InterSystems Symposium 2009

З а щ и т а персональных данных в медицинских ИС

проф., д.т.н. Столбов А.П., МИАЦ РАМН

Москва, 15 сентября 2009 г.

Закон "О персональных данных" (ПДн), № 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. 61

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

Об утверждении Положения об обеспечении безопасности ПДн при их обработке в информационных системах персональных данных (ИСПДн), постановление Правительства РФ от 17.11.07 г. № 781 *

Об утверждении требований к материальным носителям биометрических ПДн и технологиям хранения таких данных вне ИСПДн, постановление Правительства РФ от 06.07.08 г. № 512

Об утверждении положения об особенностях обработки ПДн, осуществляемой без использования средств автоматизации, постановление Правительства РФ от 15.09.08 г. № 687 пп.4, 7 - обособление !

пример приказ МЗСР от 18.03.09 № 119н (о ВМП) - талон, заявление на согласие

Об утверждении Порядка проведения классификации ИСПДн, приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.08 г. № 55/86/20 *

Об утверждении Положения о ведении реестра операторов, осуществляющих обработку ПДн, приказ Россвязьохранкультуры от 28.03.08 г. № 154

Об утверждении образца формы уведомления об обработке ПДн, приказы Россвязькомнадзора от 17.07.08 г. № 8, от 18.02.09 г. № 42

НОРМАТИВНО-МЕТОДИЧЕСКИЕ ДОКУМЕНТЫ ФСТЭК и ФСБ

- Методика определения актуальных угроз безопасности ПС при их обработке в информационных системах ПД (ФСТЭК, 14.02.08 г., ДСП)
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах ПД (ФСТЭК, 15.02.08 г., ДСП)
- Основные мероприятия по организации и техническому обеспечению безопасности ПД, обрабатываемых в информационных системах персональных данных (ФСТЭК, 15.02.08 г., ДСП) -> К1 -> аттестация !!!
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах ПД (ФСТЭК, 15.02.08 г., ДСП)
- Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К) (Гостехкомиссия РФ, №7.2/02.03.2001г.)
- Автоматизированные системы. Зашита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации (Гостехкомиссия РФ, 30.03.1992 г.)
- 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 ПД при их обработке в ИС ПД (ФСБ, 21.02.2008 г.)
- Методические рекомендации по обеспечению с помощью криптосредств безопасности ПД при их обработке в ИС ПД с использованием средств автоматизации (ФСБ, 21.02.2008 г.)

ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ (оператор ПД) ДОЛЖНА:

- оформить **акт** об отнесении ИС обработки ПД к классу **К1 !!?**
  - постановление Правительства РФ от 17.11.07 г. № 781 (п. 6 Положения)
  - приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.08 г. № 55 / 86 / 20

  = проблемы классификации специальных ИСПДн **!!?**
- **зарегистрироваться в качестве оператора ПД** – направить уведомление в Роскомнадзор – уполномоченный орган по защите прав субъектов персональных данных (ст. 22, 23 Закона), указать класс **К1**
- организовать **получение, учет и хранение письменного согласия** пациента на обработку его ПД (ст. 6,9,10 Закона) = печать **!!! А**
- организовать **информирование пациентов по их запросам** о способах и сроках обработки их ПД, лицах, имеющих к ним доступ (ст.14), а также об обработке их ПД, полученных от третьих лиц (ст.18)

  ответ пациенту – в течение **10** раб. дней, ответ Органу – 7 раб. дней (бесплатно)

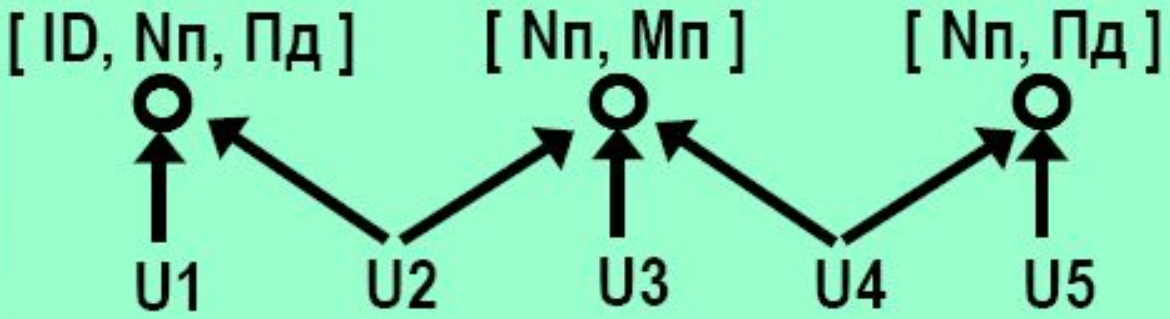
  = **Проблема -> федеративные системы управления ID !!! А**
- организовать и поддерживать **систему защиты конфиденциальной информации** от несанкционированного доступа = доступ ("Панцирь-К,С") + защита периметра + криптозащита МН **!!!**

Письмо ФФОМС от 22.04.2008 г. № 2170/90-и "Об организации работ по технической защите информации"

СОЗДАНИЕ СИСТЕМЫ ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ

- обследование объекта – определение каналов утечки информации и модели нарушителя – оформление документа "Модель угроз безопасности ... " – определение класса защиты системы от несанкционированного доступа к информации – разработка ТЗ (техпроекта) на создание системы (опеределение мер, способов и состава средств защиты и др.) = проблемы классиф-ции спец. ИСПДн !!
- закупка и установка сертифицированных средств защиты информации (срок действия сертификата на СЗИ – 3 года); установка криптосредств защиты – только организациями, имеющими лицензию ФСБ
- издание приказов о допуске персонала и регламентах обработки конфиденциальной информации, назначении ответственных за ОБИ, обучение персонала
- испытания системы -> приказ о вводе в эксплуатацию
- аттестация ИС (объекта) на соответствие требованиям защиты информации по классам К1 \ 1Г уполномоченными организациями, имеющими специальные лицензии ФСТЭК и ФСБ (срок действия аттестата ИС – 3 года)
- получение лицензии ФСТЭК на организацию технической защиты информации (срок действия лицензии – 5 лет) = обязательно нужны сотрудники со специальной подготовкой по ОБИ !?

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: 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

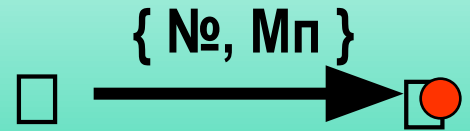
- псевдонимизированные

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

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

Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами , постановление Правительства РФ от 29.12.07 г. № 957

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 ТО 18044-2007 Методы и средства обеспечения безопасности. Менеджмент инцидентов информационной безопасности

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

(август 2009)

www.rsoc.ru - Роскомнадзор
www.ispdn.ru !!!

СПАСИБО !

Столбов Андрей Павлович

stolbov@mcramn.ru
ap100lbov@mail.ru

www.mcramn.ru