УДК 004.056.53 **DOI: 10.20998/2411-0558.2017.21.14**

И.Ю. ГРИШИН, д-р техн. наук, проф., КубГТУ, Краснодар,
Р.Р. ТИМИРГАЛЕЕВА, д-р экон. наук, проф., КубГТУ, Краснодар,
М.В. МИРОНОВ, асп., КубГТУ, Краснодар

АНАЛИЗ ЭФФЕКТИВНОСТИ МОДЕЛЕЙ АУТЕНТИФИКАЦИИ ПОЛЬЗОВАТЕЛЯ НА ОСНОВЕ КЛАВИАТУРНОГО ПОЧЕРКА

Задачей исследования явилась проверка работоспособности программного прототипа модели, а также исследование его функциональных возможностей. Осуществлена оценка правильности работы программного прототипа модели на каждом из этапов: регистрация нового пользователя в системе, формирование на основе статистических данных эталонного профиля пользователя, проведение процедур идентификации и аутентификации пользователя с учётом установленных администратором фильтров, просмотр результата авторизации пользователя. Для проведения исследований разработан программный комплекс, позволяющий провести необходимый перечень экспериментов, а также осуществить статистическую обработку результатов, оценить значения ошибок первого и второго рода при аутентификации. Ил.: 5. Библиогр.: 13 назв.

Ключевые слова: модель аутентификации пользователя; ошибки первого и второго рода; клавиатурный почерк.

Постановка проблемы. Основу любой информационной системы предприятия составляют компьютерные комплексы, представляющие собой серверы и автоматизированные рабочие места пользователей, предназначенные для обработки информации с целью реализации ключевых бизнес-процессов организации. При работе пользователя на компьютере фиксируется различная информация, связанная с его деятельностью. Эта информация может быть отнесена к критической или чувствительной, несанкционированное раскрытие, модификация или утрата которой может привести к ощутимому убытку или ущербу предприятия и даже государства. Такая информация относится к различным видам информации ограниченного доступа и должна защищаться в соответствии с требованиями действующего в стране законодательства.

Для защиты от несанкционированного доступа к информации ограниченного доступа, в соответствии с требованиями регуляторов в области информационной безопасности, используется процедура аутентификации, от качества и стойкости которой будет зависеть эффективность защиты компьютерной системы. В настоящее время существует множество систем аутентификации, в основе которых лежат самые разнообразные методы: от простой двухфакторной

аутентификации "логин-пароль" до многофакторной аутентификации с применением биометрических методов распознавания. Использование биометрической аутентификации позволяет привязать пароль к субъекту, тем самым делая процедуру аутентификации более эффективной. Основными критериями качества процедуры аутентификации являются её стойкость и надёжность при идентификации субъекта доступа. Поэтому в настоящее время актуальны исследования, связанные с разработкой новых методов аутентификации и повышением качества существующих.

Анализ литературы. Проблемам разработки и исследованиям систем аутентификации посвящены работы отечественных и зарубежных учёных [1 – 4]. В их работах затрагиваются вопросы, связанные с уровнями строгости аутентификации, методами динамической и статической биометрической аутентификации, способами повышения надёжности и стойкости процесса аутентификации в различных системах.

Биометрическая аутентификация личности относится к технологиям, используемым для контроля физических или поведенческих характеристик человека, которые предлагают радикальную альтернативу традиционным методам аутентификации. Поскольку биометрические методы представляют ряд ограничений с точки зрения точности, универсальности, своеобразия и приемлемости, рассматриваемые методы привлекли повышенное внимание исследователей с целью улучшения способности систем для обработки низкокачественных и неполных данных, обеспечения масштабируемости для управления огромными базами данных пользователей, обеспечения совместимости и защиты конфиденциальности пользователей от атак. В работе [2] осуществлён анализ различных методов использования информации, применяемой в биометрической области. Приводится обзор нескольких систем и архитектур, связанных с комплексным использованием биометрических систем, как унимодальных так и мультимодальных, их классификация в соответствии с указанным контекстом. Здесь также обращено внимание на проблему оценки биометрической системы, обсуждены основные подходы к анализу показателей эффективности, предложены некоторые перспективные направления исследований.

В работе [5] рассмотрен новый подход к проблеме биометрической аутентификации, состоящий в применении аппарата нечёткого распознавания образов. Показано, что данный метод позволяет снизить размер базы данных, используемой для аутентификации, однако вычислительная трудоёмкость метода является достаточно высокой, что

не позволяет его применить в низкопроизводительных компьютерных системах.

Ряд работ посвящён проблеме аутентификации пользователей в мобильных устройствах, смарт-устройствах [6, 7], особенностью которых является достаточно низкая вычислительная производительность, что сильно ограничивает возможность использования традиционных подходов решения рассматриваемой задачи.

В работе [8] в качестве идентифицируемого признака используется радужная оболочка глаз. Такой метод аутентификации требует достаточно большой базы исходных изображений для каждого пользователя.

При этом следует отметить, что в рассмотренных работах авторы не уделяли должного внимания исследованию метрик определения аффинности и их влиянию на качество аутентификации пользователей в биометрических системах [9, 10].

Цель статьи состоит в исследовании качества процедуры аутентификации с использованием методов поведенческой биометрии за счёт оценки влияния метрики определения аффинности признаков на точность классификации.

Материалы и методы. При проведении экспериментальных исследований и тестирования разработанного программного комплекса биометрической аутентификации пользователя в компьютерной системе на основе клавиатурного почерка применялось следующее аппаратное и программное обеспечение.

Аппаратное обеспечение: компьютер Intel(R) Core(TM) i7 CPU; процессор i7-2670-QM@ 2.2 ГГц; оперативная память 6 ГБ.

Программное обеспечение: операционная система Windows7, домашняя базовая SP1; Microsoft Visual Studio .Net 2010.

При взаимодействии пользователей с программой использованы следующие элементы управления (ЭУ): стандартные ЭУ окном Windows; кнопки различных размеров и видов; выпадающие списки; поля ввода и вывода цифровых данных.

Для взаимодействия пользователя с ЭУ применяется манипулятор типа "мышь", touchpad, сенсор или др. Также возможно использование для этой цели клавиатуры ЭВМ.

Программный комплекс является 32-разрядным приложением, работающим под управлением ОС WindowsXP/7/8/10. Программа имеет оконный интерфейс. Работа пользователя с ней строится на принципах, принятых в ОС Windows. Программа написана на языке VisualC# 2010 среды разработки Visual Studio, Microsoft .Net, Framework 4.0.

Оценка эффективности модели аутентификации пользователя на основе клавиатурного почерка. Задачами первого эксперимента

является проверка работоспособности программного прототипа модели, исследование его функциональных возможностей и оценка показателя эффективности. Для этого необходимо оценить правильность и адекватность работы программного прототипа модели на следующих этапах [11, 12]:

1) регистрация нового пользователя в системе;

2) формирование на основе статистических данных эталонного профиля пользователя;

3) проведение процедур идентификации и аутентификации пользователя с учётом установленных администратором фильтров;

4) просмотр результата авторизации пользователя.

Результаты первого этапа – регистрации пользователя.

В процессе регистрации пользователя в системе пользователю необходимо ввести свои аутентификационные данные, состоящие из логина и пароля, а также заполнить следующие поля: Ф.И.О, опыт работы, сфера деятельности, электронная почта.

Ожидаемыми результатами данного этапа после прохождения процедуры регистрации будет добавление данных пользователя в анкету и генерирование текста для составления биометрического профиля пользователя на основе парольной фразы.

Следующий этап – формирование на основе статистических данных эталонного профиля пользователя (рис. 1).

В процессе формирования профиля пользователя вводится текст, сгенерированный на основе парольной фразы и осуществляется переход к следующему этапу (кнопка "далее").

Ожидаемым результатом данного шага после процедуры регистрации, формирования эталонного профиля пользователя будет являться создание эталонного профиля пользователя и добавление его во вкладку "пользователи".

Функциональные возможности данной вкладки позволяют также удалять и добавлять новых пользователей информационной системы.

Очередной этап – проведение процедур идентификации и аутентификации пользователя с учётом установленных администратором фильтров (рис. 2).

Осуществлялось моделирование двух попыток входа в систему. В первом случае рассматривался санкционированный пользователь, эталонный профиль которого зарегистрирован в системе. Во втором случае – потенциальный злоумышленник, не имеющий зарегистрированного эталонного профиля в системе и пытающийся войти под учётными данными другого пользователя.

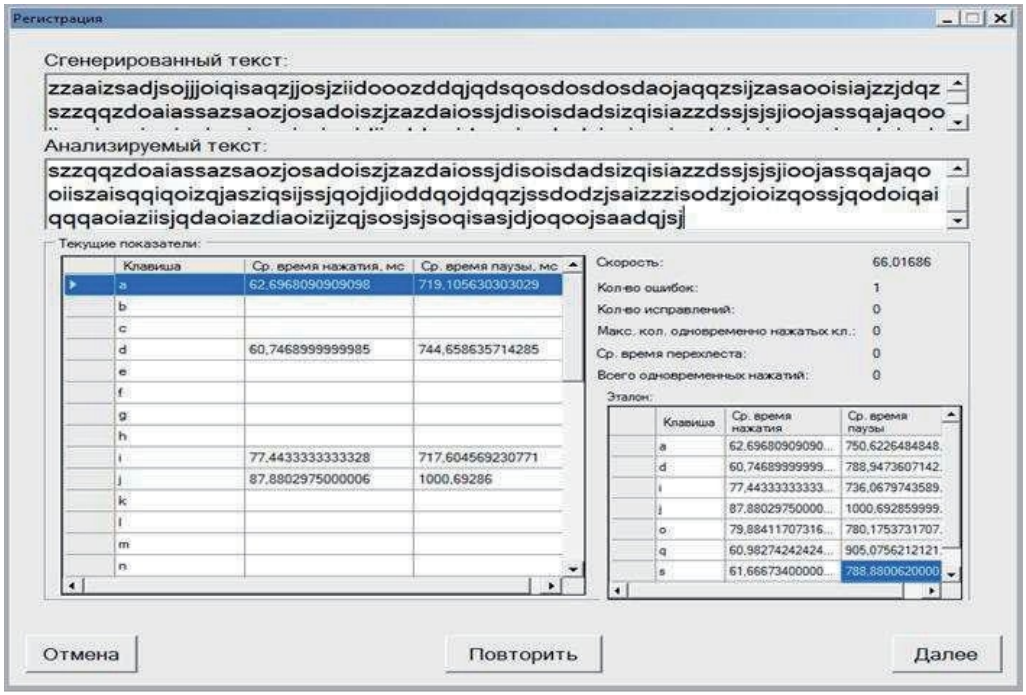

Рис. 1. Вкладка "регистрация", формирование на основе статистических данных эталонного профиля пользователя

Следующий этап – анализ результатов авторизации пользователя. В указанной вкладке администратор имеет возможность посмотреть дату авторизации конкретного пользователя, таблицы с показателями эталона, параметрами авторизации и коэффициентами отклонения.

Ожидаемым результатом данного шага является информация о пользователе, выполнявшем процедуры авторизации.

Под эффективностью разрабатываемой модели аутентификации пользователя на основе клавиатурного почерка будем понимать отношение показателей ошибок первого и второго рода при использовании биометрической аутентификации на основе клавиатурного почерка и при использовании других видов биометрической аутентификации. При расчёте показателя эффективности соответствующие отношения оказались равными 0,99 и 0,87, что говорит об эффективности применения клавиатурного почерка для биометрической аутентификации.

Таким образом, исходя из полученных результатов на каждом шаге данного эксперимента, можно сделать вывод об адекватности результатов и о работоспособности модели аутентификации пользователя в компьютерной системе на основе поведенческой биометрии.

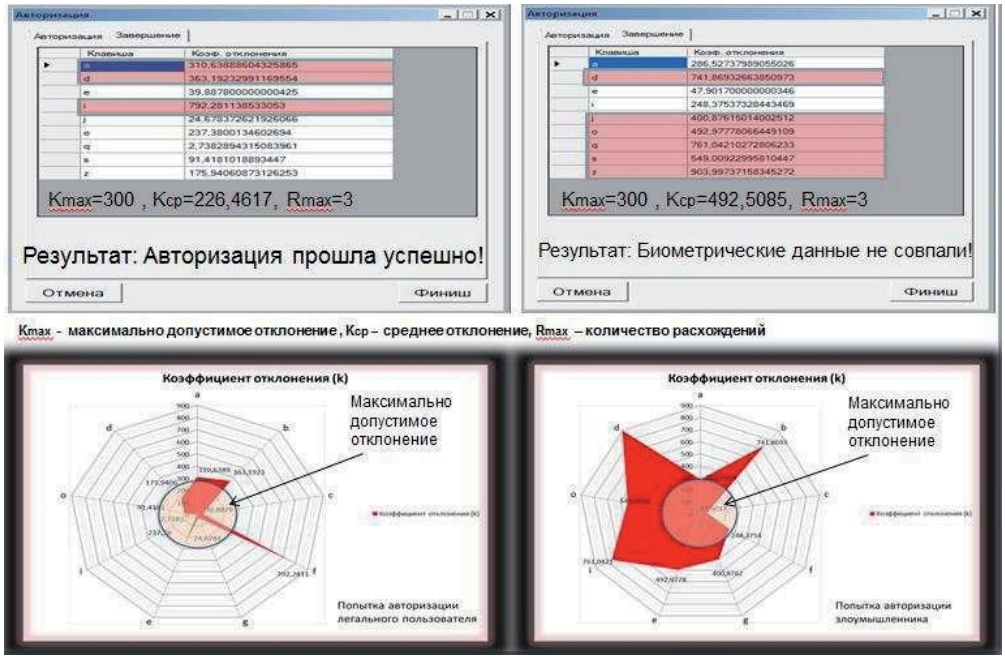

Рис. 2. Результат процедуры идентификации и аутентификации пользователя с учётом установленных администратором фильтров

Выбор метрики для расчёта аффинности эталонных и входящих параметров статистического профиля пользователя. В процессе исследования проведена серия экспериментов, целью которых являлось выявление лучшей метрики для определения аффинности эталонного профиля пользователя, зарегистрированного в системе, и профиля пользователя, пытающегося войти в систему [12].

Для одного и того же пользователя было произведено по 100 попыток входа в систему аутентификации пользователя на основе методов, использующих следующие метрики определения аффинности [1]:

1) относительное евклидово расстояние;

2) квадратичный индекс нечёткости.

Для каждой попытки входа был произведён расчёт ошибок первого и второго рода. Результаты в виде графиков зависимости ошибок первого и второго рода от количества экспериментов представлены на рис. 3.

Анализ полученных результатов показывает, что наилучшей метрикой для определения аффинности является метрика "Относительное евклидово расстояние". Поэтому именно она будет использоваться в дальнейшем при проведении экспериментов.

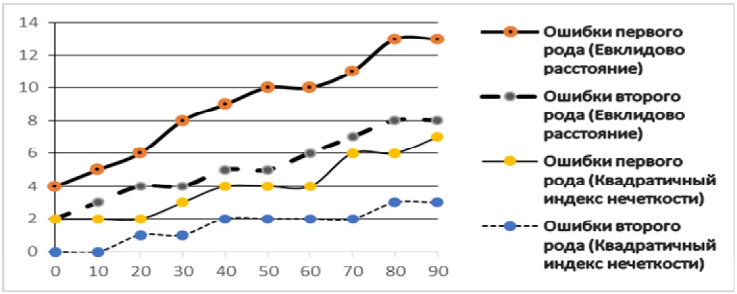

Рис. 3. График зависимости количества ошибок первого и второго рода от количества экспериментов

Таким образом, можно сделать вывод, что используемая метрика "Относительное евклидово расстояние" повышает эффективность разработанной модели биометрической аутентификации на основе клавиатурного почерка по отношению к другим методам биометрических аутентификаций более чем на 15%.

Оценка степени влияния парольной фразы на точность аутентификации. Была проведена серия экспериментальных исследований, целью которых являлось выявление рациональной длины парольной фразы, при которой количество ошибок первого и второго рода будет наименьшим.

Зависимость длины парольной фразы от показателей ошибок первого и второго рода при проведении N-го количества экспериментов (в данной работе $N = 300$) представлена на рис. 4.

Рис. 4. Зависимость длины парольной фразы от показателей ошибок первого и второго рода

Анализ полученных результатов показывает, что при использовании длины парольной фразы от тринадцати символов и более показатели ошибок первого и второго неизменны. Следовательно, длину пароля в

тринадцать символов можно считать рациональной. В дальнейших экспериментальных исследованиях будет использоваться длина парольной фразы в тринадцать символов.

Оценка рационального объёма текста для сбора поведенческой статистики. С этой целью осуществлена серия экспериментов (N = 300). Рациональной в данной работе будет считаться такая длина текстовой последовательности, которая будет давать наименьшее число ошибок первого и второго рода при аутентификации пользователя.

Зависимость длины текста для сбора поведенческой статистики пользователя от ошибок первого и второго рода представлена на рис. 5.

Анализ полученных результатов показывает, что при использовании длины текста для сбора поведенческой статистики пользователя в 300 символов и более показатели ошибок первого и второго неизменны. Следовательно, длину текста в 300 символов можно считать рациональной.

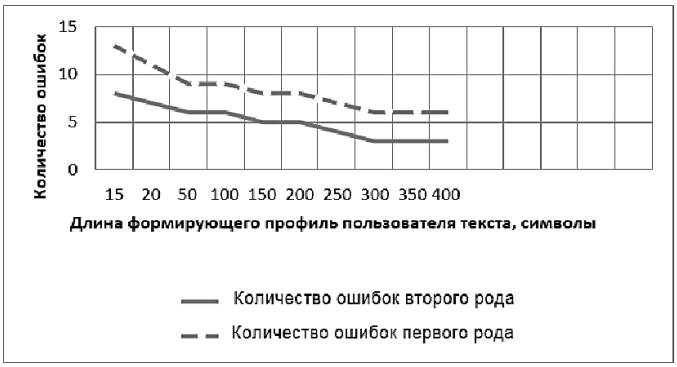

Рис. 5. Зависимость длины текста для сбора поведенческой статистики пользователя от ошибок первого и второго рода

Выводы. В результате проделанной работы описаны цели и задачи экспериментальных исследований разработанной модели аутентификации пользователя на основе поведенческой биометрии – клавиатурного почерка. Были определены требования к программным и вычислительным ресурсам, которые нужны при проведении экспериментов на разработанном программном прототипе, выделены четыре группы экспериментов, направленные на:

– проверку работоспособности программного прототипа и оценку его средней эффективности;

– определение наилучшей метрики для определения аффинности эталонных и входящих параметров статистических характеристик клавиатурного почерка;

– определение влияния парольной фразы на точность аутентификации;

– определение оптимального объёма текста для сбора поведенческой статистики.

По результатам проведённых исследований в рамках каждого эксперимента был сделан вывод о работоспособности программного комплекса и возможности применения его в качестве инструментального средства модели аутентификации пользователя в компьютерной системе на основе поведенческой биометрии, позволяющей повысить эффективность процедуры аутентификации, что показывают рассчитанные показатели эффективности (15%).

Кроме того, на эффективность аутентификации оказывают непосредственное влияние длина парольной фразы и длина первоначального текста, который используется для сбора статистики в процессе формирования эталонного профиля пользователя при его регистрации. Наилучшие показатели по ошибкам первого и второго рода (2% и 1% соответственно) в процессе аутентификации пользователя были зафиксированы при длине пароля в 13 символов и длине текста, предназначенного для сбора статистики профиля пользователя в 300 символов, что является нормой для поведенческих динамических систем. Следовательно, можно сделать вывод о достаточности длины формируемого профиля текста и отсутствии необходимости её дальнейшего увеличения.

Практическая значимость разработанной модели заключается в том, что её можно использовать: в качестве инструмента аутентификации пользователя в компьютерной системе; в учебном процессе в качестве лабораторного стенда при обучении студентов в области информационной безопасности. Например, при подготовке студентов кафедры компьютерных технологий и информационной безопасности Кубанского государственного технологического университета, обучающихся по специальности "Информационная безопасность автоматизированных систем" и по направлению подготовки бакалавров "Информационная безопасность".

Работа выполняется при поддержке РФФИ и Администрации Краснодарского края (проект - 16-46-230121).

Список литературы: **1.** *Миронов М. В.* Аутентификация пользователей в компьютерной системе на основе поведенческой биометрии / *И.Ю. Гришин, М.В. Миронов* // Проблеми інформатики та моделювання. Тези шістнадцятої міжнародної науково-технічної конференції 12-16 сентября 2016 г. – Одесса. – 2016. – С. 28. **2.** *Lumini A.* Overview of the combination of biometric matchers / *A. Lumini, L. Nanni* // Information Fusion. – Jan. 2017. – Vol. 33. – P. 71-85. **3.** *Савинов А.Н.* Математическая модель механизма распознавания клавиатурного почерка на основе гауссовского распределения / *А.Н. Савинов, И.Г. Сидоркина* // Известия Кабардино-Балкарского научного центра РАН. Вып. 1. –

Нальчик: Кабардино-Балкарский научный центр РАН, 2013. – С. 26-32. **4.** *Шарипов Р.Р.* Разработка полигауссового алгоритма аутентификации пользователей в телекоммуникационных системах и сетях по клавиатурному почерку: дис. … канд. техн. наук: 05.12.13 / Казан. гос. техн. ун-т им. А.Н. Туполева. – Казань, 2006. – 135 с. **5.** *Сафиуллин Н.Э.* Аппаратурный анализ клавиатурного почерка с использованием эталонных гауссовских сигналов / *Н.Э. Сафиуллин, Р.Р. Шарипов* // Вестник Казанского государственного технического университета. – 2006. – № 2. – С. 21-23. **6.** *Fakhara K.* Fuzzy pattern recognition-based approach to biometric score fusion problem / *K. Fakhara, M. Aroussi, M. Saidi, D. Aboutajdine* // Fuzzy Sets and Systems. – Dec. 2016. – Vol. 305. – P. 149-159. **7.** *Blasco J.* A Survey of Wearable Biometric Recognition Systems / *J. Blasco, T. Chen, J. Tapiador, P. Peris-Lopez* // ACM Computing Surveys (CSUR) Surveys Homepage archive. – Dec. 2016. – Vol. 49. – Issue 3. – Article No. 43.– P. 406-408. **8.** *Ahmad J.* Analysis of interaction trace maps for active authentication on smart devices / *J. Ahmad, M. Sajjad, Z. Jan, I. Mehmood, S. Rho, S. Baik* // Multimedia Tools and Applications. – Feb. 2017. – Vol. 76. – Issue 3. – P. 4069-4087. **9.** *Czajka A.* Verification of Iris Image Authenticity Using Fragile Watermarking / *A. Czajka, W. Kasprzak, A. Wilkowski* // Bulletin of the Polish Academy of Sciences-Technical Sciences. – Dec 2016. – Vol. 64. – Issue 4. – P. 807-819. **10.** *Гришин И.Ю.* Анализ перспективных подходов к проектированию систем безопасности распределённых компьютерных сетей / *И.Ю. Гришин* // Вестник Российского нового университета. Серия: Сложные системы: модели, анализ и управление. – 2015. – № 2. – С. 36-40. **11.** *Тимиргалеева Р.Р.* Цифровая экономика: построение и оптимизация бизнес-процессов / *Р.Р. Тимиргалеева, И.Ю. Гришин* // NovaInfo.Ru. – 2016. – Т. 1. – № 1. – С. 176-182. **12.** *Гришин И.Ю.* Проблемы управления зенитными ракетными комплексами / *И.Ю. Гришин, М.К. Можар, В.М. Решетник* // Наука и оборона. – 1994. – № 3. – С. 27-32. **13.** *Гришин И.Ю.* Особенности применения биометрических методов для аутентификации обучаемого в системе дистанционного образования / *И.Ю. Гришин, Р.Р. Тимиргалеева, М.В. Миронов, М.Г. Ефимчик* // Филологические и социокультурные вопросы науки и образования. Сборник материалов I Международной научно-практической конференции. – 2016. – С. 219-229.

References:

1. Mironov, M.V., and Grishin I.Yu. (2016), "Authentication of users in a computer system based on behavioral biometrics", Problems of Informatics and Modeling. *Theses sixteenth International Scientific Conference.* – September 12-16 2016 year, p. 28.

2. Lumini, A., and Nanni, L. (2017), "Overview of the combination of biometric matchers", *Information Fusion,* Vol. 33, pp. 71-85.

3. Savinov, A.N., and Sidorkina, I.G. (2013), "Mathematical model of the mechanism of recognition of keyboard handwriting based on the Gaussian distribution", *News of the Kabardino-Balkarian Science Center of the Russian Academy of Sciences*, No. 1, pp. 26-32.

4. Sharipov, R.R. (2006), *Development of a polygas algorithm for user authentication in telecommunication systems and networks using keyboard handwriting: dissertation*, Kazan, 135 p.

5. Safiullin, N.E., and Sharipov, R.R. (2006), "Hardware analysis of the keyboard handwriting using standard Gaussian signals", *Bulletin of the Kazan State Technical University*, No. 2, pp. 21-23.

6. Fakhara, K., Aroussi, M., Saidi, M., and Aboutajdine, D. (2016), "Fuzzy pattern recognition-based approach to biometric score fusion problem", *Fuzzy Sets and Systems*, Vol. 305, pp. 149-159.

7. Blasco, J., Chen, T., Tapiador, J., and Peris-Lopez, P. (2016), "A Survey of Wearable Biometric Recognition Systems", *ACM Computing Surveys (CSUR) Surveys Homepage archive*, Vol. 49, Issue 3, Article No. 43, pp. 406-408.
8. Ahmad, J., Sajjad, M., Jan, Z., Mehmood, I., Rho, S., and Baik, S. (2017), "Analysis of interaction trace maps for active authentication on smart devices", *Multimedia Tools and Applications*, Vol. 76, Issue 3, pp. 4069-4087.
9. Czajka, A., Kasprzak, W., and Wilkowski, A. (2016), "Verification of Iris Image Authenticity Using Fragile Watermarking", *Bulletin of the Polish Academy of Sciences-Technical Sciences*, Vol. 64, Issue 4, pp. 807-819. DOI: 10.1515/bpasts-2016-0090.
10. Grishin, I.Yu. (2015), "Analysis of prospective approaches to the design of security systems for distributed computer networks", *Bulletin of the Russian New University. Series: Complex systems: models, analysis and management*, No. 2, pp. 36-40.
11. Timirgaleeva, R.R., and Grishin, I.Yu. (2016), "Digital Economy: Building and Optimizing Business Processes", *NovaInfo.Ru*, Vol.1, No. 1, pp. 176-182.
12. Grishin, I.Yu., Mozhar, M.K., and Reshetnik, V.M. (1994), "The problems of control of anti-aircraft missile systems", *Science and defense*. No. 3. pp. 27- 32.
13. Grishin, I.Yu., Timirgaleeva, R.R., Mironov, M.V., and Efimchik, M.G. (2016), "Features of application of biometric methods for student authentication in the system of distance education", Philological and sociocultural issues of science and education. *Collection of materials of the First International Scientific and Practical Conference.* pp. 219-229.

Статью представил д-р техн. наук, профессор НТУ "ХПИ" Леонов С.Ю.

Поступила (received) 18.11.2016

Igor Yu. Grishin, Dr. Sci. Tech., Professor
Professor at the Department of Computer Technology and Information Security
Kuban State Technological University
Str. Krasnaya, 91, Krasnodar, Russia, 350000
Tel.: +7 (989) 140-57-55, e-mail: igugri@gmail.com
ORCID ID: 0000-0001-5839-1858

Rena R. Timirgaleeva, Dr.Sci. Econ., Professor
Professor at the Department of Computer Technology and Information Security
Kuban State Technological University
Str. Krasnaya, 91, Krasnodar, Russia, 350000
Tel.: +7 (989) 805-47-96, e-mail: renatimir@gmail.com

Maksim V. Mironov, aspirant
Aspirant at the Department of Computer Technology and Information Security
Kuban State Technological University
Str. Krasnaya, 91, Krasnodar, Russia, 350000
Tel.: +7 (989) 140-57-55, e-mail: igugri@gmail.com
ORCID ID: 0000-0001-5839-1858

УДК 004.056.53

Аналіз ефективності моделей аутентифікації користувачів на основі клавіатурний почерку / Грішин І.Ю., Тіміргалєєва Р.Р., Міронов М.В. // Вісник НТУ "ХПІ". Серія: Інформатика та моделювання. – Харків: НТУ "ХПІ". – 2017. – № 21 (1243). – С. 153 – 164.

Завданням дослідження була перевірка працездатності програмного прототипу моделі, а також дослідження його функціональних можливостей. Здійснено оцінку правильності роботи програмного прототипу моделі на кожному з етапів: реєстрація нового користувача в системі, формування на основі статистичних даних еталонного профілю користувача, проведення процедур ідентифікації й аутентифікації користувача з урахуванням встановлених адміністратором фільтрів, перегляд результату авторизації користувача. Для проведення експериментальних досліджень розроблений програмний комплекс, що дозволяє провести необхідний перелік експериментів, а також здійснити статистичну обробку результатів, оцінити значення помилок першого і другого роду при аутентифікації. Іл.: 5. Бібліогр.: 13 назв.

Ключові слова: модель аутентифікації користувача; клавіатурний почерк; авторизація користувача; помилки першого та другого роду.

УДК 004.056.53

Анализ эффективности моделей аутентификации пользователя на основе клавиатурного почерка / Гришин И.Ю., Тимиргалеева Р.Р., Миронов М.В. // Вестник НТУ "ХПИ". Серия: Информатика и моделирование. – Харьков: НТУ "ХПИ". – 2017. – № 21 (1243). – С. 153 – 164.

Задачей исследования явилась проверка работоспособности программного прототипа модели, а также исследование его функциональных возможностей. Осуществлена оценка правильности работы программного прототипа модели на каждом из этапов: регистрация нового пользователя в системе, формирование на основе статистических данных эталонного профиля пользователя, проведение процедур идентификации и аутентификации пользователя с учётом установленных администратором фильтров, просмотр результата авторизации пользователя. Для проведения исследований разработан программный комплекс, позволяющий провести необходимый перечень экспериментов, а также осуществить статистическую обработку результатов, оценить значения ошибок первого и второго рода при аутентификации. Ил.: 5. Библиогр.: 13 назв.

Ключевые слова: модель аутентификации пользователя; клавиатурный почерк; авторизация пользователя; ошибки первого и второго рода.

UDC 004.056.53

The analysis of the effectiveness of user authentication models based on keyboard handwriting / Grishin I.Yu., Timirgaleeva R.R., Mironov M.V. // Herald of the National Technical University "KhPI". Subject issue: Information Science and Modelling. – Kharkov: NTU "KhPI". – 2017. – №. 21 (1243). – P. 153 – 164.

The tasks of the experimental study were to test the working capacity of the software prototype of the model, as well as to study its functional capabilities. The evaluation of the correctness of the software prototype of the model at each stage was carried out: registration of a new user in the system, generation of a user's reference profile based on statistical data, conducting user identification and authentication procedures taking into account the filters set by the administrator, and viewing the user's authorization result. For carrying out studies, a software package has been developed that makes it possible to carry out the necessary list of experiments, as well as to perform statistical processing of results, to estimate the values of errors of the first and second kind for authentication. Figs.: 5. Refs.: 13 titles.

Keywords: user authentication model; keyboard handwriting; biometric authentication methods; errors of the first and second kind.