Персональные данные (ПДн). Организация работы по защите ПДн в образовательном учреждении

14 апреля 2010 года

Нормативно-правовая база

- Федеральный закон «О защите персональных данных» № 152-ФЗ от 27.07.2006
- Федеральный закон «Об информации, информационных технологиях и защите информации» № 149-ФЗ от 27.07.2006
- Трудовой кодекс Российской Федерации
- Указ Президента РФ «Об утверждении перечня сведений конфиденциального характера» № 188 от 06.03.1997
- Постановление Правительства РФ от 17.11.2007 №781 «Об утверждении Положения об обеспечении безопасности персональных данных при обработке в информационных системах персональных данных»
- Постановление Правительства РФ от 15.09.2008 № 687 «Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

Нормативно-правовая база

Министерство связи и массовых коммуникаций

- совместно с Федеральной службой по надзору в сфере связи и массовых коммуникаций издали Приказ от 17.07.2008 № 08 «Об утверждении образца формы Уведомления об обработке персональных данных», а также Рекомендации по заполнению этой формы
- Приказ от 30.01.2010 «Об утверждении Административного регламента Федеральной службы по надзору в сфере связи, информационных технологий и массовых коммуникаций по исполнению государственной функции «Ведение реестра операторов, осуществляющих обработку персональных данных»

Нормативно-правовая база (непосредственно связана с защитой ПДн при использовании ИТ)

- Постановление Правительства РФ от 15.08.2006 № 504 «О лицензировании деятельности по технической защите конфиденциальной информации»
- Приказ ФСТЭК, ФСБ, Мининформсвязи от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»
- Приложение к Приказу ФСТЭК от 05.02.2010 № 58 «Об утверждении положения о методах и способах защиты информации в информационных системах ПДн»

Нормативно-правовая база (непосредственно связана с защитой ПДн при использовании ИТ)

Методические документы ФСТЭК России:

- «Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн» от 15.02.2008
- «Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн» от 15.08.2008
- «Основные мероприятия по организации и техническому обеспечению безопасности ПДн, обрабатываемых в информационных системах ПДн» от 15.02.2008
- «Рекомендации по обеспечению безопасности ПДн при их обработке в информационных системах ПДн» от 15.02.2008
- Приложение к Приказу ФСТЭК от 05.02.2010 № 58 «Положение о методах и способах защиты информации в информационных системах ПДн»

Нормативно-правовая база (для руководства производителей программного обеспечения для обработки ПДн)

- Постановление Правительства РФ от 29.12.2007 № 957 «Об утверждении положений о лицензировании отдельных видов деятельности, связанных с шифровальными (криптографическими) средствами

Нормативно-правовая база (для руководства производителей программного обеспечения для обработки ПДн)

Документы ФСБ России:

- Приказ от 09.02.2005 № 66, которым утверждено Положение о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации
- Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в информационных системах ПДн с использованием автоматизации (от 21.02.2008 № 149/54-144)
- Типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих гостайну, в случае их использования для обеспечения безопасности ПДн при их обработке в информационных системах ПДн (от 21.02.2008 № 149/6/6-622)

Комплекс мероприятий

- инвентаризация/обследование информационных системы ПДн, созданных/ существующих в организации;
- формирование перечня подразделений и сотрудников, участвующих в обработке ПДн в рамках служебной деятельности (определить лиц, имеющих доступ к данным;
- проведение категорирования ПДн и классификации ИСПДн;
- формирование актуальной модели угроз в отношении каждой ИСПДн и разработке на основе модели угроз системы защиты ПДн;
- анализ возможности по выработке мер, направленных на снижение категорий обрабатываемых ПДн и в необходимых случаях проведение уточнения классов ИСПДн, составление и утверждение акта классификации ИСПДн;
- подготовка технического задания по созданию требуемой системы защиты с учетом присвоенного класса защиты;
- проектировка и внедрение системы защиты ПДн, в т.ч. выполнение требований по инженерно-технической защите помещений, пожарной безопасности, охране, электропитанию и заземлению, санитарные и экологические требования;

Комплекс мероприятий

- разработка пакета внутренних организационно-распорядительных документов, регламентирующих обработку ПДн, в том числе установление сроков хранения данных, а также условий прекращения обработки ПДн;
- аттестация (сертификация) или декларирование соответствия информационной системы персональных данных требованиям безопасности информации;
- назначение сотрудников (специальной комиссии), ответственных за защиту ПДн, в том числе для рассмотрения всех вопросов, связанных с исполнением законодательства о защите персональных данных;
- обучение/повышение квалификации сотрудников в области защиты персональных данных;
- эксплуатация ИС - мониторинг, выявление и реагирование на инциденты ИБ, техническая поддержка и сопровождение подсистем безопасности, контроль;
- контроль.

С чего начать?

- Определить состав и категории обрабатываемых персональных данных
- Установить категории ПДн, способы и цели их обработки
- Определить информационные системы, в которых обрабатываются ПДн (ИСПДн)
- Разработать документы, регламентирующие обработку ПДн в ОУ

Далее – Направить Уведомление в Роскомнадзор

Примерный перечень организационно-распорядительных документов

1. Акт ввода СКЗИ в эксплуатацию
2. Акт внедрения СЗИ
3. Акт уничтожения ключевой информации
4. Акт уничтожения ПДн
5. Акты проведения классификации
6. Журнал выдачи машинных носителей ПДн
7. Журнал инструктажа персонала
8. Журнал тестирования СЗИ
9. Журнал учета и выдачи носителей с ключевой информацией
10. Журнал учета мероприятий
11. Журнал учета нештатных ситуаций
12. Журнал учета носителей ПДн
13. Журнал учета обращений субъектов ПДн
14. Журнал учета пользователей криптосредств
15. Журнал учета СЗИ
16. Журнал учета СКЗИ
17. Журнал учета хранилищ
18. Заключение о возможности эксплуатации СЗИ
19. Инструкция по допуску к ИСПДн
20. Инструкция по учету носителей
21. Письменное согласие субъекта (Типовая форма)
22. План мероприятий по защите ПДн
23. План приведения в соответствие
24. Положение о защите персональных данных
25. Положение о подразделении по защите информации
26. Положение о подразделении по защите информации
27. Положение о порядке обработки персональных данных
28. Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн
29. Приказ о назначении администратора
30. Приказ о назначении ответственного за СКЗИ
31. Приказ о создании комиссии
32. Приказ об организации работ по защите ПДн
33. Приказ об утверждении должностных лиц допущенных к работе с СКЗИ
34. Приказ об утверждении перечня ПДн
35. Приказ об утверждении Положения о защите ПДн
36. Приказ об утверждении списка лиц, имеющих доступ в помещения с ИСПДн
37. Приказ об утверждении списка лиц, имеющих доступ к ИСПДн
38. Руководство администратора безопасности ИСПДн
39. Список сотрудников, допущенных к ИСПДн
40. Технический журнал СКЗИ
41. Требования по обеспечению безопасности ПДн
42. Уведомление об обработке

Реализация мер защиты

- Разработать и внедрить систему защиты персональных данных
- Провести аттестацию или декларирование соответствия ИСПДн по требованиям безопасности информации

Полезные ссылки

- www.rsoc.ru - Федеральная служба по надзору в сфере связи, информационных технологий и коммуникаций (РОСКОМНАДЗОР)
- www.pd.rsoc.ru – Портал персональных данных
- www.fctec.ru - Федеральная служба по техническому и экспортному контролю (ФСТЭК России)