ЦИФРОВОЙ РЕГИОН ЧУДПО РЦБ

Безопасность критической информационной инфраструктуры Российской Федерации

Лекция 7. Порядок определения мер защиты и требования к средствам защиты значимых объектов критической информационной инфраструктуры Российской Федерации

Порядок определения мер защиты информации

Определение **БАЗОВОГО** набора мер защиты информации

АДАПТАЦИЮ базового набора мер защиты информации

УТОЧНЕНИЕ адаптированного базового набора мер защиты информации

ДОПОЛНЕНИЕ уточненного адаптированного базового набора мер защиты информации

ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

Средства защиты информации

- Антивирусы
- Средства защиты от НСД
- Межсетевые экраны
- Средства резервного копирования
- Сканеры уязвимостей
- Средства защиты систем виртуализации
- СКЗИ
- Песочницы

- СОВ/СПВ
- SIEM
- Системы форензики
- СКЗИ
- Средства инвентаризации

Средства ГосСОПКА

Приказ ФСБ России № 196

Средства защиты информации

Приказ ФСТЭК России № 239

ЦИФРОВОЙ РЕГИОН

ЧУДПО РЦБ

Требования к средствам защиты информации

Наименование требований	Нормативный акт	Категория значимости		
		Первая	Вторая	Третья
Сертификация	**№ 235, п.18; № 239, п.28**	СЗИ, **прошедшие оценку на соответствие требованиям по безопасности** в формах обязательной сертификации, испытаний или приемки. ИЛИ **прошедшие испытаний или приемку, проводимые субъектами КИИ** самостоятельно или с привлечением лицензиата ФСБ и ФСТЭК.		
СЗИ, встроенные в ПО и ПАК объекта КИИ	**№ 235, п.19; № 239, п.27**	**Встроенные в ПО и ПАК объекта КИИ** СЗИ подлежат применению **в приоритетном порядке.**		
Наличие поддержки	**№ 235, п.21; № 239, п.31** **№ 196, п.3**	СЗИ должны быть обеспечены **гарантийной, технической поддержкой** со стороны разработчиков (производителей). Средства ГосСОПКА должны быть обеспечены технической поддержкой и иметь возможность модернизации российскими органами, не находящимися **под прямым или косвенным контролем иностранным физических или юридических лиц.**		
Классы защиты и уровни доверия к ним	**№ 239, п.29**	**Класс защиты ≥ 4** **Уровень доверия ≥ 4**	**Класс защиты ≥ 5** **Уровень доверия ≥ 5**	**Класс защиты ≥ 6** **Уровень доверия ≥ 6**
Недопустимый функционал	**№ 239, п.31; № 196, п.3**	**Удаленный доступ** для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ; **Локальный бесконтрольный доступ** для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ; **Передача информации, в том числе технологической**, разработчику (производителю) СЗИ или иным лицам без контроля со стороны субъекта КИИ		