



АБИСС

Зрелость в цифрах

что показывает методика ФСТЭК,
и что остаётся за рамками оценки

Алексей Орехов

Руководитель производственно-технологического
управления НТЦ «Вулкан»

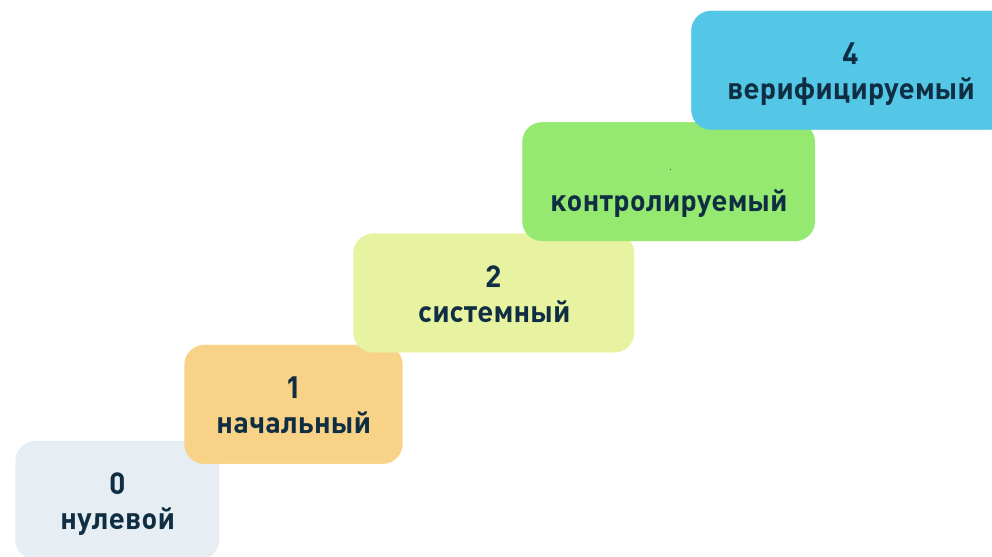
Методика ФСТЭК: для кого и зачем

Методика предназначена для оценки зрелости деятельности в области защиты информации и обеспечения безопасности значимых объектов КИИ. Она может применяться операторами, подрядчиками и заказчиками работ и услуг.

Оценка может проводиться самостоятельно или с привлечением внешней организации. Внешняя оценка повышает объективность результата за счёт независимости.

Ключевой вопрос

Оценка отвечает прежде всего на вопрос «насколько зрелой является деятельность по защите информации», а не напрямую на вопрос «может ли организация противостоять конкретной атаке».



Шкала зрелости

Что именно оценивает Методика

Оценка строится по 21 направлению деятельности по 8 критериев в каждом : от организации и управления, управления уязвимостями и обновлениями до мониторинга ИБ, безопасной разработки, взаимодействия с подрядчиками и контроля уровня защищённости.

Объект оценки — не отдельные средства защиты и не инфраструктура сама по себе, а то, насколько системно организованы соответствующие процессы и мероприятия.



Как проводится оценка

Оценка начинается со сбора подтверждающих данных: внутренних документов и регламентов, отчётов, результатов предыдущих проверок, интервью с сотрудниками, наблюдения за работой персонала и средств защиты, результатов инструментального анализа и мониторинга.

Что проверяем

исходные данные и
область оценки

Чем подтверждаем

8 видов требований:
документирование, выполнение,
инструменты, квалификация, контроль,
обучение, аудит, актуализация

Как получаем уровень

вес критерия × степень
выполнения → уровень
направления → профиль
зрелости

Методика проверяет не только наличие документа, но сразу несколько признаков зрелого процесса.

Расчёт зрелости: пороги важнее простой суммы

Оценка складывается из взвешенных требований, но для каждого уровня установлены обязательные минимумы по отдельным критериям.

1

Начальный

Документирование + выполнение + инструменты

2

Системный

Также квалификация и контроль



Контролируемый

Полное документирование, выполнение и контроль;
обучение

4

Верифицируемый

Дополнительно полный аудит и актуализация

Важно: одинаковый уровень не означает, что все критерии набраны одинаково. Но обязательные пороги нельзя компенсировать баллами по другим требованиям.

Основание: Методика ФСТЭК, таблицы 2–3; модель интерпретации, не расчёт конкретного объекта.

Одинаковая зрелость ≠ одинаковая эффективность

Одинаковая оценка «частично выполнено» может скрывать принципиально разный масштаб внедрения и охват активов.

Организация А

1 / 1 000

защищён 1 компьютер из 1 000

Организация Б

900 / 1 000

защищены 900 компьютеров из 1 000

Вопрос к интерпретации критерия: где проходит граница «частичного выполнения»?

Два ошибочных суждения: «все типы СрЗИ есть → мы зрелые» и «средств мало → мы незрелые». Число продуктов не заменяет оценку применимых процессов и их фактической реализации.

Синтетический пример для обсуждения критерия «выполнение», а не готовый результат оценки ФСТЭК.

Зрелость ≠ состояние защищённости

Методика оценивает зрелость деятельности по защите информации: насколько процессы описаны, выполняются, контролируются, поддерживаются инструментами, обеспечены компетенциями и совершенствуются.

**Насколько хорошо
организована деятельность
по защите?**



**Насколько хорошо
мы защищены
прямо сейчас?**

Итоговый уровень зрелости сам по себе не является оценкой фактического состояния защищённости конкретной инфраструктуры.

Методика описывает «что» организовано и подтверждено, но не исчерпывает вопрос «как» это работает на конкретных активах.

Методика отвечает на «что», но не полностью на «как»

Что можно подтвердить оценкой

- Наличие и документирование процесса
- Выполнение и контроль
- Компетенции, инструменты, аудит
- Динамику зрелости и зоны роста

Какие вопросы остаются

- Достаточен ли фактический охват?
- Адекватны ли способ и частота работ?
- Нейтрализуются ли актуальные угрозы?
- Снижается ли риск на важных активах?

Профиль зрелости помогает решить, где необходимо улучшение. Чтобы выбрать, как именно его реализовать, нужны контекст системы, оценка рисков и дополнительные критерии эффективности.

Пример: наличие централизованного сбора событий ещё не доказывает полноту сценариев обнаружения.

От балла к плану развития

После расчёта начинается наиболее полезная для организации часть оценки: переход от общего показателя к конкретным управленческим решениям.



Профиль отвечает, ГДЕ улучшать. Выбор способа реализации требует анализа активов, угроз, качества мер и ресурсов.

А всё ли так страшно?

Критерий Методики	ЗОКИИ · приказ ФСТЭК № 29	ГИС · приказ ФСТЭК № 117
Документирование	Приложение: ИАФ.0, АУД.0, ИПО.0 — регламентация; п. 13 — ОРД при эксплуатации.	Пп. 14–15 — политика ЗИ; пп. 25–26 — внутренние стандарты, регламенты и доведение.
Выполнение	П. 13 (а–з) — мероприятия в эксплуатации; приложение: АУД.2, АУД.4, АВЗ.1 — реализуемые меры.	П. 28 (б), п. 34 — проведение мероприятий; п. 38 — выявление и устранение уязвимостей.
Инструменты	Приложение: АУД.4 (регистрация событий), АУД.7 (мониторинг), АВЗ.1 (антивирусная защита).	П. 23 — программные и программно-аппаратные средства; пп. 70–71 — технические меры и СрЗИ.
Квалификация	П. 13.1 — ответственные за реагирование; п. 13.7 (в) — обучение работе со СрЗИ. Прямой аналог оценки компетенций — не полный.	П. 20 — компетенции работников ЗИ; ≥30% профильное образование / профпереподготовка.
Контроль	П. 13.8 (а–г) — анализ защищённости, оценка подсистемы безопасности; АУД.10 — внутренние аудиты.	Пп. 31–32 — показатели состояния ЗИ и зрелости; пп. 66–67 — контроль защищённости.
Обучение	П. 13.7 (а–г); приложение: ИПО.1–ИПО.4 — информирование, обучение, практика, проверка знаний.	П. 14 (д) — информирование; пп. 56–57 — обучение, тренировки и проверка знаний.
Внешний аудит	Приложение: АУД.11 — внешние аудиты, но не входит в базовые наборы «+». Не равен обязательному аудиту.	П. 24 — возможно привлечение лицензированной организации; пп. 66–67 — контроль. Обязательный внешний аудит прямо не установлен.
Актуализация	П. 13.8 (г) — решение о модернизации после контроля; п. 13.6 (е) — меры против повторения нештатных ситуаций.	П. 28 (г) — совершенствование мер; п. 33 — план совершенствования (по решению руководителя).

**Нормативные требования задают основу зрелости, но обязанность ≠ фактическое выполнение.
Как оценивать зрелость подрядчика и масштаб «частичного» выполнения?**



АБИСС

Спасибо за внимание

Москва

Электrozаводская, 27с4

ntc-vulkan.ru

+7 (495) 777-1310

marketing@ntc-vulkan.ru