Приведение в соответствие информационных систем персональных данных с требованиями Федерального закона № 152-ФЗ «О персональных данных» на федеральном и региональном уровнях

Начальник отдела по информационной безопасности ФГУ ФЦТ

Григорьев Александр Викторович

2010 г.

С чего все начиналось

COUNCIL OF EUROPE CONSEIL DE L'EUROPE

Конвенция совета Европы

О защите физических лиц при автоматизированной обработке данных

Страсбург , 28 января 1981 г.
изменения от 15 июня 1999 г.
Подписана Россией 7 ноября 2001г.

Федеральный закон № 160-ФЗ

О ратификации Конвенции Совета Европы, о защите физических лиц при автоматизированной обработке данных . *19 декабря 2005г.*

Федеральный Закон № 152-ФЗ «О персональных данных»

от 27.07.2006 г.

Постановление Правительства России № 781

"Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных»

Утверждено 17.11.2007 г.

Приказ ФСТЭК, ФСБ и МинИнформсвязи России № 55/86/20 г. Москва

"Об утверждении Порядка проведения классификации информационных систем персональных данных" *от 13 февраля 2008 г.*

Что определяет закон и его цель?

Целью настоящего Федерального закона является обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных, в том числе защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

Статья 3

персональные данные - **любая информация**, относящаяся к определенному или определяемому на основании такой информации физическому лицу (**субъекту персональных данных**), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, **другая информация;**

оператор - государственный орган, муниципальный орган, юридическое или физическое **лицо**, организующие и (или) **осуществляющие обработку персональных данных**, а также определяющие цели и содержание обработки персональных данных;

Что обязан сделать Оператор ?

Статья 19. Меры по обеспечению безопасности персональных данных при их обработке

1. Оператор при обработке персональных данных

обязан принимать необходимые организационные и технические меры,

~~в том числе использовать шифровальные (криптографические) средства,~~ для защиты персональных данных ***N 363-ФЗ от 27 декабря 2009 г.***

Статья 25. Заключительные положения

1. Настоящий Федеральный **закон вступает в силу** по истечении ста восьмидесяти дней после дня его официального опубликования. **(УЖЕ ВСТУПИЛ)**

2. После дня вступления в силу …….**обработка персональных данных**, ……. **осуществляется в соответствии с настоящим Федеральным законом.**

3. **Информационные системы** персональных данных, **созданные до** дня вступления в силу настоящего Федерального закона, **должны быть приведены** в соответствие с требованиями настоящего Федерального закона

не позднее 1 января 2010 2011~~года~~. ***N363-ФЗ от 27 декабря 2009 г.***

4. **Операторы**, ……., **обязаны направить в уполномоченный орган** ……. **уведомление**, предусмотренное частью 3 статьи 22 настоящего Федерального закона,

не позднее 1 января 2008 года.

Что мешало выполнять Закон ?

Информационные системы должны быть приведены в соответствие **2011 не позднее 1 января ~~2010~~ года.** *27 июля 2006г.*
N 363-ФЗ от 27 декабря 2009 г.

Операторы обязаны направить в уполномоченный орган уведомление, **не позднее 1 января 2008 года.**

Нормативно-методические документы

ФСТЭК России *14, 15 февраля 2008 г.*
ФСБ России *21 февраля 2008 г.*

Уполномоченный орган

Постановление Правительства №878 (упоминание) О некоторых вопросах деятельности Федеральной службы Россвязьохранкультуры *15 декабря 2007 г.*
Указ Президента № 1715 о создании Федеральной службы Роскомнадзор *3 декабря 2008 г.*
Постановление Правительства № 228 Положение о Федеральной службе Роскомнадзор *16 марта 2009 г.*

Теперь ничего не мешает !!!

С чего начать?

Уведомление в уполномоченный орган

1) наименование (фамилия, имя, отчество), адрес оператора;
2) цель обработки персональных данных;
3) категории персональных данных;
4) категории субъектов, персональные данные которых обрабатываются;
5) правовое основание обработки персональных данных;
6) перечень действий с персональными данными, общее описание используемых оператором способов обработки персональных данных;
7) описание мер, которые оператор обязуется осуществлять при обработке персональных данных, по обеспечению безопасности персональных данных при их обработке;
8) дата начала обработки персональных данных;
9) срок или условие прекращения обработки персональных данных.

Статья 22. 152-ФЗ

Меры по обеспечению безопасности определяются КЛАССОМ информационной системы

Категории персональных данных

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.

Приказ № 55/86/20

Классы типовых информационных систем

$X_{пд}$ \ $X_{нпд}$	3 менее 1000	2 1000-100 000	1 более 100 000
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	**К2**	К1
категория 1	К1	К1	К1

Приказ № 55/86/20

бязательная сертификация (аттестация) по требованиям безопасности информации;

екларирование соответствия или обязательная сертификация (аттестация) по требованиям безопасности информации (по решению оператора);

ператоры ИСПДн при проведении мероприятий по обеспечению безопасности ПДн (конфиденциальной информации) при их обработке в ИСПДн 1, 2 классов и распределенных информационных систем 3 класса должны получить лицензию на осуществление деятельности по технической защите конфиденциальной информации

Нормативные документы ФСТЭК

Класс специальных информационных систем

Специальные информационные системы – информационные системы, в которых вне зависимости от необходимости обеспечения конфиденциальности персональных данных требуется обеспечить хотя бы одну из характеристик безопасности персональных данных, отличную от конфиденциальности (защищенность от уничтожения, изменения, блокирования, а также иных несанкционированных действий).

К специальным информационным системам должны быть отнесены:
информационные системы, в которых обрабатываются персональные данные, касающиеся состояния здоровья субъектов персональных данных;
информационные системы, в которых предусмотрено принятие на основании исключительно автоматизированной обработки персональных данных решений, порождающих юридические последствия в отношении субъекта персональных данных или иным образом затрагивающих его права и законные интересы.

По результатам анализа исходных данных класс специальной информационной системы определяется на основе модели угроз безопасности персональных данных в соответствии с методическими документами, …….

Приказ № 55/86/20 основание - Постановление Правительства № 781

Наша система: **специальная, 3 класса, не распределенная**

Итоги работы Роскомнадзора за первую половину 2009 года

205 проверок, из которых 119 – плановые, 86 – внеплановые.

Вынесено 293 предписания

Составлено 27 протоколов об административных правонарушениях.

Судами рассмотрено 14 административных дел и взыскано штрафов на 28 тыс. руб.

Что такое защита информации?

Технические меры защиты

Организационно-технические меры и средства защиты

- Резервное копирование
- Изолирование участков оперативной памяти
- Уничтожение остаточных данных
- Контроль целостности данных и программ
- Смена паролей
- Ограничения на использование сетевых сервисов, служб, сетевых протоколов, сценариев

Программные средства ОС

- Средства блокирования исследования, модификации и несанкционированного запуска
- Средства предупреждения пользователей о выполнении опасных действий
- Программные средства администрирования (разграничения полномочий, регистрации и контроля)
- Программные средства идентификации и аутентификации
- Программные средства резервного копирования

Дополнительные программные средства

Криптографические средства

- Абонентского шифрования
- Пакетного шифрования
- Шифрования паролей
- Стеганографии
- ЭЦП
- VPN-технологии

Средства защиты от ПМВ

- Средства контроля целостности
- Специальные средства обнаружения вредоносных программ и «лечения»
- Средства тестирования
- Утилиты для восстановления информации

Другие средства защиты

- Средства тестирования сетей и программ
- Средства обнаружения атак
- Межсетевые экраны

Люди, способные ВСЕ ЭТО эксплуатировать!!!

Что делать в первую очередь?

Модель угроз безопасности → Акт классификации специальной ИСПДн

Уведомление Роскомнадзор

Перечень законодательных требований по обеспечению защиты ПД

Рекомендации по выполнению требований законодательства РФ по организационным аспектам обработки и защиты ПД

Рекомендации по структуре и составу системы защиты ПД в целом

План-график внедрения СЗПДн и финансирование

Результаты обследования технологических процессов обработки и обеспечения защиты ПДн

№	Описание критерия	Источник	Пункт	Соответствует (да/нет/частично)/Не применимо	Пояснение
1.	Законность целей и способов обработки ПДн.	ФЗ-152	статья 5, п.1.1	да	Основаниями для обработки ПДн является Приказ № 2249 от 26.12.2008 Федеральной службы по надзору в сфере образования и науки «О закреплении за Федеральным государственным учреждением «Федеральный центр тестирования» полномочий по осуществлению организационного и информационно-технологического обеспечения организации и проведения единого государственного экзамена».
2.	Соответствие целей обработки ПДн целям, заранее определенным и заявленным при сборе ПДн, а также полномочиям оператора.	ФЗ-152	статья 5, п.1.2	да	Цели обработки ПДн соответствуют целям, заранее заявляемым при сборе ПДн, а также полномочиям оператора.
3.	Соответствие объема и характера обрабатываемых ПДн, а также способов обработки ПДн целям обработки ПДн.	ФЗ-152	статья 5, п.1.3	да	Объем и характер обрабатываемых ПДн, а также и способы обработки ПДн соответствуют целям обработки ПДн.

……И Т. Д.

Что дальше?

Подготовка объекта защиты к вводу СЗИ в действие (организационно-техническая документация)

Установка и настройка СЗПДн

Проведение обучения персонала

Проведение испытаний

Анализ результатов, выдача заключения, аттестатов соответствия на объекты информатизации

Подготовка документов для подачи заявки во ФСТЭК России на получение лицензии

Аттестация

Лицензирование

Организационно-техническая документация

Разработка организационных мер по соблюдению требований законодательства РФ к обеспечению защиты ПДн;

Разработка проектов документов, приказов и распоряжений по реализации разработанных организационных мер по защите ПДн.

Разработка и согласование решений по организационной структуре, обязанностям и правам пользователей при работе в ИСПДн.

Определение подразделений и назначение лиц, ответственных за эксплуатацию средств защиты информации;

«Техническое задание на создание СЗПДн»

«Пояснительная записка на создание СЗПДн»

«Описание технического, программного, информационного обеспечения и технологии обработки (передачи) информации в ИСПДн»

«Программа и методика испытаний»

«Руководство администратора»

«Руководство пользователя»

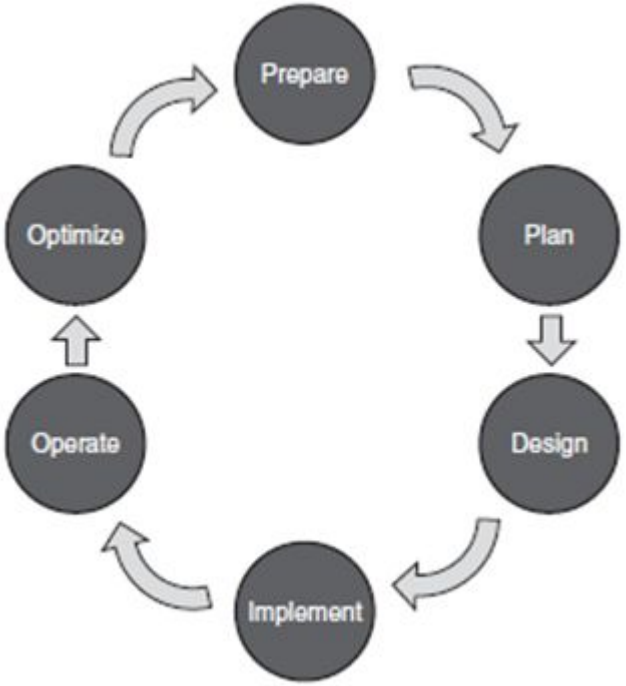
«Инструкция по установке и настройке СЗПДн и ее частей».

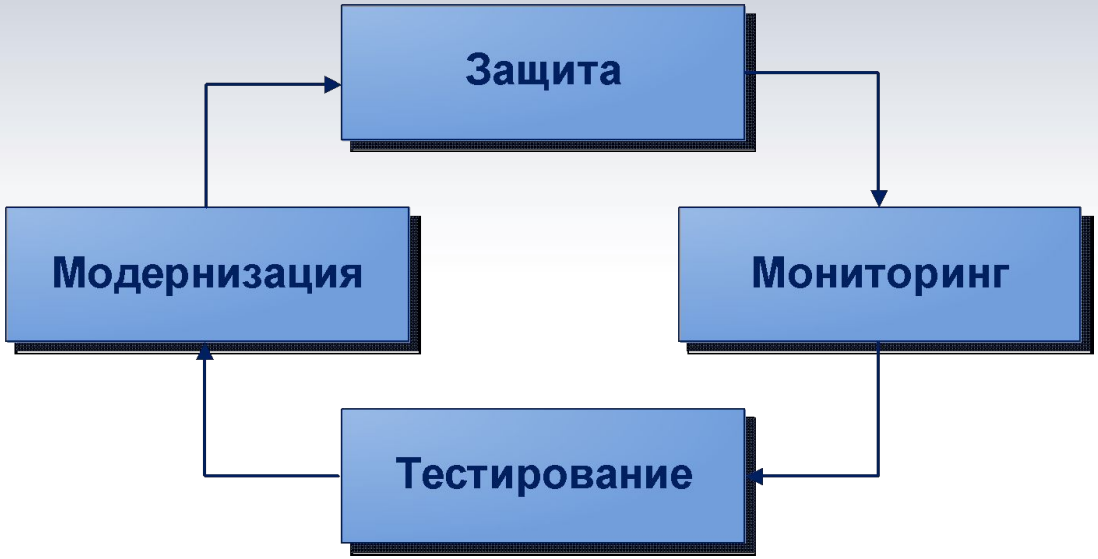
«Акт предварительных испытаний СЗПДн», «Протокол предварительных испытаний СЗПДн».

«Акт приемочных испытаний СЗПДн»,

«Протокол приемочных испытаний» СЗПДн».

Что потом?


Prepare
Plan
Design
Implement
Operate
Optimize


Защита
Мониторинг
Тестирование
Модернизация

Наши контакты

тел. +7 495 530-10-25
факс. +7 495 530-10-30

E-mail: test@rustest.ru

www.RUSTEST.ru