MedSoft - 2010

Методические и практические аспекты организации обработки и защиты персональных данных

Столбов А.П., д.т.н., МИАЦ РАМН

Москва, 16 апреля 2010 г.

Конституция Российской Федерации (12.12.1993 г., ред. ... от 21.07.07 г. № 5-ФЗ), ст. 23, 24 (неприкосновенность частной жизни, личная и семейная тайна), ст. 41, 42 (недопустимость сокрытия информации ... угроза жизни и здоровью)

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 "Об информации, информационных технологиях и защите информации", № 149-ФЗ от 27.07.2006 г.

Закон "О персональных данных", № 152-ФЗ от 27.07.2006 г. (Закон)
(в ред. закона от 27.12.2009 г. № 363-ФЗ - изм. ст. 19, ст. 25 !!!)

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

Закон "О медицинском страховании граждан в Российской Федерации, № 1499-1 от 28.07.1991 г. (ред. от 29.12.06 г. № 258-ФЗ) [ст. 12 ведение баз данных]

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)

Трудовой кодекс Российской Федерации, ст. 85-90 (защита персональных данных работника) (ст. 88 – согласие сотрудника на передачу его ПД) !

Закон "Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования", № 27-ФЗ от 01.01.1996 г. (ред. ... от 19.07.07 г. № 140-ФЗ)

О мерах по обеспечению информационной безопасности РФ при использовании информационно-телекоммуникационных сетей международного информацинного обмена, Указ Президента РФ от 17.03.2008г. № 351 [Интернет]

Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, постановление Правительства РФ от 17.11.2007 г. № 781

Об утверждении Требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных, постановление Правительства РФ от 06.07.2008 г. № 512

Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации, постановление Правительства РФ от 15.09.2008 г. № 687

!!! пп. 4, 7 = обособление ПД от других сведений + подпись пациента о согласии на обработку ПД = приказ МЗСР от 18.03.2009 г. № 119н (по ВМП)

-> пересмотр большинства форм учетно-отчетных документов !?

Регламенты проверок операторов (см. на сайтах):

- приказ Роскомнадзора от 01.12.2009 г. № 630 (зарегистрирован в Минюсте)
- утвержден ФСБ 08.08.2009 г.

ВРАЧЕБНАЯ ТАЙНА – информация о факте обращения за медицинской помощью, состоянии здоровья гражданина, диагнозе его заболевания и иные сведения, полученные при его обследовании и лечении

Необходимость [письменного] согласия пациента или его законного представителя на передачу сведений, составляющих врачебную тайну, другим лицам, в том числе должностным лицам, в интересах его обследования и лечения

Предоставление этих сведений БЕЗ согласия пациента допускается:

- **в целях его обследования и лечения, в случае если он не способен из-за своего состояния выразить свою волю**
- **при угрозе распространения инфекционных заболеваний, массовых отравлений и поражений**
- **по запросу органов дознания и следствия, и суда**
- **в случае оказания помощи несовершеннолетнему в возрасте до 15 лет для информирования его родителей или законных представителей**
- **при наличии оснований, позволяющих полагать, что вред здоровью причинен в результате противоправных действий;**
- **в целях проведения военно-врачебной экспертизы**

[ст. 61 "Основ ... об охране здоровья ..."]

ПЕРСОНАЛЬНЫЕ ДАННЫЕ (ПД) – сведения о фактах, событиях и обстоятельствах частной жизни гражданина, позволяющие идентифицировать его личность [Указ Президента РФ от 06.03.97 г. № 188]

ПЕРСОНАЛЬНЫЕ ДАННЫЕ – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его Ф.И.О., год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

ОБРАБОТКА персональных данных – действия (операции) с персональными данными, включая сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в том числе передачу), обезличивание, блокирование, уничтожение

ОПЕРАТОР – государственный или муниципальный орган, юридическое или физическое лицо, организующее и(или) осуществляющее обработку ПД, а также определяющее цели и содержание обработки ПД

[закон "О персональных данных", ст. 3]

КОНФИДЕНЦИАЛЬНОСТЬ персональных данных – обязательное для соблюдения оператором или иным получившим доступ к персональным данным лицом требование не допускать их распространение без согласия субъекта персональных данных или наличия иного законного основания

ОБЛАДАТЕЛЬ информации – лицо, самостоятельно создавшее информацию либо получившее право разрешать или ограничивать доступ к информации, определяемой по каким-либо признакам [**обладатель информации = пациент**] **!!!**

Кодекс об административных правонарушениях РФ

ст. 13.11 -- нарушение порядка сбора, хранения, использования или распространения информации о гражданах –> штраф до 10 тыс. руб

ст. 13.12 -- нарушение правил защиты данных –> штраф до 20 тыс. руб или приостановление деятельности на срок до 90 суток

Уголовный кодекс РФ, ст. 137 -- незаконный сбор или распространение сведений о частной жизни лица, личной и семейной тайне –> штраф до 300 тыс. рублей, запрет занимать должность до 5 лет, арест до 6 месяцев

ИСПОЛЬЗОВАНИЕ персональных данных – действия (операции) с персональными данными, совершаемые оператором в целях принятия решений или совершения иных действий, порождающих юридические последствия в отношении субъекта ... или других лиц либо иным образом затрагивающих права и свободы субъекта ... или других лиц

ПЕРЕДАЧА (предоставление*) персональных данных – действия, направленные на их получение ОПРЕДЕЛЕННЫМ кругом лиц

РАСПРОСТРАНЕНИЕ* персональных данных – их ПЕРЕДАЧА или действия, направленные на их получение НЕОПРЕДЕЛЕННЫМ кругом лиц

БЛОКИРОВАНИЕ персональных данных – временное прекращение их обработки, в том числе их использования и передачи

ОБЕЗЛИЧИВАНИЕ персональных данных – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту персональных данных

[закон "О персональных данных", ст. 3]

Данные о состоянии здоровья могут обрабатываться только (ст. 10) [цели и условия обработки]:

- **на основании письменного согласия пациента**
- **для осуществления правосудия, безопасности РФ и т.д.**

- **если они необходимы для защиты его жизни или здоровья, жизни или здоровья других лиц, и получение согласия пациента невозможно**
- **в медико-профилактических целях, в целях установления медицинского диагноза, оказания медицинских и медико-социальных услуг при условии, что их обработка осуществляется лицом, профессионально занимающимся медицинской деятельностью и обязанным сохранять врачебную тайну**

[п.п. 3, 4 части 2 статьи 10 закона "О персональных данных"]

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

- гарантии конфиденциальности персональных данных при их обработке (ст. 7), но нет явной нормы об уведомлении субъекта ПД о случаях нарушении конфиденциальности (см. ст. 21 !?)
- контроль и надзор за их выполнением (ч. 3 ст.19)
  Россвязькомнадзор – уполномоченный орган по защите прав субъектов персональных данных (ст. 23), ФСТЭК, ФСБ
- письменное (!) согласие пациента на обработку и передачу его персональных данных и обязанность оператора предоставить доказательства этого согласия (ст. 9)
- право пациента на получение от оператора сведений о цели, способах и сроках обработки его персональных данных, и лицах которые имеют или могут иметь к ним доступ (ст. 14)
- обязанность оператора предоставить субъекту сведения об обработке его ПД, полученных от третьих лиц (ст. 18)
- уведомление об обработке персональных данных (ст. 22)

  БЕЗ уведомления - если обработка ПД -- без передачи третьим лицам:
  - данные о своих сотрудниках ("кадры")
  - данные о клиентах, необходимые для выполнения договора
- возможность аутсорсинга обработки ПД (часть 4 ст. 6)

До **1 января 2011** г. все ИС персональных данных должны быть приведены в соответствие требованиям этого закона **(ст. 25 - перенос на 1 год) !!!**

ОРГАНИЗАЦИЯ ЗДРАВООХРАНЕНИЯ (оператор ПД) ДОЛЖНА:

- провести обследование ИС, определить состав ИС ПД
  отдельные ИС = ИС "Пациенты" + ИС "Сотрудники" (кадры + зарплата)
- оформить акт об отнесении ИС обработки ПД к классу **К1 \ К3 !?**
  постановление Правительства РФ от 17.11.07 г. № 781 (п. 6 Положения)
  Класс ИС ПД -> требования к защите ПД (состав мер, методы, ...) **!!!**
- зарегистрироваться в качестве оператора ПД – направить уведомление в Роскомнадзор – уполномоченный орган по защите прав субъектов персональных данных (ст. 22, 23 Закона), указать класс ИС
- 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) = печать (**А**) (бесплатно)
  ответ пациенту – в течение **10** раб. дней, ответ Органу – 7 раб. Дней
- организовать и поддерживать систему обеспечения безопасности конфиденциальной информации **!!!**
  надо издать около 40 организационно-рапорядительных документов **!**

Закон "О персональных данных", ст. 9 – письменное согласие пациента на обработку персональных данных:

- Ф.И.О., адрес проживания пациента, номер документа, удостоверяющего личность, сведения о дате его выдачи и выдавшем органе
- наименование и адрес медицинского учреждения (оператора)
- цель обработки персональных данных = см. ст. 10 Закона \ основания !!
- перечень персональных данных, на обработку которых дается согласие
- перечень действий с персональными данными (... передача ... !?)
- способы обработки персональных данных
- состав передаваемых данных !?
- срок действия согласия, порядок его ОТЗЫВА !

Получение, учет и хранения согласия пациента !? Для другого оператора ?
Как передать, где хранить? Хранение на основе соглашения (СМО - ТФОМС)
Согласие: а) отдельный документ или б) в общем журнале !?
Автоматизация печати заполненного бланка согласия.
Отзыв согласия -> уничтожение ПДн !?

"вторичный" оператор

Типы операторов, получающих ПД:

- только от пациента
- только от других операторов
- от пациента и других операторов

Учетность и неотказуемость по фактам отправления и получения ПДн при межсетевом взаимодействии ИС разных операторов !!! (пр. № 58)

- передающих и - **не** передающих ПДн другим операторам

Закон "О персональных данных", ст. 9 – письменное согласие пациента на обработку персональных данных:

- Ф.И.О., адрес проживания пациента, номер документа, удостоверяющего личность, сведения о дате его выдачи и выдавшем органе
- наименование и адрес медицинского учреждения (оператора)
- цель обработки персональных данных = см. ст. 10 Закона
- перечень персональных данных, на обработку которых дается согласие =
  Ф.И.О., пол, дата рождения, адрес проживания, телефон, реквизиты полиса ОМС (ДМС), СНИЛС, данные о состоянии здоровья, заболеваниях, случаях обращения за медицинской помощью (*)
- перечень действий с персональными данными =
  сбор, систематизация, накопление, хранение, обновление, изменение, использование, обезличивание, блокирование, уничтожение, ПЕРЕДАЧА в страховую медицинскую организацию и фонд ОМС !?
- способы обработки персональных данных =
  ввод в базу данных, хранение, просмотр, печать, включение в реестры (списки), передача по внутренней сети, ПЕРЕДАЧА по каналам связи, на машинных носителях с соблюдением мер защиты от НСД !?
- состав передаваемых данных !? = см. перечень выше (*)
- срок действия согласия, порядок его ОТЗЫВА !

См. пример в файле и на www.mcramn.ru !!!

Уведомление -> портал Роскомнадзора www.pd.rsoc.ru - эл. гос. услуга !!!

Об утверждении образца формы уведомления об обработке персональных данных, приказы Рос[связь]комнадзора от 17.07.08 г. № 8, от 18.02.09 г. № 42

Форма уведомления + рекомендации по его заполнению (приложения)

- реквизиты медучреждения (оператора) = наименование, ИНН, адрес и др.
- цель обработки = см. п. 3, 4 части 2 ст. 10 закона "О персональных данных"
- категории персональных данных = для пациентов:
  Ф.И.О., пол, дата рождения, адрес места жительства, реквизиты паспорта, полиса ОМС и др., данные о состоянии здоровья
- категории субъектов персональных данных = работники + пациенты
- правовое обоснование =
  п.3, 4 ч. 2 ст.10 закона "О персональных данных", реквизиты лицензии на медицинскую деятельность + ссылки на нормативно-методические документы органа управления здравоохранением, фонда ОМС и др.
- перечень действий и способы обработки персональных данных =
  смешанная обработка, ввод, сбор, систематизация, накопление, хранение, изменение, удаление, использование, передача по внутренней сети, ПЕРЕДАЧА другим операторам на МН, по каналам связи !
- меры по защите информации =
  разграничение и контроль доступа к данным, сертифицированные средства защиты, отключение от Интернет и др.
  класс ИС ПД (К1 \ К3) - если несколько ИСПДн, то наивысший класс !

Ведение Реестра операторов Роскомнадзор www.pd.rsoc.ru

Приказ Россвязьохранкультуры от 28.03.2008 г. № 154 "Об утверждении Положения о ведении реестра операторов, осуществляющих обработку персональных данных"

- принятие решения о включении в Реестр или отказе на основании уведомления в течение 30 дней
- обязанность оператора в 10-дневный срок уведомлять о всех изменениях
- исключение из Реестра по письменному заявлению оператора (с обоснованием) или по решению суда
- публикация сведений о включении или исключении из Реестра в 3-дневный срок на сайте www.rsoc.ru (оператору присаивается рег.№, выдача свидетельства о включении в Реестр не предусмотрена)
- право Россвязькомнадзора:
  - проводить проверку полноты и достоверности сведений, запрашивать и безвозмездно получать необходимую информацию
  - принимать решение о приостановлении или прекращении деятельности по обработке ПД, осуществляемой с нарушением требований Закона

Доступ к Реестру – http://pd.rsoc.ru (по наименованию, ИНН)

- Прием уведомлений и ведение Реестра операторов ПД – за счет средств федерального бюджета

Выписка из реестра -> портал www.rsoc.ru - эл. гос. услуга !!!

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

Характеристики безопасности информации:

- **конфиденциальность** -- защита от несанкционированного доступа
- **целостность** -- защита от несанкционированого удаления и изменения
- **доступность** -- возможность получения доступа "в любое время"

- категорирование всех массивов данных (ИР) -> персональная, конфиденциальная, открытая информация (инвентаризация, идентификация и учет ИР, ответственные) -- очень трудоемкий этап !!!
- разграничение полномочий доступа к ресурсам ИС -> приказ о допуске
- авторизация, контроль и учет действий с данными + контроль копирования, печати, обмена данными по каналам связи -> регистрация событий в спец. электр. журналах ("черный ящик") -> просмотр + мониторинг = учётность + неотказуемость !!!
- применение устройств аутентификации пользователей для доступа в ИС, двухфакторная идентификация, пароли, карточки, e-Token, биометрические средства (отпечаток пальца) и др.
- межсетевые экраны -> выход в Интернет, интеграция ИС разного класса
- защита от вирусов

ЗАЩИТА ИНФОРМАЦИИ

- использование средств ЭЦП -> обеспечение целостности информации
- шифрование ПДн при передаче по каналам связи и на внешних МН *
  - сертифицированные ФСБ средства криптозащиты
  - ответственные (отдельный приказ), журнал учета криптоключей и др.
- учет внешних носителей данных (маркировка, журнал учета и др.)
- резервное копирование / восстановление данных (регламент, учет копий) -> обеспечение целостности данных
- раздельное хранение носителей данных с резервными копиями
- функциональная безопасность -> обеспечение непрерывности функционирования - доступность информации (надежность, отказоустойчивость, резервирование техники
- использование источников бесперебойного питания
- физическая защита = контроль доступа в помещения и к компьютерам, охрана периметра (контролируемой зоны)
- комплексное планирование, обеспечение ресурсами
- обучение персонала (инструктажи, допуск к работе, ознакомление с документы под роспись и т.д.)
- систематические проверки и контроль

Комплексность и равнопрочность системы защиты информации !!!

Порядок проведения классификации информационных систем персональных данных (приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008 г. № 55/86/20 = приказ "трех")

Методика определения актуальных угроз безопасности ПД при их обработке в информационных системах ПД (ФСТЭК, 14.02.2008 г., гриф "ДСП" снят 16.11.2009 г.)

Базовая модель угроз безопасности персональных данных при их обработке в информационных системах ПД (ФСТЭК, 15.02.2008 г., ДСП, выписка на сайте www.fstec.ru *)

Положение о методах и способах защиты информации в информационных системах персональных данных (приказ ФСТЭК от 05.02.2010 г. № 58, рег. № 16456 в Минюсте РФ от 19.02.2010 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.)

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К, Гостехкомиссия РФ, 30.08.2002 г.)

Методические рекомендации по организации защиты информации при обработке персональных данных в учреждениях здравоохранения, социальной сферы, труда и занятости (23.12.2009 г., согласованы с ФСТЭК)

Методические рекомендации по составлению частной модели угроз угроз безопасности персональных данных при их обработке в информационных системах персональных данных учреждений и организаций здравоохранения, социальной сферы, труда и занятости (23.12.2009 г.)

Модель угроз типовой медицинской информационной системы типового лечебно-профилактического учреждения (согласована с ФСТЭК, письмо от 27.11.09 г. № 240/2/4009) -> КЗ

www.minzdravsoc.ru/docs/mzsr/informatics/ - 26.12.2009 г.

Об организации работ по технической защите информации (письмо Федерального фонда ОМС от 22.04.2008 г. № 2170/90-и)

Call-центр 8-800-100-3984 (круглосуточно, бесплатно, до июля 2010) !!!

Реализация в МИС функций (печать и учет согласия пациента, блокирование и удаление ПДн, печать списка \ журнала доступа и т.д.) и требований по защите ПДн !?

Создание системы защиты персональных данных

- обследование объекта - определение класса ИСПД по таблице (**К1**)
- разработка "Модели угроз безопасности... " (определение каналов утечки информации и модели нарушителя, оценка актуальности угроз)
- разработка требований по защите ИСПДн на основе типовых требований и модели угроз -> разработка ТЗ (техпроекта) на создание системы (определение мер, способов и состава средств защиты и др.)
- закупка и установка сертифицированных средств защиты информации (срок действия сертификата на СЗИ – 3 года); установка средств защиты лицензиатами ФСТЭК и ФСБ **!?**

  постановление Правительства РФ от 17.11.07 г. № 781, п. 5 + СТР-К, п. 2.16 -> применение сертифицированных СЗИ **!!**
- издание приказов о допуске персонала и регламентах обработки конфиденциальной информации, назначении ответственных за ОБИ, обучение персонала и др., всего ~ 40 документов **!!!**
- испытания системы -> приказ о вводе в эксплуатацию
- декларирование соответствия (аттестация) объекта информатизации (**!**) (ИС) на соответствие требованиям защиты информации (см. СТР-К) **!!!**

Лицензия ФСТЭК на техническую защиту информации (лицензия – на 5 лет) = нужны сотрудники со спецподготовкой по ОБИ **!?**

Обследование и анализ информационной системы

- Анализ информационных ресурсов
  - Определение состава, содержания и местонахождения защищаемых ПДн
  - Категорирование ПДн -> всего 4 категории + категории субъектов ПДн
  - Оценка выполнения оператором обязанностей по обеспечению безопасности ПДн
- Анализ уязвимых элементов и возможных угроз безопасности ПДн
  - Оценка возможности физического доступа к ИС ПДн
  - Выявление возможных технических каналов утечки информации
  - Анализ возможностей программно-математического воздействия на ИС ПДн
  - Анализ возможностей электромагнитного воздействия на ПДн в ИС ПДн
- Оценка возможного ущерба от реализации угроз безопасности ПДн
  - Оценка непосредственного ущерба – причинения вреда субъекту ПДн
  - Оценка опосредованного ущерба – причинения вреда обществу или государству
- Анализ имеющихся мер и средств защиты ПДн
  - от физического доступа → Контролируемая зона -- территория, на которой исключено несанкционированное нахождение посторонних лиц, технических средств и т.п. -> охрана "периметра"
  - от утечки по техническим каналам
  - от несанкционированного доступа
  - от программно-математических воздействий
  - от электромагнитных воздействий

Рекомендации по обеспечению безопасности персональных данных при их обработке в ИС ... [ФСТЭК, 15.02.08 г.] - Отменены с 15.03.2010 г. !!!

Классификационные характеристики ИС персданных

- Категория обрабатываемых персональных данных (Хпд)
- Объем обрабатываемых ПДн -- количество субъектов ПДн (Хнпд)

→ Класс ИС

- Заданные характеристики безопасности ПДн в ИС
  - типовая ИС: только конфиденциальность
  - специальная ИС: конфиденциальность + целостность и\или доступность

Модель угроз ... → Методы и способы защиты (пр. № 58)

- Структура ИС
  - автономная (АРМ)
  - локальная (кампусная ЛВС)
  - распределенная

Взаимодействие между компьютерами -- по линиям связи, выходящим за пределы контролируемой зоны \ через Интернет

- Подключение к сетям общего пользования (Интернет): **Есть \ Нет**
- Режим обработки ПДн
  - однопользовательские
  - многопользовательские
- Разграничение прав доступа к ПДн
  - с равными
  - с разными правами

Критерии выделения отдельных ИС ПДн:
- категории субъектов → - пациенты, - сотрудники
- цель обработки
- категория ПДн

Матрица доступа к ресурсам ИС

- Местонахождение технических средств ИС: **в РФ \ вне РФ (частично)**

Приказ ФСТЭК, ФСБ, Мининформсвязи России от 13.02.2008 г. № 55/86/20

Классификация ИС персональных данных

Класс ИС ПД -> требования к защите ПД (состав мер, методы, ...) **!!!**

Категория 1 -- раса, национальность, политические взгляды, религиозные, философские убеждения, данные о СОСТОЯНИИ ЗДОРОВЬЯ, интимной жизни

Категория 2 -- данные, позволяющие идентифицировать субъекта ПД и получить о нем дополнительную информацию, за исключением ПД 1-ой категории

Категория 3 -- данные, позволяющие идентифицировать субъекта ПД

Категория 4 -- обезличенные и (или) общедоступные персональные данные.

Модель угроз типовой МИС типового ЛПУ

Категория	< 1000	< 100 тыс.	> 100 тыс.
4	К4	К4	К4
3	К3	К3	К2
2	К3	К2	К1
1	К1	К1	К1

Приказ "трёх"

Информационные системы, для которых нарушение заданной характеристики безопасности ПД может привести:

К1 -- к **значительным негативным последствиям** для субъектов ПД

К2 -- к **негативным последствиям** для субъектов ПД

К3 -- к **незначительным негативным последствиям** для субъектов ПД

К4 -- **не приводит** к негативным последствиям для субъектов ПД

Разработка замысла системы обеспечения безопасности ПДн

- Определение основных направлений по защите ПДн
  - по подразделениям
  - по уязвимым элементам, направлениям защиты
  - по категориям ПДн
- Выбор способов защиты ПДн
  - по направлениям защиты
  - по актуальным угрозам
  - по возможности реализации с учётом затрат
- Решение основных вопросов управления защитой ПДн
  - организация охраны
  - организация служебной связи и сигнализации
  - организация взаимодействия
  - организация резервирования программного и аппаратного обеспечения
  - организация управления администрированием
- Решение основных вопросов обеспечения защиты ПДн
  - финансового (нет нормативов) !?
  - технического и программного
  - информационного (в т.ч. наличия нужных НМД)
  - кадрового (в т.ч. обучение, мотивация)

+ Системность
+ Комплексность

Синергия !!!

ПРИНЦИПЫ

Законность
Персон. ответственность
Адекватность \ достаточность
Минимизация прав доступа
Комплементарность
Непрерывность
Разумная открытость
Равнопрочность

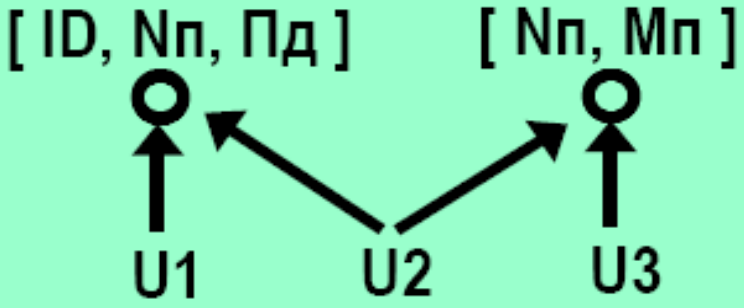
ОРД

Приказы
Отчеты, акты, перечни
Положения, инструкции
Журналы, ведомости
Техническая документация

МЕРЫ

Правовые меры
Организационные
Мотивационные
Физические меры
Технические средства
Программные
Программно-аппаратные

Ролевой доступ к персональным данным



U1 – регистратор
U2 – врач, сестра
U3 – лаборант, эксперт
Особый статус администратора безопасности - без допуска к Пд

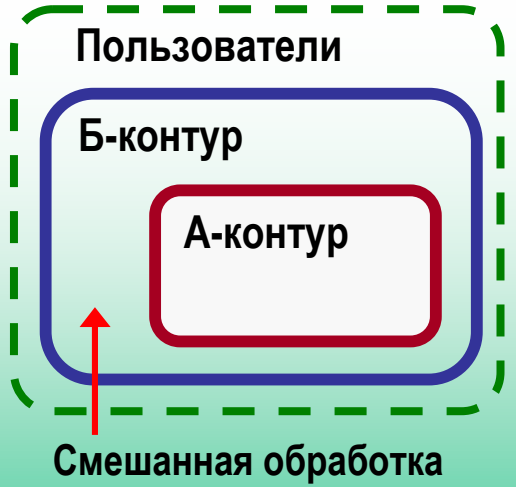
Аутентификация + Авторизация
Учетность + Неотказуемость
Равнопрочность

Права доступа
а) равные !?
б) разные

Разрешительная система доступа = запрещено все, что явно не разрешено !

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

Организация = { роль } + ИС = { ресурс ИС } (роль = функция)
Объект доступа = ресурс ИС (именованный объект ОС \ СУБД)
Матрица доступа пользователей к ресурсам ИС =
роль : { ресурс ИС : { право доступа } }
роль : { пользователь }
пользователь : { роль }
часто
редко
изменяется
право доступа = { создание, удаление, чтение, изменение, запуск, … }



Объем прав доступа в А-контуре = Объем возможностей доступа в Б-контуре

Передача \ доступ к данным о состоянии здоровья (оптимизация !?)

- персонифицированные { Пд, Мп, ID*, Nп } — ISO/TS 22220, prCEN/TR 15872

Принято сейчас !!!

- с использованием внешних ID (СНИЛС, № паспорта, полиса ОМС)

Контроль доступа ?

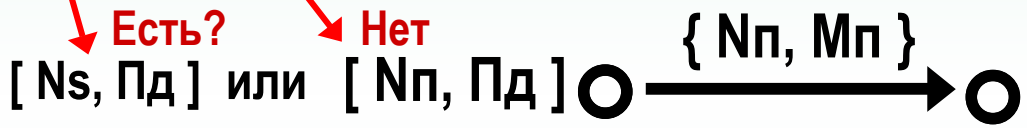
Нет

регистр ПФР

- с использованием локальных Nп (номер медкарты, талона, …) или Ns

Ns - внутрисистемный номер

Есть? Нет



Возможна идентификация пациента по запросу Nп, Ns

- псевдонимизированные

Ps = Cr(ID)

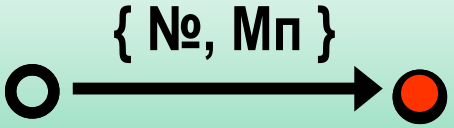
ID = $Cr^{-1}(Ps)$

Идентификация по запросу Ps

SUS NHS, ISO/TS 25237:2008

● – "вторичный" пользователь

- обезличенные и анонимные



Идентификация пациента невозможна !!!

Нет соответствия [Пд : №] !!!

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

Постановления Правительства РФ о лицензировании деятельности …

№ 504 от 15.08.06 г. по технической защите … информации

№ 957 от 29.12.07 г. … связанных с криптографическими средствами

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 Функциональные требования безопасности + ГОСТ Р ИСО/МЭК ТО 15446-2008 Руководство по разработке профилей защиты и заданий по 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 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

ISO/TS 22220:2009 Health informatics. Identification of subject of health care.

ISO/TS 25237:2208 Health informatics. Pseudonymization.

prCEN/TR 15872 Health informatics. Guidance on patient identification and cross-referencing of identities \ www.cen.eu/cenorm/homepage.htm

Смешанная обработка -> трудности организации контроля и учета доступа к конфиденциальной информации \ документам

Оценка достаточности мер по защите ПД -- при проведении государственного контроля и надзора (п. 3 Положения, пост. № 781) !!

Нужна ли оператору лицензия ФСТЭК на тех. защиту информации !?

Достаточность лицензии ФСТЭК для "самоаттестации" ИС ПДн (ОИ) !?

Аутсорсинг \ консалтинг при создании системы защиты информации !?

Создание системы защиты информации "под ключ" !?

При обследовании ИС -- до 50% трудозатрат оператора (подготовка исх. данных, инвертаризация ИР и т.д., если нет полных спецификаций процессов и ресурсов) + почти 80% -- при подготовке ОРД по шаблонам.

Аутсорсинг обработки ПД (часть 4 ст. 6 Закона) !!?

В договоре - обязанность уполномоченного оператора (аутсорсера) обеспечить конфиденциальность и безопасность ПД (п.10 Положения)

Передача работ по защите информации на аутсорсинг (полностью или частично) !?

Соглашение об уровне и качестве технического обслуживания (SLA, Services Level Agreement -> стандарты ITSM-ITIL, CobIT)

Вся ответственность на операторе !!!

Аутсорсер должен соответствовать всем требованиям (иметь лицензии, аттестаты и т.д.) !!!

Основы законодательства Российской Федерации об охране здоровья граждан

- ст.ст. 30, 31 права пациента, право на информацию о состянии здоровья
- ст.ст. 32, 33, 34 согласие на мед.помощь, отказ, оказание помощи без согласия
- ст. 61 врачебная тайна, согласие пациента на передачу сведений кому-либо !!!

О медицинском страховании граждан в Российской Федерациии
О психиатрической помощи и гарантиях прав граждан при ее оказании
О донорстве крови и ее компонентов
О трансплантации органов и тканей человека
Об основах обязательного социального страхования
О государственной социальной помощи
О санитарно-эпидемиологическом благополучии населения
Об индивидуальном (персонифицированном) учете в системе обязательного пенсионного страхования

В ЕС использование ИКТ в здравоохранении и вопросы безопасности медицинских данных регулируются **специальными законами !**

Права и обязанности (!) пациента и оператора

Рекомендации Госдумы от 20.10.2009 г. !!!

- согласие на медпомощь = согласие на обработку ПД !? (ст. 6)
- информирование пациента об обработке его ПД (ст.14)
- уведомление пациента о получении ПД от третьих лиц (ст.18)
- уничтожение ПД по требованию пациента \ сроки хранения МД (ст. 21)
- уведомление об утечке + усиление ответственности (ст. 21)

Нужен ПЛАН подготовки и внесения изменений !!!

- формальное и НЕформальное выполнение требований по защите персональных данных !?
- учет отраслевой специфики -> изменения в законах !!!
- соотнесение прав и обязанностей и пациентов и медучреждений
- принцип разумной достаточности и необходимости
- возможности сорсинга (финансы, кадры, время, лицензиаты ...)
- бюджет + рынок -> нормативы + тарифное регулирование
- специализация консультантов \ центры компетенции
- критерии консалтинга \ этика поставщика \ экспертиза
- аутсорсинг, аутстаффинг, аренда защищищенных ИС (ОИ)
- типовые решения \ пакет типовых ОРД \ комплект СЗИ-ЭЦП-ЭДО
- координация и кооперация : ОУЗ + ТФОМС + РЗН + ...
- классификация операторов \ аутсорсеры \ реестр операторов !!
- распределенные федеративные системы \ операторы \ пользователи \ особенности ОРД !?
- обезличивание + псевдонимизация (ISO/TS 25237) !! (анонимность)
- внедрение социальной карты \ профкарта \ портал госуслуг

www.rsoc.ru – Роскомнадзор (план проверок)
www.pd.rsoc – портал "Персональные данные" Роскомнадзора
www.fstec.ru – ФСТЭК
www.ispdn.ru + www.54.rsoc.ru + www.admin.smolensk.ru
www.medctat.narod.ru + + www.omskminzdrav.ru + www.miac74.ru

СПАСИБО !

Столбов Андрей Павлович
stolbov@mcramn.ru
ap100lbov@mail.ru

www.mcramn.ru