**Инструкция для ИТ-службы: как выполнить требования приказа ФСТЭК № 117**

Кому: руководителю ИТ-службы, инженеру по защите информации
Документ: приказ ФСТЭК от 11.04.2025 № 117
Действует с: 1 марта 2026

Что изменилось.

Установлены новые требования к защите информации в государственных информационных системах. Требования распространяются на все клиники, работающие с ОМС (через интеграцию с ЕГИСЗ).

Какие показатели нужно рассчитывать.

| Показатель | Периодичность оценки | Ответственный |
|---|---|---|
| Показатель защиты информации значимых объектов критической информационной инфраструктуры (КЗИ) | Не реже 1 раза в 6 месяцев | Инженер по защите информации |
| Показатель уровня зрелости информационной безопасности (ПЗИ) | Не реже 1 раза в 2 года | Руководитель ИТ-службы |

Где смотреть методику расчета.

Методика расчета показателей утверждена отдельным документом ФСТЭК от 02.05.2024. Документ есть в открытом доступе. Основные параметры:

- для КЗИ оцениваем: защищенность каналов связи, разграничение доступа, антивирусную защиту, регистрацию событий;

- для ПЗИ оцениваем: полноту организационно-распорядительной документации, регулярность обучения персонала, наличие средств защиты, реагирование на инциденты.

Что делаем в марте.

Этап 1. Ревизия документации.
Проводим учет организационно-распорядительной документации по информационной безопасности. Проверяем, какие требования из приказа № 117 уже выполнены в рамках:

- приказа ФСТЭК № 21 (защита персональных данных);
- приказа ФСТЭК № 31 (критическая инфраструктура);
- внутренних политик безопасности.

Этап 2. Расчет показателей.
Рассчитываем текущие значения КЗИ и ПЗИ по методике. Фиксируем результаты в служебной записке.

Этап 3. Планирование.
Если значения ниже нормативных, составляем план мероприятий по их повышению с указанием сроков и ответственных.

Результат работы:

1. Акт ревизии документации.
2. Расчет КЗИ и ПЗИ на текущую дату.
3. План мероприятий (при необходимости).