# СИСТЕМА ТЕЛЕМЕДИЦИНЫ С ПРЕДВАРИТЕЛЬНЫМ ШИФРОВАНИЕМ БИОМЕТРИЧЕСКОЙ ИНФОРМАЦИИ

***Горшков Ю.Г.[1], Каиндин А.М.[2], Веряев А.С.[3], Зорин Е.Л.[4], Марков А.С.[5], Цирлов В.Л.[6]***

*В статье представлены основные характеристики системы телемедицины нового поколения "АКУСТОМЕД". Рассмотрен состав аппаратно–программных средств, обеспечивающих экспресс–диагностику состояния сердечно–сосудистой системы человека по акустическим биомедицинским сигналам. Предложены решения по предварительному шифрованию персональных биометрических данных. Приводятся примеры вейвлет–сонограмм исходных и засекреченных сигналов. Даны рекомендации по реализации системы с тактическим и стратегическим уровнем стойкости линейных передач к "взлому".*

***Ключевые слова**: телемедицина, акустические биомедицинские сигналы, персональные биометрические данные, предварительное шифрование, криптографическая стойкость*

**Введение**

Необходимость развития телемедицины признана в ведущих странах мира, среди которых дистанционные медицинские технологии особенно широко применяются в США. Телемедицина оказывается крайне эффективной при организации медицинской помощи как в мирное время, так и вооруженных конфликтах на поле боя [1-3]. В последние годы, при эксплуатации действующих систем телемедицины и создании новых, особое место отводится решению задач, связанных с обеспечением конфиденциальности персональных данных. Решения используемые ФСТЭК России при разработке современных требований к средствам защиты информации (СрЗИ) и наработки по формализации требований безопасности информации к средствам аназиза защищенности (САЗ) представлены в работах [4, 5]. Рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения России подготовлены в 2009 году [6]. Для обеспечения реализации положений Федерального закона № 152-ФЗ «О персональных данных» действуют документы [7, 8]. В соответствии с классификацией компании «Аладдин Р.Д.» категории обрабатываемых персональных данных (ПДн) подразделяются на 4 группы [9], следовательно, акустические биометрические ПДн относятся к 1 группе (раздел: информация о здоровье) и 2 группе (раздел: биологические или физиологические особенности субъекта).

Специалистами кафедры «Информационная безопасность» МГТУ им. Н.Э. Баумана и Группы компаний НПО «Эшелон» завершены поисковые исследования по созданию системы телемедицины нового поколения «АКУСТОМЕД» с засекречиванием акустических биомедицинских сигналов (АБС). Засекречивание АБС осуществляется так называемым предварительным шифрованием, осуществляемым перед передачей биометрической информации по сети. Данный подход наиболее удобен в глобальных информационных сетях, например, Internet. Суть его заключается в том, что пользователи, предварительно обменявшись ключами, шифруют свои данные, а потом передают их по каналам сети стандартными средствами файлового обмена. Выгоды этого подхода очевидны, он позволяет пользователям, работающим с различными ОС, без особых затрат обмениваться шифрованными данными. Так работают пользователи программы Pretty Good Private (PGP), разработанной Филиппом Зиммерманом в начале 90-х годов и широко распространенной во всем мире. PGP позволяет вырабатывать индивидуальные ключи пользователей, безопасно ими обмениваться и шифровать данные. В нем реализован алгоритм блочного шифрования IDEA и схема открытого распределения ключей RSA. Отечествен-

1 Горшков Юрий Георгиевич, кандидат технических наук, доцент, МГТУ им. Н.Э. Баумана, Москва, y.gorshkov@cnpo.ru,
2 Каиндин Александр Михайлович, АО "Интел А/О", Москва, alex@kaindin.ru,
3 Веряев Александр Сергеевич, ЗАО "НПО "Эшелон", Москва, a.veryev@cnpo.ru,
4 Зорин Егор Леонидович, МГТУ им. Н.Э. Баумана, Москва, e.zorin@bmstu.net,
5 Марков Алексей Сергеевич, доктор технических наук, старший научный сотрудник, МГТУ им. Н.Э. Баумана, Москва a.markov@bmstu.ru,
6 Цирлов Валентин Леонидович, кандидат технических наук, ЗАО "НПО "Эшелон", Москва, v.tsirlov@cnpo.ru

ные криптографы утверждают: «...если вы не доверяете PGP (и это, по-видимому, правильно), то можете разработать свои собственные программы шифрования, взяв за основу только его общую схему» [10].

**«АКУСТОМЕД»**

Защищенная система телемедицины ранней диагностики кардиозаболеваний с использованием технологии многоуровневого вейвлет-преобразования акустических биомедицинских сигналов.

*Назначение*: экспресс-диагностика состояния сердечно-сосудистой системы человека с целью выявления ранних стадий кардиозаболеваний на основе высокоточного анализа сигналов акустического поля сердца, звуков дыхания и оценкой состояния эмоциональной напряженности [11-17].

*Применение*: ранняя диагностика заболеваний сердца; оперативный контроль состояния работы сердца для лиц, перенесших операцию на сердце и страдающих хроническими сердечно-сосудистыми заболеваниями; детская и подростковая кардиология; медицина катастроф, военная, авиационная, космическая, морская и спортивная медицина; восстановительная медицина и курортология; «домашняя» телемедицина.

На рис. 1 представлена структура защищенной системы телемедицины «АКУСТОМЕД», где модули: 1 - ввода данных артериального давления; 2 - съема акустических сигналов сердца; 3 - ПК; 4 - ввода речевого сигнала, звуков дыхания и формирования контейнера АБС; 5 и 6 - предварительного шифрования и расшифрования АБС; 7 - данных артериального давления; 8 - получения вейвлет-сонограмм звуков сердца, легких и речи пациента.

В кардиологическом центре врач получает вейвлет-сонограммы АБС пациента, оценивает его эмоциональное состояние, подготавливает заключение экспресс-диагностики и вносит полученные материалы в базу данных.

**«Акустокард»**

Портал дистанционной обработки акустограмм (фонокардиограмм) с оценкой эмоциональной напряженности пациента по голосу. В 2010 году отмечен Специальным дипломом конкурса раз-

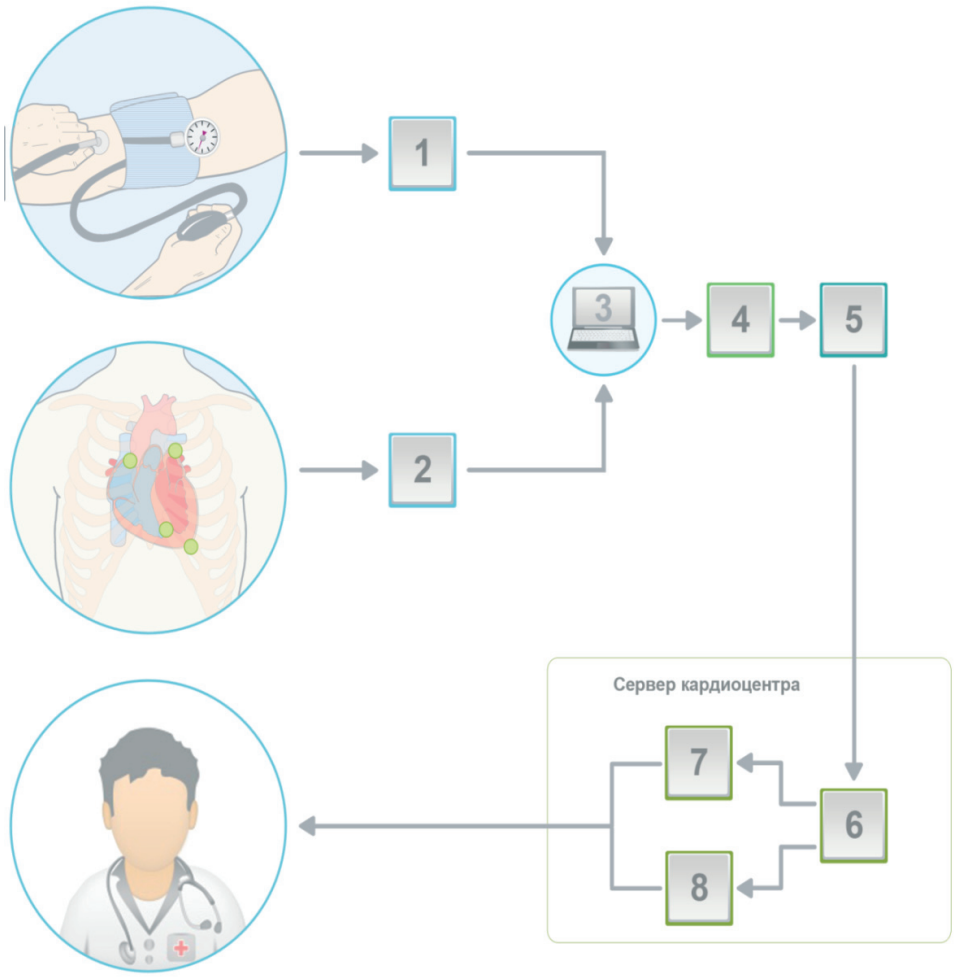


***Рис. 1.*** *Структура защищенной системы телемедицины «АКУСТОМЕД»*

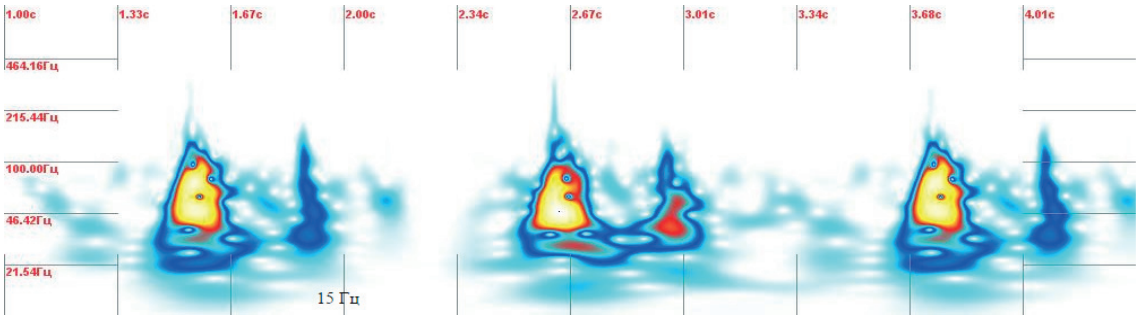


***Рис. 2.*** *Сонограмма акустического кардиосигнала (фонокардиограммы) пациента*

работок в области здравоохранения «Лучшая медицинская информационная система». Является развитием направления «Акустокардиограф» (Первая Национальная Премия России в области кардиологии «Пурпурное сердце», номинация научный проект года, 2009) [18].

*Назначение*: удаленный мониторинг работы сердца пациентов с оценкой эмоциональной напряженности по голосу в режиме on-line.

На рис. 2, 3 и 4, соответственно, представлены сонограммы акустического кардиосигнала и речи пациента.

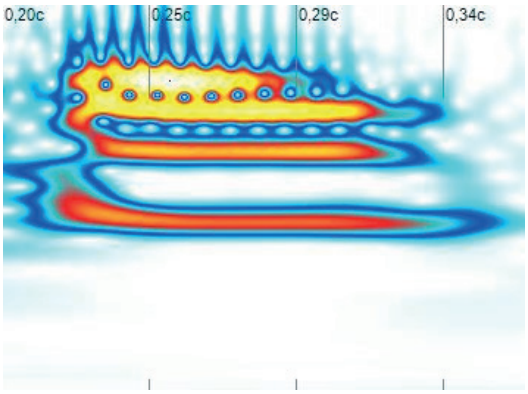


***Рис. 3****. Сонограмма речи пациента без эмоциональной напряженности*

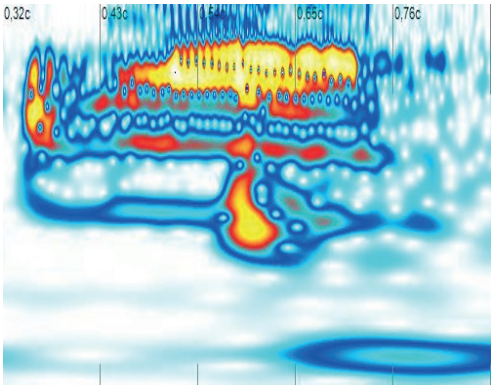


***Рис. 4.*** *Сонограмма речи пациента с высоким уровнем эмоциональной напряженности*

Отличительные особенности: для записи фонокардиограмм могут использоваться стетоскопы JABES ANALYZER, речи - Logitech USB Desktop Microphone. Формат записи WAV. Интервал анализа при получении акустокардиограмм и сонограмм речи - 8 сек.

**Предварительное шифрование АБС**

Контейнер передаваемых АБС формируется с использованием предварительного шифрования. Засекречивание линейной передачи осуществля-

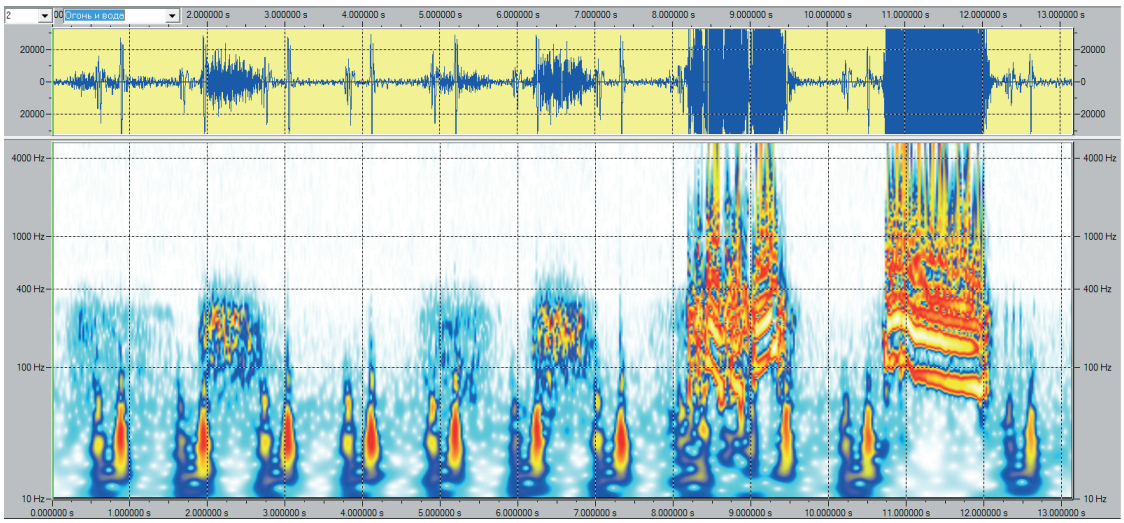


***Рис. 5.*** *Сонограмма звуков сердца, дыхания и речи*

ется специальным программным обеспечением (СПО) WAVELET-FONE [19, 20]; объем контейнера 1,3 МБ (длительность записи сигналов 1 мин.).

На рис. 5 представлена вейвлет-сонограмма звуков сердца, дыхания и речи.

На рис. 6 сонограмма засекреченного сигнала.

На рис. 7 сонограмма восстановленного сигнала звуков сердца.

На рис. 8 сонограмма восстановленного сигнала звуков дыхания.

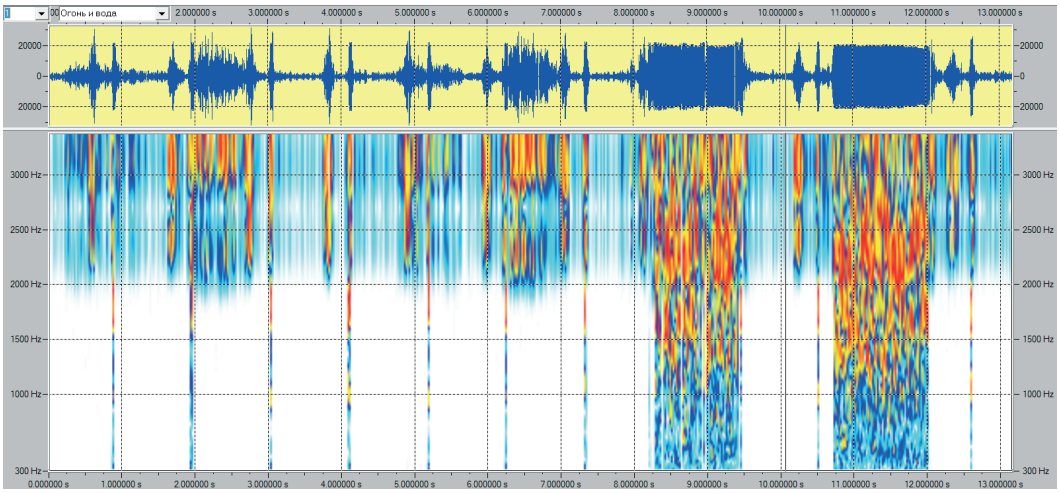


***Рис. 6**. Сонограмма засекреченного сигнала звуков сердца, дыхания и речи в полосе частот стандартного телефонного канала 300-3400 Гц*

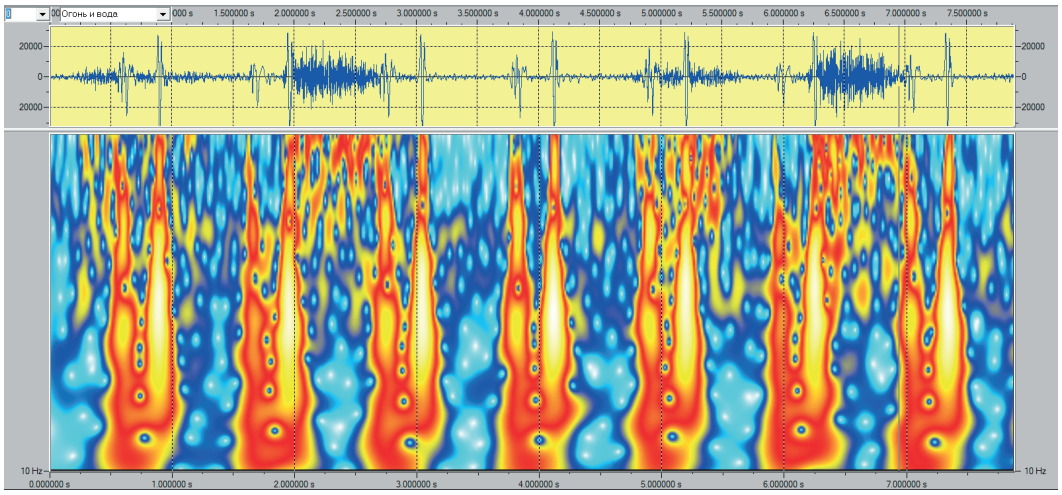


***Рис. 7**. Сонограмма восстановленного сигнала звуков сердца*

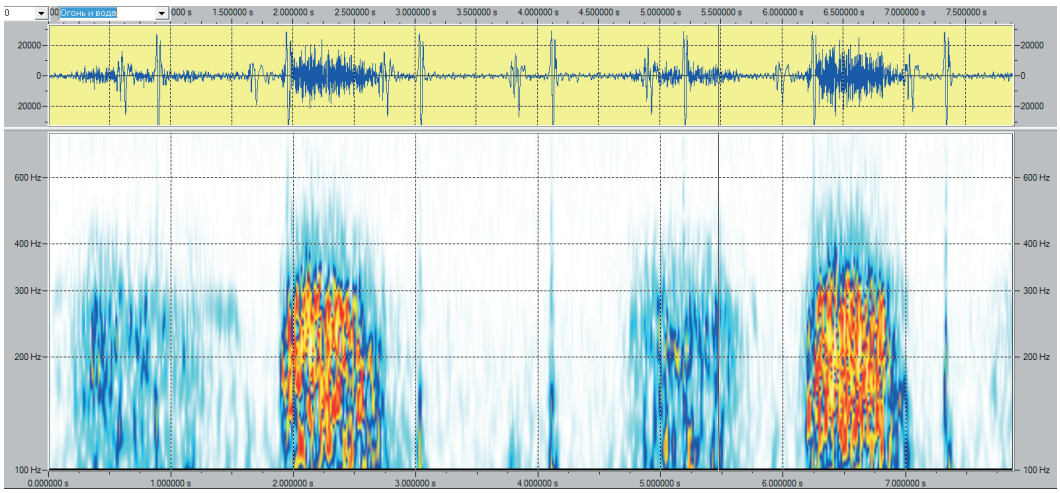


***Рис. 8**. Сонограмма восстановленного сигнала звуков дыхания*

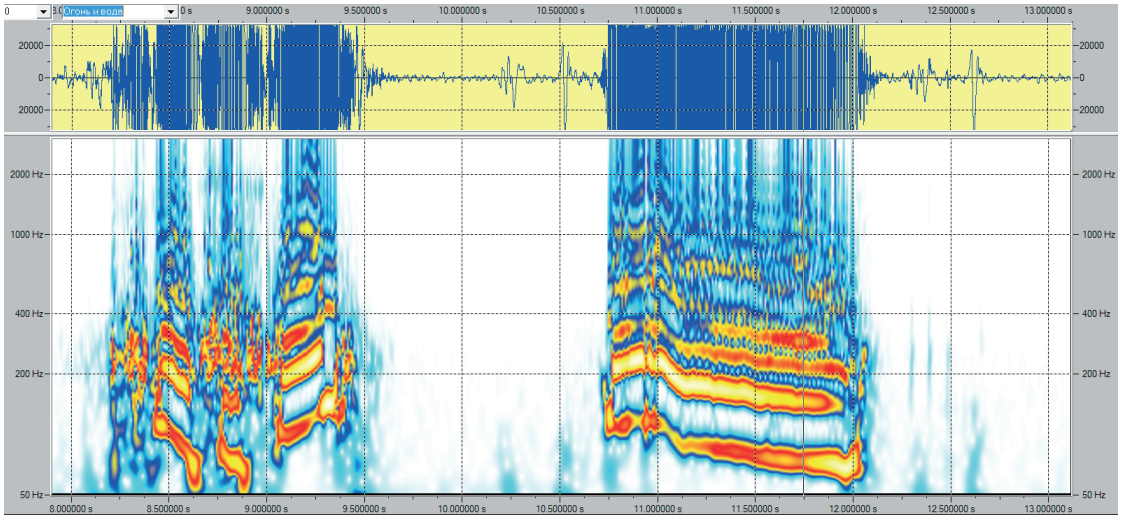


***Рис. 9**. Сонограмма восстановленного речевого сигнала*

На рис. 9 сонограмма восстановленного речевого сигнала.

Решения по защите акустических биомедицинских данных с использованием криптографических методов, разработанные для системы телемедицины «АКУСТОМЕД» обеспечивают необходимый уровень стойкости к «взлому» и соответствуют международному стандарту ISO/IEC 24745:201 от 17 июня 2011 года. СПО WAVELET-FONE в соответствии с международной классификацией выполняет засекречивающие преобразования в частотной области: Frequency-Domain Scramblers (FDS). Обеспечивается 4 уровня засекречивания. Для каждого уровня задается фиксированное число частотных полос: минимальный уровень безопасности - 4 частотные полосы; средний - 8 частотных полос; высокий уровень - 16; максимальный уровень безопасности - 32 частотные полосы.

*Формирование массивов подстановок*. С учетом перестановок частотных полос и инверсии спектра сигнала, общее количество возможных подстановок составляет:

$$(32!\cdot 232 + 16!\cdot 216 + 8!\cdot 28 + 4!\cdot 24)\cdot 15 \approx 2153$$

Причем для участка речевого сигнала, с учетом использования критерия «на открытую речь» не все из общего числа подстановок обеспечивают высокий уровень засекречивания. В ходе экспериментальных исследований для каждого уровня безопасности выполнен выбор массивов наиболее «стойких» к «взлому» подстановок, обеспечивающих максимальную неразборчивость сигнала линейной передачи. СПО WAVELET-FONE обеспечивает возможность реализации стратегического и тактического уровней стойкости передаваемой биометрической информации к «взлому».

**Стратегический уровень стойкости**

Компоновка файла биомедицинских сигналов, содержащего акустические сигналы сердца, легких, а также речи пациента, его предварительное шифрование в частотно-временной области обеспечивает возможность использования всего массива подстановок (2153). Получение знаков гаммы обеспечивается сертифицированным решением «ГЕНЕРАТОР» (средство генерации и управления паролями), разработчик: ГК НПО «Эшелон».

**Тактический уровень стойкости**

Применительно к домашней телемедицине (home telemedicine) данный уровень безопасности биометрических данных может быть обеспечен исключительно возможностями СПО WAVELET-FONE.

**Заключение**

Система телемедицины «АКУСТОМЕД» минимальным составом аппаратно-программных средств обеспечивает экспресс-диагностику состояния сердечно-сосудистой системы человека с оценкой его эмоционального состояния. Предварительное шифрование персональных биометрических данных обеспечивает гарантированный уровень безопасности, не зависящий от защищенности возможных используемых облачных сервисов.

Портал «Акустокард», как одно из важных звеньев системы телемедицины «АКУСТОМЕД», с 2012 года используется студентами 6 курса кафедры ИУ-8 при выполнении цикла лабораторных работ «Криминалистическое исследование фонограмм». С 2013 года - студентами 6 курса и магистрами факультета БМТ при освоении спецкурса и проведении практических занятий.

По проекту «МАРС-500» специалистами института общей физики им. А.М. Прохорова, РАН выполнена дистанционная обработка материалов эксперимента - получены высокоточные «звуковые портреты» (многоуровневые вейвлет-сонограммы) файлов акустики сердца членов экипажа, зарегистрированных при длительной изоляции. Решения защищены патентами [12, 21, 22].

**Рецензент**: Бельфер Рувим Абрамович, кандидат технических наук, доцент, a.belfer@yandex.ru

**Литература**:

1. Справка об использовании современных информационных технологий в вопросах повышения эффективности функционирования системы здравоохранения в Российской Федерации, включая предложения по ИКТ мероприятиям в приоритетный национальный проект «Здоровье». 2015. 14 с. URL: http://inforegion.ru/ru/main/medicine/IT/ (дата обращения: 09.12.2015).
2. Национальный центр управления обороной РФ задействуют в развитии военной телемедицины. ТАСС информационное агентство. URL: http://tass.ru/obschestvo/2060242 (дата обращения: 09.12.2015).
3. NATO tests telemedicine system in Ukraine. NATO. URL: www.nato.int/cps/en/natohq/news_123670.htm (дата обращения: 09.12.2015).
4. Марков А.С., Цирлов В.Л., Барабанов А.В. Методы оценки несоответствия средств защиты информации. М.: Радио и связь, 2012. 192 с.
5. Веряев А.С., Фадин А.А. Формализация требований безопасности информации к средствам анализа защищенности // Вопросы кибербезопасности. 2015. № 4 (12). С. 23-27.
6. Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения. Минздрав России, 2009. URL: http://www.rosminzdrav.ru/documents/7570-rekomendatsii-ot-24-dekabrya-2009-g (дата обращения: 09.12.2015).
7. Постановление Правительства РФ от 1 ноября 2012 года № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных». URL: http://www.consultant.ru/document/cons_doc_LAW_137356/92d969e26a4326c5d02fa79b8f9cf4994ee5633b/ (дата обращения: 09.12.2015).
8. Приказ ФСТЭК России от 18.02.2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». URL: http://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 09.12.2015).
9. Защита персональных биометрических данных. URL: www.aladdin-rd.ru/solutions/ispdn/. (дата обращения: 09.12.2015).
10. Введение в криптографию / Под общ. ред. В.В. Ященко. 4-е изд., доп. М.: МЦНМО, 2012. 347 с.
11. Горшков Ю.Г., Каиндин А.М., Романовский К.В. Защищенный интернет-портал «Акустокард» ранней диагностики заболеваний сердца. URL: http://acustocard.ru (дата обращения: 09.12.2015).
12. Горшков Ю.Г., Калинкин А.Л., Каиндин А.М., Марков А.С., Цирлов В.Л. Защищенная система телемедицины дистанционного выявления ранних стадий заболеваний сердца. Патент на полезную модель RUS 127605. 18.12.2012; Заявка № 2012154801; опубл. 10.05.2013. Бюл. № 13.
13. Горшков Ю.Г. Многоуровневые вейвлет-технологии: от засекречивания речевых сигналов к ранней диагностике заболеваний сердца // «Безопасные информационные технологии». Всероссийская научно-техническая конференция. Москва. 2010. С. 79-82.
14. Gorshkov Y.G. Detection and Processing of Multilevel Acoustic Cardiograms. Biomedical Engineering, 2013, Volume 47, Issue 1 (May 2013), pp 18-21. DOI = 10.1007/s10527-013-9325-x.
15. Gorshkov Y., Shchukin S. Early Detection of Heart Diseases on the Basis Multilevel Wavelet Analysis of Acoustic Signals. In Proceedings of the X Russian-German conference of biomedical engineering (Saint Petersburg, Russia, 25-27 June 2014). RGC - 2014. St. Petersburg State Electrotechnical University («LETI»), Russia, pp. 38-41.
16. Горшков Ю.Г. Оценка эмоционального состояния человека на основе многоуровневого вейвлет-анализа речи // Биомедицинская радиоэлектроника. 2014. № 10. С. 64-69.
17. Gorshkov Y.G. Computerized Respiratory Sounds Analysis on the Basis of Multilevel Wavelet Transform. In Proceedings of the 40th International Lung Sounds Association Conference (Saint Petersburg, Russia, 24-25 September 2015). ILSA, USA, St. Petersburg State Electrotechnical University («LETI»), Russia, pp. 27-28.
18. Ежегодная Национальная премия в области кардиологии, лауреаты-2009, номинация «Лучший кардиологический проект», разработка комплекса аппаратно-программных средств для ранней диагностики заболеваний сердца «АКУСТОКАРДИОГРАФ». Москва. 2009. URL: http://purpurnoe-serdce.ru/joom/index.php?option=com_content&task=view&id=75 (дата обращения: 09.12.2015).
19. Горшков Ю.Г. Тестирование средств засекречивания речи // Вопросы кибербезопасности. 2015. № 2 (10). С. 26-30.
20. Горшков Ю.Г. Методы и средства многоуровневого вейвлет-анализа и засекречивания речи // Спецтехника и связь. 2015. Т. 2. С. 42-50.
21. Горшков Ю.Г., Марков А.С., Цирлов В.Л., Веряев А.С. Устройство съема и засекречивания акустических биомедицинских сигналов. Патент на полезную модель RUS 155677. 04.06.2015. Заявка № 2015121305. Бюл. №29.
22. Горшков Ю.Г., Каиндин А.М., Марков А.С., Цирлов В.Л. Система определения подлинности фонограмм. Патент на полезную модель RUS 150244 30.12.2013. Заявка № 2013158829/08. Бюл. № 4.

# OFFLINE BIOMETRIC DATA ADVANCED ENCRYPTION TELEMEDICINE SYSTEM

*Gorshkov Y.G.[7], Kaindin A.M.[8], Veryaev A.S.[9], Zorin E.L.[10], Markov A.S.[11], Tirlov V.L.[12]*

*The article presents basic specifications of the new generation telemedicine system AKUSTOMED. The article describes the configuration of software and hardware that enable an instant diagnostics of human cardiovascular system by acoustic biomedical signals. There are solutions proposed for offline encryption of personal biometric data. Some examples of wavelet sonograms are given for source and encrypted signals. The article sets out recommendations as to implementation of the system with a tactic and strategic crack security levels of linear transfers.*

***Keywords**: telemedicine, acoustic biomedical signals, personal biometric data, offline encryption, cryptographic security*

References:

1. Markov A.S., Tsirlov V.L., Barabanov A.V. Metody otsenki nesootvetstviya sredstv zashchity informatsii. M.: Radio i svyaz', 2012. 192 P.
2. Veryaev A.S., Fadin A.A. Formalizatsiya trebovaniy bezopasnosti informatsii k sredstvam analiza zashchishchennosti, Voprosy kiberbezopasnosti. 2015. No 4 (12), pp. 23-27.
3. Vvedenie v kriptografiyu, Pod obshch. red. V.V. Yashchenko. 4-e izd., dop. M.: MTsNMO, 2012. 347 c.
4. Gorshkov Yu.G., Kaindin A.M., Romanovskiy K.V. Zashchishchennyy internet-portal «Akustokard» ranney diagnostiki zabolevaniy serdtsa. URL: http://acustocard.ru (data obrashcheniya: 09.12.2015).
5. Gorshkov Yu.G., Kalinkin A.L., Kaindin A.M., Markov A.S., Tsirlov V.L. Zashchishchennaya sistema telemeditsiny distantsionnogo vyyavleniya rannikh stadiy zabolevaniy serdtsa. Patent na poleznuyu model' RUS 127605. 18.12.2012; Zayavka No 2012154801; opubl. 10.05.2013. Byul. No 13.
6. Gorshkov Yu.G. Mnogourovnevye veyvlet-tekhnologii: ot zasekrechivaniya rechevykh signalov k ranney diagnostike zabolevaniy serdtsa, «Bezopasnye informatsionnye tekhnologii». Vserossiyskaya nauchno-tekhnicheskaya konferentsiya. Moskva. 2010, pp. 79-82.
7. Gorshkov Y.G. Detection and Processing of Multilevel Acoustic Cardiograms. Biomedical Engineering, 2013, Volume 47, Issue 1 (May 2013), pp 18-21. DOI = 10.1007/s10527-013-9325-x.
8. Gorshkov Y., Shchukin S. Early Detection of Heart Diseases on the Basis Multilevel Wavelet Analysis of Acoustic Signals. In Proceedings of the X Russian-German conference of biomedical engineering (Saint Petersburg, Russia, 25-27 June 2014). RGC - 2014. St. Petersburg State Electrotechnical University («LETI»), Russia, pp. 38-41.
9. Gorshkov Yu.G. Otsenka emotsional'nogo sostoyaniya cheloveka na osnove mnogourovnevogo veyvlet-analiza rechi, Biomeditsinskaya radioelektronika. 2014. No 10, pp. 64-69.
10. Gorshkov Y.G. Computerized Respiratory Sounds Analysis on the Basis of Multilevel Wavelet Transform. In Proceedings of the 40th International Lung Sounds Association Conference (Saint Petersburg, Russia, 24-25 September 2015). ILSA, USA, St. Petersburg State Electrotechnical University («LETI»), Russia, pp. 27-28.
11. Gorshkov Yu.G. Testirovanie sredstv zasekrechivaniya rechi, Voprosy kiberbezopasnosti. 2015. No 2 (10), pp. 26-30.
12. Gorshkov Yu.G. Metody i sredstva mnogourovnevogo veyvlet-analiza i zasekrechivaniya rechi, Spetstekhnika i svyaz'. 2015. T. 2, pp. 42-50.
13. Gorshkov Yu.G., Markov A.S., Tsirlov V.L., Veryaev A.S. Ustroystvo s"ema i zasekrechivaniya akusticheskikh biomeditsinskikh signalov. Patent na poleznuyu model' RUS 155677. 04.06.2015. Zayavka No 2015121305. Byul. No 29.
14. Gorshkov Yu.G., Kaindin A.M., Markov A.S., Tsirlov V.L. Sistema opredeleniya podlinnosti fonogramm. Patent na poleznuyu model' RUS 150244 30.12.2013. Zayavka No 2013158829/08. Byul. No 4.

7 Yurii Gorshkov, Ph.D., Associate Professor, Bauman Moscow State Technical University, Moscow, y.gorshkov@cnpo.ru,
8 Aleksandr Kaindin, Intel A/O, Moscow, alex@kaindin.ru,
9 Aleksandr Veryaev, NPO Echelon, Moscow, a.veryev@cnpo.ru,
10 Yegor Zorin, Bauman Moscow State Technical University, Moscow, e.zorin@bmstu.net,
11 Alexey Markov, Dr.Sc., Professor, Bauman Moscow State Technical University, Moscow, a.markov@bmstu.ru,
12 Valentin Tsirlov, Ph.D., NPO Echelon, Moscow, v.tsirlov@cnpo.ru