136 стр. PDF 2017 г.

Согласно российскому законодательству, персональнык данные (ПДн) представляют собой информацию, подлежащую обязательной защите.

Настоящее пособие является его четвертой редакцией, в которой учтены изменения и дополнения законодательной базы в данной области, актуальные на декабрь 2016 года. Приведенные рекомендации по созданию системы защиты ПДн основаны, в том числе на положениях Приказа ФСТЭК России № 17 от 11.02.2013. В пособии также рассматриваются требования других законодательных актов, нормативных и методических документов, организация и технология проведения работ по обеспечению безопасности ПДн при их обработке в информационных системах персональных данных на предприятиях различных форм собственности.

Типовые формы документов, приведенные в пособии, могут послужить основой для построения системы защиты информации, соответствующей требованиям юридически значимых нормативных документов. Внутренние организационно-распорядительные документы компании, реализованные на основе этих форм, позволят не опасаться проверок регулирующих ведомств и создать защищенную информационную систему, предоставляющую возможность организации в полной мере реализовать свой конкурентоспособный потенциал.

5. Характеристика и порядок определения актуальных угроз безопасности персональным данным при их обработке в ИСПДн

- *Распределение утечек по видам конфиденциальных данных*
- *Структура источников угроз ИБ*
- *Характеристика внутреннего нарушителя*
- *Модель каналов утечки персональных данных, обрабатываемых в ИСПДн*
- *Типы, виды и классы угроз*
- *Потенциальные технические каналы утечки персональных данных*
- *Алгоритм определения типа и актуальности угроз безопасности информации в ИСПДн*

6. Создание системы обеспечения безопасности персональных данных при их обработке в ИСПДн

- *Система защиты информации предприятия, цели создания и задачи СЗИ, ее состав*
- *Определение уровня защищенности ПДн по исходным данным ИСПДн*
- *Требования к защите ПДн в зависимости от уровня защищенности (ПП № 1119 от 01.11.2012)*
- *Перечень работ по обеспечению безопасности персональных данных*
- *Порядок организации обеспечения безопасности персональных данных в информационных системах ПДн. Оценка обстановки, формирование замысла*
- *Меры и средства защиты от НСД с применением программных и программно-аппаратных средств*
- *Предпроектное обследование, мероприятия на стадии проектирования, затраты на построение СЗПДн, требования к криптогафическим средствам, стадия ввода в действие ИСПДн, аттестация на соответствие требованиям по безопасности информации, разработка документации по вопросам обеспечения безопасности ПДн и эксплуатации СЗПДн*

7. Организация обеспечения безопасности персональных данных при их обработке без использования средств автоматизации

- *Обособление персональных данных от иной информации*
- *Обособление персональных данных с несовместимыми целями обработки*
- *Меры по обеспечению раздельной обработки ПДн*
- *Меры по обезличиванию персональных данных*

8. Особенности порядка получения, обработки, хранения, передачи и любого другого использования персональных данных государственных гражданских служащих РФ

Требования «Положения о персональных данных государственных гражданских служащих РФ и ведение его личного дела» (Указ Правительства РФ № 609 от 30.05.2005)

9. Меры по защите персональных данных операторами, являющимися государственными или муниципальными органами *(Постановление Правительства РФ № 211от 21.03.2012)*

10. Защита автоматизированных систем, обрабатывающих конфиденциальную информацию и имеющих в своем составе ИСПДн в соответствии с руководящим документом «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требований по защите информации» *(утвержден решением Гостехкомиссии России от 30.03.1992)*

11. Защита автоматизированных систем, обрабатывающих конфиденциальную информацию и имеющих в своем составе государственные или муниципальные информационные системы, в соответствии с требованиями о защите информации, не составляющей государственную тайну *(утверждено Приказом ФСТЭК России № 17 от 11.02.13 и Постановлением Правительства РФ № 1119 от 01.11.2012)*

12. Контроль и надзор за выполнением требований нормативных правовых актов Российской Федерации по защите персональных данных

Заключительные положения

Ответы на типовые вопросы по организации защиты персональных данных

В разделе содержатся подробные ответы на 38 вопросов, касающихся ключевых аспектов, связанных с практическим воплощением требований законодательства в сфере обеспечения безопасности ПДн

Приложение 1. Реализация требований законодательства в области обработки и защиты ПДн

Часть 1. Варианты документов по защите автоматизированных систем, в состав которых входит ИСПДн

1. Трудовой кодекс Российской Федерации от 30.12.2001 № 197-ФЗ

   Приведено базоаое положение о персональных данных в организации, которое, согласно гл. 14 Трудового кодекса РФ «Защита персональных данных работника», должно быть в каждой организации, занимающейся обработкой персональных данных

2. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

   Приведены методы организации защиты персональных данных в информационных системах

3. Федеральный закон от 27.07.2004 № 79-ФЗ «О государственной гражданской службе Российской Федерации». Указ Президента РФ от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела»

   В соответствии с Указом Президента РФ от 30.05.2005 № 609 «Об утверждении Положения о персональных данных государственного гражданского служащего Российской Федерации и ведении его личного дела», организация, обрабатывающая персональные данные государственных гражданских служащих Российской Федерации, должна разработать свой нормативный документ, регламентирующий эту деятельность. В качестве примера такого документа приведем документ, разработанный Роскомнадзором

4. Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

   Приведен перечень необходимых документов по обработке и защите персональных данных, направленных на оптимизацию системы защиты информации организации

5. Постановление Правительства РФ от 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»

   Вариант документа по реализации указанного Постановления Правительства РФ приведен в Части 2 Приложения 1

6. Постановление Правительства РФ от 21.03.2012 № 211 «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»

   В качестве примера выполнения требований «Перечня мер...» приведены следующие документы: Приказ «Об утверждении документов по обработке и защите персональных данных в Управлении Федерального казначейства по Волгоградской области», Политика Управления Роскомнадзора по Волгоградской области и Республике Калмыкия по обработке персональных данных, Приказ об утверждении Политики Управления Роскомнадзора по Волгоградской области и Республике Калмыкия по обработке персональных данных и реализации требований к защите персональных данных

7. Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»

   Варианты документов по реализации указанных актов приведены в Части 2 Приложения 1

8. Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»

   Варианты документов по реализации указанных актов приведены в Части 2 Приложения 1

9. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»

   Варианты документов по реализации указанных актов приведены в Части 2 Приложения 1

Часть 2. Варианты документов по защите автоматизированных систем, в состав которых входят ГИС или МИС

1. Сводный перечень организационно-распорядительных документов, регламентирующих организацию работ в организации по защите конфиденциальной информации и персональных данных
2. Приказ о назначении ответственных лиц за обеспечение защиты информации
3. Приказ о назначении сотрудников, ответственных за обеспечение безопасности персональных данных при их обработке в информационных системах персональных данных
4. Приказ о назначении ответственного за выполнение работ по технической и криптографической защите ПДн
5. Приказ о создании комиссии по классификации автоматизированных систем, обрабатывающих конфиденциальную информацию
6. Приказ о создании комиссии по определению уровня защищенности ИСПДН
8. Приказ о выделении помещений для обработки персональных данных
9. Приказ о назначении администратора безопасности средств защиты конфиденциальной информации и ПДн
10. Инструкции по порядку учета и хранению в организации носителей, содержащих конфиденциальную информацию (персональные данные)
11. Положение о порядке организации и проведения работ по защите конфиденциальной информации в организации
13. Инструкции о порядке резервирования и восстановления работоспособности технических средств и программного обеспечения, баз данных и средств защиты информации информационных систем персональных данных в организации
14. Руководство пользователя по обеспечению безопасности ИСПДн в организации
15. Руководство администратора по обеспечению безопасности ИСПДн в организации
16. Журнал учета носителей конфиденциальной информации (персональных данных)
17. Журнал регистрации и учета обращений субъектов персональных данных
18. Журнал учета средств криптографической защиты информации
19. Журнал учета ключевых носителей
20. Журнал учета персональных данных для пропуска субъекта персональных
21. Журнал учета сертифицированных средств защиты информации
22. Перечень сведений конфиденциального характера, подлежащих защите, в том числе ПДн, и лист ознакомления к нему в организации
23. Перечень автоматизированных и информационных систем, обрабатывающих конфиденциальную информацию и персональные данные организации
24. Список лиц, допущенных в защищаемое помещение
25. Список лиц, допущенных к работе на АС (ИСПДн)
26. Список сотрудников, допущенных к работе с персональными данными
27. Акт классификации автоматизированной системы, предназначенной для обработки конфиденциальной информации
28. Акт определения уровня защищенности ИСПДН
29. Акт установки средств защиты информации на объекте вычислительной техники — автоматизированное рабочее место
30. Акт об уничтожении персональных данных
31. Модель угроз безопасности информации и модель нарушителя в организации
32. Частная модель угроз безопасности персональных данных организации
33. План мероприятий по технической защите конфиденциальной информации и персональных данных в организации
34. План внутренних проверок состояния защиты конфиденциальной информации в организации
35. План внутренних проверок состояния защиты персональных данных в организации
36. Матрица доступа сотрудников к сведениям конфиденциального характера (персональным данным)
37. Описания конфигурации и топологии АС (ИСПДн) в организации
38. Схема расположения объекта информатизации относительно границы КЗ, размещения АС и ЗП относительно контролируемой зоны, топологической схемы АС, схем коммуникаций, электропитания и заземления объекта
39. Технический паспорт объекта информатизации

40. Технический паспорт защищаемого помещения
41. Технический паспорт информационной системы персональных данных
42. Заключение о возможности эксплуатации средств защиты информации в информационной системе персональных данных
43. Уведомление об обработке (о намерении осуществлять обработку) персональных данных
44. Раздел должностных инструкций (должностного регламента) сотрудников, имеющих доступ к ИСПДн, в части обеспечения безопасности ПДн
45. Письменное согласие субъектов персональных данных на обработку их персональных данных
46. Требования по защите информации АС от несанкционированного доступа
47. Содержание мер по обеспечению безопасности персональных данных в зависимости от уровня защищенности персональных данных
48. Типовая форма шаблона содержания персональных данных, определенных оператором
49. Положение о разрешительной системе допуска к информационным ресурсам организации, содержащим персональные данные (работников, клиентов, граждан)
50. Определение уровня защищенности информационной системы персональных данных в организации

Часть 3. Варианты документов по защите автоматизированных систем, обрабатывающих конфиденциальную информацию и имеющих в своем составе государственные или муниципальные информационные системы

1. Акт классификации информационной системы

2. Техническое задание на создание информационной системы

   Техническое задание на создание конкретной государственной или муниципальной информационной системы должно быть разработано с учетом всех требований Приказа ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

3. Состав мер защиты информации и их базовые наборы для соответствующего класса защищенности информационной системы

   Определен Приказом ФСТЭК России от 11.02.2013 № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»

Приложение 2. Нормативные правовые акты

Раздел содержит тексты Федеральных законов, Указов Президента РФ, Постановлений Правительства РФ, приказов и руководящих документов федеральных министерств и ведомств, ГОСТов, рекомендаций и комментариев Роскомнадзора и пр. (всего – 43 документа)

Приложение 3. Презентации

1. Основные требования Правительства РФ к обеспечению безопасности ПДн
2. Нормативные правовые акты РФ в области защиты персональных данных и рекомендации по выполнению их требований
3. Формирование модели угроз безопасности персональным данным
4. Порядок разработки организационно-распорядительных документов предприятия по защите ПДн
5. Организация работ по созданию системы технической защиты ПДн при их обработке в ИСПДн. Рекомендации по выбору и применению аппаратно-программных средств защиты ПДн
6. Угрозы безопасности ПДн при их обработке в ИСПДн. Модель угроз безопасности ПДн
7. Практические проблемы, заблуждения и реальности в организации работ по защите ПДн на предприятиях и в организациях (дискуссия)

Приложение 4. Дополнительные публикации

Раздел содержит подборку из 21 тематической публикации