



Информзащита  
Учебный центр



# Техническая защита Персональных данных

# Защита ПДн правовые основания



Конституция Российской Федерации

Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»

Постановление  
Правительства Российской Федерации  
от 1 ноября 2012 г. №1119

Постановление  
Правительства Российской Федерации  
от 6.07.2008 № 512

Постановление  
Правительства Российской Федерации  
от 15.09.2008 № 687

Постановление  
Правительства Российской Федерации  
от 17.11.2007 № 704

Постановление Правительства  
Российской Федерации  
от 21.03.2012 № 211

~~Приказ № 21 ФСТЭК России~~

~~Приказ ФСТЭК России от 19.05.2010 № 26 «Об утверждении требований к средствам защиты информации в системах, обеспечивающих функционирование сетей связи России»~~

~~Проект Приказа ФСБ~~

~~Методические документы ФСТЭК России~~

Методические документы ФСБ России

# БЕЗ использования средств автоматизации



Определяет требования к обработке ПДн, осуществляемой без использования средств автоматизации:

- ✓ обособления ПДн, собранных для разных целей, «для каждой категории ПДн должен использоваться отдельный материальный носитель» (п.5)
- ✓ уведомления лиц, обрабатывающих ПДн, о факте обработки ПДн, «а также об особенностях и правилах осуществления такой обработки» (п. 6)
- ✓ учета мест хранения ПДн «чтобы в отношении каждой категории ПДн можно было определить места хранения ПДн» (п. 13)
- ✓ учета лиц ведущих обработку ПДн «установить перечень лиц, осуществляющих обработку ПДн либо имеющих к ним доступ» (п. 13)
- ✓ перечень мер устанавливает оператор (п. 15)

# Требования к защите ПДн при их обработке в ИСПДн

4 уровня защищенности ПДн.

Требования для достижения соответствующего УЗ

Категория ПДн		Объем ПДн	Угрозы		
			1 типа	2 типа	3 типа
Спец. категория	НЕ сотрудники оператора	Более 100 000	1 уровень	1 уровень	2 уровень
		Менее 100 000	1 уровень	2 уровень	3 уровень
	Сотрудники оператора			1 уровень	2 уровень
Биометрические ПДн			1 уровень	2 уровень	3 уровень
Иные ПДн	НЕ сотрудники оператора	Более 100 000	1 уровень	2 уровень	3 уровень
		Менее 100 000	1 уровень	3 уровень	4 уровень
	Сотрудники оператора			1 уровень	3 уровень
Общедоступные	НЕ сотрудники оператора	Более 100 000	2 уровень	2 уровень	4 уровень
		Менее 100 000	2 уровень	3 уровень	4 уровень
	Сотрудники оператора			2 уровень	3 уровень

# Количество базовых мер безопасности

Уровень защищенности	Количество базовых мер безопасности
1	70
2	67
<b>3</b>	<b>41</b>
<b>4</b>	<b>27</b>



Общее количество мер по обеспечению безопасности персональных данных – **110**

# Выбор мер по защите ПДн

п. 9

Выбор мер по обеспечению безопасности персональных данных, подлежащих реализации в информационной системе в рамках системы защиты персональных данных, включает:

1. **определение** базового набора мер по обеспечению безопасности ПДн для установленного уровня защищенности (УЗ) ПДн;
2. **адаптация** базового набора ... с учетом:
  - ✓ структурно-функциональных характеристик информационной системы,
  - ✓ информационных технологий,
  - ✓ особенностей функционирования информационной системы (в том числе исключение из базового набора мер, непосредственно связанных с информационными технологиями....);
3. **уточнение** адаптированного базового набора мер ... с учетом не выбранных ранее мер, ... в результате чего определяются меры, направленные на нейтрализацию всех актуальных угроз безопасности;
4. **дополнение** уточненного адаптированного базового набора мер ... установленными иными нормативными правовыми актами в области обеспечения безопасности ПДн и защиты информации.

# Требования по сертификации



Ст. 19 ч .2. Обеспечение безопасности персональных данных достигается, в частности:

3) применением прошедших в установленном порядке процедуру оценки соответствия средств защиты информации;

ФЗ № 152 «О персональных данных»

4. Меры по обеспечению безопасности персональных данных реализуются в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных.
12. При использовании в информационных системах сертифицированных по требованиям безопасности информации средств защиты информации:

(Приказ ФСТЭК России от 18 февраля 2013 г. № 21)



# Требования к СЗИ в зависимости от уровня защищенности

	УЗ - 1	УЗ - 2	УЗ - 3	УЗ - 4
СВТ	5	5	5	6
СОВ	4	4	4 <sup>1</sup> / 5 <sup>2</sup>	5
Антивирус	4	4	4 <sup>1</sup> /5 <sup>2</sup>	5
МЭ	3 <sup>3</sup> / 4 <sup>2</sup>	3 <sup>3</sup> / 4 <sup>2</sup>	3 <sup>1</sup> /4 <sup>2</sup>	5
Контроль отсутствия НДВ.	4 уровень	4 уровень	4 уровень <sup>4</sup> /-	-

1. В случае актуальности угроз 2-го типа **или** взаимодействия ИСПДн с информационно-телекоммуникационными сетями международного информационного обмена.
2. В случае актуальности угроз 3-го типа **и** отсутствия взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.
3. в случае актуальности угроз 1-го или 2-го типов **или** взаимодействия информационной системы с информационно-телекоммуникационными сетями международного информационного обмена.
4. Если актуальны угрозы 2-го типа

п. 12 Приказ ФСТЭК России от 18 февраля 2013 г. № 21

# Методические документы ФСБ России



- ❖ «**Методические рекомендации** по обеспечению с помощью криптосредств безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств автоматизации»  
(утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/54-144)
- ❖ «**Типовые требования** по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных»  
(утверждены руководством 8 Центра ФСБ России 21.02.2008 № 149/6/6-622)

# Методические документы ФСБ



Методические рекомендации не распространяются на системы, где:

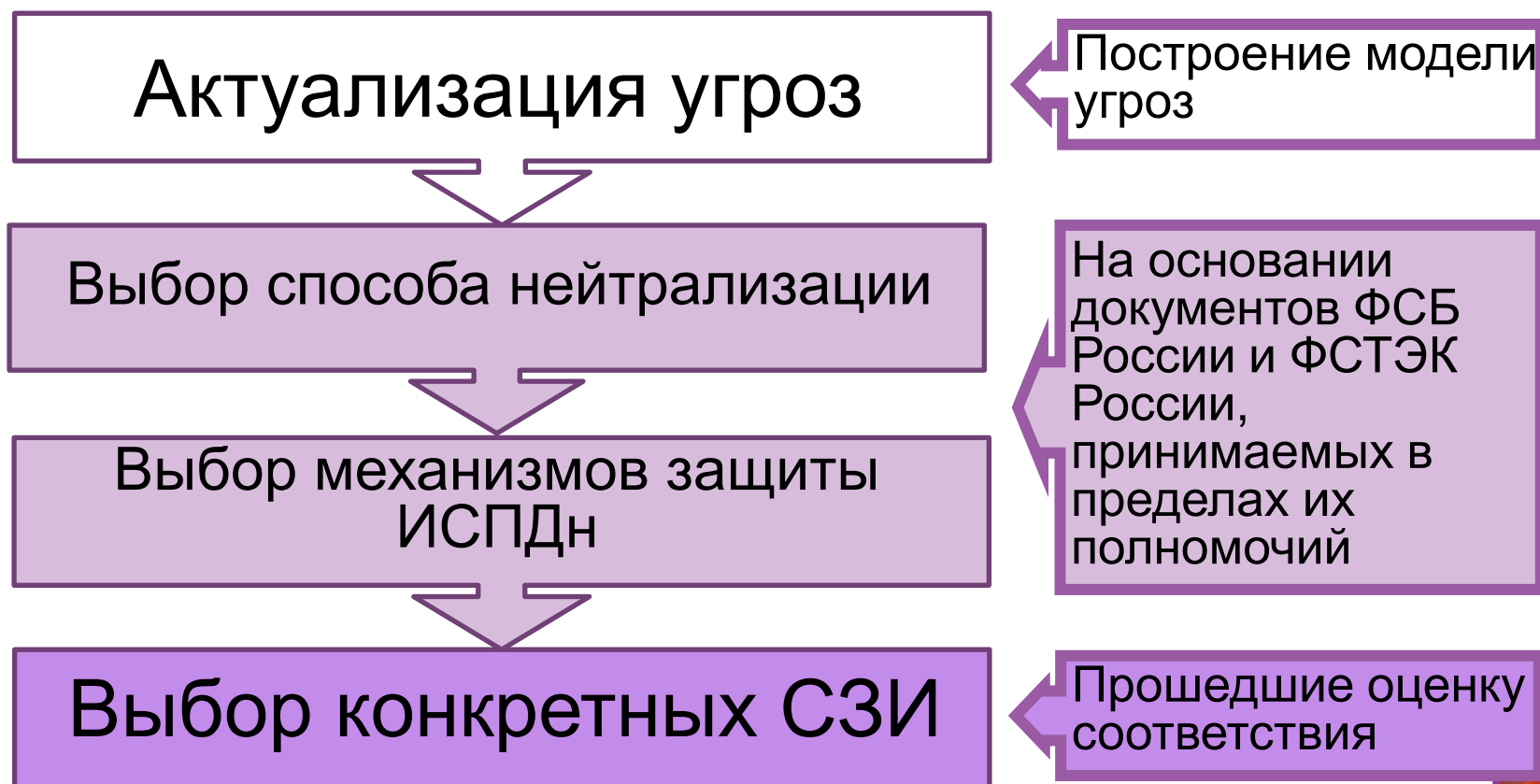
- ❖ ПДн обрабатываются без использования средств автоматизации;
- ❖ ПДн, отнесены к сведениям, составляющим государственную тайну;
- ❖ технические средства частично или целиком находятся за пределами Российской Федерации.

Определяет методологию формирования:

1. Модели угроз верхнего уровня (характеристики безопасности ПДн и объектов защиты);
2. Детализированной модели угроз (определения уровня криптографической защиты);
3. Модели нарушителя (Н1, Н2, ... , Н6);

<b>Модель Нарушителя</b>	<b>№ п.</b>	<b>Н1</b>	<b>Н2</b>	<b>Н3</b>	<b>Н4</b>	<b>Н5</b>	<b>Н6</b>
Уровень криптографической защиты	<b>п. 4.1</b>	КС1	КС2	КС3	КВ1	КВ2	КА1
Защита от ПЭМИН	<b>п. 4.2</b>	КС			КВ		КА
Уровень защиты от НСД	<b>п. 4.3</b>	АК1	АК2	АК3	АК4	АК5	АК6

# Алгоритм по созданию системы защиты ПДн





Вопросы ?

