Многофункциональный общий центр обслуживания
Госкорпорации «Росатом»
Акционерное общество «Гринатом»

Способы оптимизации стоимости работ по аттестации информационных систем

Начальник управления информационной безопасности

Ершов Сергей Викторович

г. Смоленск,
16 февраля 2017 г.

Информационные системы

Государственные информационные системы (ГИС)

федеральные информационные системы и региональные информационные системы, созданные на основании соответственно федеральных законов, законов субъектов Российской Федерации, на основании правовых актов государственных органов

2

Информационные системы персональных данных (ИСПДн)

информационные системы , представляющие собой совокупность персональных данных, содержащихся в базе данных, а также информационных технологий и технических средств, позволяющих осуществлять обработку таких персональных данных с использованием средств автоматизации или без использования таких средств

Требования по аттестации объектов информатизации

«Положение по аттестации объектов информатизации по требованиям безопасности информации» 25.11.1994

Постановление Правительства Российской Федерации

от 15.05.2010 № 330

ГОСТ РО 0043-003-2012

«Защита информации. Аттестация объектов информатизации. Общие положения»

Баланс

Правовые меры

Федеральный закон Российской Федерации

№ 149-ФЗ
от 27.07.2006

Трудовой кодекс Российской Федерации
(№ 197-ФЗ
от 30.12.2001)

Гл.14 «Защита ПДн работников»

Федеральный закон Российской Федерации

№ 152-ФЗ
от 27.07.2006

Постановление Правительства Российской Федерации

от 03.11.1994
№ 1233

Постановление Правительства Российской Федерации

от 01.11.2012
№ 1119

Организационные меры

- Назначение ответственных должностных лиц, администраторов информационной безопасности.
- Разработка локальных нормативных актов, организационно-распорядительной документации.
- Организация контроля за нелегитимными действиями пользователей и обслуживающего персонала информационной системы.
- Разработка правил разграничения доступа к защищаемым ресурсам.
- Планирование и выделение ресурсов: персонала, бюджетных и материальных средств.

Технические меры

Реализуются посредством внедрения следующих основных подсистем:

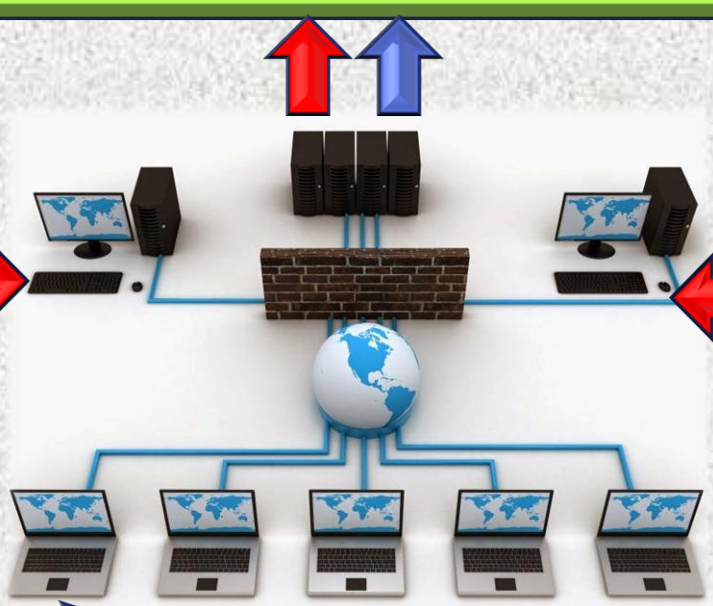
- защиты информации от несанкционированного доступа;
- антивирусной защиты;
- межсетевого экранирования;
- криптографической защиты информации;
- защиты информации от утечек конфиденциальной информации;
- анализа защищённости;
- управления информацией и событиями;
- защиты среды виртуализации;
- обнаружения вторжений;
- защищённого доступа к сетям общего пользования («Интернет»).

Классификация информационной системы

Требования по защите информации

Масштаб информационной системы

(федеральный, региональный, объектовый)



Уровень значимости информации

(УЗ1 - УЗ4)

Тип актуальных угроз безопасности ПДн

(1, 2, 3)

Объём ПДн субъектов ПДн, обрабатываемых в ИСПДн

(сотрудники/ не сотрудники Оператора, более 100 000)

Категория ПДн

(Специальные, биометрические, общедоступные, иные)

Состав мер защиты информации

Меры защиты информации в информационных системах	Утверждены приказом ФСТЭК России							
	№ 17				№ 21			
	Класс защищён.				Уровень защищён.			
	4	3	2	1	4	3	2	1
Идентификация и аутентификация субъектов и объектов доступа								
Управление доступом субъектов к объектам доступа								
Ограничение программной среды								
Защита машинных носителей информации								
Регистрация событий безопасности								
Антивирусная защита								
Обнаружение (предотвращение) вторжений								
Контроль (анализ) защищенности информации								
Целостность информационной системы и информации								
Доступность информации								
Защита среды виртуализации								
Защита технических средств								
Защита информационной системы, ее средств, систем связи и передачи данных								
Выявление инцидентов и реагирование на них								
Управление конфигурацией ИС и системы защиты								

Требования по защите информации

Неправомерное распространение информации

Неправомерное уничтожение

Неправомерный доступ

Модифицирование

Неправомерное блокирование

Незаконное копирование

Обеспечение целостности информации

Обеспечение доступности информации

Обеспечение конфиденциальности информации

Определение актуальных угроз безопасности информации

ФСТЭК России

«Методика определения актуальных угроз безопасности персональных данных при их обработке в ИСПДн»

14.02.2008

ФСТЭК России

«Базовая модель угроз безопасности персональных данных при их обработке в ИСПДн»

15.02.2008

Система сертификации ФСТЭК России

Постановление Правительства Российской Федерации

«О сертификации средств защиты информации»

от 26.06.1995 № 608

ГОСУДАРСТВЕННАЯ ТЕХНИЧЕСКАЯ КОМИССИЯ
ПРИ ПРЕЗИДЕНТЕ РОССИЙСКОЙ ФЕДЕРАЦИИ

СИСТЕМА СЕРТИФИКАЦИИ СРЕДСТВ ЗАЩИТЫ ИНФОРМАЦИИ
ПО ТРЕБОВАНИЯМ БЕЗОПАСНОСТИ ИНФОРМАЦИИ
№ РОСС RU.0001.01БИ00

СЕРТИФИКАТ
№ 1

Выдан: 23 декабря 1993 г.
Действителен до: 23 декабря 1998 г. Действие сертификата продлено до 23 декабря 2001 г.

Настоящий Сертификат удостоверяет, что **система защиты информации от НСД «СНЕГ 1.0»** (ВТГА.7101-01) для ПЭВМ типа IBM PC XT/AT, работающих в операционной среде MS DOS версий 3.30, 4.01, 5.0, соответствует требованиям класса защищенности «1Б» установленным Гостехкомиссией России согласно:

РД «АС. Защита от НСД к информации. Классификация АС и требования по защите информации»;

РД «СВТ. Защита от НСД к информации. Показатели защищенности от НСД к информации»;

ГОСТ и другим НД, указанным в «Перечне нормативных документов, необходимых при аттестации объектов информатики и сертификации средств вычислительной техники и связи».

Средство криптографической защиты данных (СКЗД) «ИНЕЙ», входящее составной частью в систему защиты информации от НСД «СНЕГ 1.0», сертифицировано войсковой частью 43753-С, имеет заключение по результатам инженерно-криптографического анализа от 19.12.91 г. за № 8/9/3-1611 и учитывалось при оценке соответствия требованиям безопасности информации системы защиты информации от НСД в целом.

Сертификат выдан на основании технического заключения о результатах сертификации системы защиты информации от НСД «СНЕГ 1.0» и акта технической приемки и ввода в эксплуатацию системы, утвержденных Гостехкомиссией России 15 июня 1993 года, согласно договору от 12.04.93 г. за № 21-32/1695-471.

Заявитель – Центральный научно-исследовательский институт управления, экономики и информации (ЦНИИАтоминформ) Минатома России
Адрес - 127434, Москва, а/я 971
Тел. - (095) 210-78-56

Инспекционный контроль соответствия системы защиты информации от НСД «СНЕГ 1.0» (ВТГА.7101-01) требованиям руководящих документов Гостехкомиссии России осуществляется 5 ЦНИИИ Минобороны России.

ЗАМЕСТИТЕЛЬ ПРЕДСЕДАТЕЛЯ ГОСТЕХКОМИССИИ РОССИИ

А.П.Каландин

Настоящий сертификат внесен в Государственный реестр сертифицированных средств защиты информации 20 декабря 1993 г.

«Положение о сертификации средств защиты информации по требованиям безопасности информации»

Приказ Гостехкомиссии России от 27.10.1995 № 199

Компенсирующие меры

При невозможности реализации в информационной системе отдельных мер защиты информации, а также с учётом экономической целесообразности на этапах адаптации базового набора мер могут разрабатываться иные (компенсирующие) меры защиты информации, обеспечивающие адекватное блокирование (нейтрализацию) угроз безопасности информации.

Приказ ФСТЭК России

от 11.02.2013 № 17

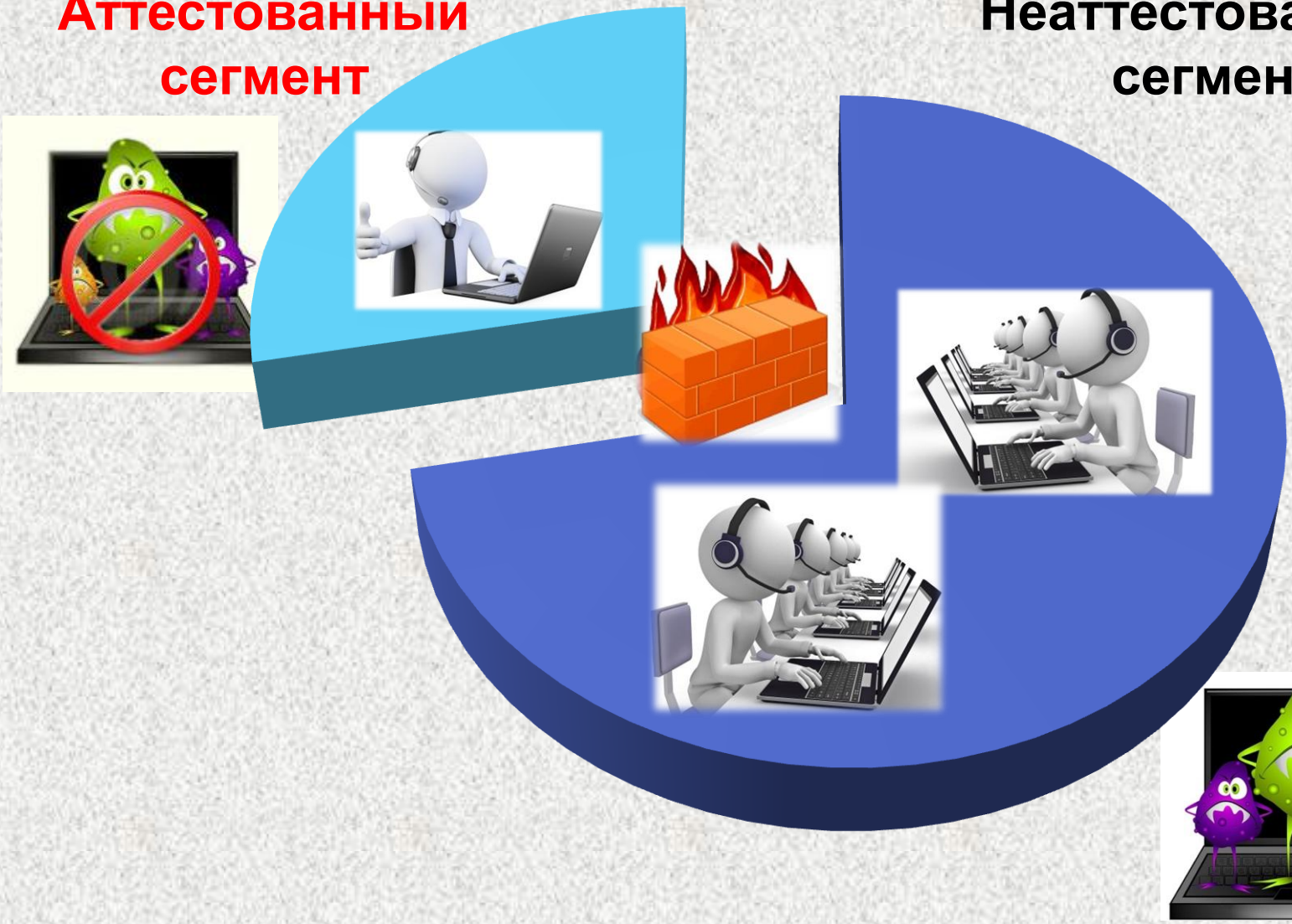
Приказ ФСТЭК России

от 18.02.2013 № 21

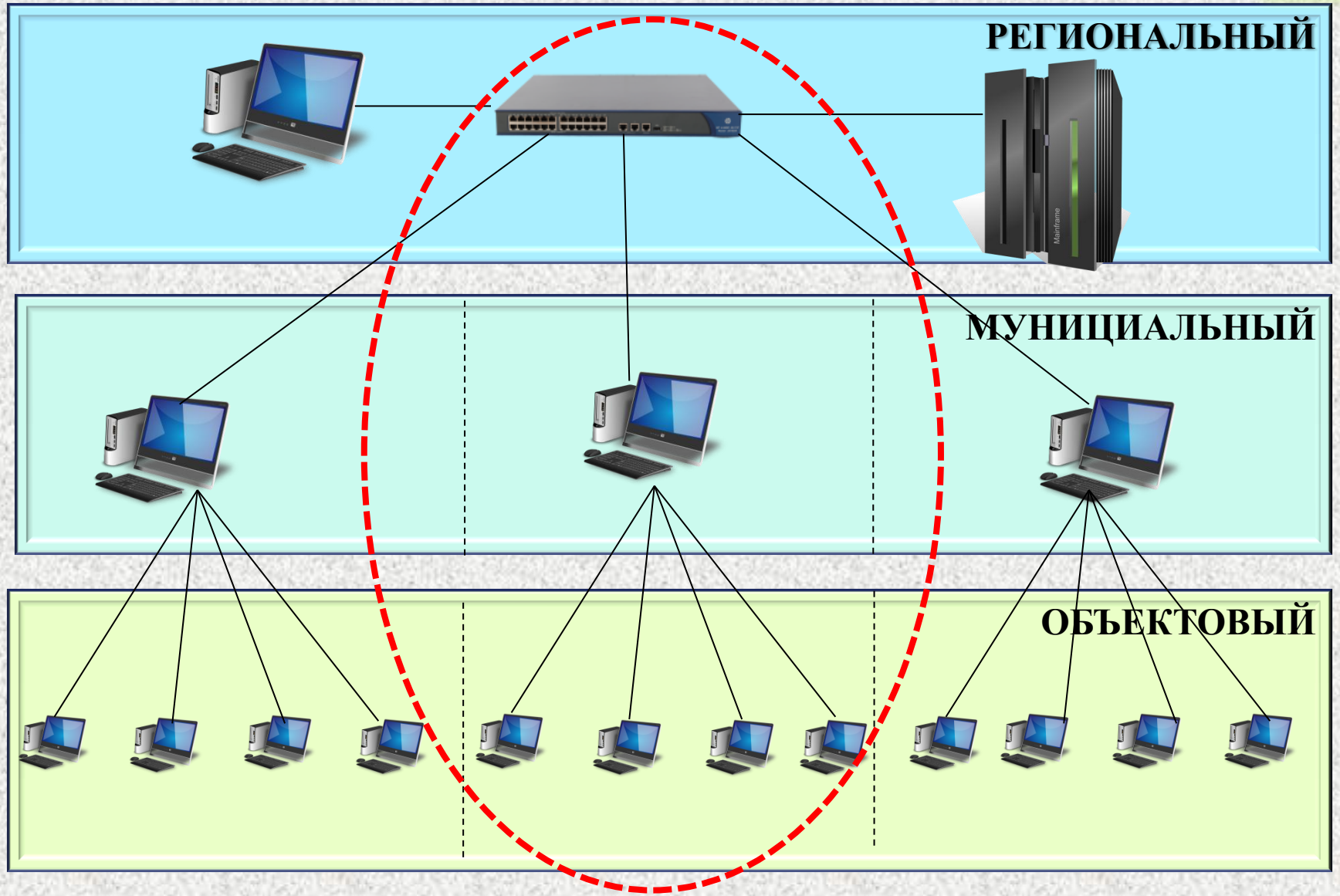
Сегментирование информационной системы

Аттестованный сегмент

Неаттестованный сегмент



Пример определения типовых сегментов



Объекты защиты в информационной системе

Информация

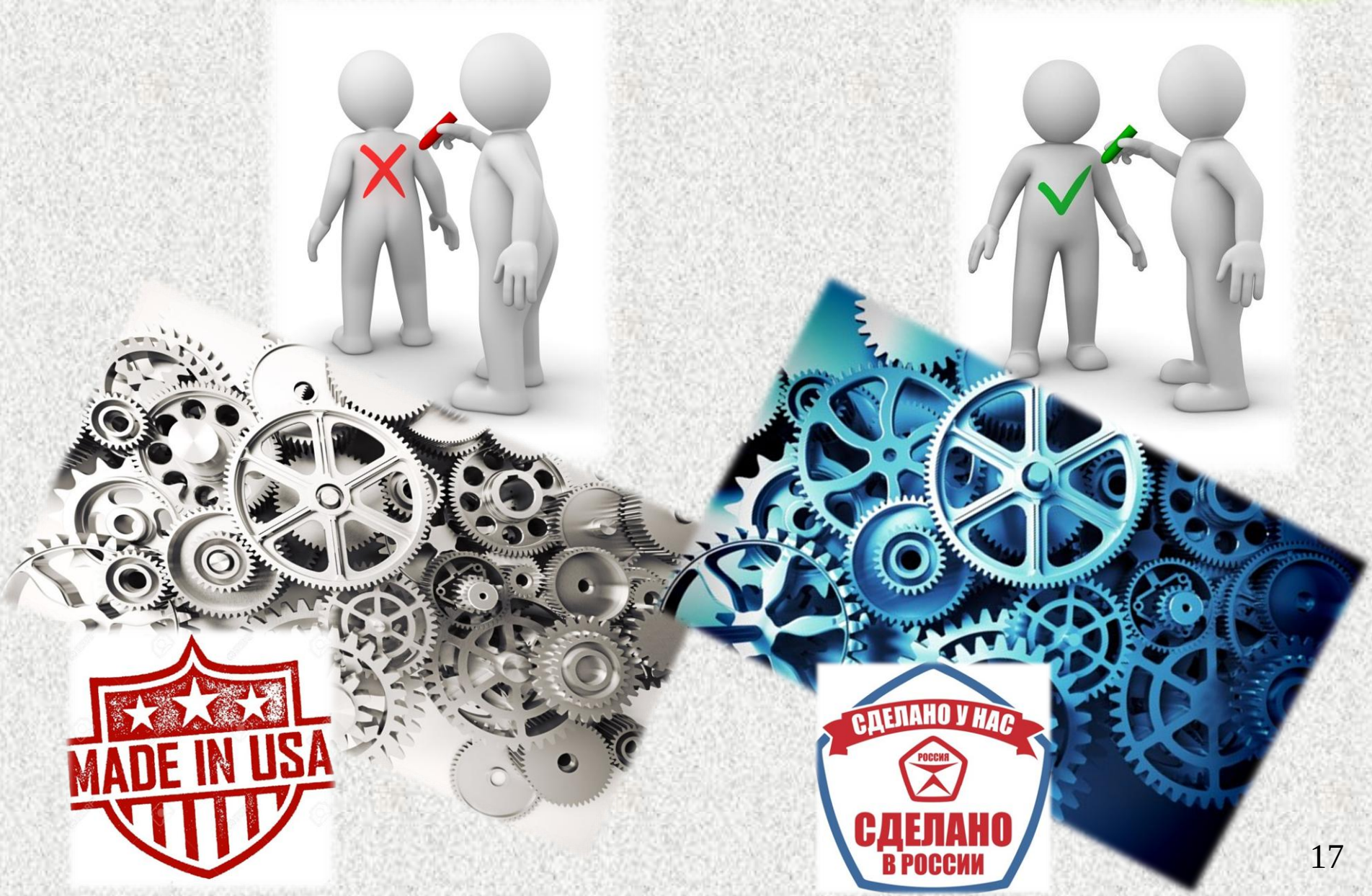
Технические средства

Средства защиты информации

Программное обеспечение

Информационные технологии

Импортозамещение



Аутсорсинг

- **Повышение эффективности использования систем информационной безопасности.**
- **Уменьшение количества технических средств оснащения.**
- **Отсутствие необходимости содержания дорогостоящих специалистов.**
- **Снижение фонда заработной платы.**
- **Передача функций организации, имеющей опыт и специалистов.**

- **Проблема доверия к исполнителю работ.**
- **Вопрос актуальности применения для информационных систем ОГВ и ОМСУ.**

Типовой жизненный цикл информационной системы и системы защиты информации




Анализ требований к ИС (замысел)

Формирование требований по защите информации

Проектирование (разработка) ИС

Разработка системы защиты информации

Создание ИС (реализация требований)

Внедрение системы защиты информации

Тестирование ИС (испытания)

Аттестация по требованиям безопасности информации

Ввод в эксплуатацию

Ввод в эксплуатацию

Эксплуатация

Эксплуатация (периодический (ежегодный) контроль соответствия)

Вывод из эксплуатации (модернизация)

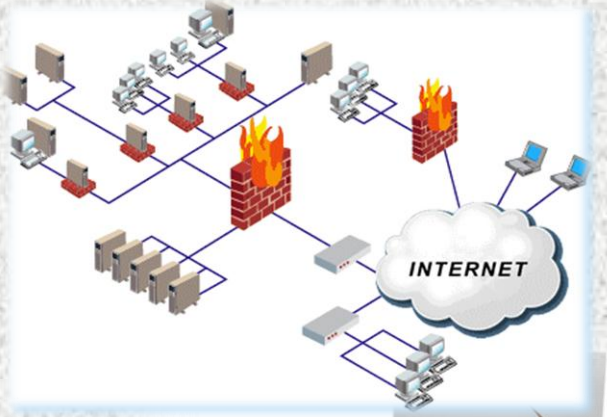
Вывод из эксплуатации (согласование изменений при модернизации)



Сопровождение (контроль и поддержка) на всех стадиях жизненного цикла

Исключение из обращения избыточной информации, правильное категорирование информации, своевременная инвентаризация информационных ресурсов

Квалификация специалистов по технической защите конфиденциальной информации



Приказ Минздравсоцразвития России от 22.04.2009 № 205

«Единый квалификационный справочник должностей руководителей, специалистов и служащих, раздел «Квалификационные характеристики должностей руководителей и специалистов по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию техническим разведкам и технической защите информации»

Приказы Минтруда России «Об утверждении профессиональных стандартов»

ОТ 15.09.2016 N 522Н

"СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ СИСТЕМАХ" (ЗАРЕГИСТРИРОВАНО В МИНЮСТЕ РОССИИ 28.09.2016 N 43857)

ОТ 01.11.2016 N 598Н

"СПЕЦИАЛИСТ ПО БЕЗОПАСНОСТИ КОМПЬЮТЕРНЫХ СИСТЕМ И СЕТЕЙ" (ЗАРЕГИСТРИРОВАНО В МИНЮСТЕ РОССИИ 28.11.2016 N 44464)

ОТ 01.11.2016 N 599Н

"СПЕЦИАЛИСТ ПО ТЕХНИЧЕСКОЙ ЗАЩИТЕ ИНФОРМАЦИИ" (ЗАРЕГИСТРИРОВАНО В МИНЮСТЕ РОССИИ 25.11.2016 N 44443)

ОТ 03.11.2016 N 608Н

"СПЕЦИАЛИСТ ПО ЗАЩИТЕ ИНФОРМАЦИИ В ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМАХ И СЕТЯХ" (ЗАРЕГИСТРИРОВАНО В МИНЮСТЕ РОССИИ 25.11.2016 N 44449)

Законодательство в области технической защиты информации

Федеральный закон Российской Федерации

№ 149-ФЗ
от 27.07.2006

Федеральный закон Российской Федерации

№ 152-ФЗ
от 27.07.2006

Федеральный закон Российской Федерации

№ 98-ФЗ
от 29.07.2004

Федеральный закон Российской Федерации

№ 79-ФЗ
от 27.07.2004

Трудовой кодекс Российской Федерации
(№ 197-ФЗ
от 30.12.2001)

Гл.14 «Защита ПДн работников»

Нормативно-правовые акты Президента и Правительства Российской Федерации

Указ Президента Российской Федерации

от 17.03.2008 № 351

Указ Президента Российской Федерации

от 06.03.1997 № 188

Постановление Правительства Российской Федерации

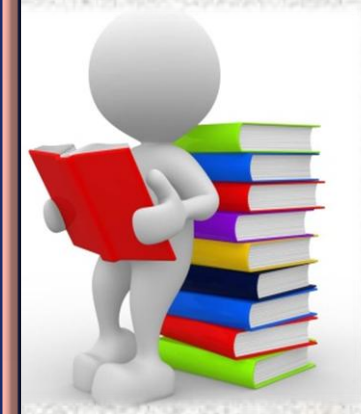
от 03.11.1994 № 1233

Постановление Правительства Российской Федерации

от 15.05.2010 № 330

Постановление Правительства Российской Федерации

от 01.11.2012 № 1119



Руководящие и нормативно-методические документы ФСТЭК России и национальные стандарты

«Сборник Руководящих документов по защите информации от несанкциони-рованного доступа» 1998	«Положение по аттестации объектов информатизации по требованиям безопасности информации» 25.11.1994	«СТР-К», утвержденные приказом Гостехкомиссии России от 30.08.2002 № 282	Приказ ФСТЭК России от 11.02.2013 № 17	Приказ ФСТЭК России от 18.02.2013 № 21
ГОСТ Р 51624–2006	ГОСТ 51583-2014	ГОСТ РО 0043-003-2012	ГОСТ РО 0043-004-2013	

Оптимизация затрат на техническую защиту конфиденциальной информации

- Разработка «Модели угроз безопасности информации».
- Использование сертифицированных средств защиты информации только для нейтрализации актуальных угроз безопасности информации.
- Применение компенсирующих организационные и/или технические мер защиты.
- Сегментирование информационной системы.
- Импортозамещение.
- Аутсорсинг.
- Исключение из обращения избыточной информации, правильное категорирование информации, своевременная инвентаризация информационных ресурсов.

Благодарю за внимание!

Начальник управления информационной безопасности акционерного общества «Гринатом»

Ершов Сергей Викторович

115230, Москва, 1-й Нагатинский проезд, д. 10, стр. 1

+7 (499) 949-49-19, доб. 3833

+7 (916) 265-00-51

www.greenatom.ru