УДК 004.056

*Е. К. Брагина, С. С. Соколов*

**СОВРЕМЕННЫЕ МЕТОДЫ БИОМЕТРИЧЕСКОЙ АУТЕНТИФИКАЦИИ:  
ОБЗОР, АНАЛИЗ И ОПРЕДЕЛЕНИЕ ПЕРСПЕКТИВ РАЗВИТИЯ**

Исследуется проблема минимизации возможности получения несанкционированного доступа к информации. Рассматривается понятие процесса аутентификации и его виды. Описаны статические и динамические методы биометрической аутентификации, основанные на использовании таких биометрических характеристик, как отпечаток пальца, радужная оболочка глаза, сетчатка глаза, геометрия руки, геометрия лица, термограмма лица, голос и рукописный почерк. Выявлены достоинства динамических методов биометрической ау­тентификации. По результатам анализа данных методов предложено использовать в качест­ве биометрической характеристики мимику лица человека. Сделан вывод о том, что наибо­лее современным и перспективным методом биометрической аутентификации является оценка эмоционального состояния и мимики путем постоянного скрытого мониторинга при помощи web-камеры. Перспективой исследований в области развития данного метода био­метрической аутентификации является разработка математического аппарата, методов и технологий алгоритмического, информационного и программного обеспечения в данной предметной области. Развитие математического аппарата должно быть основано на исполь­зовании методов локальных бинарных шаблонов и *^*--ближайших соседей. Метод, основан­ный на оценке эмоционального состояния и мимики, является наиболее перспективным, од­нако исследования в этой области в настоящее время находятся на стадии развития, что не даёт полного представления обо всех возможностях применения метода.

**Ключевые слова**: идентификация, аутентификация, биометрическая аутентификация, биометрические характеристики, статические методы, динамические методы.

Введение

В настоящее время неотъемлемой частью различных сфер деятельности человека стало использование информационных систем. Огромное количество информации ограниченного доступа переносится, хранится и обрабатывается в информационных системах, что формирует потребность в обеспечении их информационной защищенности [1-2].

Защита информации в информационных системах обеспечивается созданием комплексной системы защиты, одной из главных составляющих которой являются методы защиты от несанкцио­нированного доступа (НСД). Согласно результатам глобального исследования по вопросам обеспе­чения информационной безопасности, проведенного международной сетью компаний PricewaterhouseCoopers в начале 2015 г., лишь 55 % респондентов осуществляют мониторинг несанкционированного использования или НСД. При этом только 20 % бюджета, выделенного на обеспечение информационной безопасности, отводится на приобретение средств блокировки НСД и 20 % - на приобретение средств обнаружения НСД [3].

Основой программно-технических средств защиты от НСД являются процедуры идентифи­кации (пользователь называет себя) и аутентификации (проверки подлинности) пользователей [4].

Процесс аутентификации пользователя возможен по предъявлении:

* знания чего-либо (пароль, личный номер и т. п.);
* владения чем-либо (карточка, ключ и т. п.);
* части самого пользователя (биометрические характеристики) [5].

Самым распространенным методом аутентификации пользователей по предъявлении зна­ния чего-либо является аутентификация с использованием специальной информации (пароля). Данный метод является простым как для использования, так и для атак, предпринимаемых зло­умышленниками.

Аутентификация по предъявлении чего-либо, чем владеет пользователь, имеет сходные недостатки, и, кроме того, добавляется риск передачи, утери, кражи или копирования ключа.

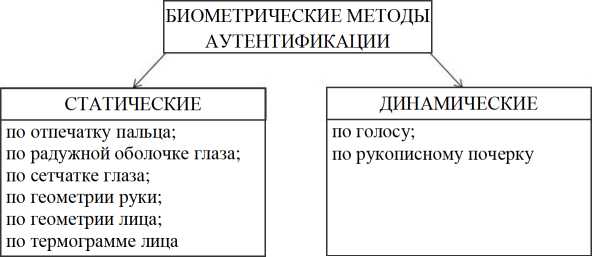
Биометрическая аутентификация и биометрические характеристики

Биометрическая аутентификация или аутентификация на основе биометрических характе­ристик имеет следующие преимущества:

* удобно использовать благодаря отсутствию необходимости контакта;
* невозможно потерять или забыть, т. к. биометрические характеристики являются частью идентифицируемого пользователя;
* значительно затруднены передача и подделка биометрических характеристик.

Биометрическая аутентификация является перспективным направлением, позволяющим ре­шить ряд задач, которые возникают при использовании традиционных процедур аутентификации.

В настоящее время существуют два класса методов биометрической аутентификации: ос­нованные на статических методах и основанные на динамических методах (рис.) [6].



Биометрические методы аутентификации

Статические методы биометрической аутентификации

Статические методы основаны на биометрических характеристиках человека, которые присутствуют у него от рождения. Такие характеристики не могут быть утеряны, украдены или забыты.

Аутентификация *по отпечатку пальца* - линии, образующие кожные узоры на пальцах, обладают следующими свойствами: индивидуальность, относительная устойчивость, восстанав­ливаемость. Существует несколько методов получения отпечатков пальцев: оптические, ёмко­стные, радиочастотные, ультразвуковые, давления, температурные [7].

Аутентификация *по радужной оболочке глаза* является одним из наиболее надёжных спосо­бов. Радужная оболочка глаза каждого человека имеет особую уникальную структуру. Преимуще­ство данного способа заключается в том, что методы идентификации являются бесконтактными.

Аутентификацию *по сетчатке глаза,* в зависимости от применяемого алгоритма, подраз­деляют на два типа: использующие алгоритмы сегментации и извлекающие признаки с изобра­жения сетчатки. Данный метод имеет значительный недостаток - движение головы или глаза во время сканирования, что с большой вероятностью может привести к ошибкам первого («своего» принимаем за «чужого») и второго рода («чужого» принимаем за «своего») [8].

В ходе аутентификации *по геометрии руки* используется сканирование формы кисти руки (изгибы, длина, толщина пальцев; ширина и толщина тыльной стороны руки; расстояние между суставами и структура кости). Данный метод не является безошибочным из-за чувствительности сканеров к проявлениям различных заболеваний суставов.

Аутентификация *по геометрии лица* отличается наиболее сложной технической реализа­цией. Метод основан на построении трёхмерной модели человеческого лица, для этого выделя­ются контуры различных элементов лица, вычисляется расстояние между ними. Для определе­ния уникального шаблона необходимо от 12 до 40 характерных элементов. Уникальный шаблон должен учитывать множество вариаций изображения.

Аутентификация *по термограмме лица* - метод, в настоящее время не имеющий широко­го распространения. Наиболее устойчивой среди биометрических характеристик лица является изображение кровеносных сосудов. Метод основан на создании температурной карты (термо­граммы) путём сканирования лица в инфракрасном свете. Исследованиями доказано, что термо­грамма лица является уникальной биометрической характеристикой.

Неизменяемость и открытость биометрических характеристик, используемых в статиче­ских методах, допускают подделку биометрического ключа. Вследствие этого ряд преимуществ имеет использование динамических методов биометрической аутентификации.

Динамические методы биометрической аутентификации

Динамические методы основываются на поведенческих характеристиках людей [9].

В настоящее время широко используется аутентификация *по голосу.* Основными преиму­ществами данного метода являются простота в использовании и реализации, общедоступность и наличие множества способов построения шаблона. Однако существует и множество проблем, связанных с изменчивостью голоса вследствие влияния различных факторов (состояние здоро­вья, возраст, настроение). Сам процесс обработки голоса разбивают на следующие этапы: пре­добработка сигнала, выделение критериев, распознавание [10, 11].

Аутентификация *по рукописному почерку* основана на специфике движений руки при подпи­сании документов. Выделяют два способа обработки данных о подписи: анализ самой подписи, ана­лиз динамических характеристик написания. Ведутся также исследования аутентификации пользо­вателя по клавиатурному почерку, что, несомненно, имеет перспективы дальнейшего развития.

Традиционно биометрическая аутентификация *по геометрии лица* относится к классу, ос­нованному на статических методах. Принято также считать, что геометрия лица обладает низ­кой уникальностью, что впоследствии приводит к значительным ошибкам первого и второго рода [12, 13].

Следует отметить, что даже если первичная аутентификация прошла без ошибок и систе­ма приняла «своего» за «своего», это не даст 100 % защиты информации [14, 15].

Современные методы биометрической аутентификации

Наиболее современным и перспективным методом биометрической аутентификации яв­ляется *оценка эмоционального состояния и мимики человека* путем постоянного скрытого мони­торинга при помощи web-камеры [16].

Эмоциональное состояние и мимика человека постоянно меняются в зависимости от внешних и внутренних факторов. При этом выражение эмоций - это неосознанный процесс (че­ловек не несёт ответственности за свое эмоциональное состояние) [17], что практически исклю­чает возможность сокрытия и подмены этой биометрической характеристики.

Лицо человека, готового к атаке на информационную систему, будет выражать опреде­ленные эмоции, которые будут отличаться от повседневных. С учетом этого обоснованным яв­ляется изучение изменения эмоционального состояния и мимики пользователей для снижения вероятности ошибок первого и второго рода, а также повышения защищенности информации при попытке нанесения вреда сотрудниками, которые успешно прошли процедуры идентифика­ции и аутентификации.

При проведении исследований в области развития современных методов биометрической аутентификации перспективным является развитие математического аппарата, методов и техно­логий алгоритмического, информационного и программного обеспечения в данной предметной области [18, 19].

Развитие математического аппарата должно быть основано на использовании методов ло­кальных бинарных шаблонов (Local Binary Patterns (LBP)) и *k*-ближайших соседей.

Метод LBP представляет собой описание окрестности пикселя изображения в двоичной форме для получения восьмиразрядного бинарного кода. В качестве порога принимается цен­тральный пиксель. Пиксели, значения которых больше, чем значение центрального пикселя или равные ему, принимают значение «1», пиксели, значения которых меньше значения центрально­го, принимают значение «0» [20].

Метод *k*-ближайших соседей - это метод, относящий объекты к классу, которому принад­лежит большинство из *k* его ближайших соседей в многомерном пространстве признаков. Число *k* - это количество соседних объектов в пространстве признаков, которое сравнивается с клас­сифицируемым объектом [21].

Построение алгоритмических структур представляется целесообразным в части структу­рирования следующих процедур:

* установления минимального и максимального порога биометрической характеристики;
* определения устойчивости биометрической характеристики пользователя в зависимости от стабильности его эмоционального состояния и мимики;
* установления минимальных и максимальных пределов, в которых будет работать алго­ритм повышения защищенности информации;
* вычисления «пропускного коридора» и среднего значения для каждой биометрической характеристики пользователя;
* разработки алгоритма повышения защищенности информации на основе оценки эмо­ционального состояния и мимики;
* создание биометрического ключа пользователя.

Разработка информационного и программного обеспечения представляет собой автомати­зацию и информационное сопровождение таких процессов, как идентификация и аутентификация.

Заключение

По результатам обзора и анализа современных методов биометрической аутентификации можно сделать вывод о том, что метод, основанный на оценке эмоционального состояния и мимики, является наиболее перспективным, т. к. его использование снижает вероятность возникновения ошибок первого и второго рода, тем самым повышая защищенность информационных систем. Пол­ное представление обо всех возможностях применения данного метода составить пока сложно, вследствие того, что исследования в этой области в настоящее время находятся на стадии развития.

*СПИСОК ЛИТЕРАТУРЫ*

1. *Нырков А. П.* Мультисервисная сеть транспортной отрасли / А. П. Нырков, С. С. Соколов,
2. С. Белоусов // Вестн. компьютерных и информационных технологий. 2014. № 4 (118). С. 33-38.
3. *Нырков А. П.* Обеспечение безопасного функционирования мультисервисной сети транспортной отрасли / А. П. Нырков, С. С. Соколов, А. С. Белоусов // Докл. Томск. гос. ун-та систем управления и ра­диоэлектроники. 2014. № 2 (32). С. 143-149.
4. *Глобальное* исследование по вопросам обеспечения информационной безопасности. Перспективы на 2015 год // URL: <http://www.pwc.ru/ru/riskassurance/publications/managing-cyberrisks.html> (дата обраще­ния: 28.03.2016).
5. *Методы* и средства защиты от несанкционированного доступа // URL: <http://www.panasenko.ru/> Articles/77/77.html (дата обращения: 31.03.2016).
6. *Идентификация* и аутентификация, управление доступом // URL: <http://citforum.ru/security/articles/> galatenko (дата обращения: 27.03.2016).
7. *Биометрические* системы аутентификации // URL: [https://ru.wikipedia.org/wiki/Биометрические\_](https://ru.wikipedia.org/wiki/%d0%91%d0%b8%d0%be%d0%bc%d0%b5%d1%82%d1%80%d0%b8%d1%87%d0%b5%d1%81%d0%ba%d0%b8%d0%b5_) системы\_аутентификации#Л0.А1Л 1.82.D0.B0.D 1.82.D0.B8.D 1.87.D0.B5.D 1.81 .D0.BA.D0.B8.D0.B5\_.D0. BC.D0.B5.D1.82.D0.BE.D0.B4.D1.8B (дата обращения: 28.03.2016).
8. *Гуреева О.* Биометрическая идентификация по отпечаткам пальцев. Технология FingerChip // Компо­ненты и технологии. 2007. № 4 С. 176-180 // URL: <http://www.kit-e.ru/assets/files/pdf/2007_04_176.pdf>.
9. *Методы* аутентификации по сетчатке глаза // URL: <https://habrahabr.ru/post/261309/> (дата обраще­ния: 01.04.2016).
10. *Динамические* методы биометрической аутентификации личности // URL: <http://re.mipt.ru/infsec/>

2006/essay/2006\_Dynamic\_biometric\_authentification Cherkezov.pdf (дата обращения: 28.03.2016).

1. *Щемелинин В. Л.* Исследование устойчивости голосовой верификации к атакам, использующим систему синтеза / В. Л. Щемелинин, К. К. Симончик // Изв. высш. учеб. завед. Приборостроение. 2014. Т. 57, № 2. С. 84-88.
2. *Тассов К. Л.* Метод идентификации человека по голосу / К. Л. Тассов, Р. А. Дятлов // Инженер­ный журнал: наука и инновации. 2013. Вып. 6 // URL: <http://engjournal.ru/catalog/it/biometric/1103.html>.
3. *Выскуб В. Г.* Возможности повышения точности биометрических распознающих систем /
4. Г. Выскуб, И. В. Прудников // Инженерная физика. 2009. Вып. 5. С. 41-43.
5. *Маркелов К. С.* Биометрические информационные технологии: актуальные и перспективные ме­тоды / К. С. Маркелов, В. В. Нечаев // Информационные и телекоммуникационные технологии. 2013. № 18. С. 24-42.
6. *Шибанов С. В.* Сравнительный анализ современных методов аутентификации пользователя /
7. В. Шибанов, Д. А. Карпушин // Математическое и программное обеспечение систем в промышленной и социальной сферах. 2015. № 1. С. 33-37.
8. *Соколов С. С.* Построение защищенной информационной системы персональных данных монито­рингового центра оказания телематических услуг безопасности на транспорте / С. С. Соколов, С. С. Малов, А. С. Карпина // Вестн. Гос. ун-та морского и речного флота им. адм. С. О. Макарова. 2014. № 5. С. 148-157.
9. *Майоров А. В.* Особенности технологии биометрической защиты программного обеспечения / А. В. Майоров // Науч.-техн. конф. молодых специалистов ФГУП «ПНИЭИ». Пенза, 2009. 7 с.
10. *Экман П.* Психология эмоций. Я знаю, что ты чувствуешь / П. Экман. СПб.: Питер, 2010. 180 с.
11. *ГОСТ Р* ИСО/МЭК 197194-5-2006. Автоматическая идентификация. Идентификация биометриче­ская. Форматы обмена биометрическими данными. Часть 5. Данные изображения лица // URL: <http://snipov.net/database/c_3944567195_doc_4293849863.html>.
12. *Хомяков М. Ю.* Принципы построения пакета программ для моделирования систем распознава­ния изображений лиц / М. Ю. Хомяков, Г. А. Кухарев // Изв. Санкт-Петербург. гос. электротехн. ун-та «ЛЭТИ». 2010. № 7. С. 41-46.
13. *Локальные* бинарные шаблоны // URL: ЬПр8://ги.’так1реб1а.огд^1к1/Локальные\_бинарные\_шаблоны (дата обращения: 06.04.2016).
14. *Метод k*-ближайших соседей // URL: <https://basegroup.ru/community/glossary/nearest-neighbor> (да­та обращения: 05.04.2016).

Статья поступила в редакцию 22.04.2016

ИНФОРМАЦИЯ ОБ АВТОРАХ

***Брагина Елизавета Константиновна*** *-* Россия, 198035, Санкт-Петербург; Государст­венный университет морского и речного флота им. адмирала С. О. Макарова; доцент кафедры «Комплексное обеспечение информаионной безопасности»; [braginaek@gumrf.ru](mailto:braginaek@gumrf.ru).

***Соколов Сергей Сергеевич*** — Россия, 198035, Санкт-Петербург; Государственный университет морского и речного флота им. адмирала С. О. Макарова; канд. техн. наук, доцент; доцент кафедры «Комплексное обеспечение информационной безопасности»; [SokolovSS@gumrf.ru](mailto:SokolovSS@gumrf.ru).

*E. K. Bragina, S. S. Sokolov*

**MODERN METHODS OF BIOMETRIC AUTHENTICATION:  
REVIEW, ANALYSIS AND DETERMINATION OF OUTLOOK**

**Abstract.** The paper studies the problem of minimization of unauthorized access to informa­tion. The idea of authentication process and its types are considered. The static and dynamic meth­ods of biometric authentication, based on using such biometric parameters as fingerprint, iris, ret­ina, hand geometry, face geometry, face thermogram, voice and manuscript, are described. The ad­vantages of the dynamic methods of biometric authentication are revealed. According to the analy­sis of these methods it is offered to use mimicry of human face as a biometric characteristic. It is concluded that the most modern and perspective method of biometric authentication is an assess­ment of emotional state and mimicry by using permanent secret monitoring with webcam. The per­spective of the research of this method is the development of mathematical apparatus, methods and algorithmic, information and software technologies in the given subject area. The development of the mathematical apparatus should be based on the methods of local binary patterns and *k*-nearest neighbours. The method based on the evaluation of the emotional state and facial expressions is the most promising, however, the researches in this area are now at the stage of the development that does not give a complete picture of all the possibilities of this method.

**Key words**: identification, authentication, biometric authentication, biometric characteristics, static methods, dynamic methods.

*REFERENCES*

1. Nyrkov A. P., Sokolov S. S., Belousov A. S. Mul'tiservisnaia set' transportnoi otrasli [Multi-service net­work of transport sphere]. *Vestnik komp'iuternykh i informatsionnykh tekhnologii,* 2014, no. 4 (118), pp. 33-38.
2. Nyrkov A. P., Sokolov S. S., Belousov A. S. *Obespechenie bezopasnogo funktsionirovaniia mul'tiservisnoi seti transportnoi otrasli* [Maintenance of safe operations of multi-service network of transport sphere]. Doklady Tomskogo gosudarstvennogo universiteta sistem upravleniia i radioelektroniki, 2014, no. 2 (32), pp. 143-149.
3. *Global'noe issledovanie po voprosam obespecheniia informatsionnoi bezopasnosti. Perspektivy na 2015 god* [Global study on the issues of ensuring the information security. Prospects for 2015]. Available at: <http://www.pwc.ru/ru/riskassurance/publications/managing-cyberrisks.html> (accessed: 28.03.2016).
4. *Metody i sredstva zashchity ot nesanktsionirovannogo dostupa* [Methods and means of protection from unauthorized access]. Available at: <http://www.panasenko.ru/Articles/77/77.html> (accessed: 31.03.2016).
5. *Identifikatsiia i autentifikatsiia, upravlenie dostupom* [Identification and authentication, access control]. Available at: <http://citforum.ru/security/articles/galatenko/(accessed>: 27.03.2016).
6. *Biometricheskie sistemy autentifikatsii* [Biometric systems of authentication]. Available at: <https://ru>. wikipedia.org/wiki/Biometricheskie\_sistemy\_autentifikatsii#.D0.A1.D 1.82.D0.B0.D 1.82.D0.B8.D 1.87.D0.B5.D 1.81. D0.BA.D0.B8.D0.B5\_.D0.BC.D0.B5.D1.82.D0.BE.D0.B4.D1.8B (accessed: 28.03.2016).
7. Gureeva O. Biometricheskaia identifikatsiia po otpechatkam pal'tsev. Tekhnologiia FingerChip [Biomet­ric identification by fingerprints. FingerChip technology]. *Komponenty i tekhnologii,* 2007, iss. 4. Available at: <http://www.kit-e.ru/assets/files/pdf/2007_04_176.pdf>.
8. *Metody autentifikatsii po setchatke glaza* [Methods of authentication by retina]. Available at: https:// habrahabr.ru/post/261309/ (accessed: 01.04.2016).
9. *Dinamicheskie metody biometricheskoi autentifikatsii lichnosti* [Dynamic methods of biometric authenti­cation of personality]. Available at: <http://re.mipt.ru/infsec/2006/essay/2006_Dynamic_biometric_authentification__> Cherkezov.pdf (accessed: 28.03.2016).
10. Shchemelinin V. L., Simonchik K. K. Issledovanie ustoichivosti golosovoi verifikatsii k atakam, is- pol'zuiushchim sistemu sinteza [Study of stability of voice verification to attacks, using synthesis system]. *Izves- tiia vysshikh uchebnykh zavedenii. Priborostroenie,* 2014, vol. 57, no. 2, pp. 84-88.
11. Tassov K. L., Diatlov R. A. Metod identifikatsii cheloveka po golosu [Method of identification of per­sonality by voice]. *Inzhenernyi zhurnal: nauka i innovatsii,* 2013, iss. 6. Available at: <http://engjournal.ru/> catalog/it/biometric/1103.html.
12. Vyskub V. G., Prudnikov I. V. Vozmozhnosti povysheniia tochnosti biometricheskikh raspoznaiushchikh sistem [Possibility of increase in the accuracy of biometric identifying systems]. *Inzhenernaia fizika,* 2009, iss. 5, pp. 41-43.
13. Markelov K. S., Nechaev. V. V. Biometricheskie informatsionnye tekhnologii: aktual'nye i perspektivnye metody [Biometric information technologies: actual and perspective methods]. *Informatsionnye i telekommunikatsionnye tekhnologii,* 2013, no. 18, pp. 24-42.
14. Shibanov S. V., Karpushin D. A. Sravnitel'nyi analiz sovremennykh metodov autentifikatsii pol'zovatelia [Comparative analysis of the present methods of authentication of user]. *Matematicheskoe i programmnoe obe- spechenie sistem v promyshlennoi i sotsial'noi sferakh,* 2015, no. 1, pp. 33-37.
15. Sokolov S. S., Malov S. S., Karpina A. S. Postroenie zashchishchennoi informatsionnoi sistemy personal'nykh dannykh monitoringovogo tsentra okazaniia telematicheskikh uslug bezopasnosti na transporte [Design of secured in­formation system of personal data of the monitoring center of telematics services of safety in transport]. *Vestnik Gosu- darstvennogo universiteta morskogo i rechnogo flota imeni admirala S. O. Makarova,* 2014, no. 5, pp. 148-157.
16. Maiorov A. V. Osobennosti tekhnologii biometricheskoi zashchity programmnogo obespecheniia [Pecu­liarities of technology of biometric protection of software]. *Nauchno-tekhnicheskaia konferentsiia molodykh spet- sialistov FGUP «PNIEI».* Penza, 2009. 7 p.
17. Ekman P. *Psikhologiia emotsii. Ia znaiu, chto ty chuvstvuesh'* [Emotional psychology. I know what you feel]. Saint-Petersburg, Piter Publ., 2010. 180 p.
18. *GOST R ISO/MEK 197194-5-2006. Avtomaticheskaia identifikatsiia. Identifikatsiia biometricheskaia. Formaty obmena biometricheskimi dannymi. Chast' 5. Dannye izobrazheniia litsa* [Automatic identification. Biometric identification. Formats of exchange of biometric data. Part 5. Data of human image]. Available at: <http://snipov.net/database/c_3944567195_doc_4293849863.html>.
19. Khomiakov M. Iu., Kukharev G. A. Printsipy postroeniia paketa programm dlia modelirovaniia sistem raspoznavaniia izobrazhenii lits [Principles of designing the packet of software for modeling the systems of iden­tification of human faces]. *Izvestiia Sankt-Peterburgskogo gosudarstvennogo elektrotekhnicheskogo universiteta «LETI»,* 2010, no. 7, pp. 41-46.
20. *Lokal'nye binarnye shablony* [Local binary patterns]. Available at: <https://ru.wikipedia.org/wiki/LokaTnye_> binarnye\_shablony (accessed: 06.04.2016).
21. *Metod k-blizhaishikh sosedei* [Method of k-nearest neighbours]. Available at: <https://basegroup.ru/> community/glossary/nearest-neighbor (accessed: 05.04.2016).

The article submitted to the editors 22.04.2016

INFORMATION ABOUT THE AUTHORS

***Bragina Elizaveta Konstantinovna*** *-* Russia, 198035, Saint-Petersburg; Admiral Makarov State University of Maritime and Inland Shipping; Assistant Professor of the Department "Complex Maintenance of Information Security"; [braginaek@gumrf.ru](mailto:braginaek@gumrf.ru).

***Sokolov Sergey Sergeevich*** - Russia, 198035, Saint-Petersburg; Admiral Makarov State University of Maritime and Inland Shipping; Candidate of Technical Sciences, Assistant Pro­fessor; Assistant Professor of the Department "Comprehensive Information Security"; [SokolovSS@gumrf.ru](mailto:SokolovSS@gumrf.ru).