

# **ЧТО ИЗМЕНИЛОСЬ ПОСЛЕ ВЫХОДА ПРИКАЗА ФСТЭК РОССИИ № 58?**




**Центр безопасности информации**



# Действующая нормативная база

- Закон «О персональных данных» (статья 19)
- Положение об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных, Постановление правительства от 17.11.2007 № 781
- Порядок проведения классификации информационных систем персональных данных, Приказы ФСТЭК России, ФСБ России, Мининформсвязи России от 13.02.2008 № 55/86/20
- Базовая модель угроз безопасности ПДн при их обработке в информационных системах ПДн, ФСТЭК России, 2008
- Методика определения актуальных угроз безопасности ПДн при их обработке в информационных системах ПДн, ФСТЭК России, 2008
- Положение о методах и способах защиты информации в информационных системах персональных данных, утверждено приказом ФСТЭК России от 5 февраля 2010 г. № 58 (зарегистрирован в Минюсте РФ 19 февраля 2010 г., регистрационный № 16456)



# Методы и способы защиты информации в ИСПДн

Методы и способы  
защиты  
информации от  
несанкционирован  
ного доступа

Методы и способы  
защиты  
информации от  
утечки по  
техническим  
каналам



## Функции, реализуемые в системе защиты ПДн методами и способами защиты информации от НСД:

- управление доступом;
- регистрация и учет;
- обеспечение целостности;
- анализ защищенности;
- обеспечение безопасности межсетевых взаимодействий;
- обнаружение вторжений;

# Методы и способы защиты информации в зависимости от класса ИСПДн

Режим обработки информации в ИСПДн	Однопользовательский			Многопользовательский					
Права доступа пользователей				Равные			Разные		
Класс ИСПДн	К3	К2	К1	К3	К2	К1	К3	К2	К1
Функции управления доступом, регистрации и учета, обеспечения целостности	ЗБ	ЗБ	ЗБ+	2Б	2Б	2Б+	1Д	1Д	1Г
	Применение СЗИ, сертифицированных на соответствие требованиям к показателям 5 класса по РД СВТ								
Контроль отсутствия НДВ ПО СЗИ	Необходимость определяется оператором		Соответствие 4 уровню контроля НДВ	Необходимость определяется оператором		Соответствие 4 уровню контроля НДВ	Необходимость определяется оператором		Соответствие 4 уровню контроля НДВ
Использование средств антивирусной защиты	Обязательно в ИСПДн, подключенных к ССОП и при использовании съемных носителей информации								
Защита ПДн от утечки за счет ПЭМИН		Соответствие стандартам по ЭМС и санитарным нормам	Аналогично СТР-К		Соответствие стандартам по ЭМС и санитарным нормам	Аналогично СТР-К		Соответствие стандартам по ЭМС и санитарным нормам	Аналогично СТР-К

# Методы и способы защиты информации в зависимости от класса ИСПДн

Режим обработки информации в ИСПДн		Однопользовательский			Многопользовательский					
					Равные			Разные		
Права доступа пользователей										
Класс ИСПДн		К3	К2	К1	К3	К2	К1	К3	К2	К1
Межсетевое взаимодействие	Распределенные ИСПДн 2 и 1 классов	Применение межсетевых экранов 4 класса в соответствии с РД МСЭ								
	При подключении к ССОП	Применение межсетевых экранов								
		4 класса		3 класса	4 класса		3 класса	4 класса		3 класса
	При получении общедоступной информации из ССОП	Применение систем обнаружения вторжений Применение средств и специальных комплексов анализа защищенности								
	При удаленном доступе через ССОП	Создание канала связи, обеспечивающего защиту передаваемой информации Проверка подлинности отправителя и целостности передаваемых данных Управление доступом к защищаемым персональным данным ИСПДн Использование атрибутов безопасности								
	При взаимодействии ИСПДн через ССОП	Создание канала связи, обеспечивающего защиту передаваемой информации Осуществление аутентификации взаимодействующих ИСПДн Проверка подлинности пользователей и целостности передаваемых данных								
При взаимодействии ИСПДн разных операторов через ССОП	Создание канала связи, обеспечивающего защиту передаваемой информации Осуществление аутентификации взаимодействующих ИСПДн Проверка подлинности пользователей и целостности передаваемых данных Предотвращение возможности отрицания факта отправки и получения ПДн									



**Выбор и реализация методов и способов  
защиты информации в ИСПДн может  
осуществляться:**

**Структурным подразделением или должностным  
лицом оператора**

**С привлечением организации, имеющей  
оформленную в установленном порядке  
лицензию на осуществление деятельности по  
технической защите конфиденциальной  
информации**



## Нужна ли лицензия оператору?

- **Указ Президента РФ № 188 от 6.03.97 :**  
ПДн включены в Перечень сведений конфиденциального характера.
- **Федеральный закон О персональных данных от 27.07.06 № 152-ФЗ**  
Статья 7. должна обеспечиваться конфиденциальность ПДн
- **Федеральный закон О лицензировании отдельных видов деятельности от 8.08.01 № 128-ФЗ**  
Деятельность по технической защите конфиденциальной информации отнесена к лицензируемой
- **Постановление Правительство Российской Федерации от 15.08.06 № 504**  
Под технической защитой конфиденциальной информации понимается комплекс мероприятий и (или) услуг по ее защите от несанкционированного доступа





## Обязательна ли сертификация СЗИ, применяемых в ИСПДн?

- **Постановление Правительства РФ от 17 ноября 2007 г. № 781**

Пункт 5 Положения об обеспечении безопасности ПДн при их обработке в ИСПДн:  
Средства защиты информации, применяемые в информационных системах, в установленном порядке проходят процедуру соответствия

- **Положение, утвержденное приказом № 58:**

Пункт 2.1. Методами и способами защиты информации от НСД являются:  
использование средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия.

- **Федеральный закон О техническом регулировании от 27.12.02 № 184-ФЗ**

Статья 5. Особенности оценки соответствия продукции (работ, услуг), используемой в целях защиты сведений, составляющих государственную тайну или относимых к охраняемой в соответствии с Законодательством Российской Федерации иной информации ограниченного доступа, устанавливаются Правительством Российской Федерации.

3 формы подтверждения соответствия:

- добровольная сертификация;
- обязательное декларирование соответствия;
- обязательная сертификация.

- В настоящее время действует только одна форма: **обязательная сертификация**, порядок проведения которой установлен постановлением Правительства РФ от 26 июня 1995 г. № 608 и приказом Председателя Гостехкомиссии России от 27 октября 1995 г. № 199.



## Обязательна ли аттестация ИСПДн?

- В соответствии с Положением, утвержденным **приказом Председателя Гостехкомиссии России от 27 октября 1995 г. №199** система сертификации средств защиты информации по требованиям безопасности информации включает в себя аттестацию объектов информатизации по требованиям безопасности информации.

То есть аттестация является формой оценки соответствия работ, услуг, выполненных в целях защиты сведений, относимых к охраняемой в соответствии с законодательством РФ информации ограниченного доступа.

- **СТР-К:**

Пункт 2.17 Объекты информатизации должны быть аттестованы по требованиям безопасности информации в соответствии с нормативными документами ФСТЭК России и требованиями настоящего документа.