# Информационная безопасность

#### Понятие информации, информационной системы

Информация – отражение реального мира, выражающееся в виде сигналов, знаков.

**Информационная система** — взаимосвязанная совокупность **средств, методов и персонала**, используемая для хранения, обработки и выдачи информации в интересах достижения поставленной цели.

#### Общие сведения о защите информации

«Информационная безопасность — это свойство сетей связи общего пользования противостоять возможности реализации нарушителем угрозы информационной безопасности».

#### Субъекты информационных отношений

владельцы и пользователи информации и поддерживающей инфраструктуры.

#### Поддерживающая инфраструктура

средства вычислительной техники, помещения, системы электро-, водо- и теплоснабжения, кондиционеры, средства коммуникаций и обслуживающий персонал

#### Защита информации

комплекс правовых, организационных и технических мероприятий и действий по предотвращению угроз информационной безопасности и устранению их последствий в процессе сбора, хранения, обработки и передачи информации в информационных системах

**Цель защиты информации -** уменьшение размеров ущерба до допустимых значений

#### Концепция Информационной Безопасности

- Что защищать?

- От чего (кого) защищать?

- Как защищать?

#### Основные составляющие информационной безопасности

**Confidentiality**— «конфиденциальность» — свойство информации быть недоступной или закрытой для неавторизованных лиц, сущностей или процессов;

**Integrity** с англ. — «**целостность**» — свойство сохранения правильности и полноты активов (статическая, динамическая);

**Availability** — «доступность» — свойство быть доступным и готовым к использованию по запросу авторизованного субъекта

Нарушение любой из трех составляющих приводит к нарушению информационной безопасности в целом.

#### Объекты защиты

- Все виды информационных ресурсов
- Права граждан, юридических лиц и государства
- Система формирования, распространения и использования информации
- Система формирования общественного сознания

## Правовые основы информационной безопасности общества.

Конституция РФ Стратегия национальной безопасности РФ

Федеральные законы Указы Президента РФ Постановления Правительства РФ Межведомственные руководящие документы и стандарты

## Федеральные органы, регулирующие деятельность в сфере обработки ПДн

Роскомнадзор

ФСТЭК России

ФСБ России

## Федеральный закон 149-Ф3 "Об информации, информационных технологиях и о защите информации" 27 июля 2006 г.

Закон регулирует отношения, возникающие при:

- осуществлении права на поиск, получение, передачу, производство и распространение информации
- применении информационных технологий
- обеспечении защиты информации.

Ф3-149 "Об информации, информационных технологиях и о защите информации" создает правовую основу информационного обмена в РФ и определяет права и обязанности его субъектов.

принципы правового регулирования отношений в сфере информации, информационных технологий и защиты информации

категории информации в зависимости от порядка ее предоставления или распространения

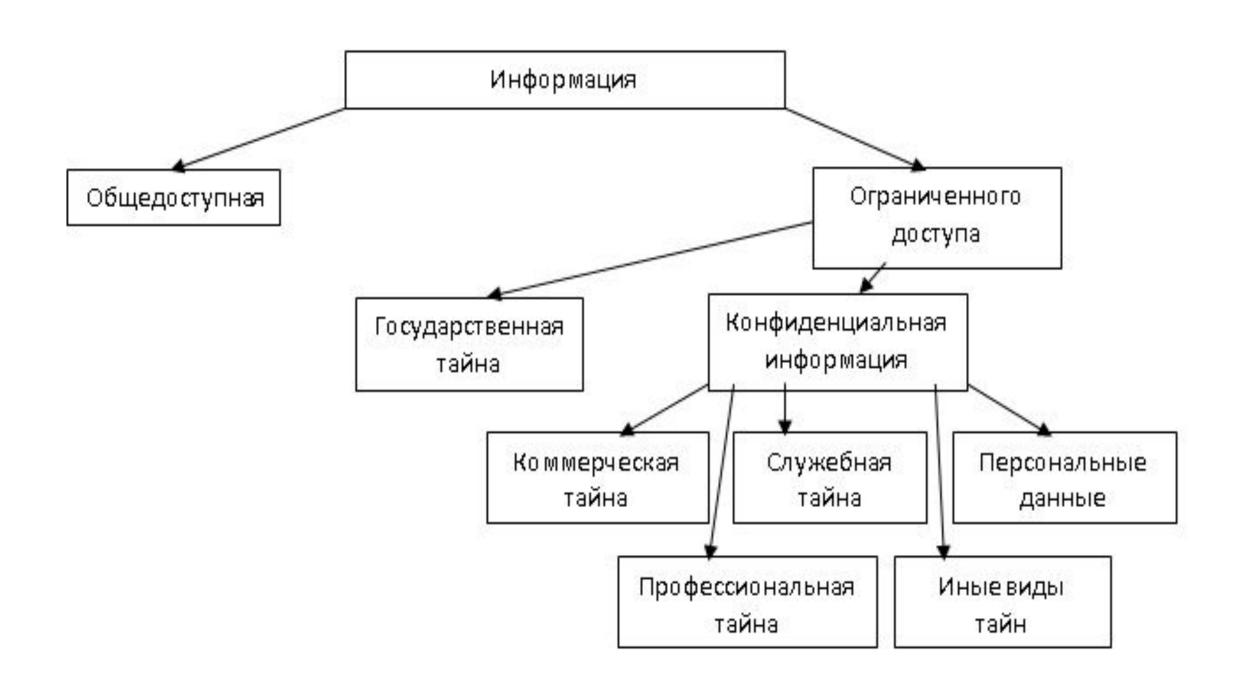
права и обязанности обладателя информации (оператора)

Порядок отнесения информационных систем (ИС) к муниципальным, государственным и иным ИС

Нельзя собирать и распространять информацию о жизни человека **без его согласия**.

Все информационные технологии равнозначны.

- Есть информация, к которой нельзя ограничивать доступ
- Некоторую информацию распространять запрещено
- Обязательность защиты информации
- Реестр запрещенных сайтов.
- Блокировка/разблокировка сайтов



#### Органы защиты государственной тайны

- Межведомственная комиссия по защите государственной тайны;
- Федеральные органы исполнительной власти, уполномоченные в области:
- обеспечения безопасности Федеральная служба по техническому и экспортному контролю (ФСТЭК);
- обороны Министерство обороны
- внешней разведки ФСБ
- противодействия техническим разведкам и технической защиты информации ФСТЭК;
- другие органы.

#### Конфиденциальная информация

Указ Президента РФ №188 от 06.03.1977 «Перечень сведений конфиденциального характера

ПДн

Тайна следствия и судопроизводства Служебные сведения Профессиональная тайна Коммерческая тайна «Ноу Хау» личные делах осужденных

### **Требования о защите информации, не составляющей** государственную тайну

Приказ ФСТЭК России от 11 февраля 2013 г. № 17 «Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах».

#### Объекты защиты

Информация, содержащаяся в ИС, технические, общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации.

**CIA** (Confidentiality- Integrity – Availability)

#### Этапы работ по обеспечению ИБ

- 1. Формирование требований к защите информации
- 2. Разработка системы защиты
- 3. Внедрение системы защиты
- 4. Аттестация ИС и ввод ее в действие
- 5. Обеспечение защиты в процессе эксплуатации
- 6. Обеспечение защиты при выводе из эксплуатации.

#### Формирование требований к защите информации

**Класс защищенности** определяет уровень защищенности информации. Классов три: К1, К2 и К3. Самый низкий класс – третий (К3), самый высокий – первый(К1).

**Уровень значимости** определяется степенью возможного ущерба от нарушения конфиденциальности, целостности или доступности информации. Может быть: высоким (УЗ 1), средним (УЗ 2) и низким (УЗ 3).

#### Разработка и внедрение системы защиты

- установка и настройка СЗ;
- разработка документации
- внедрение организационных мер защиты информации;
- предварительные испытания;
- опытная эксплуатация;
- анализ уязвимостей и принятие мер защиты информации по их устранению;
- приемочные испытания

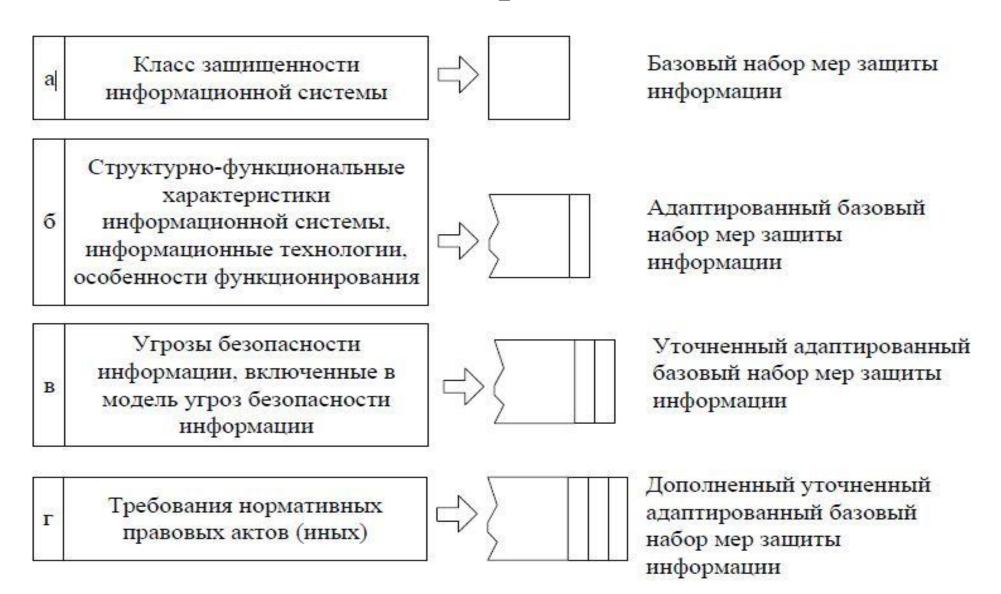
## **Аттестация и ввод в** действие

## Обеспечение защиты в процессе эксплуатации и выводе из эксплуатации

### Требования к мерам защиты информации, содержащейся в ИС

- идентификацию и аутентификацию;
- управление доступом;
- ограничение программной среды;
- защиту носителей информации;
- регистрацию событий безопасности;
- антивирусную защиту;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности информации;
- целостность информационной системы и информации;
- доступность информации;
- защиту среды виртуализации;
- защиту технических средств;
- защиту информационной системы, ее средств, систем связи и передачи данных.

## Общий порядок действий по выбору мер защиты информации для их реализации



Условное обозначени е и номер меры	Меры защиты информации в информационных системах	Классы защищенности информационн ой системы							
		3	2	1					
I. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)									
ИАФ.1	Идентификация и аутентификация пользователей, являющихся работниками оператора	+	+	+					
ИАФ.2	Идентификация и аутентификация устройств, в том числе стационарных, мобильных и портативных		+	+					

#### Группировка мер защиты по назначению

- І. Идентификация и аутентификация субъектов доступа и объектов доступа (ИАФ)
- II. Управление доступом субъектов доступа к объектам доступа (УПД)
- III. Ограничение программной среды (ОПС)
- IV. Защита машинных носителей информации (ЗНИ)
- V. Регистрация событий безопасности (РСБ)
- VI. Антивирусная защита (AB3)
- VII. Обнаружение вторжений (COB)
- VIII. Контроль (анализ) защищенности информации (AH3)
- ІХ. Обеспечение целостности информационной системы и информации (ОЦЛ)
  - Х. Обеспечение доступности информации (ОДТ)
- XI. Защита среды виртуализации (3CB)
- XII. Защита технических средств (3TC)
- XIII. Защита информационной системы, ее средств, систем связи и передачи данных (ЗИС)

Мера защиты информации	Класс защищенности ИС					
	К4	К3	К2	K1		
3НИ.1	+	+	+	+		
Усиление ЗНИ.1			1a	1a, 16		

#### ПЕРСОНАЛЬНЫЕ ДАННЫЕ.

Ф3-152 «Закон о Персональных Данных».

#### Цель закона:

- 1. Обеспечение защиты прав и свобод человека и гражданина при обработке его персональных данных
- 2. В т.ч. защиты прав на неприкосновенность частной жизни, личную и семейную тайну.

#### Обработка ПДн

- сбор
- запись
- систематизацию
- накопление
- хранение
- уточнение (обновление, изменение)
- извлечение
- использование
- передачу (распространение, предоставление, доступ)
- обезличивание
- блокирование
- удаление
- уничтожение ПД

#### Категории ПДн

Постановление Правительства №119 от 01.11.2012

- общедоступные сведения
- специальные категории
- биометрические параметры
- иные

#### Права субъекта ПДн и Оператора

#### Обязанности оператора

- 1. Перед сбором и обработкой ПДн необходимо согласие их владельца.
- 2. Для защиты информации закон обязывает собирать ПДн только с конкретной целью.
- 3. ПДн подлежат удалению по требованию владельца.
- 4. Хранение и обработка баз ПДн должно осуществляться на территории Российской Федерации.
- 5. ПДн не подлежат разглашению и требуют защиты.

#### Требования к защите ПДн

Постановление Правительства РФ от 1.11.20212г. № 1119 «Об утверждении требований к защите ПД при их обработке в информационных системах ПД»

#### Основные положения постановления

Требования к защите ПДн и уровни защищенности

Организационные и (или) технические меры, определенные с учетом актуальных угроз безопасности

Выбор средств защиты

# Классификация ИС по виду обрабатываемых ПД

Специальные категории ПДн Биометрические ПДн Общедоступные ПДн Иные ПДН

ПДн сотрудников ПДн НЕ сотрудников

## Класс защищенности ИС

Класс защищенности (К) = [уровень значимости информации; масштаб системы].

Устанавливаются три класса защищенности информационной системы, определяющие уровни защищенности содержащейся в ней информации. Самый низкий класс – третий (К3), самый высокий – первый(К1)

# Уровень значимости информации

Уровень значимости информации определяется степенью возможного ущерба от нарушения, целостности или доступности информации.

УЗ (УЗ 1 УЗ 2 УЗ 3) = [(конфиденциальность, степень ущерба) (целостность, степень ущерба) (доступность, степень ущерба)],

# Степень возможного ущерба

Высокая Средняя Низкая

УЗ 1 УЗ 2 УЗ 3

#### Масштаб ИС

Федеральный

Региональный

Объектовый

## Класс защищенности информационной системы

Уровень	Масштаб информационной системы						
<b>значимости</b> информации	Федеральный	ий Региональный Объектов					
УЗ 1	К1	К1	К1				
УЗ 2	К1	К2	К2				
УЗ 3	К2	К3	К3				

# УРОВЕНЬ ЗАЩИЩЕННОСТИ ПДН

При определении уровня защищенности ПДн учитываются

- А) категория обрабатываемых ПД
- Б) вид обработки по форме отношений
- В) количество субъектов
- Г) типы угроз.

Самым высоким уровнем защищенности является первый – УЗ1, а самым низким – четвертый – УЗ4

## Угрозы информационной безопасности

**Информационная безопасность** - это защищенность информации и поддерживающей ее инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, чреватых нанесением ущерба владельцам или пользователям информации и поддерживающей инфраструктуры

Триада CIA (Confidentiality- Integrity – Availability)

Нарушение любой из трех составляющих приводит к нарушению информационной безопасности в целом.

# Классификация угроз ИБ

- 1. По природе возникновения
- 2. По степени преднамеренности проявления
- 3. По источнику угроз
- 4. По положению источника угроз
- 5. По степени зависимости от активности ИС.
- 6. По степени воздействия на ИС
- 7. По этапам доступа пользователей или программ к ресурсам
- 8. По месту расположения информации

# Угрозы безопасности ПД, актуальные угрозы безопасности ПД

Угрозы безопасности

Актуальные угрозы

# Типы угроз

1-го типа

2-го типа

3-го типа

# Уровни защищенности ПДн

Тип ИСПДн			Тип	Тип актуальных угроз				
	категории субъектов			2 тип	3 тип			
	Не сотрудников	Более 100 000	У31	У31	У3 2			
550000	3557.555	Менее чем 100 000	У3 1	У3 2	У3 3			
испдн-с	Сотрудников	Более 100 000	У3 1	У3 2	У3 3			
		Менее чем 100 000	УЗ 1	У32	У3 3			
ИСПДн-Б	Не сотрудников	Более 100 000	У3 1	У3 2	УЗ 3			
		Менее чем 100 000	У31	У32	У3 3			
	Сотрудников	Более 100 000	У31	У3 2	У3 3			
		Менее чем 100 000	У31	У3 2	У3 3			
ИСПДн-И	Не сотрудников	Более 100 000	У3 1	У32	У3 3			
aparta (orași de la companio)		Менее чем 100 000	У31	У3 3	У3 4			
	Сотрудников	Более 100 000	У31	У3 3	У3 4			
		Менее чем 100 000	У3 1	У33	уз 4			
ИСПДн-О	Не сотрудников	Более 100 000	У3 2	У32	У3 4			
DOMESTICAL SUR	DOMAINS OF THE PARTY OF THE PARTY OF THE	Менее чем 100 000	У3 2	У3 3	У3 4			
	Сотрудников	Более 100 000	У3 2	У33	У34			
	3838	Менее чем 100 000	У3 2	У3 3	У3 4			

# Меры по обеспечению безопасности

- идентификация и аутентификация
- управление доступом
- ограничение программной среды
- защита машинных носителей информации
- регистрация событий безопасности
- антивирусная защита
- обнаружение (предотвращение) вторжений
- контроль (анализ) защищенности персональных данных
- обеспечение целостности
- обеспечение доступности
- защита среды виртуализации
- защита технических средств
- защита информационной системы, ее средств, систем связи и передачи данных
- выявление инцидентов и реагирование на них
- управление конфигурацией информационной системы и системы защиты персональных данных.

Условное	Содержание мер по обеспечению безопасности	Уровни защищенности			ости
обозначение	персональных данных	персоп	персональных данных		ных
и номер		4	3	2	1
меры		_			
I. Идентифика	ция и аутентификация субъектов доступа и объектов	в достуг	па (ИА	Φ)	
ИАФ.1	Идентификация и аутентификация	+	+	+	+
	пользователей, являющихся работниками				
	оператора				
ИАФ.2	Идентификация и аутентификация устройств, в			+	+
	том числе стационарных, мобильных и				
	портативных				
ИАФ.3	Управление идентификаторами, в том числе	+	+	+	+
	создание, присвоение, уничтожение				
	идентификаторов				

# Средства защиты информации

Средство защиты информации – техническое, программное, программно-техническое средство, вещество и (или) материал, используемые для защиты информации (ГОСТ Р 50922-2006)

# Классификация средств защиты информации



# Уровни доверия к средствам технической защиты информации и средствам обеспечения безопасности

Уровни, характеризующие безопасность применения средств для обработки и защиты информации

Устанавливается 6 уровней доверия.

Самый низкий уровень – шестой, самый высокий – первый

Уровень доверия ->	6	5	4	3, 2, 1
ГИС класса 3,4; АСУ				
класса 3; ИСПДн класса				
3,4				
ГИС класса 2; АСУ класса				
2; ИСПДн класса 2				
ГИС класса 1; АСУ класса				
1; ИСПДн класса 1;				
ИСПДн класса 1, ГИС,				
ИСОП класса 2				
ИС (гос. тайна)				

# Использование средств защиты информации в ИС для обеспечения **уровня защищенности** (ФСТЭК Приказ №21

Пример:

а) для обеспечения 1 и 2 уровней защищенности ПД применяются:

СВТ не ниже 5 класса;

СОВ и САВ не ниже 4 класса;

<u>МЭ</u> не ниже 3 класса (угрозы 1-го или 2-го типов) не ниже 4 класса (угрозы 3-го)

#### Классы СВТ

Классификация СВТ по уровню защищенности от НСД (класс защищенности CBT)

CBT – совокупность программных и технических элементов систем обработки данных, способных функционировать самостоятельно или в составе других систем.

Устанавливается семь классов защищенности СВТ от НСД к информации.

Самый низкий класс – седьмой, самый высокий – первый.

Группа	1	2	2 3	
Класс	7	6,5	4, 3, 2	1

# Перечень минимально необходимых показателей по классам защищенности СВТ

Наименование показателя		Класс защищенности					
		5	4	3	2	1	
Дискреционный принцип контроля доступа	+	+	+	=	+	=	
Мандатный принцип контроля доступа		-	+	=	=	=	
Очистка памяти	-	+	+	+	=	=	
Изоляция модулей		-	+	=	+	=	
Маркировка документов	-	-	+	=	=	=	
Защита ввода и вывода на отчуждаемый физический носитель информации	-	-	+	=	=	=	
Сопоставление пользователя с устройством		-	+	=		=	
Идентификация и аутентификация	+	=	+	=	=	=	

Седьмой класс присваивают СВТ, к которым предъявлялись требования по защите от НСД к информации, но при оценке защищенность СВТ оказалась ниже уровня требований шестого класса

# Классы систем обнаружения вторжений (СОВ)

Системы для обнаружения вторжений — программно-аппаратные решения, детектирующие попытки нелегального доступа в ИС. (IDS – Intruson Detection System)

Системы для предотвращения вторжений — программно-аппаратные решения, предотвращающие попытки нелегального доступа в ИС. (IPS – Intruson Prevention System)

Класс защиты СОВ ->	6	5	4	3, 2, 1
ИСПДн класса 3,4				
ИСПДн класса 2				
ИСПДн класса 1, ГИС, ИСОП класса 2				
ИС (гос. тайна)				

#### Идентификатор профиля защиты СОВ

## ИТ.СОВ. ҮХ.ПЗ

- Ү СОВ уровня сети (С) или уровня узла(У)
- X класс защиты COB (1-6)

# Классы средств антивирусной защиты (САВ)

Средство антивирусной защиты — программное средство, реализующее функции обнаружения компьютерных программ либо иной компьютерной информации, предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты информации, а также реагирования на обнаружение этих программ и информации

Класс защиты САВ ->	6	5	4	3, 2, 1
ИСПДн класса 3,4				
ИСПДн класса 2				
ИСПДн класса 1, ГИС, ИСОП класса 2				
ИС (гос. тайна)				



#### Идентификатор профиля защиты САВ

#### ИТ.САВ.ҮХ.ПЗ

где

Y – тип CAB (A- $\Gamma$ )

X - класс защиты CAB (1-6)

#### Типы САВ:

Тип A - предназначены для централизованного администрирования САВ, установленных на компонентах ИС (серверы, APM)

Тип Б – предназначены для применения на серверах ИС

Тип В - предназначены для применения в АРМ ИС

Тип Г - предназначены для применения в автономных АРМ



# Классы межсетевых экранов

Межсетевые экраны - программные и программно-технические средства, реализующие функции контроля и фильтрации в соответствии с заданными правилами проходящих через них информационных потоков и используемые в целях обеспечения защиты (некриптографическими методами) информации

Установлено 6 классов защиты межсетевых экранов. Самый низкий класс — шестой, самый высокий — первый.

# Типы межсетевых экранов

```
тип «А» – межсетевой экран уровня сети
```

тип «Б» – межсетевой экран уровня логических границ сети

тип «В» – межсетевой экран уровня узла

тип « $\Gamma$ » — межсетевой экран уровня веб-сервера

тип «Д» – межсетевой экран уровня промышленной сети

Класс защиты МЭ ->	6	5	4	3, 2, 1
ГИС класса 3,4; АСУ ТП				
класса 3; ИСПДн				
класса 3,4				
ГИС класса 2; АСУ ТП				
класса 2; ИСПДн класса				
2				
ГИС класса 1; АСУ ТП				
класса 1; ИСПДн класса				
1; ИСПДн класса 1,				
ГИС, ИСОП класса 2				
ИС (гос. тайна)				

#### Идентификатор профиля защиты МЭ

#### ит.мэ.үх.пз

где

Y – тип МЭ (A-Д)

X - класс защиты MЭ (1-6)

# Уровни контроля отсутствия недекларированных возможностей ПО

Недекларированные возможности — функциональные возможности ПО, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение конфиденциальности, доступности или целостности обрабатываемой информации

Установлено 4 уровня контроля отсутствия недекларированных возможностей.

Самый высокий уровень контроля - первый, самый низкий – четвертый

Уровень контроля ->	1	2	3	4
ПО, используемое при защите				
информации, отнесенной к гос.				
тайне; с грифом «ОВ»				
ПО, используемое при защите				
информации, отнесенной к гос.				
тайне; с грифом «СС»				
ПО, используемое при защите				
информации, отнесенной к гос.				
тайне; с грифом «С»				
Защита информации с грифом				
«Конфиденциально»				

# Требования к средствам доверенной загрузки (СДЗ)

Средства доверенной загрузки — программные и программнотехнические средства, используемые в целях защиты информации и реализующие функции по предотвращению НСД к программным и (или) техническим ресурсам СВТ на этапе загрузки.

- средства доверенной загрузки уровня базовой системы ввода-вывода (УБ)
- средства доверенной загрузки уровня платы расширения (ПР)
- средства доверенной загрузки уровня загрузочной записи (33)

Установлено шесть классов защиты средств доверенной загрузки.Самый низкий класс – шестой, самый высокий – первый

Класс защиты СДЗ Система		6	5	4	3,2,1
негосударственные ИС без ПДн и ГТ					
ГИС 4 класса					
ГИС 3 класса	без сетевого взаимодействия				
	при сетевом взаимодействии				
ГИС 2 класса					
ГИС 1 класса					
ИСПДн 4 уровня					
испл. 2	без сетевого взаимодействия и при актуальности угроз 3-го типа				
ИСПДн 3 уровня	при сетевом взаимодействии и при актуальности угроз 2-го типа				
ИСПДн 2 уровня					
ИСПДн 1 уровня					
ИСОП II класса					
ГТ					

#### Идентификатор профиля защиты СДЗ

#### ИТ.СДЗ.ҮХ.ПЗ

где

Y – тип СДЗ (УБ, ПР, 33)

X - класс защиты СДЗ(1-6)

## Требования безопасности информации к операционным системам

Типы операционных систем:

тип «А» - операционная система общего назначения

тип «Б» - встраиваемая операционная система

тип «В» - операционная система реального времени

Выделяют шесть классов защиты операционных систем.

Самый низкий класс – шестой, самый высокий – первый

Класс защиты ОС ->	6	5	4	3, 2, 1
ГИС класса 3,4; АСУ ТП класса 3; ИСПДн класса 3,4				
ГИС класса 2; АСУ ТП класса 2; ИСПДн класса 2				
ГИС класса 1; АСУ ТП класса 1; ИСПДн класса 1; ИСПДн класса 1, ГИС, ИСОП класса 2				
ИС (гос. тайна)				

#### Идентификатор профиля защиты операционных систем

#### ИТ.ОС.ҮХ.ПЗ

где

Y - тип OC (A, Б, B)

X - класс защиты OC (1-6)

# Требования к средствам контроля съемных машинных носителей информации (СКН)

Машинный носитель информации — любое техническое устройство, предназначенное для фиксации, хранения, накопления и передачи компьютерной информации.

Съемный машинный носитель – носитель не находящийся в составе СВТ.

## Типы средств контроля съемных машинных носителей информации

- средства контроля подключения (П);
- средства контроля отчуждения (Н).

Выделяют шесть классов защиты средств контроля съемных машинных носителей информации.

Самый низкий класс – шестой, самый высокий – первый.

Система	Класс защиты СКН	6	5	4	3,2,1
негосударственны	е ИС без ПДн и ГТ				
ГИС 4 класса					
ГИС 3 класса	без сетевого взаимодействия				
	при сетевом взаимодействии				
ГИС 2 класса					
ГИС 1 класса					
ИСПДн 3 уровня					
ГИС 3 класса ИСПДн 3 уровня	без сетевого взаимодействия и при актуальности угроз 3-го типа				
	при сетевом взаимодействии и при актуальности угроз 2-го типа				
ИСПДн 2 уровня					
ИСПДн 1 уровня					
ИСОП II класса					
ГТ					

#### Идентификатор профиля защиты операционных систем

#### ИТ.СКН.ҮХ.ПЗ

где

Y – тип СКН (П,Н)

X - класс защиты СКН (1-6)

### Криптографические средства защиты

Приказ ФСБ России от 10 июля 2014 г. N 378 "Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности ПД при их обработке в информационных системах ПД с использованием средств криптографической защиты информации ....»

Документ определяет состав и содержание организационных и технических мер по обеспечению безопасности ПДн при их обработке в ИСПДн с использованием СКЗИ, для каждого уровня защищенности ПДн (УЗ1 – УЗ4).

## Уровни защищенности Персональных данных

(y31 - y34).

#### Классы СКЗИ

1	KC1	Возможность противостоять атакам, проводимым из-за пределов контролируемой зоны	
		(внешний нарушитель, без помощников внутри системы)	
2	KC2	Противостояния атакам класса К1, а также в пределах контролируемой зоны (внутренний нарушитель, не имеющий доступа к СКЗИ)	
	ICCO		
3	КС3	Возможность противостоять атакам при наличии физического доступа к СВТ с	
		установленными криптографическими СЗИ (внутренний нарушитель, являющийся	
		пользователем СКЗИ)	
4	КВ1	Возможность противостоять атакам, при создании которых участвовали специалисты в	
		области разработки и анализа СКЗИ (привлечение сторонних ресурсов, например,	
		специалистов по СКЗИ)	
5	КВ2	Противостояние доступа к исходным текстам прикладного, программного ПО,	
		работающего с функциями ПО СКЗИ. (нарушитель, за действиями которого стоит	
		институт или лаборатория, работающая в области изучения и разработки СКЗИ)	
6	KA1	Противостояние возможности проникновения к любому аппаратному компоненту СКЗИ,	
		а также среде функционирования (специальные службы государства)	

Для построения адекватной системы защиты, обеспечивающую безопасность (ПДн) необходимо определить требования к системе и методы реализации этих методов. Для любых информационных систем, так или иначе подлежащих защите в соответствие с законодательством необходима разработка модели угроз.

#### Модель угроз по ФСТЭК

Модель угроз безопасности информации должна содержать описание:

- ИС
- структурно-функциональных характеристики ИС
- угроз безопасности информации
- модели нарушителя
- возможных уязвимостей ИС
- способов реализации угроз
- последствий от нарушения свойств безопасности информации.

#### Базовая модель угроз безопасности

Содержит перечень угроз безопасности персональных данных

Приводится классификация угроз

Рассматриваются угрозы утечки информации по техническим каналам

#### Задачи, решаемые с применением модели угроз

- разработка частных моделей угроз безопасности ПДн в конкретных ИС
- анализ защищенности ИСПДн
- разработка системы защиты ПДн
- проведение мероприятий, обеспечивающих защиту ПДн
- контроль обеспечения уровня защищенности.

#### Источники угроз НСД в ИСПДн

Нарушитель (внешний/внутренний)

Носитель вредоносной программы

Аппаратная закладка

#### Категории внутренних нарушителей

в зависимости от способов доступа и категорий полномочий

#### Уязвимость ИСПДн



# Характеристика угроз непосредственного доступа в операционную среду

Первая группа включает в себя угрозы, реализуемые в ходе загрузки ОС.

Вторая группа - угрозы, реализуемые после загрузки операционной среды.

Третья группа включает в себя угрозы, реализация которых определяется тем, какая из прикладных программ запускается пользователем

# Угрозы безопасности ПД, реализуемых с использованием протоколов межсетевого взаимодействия

Анализ сетевого трафика
Сканирование сети
Угроза выявления пароля
Подмена доверенного объекта
Навязывание ложного маршрута сети
Внедрение ложного объекта сети
Отказ в обслуживании

Удаленный запуск приложений



#### Воздействие с помощью вредоносных программ

- программные закладки;
- классические программные (компьютерные) вирусы;
- вредоносные программы, распространяющиеся по сети (сетевые черви);
- другие вредоносные программы, предназначенные для осуществления НСД.

Классификация типов ИСПДн в зависимости от структуры, режима обработка, разграничению прав доступа, местонахождению и подключению к сетям общего пользования

#### Методика оценки угроз безопасности информации

1. Методика применяется для определения угроз безопасности информации

2. Методика ориентирована на оценку антропогенных угроз безопасности информации, возникновение которых обусловлено действиями нарушителей

## Порядок оценки угроз безопасности информации

Исходные данные для оценки

#### Рекомендуемая структура модели угроз

- 1. Общие положения
- 2. Описание систем и сетей и их характеристика как объектов защиты
- 3. Возможные негативные последствия от реализации (возникновения) угроз безопасности информации
- 4. Возможные объекты воздействия угроз безопасности информации
- 5. Источники угроз безопасности информации
- 6. Способы реализации (возникновения) угроз безопасности информации
- 7. Актуальные угрозы безопасности информации

#### Разработка системы защиты

Внедрение системы защиты

#### Стадии создания системы защиты

- предпроектное обследование, разработка аналитического обоснования необходимости создания средств защиты информации
  - стадия проектирования разработка средств защиты
- ввод в действие СЗИ (опытная эксплуатация, приемо-сдаточные испытания и аттестация объекта)

#### Аттестация объектов информатизации

(ГОСТ РО 0043-003-2012 переиздание в марте 2013 г.) (ГОСТ РО 0043-004-2013)

#### Порядок проведения аттестации

- 1. Подача и рассмотрение заявки на аттестацию.
- 2. Предварительное ознакомление с аттестуемым объектом.
- 3. Разработка программы и методик аттестационных испытаний
- 4. Проведение испытаний
- 5. Оформление, регистрация и выдача сертификата соответствия

## Ввод в действие и эксплуатация аттестованных объектов

Ввод в действие и эксплуатация осуществляется после его аттестации