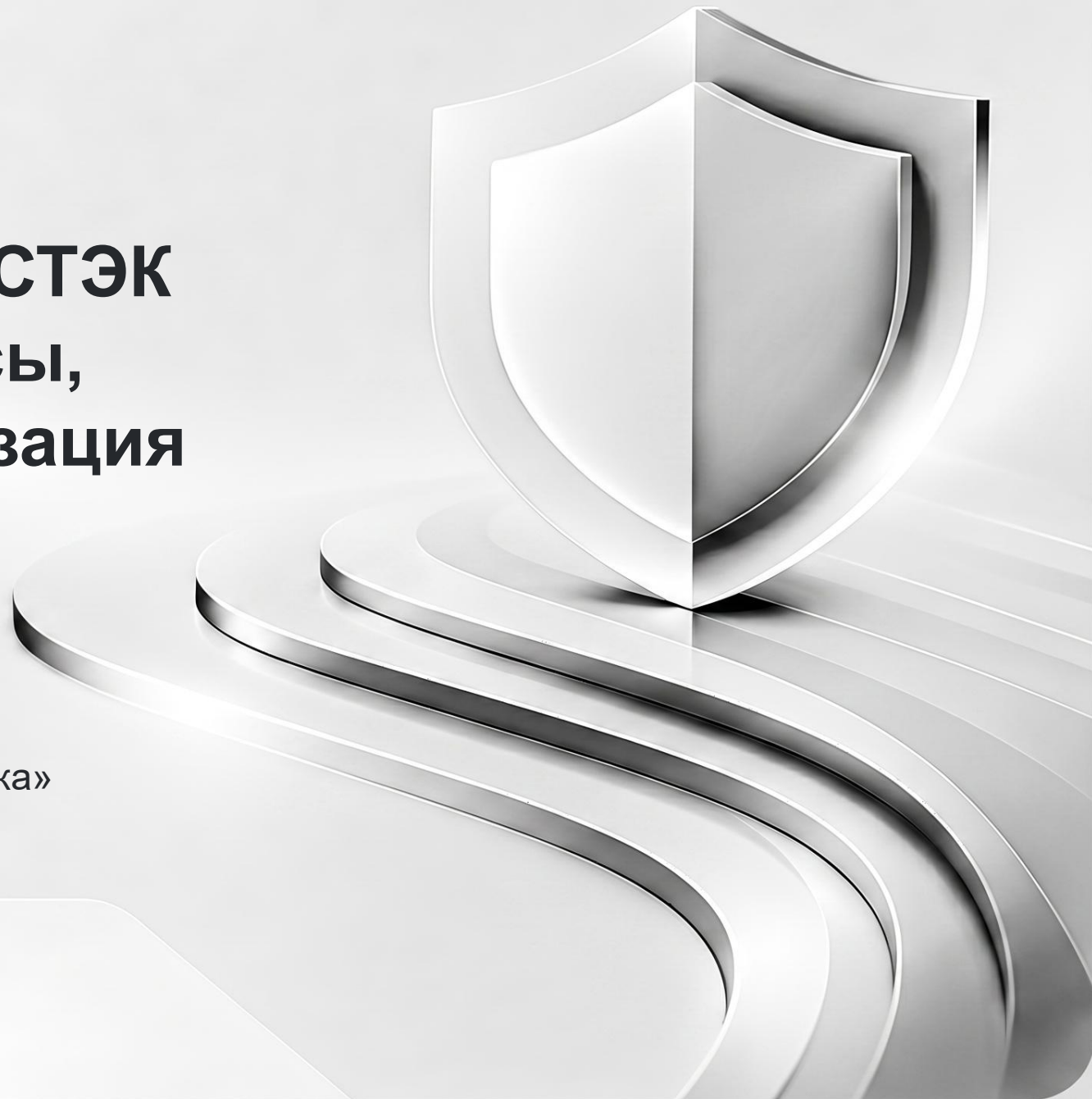


Аттестация по Приказу ФСТЭК № 117: практические кейсы, типовые ошибки и реализация защитных мер

Илья Романов

Руководитель отдела консалтинга АО «Диалог Наука»

Конференция АБИСС, 13 октября 2026 года



Зачем Приказ № 117 если у нас нет ГИС?

- Система, работающая с ГИС должна отвечать установленным требованиям защиты (149-ФЗ, ст. 14, ч. 8.1; Приказ № 117, п. 2).
- Нет подтверждения соответствия (аттестата) → риск отключения от ГИС, или в целом от СМЭВ.

Кстати: Методический документ по мерам защиты от 12 апреля 2026 г. уже сейчас применим для ЗОКИИ и ИСПДн

Что именно аттестовать?

- **Аттестуется система**, которая получает доступ к ГИС и осуществляет обмен данными.

Реализация в теории (простой контур):

— Адаптер доступа + криптошлюз — фактически единый «шлюз» для взаимодействия.

Реализация на практике (сложные контуры):

— Несколько ЦОД, распределённая инфраструктура

— Несколько серверов и криптошлюзов

— Рабочие станции, если они участвуют в процессе взаимодействия.

Оптимизация: до аттестации сократить реальные потоки данных и точки доступа.

Нужны ли сертифицированные средства защиты?

Приказ № 117, п. 71: «Для защиты информации должны применяться сертифицированные средства защиты информации».

Приказ № 117, п. 70 — «уровни» реализации СЗИ:

встроенные

- в аппаратное обеспечение;
- в системное ПО;
- в прикладное ПО;

наложенные

сетевые

Какая функция защиты требуется и каким сертифицированным средством она реализована?

Выбор мер: порядок действий

- 1** | **Базовый набор мер** — по классу защищённости ИС.
- 2** | **Адаптация** — с учётом архитектуры, технологий и особенностей функционирования.
- 3** | **Компенсирующие меры — при необходимости:** если выбранную меру невозможно реализовать в соответствии с требованиями, обосновываем замену и разрабатываем альтернативу.
- 4** | **Верификация адаптированного набора** — проверяем нейтрализацию угроз, при необходимости дополняем и (или) усиливаем меры.

Адаптация: когда меру можно исключить?

- Мера связана с технологией или свойством системы, которого нет.
- Пример: нет беспроводного доступа → меры защиты точек Wi-Fi неприменимы.
- Основание фиксируем в описании архитектуры и выборе мер.

Что делать, если меру не получается реализовать?

- «Это слишком дорого, даже дороже самой системы».
- «Это требует переработки топологии / архитектуры системы».
- «У нас старое несовместимое ПО и железо, поэтому меру не реализовать».

Что делать, если меру не получается реализовать?

Вредные советы (плохие обоснования):

- «Это слишком дорого, даже дороже самой системы».
- «Это требует переработки топологии / архитектуры системы».
- «У нас старое несовместимое ПО и железо, поэтому меру не реализовать».

Общий недостаток: не показано, что стало с актуальной угрозой.

Что учитывать при выборе мер?

Основание: методический документ ФСТЭК от 12.04.2026, приложение № 3 «Выбор мер защиты информации для реализации в информационной системе».

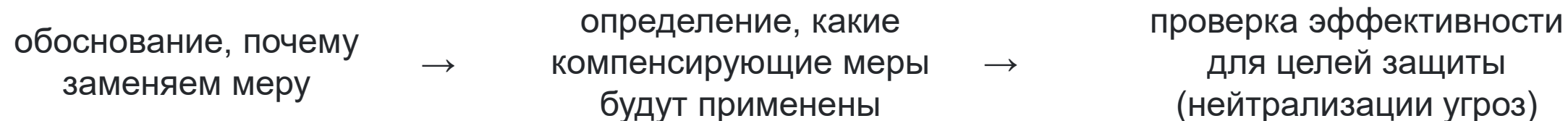
При выборе мер нужно учитывать:

- Класс защищённости.
- Угрозы безопасности информации.
- Структурно-функциональные характеристики ИС:
 - архитектуру, структуру и состав;
 - физические, логические, функциональные и технологические связи между сегментами;
 - связи с другими ИС и информационно-телекоммуникационными сетями;
 - режимы обработки информации в системе и её сегментах;
 - иные характеристики ИС, применяемые информационные технологии и особенности функционирования.

Подходы к замене мер «компенсирующими»

- Функция защиты нужна, но отдельный продукт не нужен — Иной способ реализации меры
- Требуемую меру объективно невозможно реализовать — Нужны компенсирующие меры

Для компенсации:



Кейс: виртуализация без отдельного средства ЗСВ?

- **Пример:** В системе применяется виртуализация.
 - **Инфраструктура:** Все системы виртуализации и виртуальные машины входят в единый аттестуемый контур.
 - **Доступы:** Рабочие места персонала и пользователей – в составе контура.
 - **Меры защиты:** Комплексная система защиты на разных уровнях (АРМ, сетевая безопасность, мониторинг, и т.д.)
- **Верификация:** Сопоставляем угрозы с защитными мерами (ключевое!)
 - **Решение:** Отдельное средство ЗСВ не применяем.
 - **Антипример (специальные средства ЗСВ могут быть нужны):** общая ферма ЦОД с чужими ВМ и разными администраторами.

Кейс: когда не требуются средства доверенной загрузки (СДЗ)?

- Проверяем, требуется ли **доверенная загрузка** именно для этого узла.
- Обеспечиваем ли защиту от угроз иными мерами (в том числе организационными)?
Если да – средство доверенной загрузки необязательно.
- **Антипример (СДЗ нужны):** Отдельные нормативные документы могут требовать применения СДЗ, например, в случае необходимости использования СКЗИ класса КС2 и выше.

Аттестат получен. Что дальше?

Периодический **контроль аттестованного объекта** — не реже одного раза в три года; отчёт направляют во ФСТЭК.

Изменения архитектуры, состава и средств защиты могут потребовать **дополнительных аттестационных испытаний**.

Границу объекта, угрозы и меры защиты пересматривают вместе с изменениями системы.

Спасибо за внимание

Вопросы?

