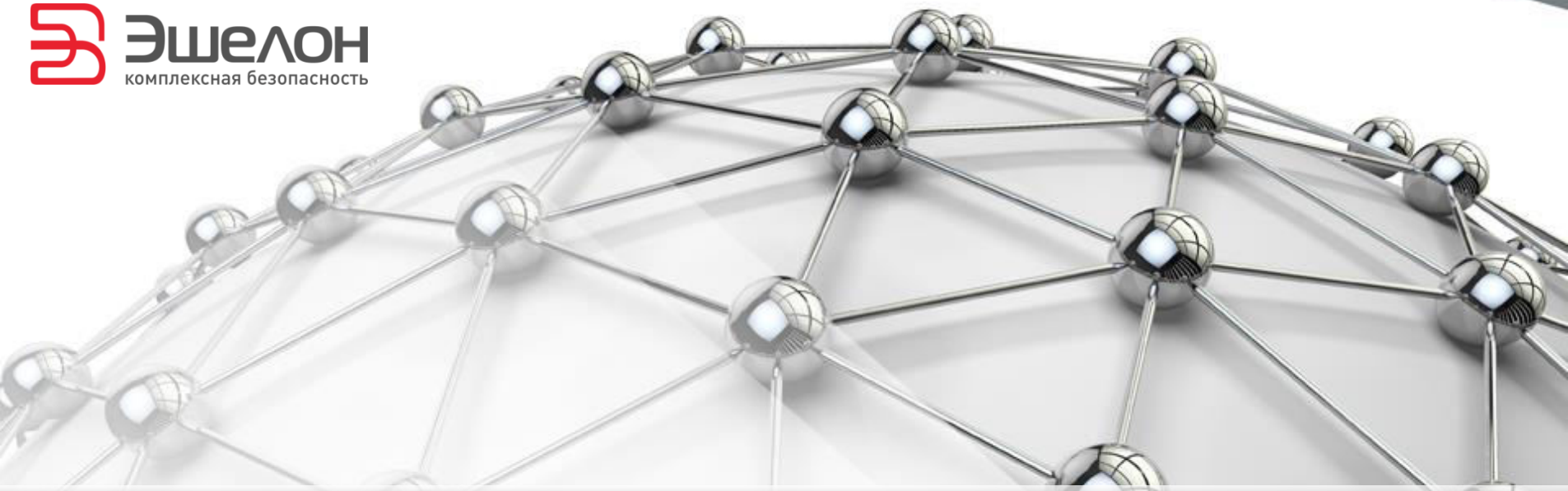
Эшелон
комплексная безопасность



Сертификация СЗИ Виртуализации

Вареница Виталий

Нормативная база

ГОСТ Р 56938 – 2016

17, 21 и 31 Приказы ФСТЭК России

Требования регуляторов (ФСТЭК, ФСБ, МО РФ)

Эшелон
комплексная безопасность

Нормативная база

Приказ 21 и 31

8.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к персональным данным, обрабатываемым в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры и (или) воздействие на них, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Приказ 17

20.11. Меры по защите среды виртуализации должны исключать несанкционированный доступ к информации, обрабатываемой в виртуальной инфраструктуре, и к компонентам виртуальной инфраструктуры, а также воздействие на информацию и компоненты, в том числе к средствам управления виртуальной инфраструктурой, монитору виртуальных машин (гипервизору), системе хранения данных (включая систему хранения образов виртуальной инфраструктуры), сети передачи данных через элементы виртуальной или физической инфраструктуры, гостевым операционным системам, виртуальным машинам (контейнерам), системе и сети репликации, терминальным и виртуальным устройствам, а также системе резервного копирования и создаваемым ею копиям.

Практическое выполнение мер ФСТЭК

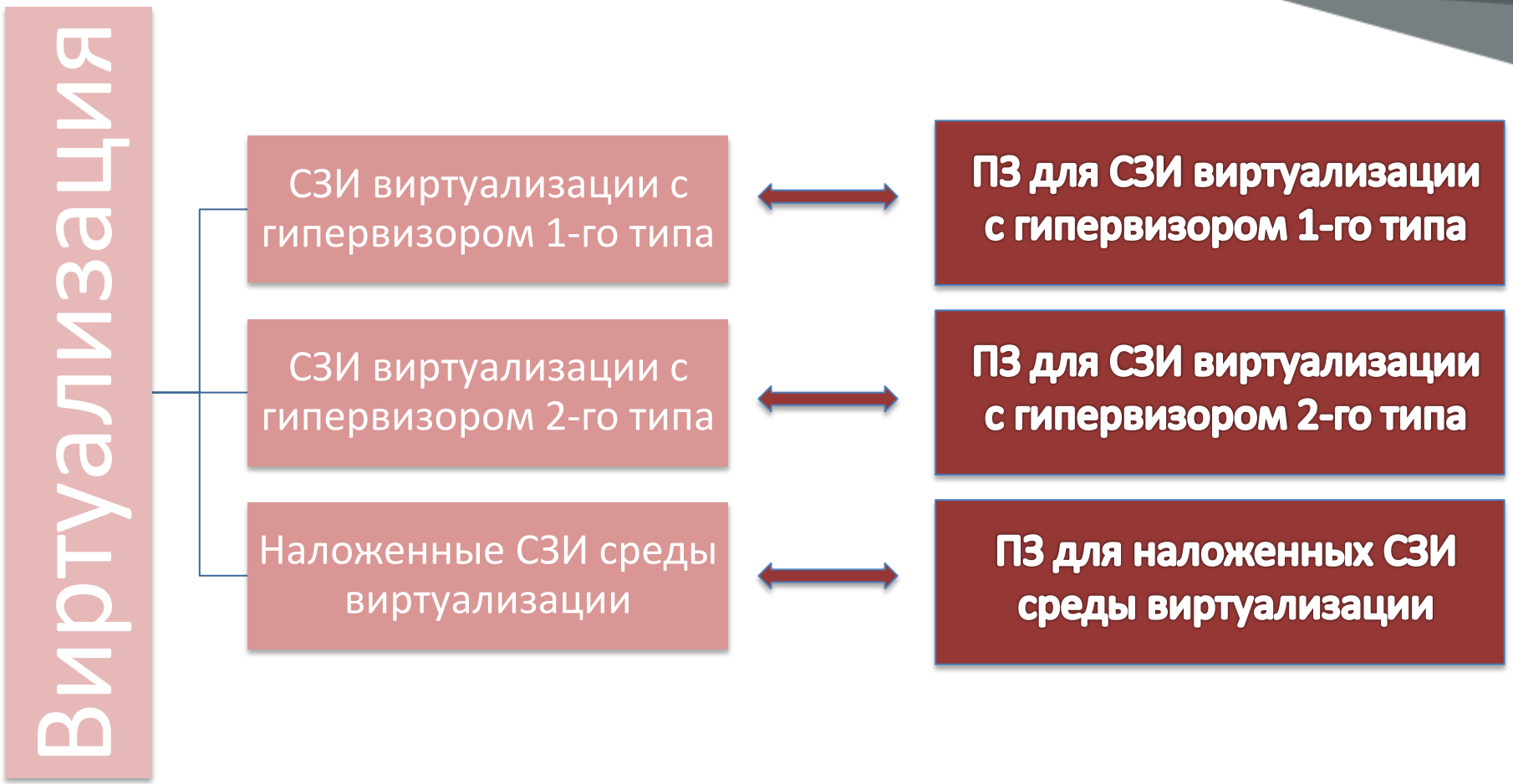
		П31 АСУ ТП			П21 ПДН				П17 ГИС			
Мера	Содержание мер по обеспечению безопасности информации	3	2	1	4	3	2	1	_4	_3	_2	_1
ЗСВ.0	Разработка правил и процедур(политик) защиты среды виртуализации	+	+	+								
ЗСВ.1	Идентификация и аутентификация субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации	+	+	+	+	+	+	+	+	+	+	+
ЗСВ.2	Управление доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин	+	+	+	+	+	+	+	+	+	+	+
ЗСВ.3	Регистрация событий безопасности в виртуальной инфраструктуре	+	+	+	-	+	+	+	-	+	+	+
ЗСВ.4	Управление (фильтрация, маршрутизация, контроль соединения, однонаправленная передача) потоками информации между компонентами виртуальной инфраструктуры, а также по периметру виртуальной инфраструктуры	-	+	+	-	-	-	-	-	-	+	+
ЗСВ.5	Доверенная загрузка серверов виртуализации, виртуальной машины (контейнера), серверов управления виртуализацией	-	-	-	-	-	-	-	-	-	-	-
ЗСВ.6	Управление перемещением виртуальных машин (контейнеров) и обрабатываемых на них данных	-	+	+	-	-	+	+	-	-	+	+
ЗСВ.7	Контроль целостности виртуальной инфраструктуры и ее конфигураций	-	+	+	-	-	+	+	-	-	+	+
ЗСВ.8	Резервное копирование данных, резервирование технических средств, программного обеспечения виртуальной инфраструктуры, а также каналов связи внутри виртуальной инфраструктуры	-	-	+	-	-	+	+	-	-	+	+
ЗСВ.9	Реализация и управление антивирусной защитой в виртуальной инфраструктуре	+	+	+	-	+	+	+	-	+	+	+
ЗСВ.10	Разбиение виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей	-	+	+	-	+	+	+	-	-	+	+

Объекты защиты информации в среде виртуализации

Виртуальная инфраструктура

Средства создания и управления виртуальной инфраструктурой	Виртуальная вычислительная система	Виртуальная система хранения данных	Виртуальный канал передачи данных	Отдельные виртуальные устройства хранения, обработки и передачи данных	Виртуальные СЗИ и СЗИ, предназначенные для использования в среде виртуализации

Виды СЗИ среды виртуализации



Эшелон
комплексная безопасность

Классификация СЗИ среды виртуализации

Классы защиты СЗИ виртуализации	Классы защищенности ГИС	Уровни защищенности ИСПДн	Классы защищенности АСУ ТП
6	3,4	3,4	3
5	2	2	2
4	1	1	1
3	Применяется к информационным системам, обрабатывающим информацию, содержащую сведения, составляющие государственную тайну		
2			
1			

Как будем сертифицировать?

На соответствие требованиям 17,21 и 31 Приказов ФСТЭК России

- ПЗ 6 класс + Анализ уязвимостей
- ПЗ 5 класс + НДВ 4 уровень + Анализ уязвимостей
- ПЗ 4 класс + НДВ 4 уровень + Анализ уязвимостей

Для применения в системах обрабатывающих ГТ

- ПЗ 3 класс + НДВ 3 уровень + Анализ уязвимостей
- ПЗ 2 класс + НДВ 2 уровень + Анализ уязвимостей
- ПЗ 1 класс + НДВ 1 уровень + Анализ уязвимостей

Эшелон
комплексная безопасность

Как сертифицируем сейчас

ФСТЭК России

ТУ + НДВ + АУ

Минобороны России

РДВ + НДВ

ФСБ России

Временные требования

Эшелон
комплексная безопасность

Спасибо за внимание!

Эшелон
комплексная безопасность

Контактная информация

107023, ул. Электрозаводская, д. 24

+7(495) 223-23-92
+7(495) 645-38-11

http://www.npo-echelon.ru