Российская академия медицинских наук

Проблемы организации обработки персональных данных в медицинских учреждениях

проф., д.т.н. Столбов А.П., МИАЦ РАМН

Москва, 30 октября 2008 г.

Конвенция Совета Европы от 28.01.1981 г. "О защите физических лиц при автоматизированной обработке персональных данных"

Закон "О ратификации Конвенции Совета Европы "О защите физических лиц при автомат-ой обработке перс. данных", № 160-ФЗ от 19.12.2005 г.

Закон "О персональных данных", № 152-ФЗ от 27.07.2006 г.

Основы законодательства Российской Федерации об охране здоровья граждан, № 5487-1 от 22.07.1993 г. (ред. от 18.10.07 г. № 230-ФЗ) ст.19,30,31,32,33,34, 61

Перечень сведений конфиденциального характера, Указ Президента РФ № 188 от 06.03.1997 г. (в ред. Указа Президента РФ от 23.09.05 г. № 1111)

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, постановление Правительства РФ от 17.11.07 г. № 781

Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, постановление Правительства РФ от 15.09.08 г. № 687 [пп.4,7 - обособление] !!

Порядок проведения классификации информационных систем персональных данных, приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.08 г. № 55/86/20

Положение о ведении реестра операторов, осуществляющих обработку персональных данных, приказ Россвязьохранкультуры от 28.03.08 г. № 154

Об утверждении образца формы уведомления об обработке персональных данных, приказ Россвязьохранкультуры от 13.05.08 г. № 340

НОРМАТИВНО-МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ФСТЭК

Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утв. 14.02.08 г.) (ДСП)

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (утвержден 15.02.08 г.) (ДСП)

Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных (утв. 15.02.08 г.) (ДСП)

Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утв.15.02.08 г.) (ДСП) К1 !!!

Специальные требования и рекомендации по технической защите конфиденциальной информации (Гостехкомиссия РФ, утв. 30.08.02 г.)

Автоматизированные системы. Зашита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (Гостехкомиссия РФ, утв. 30.03.1992 г.) 1Г

[www.government.nnov.ru/_data/objects/29371/fstek.ppt]

ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ ДОЛЖНА:

- зарегистрироваться в качестве оператора ПД – направить уведомление в Россвязькомнадзор – уполномоченный орган по защите прав субъектов персональных данных (ст. 22, 23 Закона)
- организовать получение, учет и хранение письменного согласия пациента на обработку его ПД (ст. 6,9,10 Закона)
- организовать информирование пациентов по их запросам о способах и сроках обработки их ПД, а также лицах, имеющих к ним доступ (ст. 14 Закона)
- организовать и поддерживать систему защиты информации от несанкционированного доступа (см. на сайте ФСТЭК www.fstec.ru):
  - получить лицензию ФСТЭК на организацию технической защиты информации
  - закупить и установить сертифицированные средства защиты информации и обмена данными (шифрование, ЭЦП и др.)
  - издать организационно-распорядительные документы о допуске персонала и регламентах обработки конфиденциальной информации, подобрать и обучить персонал (отв. за ОБИ)
  - аттестовать ИС на соответствие требованиям защиты информации по классам 1Г и К1* (по документам ФСТЭК \ Гостехкомиссии РФ)

Выполнимо ли всё это на практике до 1 января 2010 г. ?!

ГОСТ Р 52636-2006 Электронная история болезни. Общие положения

ГОСТ Р 52069.0-2003 Защита информации. Система стандартов. Основные положения.

ГОСТ Р 50922-2006 Основные термины и определения

ГОСТ Р ИСО/МЭК 15408-1,2,3-2002 Критерии оценки безопасности информационных технологий. Функциональные требования безопасности

ГОСТ Р ИСО/МЭК ТО 13335-5-2006, 13335-1,3,4-2007 Информационная технология. Методы и средства обеспечения безопасности.

ГОСТ Р ИСО/МЭК 27001-2006 Системы менеджмента информационной безопасности. Требования

ГОСТ Р ИСО/МЭК 17799-2005 Информационная технология. Практические правила управления информационной безопасностью

ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения

О лицензировании деятельности по технической защите конфиденциальной информации, постановление Правительства РФ от 15.08.06 г. № 504

Концепция обеспечения информационной безопасности в системе ОМС на период до 2010 года (утверждена в 2005 г.)

ЗАЩИТА ИНФОРМАЦИИ – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным

- разграничение полномочий доступа к данным (C, U, D, R, P, S и др.)
- авторизация, контроль и учет действий с данными (регистрация событий)
- контроль копирования, печати, обмена данными по каналам связи
- межсетевое экранирование + защита от вирусов
- учет внешних носителей данных
- резервное копирование / восстановление данных
- раздельное хранение носителей данных с резервными копиями
- контроль доступа в помещения и к компьютерам
- применение устройств идентификации пользователей для доступа

---

1) **ОБСЛЕДОВАНИЕ** и оформление документа о классе ИС (1Г, К1), определение способов и состава средств защиты информации (СЗИ), разработка ТЗ на создание комплексной системы защиты информации, в том числе разработка модели угроз, проектирование
2) Ввод в эксплуатацию – закупка и инсталляция сертифицированных СЗИ, обучение персонала, издание приказов о допуске персонала и регламентах обработки конфиденциальной информации
3) **АТТЕСТАЦИЯ** системы на соответствие требованиям безопасности обработки конфиденциальной информации (по кл.1Г, К1) лицензия, аттестат - на 3 года

ЗАЩИТА ИНФОРМАЦИИ – комплекс организационно-технических мероприятий, направленных на предотвращение потери, искажения и несанкционированного доступа к данным

- разграничение полномочий доступа к данным (C, U, D, R, P, S и др.)

Возможна ли передача работ по защите информации на аутсорсинг (полностью или частично) !?

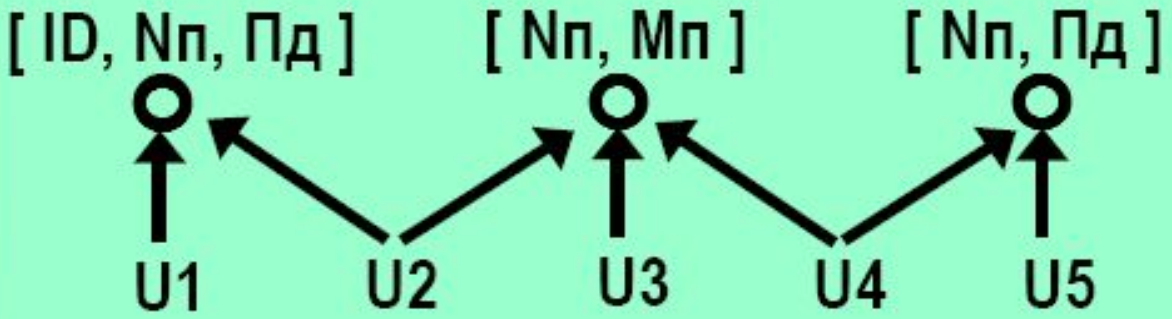
Можно ли при этом не получать лицензию на организацию технической защиты информации !?

1

2, обучение персонала, издание приказов о допуске персонала и регламентах обработки конфиденциальной информации

3) Аттестация системы на соответствие требованиям безопасности обработки конфиденциальной информации (по классам 1Г, К1)

РОЛЕВОЙ ДОСТУП К ПЕРСОНАЛЬНЫМ ДАННЫМ



U1, U5 – регистратор
U2, U4 – врач, сестра
U3 – лаборант, эксперт*

Пд – Ф.И.О., пол, дата рождения, адрес места жительства, место работы, др.
ID – внешний = СНИЛС, номер полиса ОМС, номер паспорта и т.д.
Nп – локальный = № медкарты, талона, направления и т.д.
Mп – медицинские данные, пол и возраст пациента

- Доступ к внешним базам данных по документированному запросу
- Изменение требований к внешней полицевой отчетности на основе принципа разумной достаточности и необходимости !!!

Пример нарушения -- приказ ФФОМС от 10.01.08 г. № 2 !?

Типы операторов, получающих ПД:
- только от пациента
- только от других операторов
- от пациента и других операторов

- передающих и
- НЕ передающих ПД другим операторам

Получение согласия пациента !?

пользователь = оператор, передача = доступ

ПЕРЕДАЧА \ ДОСТУП К ДАННЫМ О СОСТОЯНИИ ЗДОРОВЬЯ

- персонифицированные { Пд, Мп, ID*, Nп }

Принято сейчас !!!

- с использованием внешних ID (СНИЛС, номер паспорта, полиса ОМС)

регистр ПФР

- с использованием локальных Nп (номер медкарты, талона и т.д.)

Возможна идентификация пациента по запросу Nп

– "вторичный" пользователь

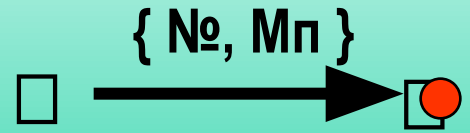
- псевдонимизированные

Ps = Cr(ID)

ID = Cr^{-1}(Ps)

Идентификация по запросу Ps SUS NHS, ISO/NP TS 25237

- и анонимные обезличенные



Идентификация пациента невозможна

Пд - Ф.И.О., адрес места жительства, место работы (персональные данные)

Мп - пол, дата рождения, медицинские и прочие данные о пациенте

Ps - псевдоним, Cr - криптопреобразование, № - условный номер, криптоним

Стандарты ISO/TC 215 Health informatics

ISO/TR 21089:2004 Trusted end-to-end information flows

ISO 22857:2004 Guidelines on data protection to facilitate trans-border flows of personal health information

ISO/TS 21091:2005 Directory services for security, communications and identification of professionals and patients

ISO/TS 22600-1,2:2006 Privilege management and access control. Part 1: Overview and policy management, Part 2: Formal models

ISO/NP TS 22600-3 Implementations; ISO/NP TS 25237 Pseudonymisation*

ISO/CD TS 21298 Functional and structural roles

ISO/NP TS 21547-1 Secure archiving of electronic health records. Principles and requirements, ISO/NP TR 21547-2 Guidelines

ISO/NP 27789 Audit trails for electronic health records

ISO 27799:2008 Information security management in health using ISO/IEC 27002:2005 Information technology. Security techniques. Code of practice for information security management (взамен ISO/IEC 17799:2005)

ISO/IEC 27006:2007 Security techniques. Requirements for bodies providing audit and certification of information security management systems

СПАСИБО !

Столбов Андрей Павлович

stolbov@mcramn.ru
ap100lbov@mail.ru

www.mcramn.ru