

Практические аспекты аттестации ЦОД по Приказу ФСТЭК № 117 для размещения ГИС

АНДРЕЙ РЯБОВ

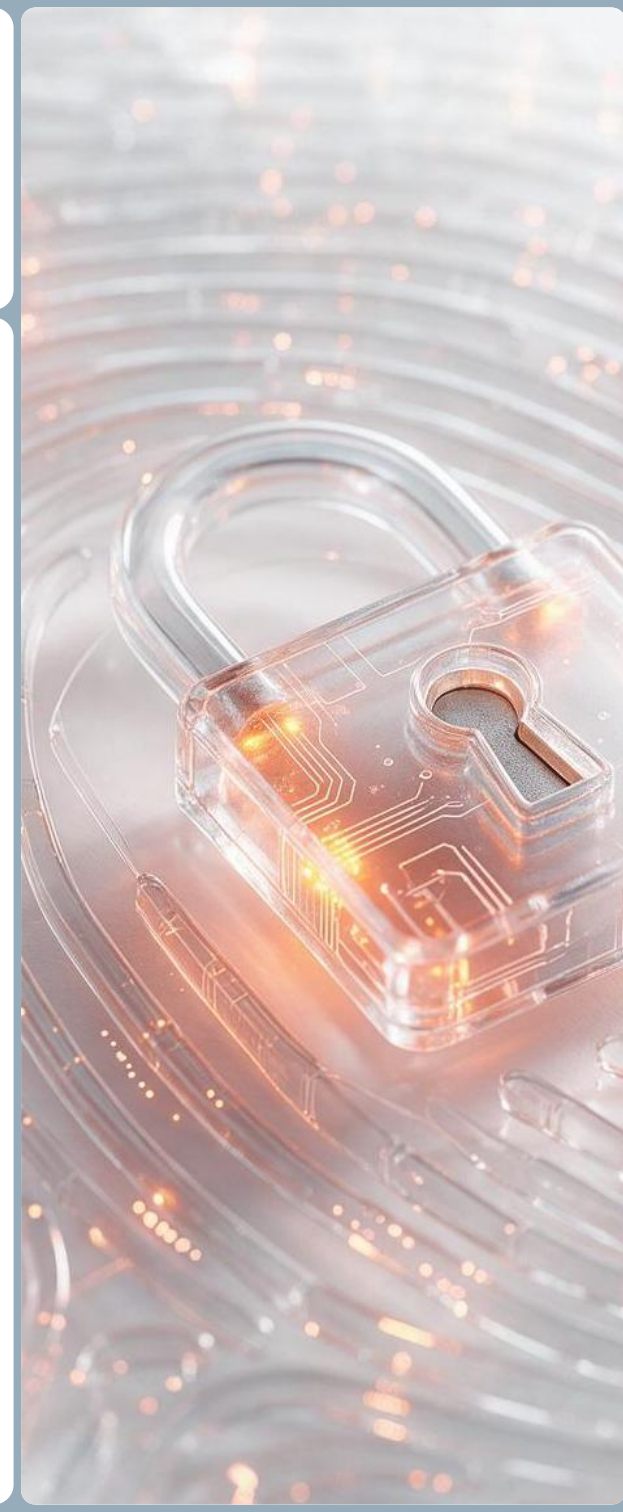
Руководитель группы по обеспечению
комплексной безопасности Angara Security





ПРЕИМУЩЕСТВА АТТЕСТОВАННЫХ ЦОД

- ✔ Требования к защите ГИС меняются из года в год на фоне растущих затрат на оборудование.
- ✔ Многим операторам становится невыгодно строить защищенную инфраструктуру самостоятельно.
- ✔ Альтернатива — разместить систему в уже аттестованном ЦОД, где значительная часть регуляторных требований выполнена на инфраструктурном уровне.
- ✔ Оператору ГИС не нужно самостоятельно строить весь защищенный инфраструктурный слой.
- ✔ Миграцию ИС с последующей аттестацией в аттестованное облако приказу №117 ФСТЭК России возможно реализовать значительно быстрее.



Аттестат на ГИС выдаётся только при наличии действующего аттестата на ЦОД, в котором она размещена



КАК БЫЛО РАНЬШЕ:

- Приказ 17 ФСТЭК
- П 17.6. ... Информационные системы, функционирующие на базе общей инфраструктуры (средств вычислительной техники, серверов телекоммуникационного оборудования) в качестве прикладных сервисов, подлежат аттестации в составе указанной инфраструктуры.
- В случае если информационная система создается на базе информационно-телекоммуникационной инфраструктуры центра обработки данных уполномоченного лица, такая инфраструктура центра обработки данных должна быть аттестована на соответствие настоящим Требованиям.
- При аттестации информационной системы должны использоваться результаты аттестации общей инфраструктуры оператора информационной системы. ...

ТЕКУЩИЕ ТРЕБОВАНИЯ:

- Приказ ФСТЭК № 117
- П 8. «Функционирование ИС на базе информационно-телекоммуникационной инфраструктуры допускается при условии защиты информационно-телекоммуникационной инфраструктуры в соответствии с **Требованиями**.»
- 65. «С целью подтверждения достаточности принятых мер защиты ИС и содержащейся в них информации до начала обработки и (или) хранения информации в ГИС должна быть проведена их **аттестация**»

Основные этапы создания аттестованного ЦОД

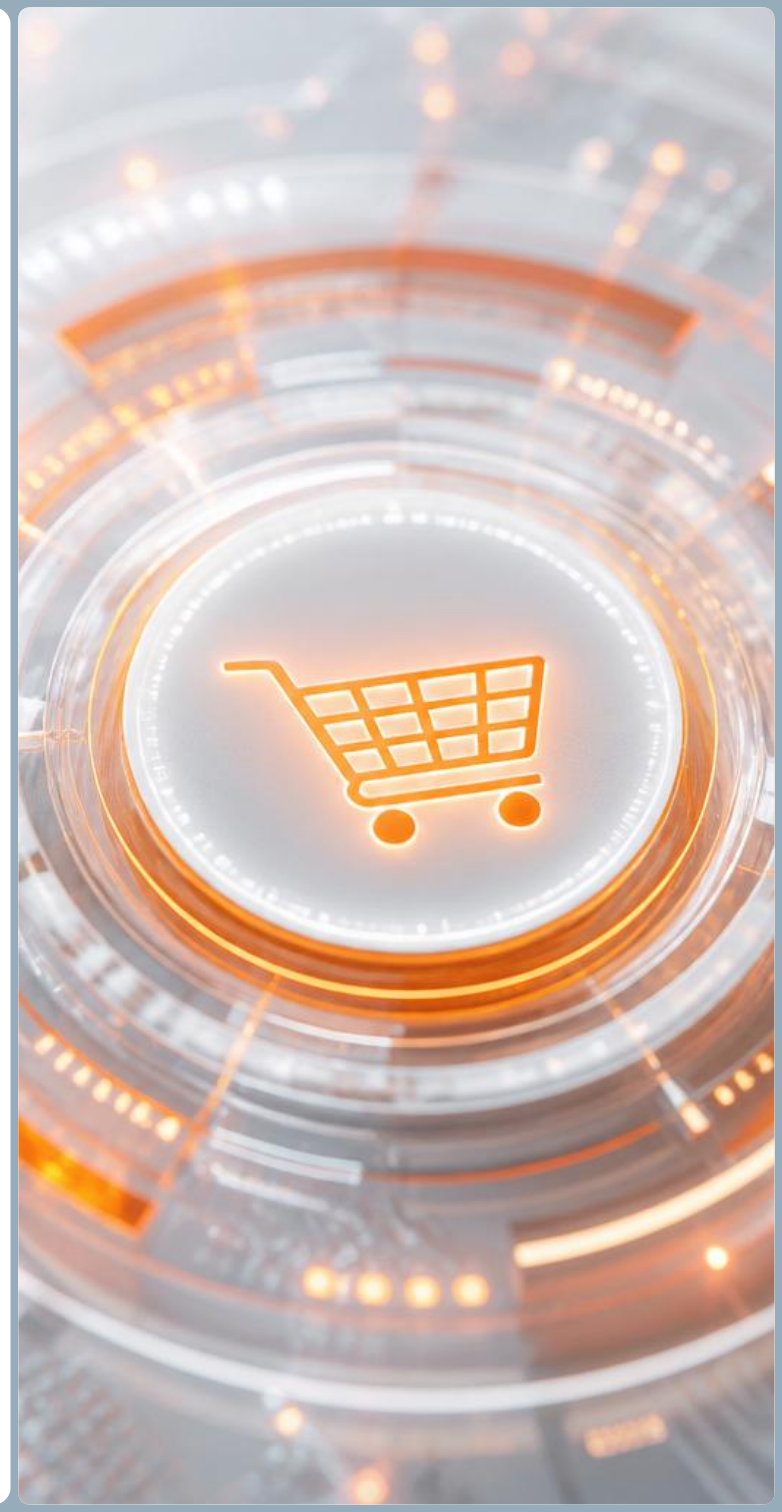


- ЭТАП 1.** Определение сегмента ЦОД для предоставления услуг по размещению ГИС;
- ЭТАП 2.** Формирование требований к СЗИ сегмента ЦОД (Модель угроз, Частное техническое задание на СЗИ сегмента ЦОД);
- ЭТАП 3.** Техническое проектирование СЗИ сегмента ЦОД (разработка технического проекта);
- ЭТАП 4.** Разработка организационно-распорядительной документации по защите информации;
- ЭТАП 5.** Ввод в действие СЗИ сегмента ЦОД (внедрение и настройка СЗИ и механизмов защит в ПО, процессы ИБ);
- ЭТАП 6.** Анализ защищенности сегмента ЦОД по Методикам ФСТЭК России;
- ЭТАП 7.** Аттестация сегмента ЦОД по требованиям безопасности.



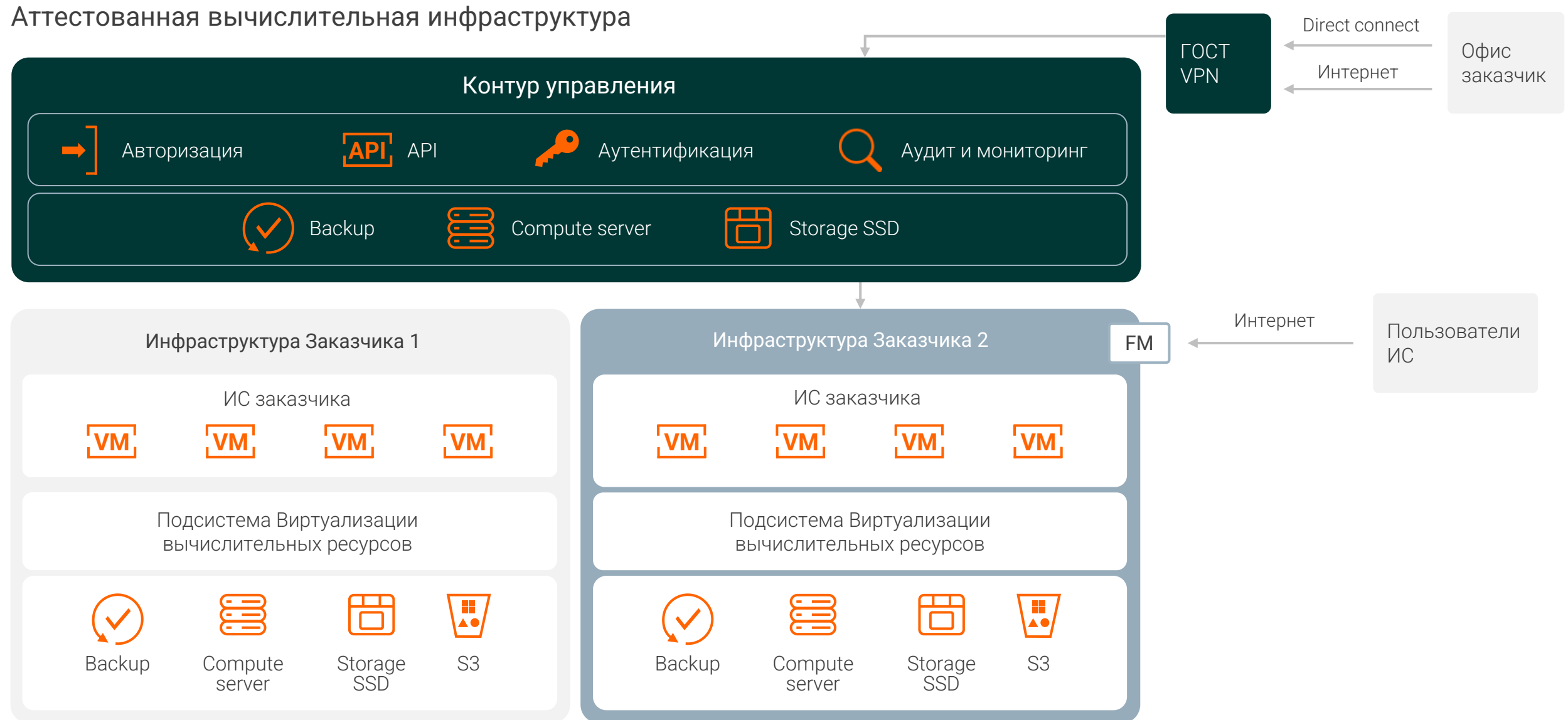


Акцентируем внимание
на основных моментах,
а именно, что стоит
учесть в рамках подготовки
сегмента ЦОД к аттестации



Типовая архитектура аттестованного ЦОД

Аттестованная вычислительная инфраструктура





Разграничение зон ответственности между оператором ГИС и поставщиком услуг (ЦОД)

Перенос ГИС в аттестованный ЦОД не означает, что ГИС автоматически получает аттестат.

Если, например, посмотреть на классическую модель IaaS, которую наиболее часто используют для размещения ресурсов, то:

ЦОД отвечает за защищенность инфраструктурного слоя:

- физические вычислительные ресурсы;
- платформу виртуализации;
- систему хранения данных
- сетевую инфраструктуру (включая межсетевые экраны и криптографические средства).

Оператор ГИС отвечает за сервисы внутри своей информационной системы (то, что лежит поверх облачного аттестованного слоя, внутри VM):

- приложения,
- данные;
- связующее ПО,
- среда исполнения;
- операционная система.



Что стоит учесть в рамках подготовки СЗИ сегмента ЦОД

- Класс, на который будет аттестован ЦОД — не ниже класса размещаемых ГИС (целесообразно К1 по Приказу № 117).
- Только сертифицированные ФСТЭК России средства защиты информации, ОС, ВИ (если сегмент под ИС К1, то СЗИ не ниже 4 класса и 4 уровня доверия).
- Для защиты каналов используем криптошлюзы и сервера доступа, сертифицированные ФСБ России (с учётом Модели угроз, в которой определяем уровень криптографической защиты информации).
- Учитываем наличие ПО (ОС, виртуализация СУБД, прикладное ПО) с End of Life.



Управляемые сервисы для ГИС в рамках сегмента ЦОД



- Если для размещения ГИС помимо модели IaaS, оператором ЦОД предоставляются дополнительные управляемые сервисы по подписке, данные сервисы должны быть также аттестованы на соответствие требованиям по безопасности информации.
- К таким сервисам относятся:
- *PaaS*:
 - сервисы управления облачными базами данных PostgreSQL,
 - Kubernetes as a Service в облаке для быстрого и надёжного развертывания приложений.
- *SecaaS*:
 - 2 FA,
 - Межсетевой экран следующего поколения;
 - WAF
 - и т.д.



Безопасная разработка ПО



- Если провайдер облачных услуг самостоятельно разрабатывает ПО для ЦОД (например, консоли управления, сервисы), он обязан внедрить процессы безопасной разработки.
- П. 14д Приказа № 117 — организация деятельности по защите информации должна включать разработку и утверждение внутренних регламентов, содержащих порядок разработки безопасного ПО в случае его самостоятельной разработки.
- П. 50 Приказа № 117 — мероприятия по разработке безопасного ПО направлены на предотвращение появления, выявление и устранение уязвимостей в разрабатываемом ПО.
- ГОСТ Р 56939-2024 (разделы 4 и 5) — обязательный стандарт при самостоятельной разработке. Описывает 25 процессов безопасной разработки (РБПО).





Анализ защищенности сегмента ЦОД по Методикам ФСТЭК России

- В рамках аттестации выполняется анализ защищённости с учетом Методического документа ФСТЭК России «Методика анализа защищенности информационных систем» (утв. от 25 ноября 2025 года).

Процедура включает:

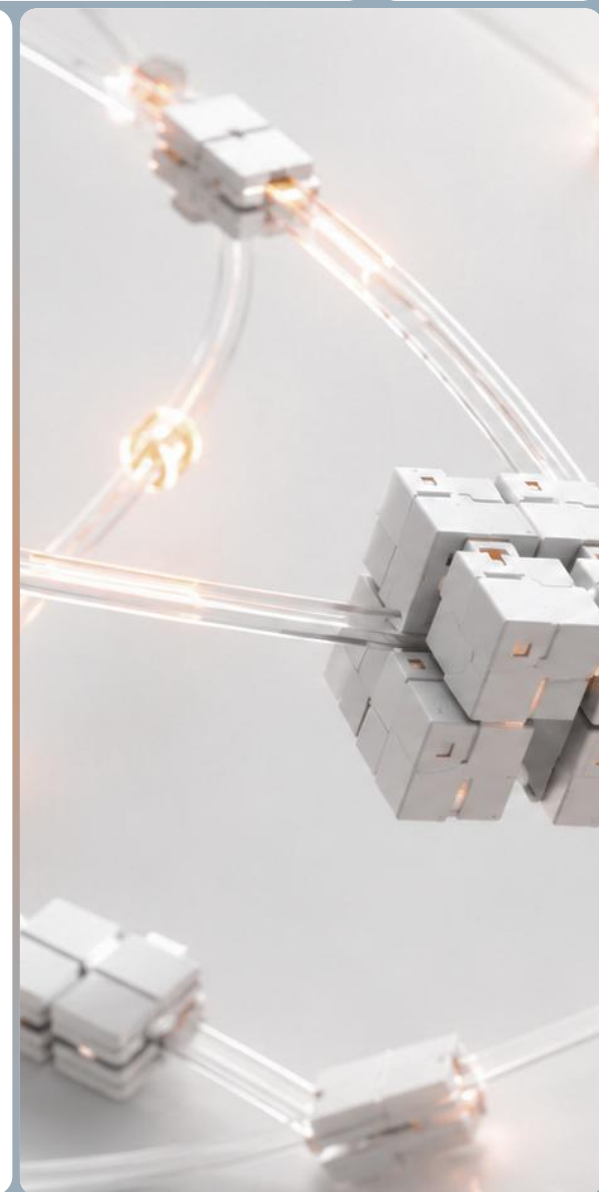
- Инвентаризация ИС (сетевые адреса/порты, ПО, СЗИ, пользователи).
- Внешний анализ уязвимостей: Сканирование периметра ИС из сети Интернет.
- Внутренний анализ уязвимостей: Сканирование изнутри периметра (внутренняя инфраструктура).
- Оценка выявленных уязвимостей: Экспертная оценка критичности на основе угроз.
- Устранение выявленных уязвимостей.
- Повторное сканирование.
- Подготовку отчета.

Анализ защищенности по Методике может проводить как оператор ИС, так и лицензиат ФСТЭК

Анализ защищенности сегмента ЦОД по Методикам ФСТЭК России



- Тестирование на проникновение (пентест) проводится по «Методике испытаний систем защиты информации информационных систем методами тестирования на проникновение». Соответствующее информационное сообщение № 240/24/4734 было опубликовано 8 сентября 2025 г.
- Методика становится обязательной для систем 1 и 2 классов защищенности, которые имеют подключение к сети Интернет и (или) взаимодействуют с **иными ИС**, в том числе с ИС подрядных организаций (за исключением случаев, когда такое взаимодействие реализовано с использованием VPN ГОСТ (с применением сертифицированных СКЗИ)).
- Пентест по Методике может проводить как оператор ИС, так и лицензиат ФСТЭК.
- Пентест проводится как завершающий этап после анализа уязвимостей.



Аттестация сегмента ЦОД по требованиям безопасности



- Работы проводятся в соответствии с Приказом ФСТЭК № 77.
- Аттестат соответствия выдается на весь срок эксплуатации объекта информатизации.
- Проведения периодического контроля уровня защиты информации – раз в 3 года.
- В случае модернизации/развития ЦОД проводятся **дополнительные аттестационные испытания.**



Основные сложности, с которыми сталкиваются ЦОД при аттестации



- Использование ПО с End-of-life.
- Создание или модернизация вычислительной инфраструктуры ЦОД идет отдельно от создания/модернизации СОИБ. Создание СОИБ создается позднее, что иногда влечет корректировки в саму инфраструктуру.
- Неверный скоуп аттестации. Например, «за бортом» остаются сервисы СОИБ, которые должны входить в состав аттестованного сегмента ЦОД.





СПАСИБО ЗА ВНИМАНИЕ!



БЦ «Парк Победы», Москва,
ул. Василисы Кожиной, д.1 к.1



info@angarasecurity.ru



+7 (495) 269 26 06



angarasecurity.ru

