Персональные данные

Федеральный закон 152-ФЗ «О персональных данных»

- Разработан во исполнение «Конвенции о защите физических лиц при автоматизированной обработке персональных данных», ратифицированной 19 декабря 2005 г. №160-ФЗ
- Принят 27 июля 2006 г., вступил в силу 26 января 2007 г.
- Вводит правовое регулирование взаимоотношений между субъектами и операторами персональных данных
- Целью ФЗ является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну
- Операторы обязаны, за исключением некоторых случаев, направить уведомление в уполномоченный орган по защите прав субъектов персональных данных не позднее 1 января 2008 года
- Информационные системы персональных данных должны быть приведены в соответствие с требованиями 152-ФЗ не позднее 1 января 2010 года

Законодательные и нормативно-правовые акты

- Конвенция о защите физических лиц при автоматизированной обработке персональных данных (Страсбург, 28.01.1981, с изменениями от 15.06.1999)
- Федеральный закон от 19.12.2005 №160-ФЗ "О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке ПДн"
- Федеральный закон от 27.07.2006 №152-ФЗ "О персональных данных"
- Трудовой кодекс Российской Федерации №197-ФЗ (с изменениями от 01.12.2007) - глава 14 "Защита персональных данных работника»
- Указ Президента РФ от 30.05.2005 №609 "Об утверждении Положения о ПДн государственного служащего РФ и ведении его личного дела»
- Постановление Правительства РФ от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в ИСПДн»
- Приказ ФСТЭК, ФСБ и Минсвязи от 13.02.2008 №55/86/20 "Об утверждении Порядка проведения классификации информационных систем персональных данных“
- *Положение о методах и способах защиты информации в информационных системах персональных данных, утверждено Приказом ФСТЭК России от 5 февраля 2010 г. №58;*
- Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты ПДн при их обработке в ИСПДн
- Приказ Россвязькомнадзора "Об утверждении образца формы уведомления об обработке ПДн" № 8 от 17.07.2008 и №42 от 18.02.2009 «О внесении изменений в приказ №8»

Законодательные и нормативно-правовые акты

Нормативно-методические документы ФСТЭК России в области персональных данных (ДСП)

1. Положение о методах и способах защиты информации в информационных системах персональных данных, утверждено Приказом ФСТЭК России от 5 февраля 2010 г. №58

2. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

3. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных;

4. Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных;

5. Рекомендации по обеспечению безопасности персональных данных при их обработке в [illegible]х персональных данных.

Для получения указанных документов операторы, осуществляющие обработку персональных данных, могут обратиться по адресу: 105175, г. Москва, ул. Старая Басманная, 17

Законодательные и нормативно-правовые акты

Конвенция	Конвенция ЕС		160-ФЗ
Законы	ТК, гл.14	152-ФЗ	КоАП
Подзаконные акты	609-УП РСКН №8+№42	781-ПП 55/86/20	Д-ты ФСБ
ДСП		ФСТЭК	

Основные положения 152-ФЗ

Основные понятия, используемые в Федеральном законе

- **персональные данные (ПДн)** – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация;
- **информационная система персональных данных (ИСПДн)** – информационная система, представляющая собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств;
- **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 персональных данных;
- **обезличивание персональных данных** – действия, в результате которых невозможно определить принадлежность персональных данных конкретному субъекту ПДн
- **общедоступные персональные данные** - ПДн, доступ неограниченного круга лиц к которым предоставлен с согласия субъекта или на которые в соответствии с федеральными законами не распространяется требование соблюдения конфиденциальности
- **специальные категории ПДн** – сведения, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни
- **согласие субъекта** – письменное согласие субъекта о предоставлении своих ПДн оператору для обработки, с указанием:

Основные положения 152-ФЗ

Права субъекта персональных данных

Распоряжаться своими персональным данным и иметь к ним доступ

- Принимать решение о предоставлении и обработке своих ПДн
- Получать сведения об операторе и о наличии у него своих ПДн
- Требовать от оператора уточнения, блокирования или уничтожения своих ПДн

На защиту своих прав и законных интересов

- Возмещение убытков и (или) компенсацию морального вреда
- Обжаловать действия или бездействия оператора

Обработка ПДн может осуществляться только с согласия субъекта

Согласие субъекта не требуется для обработки ПДн в целях:

- государственных интересов на законных основаниях;
- исполнения договора;
- статистических или иных научных при обезличивании ПДн;
- защиты жизни и здоровья, если получение согласия субъекта ПДн невозможно;
- доставки почтовых отправлений и оказания услуг связи;
- литературной, журналистской, научной или иной творческой деятельности без нарушения прав и свобод субъектов ПДн;
- обработки ПДн, подлежащих опубликованию по закону.

Основные положения 152-ФЗ

Общедоступные источники персональных данных

- В целях информационного обеспечения могут создаваться общедоступные источники персональных данных (в том числе справочники, адресные книги)

- В общедоступные источники персональных данных с письменного согласия субъекта персональных данных могут включаться:
  - фамилия, имя, отчество
  - год и место рождения
  - адрес, абонентский номер
  - сведения о профессии
  - иные данные, предоставленные субъектом

- Сведения о субъекте персональных данных могут быть в любое время исключены из общедоступных источников персональных данных по требованию субъекта персональных данных либо по решению суда или иных уполномоченных государственных органов

Основные положения 152-ФЗ

Обязанности оператора

- Информировать субъекта о целях и способах обработки ПДн при их сборе
- Принимать меры по обеспечению безопасности ПДн при их обработке
- Операторы и третьи лица обязаны обеспечить конфиденциальность ПДн, за исключением:
  - в случае обезличивания персональных данных
  - в отношении общедоступных персональных данных
- Предоставлять сведения по запросам
- Устранять нарушения, допущенные при обработке ПДн
- Уточнять, блокировать и уничтожать ПДн по требованию
- Уведомлять об обработке персональных данных

Оператор вправе осуществлять без уведомления обработку ПДн

- относящихся к субъектам персональных данных, которых связывают с оператором трудовые отношения;
- для заключения и исполнения договора с субъектом ПДн;
- общественных объединений или религиозных организаций для достижения законных целей;
- являющихся общедоступными персональными данными;
- содержащих только фамилии, имена и отчества субъектов;
- в целях однократного пропуска субъекта на территорию или в иных аналогичных целях;
- в федеральных и государственных автоматизированных информационных системах;
- обрабатываемых без использования средств автоматизации.

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (ПП 781)

Безопасность ПДн

- достигается путем исключения несанкционированного, в том числе случайного, доступа, результатом которого может стать уничтожение, изменение, блокирование, копирование, распространение персональных данных, а также иных несанкционированных действий.
- обеспечивается с помощью системы защиты персональных данных (СЗПДн), включающей организационные меры и средства защиты информации.

При обработке ПДн должно быть обеспечено:

- проведение мероприятий, направленных на предотвращение НСД и/или несанкционированной передачи ПДн третьим лицам;
- своевременное обнаружение фактов НСД к персональным данным;
- недопущение воздействия на технические средства автоматизированной обработки персональных данных, в результате которого может быть нарушено их функционирование;
- возможность незамедлительного восстановления персональных данных, модифицированных или уничтоженных вследствие несанкционированного доступа к ним;
- постоянный контроль за обеспечением уровня защищенности персональных данных.

Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных (ПП 781)

Мероприятия по обеспечению безопасности ПДн:

- классификация, формирование модели угроз и требований по защите;
- разработка СЗПДн с учетом угроз, методов и способов защиты предусмотренных для соответствующего класса систем;
- проверка готовности средств защиты информации (СЗИ) с составлением заключений о возможности их эксплуатации;
- установка и ввод в эксплуатацию средств защиты информации;
- обучение лиц правилам работы со средствами защиты информации;
- учет средств защиты информации, документации к ним, носителей данных;
- учет лиц, допущенных к работе с персональными данными, и их запросов;
- контроль за соблюдением условий использования СЗИ;
- разбирательство и составление заключений по фактам нарушения установленных правил и требований, разработку и принятие мер по предотвращению подобных инцидентов и снижению возможных опасных последствий;
- описание системы защиты персональных данных.

Классификация

Порядок проведения классификации ИСПДн (55/86/20)

При классификации учитываются следующие исходные данные:

- категория обрабатываемых в информационной системе данных (Хпд)
  - 4 категории: от общедоступных до специальных
- объем обрабатываемых персональных данных (Хнпд)
  - 3 категории по количеству/масштабу
- заданные оператором характеристики безопасности ПДн
  - типовые (только конфиденциальность) или специальные
- структура информационной системы
  - АРМ, локальная или распределенная ИС
- наличие подключений к сетям связи общего пользования
  - есть/нет
- режим обработки персональных данных
  - много/одно/пользовательский
- режим разграничения прав доступа пользователей
  - с разграничением или без
- местонахождение технических средств
  - на территории РФ, частично или полностью за рубежом

Результаты классификации оформляются соответствующим актом оператора с указанием перечисленных сведений

Классификация

Категории персональных данных (Хпд):

- **категория 1** - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, интимной жизни, [состояния здоровья специальная ИСПДн]
- **категория 2** - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1
- **категория 3** - персональные данные, позволяющие идентифицировать субъекта персональных данных
- **категория 4** - обезличенные и (или) общедоступные персональные данные

Категории субъектов (Хнпд):

- **1** - в информационной системе одновременно обрабатываются персональные данные более чем 100 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом;
- **2** - в информационной системе одновременно обрабатываются персональные данные от 1 000 до 100 000 субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования;
- **3** - в информационной системе одновременно обрабатываются данные менее чем 1 000 субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации

Классификация

Типовой информационной системе присваивается один из следующих классов:

- **класс 1 (К1)** - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к значительным негативным последствиям для субъектов персональных данных;
- **класс 2 (К2)** - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к негативным последствиям для субъектов персональных данных;
- **класс 3 (К3)** - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к незначительным негативным последствиям для субъектов персональных данных;
- **класс 4 (К4)** - информационные системы, для которых нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, не приводит к негативным последствиям для субъектов персональных данных.

Класс может быть пересмотрен:

- по решению оператора на основе проведенных им анализа и оценки угроз безопасности персональных данных с учетом особенностей и (или)изменений конкретной информационной системы;
- по результатам мероприятий по контролю за выполнением требований к обеспечению безопасности персональных данных при их обработке в информационной системе.

Хнпд →	3	2	1
Категория 4	К4	К4	К4
Категория 3	К3	К3	К2
Категория 2	К3	К2	К1
Категория 1	К1	К1	К1

Разработка моделей угроз ПДн

1. **Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных**

- Содержит полный классификатор угроз НСД и утечки по техническим каналам
- Представляет 6 типовых моделей угроз для всех структур ИСПДн (АРМ, локальная, распределенная) с подключением и без подключения к Сетям Связи Общего Пользования

2. **Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных**

- Вводит термин «исходной степени защищенности» ИСПДн (3 степени: низкая, средняя, высокая)
- Позволяет актуализировать базовую модель угроз для конкретной ИСПДн (актуальная/неактуальная)
- Организационно-технические требования по защите ИСПДн формируются по методическим материалам ФСТЭК в соответствии с составленным перечнем актуальных угроз

Определение требований по защите ПДн

1. **Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных**

- Определяет комплекс мероприятий по защите от НСД и утечек по техническим каналам на всех стадиях ЖЦ ИСПДн
- Мероприятия по защите ПДн от НСД (в зависимости от классов) реализуются в рамках подсистем:
  - управления доступом
  - регистрации и учета
  - обеспечения целостности
  - криптографической защиты
  - антивирусной защиты
  - обнаружения вторжений

2. **Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**

- Содержит общий порядок организации обеспечения безопасности персональных данных в информационных системах персональных данных
- Рекомендации по обеспечению безопасности персональных данных в информационных системах персональных данных по всему спектру угроз

Различия требований по классам

- Мероприятия по защите ПДн от утечек по техническим каналам в ИСПДн К4 и К3 не производятся
- Требования по защите ИСПДн К4 определяются оператором **самостоятельно**
- Требования по защите от НСД нарастают в зависимости от
  - класса системы (К3-К1)
  - режима обработки данных (одно/много/пользовательский)
  - наличия разграничения доступа
  - наличия подключения к ССОП
- В некоторых случаях требуется получение лицензии на осуществление деятельности по технической защите конфиденциальной информации
- В отношении ИСПДн К1 проводится аттестация АС на соответствие требованиям (типовым или специальным)

Описание СЗПДн

Должны быть разработаны документы:

- Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн
- Модель угроз нарушения безопасности ПДн при обработке в ИСПДн
- Требования по обеспечению безопасности ПДн при обработке в ИСПДн
- Должностные инструкции персоналу ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн
- Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации

Типичная ситуация

- Сбор, уточнение и согласование исходных данных
- Классификация ИСПДн
- Согласование предварительных результатов классификации
- (принятие быстрых корректирующих мер, при необходимости)
- Подготовка Актов классификации
- Совместный анализ и систематизация результатов классификации, принятие решений о применимости и возможности реализации типовых решений в условиях сложившейся у Заказчика практики и культуры
- Группировка ИСПДн по ключевым признакам на различные типы по ключевым аспектам документов ФСТЭК
- Разработка моделей угроз и требований по типам ИСПДн
- Оценка соответствия систем типовым требованиям
- Выработка возможных решений (в т.ч. «быстрых»)
- Совместный анализ оценки соответствия, согласование требований к К4, выбор подходящих «быстрых» мер
- Анализ существующих организационно-распорядительных документов Заказчика в области ИБ и ИТ (эксплуатации систем)
- Разработка Рекомендаций и Плана работ

Типовые ошибки классификации

- Некорректное обращение со специальными категориями ПДн (национальность, состояние здоровья) приводит к классификации специальных систем на К3-К1 либо наоборот – системы К3-К2 относятся к специальным
  - Наличие среди прочих данных сведений о национальности очень часто не учитывают при классификации
  - Сведения о прохождении медосмотра (лишь дата и заключение) относят к категории «сведения о состоянии здоровья», а явно указанный диагноз в больничном листе не относят
- Недобросовестность при сборе исходных данных не всегда и не легко выявляется
  - В старых кадровых и бухгалтерских ИС не замечают, что среди паспортных или других данных присутствует национальность или диагноз в больничном
- Неоднозначность нормативных требований приводит к некорректному категорированию и завышенной классификации
  - При категорировании ПДн общедоступные данные относят к категории 3 или даже 2
  - При категорировании объема ПДн пользуются только численными данными, не обращая внимания на текстовые условия
  - Так, в одной организации корпоративный справочник, содержащий ФИО, подразделение, должность, офис, кабинет, телефон, e-mail о почти 2 000 сотрудниках был классифицирован как К2

Чем мы можем помочь

- Грамотно провести классификацию
- Обсчитать специальные ИСПДн
- Подготовить Акты (под подпись)
- Оформить Уведомление
- Разработать модели угроз
- Определить требования к ИСПДн
- Определить решения «из подручных средств» и минимизировать необходимую закупку

- Внедрить необходимые технические и организационные решения
- Подготовить нужные документы (формальные)
- Сопровождать проверку (отстоять классификацию)
- Разработать и внедрить действующую СЗПДн
- Получить лицензию, аттестовать систему