Y.E. Kozlov, V.L. Evseev
*Financial University under the government of the Russian Federation (Financial University),*
*125993, GSP-3, Moscow, Leningradsky prospect, 49,*
*e-mail: kozlovye@yandex.ru,ORCID iD 0000-0002-4448-0232,*
*e-mail: VLevseev@fa.ru, ORCID iD 0000-0003-3283-3106*

**Metamathematical Model Multimodal Gestural Authentication Using Two Independent Mobile Devices**

*Key words: authentication, mobile device, accelerometer, mathematical model, personalized gesture.*
The article considered by the relevance of authentication using the gesture performed by the mobile device. Shown the urgency of the application of the proposed authentication method in mobile applications Presented it place in the classification of authentication methods. Shown approaches and application of this methodology. Formulated the problem solved in the framework of authentication through the use of two separate devices simultaneously. Presented the algorithm of authentication using the gesture performed by two mobile devices.Considered the restrictions this algorithm.For formulated mathematical problem shown mathematical model. For the proposed model determined the necessary computing power. At the end will be discussed the options, which can potentially increase the reliability techniques of authentication.

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

# МЕТАМАТЕМАТИЧЕСКАЯ МОДЕЛЬ МУЛЬТИМОДАЛЬНОЙ ЖЕСТОВОЙ АУТЕНТИФИКАЦИИ ПРИ ПОМОЩИ ДВУХ НЕЗАВИСИМЫХ МОБИЛЬНЫХ УСТРОЙСТВ

*Ключевые слова: аутентификация, мобильное устройство, акселерометр, математическая модель, персонализированный жест.*
В статье рассмотрена актуальность аутентификации при помощи жеста, выполняемого мобильным устройством. Показана актуальность применения предложенной методики аутентификации в мобильных приложениях. Приведено ее место в классификации способов аутентификации. Рассмотрены существующие подходы и область применения данной методики. Сформулирована задача, решаемая в рамках аутентификации при помощи использования двух независимых устройств одновременно. Приводится алгоритм работы жестовой аутентификации, выполняемой одновременно мобильным и запястным устройством. Рассмотрены ограничения, действующие для данного алгоритма. Для сформулированной математической задачи предложена математическая модель. Для предложенной модели определены необходимые вычислительные мощности. В заключение рассмотрены варианты, которые потенциально могут повысить надежность методики.

Современные методы аутентификации в мобильных приложениях можно подразделить на три категории:

1) то, что знает пользователь;

2) то, чем обладает пользователь;

3) то, что «есть» сам пользователь (биометрическая аутентификация).

Мало кто сегодня сомневается в том, что в будущем осуществится переход на четвертую категорию методов аутентификации клиента в мобильных приложениях - мультимодальная жестовая аутентификация [1], которая включает в себя все три вышеуказанных категории.

Данный метод аутентификации основывается на методике, в основе которой лежит выполнение специального заранее продуманного аутентифицирующего жеста мобильным устройством. С целью повышения надежности воспроизведения жеста, его регистрация производится двумя устройствами одновременно – мобильным и запястным.

В результате сам жест, известный только пользователю и «заложенный» в данную методику, позволяет отнести эту методику к первой категории. Запястное устройство, служащее также ключом к разблокировке мобильного телефона, предполагает отнесение методики ко второй категории. А аутентифицирующий жест, зависящий от анатомических особенностей человека, позволяет отнести данную методику к третьей категории.

На рис. 1 представлен пример жеста, который может служить для аутентификации (точка – начало траектории, а стрелка – ее направление).


*Рис. 1. Пример жеста пользователя*

В качестве жеста может быть использован любой жест, который пользователь сможет запомнить и впоследствии воспроизводить. Данный жест – своего рода трехмерная подпись, удостоверяющая личность.

Для определения характеристик устройства в пространстве применяют встроенный в него акселерометр. В качестве запястного устройства может использоваться любое устройство имеющее акселерометр, например умные часы или фитнес-браслет.

Работы, описывающие данную методику аутентификации, начали появляться с 2009 года. Одна из самых известных методик представлена алгоритмом uWave, использующая, в качестве основы, методику динамической трансформации шкалы времени – DTW «DynamicTimeWarping» [2]. Эксперименты, выполненные разработчиками, показали низкую надежность методики. При этом вероятность ошибки первого ли, второго

ли рода равна примерно 1,4 %, а вероятность подделки аутентифицирующего жеста для одного устройства составляла примерно 10 %, если злоумышленник видит, как пользователь выполняет свой жест [3]. При использовании же двух устройств вероятность подделки значительно снижается, так как аутентифицирующий жест содержит значительно больше анатомических особенностей строения руки человека, что будет отмечено ниже.

Рука человека представляет собой три шарнирно соединенных звена (плечо, предплечье, кисть) и имеет девять степеней свободы (подвижности).

Предполагается, что при выполнении аутентифицирующего жеста человек держит мобильное устройство, зажав его между большим пальцем и кистью (см. рис. 1). В этом случае считается, что мобильное устройство относительно кисти неподвижно. Показания акселерометра, получаемые с устройств, будут содержать следующие биометрические характеристики:

длина предплечья, которая будет влиять на расстояние между мобильным и запястным устройством, а значит, будет определять соотношение фигур, описываемых мобильным и запястным устройством;

естественное положение локтя человека, которое будет определять положение предплечья относительно плечевого сустава в горизонтальной плоскости, а значит, будет влиять на траекторию мобильного и запястного устройства;

для аутентифицирующего жеста, как и для личной подписи, можно выявить уникальные характеристики свойственные только конкретному человеку.

На рис. 2 представлена схема математической модели аутентификации, использующей мобильное и запястное устройство одновременно.

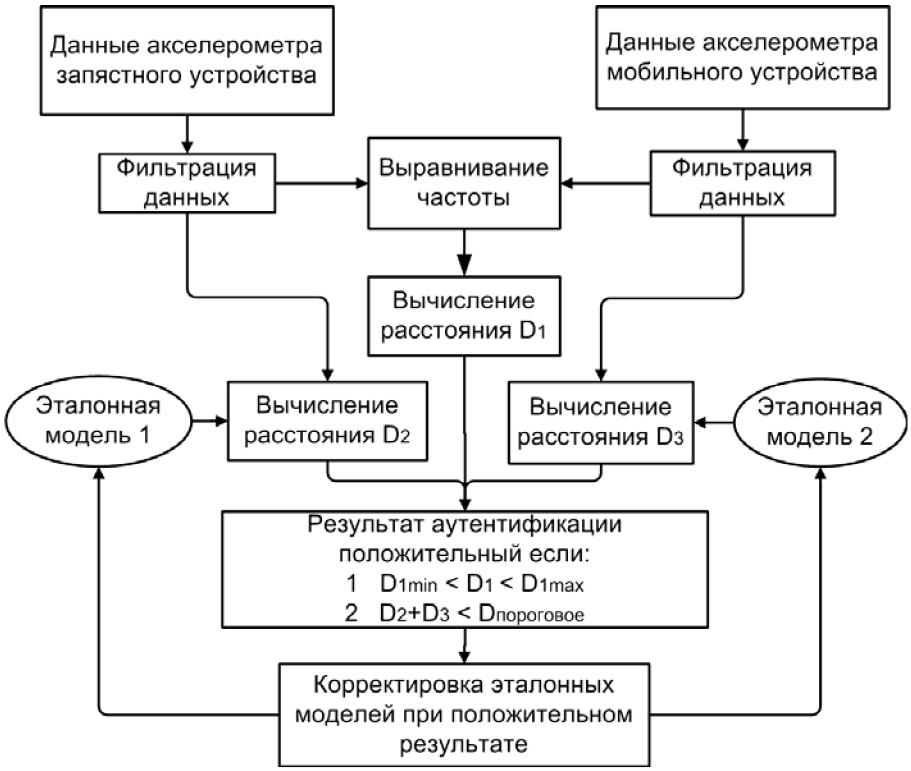


*Рис. 2. Схема математической модели аутентификации, использующей мобильное и запястное устройство одновременно*

Для блоков фильтрации, вычисления расстоянии и определения результатов модель представлена уравнениями, показанными ниже. На вход модели попадают данные акселерометров мобильного и запястного устройства. Затем осуществляется фильтрация, необходимая для удаления помех, вызванных работой самого устройства и вибрациями, создаваемыми рукой человека [4]. Фильтрация производится методом простого скользящего среднего, который хорошо подходит для данного типа сигнала [5]. Метод описывается уравнением

$$A_t = \frac{1}{n}\sum_{i=0}^{n-1} p_{t-i}\,, \tag{1}$$

где $A_t$ – значение взвешенного скользящего среднего в точке $t$; $n$ – количество значений исходной функции для расчёта скользящего среднего в реализованной математической модели; экспериментальным методом выбрано $n = 20$; $p_{t-i}$ – значение исходной функции в момент времени, отдалённый от текущего на $i$ интервалов.

Количество данных, поступающих на вход данной математической модели относительно невелико и будет составлять не более 200 кбайт для обоих устройств, при длительности жеста до 5 с, поэтому для вычисления расстояний $D_1$, $D_2$, $D_3$ хорошо подходит алгоритм *DTW* [6]. Получаемые в результате работы алгоритма *DTW* расстояния являются расстояниями Левенштейна, которые находятся следующим образом. Пусть строки $S_1$ и $S_2$ – две строки над некоторым алфавитом длиной $M$ и $N$ соответственно. Расстояние Левенштейна для каждого из $d(S_1,S_2)$ рассчитывается по рекуррентной формуле

$$d(S_1, S_2) = D(M, N), \tag{2}$$

где $D(M, N)$ представлено формулой

$$D(i,j) = \begin{cases} 0; & i = 0, j = 0 \\ i; & j = 0, i > 0 \\ j; & i = 0, j > 0 \\ \min\begin{pmatrix} D(i,j-1)+1, \\ D(i-1,j), \\ D(i-1,j-1)+m(S_1[i],S_2[j]) \end{pmatrix}; & j > 0,\ \ i > 0, \end{cases} \tag{3}$$

где $m(S_1[i], S_2[j])$ равна нулю, если $S_1[i] = S_2[j]$, и единице в противном случае. Очевидно, что $d\,(S_1, S_2) = 0$ если $S_1 = S_2$. Так как траектория движения описывается тремя координатами, то сравнение с эталонным сигналом – это три расстояния $d\,(x_1,x_2)$, $d\,(y_1,y_2)$, $d\,(z_1,z_2)$, где $x_1$, $y_1$, $z_1$ – значения хранящегося эталона, а $x_2$, $y_2$, $z_2$ – произведенный жест. Сумма всех расстояний для мобильного и запястного устройства $D_\sum$ будет сравниваться с пороговым значением $D_{\text{пор}}$ для принятия решения об аутентификации. При идеально воспроизводимом жесте $D_\sum$ будет стремиться к нулю.

Сравнение произведенного жеста с эталонным для мобильного и запястного устройства является классической задачей определения подобия и не представляет сложности. Выбор порога расхождения может осуществляться непосредственно при формировании эталонных сигналов, которые будут обновляться по мере работы системы ау-

тентификации. Предполагается хранение двух эталонных сигналов для каждого из устройств. Вычисление расстояний будет проводиться для обоих эталонных сигналов. Если аутентификация пройдена, то наиболее старый эталонный сигнал будет подменен произведенным жестом.

Вычисление расстояния $D_1$ будет иметь некоторые особенности. Рука человека устроена таким образом, что телефон, удерживаемый, как показано на рис. 1, будет развернут к надетым на руке часам приблизительно на 90°, следовательно, вычисление $D_1$ лучше всего производить по формуле

$$D_1 = d\,(x_1,z_2) + d\,(y_1,y_2) + d\,(z_1,x_2), \tag{4}$$

где $x_1$, $y_1$, $z_1$ – значения ускорений телефона, а $x_2$, $y_2$, $z_2$ – значения ускорений умных часов. На рис. 3 показаны значения ускорений при круговом жесте для осей $X_{\text{телефона}}Z_{\text{часов}}$ (верхняя часть) $Y_{\text{телефона}}Y_{\text{часов}}$ (средняя часть) и $Z_{\text{телефона}}X_{\text{часов}}$ (нижняя часть), полученные на реализованной в среде Matlab модели.

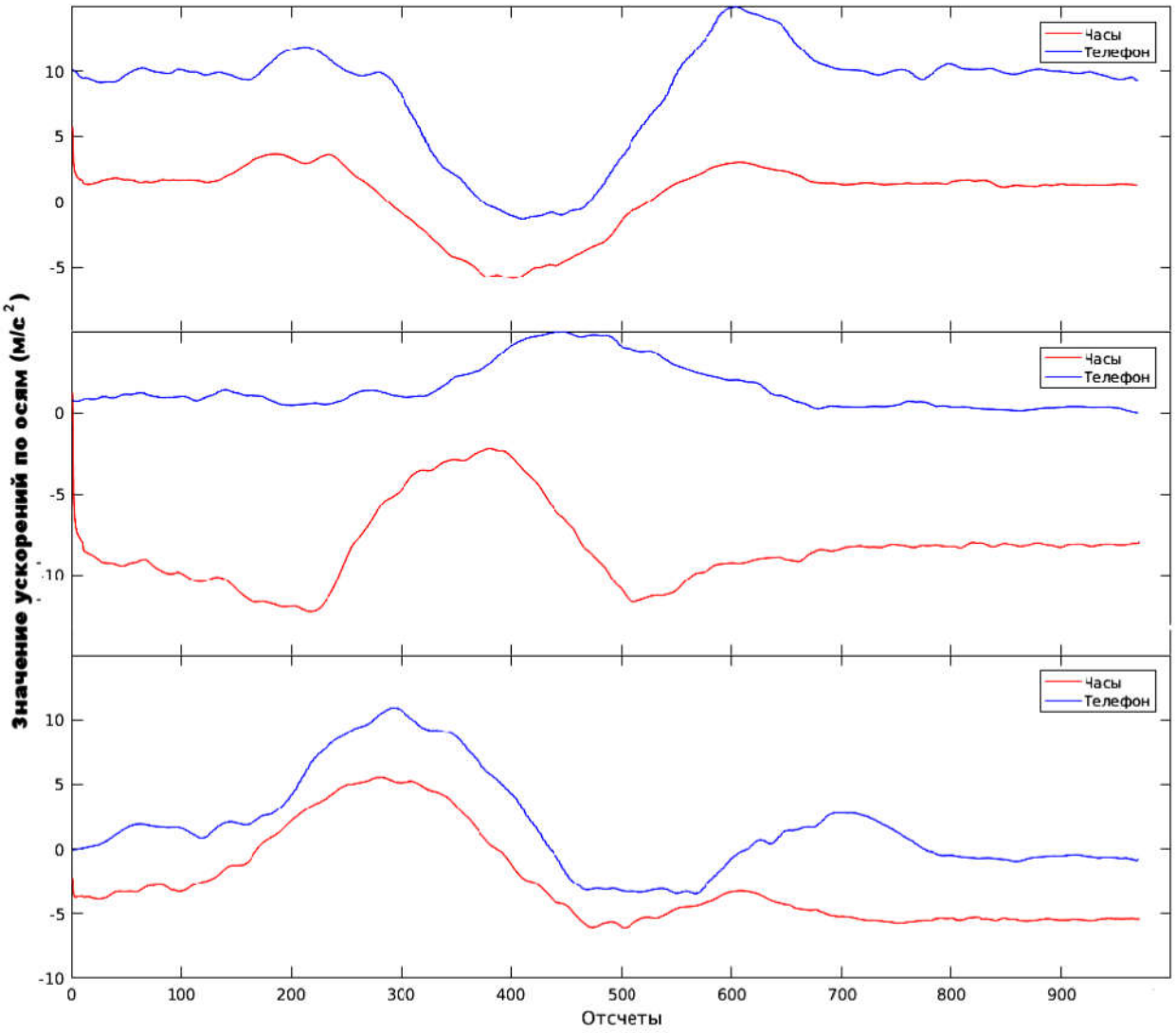


*Рис. 3. Значения ускорений по трем осям при круговом жесте*

Как видно из графиков на рис. 3, показания сильно коррелируют, но, тем не менее, разница достаточно велика. Следовательно, для идеально воспроизводимого жеста $D_1$ будет лежать в некотором интервале $D_{1\min} \le D_1 \le D_{1\max}$, где $D_{1\min}$ будет стремиться к $D_{1\max}$.

Данная методика аутентификации будет иметь следующие ограничения при реализации:

длительность жеста не должна быть слишком большой (до 5 с), если аутентификация предполагает использование вычислительных мощностей исключительно мобильного устройства;

при аутентификации обязательно, чтобы мобильный телефон и умные часы были в одной руке;

в связи с большим разбросом параметров акселерометров у различных производителей, то при замене любого из устройств потребуется повторное формирование эталонных сигналов.

Так как объем данных, требуемый для данной методики аутентификации относительно небольшой (100 – 200 кбайт), и существенно ниже, чем, например, для голосовой аутентификации, то реализация данной методики возможна как с использование мощности только мобильного телефона, так и по клиент-серверной технологии.

Использование запястного устройства совместно с мобильным имеет ряд преимуществ, позволяющих повысить надежность аутентификации. Оба устройства персонифицированы и плотно взаимодействуют друг с другом. Одним из способов защитить данные мобильного устройства при краже – это использовать запястное устройство для разблокировки. Такая функция уже внедрена во многие фитнес-браслеты и получила широкое распространение.

Представленный способ аутентификации будет особенно интересен людям, привыкшим к ношению фитнес браслетов или умных часов.

## СПИСОК ЛИТЕРАТУРЫ:

1. Шакер И.Е. Использование биометрической аутентификации и перспективы ее применения в банковской системе России // Экономика. Налоги. Право. Выпуск № 5. 2016. С. 85–86.
2. Jiayang Liu, Zhen Wang, Lin Zhong Jehan, Wickramasuriya, Venu Vasudevan «uWave: Accelerometer-based personalized gesture recognition and its applications», 2009, http://www.ruf.rice.edu/~mobile/publications/liu09percom.pdf [Электронный ресурс].
3. Jiayang Liu Lin Zhong, Jehan Wickramasuriya, Venu Vasudevan «User evaluation of lightweight user authentication with a single tri-axis accelerometer». MobileHCI, 2009, pp. 1-10.
4. Козлов Ю.Е., Евсеев В.Л. Экспериментальное определение уровня речевого сигнала в показаниях акселерометра мобильных устройств // Вопросы кибербезопасности. 2016. № 5 (18). С. 36 – 42.
5. Гафаров А.Р. Применение алгоритма Fast DTW в задаче распознавания данных с акселерометрического устройства // Информатика: проблемы, методология, технологии. Материалы XVI Международной научно-методической конференции «Технологии обработки и защиты информации. Информационные системы и базы данных», 2016 г. С. 94–100.
6. Пестов Е.А. Распознавание движения мобильного устройства // Международный журнал открытых информационных технологий. 2013. С. 5–10.

## REFERENCES:

1. Shaker I.E. Ispolzovanie biometricheskoi autentifikacii i perspektivi ee primeneniya v bankovskoi sisteme Rossii // Ekonomika.Nalogi.Pravo.Vipusk № 5. .2016. Pp. 85–86.
2. Jiayang Liu, Zhen Wang, Lin Zhong Jehan, Wickramasuriya, VenuVasudevan «uWave: Accelerometer-based personalized gesture recognition and its applications». 2009. http://www.ruf.rice.edu/~mobile/publications/liu09percom.pdf [Online].
3. Jiayang Liu Lin Zhong, Jehan Wickramasuriya, Venu Vasudevan «User evaluation of lightweight user authentication with a single tri-axis accelerometer». MobileHCI, 2009, pp. 1-10.

4. Kozlov Y.E., Evseev V.L. Eksperimentalnoe opredelenie urovnya rechevogo signala v pokazaniyah akselerometra mobilnih ustroistv // Voprosi kiberbezopasnosti. № 5(18). 2016. Pp. 36 – 42.
5. Gafarov A.R. Primenenie algoritma Fast DTW v zadache raspoznavaniya dannih s akselerometricheskogo ustroistva // Informatika: problem, metodologiya, tehnologii. Materiali XVI Mejdunarodnoi nauchno-metodicheskoi konferencii «Tehnologii obrabotki i zaschiti informacii. Informacionnie sistemi i bazi dannih», 2016. Pp. 94–100.
6. Pestov E.A. Raspoznavanie dvizhenija mobil'nogo ustrojstva // International Journal of Open Information Technologies. 2013. Pp. 5–10.