

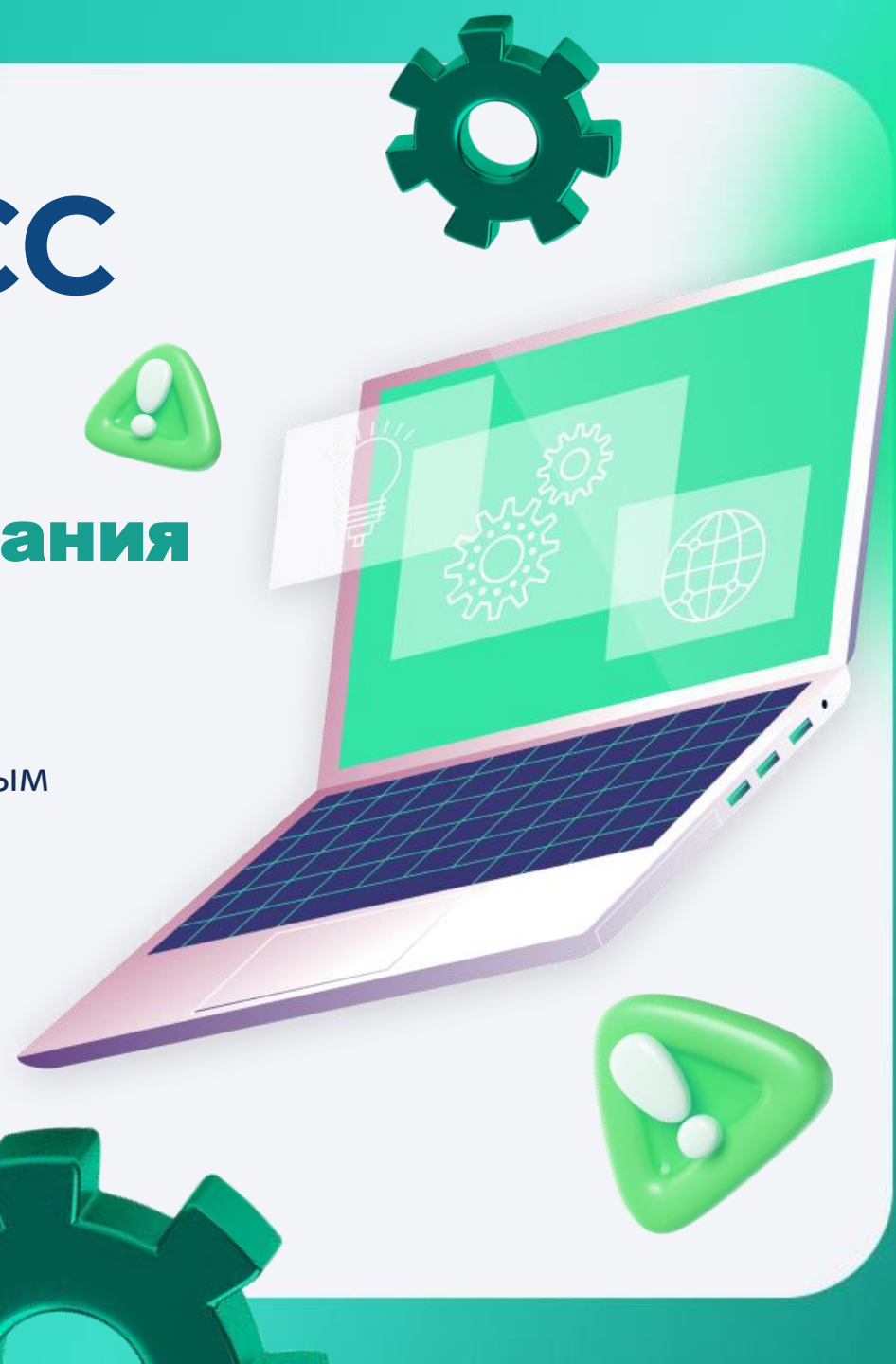


Единый контур ИБ: как перестать выполнять требования регуляторов по отдельности

От разрозненных нормативных пунктов к общим мерам, измеримым процессам и доказательствам.



Артем Четвертной
Руководитель отдела экспертизы
ИБ SECURITM





Что *на повестке?*



1

Сквозной анализ изменений

Разбор ключевых нововведений регуляторов (ФСТЭК России, ФСБ России, Правительство РФ) и карта их пересечений на уровне конкретных мер защиты.

2

Матрица гармонизации

Алгоритм построения единого профиля безопасности, где одна реализованная мера закрывает пункты сразу нескольких нормативных актов.

3

От комплаенса к процессам

Практика перевода абстрактных нормативных требований в измеримые ИБ-процессы и метрики зрелости

4

Автоматизация контроля

Способы оцифровки требований и автоматического сбора доказательной базы без использования сложного Excel-учета



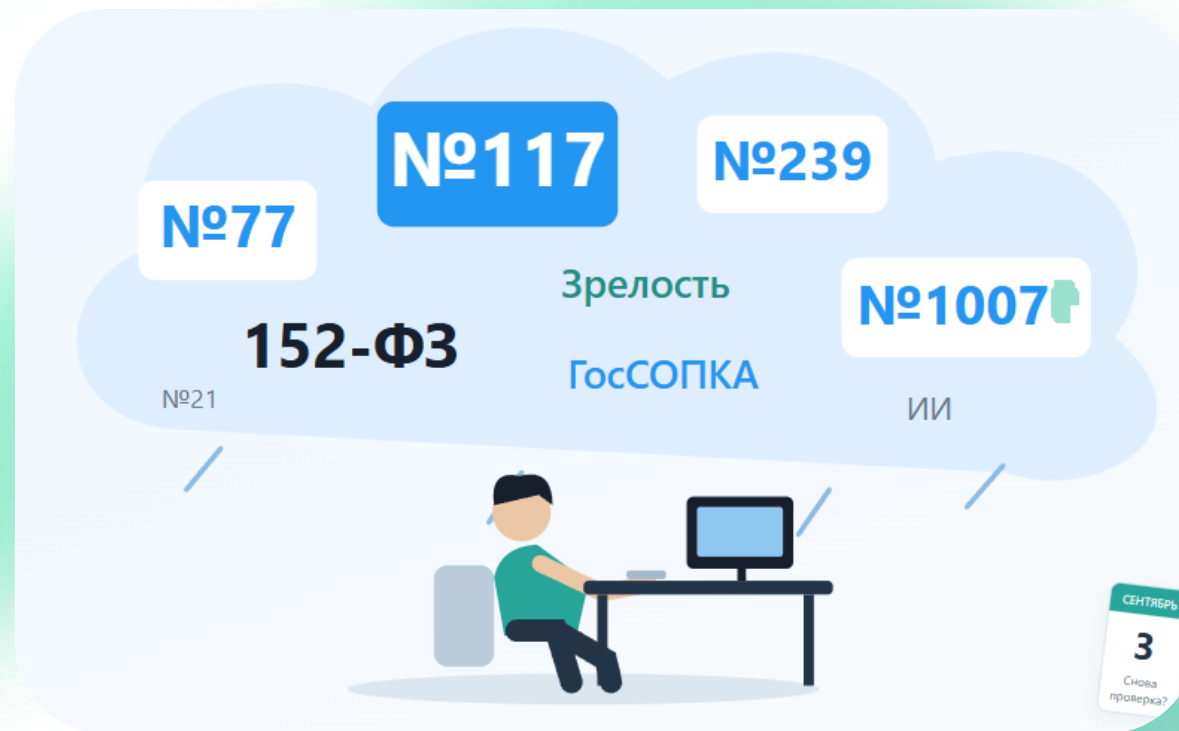


Регуляторный шторм *2025-2026*



За текущий год нормативная нагрузка резко выросла:

- ⬡ **Аттестация, защищенность и зрелость**
Обновление порядка №77, новые методики ФСТЭК России и изменения в приказе №117.
- ⬡ **КИИ и отраслевые особенности**
Типовые объекты, изменения показателей категорирования и отраслевые особенности.
- ⬡ **ГосСОПКА**
Применимость требований к иным ИС и порядки взаимодействия.
- ⬡ **Работа с ИИ**



Риск: служба ИБ превращается в «отдел по перекладыванию бумаг»



Феномен «регуляторной рассинхронизации»



Общий предмет контроля, разные формулировки, несколько комплектов отчетности.



Раздельная работа

Управление доступом

Контур ФСТЭК

Сбор доказательств №1

Контур ФСБ

Сбор доказательств №2

Отраслевой контур

Сбор доказательств №3



Единый контур

Один процесс управления доступом

Владелец

Руководитель ИТ

Проверка

По общей графике

Доказательства

Общий набор + особенности

3 x

Повторяем проверку одного процесса для трех разных отчетов.

1 + Δ

Общую часть выполняем один раз. Специальные условия подтверждаем отдельно.



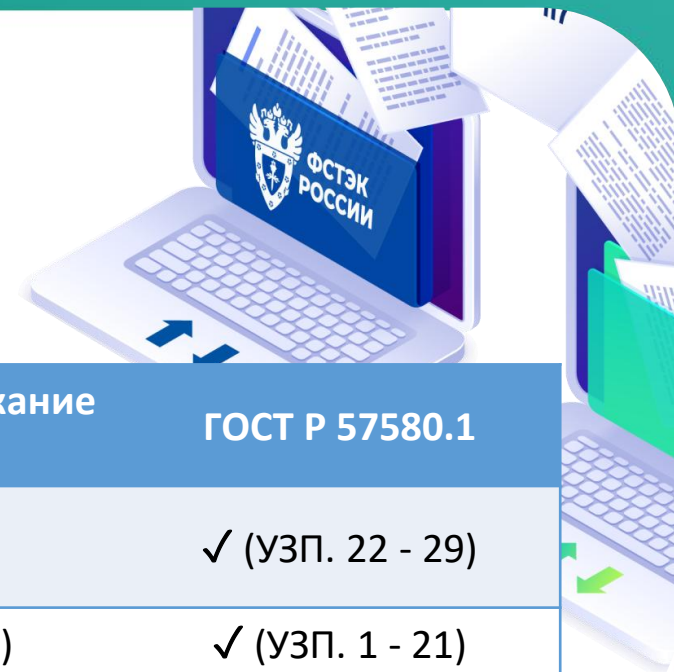
Совпадение темы ещё не означает эквивалентность требований.



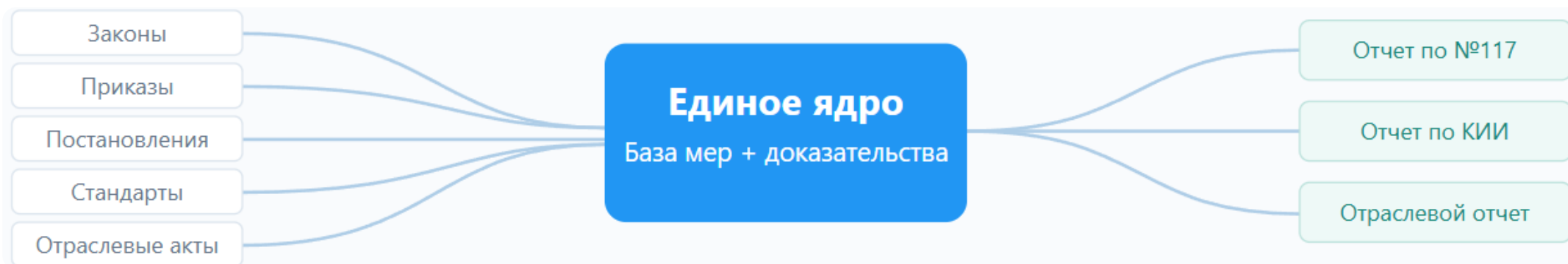


Матрица гармонизации

Берем атомарное требование и находим его во всех применимых стандартах.



Защитная мера	Приказ ФСТЭК России № 117	Приказ ФСТЭК России №239	Состав и содержание мер...	ГОСТ Р 57580.1
Регистрация событий безопасности	✓ (п. 63, е)	✓ (АУД.4)	✓ (РСБ.1)	✓ (УЗП. 22 - 29)
Управление доступом	✓ (п. 63, б)	✓ (УПД.0 - 14)	✓ (УПД.1 - 9)	✓ (УЗП. 1 - 21)
Управление уязвимостями	✓ (п. 34, в)	✓ (АУД.2)	✓ (КУ)	✓ (ЦЗИ)



В результате получаем «Золотой стандарт» ИБ вашей компании.



От «бумажного» комплаенса *к оценке зрелости*

ФЕДЕРАЛЬНАЯ СЛУЖБА
ПО ТЕХНИЧЕСКОМУ И ЭКСПОРТНОМУ КОНТРОЛЮ

Утвержден ФСТЭК России
7 августа 2026 г.

МЕТОДИЧЕСКИЙ ДОКУМЕНТ

Методика

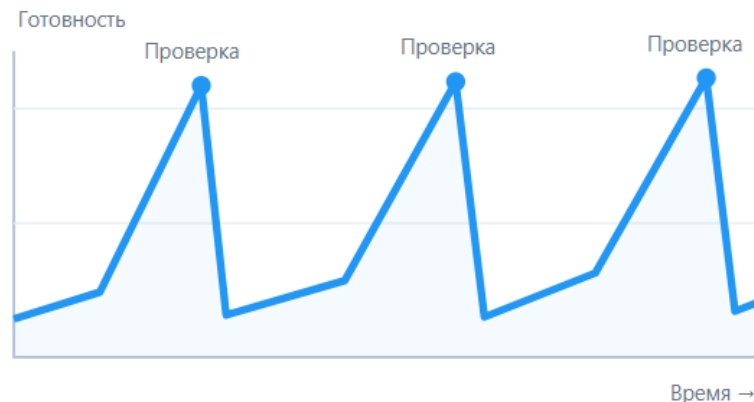
оценки уровня зрелости деятельности в области технической защиты
информации в информационных системах и обеспечения безопасности
значимых объектов критической информационной инфраструктуры
Российской Федерации

2026



РАЗОВАЯ ПОДГОТОВКА

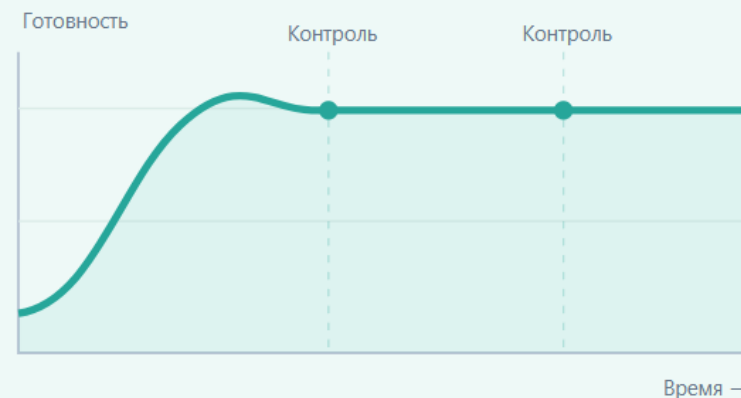
Проверка прошла. Усилия спали.



● Мобилизация перед аудитом, затем спад

НЕПРЕРЫВНЫЙ КОНТРОЛЬ

Процесс работает каждый день.



● Регулярные действия и актуальные доказательства

Методика ФСТЭК по оценке зрелости (21 направление) - это хороший инструмент, чтобы уйти от формата «есть/нет» к реальному управлению.



Требование → процесс → метрика → доказательство

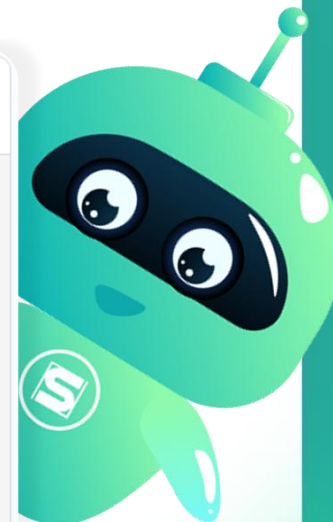
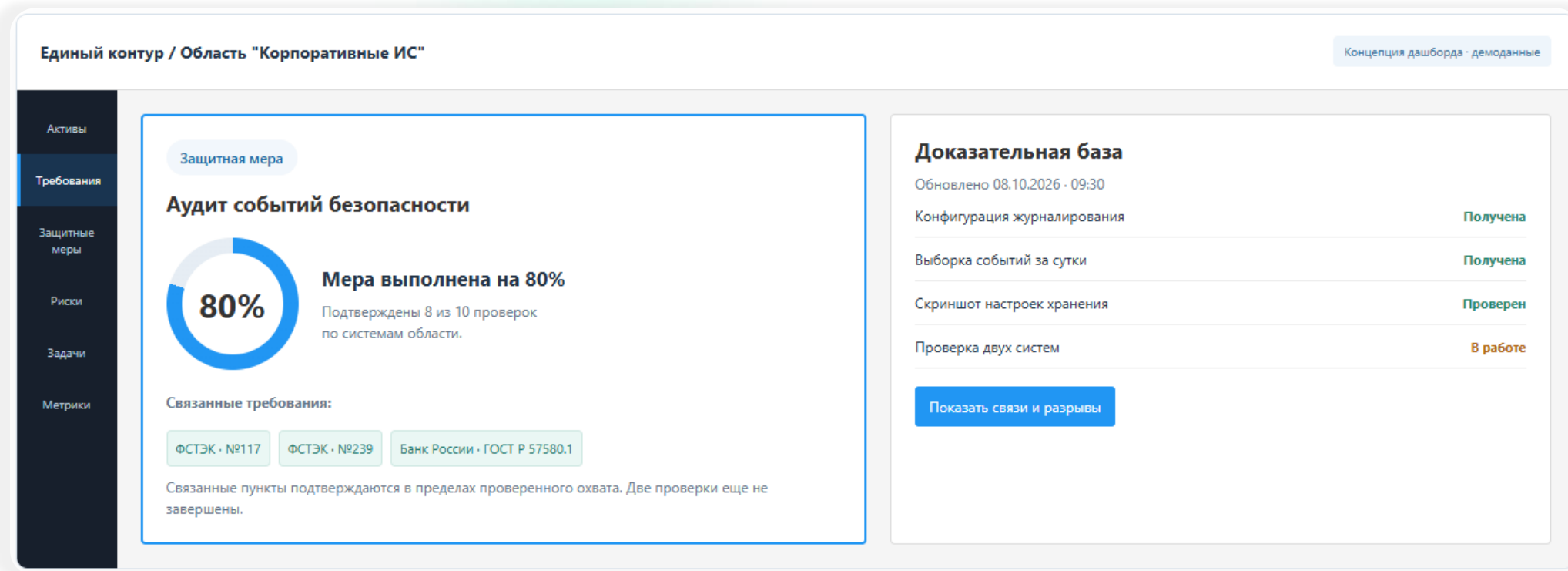




Роль *автоматизации*



Тысячи связей невозможно удержать в голове. Excel перестает справляться.

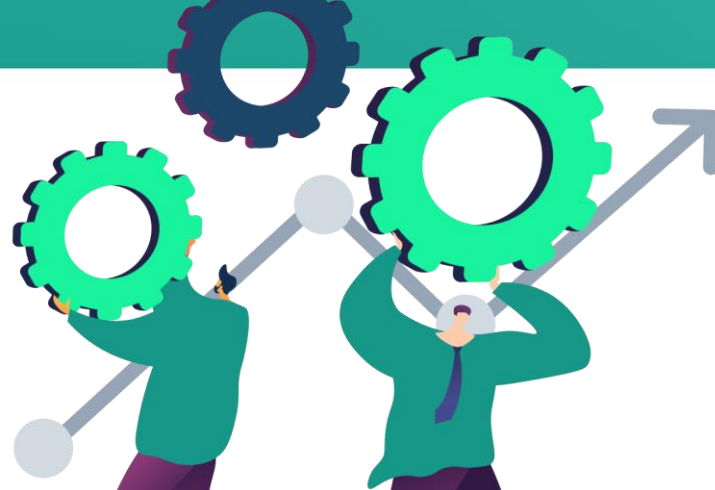


Цифровой двойник ИБ-системы: активы, угрозы, меры и доказательства в общей модели



Роль *автоматизации*

Готовые матрицы гармонизации требований



Документ	Приказ ФСТЭК России № 117	ГОСТ 57580.1 (раздел 7)	Приказ ФСТЭК России № 239	МД "Состав и содержание мер.."
Приказ ФСТЭК России № 117		6	169	157
ГОСТ 57580.1 (раздел 7)	6		90	56
Приказ ФСТЭК России № 239	169	90		235
МД "Состав и содержание мер.."	157	56	235	



Пересечения требований не по тексту, а по смыслу





Заключение



Единый контур начинается с общей модели работы.

1

Определите применимость

Одна карта систем, нормативных режимов и действующих редакций.

2

Управляйте общими мерами

Единое ядро защиты с проверенными связями и сохраненными особенностями.

3

Назначьте владельцев процессов

Сроки, критерии результата и регулярный контроль вместо подготовки в последний момент.

4

Собирайте доказательства по ходу работы

Повторно используйте актуальные подтверждения и отслеживайте разрывы.



Одна работа по защите - несколько подтвержденных нормативных связей.



service.securitm.ru



@SECURITM

✉ info@securitm.ru
☎ 8 800 300 37 64
🌐 securitm.ru



**СПАСИБО
ЗА ВНИМАНИЕ!**

