

Организация работ по технической защите информационных систем персональных данных

Слётова Елена Вячеславовна
специалист отдела внедрения систем
информационной безопасности
ООО «Кредо-С»

План выступления

- Структура законодательства в сфере защиты персональных данных
- Последствия невыполнения
- Обеспечение безопасности перс. данных
 - с чего начать
 - последовательность действий, документы
 - требования ФСТЭК
- Обзор средств защиты информации

Закон «О персональных данных» № 152-ФЗ от 27 июля 2006 года

Положение
об обесп. безопасности ПДн при
их обработке в информ. системах
Постановление правительства №781 от 17.11.2007 г

Положение об особ. обработки
ПДн, осуществляемой без исп-я
средств автоматизации
Постановление правительства №687 от 15.09.2008 г

Порядок
проведения классификации информационных систем
персональных данных
Приказы ФСТЭК России, ФСБ России, Мининформсвязи России
от 13 февраля 2008 г. № 55/86/20

Нормативные документы ФСТЭК России

Базовая модель угроз

Методика определения
актуальных угроз

Приказ ФСТЭК № 58 от 05.02.2010
ПОЛОЖЕНИЕ О МЕТОДАХ И СПОСОБАХ
ЗАЩИТЫ ИНФОРМАЦИИ В ИСПДн

Руководящие
документы
ФСТЭК

Последствия невыполнения

- ❖ Уголовная, административная, дисциплинарная ответственность
- ❖ Обоснованные судебные иски от субъектов персональных данных
- ❖ Недобросовестная конкуренция
- ❖ Репутационные риски
- ❖ Приостановка деятельности оператора персональных данных (аннулирование лицензии)

Меры защиты информации

- Организационные
- Охрана помещения (физические)
- Технические
 - защита от НСД
 - защита от утечки по техническим каналам

Если не удалось обеспечить безопасность указанными средствами, то определяется необходимость использования средств криптографии (шифрования).

Алгоритм выполнения работ

- 1) Обследование
- 2) Организационные мероприятия
- 3) Построение и ввод в действие СЗПДн

Мероприятия

1) Инвентаризация ИСПДн

- инвентаризационная комиссия
- Перечень информационных систем (ресурсов) с указанием владельца системы и ответственного за конкретный информационный ресурс)

2) Классификация ИСПДн

- собрать комиссию (можно включать специалистов лицензиата)
- составить Акт о классификации



3) Уведомление уполномоченного органа

- по форме (приказ Россвязьнадзор)

Мероприятия

4) Разработка модели нарушителя и модели угроз

- базовая модель угроз ФСТЭК
- методические рекомендации ФСБ

5) Ограничение доступа к ПДн

- перечень помещений
- оборудование помещения
- перечень лиц, допущенных к персональным данным



Мероприятия

6) Разработка орг. документов:



- Приказ о начале обработки ПДн
 - Положение об организации работы с ПДн
 - Перечень персональных данных
 - Приказ о назначении лица, ответственного за защиту ПДн
 - Журналы учета носителей ПДн, СКЗИ и проч.
- Инструкции ответственного лица, администраторов безопасности и пользователей
- Описание разрешительной системы доступа
- и др.

Мероприятия

7) Разработка технической документации на ИСПДн:

- ЧТЗ
- Технический проект



8) Приобретение средств защиты

- иметь сертификаты (копии) ФСТЭК на все СЗИ
- ответственный выбор поставщика

Мероприятия

9) Установка и настройка СЗИ

- Сертификаты на СЗИ

10) Обучение персонала работе с ПДн и средствами защиты

- Акты
- Внутренняя аттестация

11) Ввод в эксплуатацию СЗПДн

- Акты ввода в эксплуатацию



Мероприятия (метод. док-ты ФСТЭК)

Мероприятия различаются в зависимости от:

- Класса системы (К4, К3, К2, К1)
 - А к какому классу относится Ваша система???
- Режима обработки персональных данных
 - Однопользовательский
 - Многопользовательский
- Разграничения прав доступа
 - Равные права доступа
 - Разные права доступа

Конкретные меры защиты	3 класс	2 класс	1 класс
Межсетевой экран и средство обнаружения вторжений (при наличии подключения ИСПДн к Интернет)	+	+	+
Средство защиты информации от несанкционированного доступа	+	+	+
Средство анализа защищенности и выявления уязвимостей	+	+	+
Средства защиты от утечек за счет ПЭМИН	-	-	+
Криптографические средства	- +	- +	+
Антивирусы	+	+	+
Защита помещения*	+	+	+

Средства защиты информации

- Должны быть сертифицированы ФСТЭК и (или) ФСБ
- Должны вводиться в эксплуатацию организацией, имеющей лицензию на ТЗКИ
- Должны соответствовать классу защищенности
- Должны соответствовать программно-аппаратной конфигурации защищаемого РМ

Наши лицензии

- Лицензия **ФСБ** на оказание услуг в области шифрования информации
- Лицензия **ФСБ** на распространение шифровальных (криптографических) средств
- Лицензия **ФСБ** на техническое обслуживание шифровальных (криптографических средств)
- Лицензия **ФСТЭК** на техническую защиту конфиденциальной информации

СЗИ от НСД

- Обеспечивают контроль доступа к ИСПДн



Межсетевые экраны

- Обеспечивают безопасность ПДн при межсетевом взаимодействии (подключении к сети Интернет, либо другим локальным сетям организации)



СЗИ от ТКУИ

- Обеспечивают защиту от утечек по ТК



И напоследок

- Все СЗИ должны устанавливаться **ТОЛЬКО** на лицензионную операционную систему!!!





Спасибо за внимание!

ООО «Кредо-С»
Слётова Елена
Вячеславовна

slyotova@credos.ru

www.credos.ru

www.uc.credos.ru

Дальнейшее
взаимодействие: