ИНФОРМАТИКА И ВЫЧИСЛИТЕЛЬНАЯ ТЕХНИКА

COMPUTER SCIENCE, COMPUTER ENGINEERING

УДК 57.087.1
DOI: 10.21869/2223-1560-2019-23-1-84-94

Анализ современных статических методов биометрической идентификации

Калуцкий И. В. [1] ✉, Матюшин Ю. С. [1], Спевакова С. В. [1]

[1] ФГБОУ ВО «Юго-Западный государственный университет», Россия, 305040, Курск, ул. 50 лет Октября, 94

✉ e-mail: igor_kalutsky@mail.ru

Резюме

Цель исследования. *В современных системах сбора данных используются мобильные автоматизированные устройства, данные из которых в зашифрованном виде поступают в центр обработки данных. В качестве средства защиты информации в ЦОД биометрические методы идентификации обладают рядом преимуществ. В частности, им присуща высокая надёжность, так как сложно скомпрометировать или утратить биометрические данные.*

Методы. *В статье предложен метод биометрической идентификации по геометрии лица. Предлагаемый метод позволяет строить 3D-модель лица человека на основе 2D-изображений. Для определения достоверности биометрического метода идентификации предложены количественные характеристики КЛП и КЛО. КЛП – коэффициент ложного пропуска – определяет процент возникновения ситуаций, когда пользователю, не зарегистрированному в базе данных, система разрешает доступ. КЛО – коэффициент ложного отказа – определяет процент возникновения ситуаций, когда пользователю с корректными биометрическими данными система отказывает в доступе. Есть и другие характеристики, используемые при подборе систем биометрической идентификации. К ним относятся простота использования, скорость работы системы, влияние на нее факторов окружающей среды, стоимость системы и другие.*

Результаты. *Рассмотрены следующие известные методы статической идентификации: метод идентификации по отпечатку пальца, метод идентификации по сетчатке глаза, метод идентификации по радужной оболочке глаза, метод идентификации по геометрии лица, а также метод идентификации по рисунку вен руки. Приведены сравнительные характеристики каждого из них. Предложен новый метод, позволяющий повысить точность и быстродействие биометрической идентификации.*

Заключение. *В статье проведен анализ современных биометрических средств идентификации статического типа. Рассмотрены различные параметры определения эффективности методов биометрической идентификации. Представлены принципы, на которых основан каждый из перечисленных методов, а также основные достоинства и недостатки.*

Ключевые слова: *идентификация; биометрия; метод; сканер; КЛО; КЛП.*

Конфликт интересов: *Авторы декларируют отсутствие явных и потенциальных конфликтов интересов, связанных с публикацией настоящей статьи.*

Для цитирования: Калуцкий И.В., Матюшин Ю.С., Спевакова С.В. Анализ современных статических методов биометрической идентификации // Известия Юго-Западного государственного университета. 2019. Т. 23, № 1. С. 84-94. **DOI:** 10.21869/2223-1560-2019-23-1-84-94.

UDC 57.087.1

DOI: 10.21869/2223-1560-2019-23-1-84-94

Analysis of Modern Static Methods of Biometric Identification

Igor V. Kalutskiy [1]✉, Yuriy S. Matiushin [1], Svetlana V. Spevakova [1]

[1] Southwest State University, 94, 50 Let Oktyabrya str., Kursk, 305040, Russian Federation

✉ e-mail: igor_kalutsky@mail.ru

Abstract

Purpose of reseach. *Modern data collection systems use mobile automated devices, the data from which is encrypted in the data center. Biometric identification methods have several advantages as means of information security in the data center. In particular they are characterized by high reliability, since it is difficult to compromise or lose biometric data.*

Methods*. The method of biometric identification of facial geometry is proposed in the article. This method allows you to build a 3D model of a human face based on 2D images. To determine the accuracy of the biometric identification method, quantitative characteristics of FAR and FRR are proposed. FAR - false acception rate - determines the percentage of situations when the system allows access to a user who is not registered in the database. FRR - false rejection rate - determines the percentage of situations when the system denies access to a user with correct biometric data. There are other characteristics used in the selection of biometric identification systems. They are the ease of use, the speed of the system, the influence of environmental factors on it, the cost of the system and others.*

Results. *The following well-known static identification methods are considered: fingerprint identification method, eye retina identification method, eye iris identification method, face geometry identification method as well as a hand vein identification method. The comparative characteristics of each of them are given. This new method is proposed to increase the accuracy and speed of biometric identification.*

Conclusion. *The article analyzes the modern biometric identification tools of static type. Various parameters for determining the effectiveness of bio-metric identification methods are considered. The principles, on which each of these methods is based, as well as the main advantages and disadvantages, are presented.*

Key words: *identification; biometrics; method; scanner; false rejection rate; false acception rate.*

Conflict of interest: *The Authors declare the absence of obvious and potential conflicts of interest related to the publication of this article.*

For citation: Kalutskiy I.V., Matiushin Y.S., Spevakova S.V. Analysis of Modern Static Methods of Biometric Identification. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta = Proceedings of the Southwest State University*. 2019; 23(1): 84-94 (in Russ.). **DOI:** 10.21869/2223-1560-2019-23-1-84-94.

***

Введение

В современных системах сбора данных используются мобильные автоматизированные устройства, данные из которых в зашифрованном виде поступают в центр обработки данных (ЦОД)

[1]. Так как в ЦОД содержится большое количество уязвимой информации, актуальной является задача её защиты.

Одним из методов защиты информации является идентификация пользователей с помощью биометрических данных. Они обладают рядом преимуществ. Так, при идентификации пользователь может забыть пароль, пароль может стать известным посторонним лицам, физический ключ может быть утерян или украден. С другой стороны, биометрические методы основаны не на факте знания некоторой информации или обладания некоторым физическим ключом, а на определении уникальных свойств, присущих организму пользователя [2]. Биометрические данные сложно скомпрометировать и достаточно сложно утратить, что обеспечивает высокую надёжность биометрических методов идентификации.

Постановка задачи

Цель работы: на основе анализа современных методов биометрической идентификации предложить адаптированный к использованию в автоматизированных системах сбора данных с мобильных постов метод.

Для достижения поставленной цели необходимо решить следующие задачи:

1. Провести анализ известных методов и выявить количественные характеристики для их сравнения.

2. Провести сравнение и выявить недостатки методов идентификации.

3. Для устранения выявленных недостатков предложить метод биометрической идентификации, позволяющий повысить выявленные характеристики и пригодный для использования в автоматической системе сбора данных с мобильных постов.

Для определения эффективности методов идентификации введём два параметра – КЛП и КЛО.

- КЛП (коэффициент ложного пропуска) означает вероятность того, что система предоставит доступ пользователю, не имеющему на это право (т.е. не обладающему корректными биометрическими данными);
- КЛО (коэффициент ложного отказа) означает вероятность того, что система ошибочно откажет в доступе пользователю, имеющему право на доступ.

Естественно, чем ниже показатели КЛП и КЛО, тем точнее система распознаёт пользователя.

Кроме собственно параметров эффективности, стоит выделить и другие характеристики, важные при подборе системы идентификации. К ним относятся простота установки и использования системы, подверженность системы влиянию факторов внешней среды, быстродействие, стоимость применения и др. [3].

Анализ основных статических методов идентификации

Методы биометрической идентификации делятся на статические и динамические. Статические методы, в отличие от динамических, основаны на врождённых характеристиках человека, практически не изменяющихся в течение всей жизни, поэтому эти признаки позволяют построить более устойчивую

систему биометрической идентификации [4].

Рассмотрим основные статические методы идентификации, применяемые в настоящий момент.

Метод установления личности по отпечатку пальца, также известный как дактилоскопия, является наиболее распространённым методом биометрической идентификации. Его применение основано на факте уникальности рисунка папиллярных узоров на кончиках пальцев каждого человека. Суть метода заключается в следующем: пользователь прикладывает палец к специальному сканеру, затем полученные данные об отпечатке пальца преобразуются в цифровой код и сравниваются с кодами, имеющимися в базе данных системы идентификации. Весь процесс занимает не более 1 секунды [5].

Преимуществами метода являются достаточно высокая достоверность, низкая стоимость сканирующих устройств и относительная простота в применении. Также есть возможность существенно повысить точность распознавания, используя сканирование нескольких отпечатков пальца одного и того же пользователя. Основной недостаток метода связан с его неустойчивостью к шумам, вызванным различными повреждениями отпечатков пальцев.

В методе идентификации по сетчатке глаза используется сканирование рисунка капиллярных сосудов на поверхности сетчатки. Такой рисунок является уникальным для каждого человека и не меняется на протяжении всей жизни. Для применения данного метода в глаз пользователя направляется луч инфракрасного излучения низкой интенсивности, и одновременно система делает снимок глаза. Далее на основе сделанного снимка система кодирует уникальные свойства рисунка капилляров и сравнивает полученный код с уже имеющимися в базе данных. Так как для корректной работы системы идентификации требуется высокое качество снимка глаза, идентификация не произойдёт до тех пор, пока не будет получен снимок необходимого качества.

Данный метод долгое время считался наиболее надёжным среди всех биометрических методов. Однако у него есть и свои недостатки. Так, для корректной работы сканера пользователь должен смотреть в «глазок» системы в течение нескольких секунд, что не всегда удобно. Кроме того, метод может не работать при наличии у пользователя определённых заболеваний (в частности, катаракты). Наконец, системы идентификации, использующие данный метод, являются достаточно сложными и дорогостоящими [6].

Существует и другой метод идентификации пользователя по глазу – идентификация по радужной оболочке. Как и рисунок капиллярных сосудов на поверхности сетчатки, рисунок радужной оболочки является уникальной и неизменной характеристикой каждого человека. Для получения изображения радужной оболочки используется циф-

ровая камера вместе с инфракрасным освещением. Полученный снимок анализируется с помощью сканера, выделяющего более 200 точек, по которым и происходит сравнение [7].

Данный метод обладает множеством достоинств. В первую очередь, для него характерна высокая точность распознавания пользователя. При необходимости ещё большего повышения точности возможно использование системы, сканирующей оба глаза пользователя, так как даже у одного и того же человека радужные оболочки правого и левого глаза отличаются друг от друга. Кроме того, при использовании данного метода отсутствует необходимость в физическом контакте пользователя со сканером, что может быть важно по соображениям гигиены. Наконец, сама по себе радужная оболочка глаза не только является неизменной на протяжении всей жизни человека, но и практически не подвержена риску повреждений (в отличие от, например, отпечатка пальца).

Недостатком метода является его потенциальная опасность для глаз, поскольку съемка может привести к снижению зрения. Кроме того, точность распознавания может достаточно сильно снижаться в зависимости от таких показателей, как освещение и самочувствие пользователя.

Система идентификации по геометрии лица анализирует такие характеристики лица, как расстояние между глазами, ширина носа, расположение скул, форма рта и другие. Идентификация пользователя происходит на основании совокупности множества характеристик [8].

Хронологически 2D-распознавание лица является одним из первых методов биометрической идентификации, и оно значительно уступает более поздним методам по показателям надёжности. Кроме того, корректной работе системы распознавания может помешать ряд факторов. Так, система может не сработать при плохом освещении, ей может помешать наличие очков или других предметов, частично скрывающих лицо пользователя. Некоторые системы распознавания лица также требуют нейтрального выражения лица пользователя для корректной работы. Однако у системы идентификации по геометрии лица есть и свои преимущества. Так, в отличие от большинства других биометрических методов, данный метод не требует от пользователя практически никаких особенных действий (например, приложить палец к сканеру или посмотреть в него). Кроме того, с помощью данного метода возможно распознавание личности на расстоянии и даже без ведома самого объекта распознавания, что крайне важно для обеспечения безопасности объектов, требующих повышенной охраны, к которым относятся и ЦОД.

В последнее время получил распространение метод идентификации, основанный на уникальности рисунка вен руки. В системах, использующих данный метод, используется инфракрасная камера. Так как гемоглобин, содержа-

щийся в крови, способен поглощать инфракрасное излучение, вены на снимке, сделанном с помощью инфракрасной камеры, выглядят как тёмные линии. На основе сделанного снимка специальной программой создаётся цифровая свёртка, которая и используется для идентификации [9].

У этого метода есть ряд достоинств. Так, рисунки вен рук разных людей имеют между собой больше различий, чем отпечатки пальцев, что обеспечивает более высокую точность распознавания пользователя. Кроме того, подделка рисунка вен другого человека считается практически невозможной, так как вены руки находятся под кожей, и для считывания их рисунка необходимо инфракрасное излучение. Также стоит отметить, что при применении данного метода от пользователя не требуется как прикасаться к сканеру, так и смотреть в «глазок», т.е. объектив камеры. Это делает данный метод более предпочтительным с точки зрения гигиены, а также более комфортным для пользователя. К недостаткам метода можно отнести чувствительность сканеров рисунка вен к засветке галогеновыми лампами и попаданию прямого солнечного света. Также работу сканера сильно затрудняют определённые заболевания сердечно-сосудистой системы, в частности, артрит и некоторые формы анемии [10].

В результате анализа были получены характеристики КЛП и КЛО рассмотренных методов биометрической идентификации, представленные в таблице 1.

Таблица 1

Количественные характеристики основных статических методов биометрической идентификации

Название метода	КЛП, %	КЛО, %
Идентификация по отпечатку пальца	0,001	0,6
Идентификация по радужной оболочке глаза	0,000001	0,016
Идентификация по сетчатке глаза	0,0001	0,4
Идентификация по геометрии лица	0,1	2,5
Идентификация по венам руки	0,0008	0,01

Для большей достоверности и устранения выявленных недостатков рекомендуется применять усовершенствованный метод, основанный на методе идентификации по геометрии лица. Предлагаемый метод позволяет строить 3D-модель лица человека на основе 2D-изображений.

Материалы и методы решения задачи

В методе используются два алгоритма: первый алгоритм решает задачу получения цифрового слепка лица по планарному изображению и сохранения его в базу; второй алгоритм выполняет

проверку отличительных признаков субъекта по шаблонам из базы данных.

Алгоритм получения шаблонов (т.е. слепков) использует методику распознавания с помощью сеток. Однако в отличие от большинства подобных алгоритмов, он не использует затенение субъекта через световой фильтр. Вместо этого используется метод двойного цифрового кодирования, в котором применяются цветовые фильтры красного и зелёного цветов, при этом вертикальные линии фильтра имеют красный оттенок, а горизонтальные – зелёный. После того, как все необходимые подготовительные операции завершены, камера фотографирует пользователя. При помощи специального драйвера изображение попадает на компьютер и далее анализируется программой. В процессе анализа выделяются номера каждой из линий, которая нанесена на лицо пользователя. Характер отклонений линии говорит о рельефе поверхности лица. Самоочевиден тот факт, что для двух разных субъектов линии с одинаковыми номерами будут иметь разную кривизну и как следствие будут непохожи друг на друга.

Блок-схема алгоритма идентификации по сравнению цифровых слепков лица представлена на рисунке.

В результате программного анализа получается массив, содержащий номера линий и их положение на планарном изображении. Данный массив и будет являть собой совокупность информационных признаков о том, каким был рельеф исходного трехмерного объекта.

Алгоритм проверки признаков сравнивает полученный массив с эталонами, находящимися в базе данных. Для этого осуществляется поиск всех файлов в базе, размеры слепка которых совпадают с анализируемым. Далее производится центрирование изображений друг относительно друга – это сделано для того, чтобы даже если объект повернет голову на некоторый градус, или переместится чуть левее или правее, или наклонит голову, сравнение все равно завершилось успехом. После центрирования изображений относительно друг друга происходит подсчет дельт по ширине и высоте, чтобы в дальнейшем сравнивать изображения простым проходом по ширине и высоте. Сравнение выполняется следующим образом: происходит проход по анализируемому изображению и одновременный проход со смещением по эталонному. За каждое несовпадение данных в одном из каналов начисляется одна ошибка. Если в итоге количество ошибок не превышает 20% от общего количества пикселей, то изображение считается идентичным эталонному.

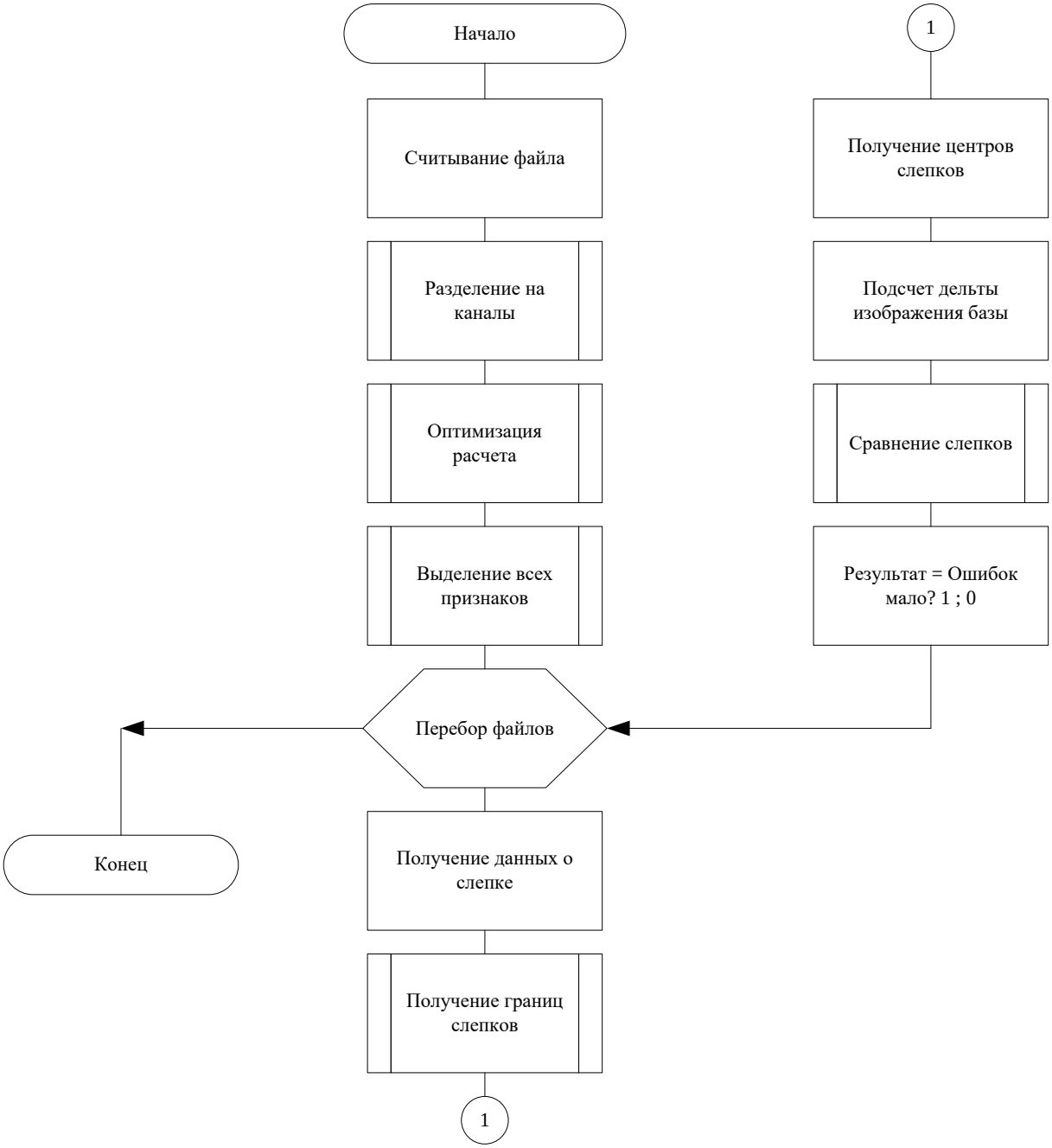

Рис. Блок-схема алгоритма идентификации по сравнению цифровых слепков лица

Результаты и их обсуждение

Было проведено численное моделирование предложенного метода. В ходе моделирования были измерены характеристики КЛО и КЛП, демонстрируемые данным методом при различных внешних условиях. Среди внешних условий, осложняющих получение достоверного результата, были поворот головы субъекта, съёмка при низкой освещённости, а также изменение внешности субъекта с помощью очков и бороды. Характеристики данного метода, полученные экспериментально, представлены в таблице 2.

Таблица 2

Достоверность предложенного метода в зависимости от изменения внешних условий

	При оптимальных условиях	Поворот головы	Низкая освещённость	Изменение внешности (очки, борода)
КЛП, %	0,0005	0,0012	0,0008	0,0017
КЛО, %	0,1	0,2	0,15	0,3

Выводы

Предложенный метод значительно повышает точность распознавания субъектов. Так, при оптимальных условиях КЛО и КЛП предложенного метода соответственно в 25 и в 200 раз меньше аналогичных характеристик стандартного метода идентификации по геометрии лица. Как следствие, предложенный метод позволяет гораздо более качественно проводить идентификацию личности человека.

Кроме достаточно высоких показателей достоверности, у предложенного метода есть и другие достоинства. Так, для его использования не требуется приобретение и установка специального оборудования. Достаточно использовать видеокамеры и специальное программное обеспечение.

Вместе с тем авторы статьи не считают, что предложенный метод, как и любой другой метод, основанный на идентификации пользователя по биометрическим признакам, должен использоваться в защите информации ЦОД в качестве основного. Более надёжным представляется вариант использования данного метода в комбинации с небиометрическим методом идентификации, например, использованием ключа или пароля.

Список литературы

1. Спеваков А.Г., Фисун А.П. Основы правового обеспечения информационной безопасности. Курск, 2013. Ч. 2. 303 с.

2. Спеваков А.Г. Таныгин М.О., Панищев В.С. Информационная безопасность. Курск, 2017. 196 с.

3. Спеваков А.Г. Методы идентификации личности человека по морфологическим признакам // Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2017: сб. ст. конф. Курск, 2017. С. 53-54.

4. Чеснокова А.А., Калуцкий И.В., Спеваков А.Г. Электронный документооборот: безопасность на этапах внедрения и эксплуатации // Известия Юго-Западного государ-

ственного университета. Серия: Управление, вычислительная техника, информатика. Медицинское приборостроение. 2017. Т. 7. №4(25). С. 13-23.

5. Обезличивание персональных данных при обработке в автоматизированных информационных системах / А.Г. Спеваков, И.В. Калуцкий, Д.А. Никулин, В.А. Шумайлова. М.: Телекоммуникации, 2016. С. 16-20.

6. Спеваков А.Г., Рубанов А.Ф. Стереоскопическая оптико-электронная система слежения // Известия высших учебных заведений. Приборостроение. 2005. №2. С. 62-67.

7. Спеваков А.Г., Ширабакина Т.А. Выделение контура объекта на основе нечеткой логики // Медико-экологические информационные технологии: сб. ст. конф. Курск, 2000. С. 149-151.

8. Спеваков А.Г., Рубанов А.Ф., Дегтярев С.В. Система обнаружения объектов изображения и выделения их контуров // Датчики и преобразователи информации систем измерения, контроля и управления: сб. ст. конф. М., 2001. С. 147-148.

9. Спеваков А.Г., Дегтярев С.В. Устройство выделения контуров изображения объекта на основе нечеткой логики // Алгоритмы, методы и системы обработки данных. Муром, 2000. С. 46-48.

10. Спевакова С.В., Применко Д.В. Метод обезличивания персональных данных в автоматизированных системах // Оптико-электронные приборы и устройства в системах распознавания образов, обработки изображений и символьной информации. Распознавание – 2017: сб. ст. конф. Курск, 2017. С. 330-333.

Поступила в редакцию 09.01.2019
Подписана в печать 06.02.2019

Reference

1. Spevakov A.G., Fisun A.P. Osnovy pravovogo obespechenija informacionnoj bezopasnosti. Kursk, 2013, 303 p.

2. Spevakov A.G., Tanygin M.O., Panishhev V.S. Informacionnaja bezopasnost'. Kursk, 2017, 196 p.

3. Spevakov A.G. Metody identifikacii lichnosti cheloveka po morfologicheskim priznakam. Optiko-jelektronnye pribory i ustrojstva v sistemah raspoznavanija obrazov, obrabotki izobrazhenij i simvol'noj informacii. Raspoznavanie – 2017. Sb. st. konf. Kursk, 2017, pp. 53-54.

4. Chesnokova A.A., Kaluckij I.V., Spevakov A.G. Jelektronnyj dokumentooborot: bezopasnost' na jetapah vnedrenija i jekspluatacii. *Izvestiya Yugo-Zapadnogo gosudarstvennogo universiteta. Seriya: Upravlenie, vychislitel'naja tehnika, informatika. Medicinskoe priborostroenie,* 2017, vol. 7, no. 4, pp. 13-23.

5. Spevakov A.G., Kaluckij I.V., Nikulin D.A., Shumajlova V.A. Obezlichivanie personal'nyh dannyh pri obrabotke v avtomatizirovannyh informacionnyh sistemah. Moscow, Telekommunikacii Publ., 2016, pp. 16-20.

6. Spevakov A.G., Rubanov A.F. Stereoskopicheskaja optiko-jelektronnaja sistema slezhenija. *Saint-Petersburg Izvestija vysshih uchebnyh zavedenij. Priborostroenie*, 2005, no.2, pp. 62-67.

7. Spevakov A.G., Shirabakina T.A. Vydelenie kontura ob#ekta na osnove nechetkoj logiki. Mediko-jekologicheskie informa-cionnye tehnologii. Sb. st. konf. Kursk, 2000, pp. 149-151.

8. Spevakov A.G., Rubanov A.F., Degtjarev S.V. Sistema obnaruzhenija ob#ektov izobrazhenija i vydelenija ih konturov. Datchiki i preobrazovateli informacii sistem izmerenija, kontrolja i upravlenija. Sb. st. konf. Moscow, 2001, pp. 147-148.

9. Spevakov A.G., Degtjarev S.V. Ustrojstvo vydelenija konturov izobrazhenija ob#ekta na osnove nechetkoj logiki. Algoritmy, metody i sistemy obrabotki dannyh. Murom, 2000, pp. 46-48.

10. Spevakova S.V., Primenko D.V. Metod obezlichivanija personal'nyh dannyh v avtomatizirovannyh sistemah. Optiko-jelektronnye pribory i ustrojstva v sistemah raspoznavanija obrazov, obrabotki izobrazhenij i simvol'noj informacii. Raspoznavanie – 2017. Sb. st. konf. Kursk, 2017, pp. 330-333.

Received 09.01.2019
Accepted 06.02.2019

Информация об авторах / Information about the Authors

Игорь Владимирович Калуцкий, кандидат технических наук, доцент, ФГБОУ ВО «Юго-Западный государственный университет»**,** Курск, Российская Федерация
e-mail: igor_kalutsky@mail.ru

Igor V. Kalutskiy, Candidate of Engineering Sciences, Associate Professor, Southwest State University, Kursk, Russian Federation
e-mail: igor_kalutsky@mail.ru)

Юрий Сергеевич Матюшин, студент, ФГБОУ ВО «Юго-Западный государственный университет»**,** Курск, Российская Федерация
e-mail: steelrat116@gmail.com

Yuriy S. Matiushin, Student, Southwest State University, Kursk, Russian Federation
e-mail: steelrat116@gmail.com)

Светлана Викторовна Спевакова, аспирант, ФГБОУ ВО «Юго-Западный государственный университет»**,** Курск, Российская Федерация,
e-mail: sspev@yandex.ru

Svetlana V. Spevakova, Post-Graduate Student, Southwest State University,
Kursk, Russian Federation,
e-mail: sspev@yandex.ru)