Приведение информационных систем организаций в соответствие с ФЗ № 152 «О персональных данных»

Сергей Любарский

sergey@lubarsky.ru

www.lubarsky.ru

Вопросы для обсуждения:

- Как провести инвентаризацию информационных систем персональных данных.
- Как определить категорию персональных данных и класс информационной системы персональных данных (ИСПДн).
- Определение актуальных угроз и разработка модели угроз безопасности персональным данным.
- Как подготовить уведомление в уполномоченный орган по защите прав субъектов персональных данных.
- Перечень организационно-распорядительной документации предприятия по защите персональных данных.
- Как оптимизировать технические решения и снизить затраты на создание СЗПДн.
- Как подготовить декларацию соответствия требованиям безопасности информации.
- Как организовать эксплуатацию ИСПДн в соответствии с требованиями по безопасности и контроль эффективности защиты персональных данных.

Правовое поле

Правовое поле

1981 **Конвенция о защите физических лиц при автоматизированной обработке персональных данных**
Совет Европы, 28 января 1981 г., Страсбург, Франция

1996 **28 февраля 1996 г. – вступление России в Совет Европы**
Российская Федерация становится 39 членом СЕ и берет на себя ряд обязательств в области защиты прав человека

2001 **О подписании Конвенции о защите физических лиц при автоматизированной обработке персональных данных**
Распоряжение Президента Российской Федерации от 10.07.2001 г. № 366-рп

2005 **О ратификации Конвенции Совета Европы о защите физических лиц при автоматизированной обработке персональных данных**
Федеральный закон от 19.12.2005 г. № 160-ФЗ

2006 **О персональных данных**
Федеральный закон от 27.06.2006 г. № 152-ФЗ

Федеральные органы исполнительной власти, регулирующие вопросы использования и защиты персональных данных

- **Федеральная служба безопасности Российской Федерации**
- **Федеральная служба по техническому и экспортному контролю**
- **Федеральная служба по надзору в сфере связи, информационных технологий и массовых коммуникаций**
- **Министерство связи и массовых коммуникаций Российской Федерации**

Какие действия необходимо совершить оператору - кооперативу

Какие действия необходимо совершить оператору для приведения информационной системы персональных данных в соответствие с требованиями законодательства?

- провести их классификацию с оформлением соответствующего акта;
- Информационные системы классифицируются операторами в зависимости от объема обрабатываемых ими персональных данных и угроз безопасности жизненно важным интересам личности, общества и государства (п.6 Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, утв. Постановлением Правительства РФ от 17.11.2007 № 781) (далее – Положение от 17.11.2007 № 781).
- Порядок проведения классификации информационных систем установлен Приказом ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008. Согласно п.4 Порядка.., утв. Приказом ФСТЭК РФ № 55, ФСБ РФ № 86, Мининформсвязи РФ № 20 от 13.02.2008, проведение классификации информационных систем включает в себя следующие этапы:
- сбор и анализ исходных данных по информационной системе;
- присвоение информационной системе соответствующего класса и его документальное оформление.

Классификационные признаки типовых ИСПДн

Количество субъектов ПДн в системе ($X_{нпд}$) / Количество обрабатываемых ПДн ($X_{пд}$)	$X_{нпд} = 1$			$X_{нпд} = 2$				$X_{нпд} = 3$	
	Более 100 000 ПДн	В объеме РФ	В объеме субъекта РФ	От 100 000 до 1 000 000 ПДн	В объеме отрасли	В объеме органа власти	В объеме муниципа-льного образова-ния	До 1000 ПДн	В объеме одной организа-ции
$X_{пд} = 1$ (Расовая, национальная принадлежность, политические взгляды, религиозные и философские убеждения, состояние здоровья, интимная жизнь)	К1								
$X_{пд} = 2$ (Данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию)				К2					
$X_{пд} = 3$ (Данные, позволяющие идентифицировать субъекта персональных данных)	К2			К3					
$X_{пд} = 4$ (Обезличенные и (или) общедоступные персональные данные)	К4								

Особенности обеспечения безопасности персональных данных в случае, если их обработка осуществляется в информационных системах персональных данных

- В письме Рособразования от 29.07.2009 № 17-110 уточнено, что обеспечение безопасности персональных данных должно осуществляться в соответствии с методическими документами ФСТЭК России:
- "Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных" от 15 февраля 2008 года;
- "Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года;
- "Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных" от 15 февраля 2008 года;
- "Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных" от 15.02.2008

С ними можно ознакомиться на официальном сайте Службы по адресу - http://www.fstec.ru/_razd/_ispo.htm (закладка "Нормативные и методические документы по технической защите информации", рубрика "Специальные нормативные документы").

Реализовать до 01.01.2011 комплекс мер по защите персональных данных в соответствии с действующими правовыми актами и методическими документами в виде системы защиты персональных данных

- Мероприятия по обеспечению безопасности персональных данных при их обработке в информационных системах перечислены в п.12 Положения от 17.11.2007 № 781 и включают в себя:
- определение угроз безопасности персональных данных при их обработке, формирование на их основе модели угроз;
- разработку на основе модели угроз системы защиты персональных данных, обеспечивающей нейтрализацию предполагаемых угроз с использованием методов и способов защиты персональных данных, предусмотренных для соответствующего класса информационных систем;
- проверку готовности средств защиты информации к использованию с составлением заключений о возможности их эксплуатации;
- установку и ввод в эксплуатацию средств защиты информации в соответствии с эксплуатационной и технической документацией;
- обучение лиц, использующих средства защиты информации, применяемые в информационных системах, правилам работы с ними;

Требования к техническим средствам защиты персональных данных

Защита ПДн должна охватывать все элементы информационной системы как подключенные к ней, так и участвующие в обработке ПДн:

- рабочие станции пользователей;
- файловые и архивные сервера;
- сервера приложений;
- сервера операционных систем;
- почтовые сервера;
- места логического выделения сегментов ЛВС, обрабатывающих ПДн;
- передачу ПДн через общедоступные и международные сети

Рекомендации:

сервер и коммутатор в шкаф, под замок с контролем доступа

Ревизия кабельного хозяйства: все кабели под контролем

Выделить рабочие места с обработкой Пдн в локальный сегмент и изолировать их.

Изображения на мониторах ПДн должны быть недоступны для просмотра посторонних

Отключить локальный сегмент ПДн от общедоступных сетей.

Защита ПДн должна охватывать все элементы информационной системы как подключенные к ней, так и участвующие в обработке ПДн:

- **Системное программное обеспечение;**
- **Прикладное программное обеспечение;**
- **Другое программное обеспечение (почтовые клиенты, антивирусное ПО, архиваторы, текстовые и табличные процессоры)**

Рекомендации:

Инвентаризация ПО

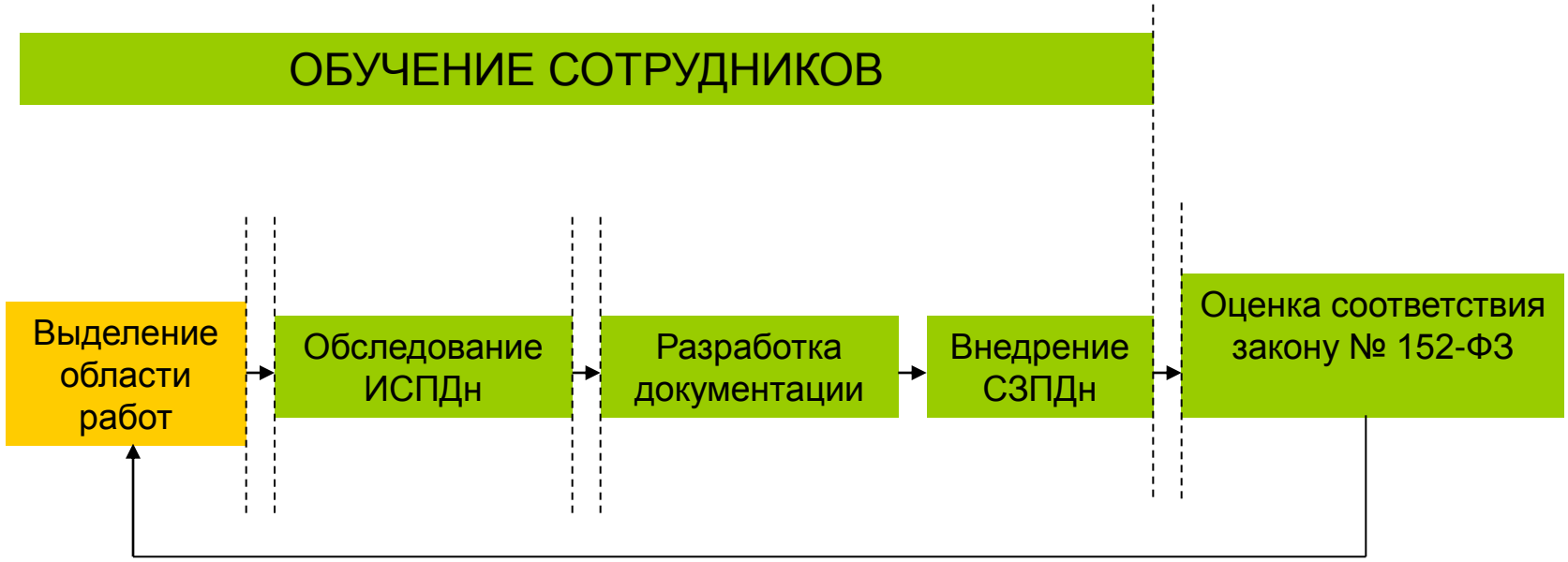
Использовать лицензионное ПО, сертифицированное ФСТЭК

Обновляемое системное, прикладное и антивирусное ПО из надежных источников.

Требования к организационно-распорядительной документации

Рекомендации по построению системы защиты персональных данных

Схема выполнения работ по построению СЗПДн низких классов ИСПДн



Стадии построения системы защиты персональных данных

- Предпроектная стадия по обследованию ИСПДн.

- Стадия проектирования и реализации ИСПДн.

- Стадия ввода в действие СЗПДн.

Декларирование соответствия

Декларирование соответствия - это подтверждение соответствия характеристик информационной системы персональных данных предъявляемым к ней требованиям, установленным законодательством Российской Федерации, руководящими и нормативно-методическими документами ФСТЭК России и ФСБ России.

Декларирование соответствия может осуществляться на основе собственных доказательств или на основании доказательств, полученных с участием привлеченных организаций, имеющих необходимые лицензии. Декларации о соответствии, полученные на основе собственных доказательств и с участием третьей стороны имеют одинаковую юридическую силу. Также они имеют действие, аналогичное действию сертификата (аттестата) соответствия, и также действительны на территории всей страны и стран, признающих разрешительные документы системы ГОСТ Р в течение всего срока действия.

ВНИМАНИЕ: ПРОВЕРКА!
ПРОВЕРКИ СОБЛЮДЕНИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

Роскомнадзором в адрес Оператора направляется уведомление о проведении документарной проверки. Такое уведомление должно быть направлено не позднее, чем в течение трех рабочих дней до дня начала ее проведения (п.67.3 Приказа №630). Получив запрос, Оператор обязан предоставить указанные в запросе документы в Роскомнадзор либо его территориальный орган в течение десяти рабочих дней.

Документы должны быть предоставлены в виде копий, заверенных печатью организации - Оператора (при наличии таковой), а также подписью руководителя или иного уполномоченного представителя Оператора.

Основаниями для проведения выездной проверки являются случаи, когда при документарной проверке не представляется возможным:

удостовериться в полноте и достоверности сведений, содержащихся в уведомлении об обработке персональных данных и иных документах Оператора, которыми располагает Роскомнадзор;

оценить соответствие деятельности Оператора требованиям, установленным законодательством РФ в области защиты персональных данных.

ВНИМАНИЕ: ПРОВЕРКА!
ПРОВЕРКИ СОБЛЮДЕНИЯ ЗАКОНОДАТЕЛЬСТВА О ЗАЩИТЕ ПЕРСОНАЛЬНЫХ ДАННЫХ

1. Проверить документы сотрудников Роскомнадзора
2. Потребовать предъявить приказ руководителя Роскомнадзора или его территориального органа.
3. В случае правильного оформления распоряжения на проведение проверочных мероприятий и служебного удостоверения - впустить проверяющих для проведения проверки
Основная задача пришедшего с проверкой сотрудника Роскомнадзора - установить, не нарушаются ли Оператором нормы законодательства, защищающие персональные данные.
Выездная проверка проводится, если при документарной проверке не представляется возможным:
•удостовериться в полноте и достоверности сведений, содержащихся в уведомлении об обработке персональных данных и иных документах Оператора, которыми располагает Роскомнадзор;
•оценить соответствие деятельности Оператора требованиям, установленным законодательством РФ в области защиты персональных данных.
4. По окончании проверки - подписать акт, которым оформляется результат проверки
5. Исполнить предписание либо обжаловать решение Роскомнадзора