СТАНДАРТ БЕЗОПАСНОСТИ
БЕЗОПАСНОСТЬ КАК СТАНДАРТ

Комплексные решения технической безопасности

Приведение информационных систем персональных данных в соответствие требованиям законодательства Российской Федерации

Начальник аналитического отдела
ООО «Стандарт безопасности»
Дмитрий Мурин
29.03.2012

Основные документы в области обеспечения безопасности персональных данных

Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных»

- Основные определения (ПДн, оператор ПДн, ИСПДн…).
- Принципы и условия обработки ПДн.
- Права Субъекта ПДн.
- Обязанности Оператора ПДн.
- Контроль и надзор за обработкой ПДн.
- Ответственность за нарушение требований.

Перечень Постановлений Правительства Российской Федерации

- Постановление Правительства Российской Федерации от 17.11.2007 № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»
- Постановление Правительства Российской Федерации 15.09.2008 № 687 «Об утверждении Положения об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации»
- Постановление Правительства Российской Федерации от 6.07.2008 № 512 «Об утверждении требований к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных»

Классификация информационных систем персональных данных:

- Совместный приказ ФСТЭК России, ФСБ России и Мининформсвязи России от 13.02.2008 № 55/86/20 «Об утверждении порядка проведения классификации информационных систем персональных данных»

Категории персональных данных ($X_{пд}$)

- категория 1 - персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, **состояния здоровья, интимной жизни**;
- категория 2 - персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к категории 1;
- категория 3 - персональные данные, позволяющие идентифицировать субъекта персональных данных;
- категория 4 - обезличенные и (или) общедоступные персональные данные.

Объем персональных данных (Хндп)

- 1 - в информационной системе одновременно обрабатываются ПДн более чем 100 000 субъектов ПДн;
- 2 - в информационной системе одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн;
- 3 - в информационной системе одновременно обрабатываются данные менее чем 1000 субъектов ПДн.

Классы ИСПДн:

Хпд/Хндп	3	2	1
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

Перечень нормативно-методических документов ФСТЭК России

- Приказ ФСТЭК России от 5.02.2010 №58 «Об утверждении положения о методах и способах защиты информации в информационных системах персональных данных».
- Нормативно-методический документ ФСТЭК России от 15.02.2008 «Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных».
- Нормативно-методический документ ФСТЭК России от 15.02.2008 «Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных» (ДСП).
- Нормативно-методический документ «Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К)», утвержденный приказом Гостехкомиссии России от 30.08.2002 №282 (ДСП).

Перечень нормативно-методических документов 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 персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством 8 Центра ФСБ России 21.02.2008 №149/6/6-622.

- Методические рекомендации по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации, утвержденные руководством 8 Центра ФСБ России 21.02.2008 №149/54-144.

Регламенты проведения проверок

- 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 РФ в области персональных данных, утвержденный приказом МинКомСвязи России от 14.11.2011 №312.
- Типовой регламент проведения в пределах полномочий мероприятий по контролю (надзору) за выполнением требований, установленных Правительством РФ, к обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденный руководством 8 Центра ФСБ России 8.08.2009 №149/7/2/6-1173.

Этапы работ по приведению информационных систем персональных данных в соответствие требованиям законодательства Российской Федерации

Основные этапы работ

1. Подготовительный (аналитический) этап.
2. Этап разработки организационно-распорядительных документов.
3. Этап разработки модели угроз безопасности персональных данных.
4. Этап проектирования.
5. Этап установки средств и систем защиты (СЗИ).
6. Этап оценки соответствия (аттестации) информационных систем.

Задачами подготовительного этапа являются:

- Выявление фактов обработки ПДн.
- Определение технологического процесса обработки ПДн.
- Определение правовых основ процесса обработки ПДн.
- Определение границ рассматриваемых ИСПДн.
- Предварительная классификация систем.
- Формирование требований, предъявляемых к системе защиты ПДн.

Результатом подготовительного этапа является:

Отчетный документ по результатам проведенного аналитического обследования ИСПДн включающий в себя:

- Описание информационной инфраструктуры организации (топология сети, применяемые технические средства и ПО…).
- Описание принятых мер по защите информации.
- Перечень выявленных АС, в которых обрабатываются ПДн (ИСПДн).
- Перечень ПДн, обрабатываемых в ИСПДн.
- Технологический процесс обработки.
- Анализ правовых основ обработки информации в выявленных ИСПДн.
- Сведения, необходимые для проведения классификации рассматриваемых ИСПДн.
- Анализ соответствия процесса обработки ПДн требованиям законодательства РФ в области обеспечения безопасности ПДн;
- Предположение классов ИСПДн.

Задачами этапа разработки организационно-распорядительных документов являются:

- Проведение анализа разработанных внутренних организационно-распорядительных документов, регламентирующих деятельность организации в области обеспечения информационной безопасности, с подготовкой предложений по их доработке.
- Доработка и разработка комплекта проектов внутренних организационно-распорядительных документов (в соответствии с перечнем раздаточного материала).
- Внедрение организационно-распорядительных документов, проекты которых были разработаны.
- Установка режима защиты ПДн в соответствии с разработанными документами.

Результатом этапа является:

- Комплект актуальных, утвержденных организационно-распорядительных документов.
- Режим обеспечения безопасности ПДн, введенный в соответствии с указанными документами.

Задачами этапа разработки модели угроз безопасности ПДн являются:

- Разработка методики определения актуальности угроз безопасности ПДн и составления модели нарушителя.
- Описание нарушителей (субъектов атак) и определение их актуальности.
- Описание каналов атак, доступных каждой актуальной категории нарушителей, и определение класса актуальной категории нарушителей.
- Формирование исходного перечня угроз безопасности ПДн.
- Проведение анализа исходного уровня защищенности ИСПДн.
- Проведение анализа вероятности реализации угроз из исходного перечня.
- Определение возможности реализации угроз из исходного перечня.
- Определение опасности угроз из исходного перечня.
- Определение актуальности угроз.

Результатом этапа является:

Модель угроз безопасности ПДн, включающая в себя:

- обоснованное предположение о границах контролируемой зоны исследуемого объекта;
- методику определения актуальности угроз безопасности информации и составления модели нарушителя;
- описание нарушителей (субъектов атак) и определение их актуальности;
- описание каналов атак, доступных каждой актуальной категории нарушителей, и определение класса актуальной категории нарушителей;
- сформированный (исходный) перечень угроз безопасности ПДн;
- анализ исходного уровня защищенности ИСПДн;
- анализ вероятности реализации угроз из исходного перечня;
- определение возможности реализации угроз из исходного перечня;
- определение опасности угроз из исходного перечня;
- определение актуальности угроз.

Задачами этапа проектирования являются:

- Выработка конкретных технических решений, удовлетворяющих требованиям, предъявляемым к уровню обеспечения безопасности информации заданного типа.
- Выбор согласующихся между собой средств защиты информации (СЗИ), реализующих указанные выше требования.
- Выбор оптимального решения.
- Определение мест размещения СЗИ.

Результатом этапа является:

Технический проект на систему защиты ПДн (СЗПДн), обрабатываемых в ИСПДн организации, включающий:

- общее описание СЗПДн;
- пояснительную записку к техническому проекту СЗПДн;
- описание комплекса технических средств;
- описание программного обеспечения;
- описание автоматизируемых функций;
- схему автоматизации СЗПДн;
- схему функциональной структуры СЗПДн;
- структурную схему комплекса технических средств СЗПДн;
- логическую схему СЗПДн;
- спецификация на оборудование и программное обеспечение;
- ведомость покупных изделий;
- ведомость технорабочего проекта.

Задачами этапа установки средств и систем защиты являются:

- Закупка средств защиты информации (СЗИ) в соответствии с разработанной проектной документацией.
- Установка и настройка необходимых СЗИ в соответствии с разработанной проектной документацией, требованиями руководящих и нормативно-методических документов.
- Разработка приказа о контролируемой зоне.
- Разработка перечня защищаемых ресурсов.
- Разработка разрешительной системы доступа к защищаемым ресурсам.
- Разработка проекта технического паспорта.

Результатом этапа является:

- Утвержденные:
- приказ о контролируемой зоне;
- перечень защищаемых ресурсов;
- разрешительная система (матрица) доступа к защищаемым ресурсам;
- технический паспорт.
- Установленная и настроенная в соответствии с техническим проектом, введенная в эксплуатацию система защиты персональных данных.

Задачами этапа оценки соответствия (аттестации) информационных систем являются:

- Оценка качества и полноты реализованных организационно-режимных и технических мер защиты информации (ПДн).
- Разработка заключения по результатам оценочных испытаний.
- Оформление заключения о соответствии требованиям по безопасности информации (либо аттестата соответствия требованиям по безопасности информации)

Результатом этапа является:

- Заключения о соответствии требованиям по безопасности информации

Либо

- Аттестат соответствия требованиям по безопасности информации (К1)

Слайд вопросов и комментариев

город Ярославль, ул. Угличская, 39В, офис 211
Тел: +7 (4852) 587-300
Факс: +7 (4852) 587-302
http://www.yarsec.ru