



# **Приказ ФСТЭК России 2013 г. № 21: «Тонкие» места. Практические рекомендации.**

Михаил Булаев,  
Ведущий консультант-аналитик ОАО «ЭЛВИС-ПЛЮС»

## Введение

Документ «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в ИСПДн» (утверждён приказом ФСТЭК России от 18.2.2013 г. № 21):

- принят во исполнение ч. 4 ст. 19 Федерального закона от 27.07.2006 г. № 152-ФЗ «О персональных данных»;
- устанавливает перечень **обязательных мер по обеспечению безопасности ПДн, принимаемых для защиты ПДн от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения** а также от иных неправомерных действий;
- требования приказа носят **обязательный характер** для операторов или лиц, осуществляющих обработку персональных данных по поручению оператора.

# Что такое «мера защиты информации»?

## Группы мер защиты

**Мера защиты** = требование по защите информации - установленное правило или норма, которая должна быть выполнена при организации и осуществлении защиты информации.

*Приказ № 21 ФСТЭК России предусматривает возможность применения 109 мер защиты сгруппированных в 15 групп:*

1. Идентификация и аутентификация субъектов и объектов доступа (ИАФ).
2. Управление доступом субъектов к объектам доступа (УПД).
3. Ограничение программной среды (ОПС).
4. Защита машинных носителей информации (ЗНИ).
5. Регистрация событий безопасности (РСБ).
6. Антивирусная защита (АВЗ).
7. Обнаружение вторжений (СОВ).
8. Контроль (анализ) защищенности персональных данных (АНЗ).
9. Обеспечение целостности ИС и ПДн (ОЦЛ).
10. Обеспечение доступности ПДн (ОДТ).
11. Защита среды виртуализации (ЗСВ).
12. Защита технических средств (ЗТС).
13. Защита ИС, ее средств, систем связи и передачи данных (ЗИС).
14. Выявление инцидентов и реагирование на них (ИНЦ).
15. Управление конфигурацией ИС и СЗПДн (УКФ).

# Как выбрать необходимые меры защиты?

*Определение базового набора мер*

Требуемый уровень защищённости ПДн (по ПП1119)

Базовый набор мер ЗИ

*Адаптация базового набора*

Структурно-функциональные характеристики ИСПДн

Адаптированный базовый набор

*Уточнение адаптированного набора*

Актуальные угрозы безопасности ПДн

Уточнённый адаптированный базовый набор мер ЗИ

*Дополнение уточненного адаптированного набора (при необходимости)*

Дополнение уточнённого адаптированного набора

Дополненный уточнённый адаптированный базовый набор



# Выбор уровня защищённости ПДн

Категория ПДн	Тип угрозы				
	1-тип	2-тип		3-тип	
Специальные	<b>УЗ-1</b>	<b>УЗ-1</b> при обраб-ке ПДн >100 тыс. др. субъектов	<b>УЗ-2</b> при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов	<b>УЗ-2</b> при обраб-ке ПДн >100 тыс. др. субъектов	<b>УЗ-3</b> при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов
Биометрические	<b>УЗ-1</b>	<b>УЗ-2</b>		<b>УЗ-3</b>	
Иные категории	<b>УЗ-1</b>	<b>УЗ-2</b> при обраб-ке ПДн >100 тыс. др. субъектов	<b>УЗ-3</b> при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов	<b>УЗ-3</b> при обраб-ке ПДн >100 тыс. др. субъектов	<b>УЗ-4</b> при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов
Общедоступные	<b>УЗ-2</b>	<b>УЗ-2</b> при обраб-ке ПДн >100 тыс. др. субъектов	<b>УЗ-3</b> при обр. ПДн сотрудников оператора или <100 тыс. др. субъектов	<b>УЗ-4</b>	



# Что такое «тип угроз»?

**Тип угроз** – характеристика нарушителя, который может реализовать угрозы и которому должна противостоять система защиты

Характеристика нарушителя		Тип угроз, которые может реализовать нарушитель	
Потенциал	Возможности		
<b>Высокий</b> (нарушитель государственного типа – Спецслужбы ИГ)	Создание способов, подготовка и проведение атак <u>с привлечением специалистов для реализации атак в области использования недокументированных (недекларированных) возможностей (НДВ) системного ПО</u>	<b>1 тип</b>	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в системном ПО, используемом в ИС.
<b>Средний</b> (нарушитель корпоративного типа – Специализированные корпорации (Гугл, Оракл, IBM, SAP....))	Создание способов, подготовка и проведение атак <u>с привлечением специалистов в области использования для реализации атак НДВ прикладного ПО</u>	<b>2 тип</b>	Угрозы, связанные с наличием недокументированных (недекларированных) возможностей в прикладном ПО, используемом в ИС.
<b>Базовый</b> (нарушитель физическое лицо или группа физических лиц – хакер, криминал)	Создание способов, подготовка и проведение атак <u>без привлечения специалистов в области разработки и анализа СЗИ (в т.ч. СКЗИ)</u>	<b>3 тип</b>	Угрозы не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном ПО, используемом в ИС.

# Что такое «недекларированные (недокументированные) возможности ПО»?

**Недекларированные (недокументированные) возможности ПО** - функциональные возможности программного обеспечения, не описанные или не соответствующие описанным в документации, при использовании которых возможно нарушение характеристик безопасности защищаемой информации

*п. 2.1. РД «Защита от НСД к информации. Часть 1. ПО СЗИ. Классификация по уровню контроля отсутствия НДВ», Гостехкомиссия России, 1999 г.*

## Важно:

К недокументированным (недекларированным) возможностям программного обеспечения не относятся уязвимости, возникающие за счёт ошибок программирования, недостатков, допущенных при проектировании системы, ненадежных паролей, вирусов и других вредоносных программ.

*(см. РД НДВ, Рек-ции по стандартизации Р 50.1.056 и ГОСТ Р 50922)*



## Адаптация базового набора мер защиты

*При адаптации базового набора мер защиты информации учитываются:*

- цели (обеспечение **конфиденциальности**, **целостности** и (или) **доступности** информации) и задачи защиты информации в информационной системе;
- **перечень мероприятий** проводимых оператором по обеспечению **безопасности** в рамках организации в целом;
- применяемые **информационные технологии** и **структурно-функциональные характеристики** информационной системы.

**Адаптация базового набора мер защиты, как правило, предусматривает исключение мер, непосредственно связанных с информационными технологиями, не используемыми в информационной системе, или структурно-функциональными характеристиками, не свойственными информационной системе.**





# Что такое структурно-функциональные характеристики ИСПДн?

*Структурно-функциональные характеристики ИС включают:*

- особенности архитектуры построения ИС, (автономные, локальные территориально-распределённые) в т.ч. наличие уровней (сегментов) ИС;
- состав программно-аппаратных компонент ИС;
- используемые информационные технологии;
- физические, логические, функциональные и технологические взаимосвязи в ИС;
- взаимодействие с другими ИС и информационно-телекоммуникационными сетями;
- режимы функционирования ИС и обработки информации (использование разграничения полномочий пользователей и др.);
- иные особенности построения и функционирования ИС.

## Что такое «компенсирующие меры» (1)?

*«При невозможности технической реализации отдельных мер по обеспечению безопасности ПДн, а также с учетом экономической целесообразности могут разрабатываться иные (компенсирующие) меры, направленные на нейтрализацию актуальных угроз безопасности ПДн.*

*В этом случае в ходе разработки системы защиты ПДн **должно быть проведено обоснование применения компенсирующих мер для обеспечения безопасности ПДн».***

*П. 10 Приказа ФСТЭК России 2013 г. № 21*

- Использование дополнительных (необязательных) мер защиты из 21 приказа.
- Принятие технических решений.
- Применение средств шифрования для реализации функций защиты, реализуемых «обычными» СЗИ.
- Замена отдельных технических мер защиты на организационные.

***Замена сертифицированных СЗИ на несертифицированные – это не компенсирующая мера!***



## Что такое «компенсирующие меры» (2)?

**Обоснование применения компенсирующих мер защиты информации должно включать:**

- изложение причин исключения меры (мер) защиты информации;
- сопоставление исключаемой меры (мер) защиты информации с блокируемой (нейтрализуемой) угрозой (угрозами) безопасности информации;
- описание содержания компенсирующих мер защиты информации;
- сравнительный анализ компенсирующих мер защиты информации с исключаемыми мерами защиты информации;
- аргументацию, что предлагаемые компенсирующие меры защиты информации обеспечивают адекватное блокирование (нейтрализацию) угроз безопасности информации.



# Выбор средств защиты

Уровень защищённости ПДн	Класс защиты СЗИ									Уровень контроля ПО СЗИ на отсутствие НДВ
	СВТ	САВЗ		СОВ		МЭ		СДЗ		
		В случае актуальности угроз 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	В случае актуальности угроз 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	В случае актуальности угроз 1 или 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	В случае актуальности угроз 1 или 2 типа или при взаимодействии ИСПДн с сетями МИО	В случае актуальности угроз 3 типа и отсутствии взаимодействия ИСПДн с сетями МИО	
<b>УЗ-1</b>	Не ниже 5 класса	Не ниже 4 класса		Не ниже 4 класса		Не ниже 3 класса	Не ниже 4 класса	Не ниже 4 класса		4 уровень
<b>УЗ-2</b>	Не ниже 5 класса	Не ниже 4 класса		Не ниже 4 класса		Не ниже 3 класса	Не ниже 4 класса	Не ниже 4 класса		4 уровень
<b>УЗ-3</b>	Не ниже 5 класса	Не ниже 4 класса	Не ниже 5 класса	Не ниже 4 класса	Не ниже 5 класса	Не ниже 3 класса	Не ниже 4 класса	Не ниже 4 класса	Не ниже 5 класса	4 уровень (в случае актуальности угроз 2-го типа)
<b>УЗ-4</b>	Не ниже 6 класса	Не ниже 5 класса		Не ниже 5 класса		Не ниже 5 класса		Не ниже 5 класса		Требования не предъявляются

## Рекомендации по практической реализации мер защиты

В качестве руководства по практической реализации мер защиты рекомендуется использовать **Методический документ ФСТЭК России «Меры защиты информации в государственных информационных системах»** (утверждён 11.02.2014 г.)

*Пример реализации меры ИАФ.4 для УЗ-4 при использовании парольной защиты:*

- длина пароля не менее шести символов;
- алфавит пароля не менее 30 символов;
- максимальное количество неуспешных попыток аутентификации (ввода неправильного пароля) до блокировки от 3 до 10 попыток;
- блокировка программно-технического средства или учетной записи пользователя в случае достижения установленного максимального количества неуспешных попыток аутентификации от 3 до 15 минут;
- смена паролей не более чем через 180 дней.



## Документация системы защиты ПДн (1)

- 1) Каких-либо жестких требований по составу документации СЗПДн не существует.
- 2) Состав и содержание документации СЗПДн определяются в зависимости от перечня реализуемых СЗПДн мер защиты, требующих регламентации порядка их применения.
- 3) Оформление документации (т.е. выбор вида и формы документации) осуществляется в соответствии с принятым в организации стандартами управленческой и технической документации.

*Пример из Методического документа «Меры защиты информации в государственных информационных системах» ИАФБ: Идентификация и аутентификация пользователей*

- Правила и процедуры идентификации и аутентификации пользователей регламентируются в организационно-распорядительных документах оператора по защите информации.

## Документация системы защиты ПДн (2)

**Требования по защите ПДн (меры защиты)  
(ТЗ на СЗПДн)**

*Основание для разработки:  
Приказ № 21, требуемый УЗ ПДн, структурно-функциональные характеристики ИСПДн, МУ, политика ИБ оператора*

**Конструкторская документация на СЗПДн**

**Регламентирующая выполнение  
технических мер защиты**

**Проектная:**  
описание  
технических  
решений

**Эксплуатационная:**  
порядок применения  
технических решений  
(технологические  
инструкции, регламенты)

**Регламентирующая выполнение  
организационных мер защиты  
(Организационно-распорядительная)**

Определяет правила что и как  
выполнять:  
**Положения, правила, инструкции**

Кто выполняет:  
**должностные (функциональные) инструкции (обязанности)**

# Что такое оценка эффективности СЗПДн?

Обеспечение безопасности персональных данных достигается:

- **оценкой эффективности принимаемых мер по обеспечению безопасности персональных данных до ввода в эксплуатацию информационной системы персональных данных;**

п. 4, ч. 2, ст. 19 ФЗ № 152-ФЗ «О персональных данных»

**Эффективность защиты информации:** Степень соответствия результатов защиты информации цели защиты информации

п. 2.9.2. ГОСТ Р 50922-2006

Оценка эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн **проводится оператором самостоятельно или с привлечением на договорной основе юридических лиц, имеющих лицензию на осуществление деятельности по ТЗКИ.** Указанная оценка проводится не реже одного раза в 3 года.

п. 6 Приказа ФСТЭК России 2013 г. № 21



## Возможные формы оценки эффективности

Решение по форме оценки эффективности и документов, разрабатываемых по результатам оценки эффективности, **принимается оператором самостоятельно и (или) по соглашению с лицом, привлекаемым для проведения оценки эффективности реализованных мер по обеспечению безопасности ПДн.**

п. 3 Информационного сообщения ФСТЭК России от 15.07.2013 г. № 240/22/2637

Оценка соответствия может проводиться в формах государственного контроля (надзора), **испытания**, регистрации, подтверждения соответствия (сертификация, декларирование), приемки и ввода в эксплуатацию объекта, строительство которого закончено, и в иной форме.

ст. 7 ФЗ от 27.12.2002 г. № 184-ФЗ «О техническом регулировании»

Таким образом оптимальный вариант – проведение оценки эффективности реализованных в рамках СЗПДн мер по обеспечению безопасности ПДн **в форме приемо-сдаточных (приемочных) испытаний, проводимых после завершения работ по созданию СЗПДн.**



**Ваши вопросы?**

<http://www.elvis.ru>