Обеспечение безопасности персональных данных

НОРМАТИВНАЯ БАЗА И ПРАКТИКА

Серженко Дмитрий Иванович
заведующий центром информатизации
ИМЦ Петродворцового района

Основные понятия (по 152-ФЗ, ст. 3)

- **Персональные данные (ПДн)** — любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных)
- **Информационная система персональных данных (ИСПДн)** — совокупность содержащихся в базах данных персональных данных и обеспечивающих их обработку информационных технологий и технических средств

Основные понятия (по 152-ФЗ, ст. 3)

- **Оператор** — государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн;
- **Обработка ПДн** — любое действие (операция) или совокупность действий (операций), совершаемых с использованием средств автоматизации или без использования таких средств с ПДн, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение ПДн

Нормативная база (ФЗ)

- Федеральный закон «О персональных данных» № 152-ФЗ от 27.07.2006 (действующая редакция — от 23.07.2013)

Нормативная база (Постановления Правительства)

- Постановления Правительства:
  - № 211 от 21.03.2012 «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 или муниципальными органами»

Нормативная база (Постановления Правительства)

- Постановления Правительства:
  - № 940 от 18.09.2012 «Об утверждении Правил согласования проектов решений ассоциаций, союзов и иных объединений операторов об определении дополнительных угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении определенных видов деятельности членами таких ассоциаций, союзов и иных объединений операторов, с Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю»

Нормативная база (Постановления Правительства)

- Постановления Правительства:
  - № 1119 от 01.11.2012 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»
  - № 512 от 06.07.2008 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»
  - № 687 от 15.09.2008 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Нормативная база (приказы и иные документы)

- **Роскомнадзор**
  - Приказ № 274 от 15.03.2013 «Об утверждении перечня иностранных государств, не являющихся сторонами конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных и обеспечивающих адекватную защиту прав субъектов персональных данных»
  - Приказ № 996 от 05.09.2013 «Об утверждении требований и методов по обезличиванию персональных данных»
  - Методические рекомендации от 13.12.2013 (по применению приказа № 996)
- **ФСТЭК**
  - Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн *(15.02.2008)*
  - Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн *(14.02.2008)*
  - Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн *(Приказ ФСТЭК России № 21 от 18.02.2013)*

Нормативная база (приказы и иные документы)

- **ФСБ**
  - Методические рекомендации по обеспечению с помощью криптографических средств безопасности персональных данных при их обработке в ИСПДн с использованием средств автоматизации *(Приказ ФСБ России № 149/54-144 от 21.02.2008)*
  - 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 персональных данных при их обработке в ИСПДн *(Приказ ФСБ России № 149/6/6-622 от 21.02.2008)*
- **ФСТЭК, ФСБ и Мининформсвязи России**
  - Порядок проведения классификации информационных систем персональных данных *(Приказ № 55/86/20 от 13.02.2008)*

Регулирование и контроль

- Административный регламент Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции **«Ведение реестра операторов, осуществляющих обработку персональных данных»**
- Административный регламент **проведения проверок** Федеральной службой по надзору в сфере связи, информационных технологий и массовых коммуникаций при осуществлении федерального государственного **контроля (надзора) за соответствием обработки персональных данных требованиям законодательства** Российской Федерации в области персональных данных
- Типовой регламент проведения [ФСБ России] в пределах полномочий мероприятий по **контролю (надзору) за выполнением требований, установленных Правительством Российской Федерации, к обеспечению безопасности персональных данных** при их обработке в информационных системах персональных данных

Что каждое учреждение обязано делать (в двух словах)

- Выдержки из ст. 18.1 152-ФЗ.
  Меры, направленные на обеспечение выполнения оператором обязанностей, предусмотренных настоящим Федеральным законом
  - **Оператор обязан** принимать меры, необходимые и достаточные для обеспечения выполнения обязанностей, предусмотренных настоящим ФЗ 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 ФЗ и принятыми в соответствии с ним нормативными правовыми актами, если иное не предусмотрено настоящим ФЗ или другими ФЗ

Необходимые акты и документы (152-ФЗ; Постановление 211)

1. Приказ о назначении ответственного за *организацию* обработки ПДн
2. Правила обработки ПДн
3. Правила рассмотрения запросов субъектов ПДн или их представителей
4. Правила осуществления внутреннего контроля соответствия обработки ПДн требованиям к защите ПДн, установленным ФЗ, подзаконными актами и локальными актами оператора
5. Правила работы с обезличенными данными
6. Перечень ИСПДн
7. Перечень персональных данных, обрабатываемых в учреждении

Необходимые акты и документы (152-ФЗ; Постановление 211)

8. Перечень должностей сотрудников, ответственных за проведение мероприятий по обезличиванию обрабатываемых ПДн
9. Перечень должностей сотрудников, работа на которых предусматривает осуществление обработки ПДн либо осуществление доступа к ПДн
10. Должностная инструкция ответственного за организацию обработки персональных данных
    - Раздел должностных инструкций (должностного регламента) сотрудников, имеющих доступ к ИСПДн, в части обеспечения безопасности ПДн

Необходимые акты и документы (152-ФЗ; Постановление 211)

11. Типовое обязательство работника, непосредственно осуществляющего обработку ПДн, в случае расторжения с ним трудового договора прекратить обработку ПДн, ставших известными ему в связи с исполнением должностных обязанностей
12. Типовая форма согласия на обработку ПДн сотрудников и иных субъектов ПДн
13. Типовая форма разъяснения субъекту ПДн юридических последствий отказа предоставить свои ПДн
14. Порядок доступа работников в помещения, в которых ведется обработка персональных данных

Необходимые акты и документы (152-ФЗ; Постановление 211)

15. Положение об особенностях обработки ПДн, осуществляемой без использования средств автоматизации
16. Типовой план периодических проверок условий обработки ПДн в организации в целях осуществления внутреннего контроля соответствия обработки ПДн установленным требованиям
17. Ведомость ознакомления работников учреждения, непосредственно осуществляющих обработку ПДн, с положениями законодательства РФ о ПДн (в том числе с требованиями к защите ПДн), локальными актами по вопросам обработки ПДн

- … и другие локальные акты, подробнее — см. в нормативной базе и методичке

Чем грозит несоблюдение закона?

- Статья 13.11 КоАП Нарушение порядка сбора, хранения, использования или распространения информации о гражданах (ПДн)
- Статья 13.14 КоАП Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей.
- Статья 19.7 КоАП Непредставление или несвоевременное представление в государственный орган сведений, представление которых предусмотрено законом и необходимо для осуществления этим органом его законной деятельности, а равно представление их в неполном объеме или в искаженном виде
- Ст. 137 УК Нарушение неприкосновенности частной жизни Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия <…>
- Ст. 272 УК Неправомерный доступ к компьютерной информации Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации <…>

Для самостоятельной проработки

На сайте ЦИО (http://ci.obrpeterhof.ru/):

- Материалы вебинара «Обеспечение безопасности ПДн при их обработке в информационных системах персональных данных в образовательных организациях»
- Сборник типовых (примерных) форм организационно-распорядительных документов от КИС
- Эта презентация

Спасибо за внимание!