Защита персональных данных. Теория и практика.

Дмитрий Гусев

Зам. генерального директора ОАО «ИнфоТеКС»

gusev@infotecs.ru

План доклада

- Нормативно-правовая база
- Требования и рекомендации ФСТЭК и ФСБ России по защите ПДн
- Порядок выполнения работ
- Применение продуктов ViPNet в проектах по защите ПДн

Термины и определения

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

Информационная система персональных данных (ИСПДн) - информационная система, представляющая собой совокупность ПДн, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких ПДн с использованием средств автоматизации или без использования таких средств.

Оператор ИСПДн – государственный орган, муниципальный орган, юридическое или физическое лицо, организующие и (или) осуществляющие обработку ПДн с использованием ИСПДн, а также определяющие цели и содержание обработки ПДн

Неправомерные действия с персональными данными – преднамеренное или случайное несанкционированное ознакомление с ПДн, их копирование, распространение, передача, уничтожение, изменение (модификация), блокирование, а также любое иное несанкционированное использование, которое может нанести ущерб субъекту ПДн, обществу или государству

Нормативно-правовая база и действующие субъекты

ФЗ "О ПЕРСОНАЛЬНЫХ ДАННЫХ"

(№ 152-ФЗ от 27 июля 2006 г.)

Положение об обеспечении безопасности ПДн при их обработке в ИСПДн

(Постановление Правительства от 17.11.2007 г. № 781)

Нормативные правовые акты и методические документы

ФСБ России

ФСТЭК России

Роскомнадзор

уполномоченный ФОИВ по защите прав субъектов ПДн, Указ Президента РФ от 12.05.2008 г. №724, Пост. Правительства РФ от 2.06.2008 года №419

Оператор ПДн

Требования и рекомендации

ФСБ России (открытый документ)

- Методические рекомендации по обеспечению с помощью криптосредств безопасности ПДн при их обработке в ИСПДн с использованием средств автоматизации

ФСТЭК России (ДСП, открытые выписки)

- Основные мероприятия по организации и техническому обеспечению безопасности персональных данных, обрабатываемых в информационных системах персональных данных
- Рекомендации по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных
- Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных
- Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных

ФСБ, ФСТЭК и Минсвязи (открытый документ)

- Порядок проведения классификации информационных систем персональных данных

Требования и рекомендации

РЕКОМЕНДАЦИИ ПО ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Рекомендации предназначены для специалистов по ИБ, руководителей организаций и предприятий, организующих и проводящих работы по обработке ПДн в ИСПДн

В документе:

- раскрываются вопросы организации обеспечения безопасности ПДн;
- дается оценка опасности угроз безопасности ПДн;
- рассматриваются способы, меры и средства защиты ПДн

Требования и рекомендации

ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ И ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн, ОБРАБАТЫВАЕМЫХ В ИСПДн

Документ предназначен для государственных и муниципальных органов, юридических и физических лиц, организующих и (или) осуществляющих обработку персональных данных, определяющих цели и содержание обработки ПДн, а также заказчиков и разработчиков информационных систем персональных данных при решении ими задач по обеспечению безопасности ПДн

Документ содержит:

- Основные мероприятия по организации обеспечения безопасности ПДн (понятие организации обеспечения безопасности, стадии создания СЗПДн и их основное содержание, условия по ведению работ по обеспечению безопасности ПДн)
- Мероприятия по техническому обеспечению безопасности ПДн при их обработке в ИСПДн (виды мероприятий, перечень мероприятий по видам, конкретное содержание мероприятий для ИСПДн различных классов по подсистемам СЗПДн в соответствии с Базовой моделью угроз безопасности информации)

ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПДн

- ✓ Задание требований к ИСПДн на основе результатов обследования, ключевым моментом которого является инвентаризация ПДн и классификация ИСПДн
- ✓ Оценка соответствия ИСПДн по требованиям безопасности ПДн:
  - для ИСПДн 1 и 2 классов - обязательная сертификация (аттестация)
  - для ИСПДн 3 класса - декларирование соответствия
  - для ИСПДн 4 класса - по решению оператора.
  - Для ИСПДн, находящихся в эксплуатации до введения в действие ФЗ от 27.07.2006 г. № 152-ФЗ, в срок до 1 января 2010 г. должен быть предусмотрен комплекс мероприятий по их доработке по требованиям БИ
- ✓ Получение лицензии на осуществление деятельности по технической защите конфиденциальной информации в соответствии с законодательством операторами ИСПДн 1, 2 классов и в распределенных информационных системах 3 класса

Требования и рекомендации

МЕРОПРИЯТИЯ ПО ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

- ✓ Принципиальных особенностей программно-аппаратного элемента ИСПДн, с точки зрения защиты ПДн, не существует
- ✓ Для ИСПДн 4 класса перечень мероприятий по защите ПДн определяется оператором в зависимости от ущерба, который может быть нанесен в следствии несанкционированного или непреднамеренного доступа к ПДн
- ✓ Мероприятия по защите ПДн от утечки за счет ПЭМИН должны быть реализованы в ИСПДн 1 и 2 классов
- ✓ Мероприятия по защите акустической (речевой) информации должны быть реализованы для ИСПДн 1 класса, если ПДн воспроизводятся акустическими средствами ИСПДн или в ИСПДн предусмотрены функции голосового ввода ПДн

Требования и рекомендации

МЕРОПРИЯТИЯ ПО ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПДн

Перечень мероприятий по защите ПДн определяется в зависимости от класса и режима работы ИСПДн:

- ✓ Защита от несанкционированного доступа при однопользовательском режиме обработки ПДн
- ✓ Защита от несанкционированного доступа при многопользовательском режиме обработки ПДн и равных правах доступа
- ✓ Защита от несанкционированного доступа при многопользовательском режиме обработки ПДн и разных правах доступа
- ✓ Защита информации при межсетевом взаимодействии ИСПДн
- ✓ Антивирусная защита
- ✓ Обнаружение вторжений

Требования и рекомендации

ПОРЯДОК ПРОВЕДЕНИЯ КЛАССИФИКАЦИИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ
(Приказ ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20)

Цель классификации
установления методов и способов ЗИ, необходимых для обеспечения безопасности персональных данных

Выполняется
государственными, муниципальными органами, юридическими и физическими лицами, организующими и (или) осуществляющими обработку ПДн (ОПЕРАТОРАМИ)

Этапы
- сбор и анализ исходных данных по информационной системе
- присвоение информационной системе соответствующего класса и его документальное оформление

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Категории обрабатываемых в информационной системе ПДн:

- ✓ категория 1 - ПДн, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни *(специальные категории персональных данных) (в том числе, данных о судимостях и правонарушениях)*
- ✓ категория 2 - ПДн, позволяющие идентифицировать субъекта ПДн и получить о нем дополнительную информацию, за исключением ПДн, относящихся к категории 1 *(в частности, данные об образовании, профессиональной деятельности, финансовом положении субъекта ПДн)*
- ✓ категория 3 - ПДн, позволяющие только идентифицировать субъекта ПДн *(в дополнение к данным 4 категории – реквизиты документов, удостоверяющих личность, адрес места жительства, место работы, должность, номера телефонов)*
- ✓ категория 4 - обезличенные и (или) общедоступные ПДн *(фактически, только фамилия, имя, отчестве, год и место рождения, семейное положение)*

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Объем обрабатываемых ПДн:

- ✓ 1 - в ИС одновременно обрабатываются ПДн более чем 100 000 субъектов ПДн или ПДн субъектов ПДн в пределах субъекта РФ или РФ в целом;
- ✓ 2 - в ИС одновременно обрабатываются ПДн от 1000 до 100 000 субъектов ПДн или ПДн субъектов ПДн, работающих в отрасли экономики РФ, в органе госвласти, проживающих в пределах муниципального образования;
- ✓ 3 - в ИС одновременно обрабатываются данные менее чем 1000 субъектов ПДн или ПДн субъектов ПДн в пределах конкретной организации

КЛАССИФИКАЦИЯ ТИПОВЫХ ИСПДн

Класс типовой ИСПДн определяется в зависимости от последствий для субъектов ПДн, к которым может привести нарушение заданной характеристики безопасности ПДн:

- ✓ **класс 1** - значительные негативные последствия
- ✓ **класс 2** - негативные последствия
- ✓ **класс 3** - незначительные негативные последствия
- ✓ **класс 4**- не приводит к негативным последствиям

Объем ПДн Категория ПДн	<1000	1000-100 000	>100 000
категория 4	К4	К4	К4
категория 3	К3	К3	К2
категория 2	К3	К2	К1
категория 1	К1	К1	К1

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Характеристики безопасности ПДн, обрабатываемых в ИС:

- ✓ **Типовые** ИСПДн - ИС, в которых требуется обеспечение **только конфиденциальности** ПДн
- ✓ **Специальные** ИСПДн - ИС , в которых дополнительно требуется обеспечить хотя бы одну из характеристик безопасности ПДн, отличную от конфиденциальности – целостность, доступность, неотказуемость и др. (ИСПДн о состояния здоровья; ИСПДн в которых предусмотрено принятие на основании исключительно автоматизированной обработки ПДн решений, порождающих юридические последствия или иным образом затрагивающих права и законные интересы субъекта)

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

4/8

Структура ИС:

- ✓ Автономные ИС - (не подключенные к иным ИС) комплексы технических и программных средств, предназначенные для обработки ПДн (АРМ)
- ✓ Локальные ИС - комплексы АРМ, объединенных в единую ИС средствами связи без использования технологии удаленного доступа
- ✓ Распределенные ИС - комплексы АРМ и (или) локальных ИС, объединенных в единую ИС средствами связи с использованием технологии удаленного доступа

5/8

Наличие подключения к сетям связи общего пользования:

- ✓ Имеющие
- ✓ Не имеющие

6/8

Режим обработки ПДн:

- ✓ Однопользовательский
- ✓ Многопользовательский

Требования и рекомендации

КЛАССИФИКАЦИОННЫЕ ПРИЗНАКИ ИНФОРМАЦИОННЫХ СИСТЕМ ПЕРСОНАЛЬНЫХ ДАННЫХ

Режим разграничения прав доступа пользователей ИС: 7/8

- ✓ С разграничением прав доступа
- ✓ Без разграничения прав доступа

Местонахождение технических средств ИС: 8/8

- ✓ Системы, все ТС которых находятся в пределах РФ
- ✓ Системы, ТС которых частично или целиком находятся за пределами РФ

КЛАССИФИКАЦИЯ СПЕЦИАЛЬНЫХ ИСПДн

Класс специальной ИСПДн определяется на основе модели угроз безопасности ПДн в соответствии с методическими документами государственных регуляторов

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ	МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Требования и рекомендации

БАЗОВАЯ МОДЕЛЬ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Документ предназначен для заказчиков, разработчиков ИСПДн и их подсистем защиты ПДн , при решении задач разработки частных моделей угроз безопасности ПДн в конкретных ИСПДн с учетом их назначения, условий и особенностей функционирования, а также при анализе защищенности ИСПДн от угроз безопасности ПДн в ходе организации и выполнения работ по обеспечению безопасности ПДн и в процессе планирования и проведения контроля состояния обеспечения безопасности ПДн при их обработке в ИСПДн

В документе:

- дается характеристика объектов защиты;
- приводится классификация угроз;
- описываются модели нарушителей;
- раскрывается содержание угроз утечки информации по техническим каналам, угроз НСД, программно-математических воздействий, угроз специальных воздействий электромагнитными полями и др.

Требования и рекомендации

МЕТОДИКА ОПРЕДЕЛЕНИЯ АКТУАЛЬНЫХ УГРОЗ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ ПРИ ИХ ОБРАБОТКЕ В ИНФОРМАЦИОННЫХ СИСТЕМАХ ПЕРСОНАЛЬНЫХ ДАННЫХ

Документ предназначен для специалистов по обеспечению безопасности информации, руководителей организаций и предприятий, организующих и проводящих работы по обработке ПДн в ИСПДн

Методика содержит:

- основные понятия и определения
- показатели исходной защищенности ПДн
- порядок определения актуальных угроз безопасности ПДн в ИСПДн

Подытожим…

Основная рекомендация компании Инфотекс партнерам и клиентам

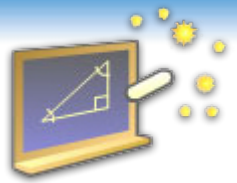
Следует активнее использовать возможность классифицировать ИСПДн как **специальную**, что позволяет в большинстве случаев понизить класс ИСПДн и требования к применяемым СЗИ

Перечень этапов построения системы защиты ПДн

Проведение предпроектного обследования ИСПДн

1. Анализ всей обрабатываемой информации, выделение персональных данных
2. Обследование технических средств, обрабатывающих персональные данные
3. Определение степени участия персонала в обработке персональных данных
4. Определение технологического процесса обработки персональных данных
5. Анализ структуры информационной системы
6. Проведение классификации ИСПДн
7. Составление модели угроз с согласованием во ФСТЭК и ФСБ России

Проектирование системы защиты ИСПДн



1. Разработка технического задания и согласование со ФСТЭК и ФСБ России
2. Разработка технического проекта
3. Разработка организационно-распорядительной документации по вопросам защиты персональных данных

Закупка, установка и ввод в эксплуатацию СЗИ ИСПДн

Средства защиты информации ИСПДн

Применение продуктов ViPNet в проектах по защите ПДн

- ✓ Использование ViPNet CUSTOM 3.0 как системы распределенных межсетевых и персональных сетевых экранов возможно в ИСПДн до 1 класса включительно (сертификат ФСТЭК на 3 класс МЭ и 3 уровень отсутствия НДВ)
- ✓ Использование ViPNet SafeDisk 4.0 как СВТ возможно до 3 класса ИСПДн включительно (сертификат ФСТЭК на 5 класс СВТ и 4 уровень отсутствия НДВ)
- ✓ Использование СКЗИ ViPNet (Домен-КС2/КМ, Client, Coordinator) возможно в ИСПДн до 1 класса (класс СКЗИ определяется моделью нарушителя из модели угроз)

Применение продуктов ViPNet в проектах по защите ПДн

ViPNet позволяет реализовать

- Подсистему разграничения доступа
- Подсистему межсетевого экранирования
- Подсистему защиты от НСД по сети
- Подсистему защиты от НСД к ПДн, хранящихся на компьютерных и отчуждаемых дисках
- Подсистему криптографической защиты

ViPNet не позволяет реализовать

- Подсистему антивирусной защиты
- Подсистему обнаружения вторжений
- Подсистему анализа защищенности
- Подсистему защиты от НСД к файлам ПДн, ОС и прикладного ПО ИСПДн
- Подсистему защиты от ПЭМИН

Спасибо за внимание!

Вопросы

Дмитрий Гусев

Зам. генерального директора ОАО «ИнфоТеКС»

gusev@infotecs.ru