ООО «ИнфоЦентр»
региональный аттестационный центр

Принципы обработки и защиты информации и персональных данных

Екатерина Трохина

Старший инженер по защите информации

ООО «ИнфоЦентр»

О чем эта презентация?

I. Законодательные акты РФ;

II. Нормативно-правовые акты;

III. Основные принципы обработки персональных данных;

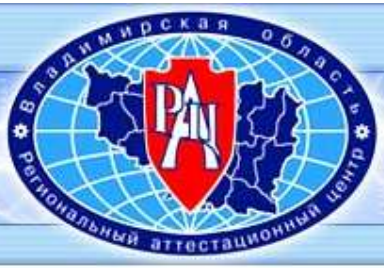
IV. Основные меры защиты персональных данных;

V. Организационные меры защиты персональных данных;

VI. Технические меры защиты персональных данных;

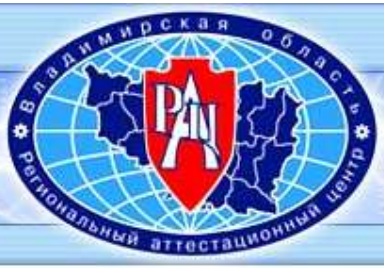
VII. Оценка соответствия требованиям безопасности персональных данных

VIII. Регуляторы



Законодательные акты Российской Федерации

- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»
- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»
- Постановление Правительства РФ от 01.11.2012 № 1119
- Постановление Правительства РФ от 21.03.2012 № 211
- Постановление Правительства РФ от 15.09.2008 № 687
- Постановление Правительства РФ от 06.07.2008 г. № 512



Законодательные акты Российской Федерации

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных» определяет:

- Основные понятия
- Цели обработки персональных данных
- Условия обработки персональных данных
- Особенности обработки персональных данных в ГИС и МИС
- Права субъектов персональных данных
- Обязанности оператора персональных данных

Федеральный закон от 27.06.2006 № 152

Основные понятия:

Персональные данные - любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)

Оператор - государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку персональных данных, а также определяющие цели обработки персональных данных, состав персональных данных, подлежащих обработке, действия (операции), совершаемые с персональными данными

Обработка персональных данных - любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с персональными данными, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных

Федеральный закон от 27.06.2006 № 152

Цели обработки персональных данных:

- До начала обработки ПДн оператор устанавливает цель обработки.
- Обработке подлежат только ПДн, которые отвечают целям их обработки.
- Не допускается объединение баз данных, содержащих персональные данные, обработка которых осуществляется в целях, несовместимых между собой.
- Содержание и объем обрабатываемых персональных данных должны соответствовать заявленным целям обработки. Обрабатываемые персональные данные не должны быть избыточными по отношению к заявленным целям их обработки.

Федеральный закон от 27.06.2006 № 152

Условия обработки персональных данных:

- обработка персональных данных осуществляется с согласия субъекта персональных данных на обработку его персональных данных.
- обработка персональных данных необходима для достижения целей, предусмотренных международным договором Российской Федерации или законом, для осуществления и выполнения возложенных законодательством Российской Федерации на оператора функций, полномочий и обязанностей.
- обработка персональных данных необходима для исполнения полномочий федеральных органов исполнительной власти, органов государственных внебюджетных фондов, исполнительных органов государственной власти субъектов Российской Федерации, органов местного самоуправления и функций организаций, участвующих в предоставлении соответственно государственных и муниципальных услуг, предусмотренных Федеральным законом от 27 июля 2010 года N 210-ФЗ "Об организации предоставления государственных и муниципальных услуг", включая регистрацию субъекта персональных данных на едином портале государственных и муниципальных услуг и (или) региональных порталах государственных и муниципальных услуг.

Федеральный закон от 27.06.2006 № 152

Условия обработки персональных данных:

- обработка персональных данных необходима для исполнения договора, стороной которого либо выгодоприобретателем или поручителем по которому является субъект персональных данных, а также для заключения договора по инициативе субъекта персональных данных или договора, по которому субъект персональных данных будет являться выгодоприобретателем или поручителем.

Федеральный закон от 27.06.2006 № 152

Особенности обработки персональных данных в ГИС и МИС:

- Государственные органы, муниципальные органы создают в пределах своих полномочий, установленных в соответствии с федеральными законами, государственные или муниципальные информационные системы персональных данных.
- Федеральными законами могут быть установлены особенности учета персональных данных в государственных и муниципальных информационных системах персональных данных, в том числе использование различных способов обозначения принадлежности персональных данных, содержащихся в соответствующей государственной или муниципальной информационной системе персональных данных, конкретному субъекту персональных данных.
- В целях обеспечения реализации прав субъектов персональных данных в связи с обработкой их персональных данных в государственных или муниципальных информационных системах персональных данных может быть создан государственный регистр населения, правовой статус которого и порядок работы с которым устанавливаются федеральным законом.

Федеральный закон от 27.06.2006 № 152

Права субъектов персональных данных:

- Право субъекта персональных данных на доступ к его персональным данным.
- Права субъектов персональных данных при обработке их персональных данных в целях продвижения товаров, работ, услуг на рынке, а также в целях политической агитации.
- Права субъектов персональных данных при принятии решений на основании исключительно автоматизированной обработки их персональных данных.
- Право на обжалование действий или бездействия оператора

Федеральный закон от 27.06.2006 № 152

Обязанности оператора персональных данных:

- Обязанности оператора при сборе персональных данных.
- Обязанности оператора принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных Федеральным законом № 152 и принятыми в соответствии с ним нормативными правовыми актами.
- Обязанности оператора принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.
- Обязанности оператора при обращении к нему субъекта персональных данных либо при получении запроса субъекта персональных данных или его представителя, а также уполномоченного органа по защите прав субъектов персональных данных

Федеральный закон от 27.06.2006 № 152

Обязанности оператора персональных данных:

- Обязанности оператора по устранению нарушений законодательства, допущенных при обработке персональных данных, по уточнению, блокированию и уничтожению персональных данных.
- Обязанности оператора уведомить об обработке персональных данных.

Законодательные акты Российской Федерации

Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации» определяет:

- Понятие информационной системы (ст. 13)

  Информационные системы включают в себя:
  1) государственные информационные системы - федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов;
  2) муниципальные информационные системы, созданные на основании решения органа местного самоуправления;
  3) иные информационные системы.

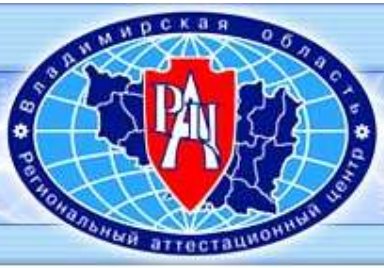
- Общие требования к ГИС (ст.14)

Законодательные акты Российской Федерации

Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» устанавливает параметры и принцип определения уровня защищенности ПДн в ИСПДн:

- Категория обрабатываемых ПДн
- Ведётся ли обработка ПДн сотрудников оператора в данной ИСПДн
- Количество субъектов ПДн, в отношении которых ведётся обработка в данной ИСПДн
- Тип актуальности угроз безопасности ПДн, связанных с недекларированными возможностями системного и прикладного программного обеспечения

Уровней защищенности ПДн в ИСПДн установлено четыре. Самый высокий и требующий усиленной защиты – первый.



Законодательные акты Российской Федерации

Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными и муниципальными органами» устанавливает перечень документов в отношении обработки ПДн, которые должны быть разработаны, утверждены и использоваться оператором, являющимся государственным или муниципальным органом

Законодательные акты Российской Федерации

Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации» устанавливает порядок работы с бумажными носителями ПДн и меры их защиты.

Законодательные акты Российской Федерации

Постановление Правительства РФ от 06.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных» устанавливает требования при работе с биометрическими персональными данными, обрабатываемыми исключительно на машиночитаемых носителях информации.

Нормативно-правовые акты

- Приказ ФСТЭК России от 18.02.2013 № 21
- Приказ ФСТЭК России от 11.02.2013 № 17
- Приказ ФСБ России от 10.07.2014 № 378
- Приказ ФСБ РФ от 09.02.2005 № 66
- Приказ ФАПСИ от 13.06.2001 №152

Нормативно-правовые акты

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных» устанавливает требования к системе защиты персональных данных, обрабатываемых в информационных системах персональных данных в соответствии с уровнем защищенности (ПП № 1119).

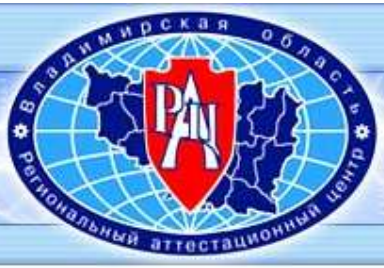
Нормативно-правовые акты

Приказ ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» устанавливает:

- Принципы классификации ИС
- Обеспечение безопасности информации в ИС, включая построение системы защиты, аттестацию и ввод ИС в действие
- требования к мерам защиты информации, содержащейся в ИС в соответствии с классом ИС.

Нормативно-правовые акты

Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности» устанавливает требования по обеспечению безопасности ПДн, при их обработке в ИСПДн, в соответствии с уровнем защищенности (ПП № 1119), при использовании СКЗИ



Нормативно-правовые акты

Приказ ФСБ России от 09.02.2005 № 66 «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации (Положение ПКЗ-2005)» устанавливает для конечного пользования СКЗИ требования по эксплуатации.

Нормативно-правовые акты

Приказ ФАПСИ от 13.06.2001 №152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну» устанавливает требования по работе с СКЗИ и формы учётных документов.

Обработка персональных данных

Персональные данные

ИСПДн

- № 152-ФЗ
- ПП 1119
- Приказ ФСТЭК № 21
- Приказ ФАПСИ № 152
- Приказ ФСБ № 378

ГИС

- № 149-ФЗ
- № 152-ФЗ
- ПП 1119
- Приказ ФСТЭК № 17
- Приказ ФАПСИ № 152
- Приказ ФСБ № 378

ПДн на бумажных носителях

- ПП 687

Виды объектов защиты персональных данных

ИСПДн — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

ГИС/МИС — федеральные, региональные/муниципальные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов РФ, правовых актов гос. органов/решений органов местного самоуправления.

Основные принципы обработки персональных данных

- Обработка ПДн должна осуществляться на законной основе
- Состав обрабатываемых ПДн должен соответствовать цели их обработки
- По достижению цели обработка должна быть прекращена, сами ПДн должны быть уничтожены/обезличены или переданы в архив (для бумажных носителей), в соответствии с законодательством, если сроки хранения не установлен федеральными законами или договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн
- При обработке ПДн оператор обеспечивает защиту ПДн

Меры защиты информации

Меры защиты информации

Организационные

- Пакет организационно-распорядительной документации (инструкции, положения, политики)
- Модель угроз и вероятного нарушителя
- Проект системы защиты ПДн

Технические

- Технический проект на построение системы защиты информации
- Средства защиты информации (средства антивирусной защиты, СЗИ от НСД, средства криптографической защиты информации…)
- Мероприятия (резервное копирование, обновление базы сигнатур….)

Организационные меры защиты персональных данных

- Назначение ответственного за организацию обработки ПДн
- Назначение системного администратора, поддерживающего работоспособность вычислительных мощностей обработки ПДн
- Составление Перечня защищаемых ПДн
- Составление Описания технологического процесса обработки ПДн
- Определение круга лиц, имеющих доступ к ПДн
- Подготовка Политики оператора в отношении обработки ПДн
- Разработка Инструкций и регламентов по обеспечению безопасности ПДн
- Выделение объектов защиты по целям обработки ПДн (ИСПДн)
- Определение уровней защищенности ПДн в ИСПДн
- Составление Технического паспорта ИСПДн
- Разработка Модели угроз безопасности ПДн в ИСПДн и вероятного нарушителя

Примерный комплект ОРД

- Модель угроз и нарушителя ИБ;
- Акт классификации информационной системы;
- Техническое задание на построение системы защиты информации;

- Приказ о проведении мероприятий по ЗИ;
- Приказ о назначении ответственного (за обработку ПДн, обеспечение ИБ);
- Приказ об утверждении документов (комплекта ОРД);
- Политика информационной безопасности организации;
- Положение об обработке персональных данных;

Примерный комплект ОРД

- План мероприятий по защите информации;
- Дополнения к должностным инструкциям…;
- Положение по защите информации;
- Перечень защищаемой информации;
- Перечень помещений;
- Методика классификации ИС;
- Перечень ИС;
- Матрица доступа;

Примерный комплект ОРД

- Инструкция пользователя;
- Инструкция по антивирусной защите;
- Инструкция по парольной защите;
- Инструкция по работе с носителями информации;
- Правила внутреннего контроля;
- Правила работы с обезличенными данными;
- Обязательство о неразглашении;
- Инструкция о порядке реагирования на инциденты ИБ;
- Правила обращений субъектов персональных данных;
- Регламент проведения резервного копирования данных.

Примерный комплект ОРД – при использовании СКЗИ

- Приказ о назначении ответственного за СКЗИ
- Модель угроз безопасности информации по НПА ФСБ России. Возможно использование отраслевой модели, адаптированной под оператора
- Инструкция о порядке работы с СКЗИ - **НЕОБХОДИМО СОГЛАСОВАНИЕ С ЛИЦЕНЗИАТОМ ФСБ РОССИИ**
- Должностная инструкция лица, ответственного за СКЗИ
- Перечень лиц, допущенных в помещения, где хранятся СКЗИ
- Журнал учета ключей от помещений, где хранятся СКЗИ

Примерный комплект ОРД – при использовании СКЗИ

- Перечень лиц, имеющих право вскрытия помещений, где хранятся и установлены СКЗИ
- Приказ о допуске к работе с СКЗИ
- Журнал поэкземплярного учета СКЗИ и эксплуатационной документации
- Лицевой счет пользователя СКЗИ.

Технические меры защиты персональных данных

- Разработка Модели угроз безопасности ПДн в ИСПДн и вероятного нарушителя
- Подготовка Проекта системы защиты ИСПДн в соответствии с выявленными каналами утечки ПДн
- Выбор одного из вариантов системы защиты ПДн в ИСПДн
- Подготовка Технического задания на создание системы защиты ПДн в ИСПДн
- Закупка средств защиты информации
- Внедрение и отладка системы защиты ПДн в ИСПДн
- Эксплуатация системы защиты ПДн в ИСПДн
- Своевременное обновление средств защиты информации
- Своевременное обновление системы защиты ПДн в ИСПДн, связи с изменениями структуры защищаемого объекта, выявление новых или утрата старых каналов утечки ПДн

Оценка соответствия требованиям безопасности персональных данных

- В соответствии с Приказом ФСТЭК № 21 для ИСПДн проводится процедура оценки соответствия требованиями по безопасности ПДн. Выдается ЗАКЛЮЧЕНИЕ сроком не превышающим 3 (три) года.
- В соответствии с Приказом № 17 для ГИС/МИС проводится процедура аттестации объекта информатизации по требованиям безопасности информации. Выдается АТТЕСТАТ соответствия сроком не превышающим 5 (пяти) лет.
- Для проведения вышеуказанных мероприятий необходимо привлечение сторонней организации, имеющей лицензию ФСТЭК России на деятельность по технической защите информации.
- Ежегодно необходимо подтверждать выполнение норм безопасности защищаемого объекта путём проведения контроля эффективности мер защиты ПДн/информации. Эту процедуру могут делать сотрудники подразделения безопасности оператора. Результат оформляется Протоколом и Заключением о соблюдении принятых мер.

Регуляторы

В области защиты ПДн и информации ограниченного доступа, не составляющей государственную тайну, контроль за соблюдением требований законодательных и нормативно-правовых актов на территории Владимирской области и г.Владимира возложен на:

- Управление Роскомнадзора по Владимирской области, в части соблюдения требований ФЗ № 152 и подзаконных актов, а так же оказания методической помощи операторам, принятия обращений субъектов.
- Управление ФСТЭК России по ЦФО, в части соблюдения требований по технической защите, аттестации/оценке эффективности, проведению ежегодного контроля эффективности принятых мер защиты объектов информатизации (ИСПДн, ГИС/МИС).
- Управление ФСБ России по Владимирской области, в части соблюдения требований нормативно-правовых актов при работе с СКЗИ.

Спасибо за внимание!

Екатерина Трохина

Старший инженер по защите информации

ООО «ИнфоЦентр»

e-mail: pd@icentr.ru

тел. 8(4922) 25-00-25