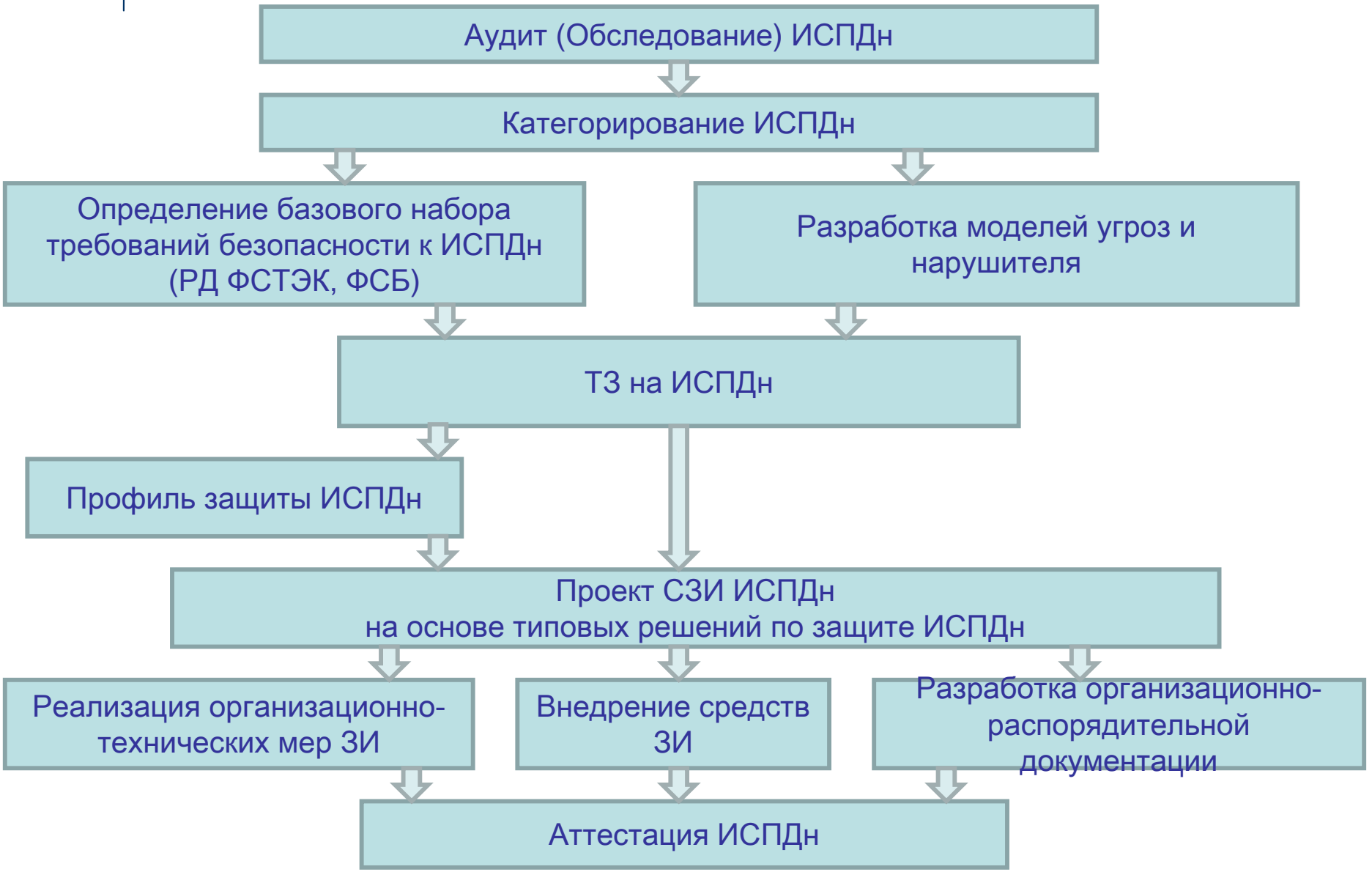
Защита персональных данных

ФЗ 152 «О персональных данных» и иные регламентирующие документы

Практический подход к реализации требований законодательства

Общая схема подхода к защите ИСПДн



Предпроектное обследование

- По результатам обследования разрабатывается **Отчет об обследовании**, показывающий проблемы, препятствующие развертыванию системы защиты персональных данных, а также пути их решения
- Продолжительность данного этапа ~ 1,5- 2 месяцев

Классификация системы

- Определение класса системы обработки персональных данных
- Определение **дополнительных** классификационных признаков системы обработки персональных данных
- Классификационные признаки определяются для каждой конкретной системы согласно Приказам ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20
- **ВАЖНО:**

Приказ №55/86/20 П.17

В случае выделения в составе информационной системы **подсистем**, каждая из которых является информационной системой, информационной системе в целом присваивается класс, соответствующий **наиболее высокому классу** входящих в неё подсистем.

Классифицировать ИСПДн

По категории обрабатываемых персональных данных:

Категория	Описание
1 Категория	Персональные данные, касающиеся расовой, национальной принадлежности, политических взглядов, религиозных и философских убеждений, состояния здоровья, интимной жизни.
2 Категория	Персональные данные, позволяющие идентифицировать субъекта персональных данных и получить о нем дополнительную информацию, за исключением персональных данных, относящихся к 1 Категории.
3 Категория	Персональные данные, позволяющие идентифицировать субъекта персональных данных.
4 Категория	Обезличенные и/или общедоступные персональные данные.

Классифицировать ИСПДн

По объему обрабатываемых персональных данных:

№	Описание
1	В информационной системе одновременно обрабатываются персональные данные более чем **100 000** субъектов персональных данных или персональные данные субъектов персональных данных в пределах субъекта Российской Федерации или Российской Федерации в целом.
2	В информационной системе одновременно обрабатываются персональные данные от **1000 до 100 000** субъектов персональных данных или персональные данные субъектов персональных данных, работающих в отрасли экономики Российской Федерации, в органе государственной власти, проживающих в пределах муниципального образования.
3	В информационной системе одновременно обрабатываются данные менее чем **1000** субъектов персональных данных или персональные данные субъектов персональных данных в пределах конкретной организации.

Определение класса системы

Объем Категория	3	2	1
Категория 4	**К4**	**К4**	**К4**
Категория 3	**К3**	**К3**	**К2**
Категория 2	**К3**	**К2**	**К1**
Категория 1	**К1**	**К1**	**К1**

Результат классификации системы

- Результатом классификации системы обработки персональных данных является **базовый набор требований** по информационной безопасности
- Базовый набор требований по информационной безопасности уточняется и дополняется по результатам разработки **Модели угроз**

Техническое задание

- Разработка системы защиты персональных данных осуществляется по **Техническому заданию** в соответствии с порядком, определённым в СТР-К, нормативных документах ФСТЭК России по обеспечению безопасности персональных данных и национальных стандартах по созданию автоматизированных систем в защищенном исполнении
- **ВАЖНО:** во многих случаях требуется согласовывать ТЗ с ФСТЭК

Профиль защиты

- Профиль защиты представляет собой совокупность минимальных требований для некоторого вида изделий или систем информационных технологий
- Эта конструкция идеально подходит для задания **обоснованных** требований обеспечения безопасности персональных данных, обрабатываемых в информационных системах персональных данных

Проект системы защиты

Включает следующие основные элементы:

- **Информационную характеристику** объекта защиты
- **Требования**, предъявляемые к системе защиты персональных данных
- **Технические решения** по построению системы защиты персональных данных, включая:
  - Структуру и состав системы защиты
  - Проектные решения по системе защиты
  - Спецификацию средств защиты

Организационно-технические меры

Организационно-технические меры по обеспечению безопасности персональных данных включают в себя:

- **процедуры**
- **регламенты**
- **инструкции**, положения которых должны выполняться на объекте информатизации, чтобы обеспечить достаточный уровень контроля и управлять информационной безопасностью

ОРД

ОРД – организационно-распорядительная документация

- ОРД содержат **состав и содержание** организационно-технических мероприятий по обеспечению безопасности персональных данных на объекте информатизации.
- ОРД должны быть разработаны **до ввода** объекта информатизации в эксплуатацию

Аттестация

- **Аттестация** – процесс подтверждения соответствия системы требованиям по безопасности информации, установленных соответствующими нормативными и руководящими документами регулирующих органов (ФТЭК России, ФСБ России). Обязателен для ИСПДН классов 1 и 2.
- Процесс аттестации информационных систем персональных данных процедурно **ничем не отличается** от процесса аттестации систем на другие классы защищенности, определяемые руководящими документами ФСТЭК России
- Аттестатом может подтверждаться соответствие системы **одновременно** нескольким классам, например, классу 1Г в соответствии с РД АС и классу К3 для информационных систем персональных данных
- **ВАЖНО:** необходимо отрабатывать будущие изменения в ИС (версии, патчи систем и проч.). «Аттестат соответствия» выдан сроком на 3 года, в течение которого должна быть обеспечена **неизменность условий** функционирования АС»
- Во многих случаях имеет смысл предусмотреть **аттестацию системы управления**.
- Этот этап занимает **не менее** 1 месяца.

Получение аттестата

2

1. Настоящим **АТТЕСТАТОМ** удостоверяется, что:
Автоматизированная информационная система …….. - «АС …» соответствует требованиям нормативной документации по безопасности информации в части защиты от несанкционированного доступа по классам защищенности:
класс **1Г** – в соответствии с классификацией Руководящего документа Гостехкомиссии России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации»;
класс **К3** – в соответствии с Порядком проведения классификации информационных систем персональных данных (утвержден приказом ФСТЭК России, ФСБ России, Мининформсвязи России от 13 февраля 2008 г. № 55/86/20).
Состав технических и программных средств **АС …** представлен в Техническом паспорте на Автоматизированную информационную систему ……..
2. Организационная структура, уровень подготовки специалистов, обеспечивают поддержание уровня защищенности **АС …** в процессе эксплуатации в соответствии с установленными требованиями.
3. Аттестация **АС …** выполнена в соответствии с “Программой и методикой аттестационных испытаний... ”, утвержденной Председателем Центра безопасности информации ___ ноября 2008 г.
4. С учетом результатов аттестационных испытаний в **АС ….** разрешается обработка конфиденциальной информации.
5. При эксплуатации **АС ….** запрещается без согласования с органом по аттестации:
изменять состав технических и программных средств, входящих в **АС ….**;
изменять установленный порядок доступа персонала к циркулирующей в **АС …** служебной и конфиденциальной информации и режим допуска лиц в помещения с оборудованием **АС ….**;
осуществлять другие технические и организационные мероприятия, которые могут создать предпосылки для утечки защищаемой информации за счет несанкционированного доступа к информации.
6. Контроль за эффективностью реализованных мер и средств защиты возлагается на ответственных за обеспечение информационной безопасности **АС ….**
7. Подробные результаты аттестационных испытаний приведены в “Заключении по результатам аттестационных испытаний на соответствие требованиям по безопасности информации **Автоматизированной информационной системы ……**

3

- «АС …» от ___ декабря 2009 г.
8. «Аттестат соответствия» выдан сроком на 3 года, в течение которого должна быть обеспечена неизменность условий функционирования АС …..
9. Перечень характеристик, об изменениях которых требуется обязательно извещать орган по аттестации:
состав и размещение технических и программных средств АС ….;
состав и настройки установленных в АС ….. средств защиты от несанкционированного доступа к информации;
изменения в технологическом процессе обработки информации в АС ……
Руководитель аттестационной комиссии

_____

“__“ января 2009 г.

“ФОРС-Центр разработки”

Москва, Трифоновский тупик, 3

Телефон: +7(495)787-7040

FDCSecure@fors.ru

http://www.fdc.ru