ИНФОКОММУНИКАЦИОННЫЕ ТЕХНОЛОГИИ

INFOCOMMUNICATION TECHNOLOGIES

УДК 004.9

МЕТОДИКА МНОГОМОДАЛЬНОЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ С УЧЕТОМ ОТКЛОНЕНИЙ ЕГО БИОМЕТРИЧЕСКИХ ПАРАМЕТРОВ ОТ НОРМЫ В РАЗЛИЧНЫХ ФУНКЦИОНАЛЬНЫХ СОСТОЯНИЯХ

THE METHOD OF MULTIMODAL USER AUTHENTICATION, TAKING INTO ACCOUNT DEVIATIONS OF ITS BIOMETRIC PARAMETERS FROM THE NORM IN VARIOUS FUNCTIONAL STATES

В.В. Никитин, О.О. Басов
V.V. Nikitin, O.O. Basov

Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский национальный исследовательский университет информационных технологий, механики и оптики (Университет ИТМО)»,
Россия, 197101, г. Санкт-Петербург, Кронверкский пер., 49

Federal state autonomous educational institute of higher education «Saint-Petersburg National Research University of Information Technologies, Mechanics and Optics (ITMO University)», 49 Kronverkskiy pr., Sankt-Peterburg, 197101, Russia

E-mail: nikitin.aktash@mail.ru, oobasov@mail.ru

Аннотация
Представлена методика многомодальной аутентификации пользователя, в основе которой заложено использование биометрических динамических способов, с учетом его взаимодействия по различным коммуникативным каналам с автоматизированной системой. Особенностью предложенной методики является реализация учета девиации значений биометрических признаков пользователя от нормы при отклонении его функционального состояния. В этих целях используется разработанная математическая модель на основе байесовской сети доверия, с использованием которой производится ранжирование и расчет весовых коэффициентов биометрических признаков, их групп, каналов взаимодействия. Непосредственная оценка достоверности многомодальной аутентификации является дополнительным критерием оценки легитимности пользователя, получающего доступ к автоматизированной системе.

Abstract
The article presents the technique of multimodal user authentication, which is based on the use of biometric dynamic methods, taking into account its interaction on various communication channels with an automated system. A feature of the proposed methodology is the implementation of accounting for the deviation of the user's biometric characteristics values from the norm in the event of its functional state variation. For this purpose, authors use the mathematical model developed on the basis of the Bayesian network of trust, which can rank and calculate the weight coefficients of biometric features, their groups, channels of interaction. Evaluation reliability of multimodal authentication is an additional criterion for assessing the legitimacy of a user, gaining access to an automated system. In the conclusion of the article, experimental data on the research of the developed technique and the direction of further research are presented.

Ключевые слова: аутентификация, биометрия, многомодальность, пользователь, автоматизированная система, защита информации.
Keywords: authentication, biometry, multimodal, user, automated system, data protection.

Резкий рост объемов информации, циркулирующей в различных информационных системах, увеличение объемов обрабатываемых данных, в том числе и содержащих конфиденциальные сведения, приводят к участившимся случаям их утечки (разглашения). Таким образом, в условиях глобального информационного противоборства особую актуальность приобретают проблемы обеспечения безопасности и защиты информации – деятельности, направленной на предотвращение утечки защищаемой информации, различных непреднамеренных и несанкционированных воздействий на защищаемую информацию [ГОСТ Р 50922-2006, 2006]. Одним из подходов при этом является реализация некриптографических методов технической защиты информации с применением различных программных и программно-технических средств. При этом некоторыми целевыми функциями защиты информации, направленными на обеспечение ее безопасности, являются: обеспечение конфиденциальности информации, идентификация и аутентификация пользователей, управление доступом к информационным ресурсам, подтверждение достоверности информации (неотказуемости).

Биометрическая аутентификация пользователя автоматизированных систем

Биометрическая аутентификация реализуется посредством анализа ряда признаков, которые характеризуются: всеобщностью, уникальностью, постоянством, измеряемостью и приемлемостью [Ruud Bolle. and etc. 2004; Проскурин, Крутов, Мацкевич, 2009]. Применение биометрической аутентификации в автоматизированных системах позволит повысить защищенность информации, так как процесс установления истинности пользователя, имеющего доступ к системе, будет возможно осуществляться постоянно. Применение динамических способов биометрической аутентификации позволяет решить сразу две проблемы: «целостности личности» (неизменность субъекта во время сеанса работы с автоматизированной системой, устраняется угроза «подмены пользователя») и «невозможности отказа от авторства» (пользователь несет полную ответственность за обрабатываемую информацию) [Ruud Bolle. and etc. 2004; Проскурин, Крутов, Мацкевич, 2009; Jain, Arun A. Ross, Nandakumar, 2011].

Однако, любой биометрический признак непрерывно связан с текущим (физиологическим, эмоциональным, психофизическим) состоянием человека [Ruud Bolle. and etc. 2004]. Всегда имеют место различные внутренние (усталость, стресс и т.п.) и внешние факторы (параметры окружающей обстановки – температура, влажность и т.д.), оказывающие влияние на получаемые значения биометрических признаков пользователя и результат аутентификации в целом.

Достоверность аутентификации при девиации биометрических признаков может быть повышена путем учета многомодального характера взаимодействия пользователя и автоматизированной системы [Басов, Карпов, Саитов, 2015]. Многомодальное взаимодействие реализуется за счет использования средств передачи информации по различным каналам коммуникации – текстовому (клавиатурный ввод, рукописный почерк, работа с указателем типа «мышь») и акустическому (голос пользователя).

В работе [Никитин, Гунченко, 2017] приведено описание математической модели многомодальной системы аутентификации пользователя на основе байесовской сети доверия [Korb, Nicholson, 2004]. Разработанная модель позволяет учитывать множество различных биометрических признаков аутентификации, объединяемых на основе методов многомодального объединения [Басов, Карпов, Саитов, 2015], а также решает задачу вероятностного прогнозирования достоверности аутентификации пользователя на основе данных о его биометрических признаках в среде моделирования GeNle [GeNIe 2.0].

Оценка условных вероятностей байесовской сети доверия данной модели при дефиците информации о взаимодействии между ее узлами реализуется посредством использования нечисловой экспертной, неточной и неполной информации [Hovanov, Yudaeva, Kolesov, 2014; Barmish, Lagoa, 1997], определяющей значимость соответствующих экспертных мнений с применением специализированного программного обеспечения APIS .

Процедура ранжирования при многомодальной аутентификации

Разработанная модель многомодальной аутентификации пользователя также позволяет установить, какие из признаков и их групп, а также коммуникативных каналов являются наиболее важными по степени влияния на решение о достоверности аутентификации, и ранжировать их по данному критерию.

Для учета результатов ранжирования при принятии решения о допуске пользователя к работе с автоматизированной системой посредством анализа вклада используемых биометрических признаков, их групп и различных каналов взаимодействия в достоверность аутентификации, ранжированным биометрическим признакам поставлены в соответствие весовые коэффициенты, полученные на основе формулы Фишберна [Баранов, 2013]:

$$\alpha_i = \frac{2(n-i+1)}{n(n+1)}, \quad (1)$$

где n – общее число ранжируемых признаков, i – порядковый номер ранжируемого признака. В данном случае, метод ранжирования основан на том, что изменение весовых коэффициентов признаков подчиняется убывающей арифметической прогрессии, при этом первый признак (i =1) имеет самое значительное влияние на достоверность аутентификации пользователя, являясь наиболее важным и имеющим наибольший весовой коэффициент.

В процессе работы были получены результаты ранжирования по трем категориям – непосредственно самих используемых при многомодальной аутентификации биометрических признаков, их групп, а также каналов взаимодействия пользователя и автоматизированной системы. Одновременно с этим были получены и зависимости достоверности аутентификации пользователя от каждой из указанной категории.

Обучение системы многомодальной аутентификации пользователя

Непосредственное функционирование системы многомодальной аутентификации предваряет этап ее обучения, заключающийся в оценке границ [Вентцель, Овчаров, 2000] $I_x^{\text{Н}}$ (2) и $I_x^{\text{В}}$ (3) для каждого биометрического признака каждого пользователя, характеризующих его в различных функциональных (физиологических, эмоциональных и психофизиологических) состояниях:

$$I_x^{\text{Н}} = \widetilde{m}_i - t_\beta \sqrt{\frac{\widetilde{D}}{n}}, \quad (2)$$

$$I_x^{\text{В}} = \widetilde{m}_i + t_\beta \sqrt{\frac{\widetilde{D}}{n}}, \quad (3)$$

где $\widetilde{m}$ и $\widetilde{D}$ – оценки математического ожидания и дисперсии биометрического параметра пользователя, t_β – табличная величина, зависящая от доверительной вероятности β, определяющая для нормального закона число СКО, которое нужно отложить вправо и влево от центра рассеивания для того, чтобы вероятность попадания в полученный участок была равна β [Jaynes, 1967; Brunk, Gref, 1964].

При обучении системы многомодальной аутентификации пользователя необходимо учитывать биологические свойства индивида, которые определяются его гено- и

фенотипом. Доказано [Milsum, 1968], что реакция биологических систем на входной сигнал зависит как от природы (сложности) системы, так и от формы входного сигнала. В зависимости от вида воздействия (импульсное, скачкообразное, линейно возрастающее) изменяется и выходной сигнал.

В ходе исследования были проанализированы особенности психомоторики пользователей при взаимодействии с устройствами ввода данных автоматизированных систем, для чего были использовано соответствующее программное обеспечение [Никитин и др. Программа определения …, 2014; Никитин и др. Программа формирования …, 2014]. Также были проанализированы изменения биометрических параметров пользователя под воздействием внутренних и внешних факторов с целью установления влияния на результат его аутентификации (табл. 1).

Выбор данных факторов был обусловлен условиями повседневной деятельности пользователей с учетом специфики выполняемых задач подразделениями специальной связи и информатизации территориальных органов безопасности. Проведенный в первой главе анализ работоспособности пользователя, показал ее связь с физическими, умственными, психическими и психологическими особенностями личности, а также квалификации и состояния здоровья сотрудника.

Таблица 1
Table 1

Воздействия на пользователя в процессе деятельности
Inpact on the user in the process of activity

Внутренние (психофизиологические) факторы	Внешние (в пределах организации) Воздействия	Внешние (за пределами организации) воздействия
Информационная нагрузка и объем выполняемых задач	Межличностные конфликты в организации	Влияние внешних угроз, в том числе и угроз собственной безопасности
Информационная неопределенность	Полифокусность технической деятельности	Нестабильность социальной динамики
Ответственность и мотивированность сотрудника	Деятельностный фактор	Сложность политической обстановки в субъекте и государстве в целом
Дефицит отводимого на выполнение задач времени	Факторы внешней среды, в том числе и экологические и эргономические показатели	Нестабильность экономической обстановки
Внутриличностные конфликты	Внутриорганизационный и объектовый режим	Контролирующие и инспекционные организации
Состояние здоровья пользователя	Объем возникающих неспецифических функций и задач	Конфликты в семье и личной жизни пользователя

В процессе работы была создана база данных, содержащая записи фрагментов текста и положений указателя мыши, соответствующих различным состояниям пользователей обоих полов. База данных содержит 31 таблицу значений моментов времени нажатия и отпускания кнопок на клавиатуре и «мыши», коды данных кнопок, а также координаты положения указателя «мыши» на экране, полученные для различных интервалов времени суток. Объем базы данных составил 1,08 Мбайт.

В процессе обучения в базу данных многомодальной системы аутентификации пользователя производится запись множеств доверительных интервалов биометрических параметров пользователя для каждого из возможных его состояний:

$$S_{id}^{\text{ЭТ}} = \left| I_{xt_1}, I_{xt_2}, \ldots I_{xt_{n1}}, I_{cm_1}, I_{cm_2}, \ldots I_{cm_{s1}}, I_{vk_1}, I_{vk_2}, \ldots I_{vk_{j1}}, I_{zw_1}, I_{zw_2}, \ldots I_{zw_{l1}} \right|, \quad (4)$$

где $I_{xt_{n1}}$ – массив доверительных интервалов для каждого биометрического признака пользователя по клавиатурному почерку, $I_{cm_{s1}}$ – по работе с указателем, $I_{vk_{j1}}$ – по голосу, $I_{zw_{l1}}$ – по рукописному вводу (работа со стилусом).

Обучение системы многомодальной аутентификации пользователя целесообразно проводить в период развертывания и установки системы в организации, стажировки и обучения работы сотрудников с ней, а также непосредственно рабочих местах в течении дня с привлечением специалистов для оценки состояния пользователя. Роль специалиста заключается в комплексной экспертной оценки состояния психофизиологического и эмоционального состояния работающего пользователя с целью необходимой корректировки формирования шаблонов.

Методика многомодальной аутентификации пользователя автоматизированной системы

С учетом определенных выше процедур методику многомодальной аутентификации пользователя автоматизированной системы можно представить в виде реализация следующих шагов (рис. 1):

Шаг 1. Определение исходных данных, к которым относятся:

1) комплектация автоматизированной системы, определяющая количество возможных для работы пользователя устройств ввода информации – N_{mod};

2) база электронных ключей и паролей пользователей для получения доступа к автоматизированной системе с использованием штатных сертифицированных аппаратно-программных модулей доверенной загрузки;

3) внутренние параметры алгоритмов выделения биометрических признаков;

4) значения весовых коэффициентов биометрических параметров – α_i;

5) значение порога принятия решения при сравнении биометрических параметров – $\Delta^{\text{ПОР}}$;

6) значение достоверности аутентификации для принятия решения о легитимности пользователя $p_{\text{ПОР}}^{\text{АУТ}}$.

Шаг 2. Получение доступа к автоматизированной системе пользователем посредством использования штатных аппаратно-программных модулей доверенной загрузки, согласно реализуемой политики безопасности [Проскурин, Крутов, Мацкевич, 2009].

Например, при интеграции предполагаемого алгоритма в аппаратно-программные модули доверенной загрузки на данном шаге пользователь осуществляет использование электронного ключа и ввод имеющегося у него логина и пароля. В результате из базы данных биометрических шаблонов зарегистрированных пользователей в соответствии с введенными идентификаторами происходит выбор шаблона пользователя $S_{id}^{\text{ЭТ}}$, полученного на этапе обучения системы многомодальной аутентификации (4).

Шаг 3. Анализ информации, поступающей по различным каналам взаимодействия, происходит постоянно, в течении того времени, пока пользователь работает с автоматизированной системой, причем организуется параллельно по различным модальностям.

Шаг 4. Получение биометрических параметров пользователя по n-й модальности реализуется посредством считывания поступающих сигналов с соответствующих устройств ввода автоматизированной системы. В случае, когда пользователь не осуществляет взаимодействие с ней ни по одной из модальностей, система аутентификации находится в режиме ожидания.

Шаг 5. Предобработка сигналов по каждой модальности реализована за счет известных и описанных в научной литературе алгоритмов фильтрации, шумоочистки и т. д.

Шаг 6. Выделение параметров аутентификации пользователя по каждой модальности осуществляется посредством известных алгоритмов, наиболее полно изложенных в [Ruud Bolle. and etc. 2004; Jain, Arun A. Ross, Nandakumar, 2011], а также с использованием разработанных при участии авторов специализированных программных средств [Никитин и др. Программа определения …, 2014; Никитин и др. Программа формирования …, 2014].

Шаг 7. Отклонение состояния пользователя по каждой модальности определяется по принадлежности полученной оценки математического ожидания $\widetilde{m}_x$ биометрического признака пользователя интервалу $I = (I_x^{\text{Н}}, I_x^{\text{В}})$, границы которого определяются согласно выражениям 4-5, и имеющемся в шаблоне пользователя $S_{id}^{\text{ЭТ}}$ (4), выбранном на шаге 2.

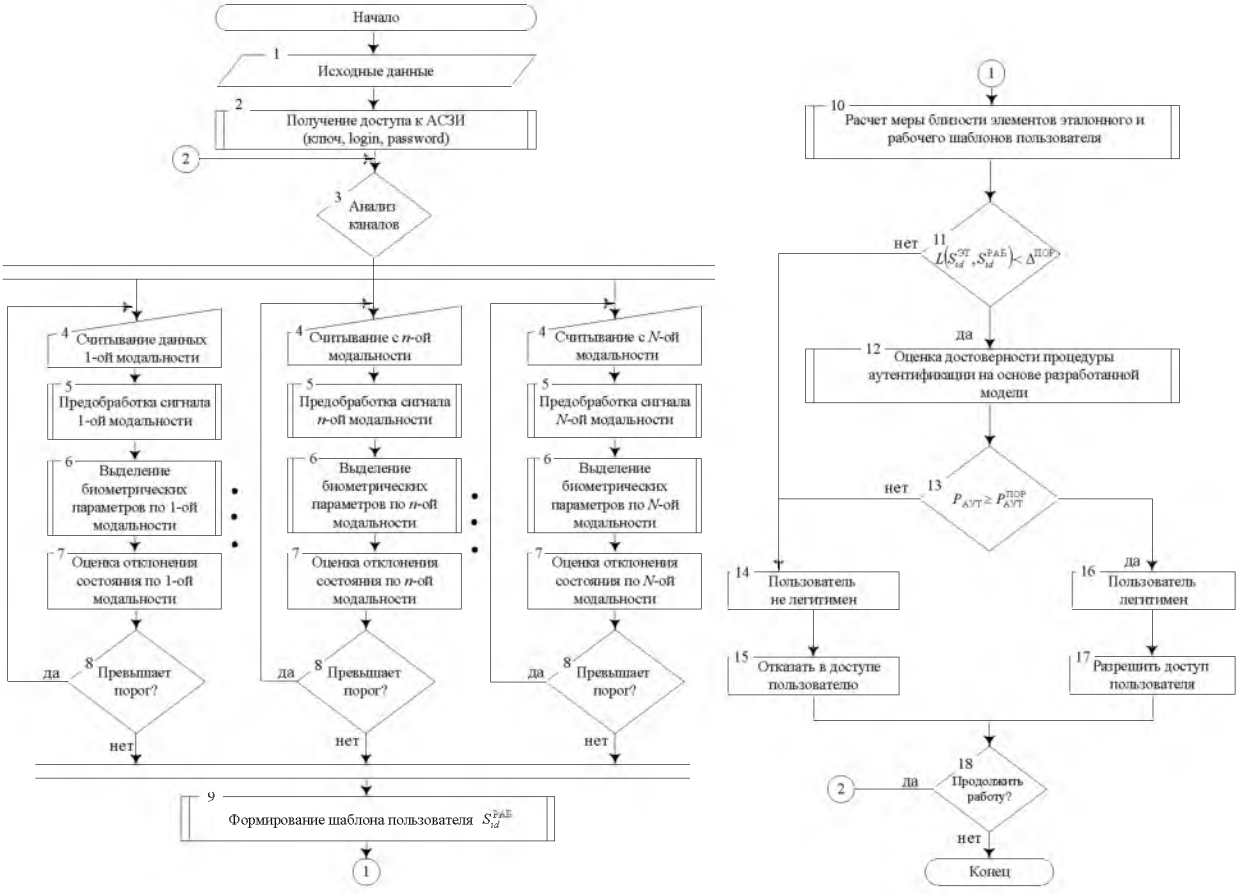

Рис. 1. Методика многомодальной аутентификации пользователя
Fig. 1. User multimodal authentication method

Шаг 8. В случае, когда вычисленное значение $\widetilde{m}_x$ находится в пределах интервала I_x, принимается решение о том, что данный параметр может принадлежать пользователю, находящемуся, возможно, в состоянии Ψ_k. В противном случае – происходит возврат к шагу 4.

Шаг 9. Формирование рабочего шаблона пользователя происходит согласно на основе получаемых оценок $\widetilde{m}_x$ и $\widetilde{D}_x$ биометрических признаков по всем используемым модальностям:

$$S_{id}^{\text{РАБ}} = \left\langle \widetilde{I}_{xt_1}, \widetilde{I}_{xt_2}, \ldots \widetilde{I}_{xt_{n1}}, \widetilde{I}_{cm_1}, \widetilde{I}_{cm_2}, \ldots \widetilde{I}_{cm_{s1}}, \widetilde{I}_{vk_1}, \widetilde{I}_{vk_2}, \ldots \widetilde{I}_{vk_{j1}}, \widetilde{I}_{zw_1}, \widetilde{I}_{zw_2}, \ldots \widetilde{I}_{zw_{l1}} \right\rangle, \quad (5)$$

где в общем случае $\widetilde{I}_x = (\widetilde{I}_x^{\text{Н}}, \widetilde{I}_x^{\text{В}})$.

Шаг 10. Мера близости элементов эталонного и рабочего шаблонов определяется на основе следующего выражения:

$$L(S_{id}^{\text{ЭТ}}, S_{id}^{\text{РАБ}}) = \sum_{x=1}^{T} \alpha_x d_x^2 (S_{id}^{\text{ЭТ}}, S_{id}^{\text{РАБ}}) \quad (6)$$

где T – число биометрических признаков, используемых системой многомодальной аутентификации пользователя автоматизированной системы, в общем случае равное $T = n_1 + s_1 + j_1 + l_1$; α_x – весовые коэффициенты ранжированных биометрических признаков, $d_x^2(S_{id}^{\text{ЭТ}}, S_{id}^{\text{РАБ}})$ – мера близости элементов шаблонов на основе эвклидовой метрики:

$$d_x^2\left(S_{id}^{\text{ЭТ}}, S_{id}^{\text{РАБ}}\right) = \left(\widetilde{m}_x - m_x\right)^2 = \left(\frac{\widetilde{I}_x^{\text{В}} + \widetilde{I}_x^{\text{Н}}}{2} - \frac{I_x^{\text{В}} + I_x^{\text{Н}}}{2}\right)^2. \quad (7)$$

В случае, когда биометрический параметр не используется при работе пользователя с автоматизированной системой (исходя из используемых пользователем каналов взаимодействия с ней и особенностей работы с устройствами ввода информации), соответствующая ему мера близости (7) не рассчитывается.

Шаг 11. На основе критерия Неймана-Пирсона принимается решение

$$s = \begin{cases} s_2, \text{ если } L(S_{id}^{\text{ЭТ}}, S_{id}^{\text{РАБ}}) \geq \Delta^{\text{ПОР}}, \\ s_1, \text{ если } L(S_{id}^{\text{ЭТ}}, S_{id}^{\text{РАБ}}) < \Delta^{\text{ПОР}}, \end{cases} \quad (8)$$

о нелегитимности пользователя (s_2), переходе к шагу 14 и последующем отказе ему в доступе на шаге 15, или о его условной «легитимности» (s_1) и переходе к шагу 12.

Шаг 12. На основе разработанной и подробно описанной в [Никитин, Гунченко, 2017] математической модели системы многомодальной аутентификации пользователя реализуется оценка достоверности $p_{\text{АУТ}}$ многомодальной аутентификации.

Шаг 13. На основе критерия Неймана-Пирсона принимается решение

$$s = \begin{cases} s_1, \text{ если } p_{\text{АУТ}} \geq p_{\text{АУТ}}^{\text{ПОР}}, \\ s_2, \text{ если } p_{\text{АУТ}} < p_{\text{АУТ}}^{\text{ПОР}}, \end{cases} \quad (9)$$

о нелегитимности пользователя (s_2), переходе к шагу 14 и последующем отказе ему в доступе на шаге 15, или о его легитимности (s_1), переходе к шагу 16 и разрешении ему доступа на шаге 17.

Шаг 18. Система многомодальной аутентификации пользователя функционирует на протяжении всего времени его работы, в случае завершения сеанса доступа пользователя к автоматизированной системе, система многомодальной аутентификации также завершает свою работу.

Таким образом, разработанный методика многомодальной аутентификации позволяет повысить достоверность данной процедуры по сравнению с процедурой классического доступа к автоматизированной системе посредством использования штатных аппаратно-программных модулей доверенной загрузки (шаг 2). Такое повышение реализуется путем учета:

– влияния функционального состояния пользователя на значения его биометрических параметров (шаги 3-8);

– различного влияния биометрических параметров пользователя на достоверность его аутентификации (9-11);

– прогнозируемого значения правильной аутентификации при принятии решения о доступе пользователя к работе с автоматизированной системой (шаги 12–13).

Экспериментальная проверка разработанной методики

Проверка разработанной методики многомодальной аутентификации пользователя была осуществлена с использованием графического планшета (Genius EasyPen i405/i405X) и электронного пера ввода, посредством анализа текстового канала взаимодействия [Никитин и др. Программа определения …, 2014; Никитин и др. Программа формирования …, 2014] на основе запатентованного способа [Никитин, Басов и др. Патент № 2546559], а также с использованием стандартных автоматизированных рабочих мест операторов компании OngNet. Для получения биометрических признаков рукописного ввода пользователя использовались характеристики чувствительности планшета к давлению кончика пера на рабочую (1024 уровня), время отклика (100 точек в секунду), размер рабочей (140x102 мм), клавиатурного почерка – стандартные параметры клавиатурного ввода, изложенные при описании математической модели [Никитин, Гунченко, 2017].

Результаты оценки достоверности аутентификации пользователя при многомодальной аутентификации на основе разработанной модели и с учетом предложенной методики представлены на рис. 2.

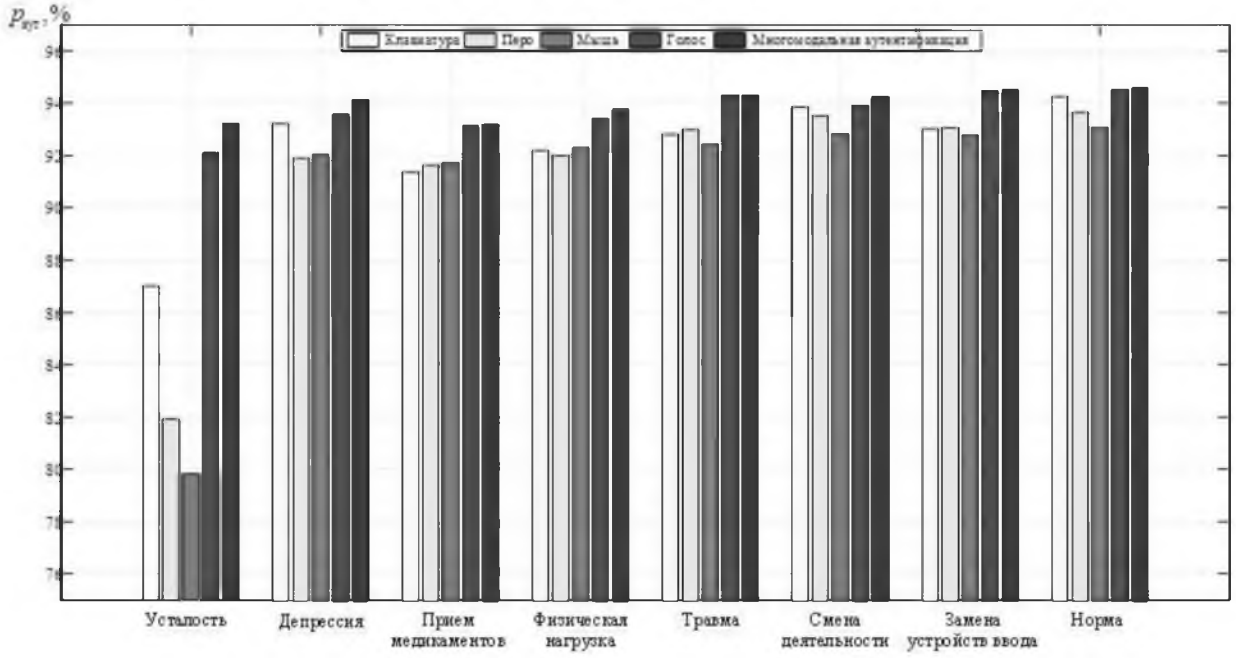

Рис. 2. Сравнение результатов разработанной методики многомодальной аутентификации с существующими решениями

Fig. 2. Comparison results of the developed multimodal authentication methodology with existing solutions

Заметно, что достоверность многомодальной аутентификации превышает имеющиеся решения в данной области на 2-6% при нормальном состоянии пользователя, а в случае отклонения его функционального состояния от нормы – превосходит существующие решения на 2-14%. Непосредственно система многомодальной аутентификации пользователя, разработанная с учетом предложенной методики, обеспечила достоверность аутентификации 97,75%.

Для определения вероятности ошибки первого рода осуществлялся анализ процесса аутентификации испытуемой группы пользователей (операторов) с использованием разработанной методики многомодальной аутентификации, в предположении, что за это время все сотрудники на рабочих местах хотя бы 2 раза в

течение рабочего дня осуществляют процедуру аутентификации. В таком случае вероятность ошибки первого рода будет определена как доля разрешений на работу, при которых открытие доступа пользователю вынужденно осуществлялось в ручном режиме с привлечением администратора безопасности, от общего количества пользователей.

Общее количество сотрудников, участвующих в экспериментальном исследовании разработанной методики составило 184 человека, с доверительной вероятностью 95 % ошибка первого рода по «правилу трех» [Румшиский, 1971] оказалась равна:

$$p' \approx \frac{3}{2N_1} = \frac{3}{2 \cdot 184} = 0{,}0081 . \quad (10)$$

Для определения вероятности ошибки второго рода было смоделировано 1200 попыток аутентификации нелегитимного пользователя с использованием имитации рукописной подписи и клавиатурного почерка, а также привлечения записей голосов незарегистрированных лиц. В этом случае с доверительной вероятностью 95 % ошибка второго рода оказалась равна:

$$p'' \approx \frac{3}{N_2} = \frac{3}{1200} = 0{,}0025 . \quad (11)$$

Таким образом, разработанная система методика многомодальной аутентификации пользователя обеспечивает достоверность аутентификации 97,75% с расчетной величиной ошибки первого рода 0,81% и второго рода – 0,25%.

Заключение

Направлениями дальнейших исследований являются модификация разработанного научно-методического инструментария многомодальной аутентификации пользователя на случай использования визуального канала его взаимодействия с автоматизированной системой. Особое внимание стоит уделить поиску оптимального сочетания биометрических параметров пользователя для обеспечения наилучших показателей системы его аутентификации. В связи с бурным развитием информационных технологий в будущем потребуется учет изменяющихся требований пользователей [Струев и др. 2016] автоматизированных систем при реализации предложенной методики многомодальной аутентификации.

Список литературы
References

1. ГОСТ Р 50922-2006. Защита информации. Основные термины и определения. Госстандарт, 2006, 18.

GOST R 50922-2006. Data protection. Basic terms and definitions. 2006, 18. (in Russian).

2. Ruud Bolle. and etc. 2004. Guide to Biometrics Guide to Biometrics, Springer Science & Business Media, 364.

3. Проскурин В.Г., Крутов С.В., Мацкевич И.В. 2009. Программно-аппаратные средства обеспечения информационной безопасности. Защита в операционных системах: уч. пособие для вузов. Москва, Радио и связь, 168.

Proskurin V.G., Krutov S.V., Matskevich I.V. 2009. Programmno-apparatnye sredstva obespecheniya informatsionnoy bezopasnosti. Zashchita v operatsionnykh sistemakh: uch. posobie dlya vuzov. [Software and hardware for information security. Protection in operating systems: manual for high schools] Moskva, Radio i svyaz', 168 (in Russia).

4. Jain A., Arun A. Ross, Nandakumar K. 2011. Introduction to Biometrics, Springer US., 212.

5. Басов О.О., Карпов А.А., Саитов И.А. 2015. Методологические основы синтеза полимодальных инфокоммуникационных систем государственного управления: монография. Орёл, Академия ФСО России, 270.

Basov O.O., Karpov A.A., Saitov I.A. 2015. Metodologicheskie osnovy sinteza polimodal'nykh infokommunikatsionnykh sistem gosudarstvennogo upravleniya: monografiya [Methodological

foundations for the synthesis of multimodal infocommunication systems of public administration: monograph] Orel, Akademiya FSO Rossii, 270 (in Russia).

6. Никитин В.В., Гунченко И.Ю. 2017. Модель системы многомодальной аутентификации пользователя на основе байесовской сети доверия. Экономика и менеджмент систем управления. Воронеж, 2.2(24), 276-282.

Nikitin V.V., Gunchenko Yu.I. 2017. Model' sistemy mnogomodal'noy autentifikatsii pol'zovatelya na osnove bayesovskoy seti doveriya [Model of multimodal user authentication system based on Bayesian network of trust] Ekonomika i menedzhment sistem upravleniya. Voronezh, 2.2(24), 276-282. (in Russia).

7. Korb K.B., Nicholson A.E. 2004. Bayesian Artificial Intelligence. New York, Chapman and Hall/CRC, 364.

8. GeNIe 2.0 Available at: https://www.bayesfusion.com.

9. Hovanov N., Yudaeva M., Kolesov D. 2014. Imprecise Event Trees Framework for Evaluation of Russian Economy Perspectives. 7th International Conference of the ERCIM WG on Computational and Methodological Statistics University of Pisa, Italy.

10. Barmish B., Lagoa C. 1997. The uniform distribution: a rigorous justification for its use in robustness analysis. Mathematical Control, Signals, Systems. 10: 203-222.

11. Баранов Ю.Г. 2013. Методы принятия управленческих решений. Псков, ПГУ, 176.

Baranov Yu.G. 2013. Metody prinyatiya upravlencheskikh resheniy [Methods of making managerial decisions]. Pskov, PGU, 176. (in Russia).

12. Вентцель Е.С., Овчаров Л.А. 2000. Теория вероятностей и ее инженерные приложения. Учеб. пособие для вузов. М., Высш. шк., 480.

Venttsel' E.S., Ovcharov L.A. 2000. Teoriya veroyatnostey i ee inzhenernye prilozheniya [Theory of probability and its engineering applications.]. Ucheb. posobie dlya vuzov. M., Vyssh. shk., 480 (in Russia).

13. Jaynes E. 1967. Foundations of Probability Theory and Statistical Mechanics. N.Y., Springer.

14. Brunk H., Gref L. 1964. A geometrical approach to probability. Mathematics Magazine. 37(5): 287-296.

15. Milsum D. 1968. Biological control systems analysis, McGraw-Hill, 466.

16. Никитин В.В., Басов О.О., Носов М.В., Гуляйкин Д.А. Программа определения параметров текстовых модальностей. Свидетельство о государственной регистрации программы для ЭВМ № 2014613478 от 27.03.2014.

Nikitin V.V., Basov O.O., Nosov M.V., Gulyaykin D.A. Program for determining the parameters of text modalities. Certificate of state registration of the computer program № 2014613478 of 27.03.2014 (in Russia).

17. Никитин В.В., Басов О.О., Носов М.В., Гуляйкин Д.А. Программа формирования характеристик случайного джиттера сигналов текстовых и речевого каналов коммуникации. Свидетельство о государственной регистрации программы для ЭВМ № 2014615750 от 02.06.2014 (in Russia).

Nikitin V.V., Basov O.O., Nosov M.V., Gulyaykin D.A. Program for the formation of characteristics of random jitter signals of text and voice communication channels. Certificate of state registration of the computer program № 2014615750 of 02.06.2014 (in Russia).

18. Никитин В.В., Басов О.О. и др. Патент № 2546559 РФ, МПК G06K 9/62. Способ биометрической аутентификации пользователя, опубл. 10.06.2015, бюл. № 16.

Nikitin V.V., Basov O.O. and etc. Patent No. 2546559 of the Russian Federation, IPC G06K 9/62. Method of Biometric User Authentication, publ. 06/10/2015, Bul. №. 16 (in Russia).

19. Румшиский Л.З. 1971. Математическая обработка результатов эксперимента. Наука, 192.

Rumshiskiy L.Z. 1971. Matematicheskaya obrabotka rezul'tatov eksperimenta [Mathematical treatment of experimental results] Nauka, 192 (in Russia).

20. Струев Д.А., Бондарева Н.В., Будков В.Ю., Басов О.О., Ронжин А.Л. 2016. Концептуальная модель многомодального интерфейса абонентского терминала. Научные ведомости БелГУ Сер. Экономика, Информатика. 23(244): 156-165.

Struev D.A., Bondareva N.V., Budkov V.Yu., Basov O.O., Ronzhin A.L. 2016. Kontseptual'naya model' mnogomodal'nogo interfeysa abonentskogo terminala [A conceptual model multimodal user interface of the subscriber terminal] Belgorod State University Scientific Bulletin (Economics, Information technologies), 23(244): 156-165. (in Russia).