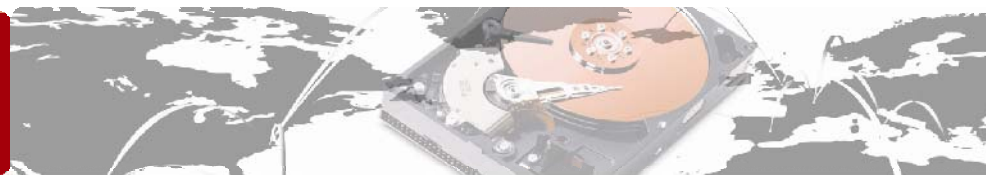


Особенности разработки систем защиты персональных данных в крупных ИСПДн и оптимизация затрат на их создание



Защита ПДн: «Хотели как лучше...» (1)



Ситуация с защитой ПДн описывается в основном негативными факторами:

- Выпущен пакет НПА, но в них есть противоречия и неопределенности
- Реализация требований законодательства влечет значительные сложности для оператора (обсудим далее)
- Реализация требований законодательства влечет значительные затраты
- Нет баланса интересов субъектов ПДн и оператора
- Следствие: ведется много дискуссий. Регуляторы не проявляют большой активности. Мнения каких «экспертов» более правильны?

Защита ПДн: «Хотели как лучше...» (2)



Ситуация с защитой ПДн описывается в основном негативными факторами:

- Мало практики по реализации СЗПДн
- Реактивно-раздражительное отношение к защите ПДн (воспринимается как дополнительный «налог»)
- Чрезмерно нагнетается атмосфера вокруг даты «01.01.2010»
- Оператору ПДн зачастую сложно самостоятельно разобраться в требованиях нормативных документов
- «Закрытый» характер методических документов ФСТЭК (ДСП) и т.д.



Итог: серьезная «головная боль» руководителей и специалистов

Проблемы и особенности крупной ИСПДн



«Маленькие дети – маленькие проблемы, большие дети – большие проблемы» (народная мудрость)

- Сложная архитектура
- Большой «физический» объем оборудования и ПО
- Значительная территориальная распределенность
- Большое число пользователей ИСПДн
- Применение «тяжелых» или «экзотических» технологий
- Высокая значимость для бизнеса/основной деятельности
- Систематическая (и частая!) модификация системы
- Большое число обрабатываемых записей о субъектах ПДн
- «Крупная ИСПДн ≈ большая компания» (интересна проверяющим)

Это только наиболее характерные моменты...

Целеполагание при создании СЗПДн

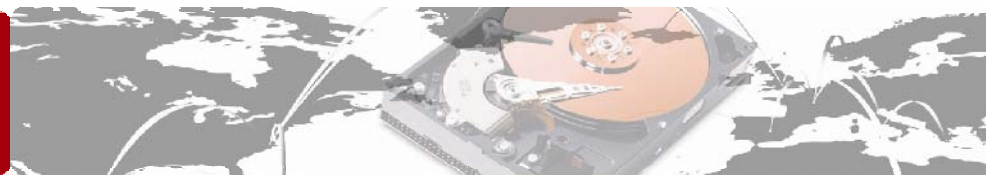


К чему стремиться?

- Цель словами законодателя: обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных (152-ФЗ, ст. 2)
- Цель словами генерального директора: защита бизнеса путем выполнения требований законодательства (иногда также: защита бизнеса путем заботы о клиентах/работниках/...)
- Цель словами главного бухгалтера: защита бизнеса с минимальными затратами
- Цель словами линейного руководителя: защита, не снижающая производственные показатели (в т.ч. - не усложняющая бизнес-процессы, не нагружающая персонал)
- Цель словами ИТ-начальника: защита бизнеса, не усложняющая ИТ-инфраструктуру (в т.ч. – не налагающая доп. обязанности на ИТ-персонал, не снижающая управляемость, не «убивающая» пропускную способность, не снижающая производительность ИС и т.д.)
- Цель словами ИБ-службы: *эффективная* защита (все, что под этим понимается)

Возможно ли? Скорее да, чем нет.

Особенности организации работ (1)



Одна из основных сложностей – планирование и бюджетирование

- Сложно (невозможно) определить заранее, сколько точно времени и средств потребует проект по созданию СЗПДн

Причины:

- Нет полных исходных данных по объекту защиты
- Следовательно, нет понимания, как его надо защищать
- Выход из ситуации: выделение обследования ИСПДн в отдельный проект
 - Просто оценить трудозатраты на аудит, т.е. оценить сроки и стоимость работ
 - Возможность согласовать «векторы» разработки технических решений до начала проектирования (вспомним слайд «Цели»...)
 - Бюджет проекта и внедрения оценивается исходя из рекомендаций по результатам обследования

Особенности организации работ (2)



Что потребовать от исполнителя «на выходе» аудита?

- Перечень ИСПДн (если их несколько)
- Перечень ПДн, обрабатываемых в ИСПДн
- Частную модель угроз
- Проект акта классификации ИСПДн
- Отчет о предпроектном обследовании, в котором содержится:
 - Описание объекта защиты и его особенностей
 - Определение границ объекта защиты (важно! смотрим определение ИСПДн в 152-ФЗ и не тратимся на защиту лишнего)
 - Анализ имеющихся мер и средств защиты информации
 - Рекомендации по созданию СЗПДн
 - Оценка стоимости создания СЗПДн
 - Проект плана создания СЗПДн
- ТЗ (ЧТЗ) на проектирование и внедрение СЗПДн

Особенности организации работ (3)

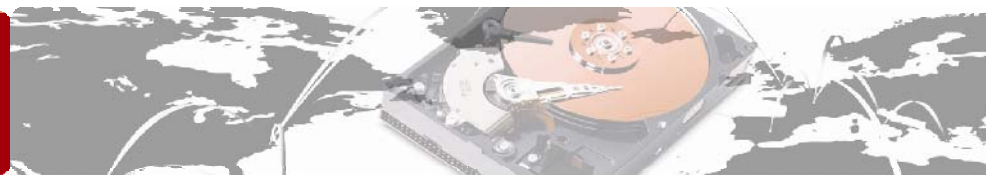


Как быть, если ИСПДн только разрабатывается?

- Существование объекта защиты «в бумаге» осложняет разработку СЗПДн, поскольку:
 - Разработчики могут значительно изменять свои технические решения по ИСПДн и/или наращивать функционал системы
 - Требуемое качество документирования системы достигается как правило к окончанию разработки
 - При наличии у головного исполнителя ИСПДн нескольких контрагентов получение исходных данных существенно усложняется
 - Бизнес-процессы, связанные с ИС, не апробированы и не «обкатаны»
- Для снижения рисков при проектировании СЗПДн нужно:
 - Спланировать проектные работы с временной задержкой относительно основного объекта
 - Определить единую «точку входа» для получения исходных данных
 - Привлечь специалистов по широкому спектру технологий

Из практики: обычно разработчики ИС стремятся учитывать рекомендации проектировщиков СЗПДн

О перечне персональных данных



Первый кубометр бетона в фундамент СЗПДн. Что вносить в Перечень?

- Что является правовым основанием для обработки ПДн?
 - Как правило, со ссылкой на ФЗ («О связи», «Об АО», ТК РФ, ...)
- Что конкретно обрабатывается?
 - Записи БД ИСПДн
 - Формализованные документы, обрабатываемые в ИСПДн
- Каковы условия прекращения обработки ПДн?
 - Типовой вариант: истечение срока исковой давности по ГК РФ
 - Типовой вариант: руководствоваться Перечнем типовых управленческих документов, образующихся в деятельности организаций, с указанием сроков хранения (утв. Федеральной архивной службой РФ 6.10.2000 г.)

Важно: к составлению Перечня необходимо привлечь юристов

О классификации ИСПДн (1)



Второй кубометр бетона в фундамент СЗПДн. Как классифицировать ?

- Типовая ИСПДн

- Таблица из «приказа трех» ($X_{пд}/X_{нпд}$)

- Специальная ИСПДн

- По результатам анализа исходных данных класс специальной ИСПДн определяется на основе модели угроз безопасности ПДн в соответствии с методическими документами, *разрабатываемыми в соответствии с пунктом 2 постановления Правительства Российской Федерации от 17 ноября 2007 г. N 781*

[методики нет, поэтому ...]

- Таблица из «приказа трех» ($X_{пд}/X_{нпд}$)

- «...на основе модели угроз безопасности», сопоставляя определения классов ИСПДн из «приказа трех» с вербальными показателями опасности угроз из Методики определения актуальных угроз (смотрим следующий слайд)

Особое мнение некоторых экспертов: у специальной ИСПДн не может быть класса, ее класс – «специальная». Но как в таком случае определить, подлежит ли ИСПДн аттестации? Нужна ли оператору лицензия ТЗКИ? Как предъявлять требования к механизмам защиты?

О классификации ИСПДн (2)



Как соотносятся классы ИСПДн с вербальными показателями угроз

Определение класса ИСПДн	Значения вербального показателя опасности угрозы
<p>K1 - нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к <u>значительным негативным последствиям</u> для субъектов персональных данных</p>	<p>Высокая опасность – реализация угрозы может привести к <u>значительным негативным последствиям</u> для субъектов персональных данных</p>
<p>K2 - нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к <u>негативным последствиям</u> для субъектов персональных данных</p>	<p>Средняя опасность - реализация угрозы может привести к <u>негативным последствиям</u> для субъектов персональных данных</p>
<p>K3 - нарушение заданной характеристики безопасности персональных данных, обрабатываемых в них, может привести к <u>незначительным негативным последствиям</u> для субъектов персональных данных</p>	<p>Низкая опасность - реализация угрозы может привести к <u>незначительным негативным последствиям</u> для субъектов персональных данных</p>

Возможный риск: ожидаемая методика классификации спецИСПДн от регулятора преподнесет сюрприз

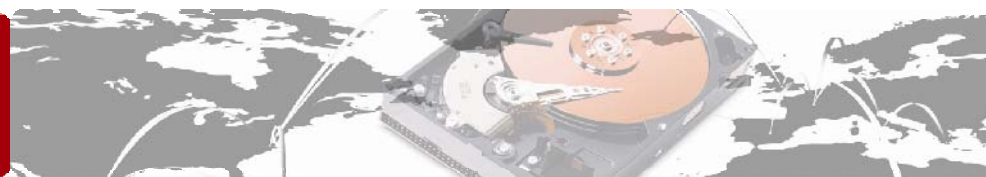
О важности частной модели угроз безопасности ПДн



Модель угроз – эффективный инструмент для оптимизации

- Частная модель угроз – склад исходных данных для дифференцированного предъявления требований к подсистемам СЗПДн
- МД регуляторов предоставляют широкие возможности по рациональному определению актуальных угроз:
 - «... вводятся четыре вербальных градации этого показателя ...»
 - «... на основе опроса экспертов (специалистов в области защиты информации) определяется вербальный показатель ...»
 - «... обоснованные ограничения на степень информированности нарушителя ...»
 - «... обоснованные ограничения на имеющиеся у нарушителя средства атак ...»

Техническое задание на СЗПДн



Чем наполнить ТЗ (ЧТЗ)?

- Общее оформление и структура - по ГОСТ 34.602-89(ТЗ на АС)
- МД ФСТЭК определяют наличие отдельных пунктов
 - Обоснование разработки СЗПДн (наилучший вариант –на базе требований ФЗ и ПП)
 - Исходные данные ИСПДн в техническом, программном, информационном и организационном аспекте (лучше сослаться на отчет об аудите)
 - Класс ИСПДн (на выходе обследования был проект Акта, надо утвердить)
 - Ссылку на НД, с учетом которых будет разрабатываться СЗПДн и приниматься в эксплуатацию ИСПДн (федеральные НПА/МД/РД + свои ОРД оператора)
 - Конкретизацию мероприятий и требований к СЗПДн (по МД ФСТЭК/ФСБ, с учетом частной модели угроз)
 - Перечень предполагаемых к использованию сертифицированных СЗИ
 - Обоснование проведения разработок собственных СЗИ (если надо)
 - Состав, содержание и сроки проведения работ по этапам разработки и внедрения СЗПДн
- Не забываем об аттестации (К1, К2)

«Сначала было слово». ОРД в ИСПДн (1)



Типовой состав нормативной базы по защите ПДн в организации:

- Перечень ПДн, обрабатываемых в ИСПДн
- Приказ о назначении комиссии по классификации ИСПДн, **акт классификации ИСПДн**, приказ об утверждении акта классификации ИСПДн
- Частная модель угроз безопасности ПДн при их обработке в ИСПДн**
- Уведомление (РКН) об обработке ПДн**, выписка из реестра операторов ПДн (выписка из приказа Роскомнадзора о включении в федеральный реестр операторов ПДн)
- ТЗ (ЧТЗ) на создание СЗПДн**
- Технический проект СЗПДн

«Сначала было слово». ОРД в ИСПДн (2)



Типовой состав нормативной базы по защите ПДн в организации (продолжение):

- План мероприятий по защите ПДн
- План внутренних проверок состояния защиты ПДн
- Положение по организации и проведению работ по обеспечению безопасности ПДн при их обработке в ИСПДн
- Требования по обеспечению безопасности ПДн при их обработке в ИСПДн
- Должностные инструкции персоналу в части обеспечения безопасности ПДн при их обработке в ИСПДн
- Рекомендации (инструкции) по использованию программно-аппаратных средств защиты
- Положение о подразделении, осуществляющем функции по организации защиты ПДн

«Сначала было слово». ОРД в ИСПДн (3)



Типовой состав нормативной базы по защите ПДн в организации (продолжение):

- Положение о подразделении, осуществляющем функции по организации защиты ПДн
- Должностной регламент лиц, имеющих доступ к ПДн (специальный технологический регламент обработки ПДн)
- Приказ о назначении ответственных лиц по защите ПДн
- Приказ о допуске к работе с ПДн
- Приказ об утверждении мест хранения материальных носителей персональных данных
- Типовая форма письменного согласия субъектов ПДн на обработку их ПДн
- Журнал учета материальных носителей персональных данных
- Журнал, содержащий ПДн, необходимые для однократного пропуска субъекта ПДн на территорию, на которой находится Оператор

«Сначала было слово». ОРД в ИСПДн (4)

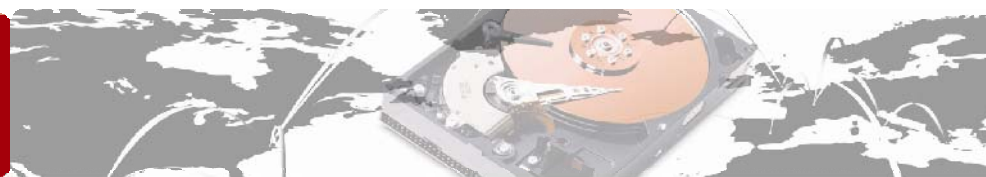


Типовой состав нормативной базы по защите ПДн в организации (продолжение):

- Журнал (книга) учета обращений граждан (субъектов ПДн)
- Акт(ы) об уничтожении персональных данных субъекта(ов) ПДн (в случае достижения цели обработки)
- Журнал (книга) учета вскрытия помещений, в которых разрешена обработка ПДн
- Пакет документов по организации криптографической защиты информации (в случае использования криптосредств)
- Акты установки средств защиты информации
- Программа и методики приемочных испытаний СЗПДн
- Протоколы приемочных испытаний СЗПДн
- Пакет документов по аттестации ИСПДн
- Документы о вводе в действие СЗПДн

Конечный перечень документов определяется особенностями конкретной ИСПДн

«Сначала было слово». ОРД в ИСПДн (5)

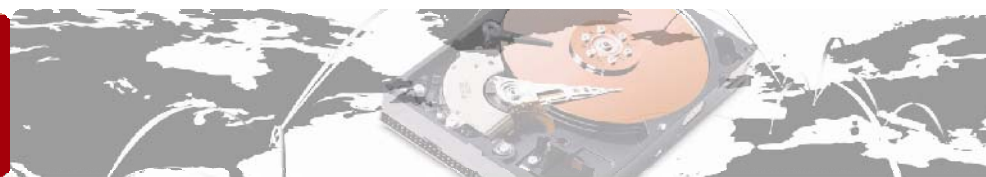


Как оптимизировать разработку пакета документов?

- Заказчику – принять участие в разработке документации
- Исполнителю – максимально использовать существующие в организации документы:
 - Приказы и распоряжения
 - Положения и политики
 - Регламенты, правила, инструкции и т.п.
- Гармонизировать имеющиеся документы в соответствии с требованиями законодательства по защите ПДн
- Интегрировать новые документы в существующую систему нормативно-правовых актов организации

Новое для многих операторов: необходимо документально закреплять все действия по защите ПДн. Формализация пусть даже очевидной практики защиты – ключ к прохождению проверок

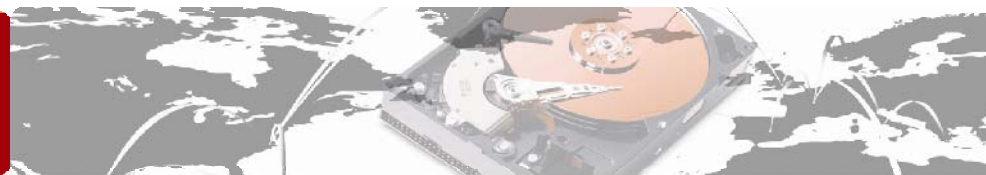
Техническое проектирование СЗПДн. Общие сведения



Чем руководствоваться при подготовке техпроекта?

- По МД ФСТЭК («Основные мероприятия...») – «разработка раздела ТП ИСПДн в части защиты информации». На практике в крупных ИСПДн формируется отдельный технический проект
- «Классика жанра» – ГОСТы 34-й серии
 - Стадии работ – придерживаемся ГОСТ 34.601-90
 - Комплектность документов, виды, обозначения – по ГОСТ 34.201-89
 - Содержание документов – в соответствии с РД 50-34.698-90 и с учетом требований ТЗ, технические решения – согласно РД/МД регуляторов
- Эксплуатационная документация на ТС – по ГОСТ 2.601-2006
- Примерный состав проектной документации:
 - Ведомость ТП
 - Пояснительная записка ТП
 - Схема структурная КТС
 - Ведомость покупных изделий
 - ...а так же другие документы по требованию заказчика

Технологические проблемы в крупных ИСПДн



Почему традиционные подходы неприменимы?

- Как обычно защищают ИСПДн?
 - Пакет организационных мер
 - Комплект наложенных сертифицированных СЗИ
- Какие проблемы появляются в крупных системах?
 - Потеря управляемости в системе защиты
 - Дополнительная нагрузка на каналы связи от трафика СЗИ
 - Организационные проблемы эксплуатации системы защиты
 - Тенденции к отказу пользователей от применения механизмов защиты
 - «Поддержка в легитимном состоянии» после аттестации
- В крупных ИСПДн стоимость внедрения системы растет пропорционально числу защищаемых компьютеров:
 - По данным ряда интеграторов: защита АРМ – 15 000 руб., защита сервера – 20 000 руб.
 - Реальная ИСПДн в телекоме: ~3000 АРМ, ~20 серверов; порядок затрат – десятки миллионов рублей

Альтернативные варианты построения СЗПДн (1)



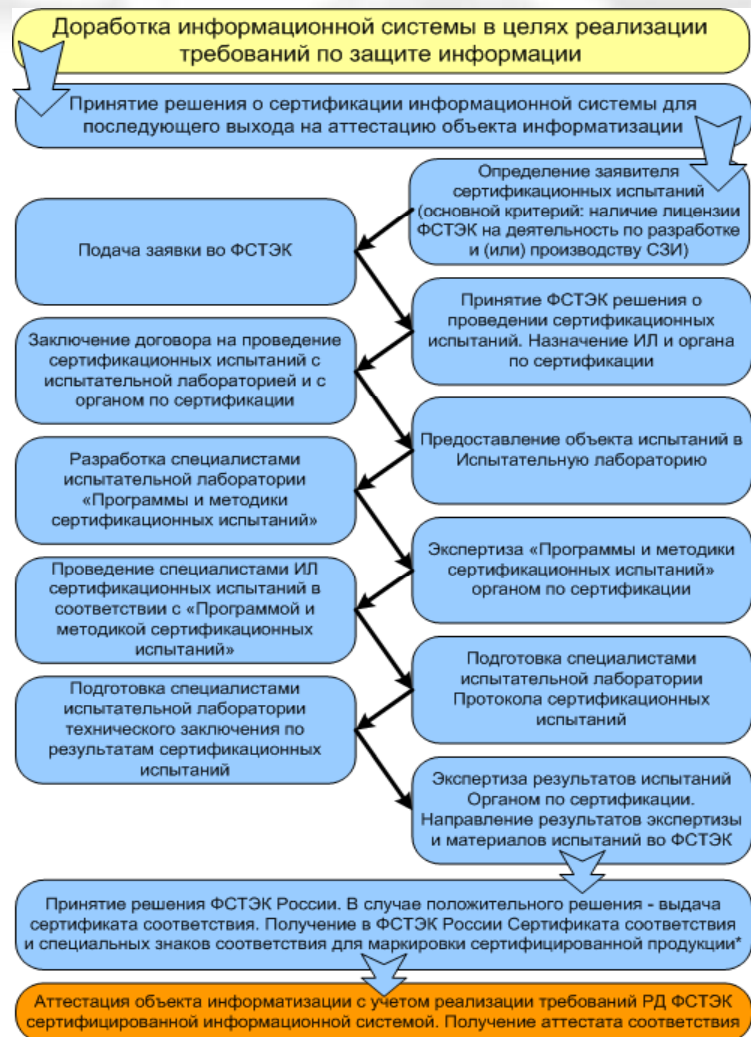
Вариант «От сертификации ПО – к аттестату соответствия»

- Реализация максимального количества требований по безопасности информации в самой информационной системе
- Сертификация на соответствие требованиям РД/МД ФСТЭК (проверка реализации требований по безопасности информации)
- Сертификации подлежит программный комплекс на базе аппаратной части (оборудование серверов и рабочих станций), состоящий из ОС сервера и клиента, СУБД и СПО
- Достоинства:
 - Обеспечивается глубокая централизация механизмов безопасности (как следствие – удобство администрирования)
 - Уход от использования «наложенных» средств защиты
 - Имеется возможность использовать встроенные механизмы безопасности ОС и СУБД
 - Снижаются затраты на внедрение СЗПДн
 - Хорошая «аттестабельность» решения
 - При изменении СПО системы несложно обеспечить сохранение действия аттестата соответствия (условия: согласование с органом по аттестации, изменения не должны касаться функций обеспечения безопасности)

Альтернативные варианты построения СЗПДн (2)



От сертификации информационной системы – к аттестации ИСПДн: «дорожная карта»



Альтернативные варианты построения СЗПДн (3)



Вариант «Терминальные решения»

- В основе решения – терминальный доступ к ИСПДн
- Вся обработка переносится на сторону серверной группы
- «В руках» у пользователей ИСПДн – бездисковый терминал с минимальной функциональностью
- Достоинства не только в ИБ, но и в ИТ:
 - Обеспечивается глубокая централизация механизмов безопасности и управления (как следствие – удобство администрирования и снижение операционных затрат)
 - Уход от использования «наложенных» средств защиты
 - Имеется возможность использовать встроенные механизмы безопасности ОС и СУБД
 - Хорошая «аттестабельность» решения
 - Простота сопровождения ИСПДн и сохранения действия аттестата соответствия
 - Кардинальная оптимизация процессов сопровождения пользователей
- Стоимость внедрения системы защиты не снижается, но альтернативный вариант «Терминальные решения» и не ориентирован только на эту цель, его миссия – помимо обеспечения безопасности реализовать принципиально иную методологию развития ИТ в организации и повышения эффективности бизнеса

Еще об уменьшении стоимости



Сообщество специалистов выработало некоторые векторы

- Не забываем про «банальные» пути экономии на требованиях и средствах их реализации, например:
 - Уменьшение количества рабочих мест, на которых ведется обработка ПДн
 - Исключение обработки ПДн из бизнес-процессов (там, где это возможно)
 - Сегментация ИСПДн (в т.ч. «дробление» БД)
 - Отказ от обработки избыточной информации о субъектах
 - Обезличивание ПДн
 - Переход к обработке без использования средств автоматизации

О корректировке бизнес-процессов



Необходимая неизбежность выполнения 152-ФЗ

- Положения законодательства требуют внедрения новых или видоизменения существующих бизнес-процессов; в частности, необходимо учесть:
 - Получение согласий субъектов ПДн на обработку их ПДн
 - Реализацию прав субъектов ПДн на доступ к их ПДн (и иные действия в соответствии с частью 3 статьи 20 152-ФЗ)
 - Исполнение обязанности сообщить в РКН по его запросу информацию, необходимую для осуществления деятельности данного органа
 - Обязанность уничтожить ПДн по достижении целей обработки/при отзыве согласия на обработку ПДн
 - Обязанность уведомлять РКН об изменениях сведений, указанных в уведомлении об обработке ПДн
 - Вопросы, связанные с эксплуатацией программно-технических средств СЗПДн

О сложностях внедрения



«Гладко было на бумаге, да забыли про овраги...» (народная мудрость)

- Сложности технического характера
 - Возможности ИТ-инфраструктуры должны быть достаточны для развертывания СЗПДн
 - При необходимости в ТП по системе защиты разрабатываются мероприятия по совершенствованию инфраструктуры (раздел пояснительной записки «Мероприятия по подготовке объекта автоматизации к вводу системы в действие»)
- Сложности организационного характера
 - Назначение ответственных лиц/подразделений (потенциальный конфликт интересов ИБ и HR)
 - Делегирование ответственности по обеспечению защиты ПДн на филиальную сеть (необходима дополнительная регламентация)
 - NB! Действия по внедрению элементов СЗПДн и важные события (установка средств защиты, проведение испытаний, приемка системы) должны документироваться

Аттестация – финальный аккорд



Главный парадокс: стоимость аттестации иногда сопоставима со стоимостью защиты

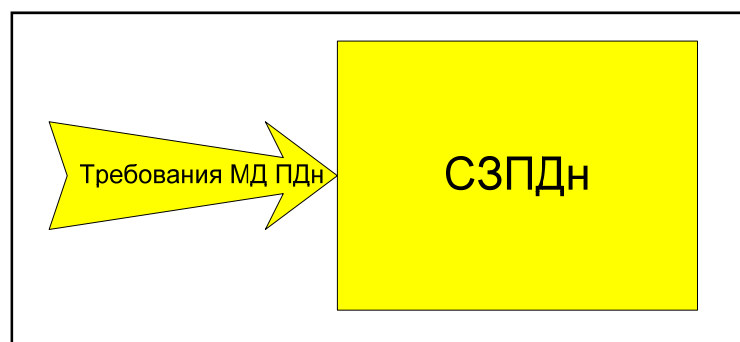
- Для комфортного прохождения оператором процедуры аттестации ИСПДн целесообразно:
 - Закладывать требования по «аттестабельности» системы еще на этапе формирования ТЗ (ЧТЗ)
 - При наличии возможности – согласовывать ключевые документы (например, модель угроз) с регуляторами
 - Заключать договор на сквозной цикл работ «под ключ» с единой точкой входа – головным исполнителем работ, несущим полную ответственность за результат
- Сопровождение аттестованной ИСПДн:
 - Как правило – на основе договора с органом по аттестации
 - Обеспечивается согласование внесения изменений в аттестованный объект
 - Для упорядочения согласования изменений необходим отдельный регламент (внутренние процедуры оператора ПДн + взаимодействие с органом по аттестации)

«Маловато будет!» О комплексной безопасности

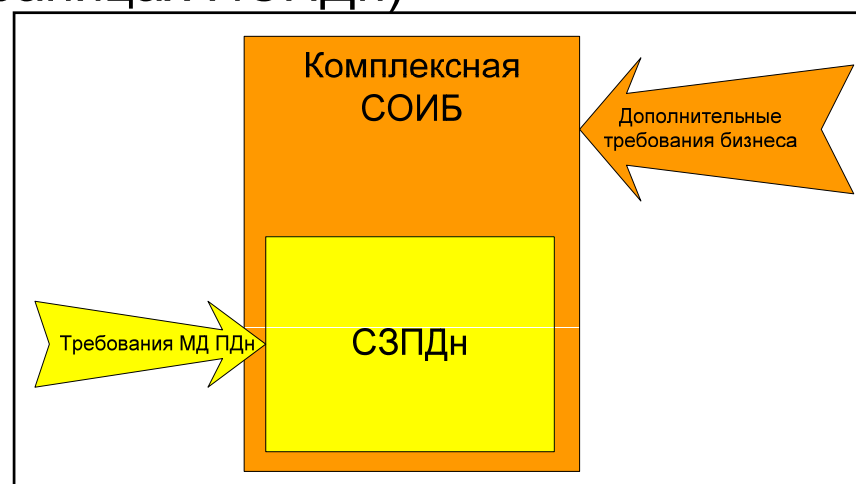


Защита ПДн – хороший повод подумать о более широких требованиях. И при этом сэкономить

- Иногда корпоративные требования к обеспечению безопасности информации перекрывают требования к защите ПДн
- В этом случае СЗПДн может быть разработана как составная часть комплексной СОИБ (и аттестована в границах ИСПДн)



vs



- Это хорошая возможность оптимизировать затраты (два проекта в одном)



Спасибо за внимание!

Контактная информация



Россия, Москва
107023, ул. Большая Семеновская 45
Тел/факс: +7 (495) 730-74-88
Электронная почта: info@inforion.ru
Адрес в сети Интернет: <http://www.inforion.ru/>