18.02.2019

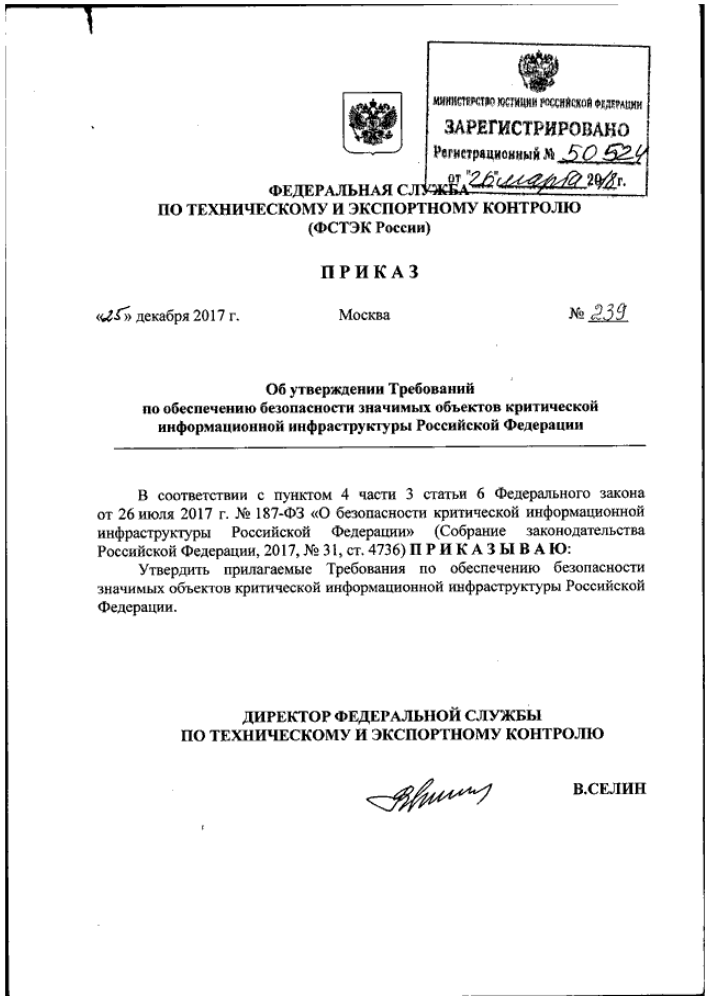
АМТ-ГРУП

Оценки СЗИ на соответствие требованиям по безопасности в формах испытаний или приемки при построении систем безопасности объектов КИИ

Формы оценки соответствия требованиям по безопасности СЗИ в СБоКИИ

П. 28. Для обеспечения безопасности значимых объектов КИИ должны применяться СЗИ, прошедшие оценку на соответствие требованиям по безопасности в формах

обязательной сертификации, испытаний или приемки



МИНИСТЕРСТВО ЮСТИЦИИ РОССИЙСКОЙ ФЕДЕРАЦИИ
ЗАРЕГИСТРИРОВАНО
Регистрационный № 50524
от "26" марта 2018 г.

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ
(ФСТЭК России)

ПРИКАЗ

«25» декабря 2017 г. Москва № 239

Об утверждении Требований
по обеспечению безопасности значимых объектов критической
информационной инфраструктуры Российской Федерации

В соответствии с пунктом 4 части 3 статьи 6 Федерального закона от 26 июля 2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» (Собрание законодательства Российской Федерации, 2017, № 31, ст. 4736) ПРИКАЗЫВАЮ:

Утвердить прилагаемые Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации.

ДИРЕКТОР ФЕДЕРАЛЬНОЙ СЛУЖБЫ
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

В.СЕЛИН

Кейс

Производственное предприятие

Проектирование и внедрение СБ ОКИИ (АСУТП)

Более 60 АСУ ТП

3-я категория ОКИИ

Для иных АСУ ТП обеспечиваем безопасность также по 3-ей категории

Сертификация СЗИ

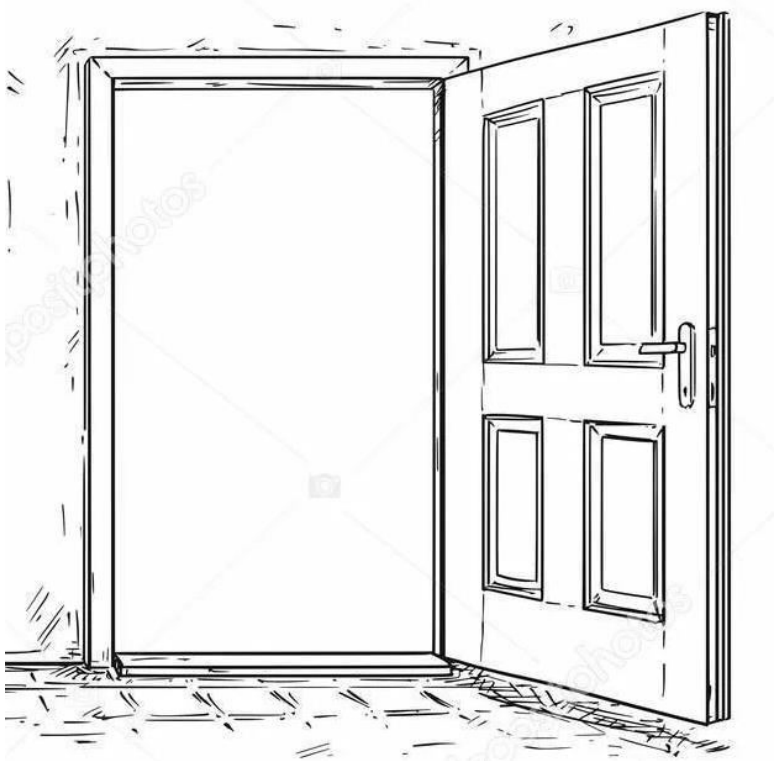
1441

сертифицированных СЗИ в Реестре ФСТЭК России):

- межсетевые экраны;
- системы обнаружения вторжений;
- средства доверенной загрузки;
- средства антивирусной защиты
- операционные системы;
- средства контроля подключения съемных машинных носителей информации;
- защита от НСД;
- ОУД;
- СВТ;
- НДВ;
- Различные ТУ

- «…в приоритетном порядке подлежат применению СЗИ, встроенные в ПО или программно-аппаратные средства объектов»;
- не для всех мер безопасности есть необходимые сертифицированные СЗИ;
- отдельные СЗИ могут негативно влиять на функционирование объектов КИИ в проектных режимах

Испытания и приемка



- Проводятся отдельно или в составе значимого объекта КИИ;
- Проводятся в соответствии с программой и методиками испытаний (приемки), утверждаемыми субъектом КИИ;
- Проводятся субъектами КИИ самостоятельно или с привлечением организаций, имеющих лицензии на деятельность в области защиты информации

Проблематика при планировании испытаний/приемки

как обеспечить объективность проверки функций безопасности СЗИ, их достаточность, качество выполнения во всех режимах функционирования?

как снизить риски предписаний по составу и содержанию ПМИ при проверках, в т.ч. в случае инцидентов на объектах КИИ?

каковы критерии приемки СЗИ?

каковы требования к квалификации людей, формирующих ПМИ и проводящих испытания?

Состав СЗИ в СБ объекта ОКИИ по приказу ФСТЭК России №239 (пример)

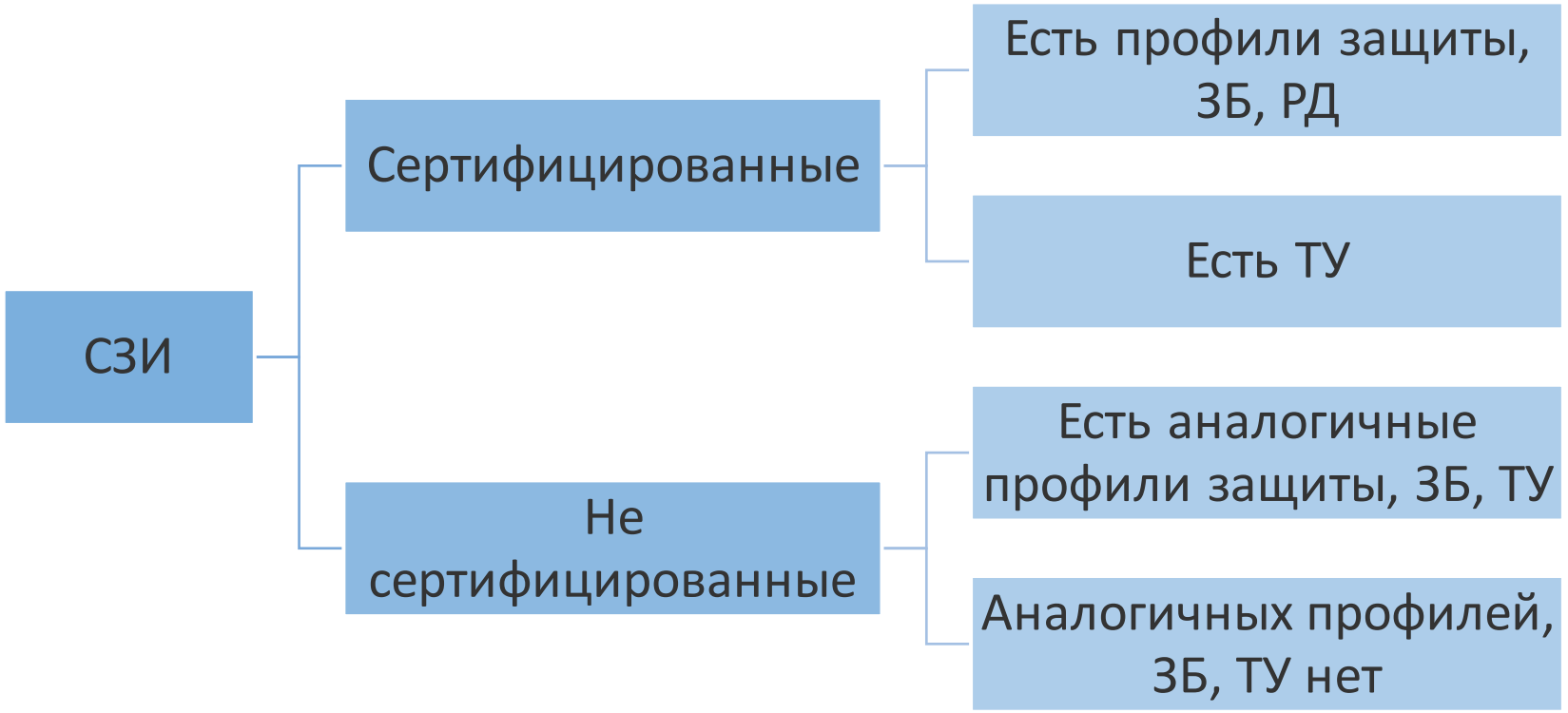
МЕРЫ		СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ					
I	ИАФ	Встроенные средства	Контроллер домена ТСПД	Защита каналов связи	Обнаружение аномалий и атак		
II	УПД	Встроенные средства	Контроллер домена ТСПД	Защита каналов связи	МСЭ	Контроль за учетными записями и сессиями	
III	ОПС	Встроенные средства	Контроллер домена ТСПД	Защита промышленных конечных узлов			
IV	ЗНИ	Встроенные средства	Контроллер домена ТСПД	Защита промышленных конечных узлов			
V	АУД	Встроенные средства	Контроллер домена ТСПД	Анализ уязвимостей	SIEM	NTP	
VI	АВЗ	Защита промышленных конечных узлов					
VII	СОВ	IPS					
VIII	ОЦЛ	Защита промышленных конечных узлов					
IX	ОДТ	Встроенные средства	Резервное копирование	ИТ-системы мониторинга			
X	ЗТС	Меры физической безопасности					
XI	ЗИС	Встроенные средства	Контроллер домена ТСПД	Обнаружение аномалий и атак	Защита каналов связи	МСЭ	IPS
XII	ИНЦ	Встроенные средства	SIEM	IRP			
XIII	УКФ	Встроенные средства	Контроллер домена ТСПД	Защита промышленных конечных узлов	версий, конфигураций		
XIV	ОПО	Встроенные средства	Контроллер домена ТСПД	Утилиты для расчета контрольных сумм			
XV	ПЛН	SGRC					
XVI	ДНС	Резервное копирование					
XVII	ИПО	Система обучения и контроля знаний					

Встроенные средства Наложенные средства

Группировка СЗИ в составе СБ ОКИИ для выбора подхода к оценке соответствия

Состав СЗИ:

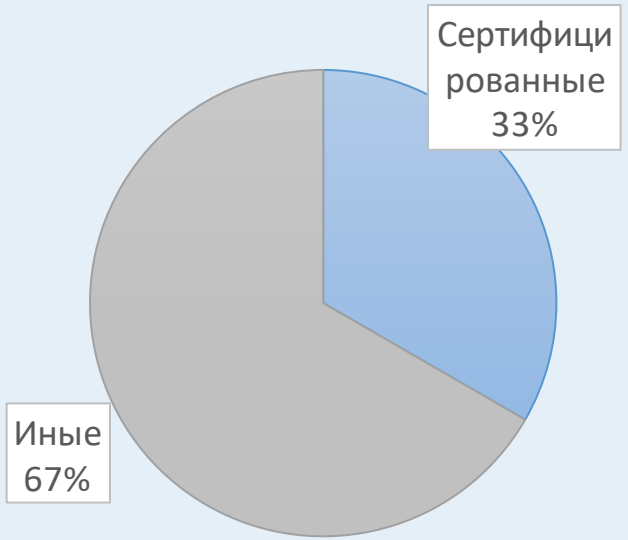
- Встроенные средства;
- Контроллер домена ТСПД;
- Защита каналов связи;
- Обнаружение аномалий и атак;
- МСЭ, IPS;
- Контроль за учетными записями и сессиями;
- Защита промышленных конечных узлов;
- Анализ уязвимостей;
- Резервное копирование;
- IRP, SGRC;
- Утилиты для расчета контрольных сумм;
- SIEM;
- Контроль версий, конфигураций



Сертифицированные СЗИ

СЗИ:

- Защита каналов связи;
- Обнаружение аномалий и атак;
- Контроль за учетными записями и сессиями;
- Защита промышленных конечных узлов;
- Анализ уязвимостей

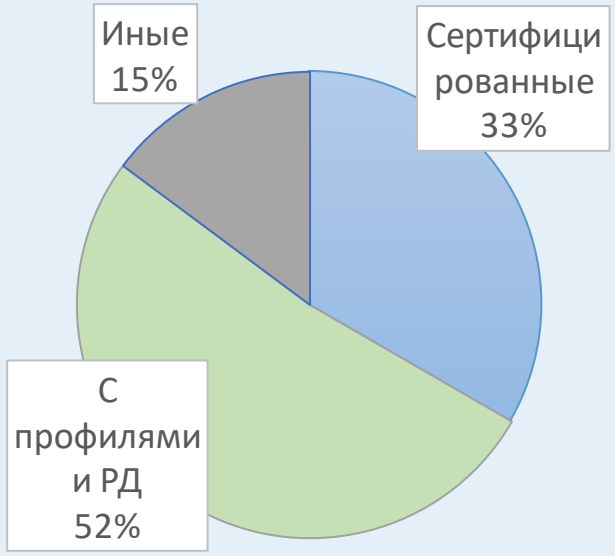


- Проверяем, что профили защиты, задания по безопасности предусматривают необходимые требования и функции безопасности;
- Анализируем технические условия на предмет выполнения СЗИ необходимых функций;
- «Доверяем» решению органа по сертификации и испытательной лаборатории

Не сертифицированные, для которых есть аналогичные профили защиты, ЗБ, ТУ

СЗИ:

- Встроенные средства (частично);
- Контроллер домена ТСПД (частично);
- МСЭ;
- IPS;
- SIEM

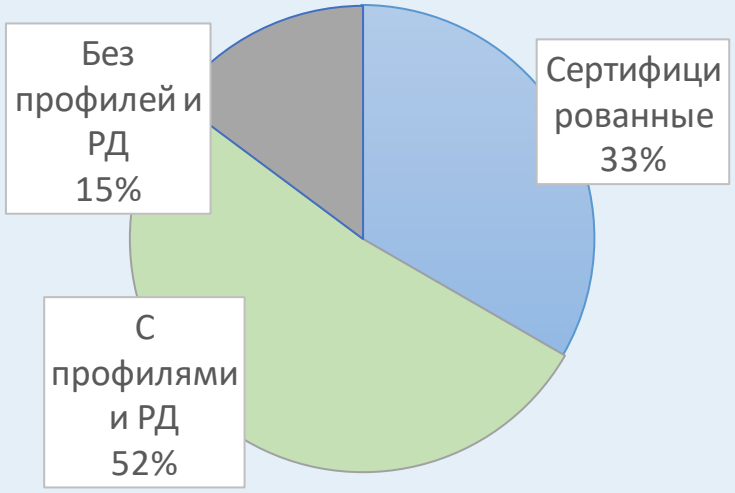


- При подготовке ПМИ учитываем содержание аналогичных профилей защиты, ЗБ, ТУ;
- Где возможно, дополняем проверками выполнения требования нормативно-правовых актов;
- Формируем проверки с учетом результатов моделирования угроз и анализа технических уязвимостей

Не сертифицированные, для которых нет аналогичных профилей защиты, ЗБ, ТУ

СЗИ:

- Встроенные средства (частично);
- Контроллер домена ТСПД (частично);
- Резервное копирование;
- IRP, SGRC;
- Утилиты для расчета контрольных сумм;
- Контроль версий, конфигураций



- Учитываем проверки выполнения требования нормативно-правовых актов;
- Формируем проверки с учетом результатов моделирования угроз и анализа технических уязвимостей;
- Учитываем ГОСТ Р ИСО/МЭК 15408;
- Где возможно, учитываем «лучшие практики», международные и отечественные стандарт

Что учесть в ПМИ

- перечень объектов, выделенных для испытаний и перечень требований, которым они должны соответствовать;
- критерии приемки системы и ее частей;
- условия и сроки проведения испытаний;
- средства для проведения испытаний;
- методику испытаний и обработки их результатов и др.

Заключение

- В установленных законодательством случаях сертификация обязательна;
- В иных случаях решение принимает субъект, но сертификация в данном случае может быть дополнительной «страховкой»;
- ПМИ для оценки соответствия СЗИ ≠ ПМИ для проверки работоспособности;
- Конечную ответственность за корректность ПМИ и ее проведение несет субъект КИИ