ОРГАНИЗАЦИЯ РАБОТЫ С ПЕРСОНАЛЬНЫМИ ДАННЫМИ

Особенности защиты персональных данных: основы, нормативно-правовая база, примеры

Заведующий кафедрой социально-гуманитарных дисциплин
доктор педагогических наук, профессор
Долматов Александр Васильевич

В лекции использованы материалы
Бориса Сухинина (ЗАО «НПО «Эшелон» РусКрипто)

Нормативная база
Федеральное законодательство

- Конституция Российской Федерации
- Конвенция Совета Европы о защите физических лиц при автоматизированной обработке персональных данных
- Федеральный закон «Об информации, информационных технологиях и о защите информации»
- Федеральный закон «О персональных данных»

Нормативная база
Постановления Правительства РФ

- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных
- Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации

Нормативная база
Приказ ФСТЭК, ФСБ и Мининформсвязи

- Порядок проведения классификации информационных систем персональных данных

Нормативная база
Документы ФСТЭК России

- **Основные мероприятия** по организации и техническому обеспечению безопасности ПДн, обрабатываемых в ИСПДн
- **Рекомендации** по обеспечению безопасности ПДн при их обработке в ИСПДн
- **Базовая модель угроз** безопасности ПДн при их обработке в ИСПДн
- **Методика определения актуальных угроз** безопасности ПДн при их обработке в ИСПДн

Нормативная база
Документы ФСБ России

- **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 ПДн при их обработке в ИСПДн
- **Методические рекомендации** по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации

Основные понятия

Персональные данные

- **Персональные данные** (ПДн) – любая информация, относящаяся к ***определенному*** или ***определяемому*** на основании такой информации физическому лицу, в том числе:
  - фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация
- Относятся ли к персональным данным:
  - фамилия, имя, отчество
  - только имя и отчество
  - ИНН
  - номер автомобиля

Основные понятия

Конфиденциальность персональных данных

- **Конфиденциальность персональных данных** – ***обязательное*** для соблюдения оператором или иным получившим доступ к ПДн лицом требование ***не допускать их распространения без согласия субъекта*** персональных данных или наличия иного законного основания

Основные понятия
Обработка персональных данных

- **Обработка персональных данных** – действия с ПДн, включая:
  - сбор, систематизацию, накопление, хранение, уточнение (обновление, изменение), использование, распространение (в т.ч. передачу), обезличивание, блокирование, уничтожение персональных данных

Основные понятия
Обезличенные персональные данные

- **Обезличенные персональные данные** – ПДн, для которых невозможно установить принадлежность ***конкретному*** лицу
- По определению ***не относятся*** к ПДн
- Установление принадлежности ПДн – ***субъективная*** возможность
- Относятся ли к обезличенным ПДн только ФИО?

Основные понятия

Субъект и оператор персональных данных

- **Субъект** – физическое лицо, к которому относятся персональные данные
- **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, ***организующие*** и (или) ***осуществляющие*** обработку ПДн, а также ***определяющие*** цели и содержание обработки персональных данных

Основные понятия

Субъект и оператор персональных данных

- **Субъект** – физическое лицо, к которому относятся персональные данные
- **Оператор** – государственный орган, муниципальный орган, юридическое или физическое лицо, ***организующие*** и (или) ***осуществляющие*** обработку ПДн, а также ***определяющие*** цели и содержание обработки персональных данных

Основные понятия

Трансграничная передача персональных данных

- **Трансграничная передача** персональных данных - передача персональных данных на территорию иностранного государства органу власти иностранного государства, иностранному физическому лицу или иностранному юридическому лицу.

Специальные категории персональных данных

Условия обработки

- Обработка специальных категорий персональных данных, касающихся расовой, национальной принадлежности, политических взглядов, религиозных или философских убеждений, состояния здоровья, интимной жизни, не допускается, за исключением случаев, предусмотренных частью 2 статьи 10 ФЗ 152.
- Разрешается с согласия субъекта, а также в целях медицинской деятельности, осуществления правосудия, ОРД и ряде других случаев.

Биометрические персональные данные

определение

- **Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.**

Биометрические персональные данные

определение

- **Сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность (биометрические персональные данные) и которые используются оператором для установления личности субъекта персональных данных, могут обрабатываться только при наличии согласия в письменной форме субъекта персональных данных, за исключением случаев, предусмотренных частью 2 настоящей статьи.**

Действия оператора
Юридический аспект

- Уведомление Роскомнадзора о намерении осуществлять обработку ПДн
- Приведение внутренней нормативной базы в соответствие с требованиями закона
- Получение лицензий ФСТЭК России и ФСБ России

Действия оператора
Юридический аспект

- Уведомление Роскомнадзора о намерении осуществлять обработку ПДн
- Приведение внутренней нормативной базы в соответствие с требованиями закона
- Получение лицензий ФСТЭК России и ФСБ России

Действия оператора
Юридический аспект

- **Оператор обязан принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами. Оператор самостоятельно определяет состав и перечень мер, необходимых и достаточных для обеспечения выполнения обязанностей, предусмотренных настоящим Федеральным законом и принятыми в соответствии с ним нормативными правовыми актами**

Действия оператора

Организационно-управленческий аспект

- **назначение оператором, являющимся юридическим лицом, ответственного за организацию обработки персональных данных;**

- **издание оператором, являющимся юридическим лицом, документов, определяющих политику оператора в отношении обработки персональных данных, локальных актов по вопросам обработки персональных данных, а также локальных актов, устанавливающих процедуры, направленные на предотвращение и выявление нарушений законодательства Российской Федерации, устранение последствий таких нарушений;**

- **применение правовых, организационных и технических мер по обеспечению безопасности персональных данных в соответствии со статьей 19 настоящего Федерального закона;**

Действия оператора

Организационно-управленческий аспект

- осуществление внутреннего контроля и (или) аудита соответствия обработки персональных данных настоящему ФЗ и принятым в соответствии с ним нормативным правовым актам, требованиям к защите ПД, политике оператора в отношении обработки персональных данных, локальным актам оператора;
- оценка вреда, который может быть причинен субъектам персональных данных в случае нарушения настоящего ФЗ, соотношение указанного вреда и принимаемых оператором мер, направленных на обеспечение выполнения обязанностей, предусмотренных настоящим ФЗ;
- ознакомление работников оператора, непосредственно осуществляющих обработку персональных данных, с положениями законодательства РФ о ПД, в том числе требованиями к защите ПД, документами, определяющими политику оператора в отношении обработки персональных данных, локальными актами по вопросам обработки персональных данных, и (или) обучение указанных работников.

Действия оператора
Технический аспект

- Идентификация и классификация ИСПДн
- Построение частной модели угроз и определение мер по защите
- Разработка и реализация системы технической защиты ПДн
- Аттестация ИСПДн по требованиям безопасности информации

Уведомление

Нужно ли уведомлять

- Оператор вправе осуществлять обработку ПДн ***без уведомления***, если:
  - Субъекта связывают с оператором трудовые отношения
  - данные используются для выполнения договора с Субъектом
  - данные являются общедоступными
  - данные включают только ФИО
  - и в ряде других случаев
- Организации обрабатывают данные из резюме соискателей работы ***без заключения договора***

Классификация ИСПДн
Подходы к классификации

- Исходя из ***категории*** и ***количества*** ПДн
  - осуществляется для типовых систем
  - типовых систем практически не существует
- На основе ***частной модели угроз***
  - осуществляется для специальных систем
  - документы не определяют порядок классификации на основе частной модели угроз
- Исходя из ***ущерба*** для Субъекта
  - ущерб является субъективным понятием
- Классификация специальной системы осуществляется исходя ***из категории и количества*** ПДн, а защитные меры выбираются по ***частной модели угроз***
- Приказ ФСТЭК, ФСБ, Мининформсвязи 13.02.08 г. N 55/86/20

Классификация типовых систем

Исходные данные

- ***Категория*** обрабатываемых данных – $X_{пд}$
- ***Объем*** одновременно обрабатываемых данных – $X_{нпд}$
- А также:
  - характеристики безопасности
  - структура информационной системы
  - наличие подключений к ССОП
  - режим обработки ПДн
  - режим разграничения прав доступа
  - местонахождение технических средств

Классификация типовых систем

Категория обрабатываемых данных

- Определено 4 категории
  - **Категория 4** – ***обезличенные*** данные
  - **Категория 3** – данные, позволяющие ***идентифицировать*** Субъекта
  - **Категория 2** – данные, позволяющие ***идентифицировать*** Субъекта и получить о нем ***дополнительную информацию***
  - **Категория 1** – данные о состоянии ***здоровья***, расовой и национальной принадлежности, политических, религиозных и философских взглядах, интимной жизни
- Какие данные необходимы для идентификации субъекта? Является ли инвалидность сведениями о состоянии здоровья? Что такое интимная жизнь?

Классификация типовых систем
Объем обрабатываемых данных

- Определены 3 значения объема:
  - **3** – данные ***менее чем 1 000*** Субъектов или данные Субъектов в пределах конкретной организации
  - **2** – данные ***от 1 000 до 100 000*** Субъектов или данные Субъектов в пределах отрасли экономики, органа гос. власти, проживающих в пределах муниципального образования
  - **1** – данные ***более чем 100 000*** Субъектов или данные Субъектов в пределах субъекта РФ или РФ в целом
- Двойная классификация объема по количественному и территориальному признакам – ***какой критерий является основным***?

Классификация типовых систем

Выбор класса

$X_{ПД}$ \ $X_{НПД}$	3	2	1
Категория 4	4 класс	4 класс	4 класс
Категория 3	3 класс	3 класс	2 класс
Категория 2	3 класс	2 класс	***1 класс***
Категория 1	***1 класс***	***1 класс***	***1 класс***

- От выбора класса зависит состав и объем защитных мер
- Понижение класса системы
  - снижение категории (***обезличивание*** данных)
  - снижение объема (***дробление*** системы)

Общая классификация

Категории ПДн		Специальные			Биомет-рические	Иные			Общедоступные		
Собственные работники		нет	нет	да		нет	нет	да	нет	нет	да
Количество субъектов		более 100 тыс.	менее 100 тыс.			более 100 тыс.	менее 100 тыс.		более 100 тыс.	менее 100 тыс.	
Тип актуальных угроз	1	1 УЗ	1 УЗ	1 УЗ	1 УЗ	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ
	2	1 УЗ	2 УЗ	2 УЗ	2 УЗ	2 УЗ	3 УЗ	3 УЗ	2 УЗ	3 УЗ	3 УЗ
	3	2 УЗ	3 УЗ	3 УЗ	3 УЗ	3 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ	4 УЗ

Требования к системе защиты
Для 4 класса

- Перечень мероприятий ***определяется оператором*** в зависимости от возможного ущерба
- Оценка соответствия проводится ***по решению оператора***

Требования к системе защиты
Для 3 класса

- ***Декларирование*** соответствия или обязательная ***аттестация*** по требованиям безопасности информации (по решению оператора)
- Получение ***лицензии*** ФСТЭК России на ТЗКИ для распределенных систем

Класс АС	Класс СВТ	Класс МЭ (без подключения к ССОП)	Класс МЭ (с подключением к ССОП)	Уровень контроля отсутствия НДВ
3Б	5	--	4	4
2Б	5	4	2	4
1Д	5	4	2	4

Требования к системе защиты

Для 2 класса

- Обязательная ***аттестация*** по требованиям безопасности информации
- Требования по электромагнитной совместимости оборудования
- Получение ***лицензии*** ФСТЭК России на ТЗКИ

Класс АС	Класс СВТ	Класс МЭ (без подключения к ССОП)	Класс МЭ (с подключением к ССОП)	Уровень контроля отсутствия НДВ
3Б+	5	--	3	4
2Б+	5	4	2	4
1Г	5	4	2	4

Требования к системе защиты
Для 1 класса

- Обязательная ***аттестация*** по требованиям безопасности информации
- Требования соответствуют уровню защиты ***государственной тайны*** (в т.ч. по ПЭМИН)
- Получение ***лицензии*** ФСТЭК России на ТЗКИ

Класс АС	Класс СВТ	Класс МЭ (без подключения к ССОП)	Класс МЭ (с подключением к ССОП)	Уровень контроля отсутствия НДВ
3А	4	--	2	4
2А	4	4	2	4
1В	4	4	2	4

Классификация угроз

Постановление Правительства РФ от 1.11. 2012 г. № 1119

- **Угрозы 1-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном программном обеспечении, используемом в информационной системе.**
- **Угрозы 2-го типа актуальны для информационной системы, если для нее в том числе актуальны угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном программном обеспечении, используемом в информационной системе.**
- **Угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе.**

Требования к защищенности ПД

Постановление Правительства РФ от 1.11. 2012 г. № 1119

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

- **а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;**
- **б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.**

Требования к защищенности ПД

4 уровень защищенности

- **Для обеспечения 4-го уровня защищенности персональных данных при их обработке в информационных системах необходимо выполнение следующих требований:**
- **а) организация режима обеспечения безопасности помещений, в которых размещена информационная система, препятствующего возможности неконтролируемого проникновения или пребывания в этих помещениях лиц, не имеющих права доступа в эти помещения;**
- **б) обеспечение сохранности носителей персональных данных;**

Требования к защищенности ПД
4 уровень защищенности (продолжение)

- **в) утверждение руководителем оператора документа, определяющего перечень лиц, доступ которых к персональным данным, обрабатываемым в информационной системе, необходим для выполнения ими служебных (трудовых) обязанностей;**

- **г) использование средств защиты информации, прошедших процедуру оценки соответствия требованиям законодательства Российской Федерации в области обеспечения безопасности информации, в случае, когда применение таких средств необходимо для нейтрализации актуальных угроз.**

Требования к защищенности ПД

3 уровень защищенности

- Для обеспечения 3-го уровня защищенности персональных данных при их обработке в информационных системах помимо выполнения требований, предусмотренных пунктом 13 настоящего документа, необходимо, чтобы было назначено должностное лицо (работник), ответственный за обеспечение безопасности персональных данных в информационной системе.
- **Требования к защите персональных данных при их обработке в информационных системах персональных данных**
- **(утв. постановлением Правительства РФ от 1 ноября 2012 г. № 1119)**

НПБ ФСТЭК
Меры по защите ПДн

- Приказ ФСТЭК России от 18 февраля 2013 г. N 21
- **Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных**
- **в) для обеспечения 4 уровня защищенности персональных данных применяются:**
- средства вычислительной техники не ниже 6 класса;
- системы обнаружения вторжений и средства антивирусной защиты не ниже 5 класса;
- межсетевые экраны 5 класса.

Основные мероприятия по защите

- Система защиты должна включать в себя следующие подсистемы:
  - управления и контроля доступа
  - регистрации и учета
  - обеспечения целостности
  - антивирусной защиты
  - межсетевого экранирования
  - обнаружения вторжений
  - криптографической защиты

Согласие в письменной форме субъекта на обработку его персональных данных

Должно включать:

- фамилию, имя, отчество, адрес субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе;
- фамилию, имя, отчество, адрес представителя субъекта персональных данных, номер основного документа, удостоверяющего его личность, сведения о дате выдачи указанного документа и выдавшем его органе, реквизиты доверенности или иного документа, подтверждающего полномочия этого представителя (при получении согласия от представителя субъекта персональных данных);
- наименование или фамилию, имя, отчество и адрес оператора, получающего согласие субъекта персональных данных;
- цель обработки персональных данных;
- перечень персональных данных, на обработку которых дается согласие субъекта персональных данных;

Согласие в письменной форме субъекта на обработку его персональных данных

должно включать:

- наименование или фамилию, имя, отчество и адрес лица, осуществляющего обработку персональных данных по поручению оператора, если обработка будет поручена такому лицу;
- перечень действий с персональными данными, на совершение которых дается согласие, общее описание используемых оператором способов обработки персональных данных;
- срок, в течение которого действует согласие субъекта персональных данных, а также способ его отзыва, если иное не установлено федеральным законом;
- подпись субъекта персональных данных.

Минимальный пакет документов по обработке ПД в организации

– общий документ, определяющий политику оператора в отношении обработки персональных данных;
– локальный акт или несколько актов, которые могут включать в себя описание всех процессов обработки ПД, включая перечень лиц, имеющих доступ к ПД, порядок обеспечения доступа и работы с персональными данными, процесс уничтожения ПД.
– указанные акты также должны содержать конкретное описание правовых, организационных и технических мер защиты ПД от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении ПД;
– локальные акты, устанавливающие процедуры, направленные на предотвращение и выявление нарушений законодательства РФ, устранение последствий таких нарушений.

Требования к сайту образовательной организации

Приказ № 785 Федеральной службы по надзору в сфере образования и науки «Об утверждении требований к структуре официального сайта образовательной организации в информационно-телекоммуникационной сети «Интернет» и формату представления на нем информации» (от 29.05.2014 года).

- **информация должна иметь общий механизм навигации по всем страницам специального раздела;**
- **механизм навигации должен быть представлен на каждой странице специального раздела;**
- **доступ к разделу «*Сведения об образовательной организации*» должен осуществляться с главной (основной) страницы сайта, а также из основного навигационного меню сайта;**
- **страницы специального раздела должны быть доступны в Интернете без дополнительной регистрации.**

Специальный раздел сайта – должен содержать следующие подразделы:

- *«Основные сведения»;*
- *«Структура»;*
- *«Документы»;*
- *«Образование»;*
- *«Образовательные стандарты»;*
- *«Руководство. Педагогический (научно-педагогический) состав»;*
- *«Материально-техническое обеспечение и оснащенность образовательного процесса»;*
- *«Стипендии и иные виды материальной поддержки»;*
- *«Платные образовательные услуги»;*
- *«Финансово-хозяйственная деятельность»;*
- *«Вакантные места для приема (перевода)».*

Спасибо за внимание!