А.М. Алюшин[1] , С.В. Дворянкин[2]
[1]Национальный исследовательский ядерный университет «МИФИ», Каширское ш., 31, г. Москва, 115409, Россия, e-mail: alyshin@list.ru
[2]Финансовый университет при Правительстве Российской Федерации, Ленинградский проспект, 49, Москва,125993, Россия, e-mail: SVDvoryankin@mephi.ru, ORCIDiD0000-0001-6908-0676

ИСПОЛЬЗОВАНИЕ РЕЧЕВЫХ ТЕХНОЛОГИЙ ДЛЯ ЗАЩИТЫ ДОКУМЕНТООБОРОТА.

DOI: http://dx.doi.org/10.26583/bit.2017.2.01

Аннотация. Несмотря на то, что мы живем в веке информационных технологий, бумажный документооборот не теряет своей актуальности. Выделены основные аспекты защиты документов, связанные с защитой их контекстной и юридической составляющих. К контекстной составляющей отнесен смысловой информационный аспект документа. К юридической – факты и условия создания, утверждения, согласования данного документа конкретными лицами. Показаны актуальность защиты документов в связи с возможными террористическими угрозами и важность для эффективной защиты документов такого фактора, как время выявления фальсификации. Представлен анализ требований к данному фактору для документов различного характера – финансовых, юридических, управляющих. Выделены управляющие документы, используемые для оперативного управления опасными объектами. Показано, что их умышленная фальсификация может привести к возникновению аварий и катастроф техногенного происхождения, а также человеческим жертвам. Дан сравнительный анализ применяющихся в настоящее время на практике методов защиты документов. Выделены биометрические и небиометрические методы защиты документов. Представлен анализ их недостатков. Сделан вывод о перспективности применения технологии защиты документов на основе речевой подписи. Рассмотрены основные этапы обработки голосовой информации при реализации данной технологии. Разработано программное обеспечение, реализующее новую технологию защиты документов от подделок. Сущность предлагаемой технологии заключается в том, что в конец документа добавляется аудиомаркер, хранящий в себе основную информацию защищаемого документа (финансовые аспекты, обязанности сторон, сроки и т.п.). Показано, что изменение текста в этом случае будет порождать необходимость изменения связанного с ним элемента защиты – аудиомаркера. Достоинством подхода является тот факт, что сделать это без автора или собственника документа невозможно, поскольку аудиомаркер хранит в себе биометрические данные указанного лица. Разработано приложение под мобильное устройство с операционной системой android, которое позволяет считывать, распознавать и воспроизводить аудиомаркеры. Проведенные испытания программного комплекса показали его высокую эффективность, в том числе при распознавании аудиомаркеров в условиях различной освещенности. Рассмотрена возможность повышения степени защищенности подлинности документа за счет фиксации в речевой подписи текущего уровня психоэмоционального напряжения автора документа, что может быть использовано для выявления случаев его неадекватного состояния. Это позволяет выявлять случаи составления документов в случае применения физического или психического насилия.

Ключевые слова: спектрограмма, аудиомаркер, распознавание, документация, графическая картинка.

Для цитирования. **АЛЮШИН, Александр М.; ДВОРЯНКИН, Сергей В.** Использование речевых технологий для защиты документооборота. Безопасность информационных технологий, [S.l.], v. 24, n. 2, p. 6-15, june 2017. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/100>. Дата доступа: 07 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.2.01.

Благодарности. Данное исследование выполнено в рамках проекта «Апробация технологии снижения риска возникновения и уменьшение последствий катастроф техногенного происхождения за счет миниёмизации влияния человеческого фактора на надежность и безаварийность работы АЭС и других опасных объектов» в соответствии с госзаданием НИЯУ МИФИ на 2017-2019 гг.

A.M. Alyushin[1] , S.V. Dvoryankin[2]
[1]National Nuclear Research University MEPHI (Moscow Engineering Physics Institute), Kashirskoeshosse, 31, Moscow, 115409, Russia, e-mail: alyshin@list.ru
[2]Finance University under the Government of Russia, Leningradsky Prospekt, 49, Moscow,125993, Russia, e-mail: SVDvoryankin@mephi.ru, ORCID iD0000-0001-6908-0676

The Use of Speech Technology to Protect the Document Turnover

DOI: http://dx.doi.org/10.26583/bit.2017.2.01

Abstract. The wide current paper documents implementation in practice workflows are shown. The basic aspects of document protection related to the protection of their content and legal components are underlined. For contextual component assigned semantic information aspect of the document is considered. For legal component attributed facts and conditions for the creation, approval, negotiation of the document to specific persons is viewed. The documents protection problem importance is shown in connection with possible terrorist threats. The importance of such factor as the time of fraud detection towards the efficiency of documents protection is shown. The fraud detection time requirements for documents of different nature – financial, legal, management is analyzed. The documents used for the operational management of dangerous objects is point out as the most sensitive to the falsification. It is shown that their deliberate falsification can lead to accidents and technogenic catastrophes and human casualties. A comparative analysis of currently used protecting documents methods are presented. Biometric and non-biometric methods of documents protection are point out. The analysis of their short comings are given. The conclusion about the prospects of document protection on the basis of the voice signature technology are done. The basic steps of voice information processing in the implementation of this technology are analyzed. The software that implements a documents counterfeiting new protection technology is proposed. The technology is based on the audiomarkers usage at the end of the document, which contains a general information about it. The technology is applicable to the wide range of documents such as financial and valuable papers, contracts, etc. One of the most important advantages of this technology is that any changes in the document can not be done without the author of the document because audiomarker keeps the biometric data of the person. The developed software is oriented on the mobile applications on the basis of android operating system. The software has a friendly interface, which allows one to create, correct and check audiomarkers. The performed software tests shows its high efficiency, including the possibility of audiomarkers recognition in various lighting conditions. The possibility of document protection level improvement by logging in voice signature the current level of mental and emotional stress of the document author, which can be used to detect its inadequate state is shown. This makes it possible to identify cases of document preparation under the application of physical or mental violence.

Keywords: spectrogram, audiomarker, recognition, documentation, graphic image
For citation. **ALYUSHIN, Alexandr M.; DVORYANKIN, Sergey V.** The Use of Speech Technology to Protect the Document Turnover. IT Security, [S.l.], v. 24, n. 2, p. 6-15, june 2017. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/100>. Date accessed: 07 dec. 2017. doi:http://dx.doi.org/10.26583/bit.2017.2.01.
Acknowledgements: This research was performed in the framework of the project «The Testing of technologies to reduce risk and reduction of consequences of catastrophes of technogenic origin due to minimization of human factor influence on reliability and trouble-free operation of nuclear power plants and other hazardous facilities" in accordance with the state assignment NRNU MEPhI for the 2017-2019.

Введение

Мы живем в веке высоких информационных технологий. Практически все сферы жизнедеятельности человека так либо иначе связаны с компьютерной техникой. Так, еще до рождения человека компьютерные технологии широко используются для медицинских диагностических целей, например, при ультразвуковых исследованиях. Все этапы обучения также непосредственно связаны, либо просто базируются на использовании компьютеров. В настоящее время практически вся медицинская диагностическая техника, весь финансовый документооборот, средства коммуникации базируются на хранении, обработке и передаче информации в цифровом виде.

Но, несмотря на это, бумажного документооборота меньше не становится. Действительно, заключение каких-либо контрактов, договоров или других соглашений все равно фиксируется на бумаге. Практически все финансовые операции также дублируются бумажными носителями. Аналогичным образом обстоит дело и с представлением результатов различного рода проверок, результатов испытаний, тестирований, аттестаций, расследований. А это означает, что вопросы, связанные с защитой документов (как в бумажном виде, так и цифровом) от различного рода фальсификаций и подделок, не потеряли своей актуальности.

Рассматривая проблему защиты документов, следует выделить следующие основные аспекты – защиту контекстной составляющей документов и защиту юридической составляющей. В первом случае речь идет о защите смысловой информационной составляющей документов. Во втором случае – о защите самого факта создания, утверждения, согласования данного документа конкретными лицами.

Особую актуальность вопросы защиты документов приобретают в связи с террористическими угрозами. Так, например, в случае осуществления физического захвата лиц, уполномоченных подписывать какие-либо документы юридического, финансового, технического, а также информационного характера, существующими средствами защиты практически невозможно своевременно обнаружить факты насильственного, то есть сфальсифицированного незаконного создания упомянутых выше документов.

Необходимо отметить, что одним из показателей эффективности применяемой технологии защиты документов является время выявления подделки. Требования к данному фактору могут принципиальным образом отличаться для различных документов. Так, требования к данному фактору для некоторых юридических документов, например, прав на недвижимую собственность, могут быть достаточно мягкими, так как собственность такого рода не может быть физически перемещена, либо спрятана быстро. По этой причине, как правило, имеется достаточное время на оспаривание сфабрикованных документов в суде без утраты самой собственности.

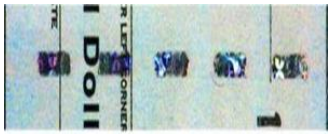
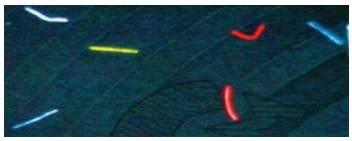
Иначе обстоит дело с финансовыми документами. Требования ко времени выявления факта фальсификации здесь достаточно жесткие. Это объясняется тем, что их фальсификация может привести к невосполнимой утрате финансов, так как денежные средства могут быть быстро переведены на подставные счета, с которых, даже в случае принятия необходимых решений суда, вернуть их будет просто невозможно.

Наиболее критична ситуация с документами, регламентирующими текущее управление опасными объектами. Показательными в этом плане являются, в первую очередь, тепловые и атомные станции, вредные производства, скоростной транспорт. Умышленная фальсификация документов такого рода может привести к авариям и катастрофам техногенного происхождения, человеческим жертвам, огромному экономическому урону. Для таких документов требования к эффективности защиты контекстной информации и юридических аспектов создания документа, а также времени выявления фактов его подделки наиболее жесткие. Отсутствие фальсификации документов

для рассмотренных выше объектов должно быть выявлено практически сразу же по их получению, либо перед исполнением содержащихся в них распоряжений.

Рассмотрим наиболее часто применяемые в настоящее время способы защиты бумажных документов [1, 2, 3]. Все способы защиты можно разделить на два раздела: биометрические и небиометрические методы защиты (таблица 1).

Таблица 1. − Небиометрические (слева) и биометрические (справа) методы защиты документов.

<table>
<tr><th colspan="2">Небиометрические методы защиты</th><th>Биометрические методы защиты</th></tr>
<tr><td>  </td><td>Защитные нити</td><td rowspan="3">Дактилоскопия
  </td></tr>
<tr><td>  </td><td>Водяные знаки</td></tr>
<tr><td>  </td><td>Защитные волокна</td></tr>
<tr><td>  </td><td>Цветопеременная краска</td><td rowspan="2">Подпись (почерк)
  </td></tr>
<tr><td>  </td><td>Орнаментальная полоса</td></tr>
</table>

Небиометрические методы защиты это: защитные нити, водяные знаки, защитные волокна, цветопеременные краски, орнаментальные полосы и др. Наглядный пример использования этих средств защиты можно увидеть на любой банковской купюре. Небиометрические методы защиты позволяют достаточно быстро выявить факт подделки документа.

Биометрические методы защиты документов − это отпечатки пальцев, подпись, почерк и др. Процесс выявления подделок документов в случае применения биометрических методов защиты требует несколько большего времени.

Из анализа биометрических и небиометрических методов защиты информации следуют два основных вывода. Первый − это то, что все они в той или иной мере могут быть подделаны (одни − более просто, другие − более сложно). Второй, и самый главный, −это то, что эти методы никак не связаны с информационным смысловым содержанием защищаемого документа. То есть, изменение сути договора не порождает изменение элементов защиты носителей этого договора.

Технология речевой подписи

Из вышеизложенного следует, что значительно повысить защищенность документов позволит использование таких биометрических технологий, которые будут связывать

защиту с самим защищаемым текстом. Одной из таких технологий является технология речевой подписи [4] (рисунок 1).

Данная технология заключается в следующем:

1. Автор защищаемого документа создает аудиофайл, в котором записан прочтенный им текст, содержащий основные моменты защищаемого документа (или весь документ целиком).
2. Автор загружает данный аудиофайл на специальный сайт для расчета и получения аудиомаркера (речевой подписи), выбирает типы границ (которые нужны для распознавания с помощью смартфона) и нажимает кнопку “Сгенерировать речевую подпись”.
3. Пользователь копирует изображение получившейся речевой подписи и вставляет в определенное место защищаемого документа, к примеру, в его конец.

Рис.1. Технология речевой подписи
Fig.1. Voice signature technology

Далее пользователь скачивает и устанавливает специальное приложение на смартфон, с помощью которого можно распознать и воспроизвести изображение речевой подписи.

4. Пользователь запускает скаченное приложение, наводит камеру на речевую подпись (аудиомаркер), ждет несколько секунд, пока программа распознает речевую подпись и просинтезирует ее, и после этих действий пользователь может прослушать получившийся результат и дать заключение о совпадении или несовпадении аудиоинформации с текстом

документа, а также голоса человека, который заключал договор, с голосом человека, который представлен в речевой подписи.

Иными словами, при использовании технологии речевой подписи (РП), можно утверждать, что злоумышленник не сможет изменить содержимое документа без изменения изображения речевой подписи (аудиомаркера), в которой хранятся основные моменты смыслового содержания защищаемого документа и биометрические данные его собственника или автора.

Рассмотрим более подробно, что же такое речевая подпись. По сути, этот аудиомаркер представляет собой изображение спектрограммы акустического (речевого) сигнала с границами для распознавания (таблица 2).

Для получения спектрограммы звукового сигнала используется математический аппарат кратковременного анализа Фурье (КАФ). В основу кратковременного анализа положено допущение, что в пределах относительно короткого интервала речь можно считать стационарным процессом. Это позволяет отражать в общем виде описания сигнала, его важнейшие временные изменения [4, 5, 6].

Спектральная плотность сигнала при построении РП вычисляется по формуле (1):

$$S(\omega, t) = \sum_{n=\frac{N-M}{2}}^{\frac{N+M}{2}-1} w(n)x(n + st \cdot k)\, e^{-\frac{2\pi i}{N} l \cdot n}, \quad (1)$$

где $\omega = 2\pi l \frac{\nu}{N}$; $t = \frac{st \cdot k}{\nu}$;
$\omega(n)$ − оконная функция;
$x(n)$ −дискретизированный аудиосигнал;
$S(\omega, t)$ − спектральная плотность сигнала на частоте ω в момент времени *t*;
$\nu = 8$ кГц − частота дискретизации аудиосигнала;
st − шаг Фурье-анализа;
N=1024 − база Фурье;
M=512 − ширина окна.

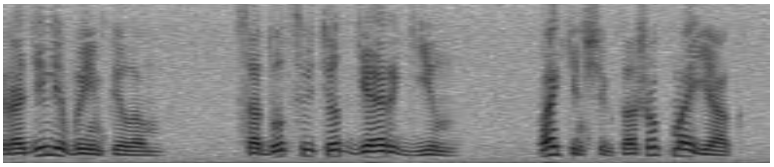
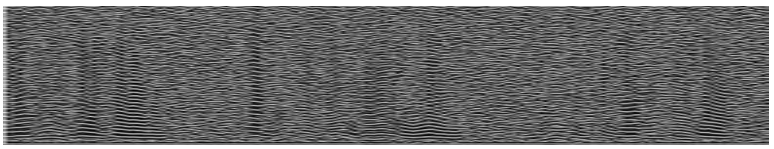
Для анализа речевого сигнала его Фурье-образ является удобным по двум причинам [6]. Во-первых, через представление РС в виде синусоид или комплексных экспонент очень удобно определять их отклик при прохождении сигнала через линейные системы с помощью основных свойств Фурье-преобразования. Во-вторых, на Фурье-образе часто выявляются такие свойства исходного сигнала, которые в первоначальном виде скрыты или не очевидны. В качестве оконной функции было выбрано окно Гаусса (2) с параметром σ = 0.17, так как оно давало лучший результат по сравнению с другими окнами.

$$w(n) = e^{-\frac{1}{2}\left(\frac{n-A}{A\sigma}\right)^2}, \text{ где } A = \frac{M-1}{2} \quad (2)$$

В таблице 2 представлены осциллограмма, спектрограмма и фазограмма участка речевого сигнала, наблюдаемого в один и тот же момент времени. Осциллограмма – это зависимость амплитуды сигнала от времени, спектрограмма показывает зависимость интенсивности сигнала от частоты в конкретный момент времени (3), а фазограмма − зависимость косинуса фазы от частоты и времени. Аудиомаркер РП в виде изображения спектрограммы можно получить, рассчитав спектральную плотность сигнала [5,7, 8, 9]:

$$p[i][j] = 255 * \left|\sin(\arg(S[i][j]) - \arg(S[i][j-1])) - s * \frac{2\pi}{N} i\right| \quad (3)$$

Таблица 2 − Изображения осциллограммы, спектрограммы, фазограммы речевого сигнала

Осциллограмма	
Спектрограмма (сонограмма − для человеческой речи)	
Фазограмма	

Соответственно, если к такой спектрограмме привязать границы для распознавания и озвучивания аудиомаркера при помощи смартфона, то в результате мы получим изображение речевой подписи [9] (рисунок 2).

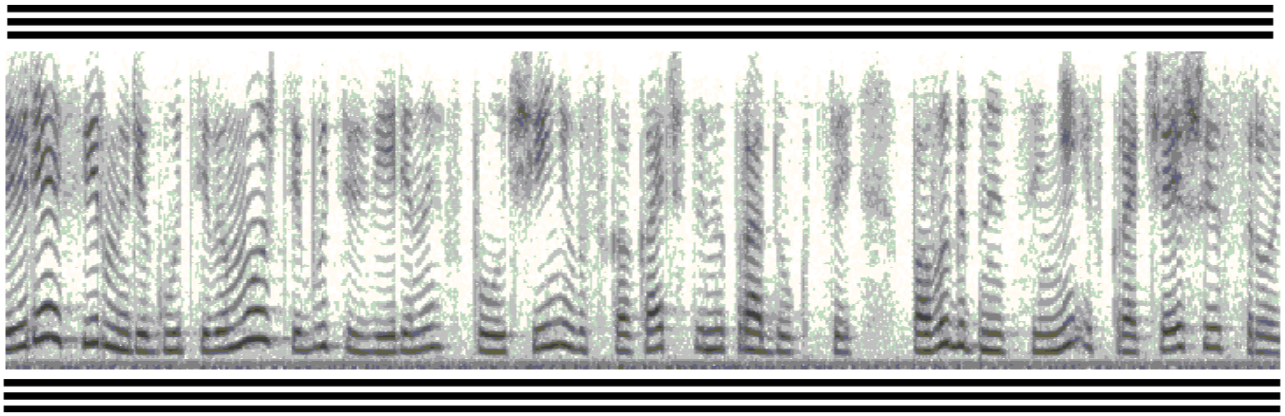


Рис. 2. Пример изображения речевой подписи как аудиомаркера защищаемого документа
Fig. 2. An example of voice signature image as audiomarker of protected document

Анализ технологии выбора границ и алгоритм распознавания речевой подписи подробно представлен в статьях [9, 10].

Применение рассматриваемой технологии речевой подписи дает возможность осуществить идентификацию автора документа на основе анализа спектра его голоса [11-15]. Для этого необходимо иметь образцы голоса в базе данных [16]. Кроме этого, разработанные к настоящему времени акустические технологии определения текущего психоэмоционального состояния говорящего [17-20], позволяют выявить факты неадекватного состояния человека, составившего и подписавшего документ, например, в состоянии алкогольного, либо наркотического опьянения, в случае физического и психологического принуждения.

Таким образом, рассматриваемая технология речевой подписи позволяет защитить как контекстную составляющую документа, так и юридические аспекты условий его создания. Последний фактор можно рассматривать как дополнительную степень защиты документа.

Данная технология также удовлетворяет жестким требованиям ко времени выявления факта подделки документа и может быть рекомендована к защите практически всех типов документов – юридических, финансовых, управляющих.

Заключение

Бумажный документооборот остается в настоящее время одним из наиболее распространенных способов фиксации, хранения и передачи правовой, финансовой, политической, научно-технической и других видов информации.

Проведенный анализ существующих биометрических и небиометрических методов идентификации для защиты документированной информации позволил выявить области возможного их применения, а также наиболее существенные недостатки, ограничивающие их эффективность, в первую очередь, по причине возможной фальсификации, а также независимости технологий защиты от содержания документа.

Предложена технология защиты документов на основе использования аудиомаркера в виде изображения спектрограммы (речевой подписи) как нового средства защиты документооборота, имеющего существенные преимущества по сравнению с существующими биометрическими методами.

Показана возможность использования аудиомаркера для решения задачи идентификации говорящего, а также выявления случаев его неадекватного поведения, вызванного, в том числе, применением физического и психического насилия, либо состоянием алкогольного, либо наркотического опьянения.

Разработаны алгоритмы построения и распознавания речевой подписи для мобильного устройства. Создано специализированное программное обеспечение, ориентированное на работу под операционной системой android.

Проведенное лабораторное тестирование разработанных методических и технических средств подтвердило высокую эффективность технологии речевой подписи.
Рассмотренная технология может быть использована для повышения степени защиты широкого спектра документов финансового, юридического, экономического и технического характера и гарантирует минимальное время выявления фактов подделки и фальсификации данных документов.

СПИСОК ЛИТЕРАТУРЫ:

1. Шашкин С.Б. Технико-криминалистические исследования документов со специальными средствами защиты от подделки: Учебное пособие. Саратов: СЮИ МВД России. 2002. − 96 с.
2. Гудилин Д. Печатные технологии и защита документов от подделки. Компьюарт, №11, 2003 2. 2000 - 2009.
3. Коншин А.А. Защита полиграфической продукции от фальсификации. М.: ООО «Синус», 2000.
4. ANSI S3.5-1997, American National Standard Methods for Calculation of the Speech Intelligibility Index – American National Standards Institute, New York. – 1997.
5. Дворянкин С.В. Речевая подпись. М. РИО. 2003. – 184 с.
6. Рабинер Л.Р. Цифровая обработка речевых сигналов/ Л.Р. Рабинер, Р.В. Шафер: Пер. с англ. / Под ред. М.В. Назарова и Ю.Н. Прохорова. М.: Радио и связь.– 1981. – 496 с.
7. Ephraim Y.A. Brief Survey of Speech Enhancement/ Y. Ephraim, H. Lev-Ari, W.J.J. Roberts // The Electronic Handbook, CRC Press. – 2005.
8. Vorobiov V.I. Inter Component Phase Processing of Speech Signals for Their Recognition and Identification of Announcers/ V.I. Vorobiov // XVIII Session of the Russian Acoustical Society, Taganrog, September 11-15, 2006.
9. Алюшин А.М., Дворянкин Н.С. Особенности распознавания изображений речевой подписи на мобильных устройствах //Безопасность информационных технологий. 2015. № 4. С. 38-45.
10. Алюшин А.М., Дворянкин Н.С. Технология защитного аудиомаркирования документированной информации с использованием мобильных устройств // Спецтехника и связь. 2015. № 6. с. 26-31.

11. Bimbot F. et al. A Tutorial on Text-Independent Speaker Verification. - EURASIP Journal on Applied Signal Processing, 2004, No4. P. 430–451.
12. Reynolds D. Experimental evaluation of features for robust speaker identification. – IEEE Trans. On Speech and Audio Processing, 1994, vol. 2, No4. P. 639-643.
13. Коваль С.Л., Лабутин П.В., Малая Е.В., Прощина Е.А. Идентификация дикторов на основе сравнения статистик основного тона голоса //В сб.трудов XV международной Научной конференции «Информатизация и информационная безопасность правоохранительных органов». –М.: Академия управления МВД России , 2006. С. 324-327.
14. Vogt R., Baker B., Sridharan S. Modeling session variability in text-independent speaker verification // In Proc. Eurospeech, Lisbon, Portugal, Sept. 2005, pp. 3109–3112.
15. Rosenberg A. et al. Cepstral channel normalization techniques for HMM-based speaker verification // In Proc. ICSLP-94, pp. 1835-1838.
16. Тимофеев А.В. Распределённая система фоноучёта «VoiceNet ID». – Речевые технологии , 2009, No 2, с. 69-73.
17. Алюшин В.М. Спектральный анализ речевой деятельности как способ оценки психологического климата в коллективе // Вопросы психологии, 2016. № 3. С.148–156.
18. Алюшин В.М. Диагностика психоэмоционального состояния на основе современных акустических технологий // Вопросы психологии, 2015. № 3. С.145–152.
19. Алюшин М.В., Колобашкина Л.В. Мониторинг биопараметров человека на основе дистанционных технологий // Вопросы психологии, 2014. № 6. С.135–144.
20. Алюшин М.В. и др. Акустические технологии для интеллектуальных систем мониторинга функционального состояния оперативного состава управления объектами атомной энергетики /М.В. Алюшин, В.М. Алюшин, С.В. Дворянкин, Л.В. Колобашкина //Глобальная ядерная безопасность. 2013. № 4(9). С. 63-71.

REFERENCES:

[1] Shashkin S.B. Technical-criminalistics research of documents with special means of protection against forgery: a tutorial. Saratov: SYUI MVD Russia, 2002. − 96 p. (in Russian).
[2] Gudilin D. Printing technologies to protect documents against forgery. Komp'yuart, №11, 2003 2. 2000 - 2009. (in Russian).
[3] Konshin A.A. Protection of printed products against falsification. M.: OOO «Sinus», 2000. (in Russian).
[4] ANSI S3.5-1997, American National Standard Methods for Calculation of the Speech Intelligibility Index – American National Standards Institute, New York. – 1997.
[5] Dvoryankin S.V. Voice signature. M. RIO. 2003, 184 p. (in Russian).
[6] Rabiner L.R. Digital processing of speech signals; L.R. Rabiner, R.V. Shafer: transl. from English. Pod red. M.V. Nazarova i Y.N. Prohorova. M.: Radio isvyaz'.– 1981. – 496 p.
[7] Ephraim Y.A. Brief Survey of Speech Enhancement; Y. Ephraim, H. Lev-Ari, W.J.J. Roberts; The Electronic Handbook, CRC Press. – 2005.
[8] Vorobiov V.I. Inter Component Phase Processing of Speech Signals for Their Recognition and Identification of Announcers; V.I. Vorobiov. XVIII Session of the Russian Acoustical Society, Taganrog, September 11-15, 2006.
[9] Alyushin A.M., Dvoryankin N.S. Features image recognition of voice signatures on mobile devices. IT Security (Russia). v.22, 4(2015), P. 38-45. (in Russian).
[10] Alyushin A.M., Dvoryankin N.S. Technology protective audiomaterialy documented information using mobile devices. Spectekhnika i svyaz'. 2015. № 6. P. 26-31. (in Russian).
[11] Bimbot F. et al. A Tutorial on Text-Independent Speaker Verification. - EURASIP Journal on Applied Signal Processing, 2004, No4. P. 430–451.
[12] Reynolds D. Experimental evaluation of features for robust speaker identification. – IEEE Trans. On Speech and Audio Processing, 1994, vol. 2, No4. P. 639-643.
[13] Koval' S.L., Labutin P.V., Malaja E.V., Proshhina E.A. Speaker identification based on the comparison of statistics primary tone of voice. V sb. trudov XV mezhdunarodnoj Nauchnoj konferencii «Informatizacija i informacionnaja bezopasnost' pravoohranitel'nyh organov» – M.: Akademija upravlenija MVD Rossii , 2006. P. 324-327.(in Russian).
[14] Vogt R., Baker B., Sridharan S. Modeling session variability in text-independent speaker verification; In Proc. Eurospeech, Lisbon, Portugal, Sept. 2005. P. 3109–3112.
[15] Rosenberg A. et al. Cepstral channel normalization techniques for HMM-based speaker verification; In Proc. ICSLP-94. P. 1835-1838.
[16] Timofeev A.V. Distributed system of Pinocheta «VoiceNet ID». – Rechevye tehnologii, 2009, No 2. P. 69-73. (in Russian).
[17] Alyushin V.M. Spectral analysis of speech as a means of assessing psychological team climate. Voprosy Psikhologii. 2016. N 3. P.148–156. (in Russian).

[18] Alyushin V.M. Diagnostics of emotional states on the basis of contemporary acoustic technologies. Voprosy Psikhologii. 2015. N 3. P. 145–152. (in Russian).
[19] Alyushin M.V., Kolobashkina L.V. Monitoring human biometric parameters on the basis of distance technologies. Voprosy Psikhologii. 2014. N 6. P.135–144. (in Russian)
[20] Alyushin M.V. i dr. Acoustic technologies for "intellectual" monitoring systems of atomic energetic objects' operational control staff current functional state./M.V. Alyushin, V.M. Alyushin, S.V. Dvoryankin, L.V. Kolobashkina. Global'naya yadernaya bezopasnost'. 2013. N 4(9). P. 63-71. (in Russian).

Поступила в редакцию – 19 февраля 2017 г. Окончательный вариант – 20 мая 2017 г.
Received – February 19, 2017. The final version – May 20, 2017.