. A real-time in-air signature biometric technique using a mobile device embedding an accelerometer. International Conference on Networked Digital Technologies. – Springer, Berlin, Heidelberg, 2010. – P. 497-503.
[9] Kozlov Ju.E., Evseev V.L. « Multimodal three-dimensional dynamic signature". Security of information technologies. – 2017 г., № 4, P. 44-51. (in Russian)
[10] Kozlov Ju.E., Evseev V.L. «Metamathematics model multimodal gestural authentication with two independent mobile devices." Security of information technologies. – 2017 г., № 1, P. 49-55. (in Russian)
[11] Bailador G. et al. «Analysis of pattern recognition techniques for in-air signature biometrics». Pattern Recognition. – 2011. – T. 44. – №. 10. – P. 2468-2478.
[12] Salvador S., Chan P. «Toward accurate dynamic time warping in linear time and space». Intelligent Data Analysis. – 2007. – T. 11. – №. 5. – P. 561-580.
[13] Kaur J., Sharma R. «A comparison of artificial neural network and k-nearest neighbor classifiers in the off-line signature verification». International Journal. – 2017. – T. 8. – №. 7. P. 380-383.
[14] Lozhnikov P. S. i dr. «Experimental estimation of reliability of signature verification by networks of quadratic forms, fuzzy extractors and perceptrons". Information and control systems. – 2016. – №. 5 (84). P. 73-85. (in Russian)
[15] Aljushin A.M., Dvorjankin S.V. « Use of speech technologies to protect document flow". Security of information technologies. – 2017. № 2. P. 6-15. (in Russian)

Поступила в редакцию – 18 декабря 2017 г. Окончательный вариант – 06 февраля 2018г.
Received – December 18, 2017. The final version – February 06, 2018.