национальный аттестационный центр

Головная боль по-новому: как пройти аттестацию по изменившимся правилам и не сойти с ума

Национальный аттестационный центр

21 год успешной работы компании на рынке аттестационных услуг

Осуществление деятельности на основании лицензий **ФСБ России и ФСТЭК России**

Успешно реализованные проекты:

О чем будем говорить?

01 Аттестация по новым требованиям

02 Эксплуатация аттестованных объектов информатизации

03 Внесение изменений и модернизация без потери аттестата соответствия

Проблематика

- Обилие изменений в нормативных актах
- Эксплуатация аттестованного объекта – это не статика, а непрерывный процесс
- По данным ФСТЭК России **≈30% инцидентов** происходят из-за ошибок после аттестации

Аттестация по новым требованиям

Приказы:

- **Приказ ФСТЭК России от 11.04.2025 г. № 117**

Требования о защите информации в ГИС и иных ИС государственных органов, унитарных предприятий, учреждений
(замена Приказа ФСТЭК России от 11.02.2013 № 17)

- **Приказ ФСБ России от 18.03.2025 г. № 117**

Требования о защите информации, содержащейся в ГИС и иных ИС государственных органов, унитарных предприятий, учреждений, с использованием СКЗИ
(отмена Приказа ФСБ России от 24.10.2022 г. № 524)

Аттестация по новым требованиям

Методики:

- **Методический документ ФСТЭК России от 25.11.2025 г.**

«Методика анализа защищенности информационных систем»

- **Методический документ ФСТЭК России от 25.06.2025 г. (дсп)**

«Методика испытаний систем защиты информации систем методами тестирования на проникновение»

- **Методический документ ФСТЭК России от 12.04.2026 г.**

«Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» (замена методического документа с мерами защиты ГИС от 11.02.2014)

При аттестационных испытаниях проводятся

- **анализ уязвимостей**
- испытания путем осуществления попыток несанкционированного доступа (воздействия) **в обход системы защиты** информации

(Приказ ФСТЭК России от 29.04.2021 г. № 77, п. 16, подп. «б»)

Аттестация по новым требованиям

Краткий обзор основных изменений 117 Приказа

01 **Расширение охвата** – ГИС, а также иные ИС государственных органов, унитарных предприятий, учреждений и муниципальные ИС

02 **Документация** – Политика – Стандарты – Регламенты

03 **Взаимодействие с подрядчиками** – появление требований к подрядчикам

Аттестация по новым требованиям

Краткий обзор основных изменений 117 Приказа

04 **Организационные меры** – пометка «ДСП» = УЗ1 = К1, масштаб ИС, количественный показатель персонала ИБ

05 **Технические меры** – 17 групп мер, в том числе требования защиты среды контейнеризации, веб-технологий и API, конечных устройств, интернет вещей

06 **Искусственный интеллект** – появление требований к технологиям ИИ

Аттестация по новым требованиям

Краткий обзор основных изменений 117 Приказа

07 **Безопасная разработка ПО** – привлекать специалистов по защите информации к приемке результатов разработки

08 **Контроль, мониторинг** – показатели Кзи и Пзи, сроки устранения уязвимостей, частота контроля защищённости не реже 1 раза в 3 года.

Кзи - показатель защищенности

Пзи - показатель зрелости

Аттестация по новым требованиям

Что делать и куда бежать?

- **Информационное сообщение ФСТЭК России от 12.03.2026 № 240/22/1492:**
- Аттестаты выданные по 17 Приказу действуют, их действие не прекращается, можно проводить периодический контроль
- Работы по договорам заключенным до 01.03.2026 могут быть проведены по 17 Приказу
- При модернизации объектов аттестованных по 17 Приказу есть возможность провести дополнительные аттестационные испытания и переоформить аттестат по 117 Приказу
- Разработка плана перехода на соответствие новым требованиям 117 Приказа

Аттестат соответствия выдается на **весь срок эксплуатации** объекта информатизации (Приказ ФСТЭК России от 29.04.2021 г. № 77, п. 31)

Аттестация по новым требованиям

Какие еще есть нюансы?

- Класс ИС, функционирующей на базе аттестованной информационно-коммуникационной инфраструктуры (ЦОД), не может быть выше класса самого ЦОД
- ИС, аттестованные по 117 Приказу, не могут быть размещены в ЦОД, который аттестован по 17 Приказу

Эксплуатация аттестованного объекта

Жизненный цикл

Проектирование и создание

Аттестация

Эксплуатация и поддержание соответствия

Переаттестация или вывод из эксплуатации

На что стоит обратить внимание?

- Изменения требований регуляторов
- Анализ угроз и уязвимостей, мониторинг
- Обновление программного обеспечения (ПО) и средства защиты информации (СЗИ)
- Актуализация документации
- Обучение сотрудников
- Периодический контроль

Анализ угроз и уязвимостей, мониторинг

- Банк данных угроз (БДУ) ФСТЭК России – bdu.fstec.ru
- Актуализация модели угроз («Методика оценки угроз безопасности информации» ФСТЭК России от 05 февраля 2021 г.)
- Наличие SOC и использование SIEM и EDR

Сроки устранения уязвимостей:

- Критические – **24 часа**
- Высокие – **7 дней**
- Средние и низкие – **внутренние регламенты**

(изм. Приказа ФСТЭК России от 11.04.2025 г. № 117)

Обновление ПО и СЗИ

Где отслеживать необходимость обновления?

- Сайты БДУ ФСТЭК России и вендоров
- Реестры сертифицированных СЗИ ФСТЭК России и ФСБ России

Как производить обновление?

1. Обращение к вендору в рамках тех. поддержки
2. Получение установщика и документации
3. Обновление
4. Документирование

Не стоит забывать про:

- обновление антивирусных баз, базы сигнатур для СОВ и т.д.
- создание расписания на запуск задач по обновлению

Актуализация документации

- Ведение технического паспорта:
  - сведения о периодических контролях (раздел 5)
  - лист регистрации изменений (раздел 6) (Приказ ФСТЭК России № 77 Приложение 1)
- Актуализация матрицы доступа или перечня лиц, допущенных к информационным ресурсам
- Изменения в иные документы:
  - приказы, политики, регламенты, инструкции

Структурированный перечень документации:

Политика – Стандарты - Регламенты

(изм. Приказа ФСТЭК России от 11.04.2025 г. № 117)

Обучение сотрудников

Регулярная работа с сотрудниками:

- ☑ внешнее и внутреннее обучение
- ☑ тестирование знаний

не менее 30%
сотрудников

подразделения по защите информации должны иметь
профильное ИБ-образование
или профпереподготовку

Периодический контроль

Было: для аттестованных по требованиям Приказа **№ 17**:

- К1 - не реже 1 раза в год
- К2, К3 - не реже 1 раза в два года

Стало: унифицированный подход **для всех классов**:

- Не реже 1 раза в 3 года или после инцидента

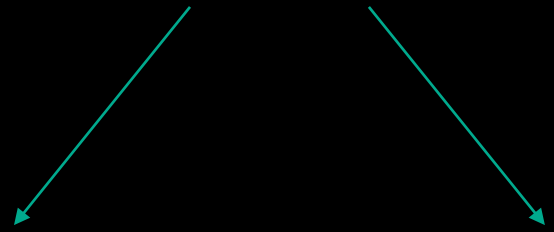
Необходимость регулярных оценок с отчетом во ФСТЭК:

- Кзи – **1 раз в полгода**
- Пзи – **1 раз в 2 года**

(изм. Приказа ФСТЭК России от 11.04.2025 г. № 117)

Модернизация аттестованных систем

2 сценария:
(Приказ ФСТЭК России № 77, пункт 33)



Дополнительные
аттестационные испытания

Повторные
аттестационные испытания

Модернизация аттестованных систем

Что можно запланировать уже сейчас?

- Разработать новый комплект документации: **политика, стандарты, регламенты**
- Провести оценку показателя защищенности **(КЗИ)**
- Подготовить или нанять персонал **с профильным образованием** в сфере ИБ
- Разработать **план перехода** на соответствие новым требованиям 117 Приказа
- Проработать вопросы **взаимодействия с подрядчиками**, у которых имеется удаленный доступ в ИС
- **Увеличение сроков** проведения работ

Почему не стоит формально подходить к вопросам эксплуатации аттестованного объекта?

- Финансовые риски и штрафы
- Риск приостановки аттестата соответствия или его аннулирование
- Репутационные риски

аттестат – это только начало

- Аттестат не является гарантом безопасности на весь срок эксплуатации системы
- Обеспечение безопасности аттестованного объекта – это непрерывный процесс
- Периодический контроль можно проводить чаще, чем требует регулятор

национальный аттестационный центр

спасибо за внимание

Артём Алексеев

заместитель начальника отдела
защиты информационных систем