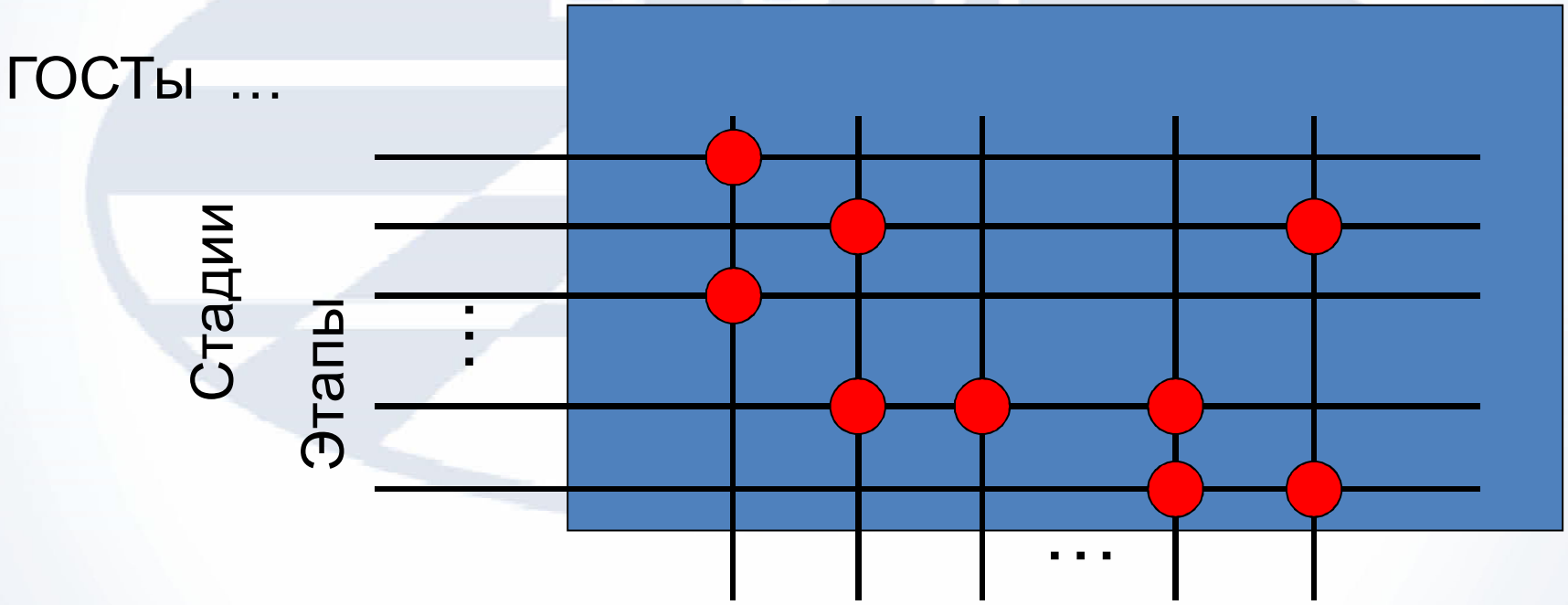
Опыт проектирования информационных систем на основе новых требований ФСТЭК России

Сидак Алексей Александрович,
Центр безопасности информации,
Заместитель Председателя, КТН

Новая нормативная база по защите информации

Законодательство РФ	Нормативные документы	Методические документы	Национальные стандарты
№152-ФЗ «О персональных данных»	Приказ ФСТЭК России от 11 февраля 2013 г. № 17	Меры защиты информации в ГосИС	ГОСТ Р 51583 «ЗИ. Порядок создания АС в защищенном исполнении. Общие положения»
№149-ФЗ «Об информации, ИТ и о ЗИ»	Приказ ФСТЭК России от 18 февраля 2013 г. № 21	Рекомендации по формированию модели угроз (проект)	ГОСТ Р 51624 «ЗИ. АС в защищенном исполнении. Общие требования»
			ГОСТ Р ИСО/МЭК 27001
			Национальные стандарты по уязвимости ИС: - Классификация уязвимостей (проект); - Правила описания уязвимостей (проект); - Содержание и порядок выполнения работ по выявлению и оценке уязвимостей (проект).
	Информационные системы		
	Средства защиты информации		
	НПА «Требования к системам обнаружения вторжений»	ПЗ для Систем обнаружения вторжений	
	НПА «Требования к средствам антивирусной защиты»	ПЗ для Средств антивирусной защиты	ГОСТ Р ИСО/МЭК 15408 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности ИТ» Часть 1,2,3
	НПА «Требования к средствам доверенной загрузки»	ПЗ для Средств доверенной загрузки	
	. . .	. . .	
	НПА «Требования к средствам…»	ПЗ для Средств…	ГОСТ Р ИСО/МЭК 18045 «Методы и средства обеспечения безопасности. Методология оценки безопасности ИТ»

Как «совместить» требования ГОСТ на разработку АС и мероприятий Приказа 17 ?

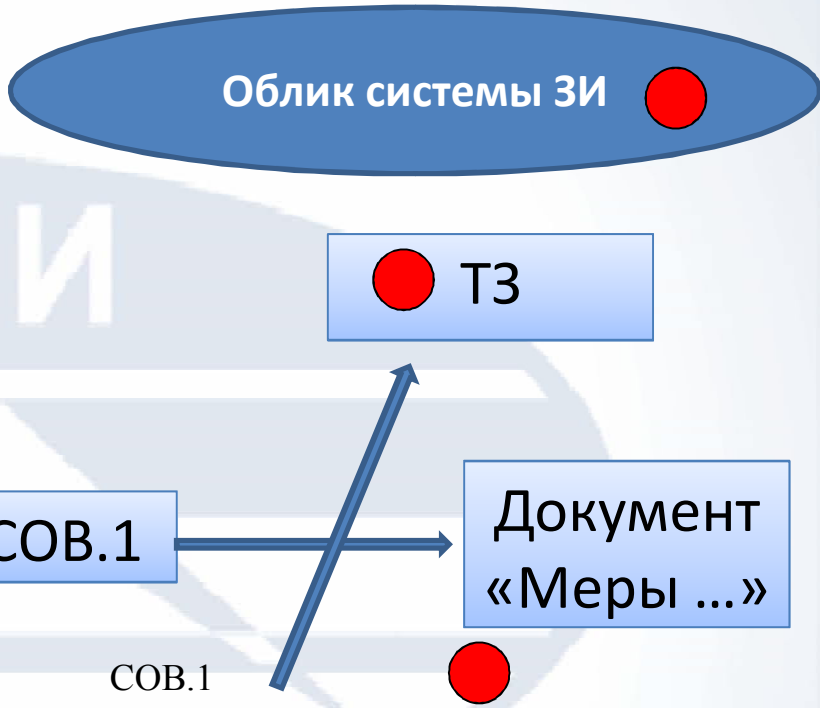


Мероприятия, предусмотренные Приказом 17

Как задавать требования ?

Приказ 17
(Приказ 21)

- Идентификация и аутентификация
- Управление доступом
- Защита МНИ
- Регистрация событий безопасности
- Антивирусная защита
- Обнаружение вторжений
- Контроль защищенности
- Целостность ИС и информации
- Доступность информации
- Защита среды виртуализации
- Защита технических средств
- Защита ИС, ее средств, систем связи и передачи данных



СОВ.1

Требования к реализации СОВ.1:

Оператором обеспечивается обнаружение …

Применяемые системы обнаружения вторжений должны …

Обнаружение (предотвращение) вторжений должно ….

…

Требования к усилению СОВ.1:

1) оператором обеспечивается …

2) в информационной системе обеспечивается …

Механизм выбора мер защиты информации

1. **Класс защищенности ИС** → Базовый набор мер ЗИ
2. **Структурно-функциональные характеристики ИС, ИТ, особенности функционирования** → Адаптированный базовый набор мер ЗИ
3. **Угрозы БИ, включенные в модель угроз БИ** → Уточненный адаптированный базовый набор мер ЗИ
4. **Требования иных НПА (в т.ч. по ПДн)** → Дополненный уточненный адаптированный базовый набор мер ЗИ

Приказ 17
(Приказ 21)

Как при проектировании выполнить все процедуры?

Определение архитектуры СЗИ

Определение конкретных средств ЗИ для реализации мер

Определение субъектов и объектов доступа

- Физ. лица
- Процессы
- ПО
- Устройства

Определение параметров настройки

- Для реализации мер
- Для устранения уязвимостей

Приказ 17
(Приказ 21)

Какие инструменты использовать для оптимизации затрат на реализацию мер?

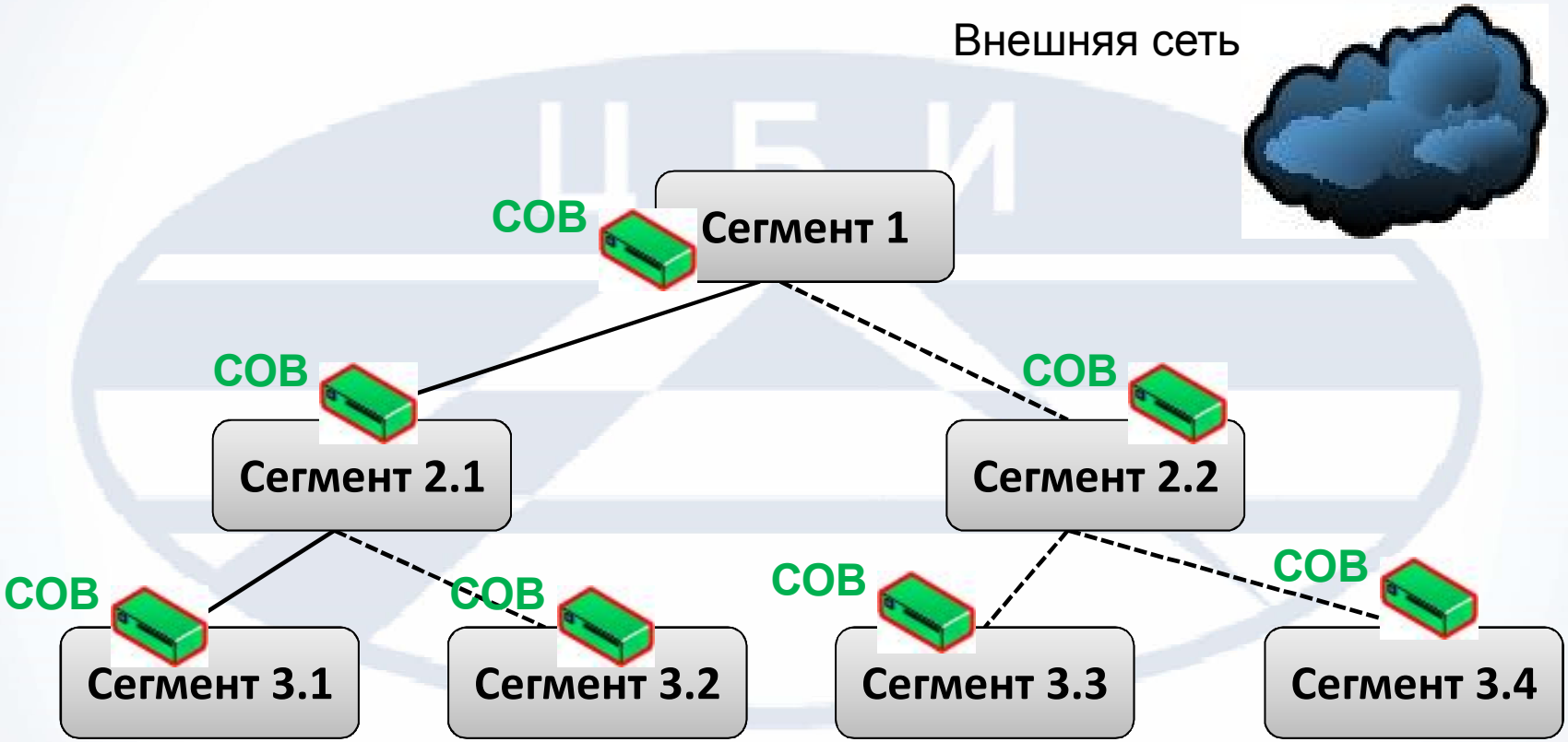
Адаптация

«Меры …»
(Пункт 2.3 б)

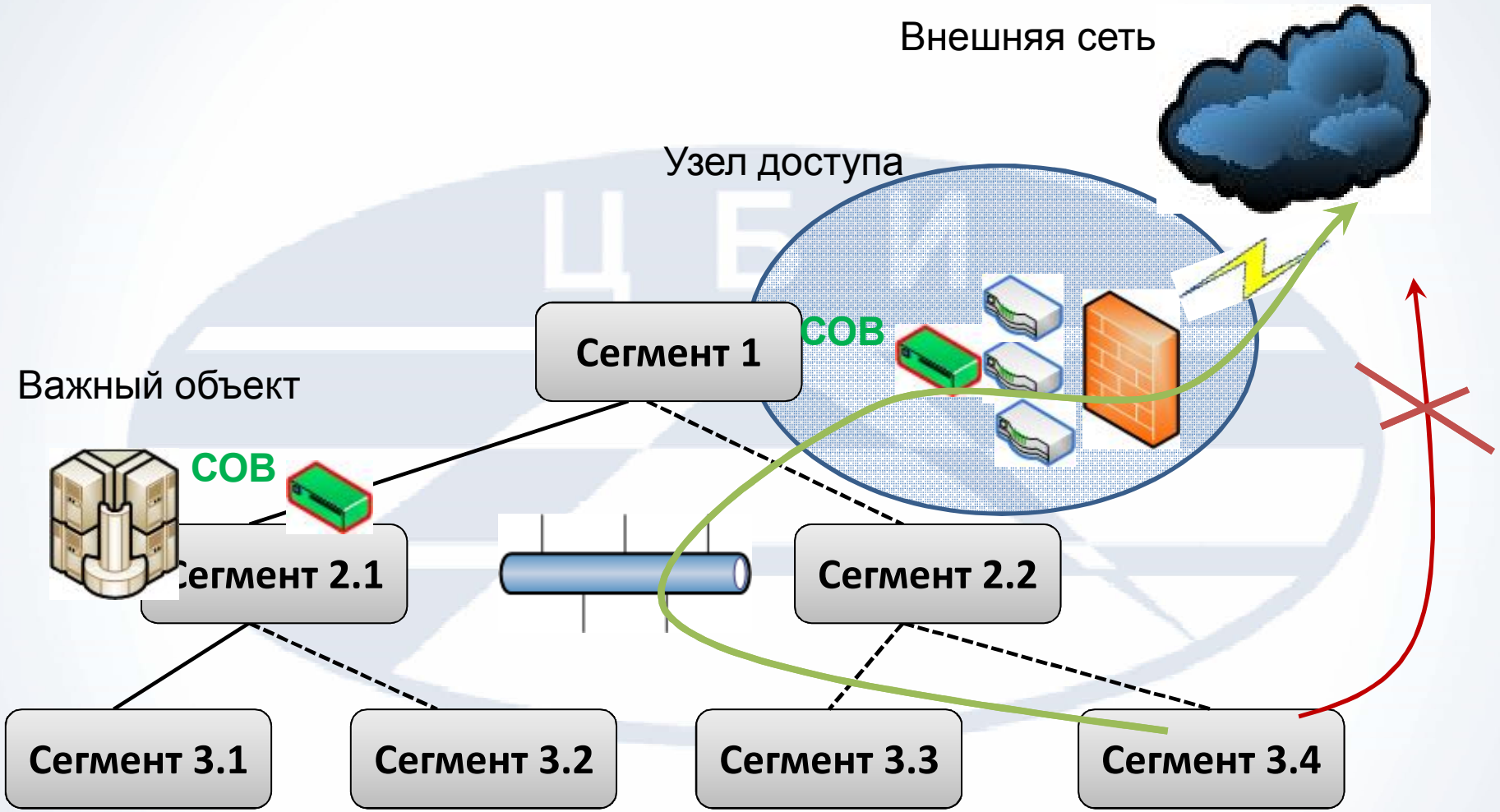
Компенсирующие меры

«Меры …»
(Пункт 2.3 д)

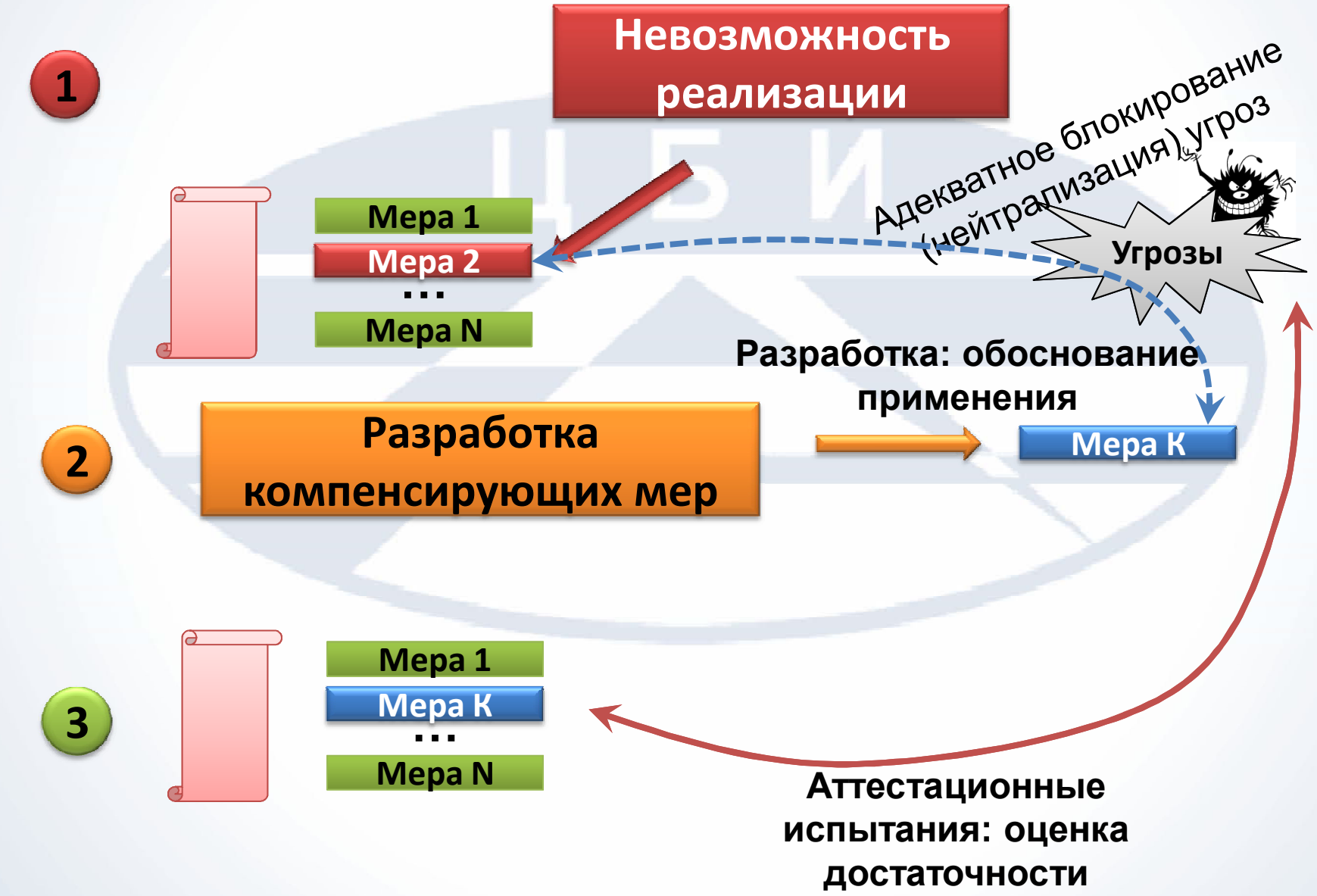
Пример: Обнаружение вторжений



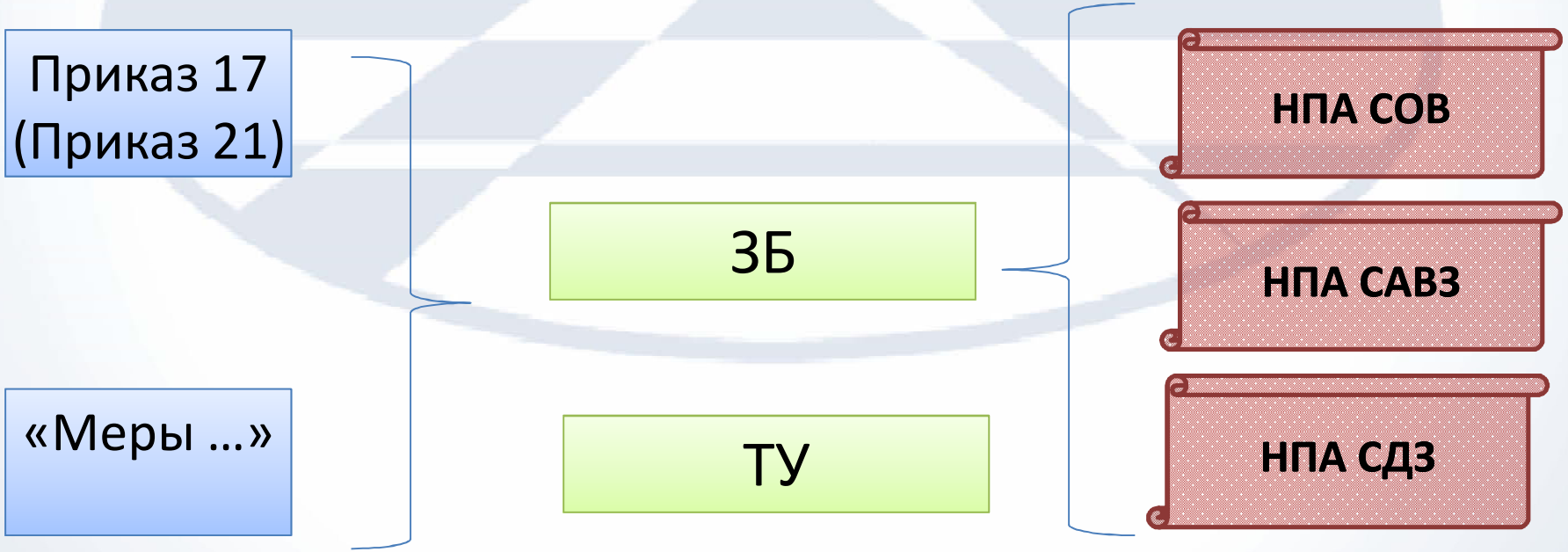
Пример: Обнаружение вторжений



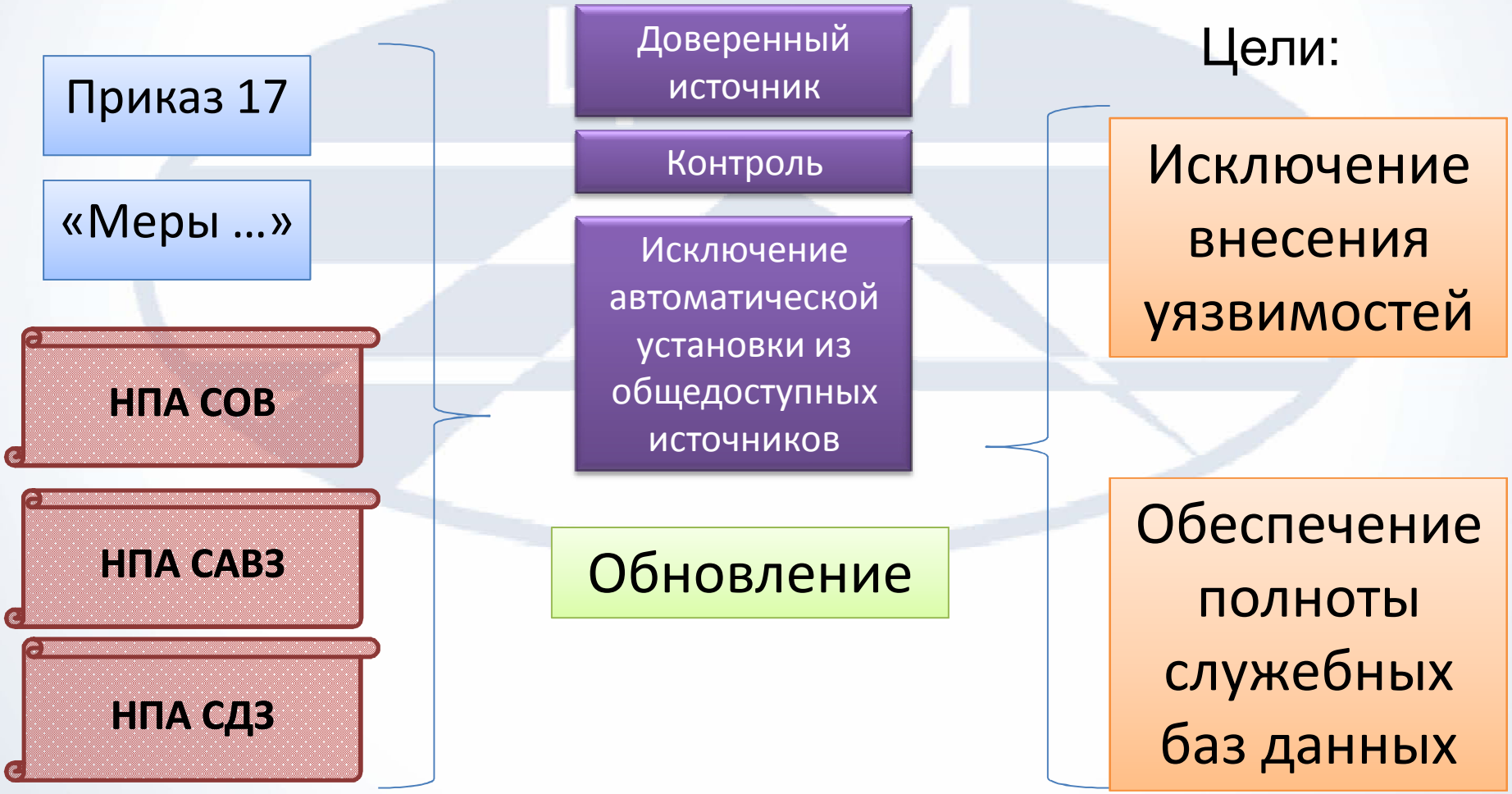
Использование компенсирующих мер ЗИ



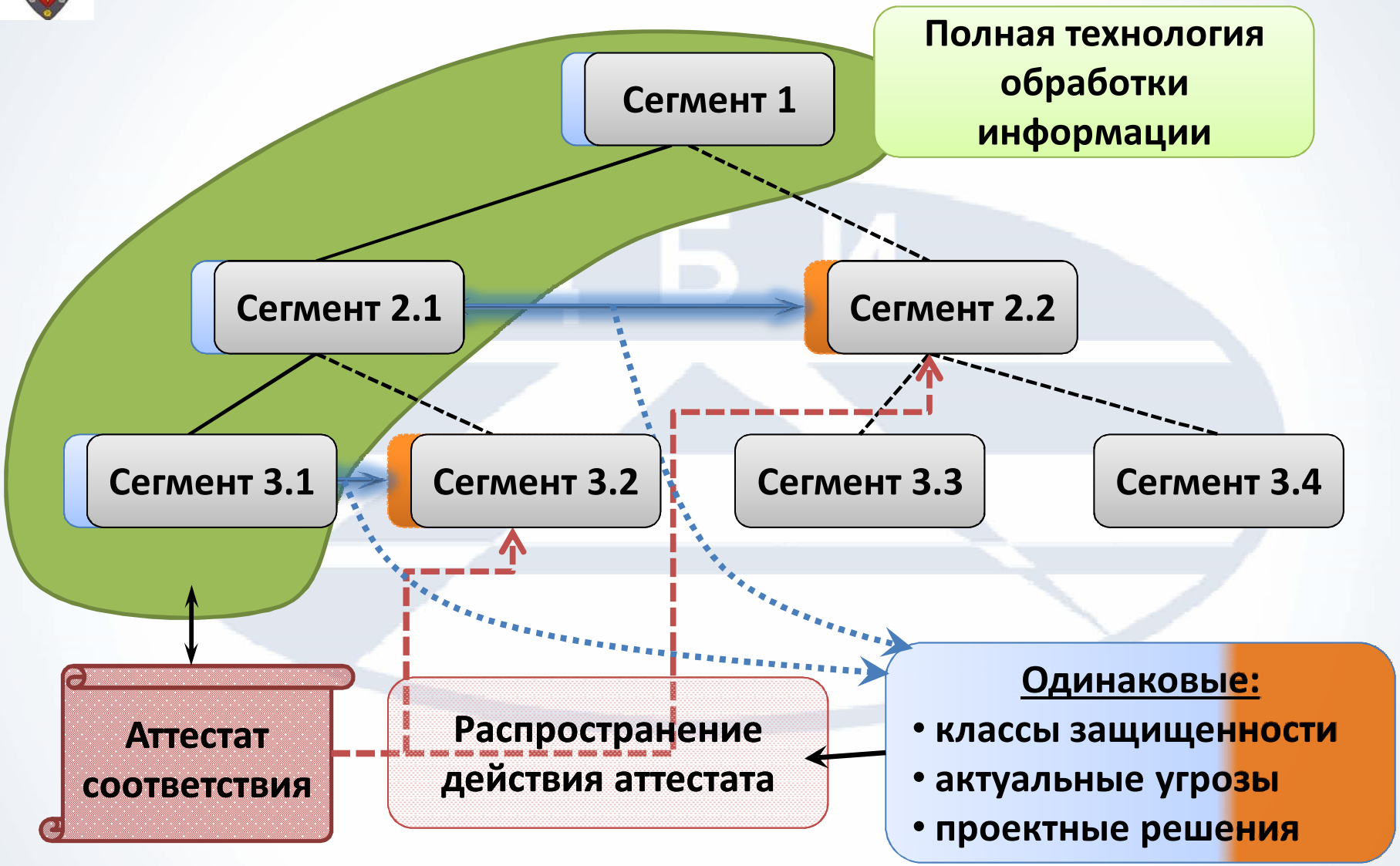
Как реализовать меры в условиях отсутствия на рынке сертифицированных средств защиты информации?



Как реализовать обновление средств ЗИ и ПО?



Аттестация информационной системы



Спасибо за внимание!

sidak@cbi-info.ru

НОУ «Учебный центр «ЦБИ»

141090, г. Юбилейный, Московской обл.,
ул. Ленинская, д. 4.

тел.: (498) 602 92 49 **факс: (495) 543 30 60, доб. 263**

http://www.cbi-info.ru **e-mail: edu@cbi-info.ru**

Дополнительная профессиональная программа повышения квалификации специалистов в области информационной безопасности

«Основы обеспечения защиты информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»