Процедуры аттестации и сертификации и их взаимосвязь в свете реализации требований 152 ФЗ

Варианты оценки соответствия ИСПДн различных классов требованиям безопасности ПДн

ИСПДн 1 и 2 классов	обязательная сертификация (аттестация) по требованиям безопасности информации
ИСПДн 3 класса	декларирование соответствия требованиям безопасности информации
ИСПДн 4 класса	оценка соответствия проводится по решению оператора

Какие уровни сертификации СВТ необходимы для каких ИСПДн?
Что будет, если аттестацию не пройти?

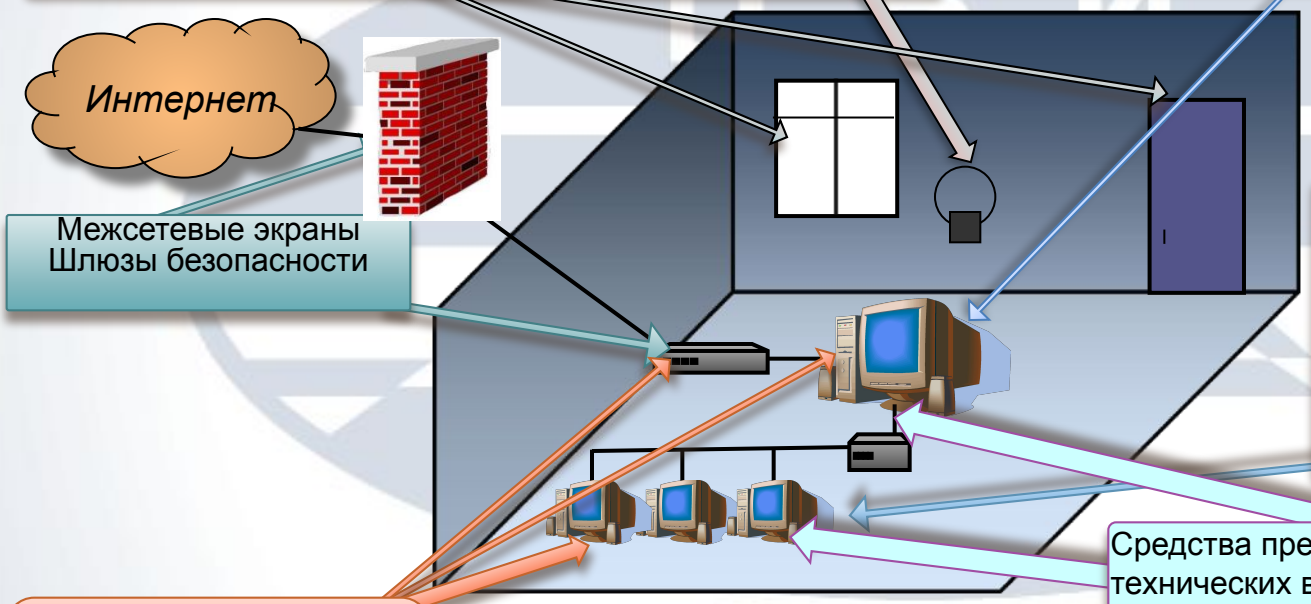
Система защиты ИСПДн

Средства предотвращения утечки информации по техническим каналам

Средства защиты речевой информации

Средства защиты информации, представленной в виде информативных электрических сигналов, физических полей

Используемые в информационной системе информационные технологии



Межсетевые экраны
Шлюзы безопасности

Средства предотвращения несанкционированного доступа к информации:
1. Защищенные ОС:
2. Специализированные средства ЗИ

Средства предотвращения программно-технических воздействий на технические средства обработки персональных данных
1. *Антивирусные средства*
2. *Программное обеспечение, сертифицированное на отсутствие НДВ.*
3. *Системы обнаружения вторжений и компьютерных атак*

Шифровальные (криптографические) средства защиты информации

Средства защиты носителей информации

Что делать, если используются несертифицированные продукты и их замена невозможна?

Большой объём и специальные категории ПДн
Высокие требования по безопасности ПДн

Пути уменьшения сложности решаемой задачи:

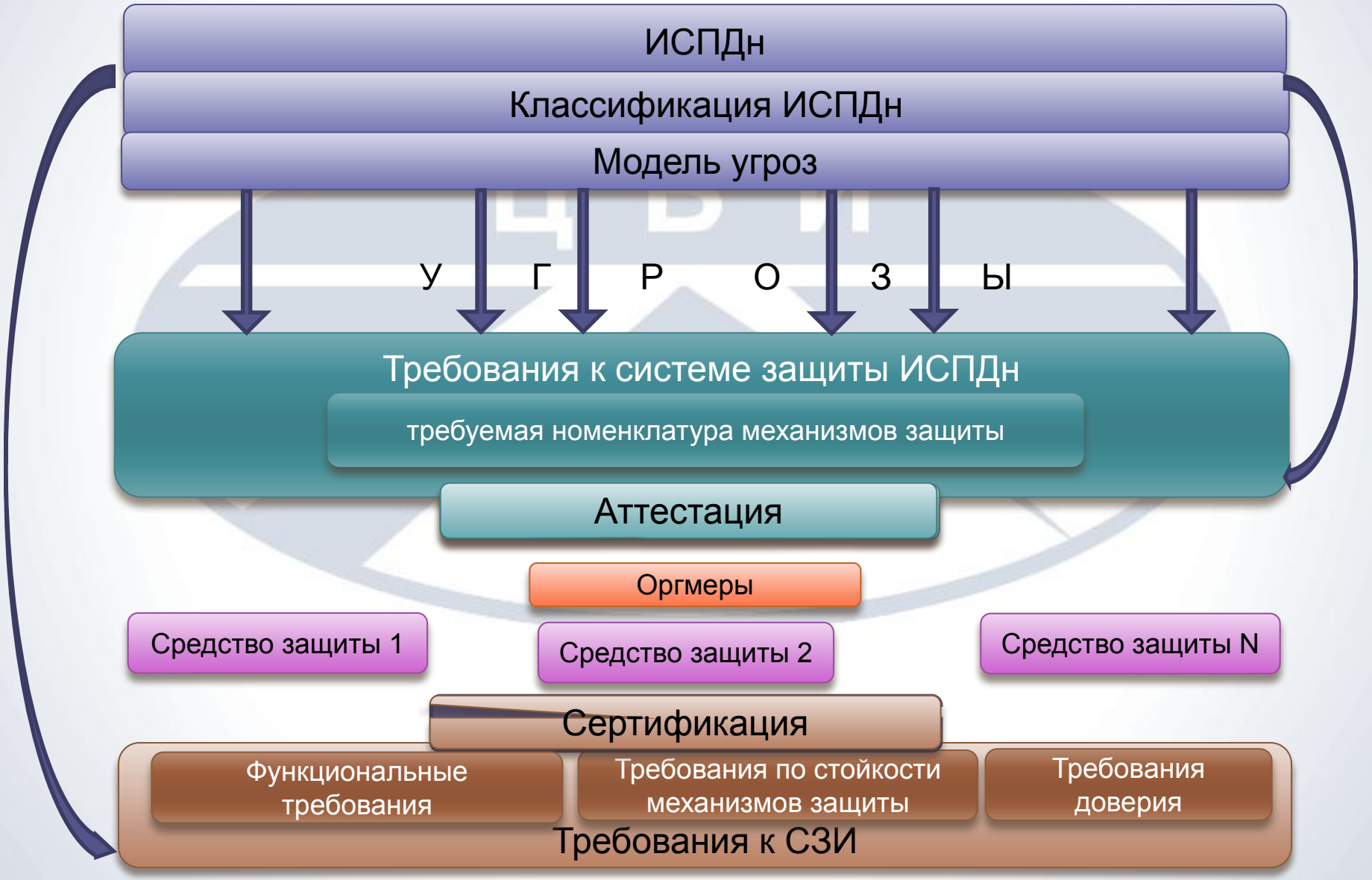
- Декомпозиция (в разрезе ИС и объектов)
- Раздельная классификация
- Модель угроз→только необходимые требования по ЗИ

Что делать, если используются несертифицированные продукты и их замена невозможна?

Модель угроз – основа для уточнения требований

Что делать, если используются несертифицированные продукты и их замена невозможна?

Определение облика системы защиты ИСПДн и оценка ее соответствия



Насколько сертифицированное оборудование и ПО помогает пройти аттестацию?

Типовое решение по защите ПДн

Состав решения:

- сертифицированная платформа (ОС, СУБД);
- сертифицированное прикладное ПО, со встроенными механизмами защиты;
- организационные мероприятия для объекта информатизации;
- комплект эксплуатационных и организационно-распорядительных документов

Эффект:

- гарантированное выполнение всех требований по защите ПДн на множестве типовых объектов
- легкость в модернизации ранее созданных ИСПДн
- сокращение сроков и стоимости внедрения в большое количество ИСПДн

Аттестация по требованиям безопасности ПДн

Кто проводит	Аттестационный центр
Основание	Программа и методика аттестационных испытаний
Этап	Ввод в эксплуатацию, аттестационные испытания
Документ	Аттестат соответствия и Заключение по результатам аттестационных испытаний ИСПДн

Как проходит процедура аттестации?

ФОРМАЛЬНЫЙ ПОРЯДОК ПРОВЕДЕНИЯ ИСПЫТАНИЙ ИСПДн

ПРОВЕРКА СОСТОЯНИЯ ТЕХНОЛОГИЧЕСКОГО ПРОЦЕССА АВТОМАТИЗИРОВАННОЙ ОБРАБОТКИ ИНФОРМАЦИИ

ПРОВЕРКА НА СООТВЕТСТВИЕ ОРГАНИЗАЦИОННО-ТЕХНИЧЕСКИМ ТРЕБОВАНИЯМ ПО ЗИ

ИСПЫТАНИЯ НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

ИСПЫТАНИЯ АС НА СООТВЕТСТВИЕ ТРЕБОВАНИЯМ ПО ЗАЩИТЕ ОТ УТЕЧКИ ПО ТЕХНИЧЕСКИМ КАНАЛАМ

ПОДГОТОВКА ОТЧЕТНОЙ ДОКУМЕНТАЦИИ И ОЦЕНКА РЕЗУЛЬТАТОВ ИСПЫТАНИЙ

Как проходит процедура аттестации? Что должен подготовить оператор системы?

Полнота реализации требования по защите информации

<table>
<tr><td colspan="2">Режим обработки информации в ИСПДн</td><td colspan="3">Однопользовательский</td><td colspan="6">Многопользовательский</td></tr>
<tr><td colspan="2">Права доступа пользователей</td><td colspan="3"></td><td colspan="3">Равные</td><td colspan="3">Разные</td></tr>
<tr><td colspan="2">Класс ИСПДн</td><td>К3</td><td>К2</td><td>К1</td><td>К3</td><td>К2</td><td>К1</td><td>К3</td><td>К2</td><td>К1</td></tr>
<tr><td colspan="2">Система управления доступом</td><td colspan="9">Реализация требований РД «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации»</td></tr>
<tr><td rowspan="2">Обеспечение безопасности межсетевого взаимодействия</td><td>Распределенная ИСПДн</td><td colspan="9" rowspan="2">Применение межсетевых экранов</td></tr>
<tr><td>Подключение к СОП</td></tr>
<tr><td colspan="2" rowspan="2">Подсистема регистрации и учета</td><td colspan="9">Реализация требований РД «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации»</td></tr>
<tr><td colspan="9">Регистрация запросов пользователей на получение ПДн и фактов их предоставления в электронном журнале, защита данных регистрации</td></tr>
<tr><td colspan="2" rowspan="2">Подсистема обеспечения целостности</td><td colspan="9">Реализация требований РД «Автоматизированные системы. Защита от НСД к информации. Классификация АС и требования по защите информации»</td></tr>
<tr><td colspan="8">Возможность незамедлительного восстановления ПДн</td><td>Резервное копирование ПДн на отчуждаемые носители</td></tr>
</table>

Как проходит процедура аттестации? Что должен подготовить оператор системы?

Полнота реализации требования по защите информации

Режим обработки информации в ИСПДн	Однопользовательский			Многопользовательский					
Права доступа пользователей				Равные			Разные		
Класс ИСПДн	К3	К2	К1	К3	К2	К1	К3	К2	К1
Контроль отсутствия НДВ	Соответствующий уровень контроля отсутствия НДВ программного обеспечения, используемого в ИСПДн (средств защиты, в том числе встроенных в общесистемное и прикладное ПО								
Подсистема антивирусной защиты	Антивирусное ПО должно быть сертифицировано по требованиям соответствующего уровня контроля НДВ, а также на соответствие ТУ с требованиям и не ниже соответствующего класса ИСПДн								
Подсистема обнаружения вторжений	Применение систем обнаружения вторжений **Своевременное обнаружение фактов НСД к ПДн** **Недопущение воздействия на технические средства автоматизированной обработки ПДн**								
Подсистема мониторинга	**Постоянный контроль за обеспечением уровня защищенности ПДн**								
Защита ПДн от утечки по техническим каналам		По действующим документам			По действующим документам			По действующим документам	

Как проходит процедура аттестации? Что должен подготовить оператор системы?

Полнота реализации мероприятия по обеспечению безопасности ПДн:

- определение угроз безопасности ПДн, формирование модели угроз;
- классификация ИСПДн;
- разработка системы защиты ПДн;
- разработка документов, регламентирующих вопросы организации обеспечения безопасности ПДн и эксплуатации СЗПДн в ИСПДн;
- установка средств защиты ПДН;
- организация охраны и физической защиты помещений ИСПДн;
- ввод в эксплуатацию системы защиты ПДн, включая оценку соответствия ИСПДн требованиям безопасности информации;
- назначение должностных лиц, ответственных за обеспечение безопасности ПДн, их обучение;
- допуск лиц к работе с ПДн;
- контроль за соблюдением условий использования СЗИ, проведение разбирательств по фактам нарушений;
- разработка и принятие мер по предотвращению возможных опасных последствий подобных нарушений.

Как проходит процедура аттестации? Что должен подготовить оператор системы?

Наличие организационно-распорядительных документов по вопросам обеспечения безопасности ПДн в ИСПДн

- 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 ИСПДн в части обеспечения безопасности ПДн при их обработке в ИСПДн.
- Рекомендации (инструкции) по использованию программных и аппаратных средств защиты информации.
- Руководство администратора безопасности информации в ИСПДн.
- Модель угроз.
- Акт классификации ИСПДн.
- Технический паспорт на ИСПДн.
- Разрешительная система доступа.

Как проходит процедура аттестации? Что должен подготовить оператор системы?

Использование сертифицированных средств защиты информации

- **Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру оценки соответствия** (ПОСТАНОВЛЕНИЕ ПРАВИТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ от 17 ноября 2007 г. N 781)

- **Для программного обеспечения, используемого при защите информации в ИСПДн (средств защиты информации – СЗИ, в том числе и встроенных в общесистемное и прикладное программное обеспечение – ПО), должен быть обеспечен соответствующий уровень контроля отсутствия в нем НДВ** (ФСТЭК РОССИИ. ОСНОВНЫЕ МЕРОПРИЯТИЯ ПО ОРГАНИЗАЦИИ И ТЕХНИЧЕСКОМУ ОБЕСПЕЧЕНИЮ БЕЗОПАСНОСТИ ПЕРСОНАЛЬНЫХ ДАННЫХ, ОБРАБАТЫВАЕМЫХ В ИНФОРМАЦИОННЫХ СИСТЕМАХ)

Какие уровни сертификации СВТ необходимы для каких ИСПДн?

Сертификация СЗИ

О чем молчат поставщики сертифицированных продуктов?

Выбор параметров сертификации:
- система сертификации
- требования – РД (СВТ, МЭ), ЗБ, ТУ, РД НДВ
- схема – единичный образец, партия, производство
- испытательная лаборатория

Подача заявки на сертификацию
Приложение: ТУ или ЗБ

Заключение договора с ИЛ

Получение сертификата

Какие сертификации бывают, и чем они отличаются?

Федеральный ОС

Выдача решения на сертификацию
Назначение органа по сертификации

Выдача сертификата

Экспертиза результатов испытаний

ОС

Отбор образца
(Акт отбора образца)

Разработка программы и методики испытаний
Согласование с ОС

Проведение испытаний образца продукции

Контроль и маркировка партии продукции

Проверка производства продукции

Оформление отчетных документов

Инспекционный контроль сертифицированной продукции

Испытательная лаборатория

Правда ли, что сертифицированное ПО нельзя обновлять?

Подготовка объекта сертификации и документации

Подготовка партии продукции

Подготовка производства продукции

Внесение изменений в сертифицированную продукцию

Разработчик, производитель

Что реально сертифицированные продукты дают организации?