CYBERSECURITY SABANTUY| УФА 2026

АУДИТ ЗАЩИЩЁННОСТИ КИИ ПО НОВОЙ МЕТОДИКЕ ФСТЭК: считаем КЗИ своими руками

Христолюбова Анна Анатольевна

Отраслевой центр компетенций по ИБ в промышленности Минпромторга России

НПП "Гамма"

ФГУП «НПП «ГАММА»
ЕКАТЕРИНБУРГСКИЙ НАУЧНО-ТЕХНИЧЕСКИЙ ЦЕНТР
12 марта 2026 г.

Нормативное обеспечение

«Методика оценки показателя состояния защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденная ФСТЭК России 11 ноября 2025 г.

Методический документ от 11 ноября 2025 г. - ФСТЭК России

~~«Методика оценки показателя состояния защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», утвержденная ФСТЭК России 02 мая 2024 г.~~

- ✓ Используется модифицированный метод взвешенной суммы (Weighted Sum Model, WSM) с элементами бинарной оценки

- ✓ Фиксированные веса не учитывают специфику организаций, типы информационных систем и профили актуальных угроз

Ключевые изменения в новой методике:

- ✓ Ужесточение требований к уровню защищенности (повышение нормированного значения КЗИ с 0,85 до 1)
- ✓ Введение системы цветовой индикации для более наглядной оценки состояния защиты
- ✓ Усиление внимания к аспектам мониторинга информационной безопасности и реагирования (повышение весового коэффициента)
- ✓ Интеграция с практиками анализа уязвимостей и тестирования на проникновение
- ✓ Ужесточение требований к документированию и подтверждению результатов оценки
- ✓ Сокращение сроков проведения оценки (с 1 раза в год до 1 раза в полгода)

Где применять?

Суть: Оценка соответствия уровню защиты информации от типовых актуальных угроз безопасности при реализации нарушителями с базовыми возможностями.

Мониторинг текущего состояния технической защиты информации и оценка эффективности деятельности по технической защите информации

Приказ ФСТЭК России от 11 апреля 2025 г. № 117 (п.31, пер. «а»):

«показателя, характеризующего текущее состояние защиты информации от базового уровня угроз безопасности информации (далее - показатель защищенности $К_{зи}$)»

С 01 марта 2026 г.

Требования к защите информации, содержащейся в:

Государственных информационных системах

Системах управления производственными процессами на критически важных объектах

Объектах критической информационной инфраструктуры РФ

Куда направлять результаты

Расчет и оценка показателя защищенности $К_{зи}$ должны проводиться оператором (обладателем информации) не реже одного раза в шесть месяцев.

Результаты оценки показателя защищенности $К_{зи}$ в срок не позднее 5 рабочих дней после дня их расчета должны направляться оператором (обладателем информации) в ФСТЭК России в целях мониторинга текущего состояния технической защиты информации и оценки эффективности деятельности по технической защите информации

Методы

Применяемые методы: экспертный, инструментальный, опрос (интервьюирование)

Экспертный метод реализуется на трех уровнях:

Нормативно-методологический (соответствие требованиям ФСТЭК России)	Организационно-управленческий (анализ политик ИБ и распределения ответственности)	Процедурный (проверка соблюдения регламентов)

Ограничения методики:

- ✓ Зависимость от полноты предоставленной документации
- ✓ Субъективность оценки, зависящая от опыта экспертов
- ✓ Влияние организационных факторов и готовности персонала

Группы показателей и весовые коэффициенты

$$К_{ЗИ} = (k11+k12+k13)R1 + (k21+k22+...+k2i)R2 + (k31+k32+...+k3i)R3 + (k41+k42+...+k4i)R4$$

Группа показателей	Весовой коэффициент (Rj)	Количество показателей
1. Организация и управление	0,10	3
2. Защита пользователей	0,25	4
3. Защита информационных систем	0,35	6
4. Мониторинг ИБ и реагирование	0,30	3

Классификация уровней защищенности

Значение $К_{ЗИ}$	Уровень защищенности	Цветовая индикация
КЗИ = 1	Минимальный базовый уровень	Зеленый
0,75 < КЗИ < 1	Низкий уровень	Оранжевый
КЗИ ≤ 0,75	Критический уровень	Красный

Группы показателей

Организация и управление ($R_1 = 0,10$)

$k_{11} = 0,30$ (полномочия возложены на заместителя генерального директора)

$k_{12} = 0,40$ (функции возложены на инженера по ИБ)

$k_{13} = 0,30$ (подрядные организации не имеют привилегированных прав)

Группа 2: Защита пользователей ($R_2 = 0,25$)

$k_{21} = 0,30$ (парольная политика утверждена)

$k_{22} = 0,00$ (многофакторная аутентификация не реализована)

$k_{23} = 0,20$ (учетные записи разработчиков отсутствуют)

$k_{24} = 0,20$ (активные учетные записи отсутствуют)

Группа 3: Защита информационных систем ($R_3 = 0,35$)

$k_{31} = 0,20$ (МСЭ уровня L3/L4 установлены)

$k_{32} = 0,25$ (уязвимости критического уровня отсутствуют)

$k_{33} = 0,00$ (уязвимости отсутствуют только на 80% устройств при требуемых 90%)

$k_{34} = 0,15$ (проверка вложений обеспечена)

$k_{35} = 0,15$ (централизованное управление антивирусной защитой)

$k_{36} = 0,10$ (обновление БД сигнатур проводится)

$k_{37} = 0,00$ (договор с провайдером на защиту от DDoS отсутствует)

Группа 4: Мониторинг и реагирование ($R_4 = 0,30$)

$k_{41} = 0,40$ (централизованный сбор событий реализован)

$k_{42} = 0,35$ (сбор и анализ событий реализован)

$k_{43} = 0,25$ (план реагирования на инциденты имеется)

Проведение оценки $К_{ЗИ}$

- Условия проведения работ: Соблюдение требований пропускного режима, конфиденциальность информации, безопасная передача результатов
- Постоценочные мероприятия: Разработка корректирующих мер, контроль их исполнения, обеспечение готовности к внешним проверкам

ПОДГОТОВКА:
подготовка проекта приказа. Ознакомление рабочей группы и ответственных работников с приказом

СБОР ИСХОДНЫХ ДАННЫХ:
Проведение инструментального контроля (сканирование сети, аудит паролей).
Проведение опросов (интервьюирования) сотрудников.

Формирование полного пакета исходных данных.

АНАЛИТИЧЕСКИЙ ЭТАП и РАСЧЕТ:
Анализ данных и оценка частных показателей k_{ji}

Расчет итогового показателя $К_{ЗИ}$

Подготовка проекта Отчета и Плана мероприятий (при необходимости)

ОТЧЕТНОСТЬ и ПРЕДСТАВЛЕНИЕ РЕЗУЛЬТАТОВ:
Доведение результатов оценки до сведения генерального директора.

Представление результатов оценки в ФСТЭК России (по запросу).

План-график проведения оценки

Процедура оценки $К_{ЗИ}$

- Формализация порядка проведения оценки
- Определение ответственных лиц и структурных подразделений
- Установление зон ответственности рабочих групп

РАБОЧАЯ ГРУППА:
создание рабочей группы сбору и анализу исходных данных, разработка и утверждение положения

ПЛАН-ГРАФИК:
Разработка Плана-графика проведения оценки

ПРИКАЗ О ПРОВЕДЕНИИ ОЦЕНКИ:

Назначение сроков и ответственного

Расчет интегрального показателя

1. Выполнение расчета сводного показателя защищенности КЗИ
2. Классификация уровня защищенности: «зеленый» (КЗИ = 1), «оранжевый» (0,75 < КЗИ < 1), «красный» (КЗИ ≤ 0,75)
3. Идентификация проблемных зон, оказывающих негативное влияние на итоговое значение

Показатель $К_{ЗИ}$ характеризует степень достижения предприятием минимально необходимого уровня защиты информации (обеспечения безопасности объектов КИИ):

- ✓ от типовых актуальных угроз безопасности информации;
- ✓ во временном интервале оценивания;
- ✓ в заданных условиях эксплуатации информационных систем, автоматизированных систем управления, информационно-телекоммуникационных сетей, иных объектов информатизации.

Нормированное значение $\boldsymbol{К_{ЗИ} = 1}$ *соответствует минимально необходимому уровню защищенности от типовых актуальных угроз безопасности информации.*

Источники информации

- Документы по результатам государственного контроля
- Результаты внутреннего контроля и внешних аудитов
- Организационно-распорядительные документы
- Эксплуатационная документация на средства защиты
- Результаты инвентаризации ИС
- Данные опросов персонала
- Результаты работы инструментальных средств анализа

Инвентаризация

Необходимые данные:

- Состав и версии ПО и ПАК
- Сетевая инфраструктура и сегменты ИС
- Особенности эксплуатации
- Список пользователей ИС

Работы этапа:

- Инвентаризация сетевых адресов, портов, служб
- Инвентаризация программных и программно-аппаратных средств
- Сбор информации о методах аутентификации пользователей

Внешний анализ уязвимостей

Цель: выявление уязвимостей периметра ИС

Объекты анализа:

- Сетевые адреса, доменные имена
- Сетевые службы и сервисы ИС
- Программное обеспечение
- Web-приложения и мобильные приложения

Методы:

- Пассивное сканирование
- Сравнение версий ПО с базами уязвимостей
- Формирование специальных тестовых запросов (активные методы)

Внутренний анализ уязвимостей

Цель: выявление уязвимостей внутренней инфраструктуры ИС

Объекты анализа:

- Серверы и системы хранения данных
- Рабочие места пользователей, сетевое оборудование
- Средства защиты информации
- Системы управления базами данных
- Программно-аппаратные комплексы

Особенности:

- Проводится в отношении внутренних сетей организации
- Может включать анализ с привилегированными учетными записями
- Учитывает особенности локальной инфраструктуры

Представление результатов и последующие действия

Документирование результатов:

Формирование отчета о расчете показателя $К_{ЗИ}$

Подготовка подтверждающих документов для каждого частного показателя

Информирование руководителя об уровне защищенности

При несоответствии нормированному значению ($К_{ЗИ} < 1$):

Разработка плана реализации мероприятий по повышению уровня защищенности

Установление приоритетности мероприятий на основе анализа частных показателей

Срок реализации мероприятий не должен превышать период до следующей плановой оценки

Предоставление результатов:

Результаты оценки предоставляются в ФСТЭК России

По запросу предоставляются подтверждающие документы в течение 30 дней

В случае непредставления материалов – соответствующим показателям присваивается значение 0

Типичные ошибки

Ошибки на этапе сбора данных

❌ Неполный сбор документов – игнорирование некоторых источников информации

❌ Отсутствие актуальных данных – использование устаревших материалов (старше 30-90 дней для уязвимостей)

❌ Отказ структурных подразделений в предоставлении запрашиваемых материалов

❌ Опрос некомпетентных сотрудников, не обладающих знаниями о функционировании ИС

Ошибки при оценке показателей

❌ Субъективная оценка частных показателей без ссылок на подтверждающие документы

❌ Игнорирование весовых коэффициентов групп показателей при приоритизации работ

❌ Расчет по формальной методике, без учета специфики значимого объекта КИИ

❌ Отсутствие проверки полученных значений несколькими специалистами

Типичные ошибки

Ошибки при документировании результатов

- ❌ Отсутствие подтверждающих материалов для значений частных показателей
- ❌ Некорректное оформление результатов оценки пользовательских устройств и серверов
- ❌ Игнорирование компенсирующих мер при невозможности реализации требований методики
- ❌ Отсутствие анализа причин получения низких значений по критически важным показателям

Ошибки при реализации последующих мероприятий

- ❌ Откладывание реализации мероприятий по повышению защищенности
- ❌ Отсутствие контроля выполнения плана мероприятий
- ❌ Непроведение внеочередной оценки при значимых изменениях архитектуры ИС
- ❌ Непредставление результатов в ФСТЭК России в установленные сроки (при наличии запроса)

Рекомендации

Рекомендации для организации процесса оценки

✅ Формирование команды из специалистов разных направлений (ИБ, администрирование ИС, аудит)
✅ Разработка внутренних регламентов проведения оценки, утвержденных руководством
✅ Автоматизация сбора данных с использованием специализированных средств мониторинга
✅ Создание единого информационного пространства для хранения и анализа результатов оценок

Рекомендации при работе с частными показателями

✅ При невозможности реализации требований – документирование компенсирующих мер
✅ Особое внимание к группе 3 показателей (защита ИС, R3=0,35) и группе 4 (мониторинг, R4=0,30)
✅ Использование актуальных баз уязвимостей (банка данных угроз ФСТЭК России)
✅ Проведение регулярных внешних аудитов и тестирований на проникновение