Основные документы

1. Информационное письмо от 1 марта 2012г. №240 «Об утверждении требований к системам обнаружения вторжений»
2. Постановление Правительства от 1 ноября 2012г. №1119 «Об утверждении требований к защите персональных данных при обработки их в ИСПДн»
3. Приказ ФСБ РФ N 416, ФСТЭК РФ N 489 от 31.08.2010 «Об утверждении Требований о защите информации, содержащейся в информационных системах общего пользования» (Зарегистрировано в Минюсте РФ 13.10.2010 N 18704)

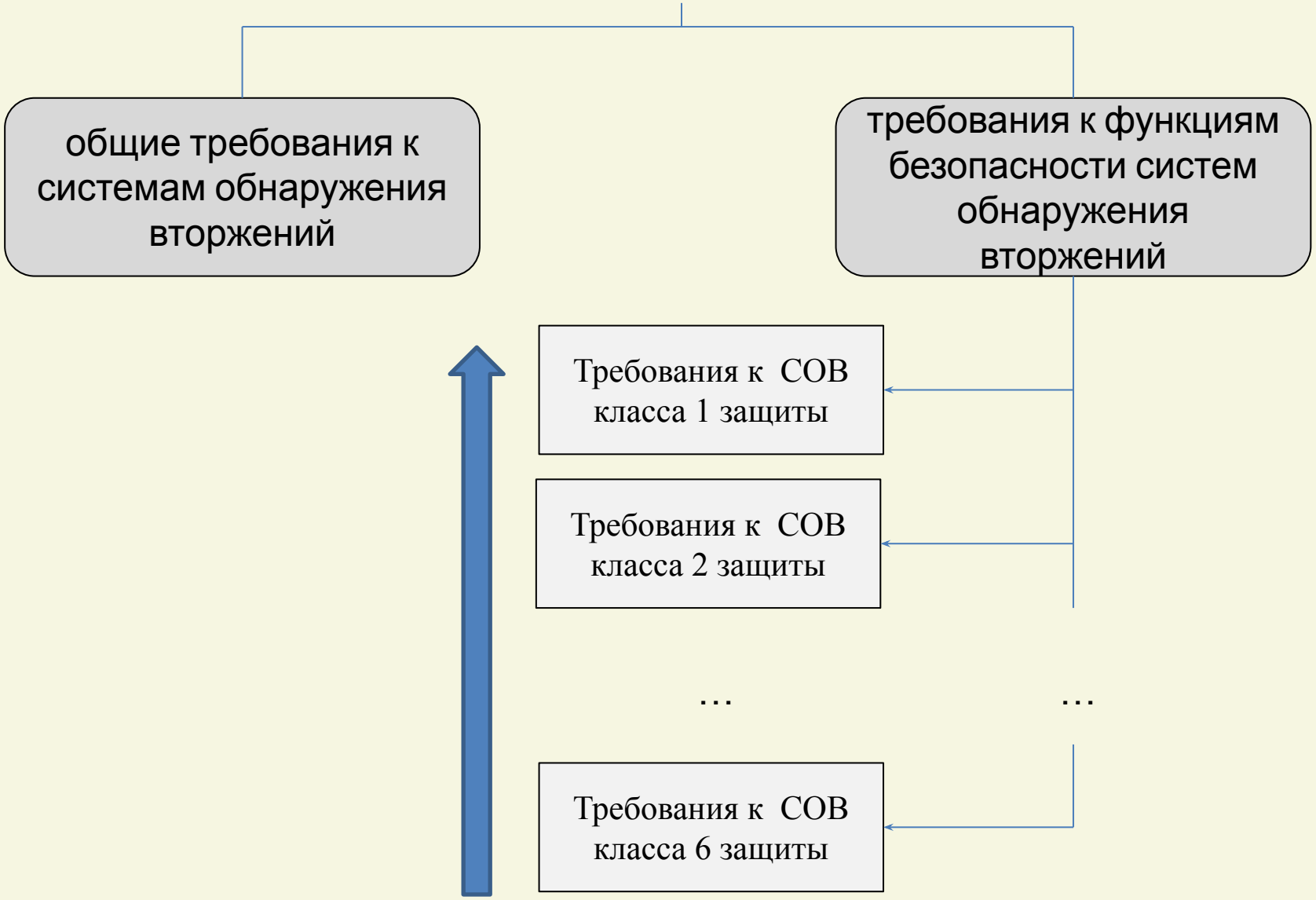
Применение требований

Требования к системам обнаружения вторжений применяются к программным и программно-техническим средствам, используемым в целях обеспечения защиты (некриптографическими методами) информации, содержащей сведения, составляющие государственную тайну, иной информации с ограниченным доступом.

Требования предназначены для:

- организаций, осуществляющих в соответствии с законодательством Российской Федерации работы по созданию средств защиты информации
- заявителей на осуществление сертификации продукции
- испытательных лабораторий и органов по сертификации

Требования к системам обнаружения вторжений



Определение необходимости обеспечения уровня защищенности ПДн при их обработки в ИСПДн

Тип ИСПДн	Категория субъектов ПДн	Количество субъектов ПДн	Тип актуальных угроз		
			1	2	3
ИСПДн со специальными категориями ПДн	Не сотрудники	> 100 000	1	1	2
		< 100 000	1	2	3
	Сотрудники	любое	1	2	3
ИСПДн с биометрическими ПДн	Не сотрудники	> 100 000	1	2	3
		< 100 000	1	2	3
	Сотрудники	любое	1	2	3
ИСПДн с общедоступными ПДн	Не сотрудники	> 100 000	2	2	4
		< 100 000	2	3	4
	Сотрудники	любое	2	3	4
ИСПДн с иными категориями ПДн	Не сотрудники	> 100 000	1	2	3
		< 100 000	1	3	4
	Сотрудники	любое	1	3	4

Определение класса ИСПДн

KHj / Ki	КН1	КН2	КН3
К1	УЗ-2	УЗ-1	УЗ-1
К2	УЗ-3	УЗ-2	УЗ-1
К3	УЗ-3	УЗ-3	УЗ-2
К4	УЗ-4	УЗ-4	УЗ-4

КН1 – нарушитель, самостоятельно осуществляющий создание методов и средств реализации атак и реализацию атак на информационную систему;

КН2 – группа нарушителей, осуществляющая создание методов и средств реализации атак и реализацию атак на информационную систему с привлечением специалистов в области разработки и анализа средств защиты информации, включая специалистов в области защиты информации от утечки по техническим каналам и (или) специалистов в области использования для реализации атак недокументированных возможностей прикладного программного обеспечения

КН3 – нарушитель или группа нарушителей, осуществляющая создание методов и средств реализации атак и реализацию атак на информационную систему с привлечением специалистов в области разработки и анализа средств защиты информации, включая специалистов в области использования для реализации атак недокументированных возможностей системного программного обеспечения.

Информационные системы общего пользования

Информационные системы общего пользования включают в себя средства вычислительной техники, информационно-вычислительные комплексы и сети, средства и системы передачи, приема и обработки информации, средства изготовления, тиражирования документов и другие технические средства обработки речевой, графической, видео- и буквенно-цифровой информации, программные средства (операционные системы, системы управления базами данных и т.п.), средства защиты информации, применяемые в информационных системах.

ИСОП в зависимости от значимости содержащейся в них информации и требований к ее защите разделяются на два класса:

1. ИСОП Правительства Российской Федерации и иные информационные системы общего пользования в случае, если нарушение целостности и доступности информации, содержащейся в них, может привести к возникновению угроз безопасности Российской Федерации.
2. Все остальные.

Классы защиты СОВ

Класс защиты	Информационные системы
6	**ИСПДн 4** класса
	ИСПДн 3 класса
5	**ИСПДн 2** класса
4	**Государственные** ИС, в которых обрабатывается информация ограниченного доступа, **не** содержащая сведения, составляющие **государственную тайну**
	ИСПДн 1 класса
	ИСОП 2 класса
3	ИС, в которых обрабатывается информация, содержащая сведения, составляющие **государственную тайну**
2	
1	

Спецификация профилей защиты СОВ для каждого типа СОВ и класса защиты СОВ

Класс защиты / Тип системы обнаружения вторжений	**6**	**5**	**4**	**3**	**2**	**1**
Система обнаружения вторжений уровня сети	ИТ.СОВ. С6.ПЗ	ИТ.СОВ. С5.ПЗ	ИТ.СОВ. С4.ПЗ	ИТ.СОВ. С3.ПЗ	ИТ.СОВ. С2.ПЗ	ИТ.СОВ. С1.ПЗ
Система обнаружения вторжений уровня узла	ИТ.СОВ. У6.ПЗ	ИТ.СОВ. У5.ПЗ	ИТ.СОВ. У4.ПЗ	ИТ.СОВ. У3.ПЗ	ИТ.СОВ. У2.ПЗ	ИТ.СОВ. У1.ПЗ

Примечание:

1. Утверждены ФСТЭК России 6 марта 2012 г. – Профиль защиты СОВ уровня сети (узла) пятого(шестого) класса защиты
2. Утверждены ФСТЭК России 3 февраля 2012 г. – Профиль защиты СОВ уровня сети(узла) четвёртого класса защиты