УДК 004.056

**В.Д. Зыков, Р.В. Мещеряков, А.С. Романов, А.А. Шелупанов**

# Обеспечение защиты информации при обработке медицинских биометрических данных

Рассматриваются вопросы обеспечения защиты информации при обработке в медицинских системах. Приводится перечень технических мероприятий, требуемых для обеспечения защиты персональной медицинской информации.
**Ключевые слова:** защита информации, медицинская информационная система, биометрический сигнал, информационная безопасность.

Для обработки медицинских данных пациентов лечебно-профилактических учреждений, как правило, используют медицинские информационные системы, которые подразумевают наличие автоматизированного документооборота, электронных архивов медицинской информации и наличия электронной истории болезни каждого пациента [1].

Практически все стандарты медицинской информатики так или иначе связаны с ведением электронной истории болезни. К известным стандартам медицинской информатики необходимо отнести HL7, DICOM, SNOMED, RCC. Одни стандарты описывают терминологию, которая должна быть в ней использована, другие – передачу медицинских документов и изображений в электронную историю болезни, третьи – способы организации данных в электронной истории болезни, четвертые – обеспечение доступа медицинских работников и самих пациентов к электронной истории болезни и т.д. [2].

По каждому пациенту ведутся персональные медицинские записи. Такая запись обычно содержит описание проведенного осмотра или обследования (в том числе лабораторного или инструментального), консультации, назначения, выполненной операции или процедуры, обобщенного заключения о состоянии больного и т.д. Совокупность таких записей, выполненных традиционным способом в конкретном медицинском учреждении, и составляет историю болезни или амбулаторную карту пациента.

Медицинские информационные системы, обеспечивающие ведение, хранение и доступ к ЭПМЗ, могут значительно повысить безопасность и качество медицинской помощи, увеличить оперативность представления медицинской информации, обеспечить комфортность в работе медицинского персонала. Такие системы могут использоваться отдельным медицинским работником, подразделением или службой или охватывать целое медицинское учреждение, включающее удаленные филиалы.

Несмотря на это, медицинские информационные системы в настоящий момент играют лишь второстепенную роль, поскольку правовой и юридический статус ЭПМЗ не определен. Фактически такие системы сейчас используются для подготовки и печати медицинских документов, которые затем подписываются и далее участвуют в традиционном медицинском документообороте, определенном существующими нормативными документами.

Для использования электронных медицинских документов в электронном документообороте необходимо решение ряда организационно-технических вопросов, в первую очередь связанных с соблюдением врачебной тайны и защитой персональных данных.

Специфика врачебной тайны [3] состоит в том, что её сохранность гарантируется законодательно так же, как и законодательно обеспечивается путём установления определённых запретов и юридической ответственности за её разглашение. К перечню сведений, которые входят в содержание врачебной тайны относятся:

- факт обращения гражданина за медицинской помощью;
- состояние его здоровья;
- диагноз, лечение и прогноз заболевания;
- наличие у гражданина психического расстройства, состояние его психического здоровья;
- факт обращения за психиатрической помощью и лечение в учреждении, оказывающем такую помощь;
- его личные и семейные тайны;
- трансплантация, искусственное оплодотворение, имплантация эмбриона;
- личность донора и реципиента.

В российском законодательстве по врачебной тайне, рассмотренном выше, не определены конкретные требования по защите сведений, относящихся к врачебной тайне. Данные требования определены законодательством в области персональных данных.

Таким образом, к операторам персональных данных относятся все медицинские учреждения, а сведения, относящиеся к врачебной тайне, входят во множество сведений, относящихся к персональным данным, образуя подмножество персональных медицинских данных. Технические меры по защите ПД выполняются в соответствии с нормативно-методическими документами регуляторов [4–12]. Комплекс мероприятий по технической защите ПД включает в себя указанные в таблице мероприятия.

**Технические мероприятия по защите персональных данных**

| № п/п | Содержание мероприятий | Комментарии |
|---|---|---|
| 1 | Инвентаризация информационных ресурсов | С целью выявления присутствия и обработки в них ПД |
| 2 | Предпроектное обследование ИСПД | На соответствие требованиям по защите персональных данных |
| 3 | Выявление актуальных угроз безопасности и разработка моделей угроз и нарушителя | |
| 4 | Разработка технического задания на систему защиты персональных данных (СЗПД) | |
| 5 | Создание СЗПД | В том числе выполнение требований по инженерно-технической защите помещений (пожарная безопасность, охрана, электропитание и заземление, санитарные и экологические требования) в соответствии с требованиями регуляторов |
| 6 | Развертывание и ввод в эксплуатацию СЗПД в ИСПД | В том числе поставка, внедрение средств защиты ПД в ИСПД |
| 7 | Аттестация СЗПД по требованиям безопасности информации | Для ИСПД 1, 2-го классов, для ИСПД 3-го класса – декларирование соответствия требованиям безопасности информации |
| 8 | Сертификация средств защиты ПД в ИСПД | При использовании несертифицированных средств защиты ПД в ИСПД |
| 9 | Эксплуатация ИСПД и СЗПД | Включает контроль безопасности ПД, сопровождение средств защиты ПД в ИСПД |

Официальным подтверждением того, что СЗПД соответствует требованиям по защите ПД, является Аттестат соответствия требованиям по безопасности информации.

Практика специалистов показывает, что наиболее важными этапами являются предпроектное обследование, построение модели угроз и классификация ИСПД, поскольку являются отправными точками для дальнейшей работы. Одним из наиболее трудоемких этапов является разработка необходимой документации и требований по защите ПД (формирование модели угроз персональным данным), которая занимает от трех до шести месяцев.

Специалисты отмечают, что последующие этапы, связанные с выбором средств защиты информации, отвечающих перечню актуальных угроз ПД, а также их внедрение не вызывают особых сложностей: на рынке представлено достаточно большое число решений, и проектировщикам остается подобрать наиболее подходящее по требованиям и условиям применения.

Таким образом, обеспечение защиты обработки медицинских биометрических данных должно проводиться в соответствии с действующим законодательством Российской Федерации. В настоящее время предлагаемые подходы проходят внедрение в ряде лечебно-профилактических учреждений Томской области.

Работа поддержана ФЦП «Научные и научно-педагогические кадры инновационной России» (ГК №П1083).

*Литература*

1. Радченко С.В. Основные подходы к автоматизации ЛПУ // Врач и информационные технологии. – 2008. – № 6. – С. 26–34.

2. Емелин И.В. Интерфейсы работы с медицинским оборудованием и стандарты передачи медицинской информации. // Компьютер-Информ. – 2006. – №23. – С. 2.

3. Федеральный закон от 22 июля 1993 г. № 5487-1, «Основы законодательства Российской Федерации об охране здоровья граждан» (с изменениями от 2 марта 1998 г., 20 декабря 1999 г., 2 декабря 2000 г., 10 января, 27 февраля, 30 июня 2003 г., 29 июня, 22 августа, 1, 29 декабря 2004 г., 7 марта 2005 г.) [Электронный ресурс]. – Режим доступа: http://www.rg.ru/1993/08/19/osnovy-zdorovya-dok.html, свободный (дата обращения: 24.10.2010).

4. Постановление Правительства Российской Федерации от 17 ноября 2007 г. № 781, г. Москва, «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2007/11/21/personalnye-dannye-dok.html свободный (дата обращения: 24.10.2010).

5. Приказ Федеральной службы по техническому и экспортному контролю (ФСТЭК России) Федеральной службы безопасности Российской Федерации (ФСБ России) Министерства информационных технологий и связи Российской Федерации (Мининформсвязи России) от 13 февраля 2008 г. № 55/86/20, г. Москва, «Об утверждении Порядка проведения классификации информационных систем персональных данных» [Электронный ресурс]. – Режим доступа: http://www.rg.ru/2008/04/12/informaciya-doc.html, свободный (дата обращения: 24.10.2010).

6. Приказ Россвязькомнадзора № 08 от 17.07.08 г. «Об утверждении образца формы уведомления об обработке персональных данных» [Электронный ресурс]. – Режим доступа: http://46.rsoc.ru/docs/46/Prikaz_Rossvjaz6komnadzora_ot_17_07_2008_N_08.rtf, свободный (дата обращения: 24.10.2010).

7. Нормативно-методический документ ФСТЭК «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 г. [Электронный ресурс]. – Режим доступа: http://www.altell.ru/assets/images/laws/rds/Fstec3.pdf, свободный (дата обращения: 24.10.2010).

8. Нормативно-методический документ ФСТЭК «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных» от 14 февраля 2008 г. [Электронный ресурс]. – Режим доступа: http://www.altell.ru/assets/images/laws/rds/Fstec4.pdf, свободный (дата обращения: 24.10.2010).

9. Нормативно-методический документ ФСТЭК «Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных» от 15 февраля 2008 года [Электронный ресурс]. – Режим доступа: http://www.altell.ru/assets/images/laws/rds/Fstec1.pdf, свобод-ный (дата обращения: 24.10.2010).

10. Нормативно-методический документ ФСТЭК «Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» от 15 февраля 2008 г. [Электронный ресурс]. – Режим доступа: http://www.altell.ru/assets/images/laws/rds/Fstec2.pdf, свободный (дата обращения: 24.10.2010).

11. Нормативно-методический документ ФСБ «Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации» от 21 февраля 2008 года [Электронный ресурс]. – Режим доступа: http://www.altell.ru/assets/images/laws/rds/149_54_144.pdf, свободный (дата обращения: 24.10.2010).

12. Нормативно-методический документ ФСБ «Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну, в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных» от 21 февраля 2008 года [Электронный ресурс]. – Режим доступа:
http://www.altell.ru/assets/images/laws/rds/149_6_6_622.pdf, свободный дата обращения: 24.10.2010).

**Шелупанов Александр Александрович**
Д-р техн. наук, проф. проректор по научной работе ТУСУРа
Тел.: (382-2) 41-34-26
Эл. почта: office@keva.tusur.ru

**Зыков Владимир Дмитриевич**
Аспирант каф. комплексной информационной безопасности электронно-вычислительных систем (КИБЭВС) ТУСУРа
Тел.: (382-2) 41-34-26
Эл. почта: zvd@udcs.ru

**Мещеряков Роман Валерьевич**
Канд. техн. наук, доцент каф. КИБЭВС
Тел.: (382-2) 41-34-26
Эл. почта: mrv@keva.tusur.ru

**Романов Александр Сергеевич**
Аспирант каф. КИБЭВС
Тел.: (382-2) 41-34-26
Эл. почта: ras@ms.tusur.ru

Zykov V.D., Mescheriakov R.V., Romanov A.S., Shelupanov A.A.
**Ensuring of information protection in the medical biometric data processing**

The ensuring problems of information protection in medical systems processing are considered. A list of the measures needed for guaranteeing protection of the personal medical information is given.
**Keywords:** information protection, medical information system, biometric signal, information safety.