Подобная работа была проделана ранее с ныне действующими ГОС по пяти специальностям: ГОС 09.01.02 – ГОС 09.01.06. Из сводной таблицы полученных аналитических данных следует, что ряд аналогичных дисциплин, входящих в различные специальности, могут быть поддержаны одними и теми же лабораторными практикумами, в которых требования к знаниям, умениям и практическим компетенциям выпускников, связанные с аттестацией ОИ по требованиям безопасности информации, затронуты лишь косвенно. Это дало возможность разработки типового перечня, структур и описаний (аннотаций) типовых лабораторных практикумов, предназначенных для профессиональной подготовки работников подразделений служб безопасности и технической защиты информации.

Последняя совокупность ФГОС третьего поколения по направлению «Информационная безопасность» представлена проектами по специальностям: 09.03.01 – КОМПЬЮТЕРНАЯ БЕЗОПАСНОСТЬ; 09.03.03 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ; 09.03.05 – ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ; 09.03.07 – ИНФОРМАЦИОННО-АНАЛИТИЧЕСКИЕ СИСТЕМЫ БЕЗОПАСНОСТИ. Анализируя состав и объем общепрофессиональных дисциплин и дисциплин специализаций, сведенных в одну таблицу, по предъявляемым требованиям к знаниям и практическим умениям выпускников, можно сделать вывод о потенциальной готовности к проведению аттестации объектов информатизации по требованиям безопасности информации лишь выпускников по так называемой пятой специальности — «Информационная безопасность автоматизированных систем». При этом только в проекте ФГОС этой специальности предполагается включение в курсы профессионального цикла (в базовую и вариативную части) лабораторных практикумов, связанных с аттестацией объектов информатизации по требованиям безопасности информации.

Еще печальнее картина с данным вопросом в проекте ФГОС ВПО выпускников с квалификацией «бакалавр». Так как в подготовленных проектах стандартов отсутствует какая-либо ориентация на первичные должности выпускников, то основное внимание уделяется дисциплинам общеобразовательного характера, в том числе гуманитарного цикла, обеспечивающим фундаментальную подготовку. Задача получения практических навыков, особенно работы с применением сложных инструментальных средств, решается очень слабо, в недопустимо малом объеме учебной нагрузки.

Все это означает, что представленные на суд научно-педагогической общественности проекты ФГОС ВПО третьего поколения пока не закрепляют достоинств действующих стандартов, по крайней мере в части повышения уровня навыков практической работы.

Ю. Г. Горшков

РЕШЕНИЕ ЗАДАЧ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОБРАБОТКЕ БИОМЕТРИЧЕСКИХ ПЕРСОНАЛЬНЫХ ДАННЫХ

За последние годы традиционный набор биометрической персональной информации отпечатков пальцев и ладоней, радужной оболочки глаз и голоса человека дополняется акустическими данными, получаемыми в процессе аускультации сердца.

В соответствии с законом о персональных данных [1], вся биометрическая информация, включающая дерматоглифические параметры пальцев и ладоней, изображений радужки, а также аудиозаписи тонов, шумов сердца, подлежит защите. Информационные системы биометрических персональных данных также должны отвечать требованиям Федерального закона № 152.

Современные технологии съема биометрических сигналов и их передачи для последующей обработки в медицинские центры способствуют развитию систем телемедицины, использующей телефонные каналы сети общего пользования, Интернет, а также беспроводные протоколы GSM, Bluetooth, Wi-Fi и другие.

На рис. 1 представлена одна из возможных схем проведения мониторинга системы массового обследования состояния здоровья населения с привлечением средств телеметрии [2].

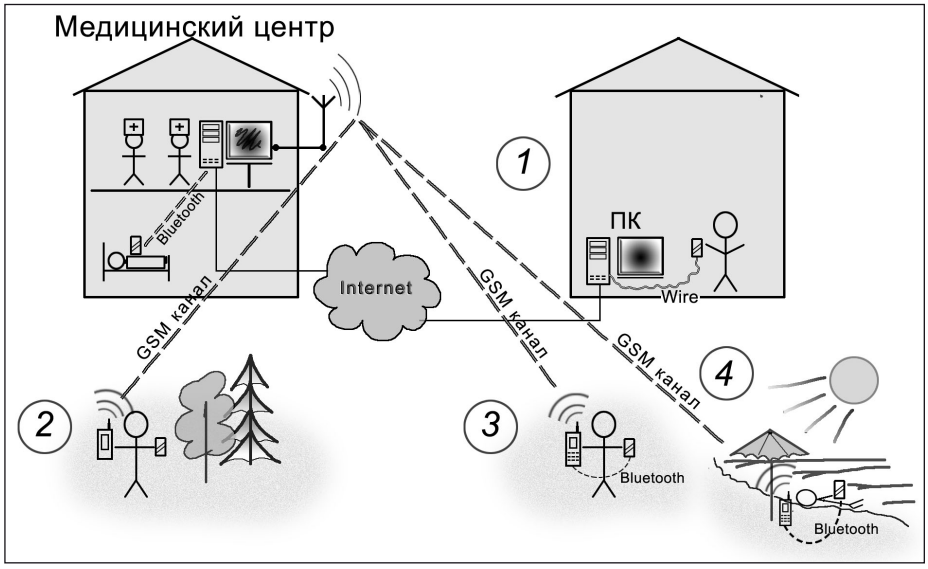

Рис. 1. Схема телеметрии при медицинском обследовании

В значительной степени возможности телемедицины в области ранней диагностики заболеваний сердца расширяются с внедрением средств «Акустокардиограф», созданных Научно-исследовательским и испытательным центром биометрической техники МГТУ им. Н. Э. Баумана и НПО «ЭШЕЛОН». «Акустокардиограф» относится к средствам контроля функционального состояния сердечно-сосудистой системы по звуковым сигналам сердца, которые пациент самостоятельно может внести в память ПК или смартфона с последующей передачей зарегистрированной информации по каналу связи.

Экспертным советом национальной премии России в области кардиологии «Пурпурное сердце» работа «Акустокардиограф» признана лучшим научным проектом 2009 г.

Развитием современных средств ранней диагностики заболеваний сердечно-сосудистой системы человека является система «Акустокард». Она предназначена для сбора записей фонограмм, получаемых пациентами самостоятельно или в ходе обследования в поликлиниках или кардиологических центрах (формат записи mp3 или wav), их обработки и рассылки полученных акустокардиограмм отправителям в защищенном режиме.

При передаче информации по каналам ТфОП, сотовой связи и Интернета файлы акустических сигналов тонов и шумов сердца могут быть защищены с использованием пакета программ компьютерной телефонии WAVELET-FONE [3] при сертификации на соответствие требованиям безопасности.

В локальных сетях телемедицины для сбора биометрических данных звуковых сигналов сердца планируется применение модулей NI 9234 и NI WLS-9163 IEEE 802.11b/g распределенной системы виброакустических измерений «National Instruments cDAQ». Применяемый в модулях NI

WLS-9163 IEEE 802.11b/g криптографический алгоритм шифрования данных AES с размерностью ключа 128 бит также подлежит сертификации на соответствие требованиям федерального закона.

СПИСОК ЛИТЕРАТУРЫ:

1. Федеральный закон Российской Федерации от 27 июля 2006 г. № 152-ФЗ «О персональных данных».
2. *Потапов А. И., Самойлов Б. В., Потапов И. А.* Технические и аппаратно-программные средства телемедицины: Научное и учебно-методическое справочное пособие. СПб.: СЗТУ, 2005. — 451 с.
3. *Горшков Ю. Г.* Новые решения речевых технологий безопасности // Специальная техника. 2006. № 4. URL: http://st.ess.ru/publications/4_2006/gorshkov/gorshkov.pdf.

Н. Е. Гунько

БИОМЕТРИЧЕСКИЕ ПРИЗНАКИ ПОЧЕРКА ДЛЯ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Системы доступа и защиты информации, основанные на биометрических технологиях, являются не только достаточно надежными (биометрические данные невозможно передать другому лицу), но и очень удобными для пользователей на сегодняшний день, поэтому они приобретают все большую популярность как среди юридических лиц (фирмы, компании, организации), так и среди физических.

Биометрические системы защиты информации в основном строятся с использованием особенностей (признаков) [1–6], которые можно условно разделить на две основные группы:

· генетические и физиологические особенности: структура ДНК, геометрия ладони, отпечаток пальца, рисунок радужной оболочки (сетчатки глаза), геометрические характеристики лица;

· индивидуальные поведенческие особенности, присущие каждому человеку: *почерк*, речь, «индивидуальный стиль работы на клавиатуре», походка и ряд других [1].

На данный момент почерк используется в системах защиты информации для идентификации пользователя. Используется его роспись (иногда написание кодового слова). Цифровой код идентификации формируется в зависимости от необходимой степени защиты и наличия оборудования (графический планшет, экран КПК Palm и т. д.) двух типов:

1) по самой росписи, т. е. для идентификации, используется просто степень совпадения двух картинок (изображений подписи);

2) по росписи и динамическим характеристикам написания, т. е. для идентификации, строится свертка, в которую входит информация по непосредственно подписи, временным характеристикам нанесения росписи и статистическим характеристикам динамики нажима на поверхность [2].

В планируемых исследованиях наша задача пойти дальше, чем известная идентификация пользователя по его почерку [5, 6], и разработать (как и в [5, 6]) *правило принятия решения* (ППР) о психологических характеристиках человека, в нашем случае потенциального злоумышленника, для систем защиты информации.

Почерк характеризуется целым набором признаков, позволяющих отличить почерк конкретного человека от почерков всех остальных людей. Многолетняя практика позволила графологам заметить определенные закономерности в почерке и их обусловленность личностными