УДК 681.323 doi: 10.26102/2310-6018/2018.23.4.039

Т.И. Лапина, Э.М. Димов, Е.А. Петрик, Д.В. Лапин

УПРАВЛЕНИЕ ДОСТУПОМ К ИНФОРМАЦИОННЫМ РЕСУРСАМ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

ФГБОУ ВПО «Юго-Западный государственный университет», Курск, Россия

В статье рассматривается поход к организации многофакторной аутентификации пользователей автоматизированных информационных систем. Показано, что при многопользовательском режиме доступа к информационному ресурсу через сетевые протоколы одной из основных задач обеспечения информационной безопасности ресурсов является подтверждение личности, вступающей в информационный обмен. В настоящее время при использовании единого информационного пространства автоматизированных информационных систем средства информационной безопасности должны обеспечивать еще поддержание детерминистической целостности. Под детерминистической целостностью информационных ресурсов подразумевается не только факт использования и взлома конфиденциальные данные предприятия, а способность средств защиты однозначно удостоверить целостность своих информационных ресурсов на основе минимизации риска проникновения посторонних пользователей. В статье рассмотрен подход организации доступа к информационным ресурсам автоматизированных информационных систем на основе многофакторной аутентификации. Проверка личности пользователя информационного ресурса выполняется после проведения стандартных процедур проверки факторов аутентификации и является одним из уровней многофакторной аутентификации. Для подтверждения личности пользователя предложено использовать методы динамической биометрической аутентификации на основе динамика рукописного почерка. Предложен комплекс технических средств получения биометрический данных пользователя, процедуры их анализа и алгоритм доступа к информационному ресурсу. Для формирования биометрического образа и эталона предложено использовать дискретное преобразование Фурье и систему ортогональных функций Хаара, позволяющих выделить существенные особенности измеряемых данных динамики рукописного почерка пользователя информационных ресурсов.

Ключевые слова: аутентификация пользователя, многофакторная аутентификация, анализ биометрических данных

В настоящее время, по результатам проведенного анализа международной исследовательской и консалтинговой компанией International Data Corporation (IDC), занимающейся изучением мирового рынка информационных технологий и телекоммуникаций, особое внимание уделяется прогнозам относительно будущего ИТ-безопасности. Особый интерес к вопросам ИТ-безопасности обусловлен широким распространением сетевых банковских технологий и необходимостью

обеспечения информационной безопасности национальных платежных систем, использованием информационно-телекоммуникационных систем специального назначения органами государственной власти (ИТКС), внедрением в деятельность компаний облачных сервисов, что ведет к резкому расширению круга пользователей и использованию программных средств, не удовлетворяющих требованиям безопасности. Поэтому, одной из основных задач при разработке информационных систем предприятий, государственных и административных учреждений является задача обеспечения информационной безопасности, которая, в свою очередь, требует разработки методов и средств мониторинга для выявления фактов несанкционированных информационных воздействий, а также средств и методов контроля личности пользователей информационных ресурсов.

Большинство разработчиков и пользователей в своей деятельности используют автоматизированные информационные системы и технологии, которые в качестве информационных ресурсов используют созданное единое информационное пространство или единую базу данных. При таком подходе при выполнении бизнес-процессов в различных предметных областях пользователи могут использовать различные проблемно-ориентированные приложения, имеющие доступ к единой базе данных, являющейся хранилищем информационных ресурсов автоматизированной системы, находят в ней необходимые сведения, обрабатывают их и помещают в единую базу данных результаты этой обработки (Рисунок 1).

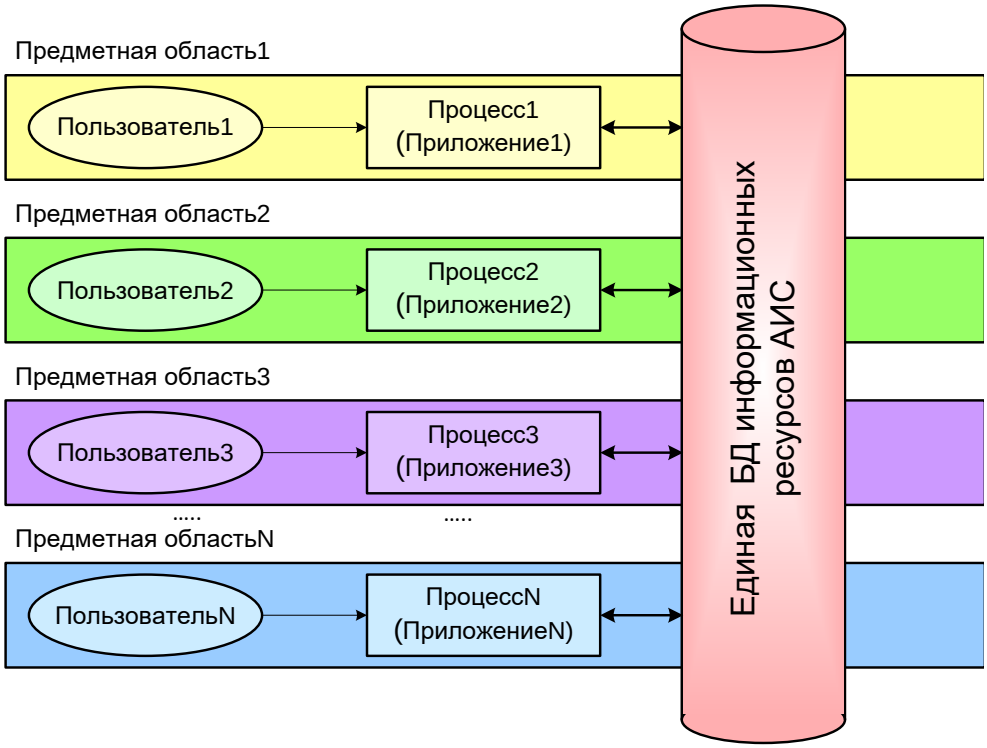

Рисунок - 1 Схема взаимоотношений моделей с общей базой данных

Таким образом, все больше пользователей прибегают к технологии удаленного доступа или общему доступу многих пользователей к одному информационному ресурсу через сетевые протоколы.

Возникает противоречие, с одной стороны количество пользователей, использующих единое информационное пространство, обеспечивает эффективность использования интегрированных ресурсов, с другой, при росте вовлеченности важных информационных ресурсов растет и риск работы с ними в сетях.

В настоящее время задача минимизации риска подключения удаленных пользователей к информационным ресурсам и контроля использования конфиденциальных данных закрытых предприятий решается с помощью аппаратных средств защиты информации, парольной защиты, средствами диспетчирования и управления вычислительными процессами операционной системы и пр.

Задача обеспечения информационной безопасности автоматизированных информационных систем (АИС), использующих единое информационное пространство, включает ряд частных задач:

– сохранение целостности данных баз данных;

– неизменность алгоритмов и технологий преобразования данных;

– обеспечение конфиденциальности и доступности информации.

То есть, в настоящее время при использовании единого информационного пространства автоматизированных информационных систем средства информационной безопасности (СИБ) должны обеспечивать еще поддержание детерминистической целостности.

Под детерминистической целостностью информационных ресурсов в контексте данных подразумевается, что они остаются не только неизменными и достоверными, но при получении информации о том, что некоторый пользователь АИС совершает определенные действия, имеется подтверждение того, что этот пользователь являются именно тем, за кого он себя выдает. Таким образом, детерминистическая целостность заключается не в том, подвергались или нет конфиденциальные данные предприятия взлому, а в способности предприятия однозначно удостоверить целостность своих информационных ресурсов на основе минимизации риска проникновения посторонних пользователей.

Рациональным решением данной задачи является применение многофакторной аутентификации при доступе пользователя к информационным ресурсам и информационным объектам АИС.

Частным случаем многофакторной аутентификации является двухфакторная аутентификация (two-factor authentication), позволяющая

проводить идентификацию пользователей с помощью комбинации различных подходов. Например, авторизация Google и Microsoft является двухфакторной аутентификацией, в случае, если пользователь получает доступ к информационным ресурсам с нового устройства, помимо аутентификации по имени-паролю, вводится шестизначный (Google) или восьмизначный (Microsoft) код-подтверждения, который можно получить по SMS.

В случае многофакторной аутентификации пользователь аутентифицируется при помощи комбинации трех факторов: пользователь предоставляет системе «то, что знает» (“something you know”) – например, пароль, PIN код, «то, что имеет» (“something you have”), какой-либо аппаратный идентификатор, а также биометрические параметры – «то, кем является» (“something you are”).

Такой подход требует разработки комплекса технических средств и процедур идентификации, аутентификации и авторизации пользователей. Точность идентификации в таких системах во многом определяется способом получения исходных данных, в качестве которых приоритет отдается динамическим биометрическим измерениям, таким как рукописный почерк, голос, а также используемым процедурам обработки данных, факторного анализа и распознавания образов.

В данной статье рассматривается подход к организации процедуры идентификации и аутентификации пользователей АИС на основе многофакторной аутентификации, одним из факторов аутентификации являются биометрические характеристика динамики рукописного почерка пользователя АИС.

Схема этапов идентификации и аутентификации пользователя при запросах на доступ к информационным ресурсам приведена на Рисунке 2.

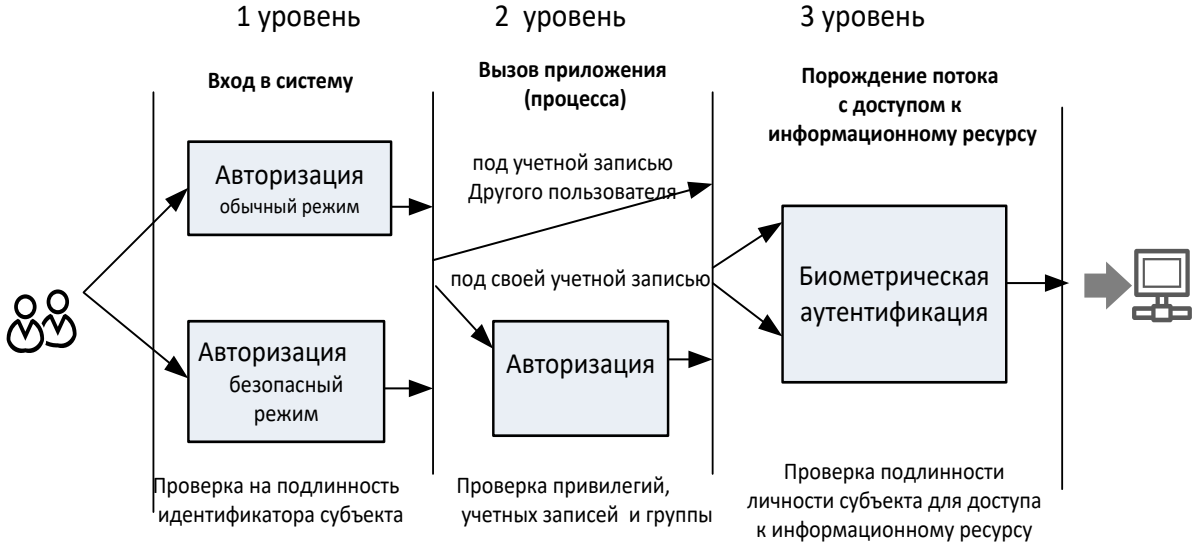

Рисунок 2 - Схема доступа к информационным ресурсам

Средства защиты информации 1 уровня должны обеспечивать идентификацию пользователей при запросах на доступ к информационным ресурсам.

На 1 уровне при входе в систему выполняется идентификация и аутентификация пользователя на основании предъявленных факторов, например, пароль, PIN код пользователя.

Авторизация пользователя, то есть, проверка привилегий пользователя и противодействие входу в систему неидентифицированного пользователя выполняется на 2 уровне.

На 2 уровне при запуске пользователем процессов (приложений), которые порождают потоки, которые используют информационные ресурсы. Кроме того, доступ к информационному ресурсу идентифицирует процесс, к которому осуществляется обращение.

На 3 уровне производится определение личности пользователя или биометрическая аутентификация по его биометрическим характеристикам.

На 3 уровне проверки пользователя выполняется детерминация, то есть установление личности (impersonation) пользователя, то есть выполняется контроль пользователя при получении доступа к информационным ресурсам. Именно на этом этапе целесообразно применять динамическую биометрическую аутентификацию, при этом в качестве фактора идентификации и аутентификации использовать динамику рукописного почерка, что по сравнению с изображением (отпечатка пальца, сетчатки глаза) обеспечивает невозможность подмены вводимого образца.

Для получения измеряемых биометрических данных используется специализированное устройство [1] (Рисунок 3).

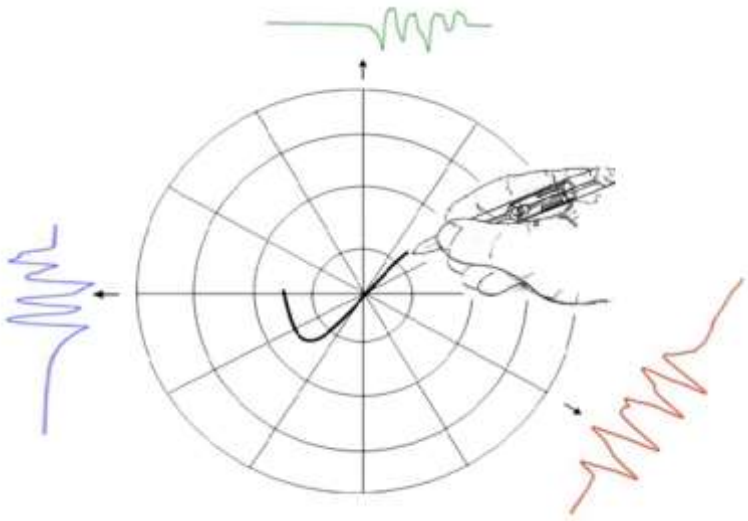

Рисунок 3 - Получения биометрических данных
по рукописному почерку

Получаемые биометрические данные представляют собой измерения давления на пишущий узел при перемещении по n направлениям датчика перемещений при написании парольной фразы, то есть кривые изменения нажима на пишущий узел по осям координат X1(t),.. Xn(t).

Устройство измерения параметров давления при получении биометрических данных по рукописному почерку приведено на Рисунке 4.

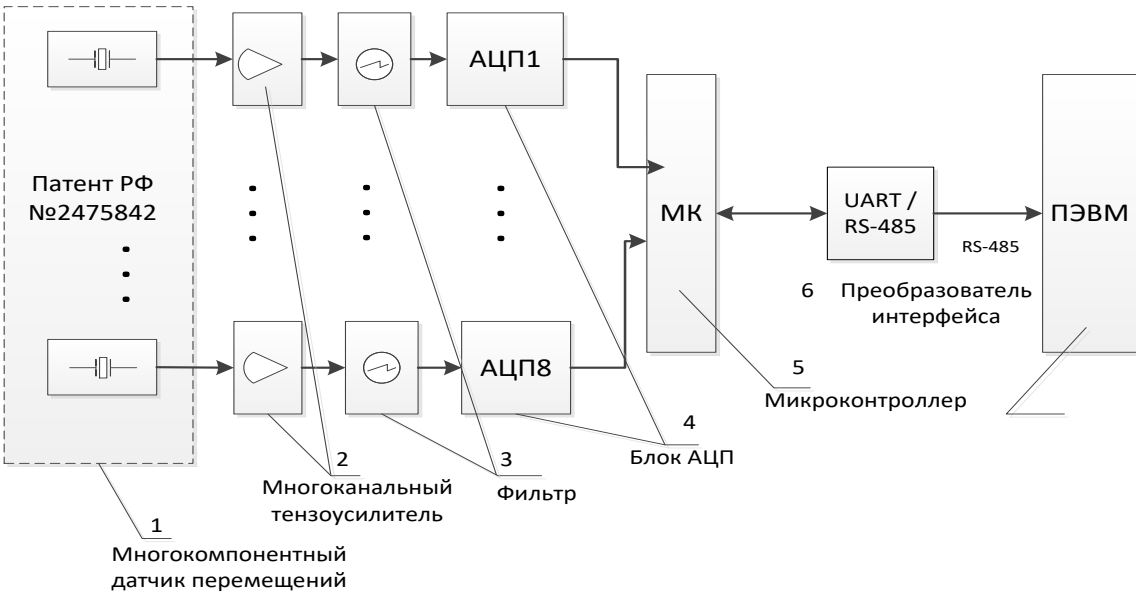

Рисунок 4 - Устройства для измерения параметров давления при получении биометрических данных по рукописному почерку

Устройство регистрации [2] позволяет фиксировать сигналы давления при перемещении датчика во время процедуры аутентификации с последующей оцифровкой измерений и передачи в блок обработки данных (Рисунок 4).

Получаемые биометрические данные представляют собой кривые изменения нажима на пишущий узел устройства при перемещении по n направлениям, то есть осям координат X1(t),.. Xn(t). Индивидуальные особенности воспроизведения парольной фразы пользователем будут отражены в частотной структуре функций $x_1(t), x_2(t),..., x_n(t)$ (Рисунок 5).

Рисунок 5 - Формирование матрицы исходных измерений

Задача проверки личности пользователя на 3 уровне контроля выполняется путем проведения биометрического анализа и сводится к извлечению полученной биометрической информации, формированию биометрического образа пользователя и передачи в систему контроля (Рисунок 6).

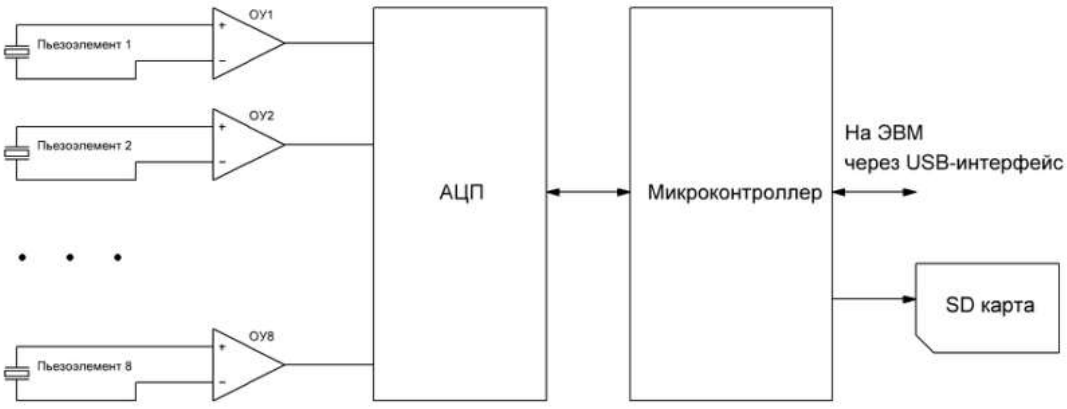

Рисунок 6 - Структурная схема устройство регистрации и обработки данных при выполнении процедуры аутентификации

Для формирования биометрического образа могут быть использованы линейные функционалы, такие как дискретное преобразование Фурье (ДПФ), системы ортогональных функций Хаара и пр., позволяющие выделить существенные особенности измеряемых данных [2,3].

В статье рассмотрено двумерное дискретное преобразование Хаара включает обработку матрицы N×N дискретных значений измерений многокомпонентного датчика перемещений.

Приведем пример выполнения преобразования Хаара для матрицы 4×4 (1):

$$P = \begin{pmatrix} 18 & 14 & 12 & 4 \\ 10 & 6 & 8 & 8 \\ 16 & 4 & 8 & 0 \\ 12 & 0 & 4 & 4 \end{pmatrix} \quad (1)$$

На первом шаге двумерного дискретного преобразования Хаара осуществляется умножение матриц **P и W (2)**.

Матрица W – ортонормальная функция Хаара четвертого порядка [5]:

$$PW = \begin{pmatrix} 18 & 14 & 12 & 4 \\ 10 & 6 & 8 & 8 \\ 16 & 4 & 8 & 0 \\ 12 & 0 & 4 & 4 \end{pmatrix} \times \frac{1}{4} \times \begin{pmatrix} 1 & 1 & 2 & 0 \\ 1 & 1 & -2 & 0 \\ 1 & -1 & 0 & 2 \\ 1 & -1 & 0 & -2 \end{pmatrix} = \begin{pmatrix} 12 & 4 & 2 & 4 \\ 8 & 0 & 2 & 0 \\ 7 & 3 & 6 & 4 \\ 5 & 1 & 6 & 0 \end{pmatrix} \quad (2)$$

Затем выполняется одномерное преобразование каждого столбца. Матрица преобразования столбцов транспонируется, затем умножается на преобразующую матрицу, после чего результат снова транспонируется (3):

$$T = ((PW)^T \times W)^T = W^T \times P \times W, \quad (3)$$

знак $()^T$ означает транспонирование.

Двумерное дискретное преобразование матрицы **будет** иметь вид (4):

$$T = W^T PW = \frac{1}{4} \times \begin{pmatrix} 1 & 1 & 1 & 1 \\ 1 & 1 & -1 & -1 \\ 2 & -2 & 0 & 0 \\ 0 & 0 & 2 & -2 \end{pmatrix} \times \begin{pmatrix} 12 & 4 & 2 & 4 \\ 8 & 0 & 2 & 0 \\ 7 & 3 & 6 & 4 \\ 5 & 1 & 6 & 0 \end{pmatrix} = \begin{pmatrix} 8 & 2 & 4 & 2 \\ 2 & 0 & -2 & 0 \\ 2 & 2 & 0 & 2 \\ 1 & 1 & 0 & 2 \end{pmatrix} \quad (4)$$

Полученная матрица коэффициентов двумерного дискретного преобразования Хаара используется в дальнейшем в качестве идентификационного образа при аутентификации пользователей информационных ресурсов [3].

Алгоритм доступа к информационному ресурсу можно представить следующим образом (Рисунок 7):

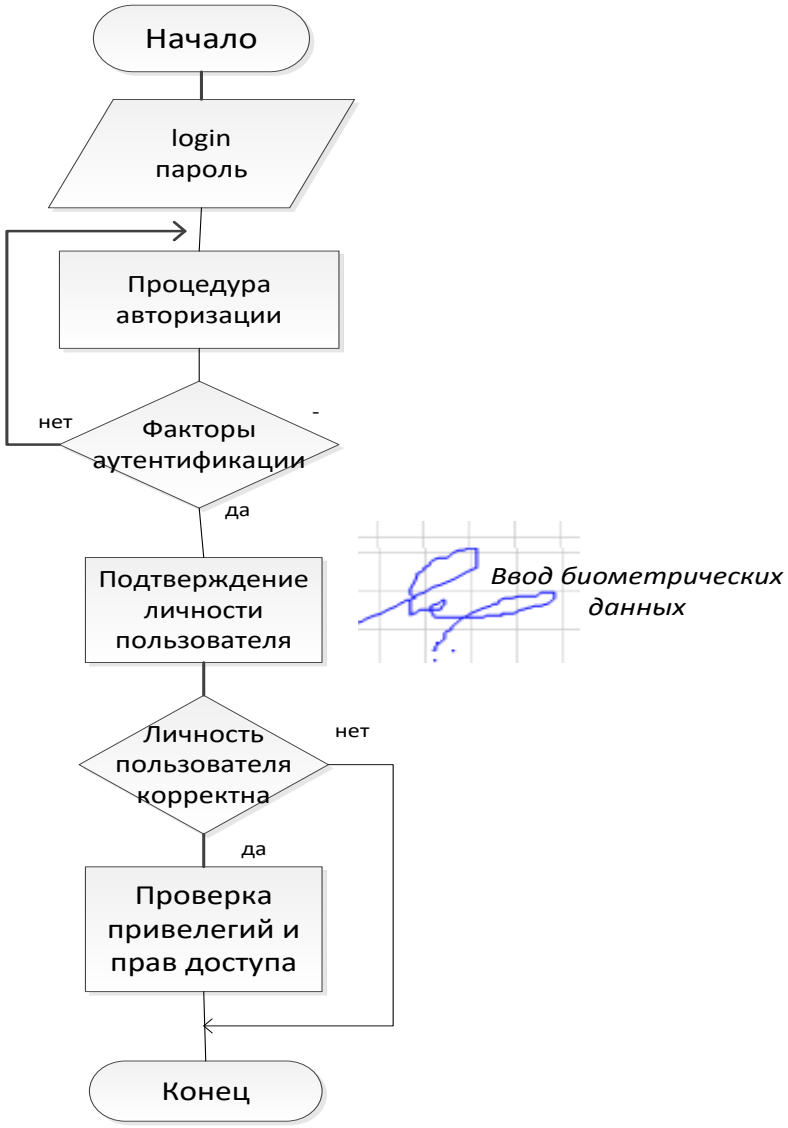

Рисунок 7 - Проверка личности пользователя информационного ресурса

Проверка личности пользователя информационного ресурса должна осуществляться уже после проведения процедуры проверки факторов аутентификации.

При расширении круга пользователей накопленных информационных ресурсов созданного единого информационного пространства компаний растет и риск работы с ними в инфокоммуникационных. При многопользовательском режиме доступа к данным одной из основных задач обеспечения информационной безопасности ресурсов является задача подтверждения личности, вступающей в информационный обмен, которая может быть решена путем использования многофакторной аутентификации пользователей.

Такой подход к организации доступа в АИС обеспечивает возможность сохранения целостности накопленных информационных ресурсов и алгоритмов их обработки, поэтому в ближайшее время задачи применения многофакторной аутентификации для обеспечения безопасности информационных ресурсов будут находиться в области особых интересов разработчиков.

ЛИТЕРАТУРА

1. Патент № 2475842 Российской Федерации Цифровой многокомпонентный датчик перемещений/ Милых В.А., Лапин Д.В., Лапина Т.И., Заявка № 2011142722/08 от 21.10.2011, опубл. 20.02.2013, Бюл. №5
2. Патент № 2475699 Российской Федерации Устройство измерения параметров пишущего узла/ Милых В.А., Лапин Д.В., Лапина Т.И. Заявка № 2011113800/28, 08.04.2011, опубл. 20.02.04.2013, Бюл. №5.
3. Лапина, Т.И. Многофакторная идентификация пользователей информационных ресурсов Т.И. Лапина, Д.В. Лапин //Информационно-измерительные и управляющие системы. 2017. т.15, №5. с. 37-42.
4. Лапина, Т.И. Способ биометрической аутентификации пользователя в компьютеризированных системах контроля доступа/ Т.И. Лапина, Д.В. Лапин, Н.Н.Епишев//Труды СПИИРАН. - СПб.: СПИИРАН, 2013.- выпуск №4 (27), с.189-199.
5. Лапина, Т.И. Подход к классификации цифровых сигналов в системах контроля доступа/ Т.И.Лапина, Д.В.Лапин, Е.А. Петрик, // Информационно-измерительные и управляющие системы. 2013. т.11, №9. с. 58-64.
6. Лапина, Т.И. Построение компьютеризированных систем контроля доступа по динамике рукописного почерка/ Т.И. Лапина, Д.В. Лапин, В.П.Добрица, Е.А.Петрик //Информационно-измерительные и управляющие системы. 2013. т.11, №8. с. 34-41.

T.I. Lapina, E.M. Dimov, E.A. Petrik, D.V. Lapin

ACCESS CONTROLS TO INFORMATION RESOURCES IN INFORMATION SYSTEMS

Southwest State University, Kursk, Russia

In article the campaign to the organization of multifactor authentication of users in automated information systems at remote access of many users to one information resource through network protocols is considered. It is shown that at a multiuser mode of data access of one of the main objectives of information security support of resources the problem of

confirmation of the personality entering information exchange which can be solved by use of multiple-factor authentication is. For confirmation of the identity of the user dynamic biometric identification and authentications on a basis is used by dynes of hand-written handwriting. The complex of technical means of receiving biometric data, the procedure of their analysis and an algorithm of access to an information resource is offered. For forming of a biometric image, it is offered to use discrete transform of Fourier and the system of the orthogonal functions of Haar allowing to select essential features of the measured data of dynamics of hand-written handwriting of the user of information resources.

Keywords: user authentication, multi-factor authentication, biometric data analysis.

REFERENCES

1. Patent № 2475842 Rossiiskoi Federacii Cifrovoi mnogokomponentnii datchik peremeschenii/ Milih V.A., Lapin D.V., Lapina T.I., Zayavka № 2011142722/08 ot 21.10.2011, opubl. 20.02.2013, Byul. №5
2. Patent № 2475699 Rossiiskoi Federacii Ustroistvo izmereniya parametrov pishuschego uzla/ Milih V.A., Lapin D.V., Lapina T.I. Zayavka № 2011113800/28, 08.04.2011, opubl. 20.02.04.2013, Byul. №5.
3. Lapina, T.I. Mnogofaktornaya identifikaciya polzovatelei infor_macionnih resursov T.I. Lapina_ D.V. Lapin //Informacionno_izmeritelnie i upravlyayuschie sistemi. 2017. t.15, №5. s. 37-42.
4. Lapina, T.I. Sposob biometricheskoi autentifikacii polzovatelya v kompyuterizirovannih sistemah kontrolya dostupa/ T.I. Lapina, D.V. Lapin, N.N. Epishev // Trudi SPIIRAN. - SPb. - SPIIRAN, 2013 . - vipusk №4 (27) s.189-199.
5. Lapina, T.I. Podhod k klassifikacii cifrovih signalov v sistemah kontrolya dostupa/ T.I.Lapina, D.V.Lapin, E.A. Petrik // Informacionno-izmeritelnie i upravlyayuschie sistemi. 2013. t.11 - .№9. s. 58-64.
6. Lapina, T.I. Postroenie kompyuterizirovannih sistem kontrolya dostupa po dinamike rukopisnogo pocherka/ T.I. Lapina, D.V. Lapin, V.P.Dobrica, E.A.Petrik //Informacionno-izmeritelnie i upravlyayuschie sistemi. 2013. t.11, №8. s. 34-41.