

Ampire 360°



ПЕРСПЕКТИВНЫЙ
МОНИТОРИНГ

Ampire 360°

ПОЛИГОН КИБЕРБЕЗОПАСНОСТИ



Threat Intelligence

SOC & DFIR

Offensive Security

Киберучения

ИИ и киберзащита

Киберполигон Ampire

📅 14 октября





Система обеспечения защиты информации по требованиям ФСТЭК России

Алексей Глазков

Начальник отдела аудита ИБ и консалтинга
Перспективный мониторинг



Нормативные документы ФСТЭК России

Нормативные документы:

- ▶ Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утверждены приказом ФСТЭК России от «11» апреля 2025 г. № 117
- ▶ Требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования, утверждены приказом ФСТЭК России от 21 декабря 2017 г. № 235
- ▶ Требования по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, утверждены приказом ФСТЭК России от 25 декабря 2017 г. № 239

В чём отличие от Приказа №17 ФСТЭК России

- ▶ Практически полностью переработан
- ▶ Выделены домены безопасности (21 направление деятельности)
- ▶ По сравнению с 17 приказом значительно расширены требования к организации управления ЗИ
- ▶ Управление ЗИ построено на основе цикла PDCA
- ▶ Установлены требования к проведению оценочных мероприятий и информирования ФСТЭК России об их результатах
- ▶ Расширился состав субъектов, на которые распространяются требования нормативного акта

Управление защитой информации



Система обеспечения ЗИ



Последние изменения в нормативные документы

- ▶ С 1 марта 2027 года вводятся требования о расчете показателя защищенности (для ЗО КИИ) и показателя уровня зрелости
- ▶ Приказ ФСТЭК от 8 мая 2026 г. № 137 вносит изменения в 117 Приказ
- ▶ Приказ ФСТЭК от 16 июля 2026 г. № 220 вносит изменения в 235 Приказ
- ▶ Расчёт показателя защищенности актуален как для ЗО КИИ, так и ГосИС и должен проводиться раз в полгода
- ▶ Показатель уровня зрелости для ЗО КИИ должен рассчитываться раз в три года, включая подрядные организации (до получения доступа к ЗО КИИ)
- ▶ Для ГосИС установлено требование расчета показателя уровня зрелости только для подрядных организаций (до получения доступа к ГосИС) раз в два года

- ▶ Методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», Утвержден ФСТЭК России 12 апреля 2026 г.
- ▶ Методический документ «Методика оценки показателя состояния технической защиты информации в информационных системах и обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации», Утвержден ФСТЭК России 11 ноября 2025 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», Утвержден ФСТЭК России 7 августа 2026 г.

Методический документ Состав и содержание мер ЗИ в ИС

- ▶ Распространяется на области 117, 31, 239, 21 Приказов
- ▶ Эволюция Методического документа ФСТЭК России «Меры защиты информации в государственных информационных системах», утвержденного 11.02.2014
- ▶ Определяет состав мер ЗИ для ИС в зависимости от установленного класса защищенности ИС.
- ▶ Для 117 Приказа применяется для направления деятельности «Защита информационных систем и содержащейся в них информации»
- ▶ Определяют усиление мер ЗИ для классов защищенности К2 и К1

Методика оценки показателя состояния ТЗИ в ИС

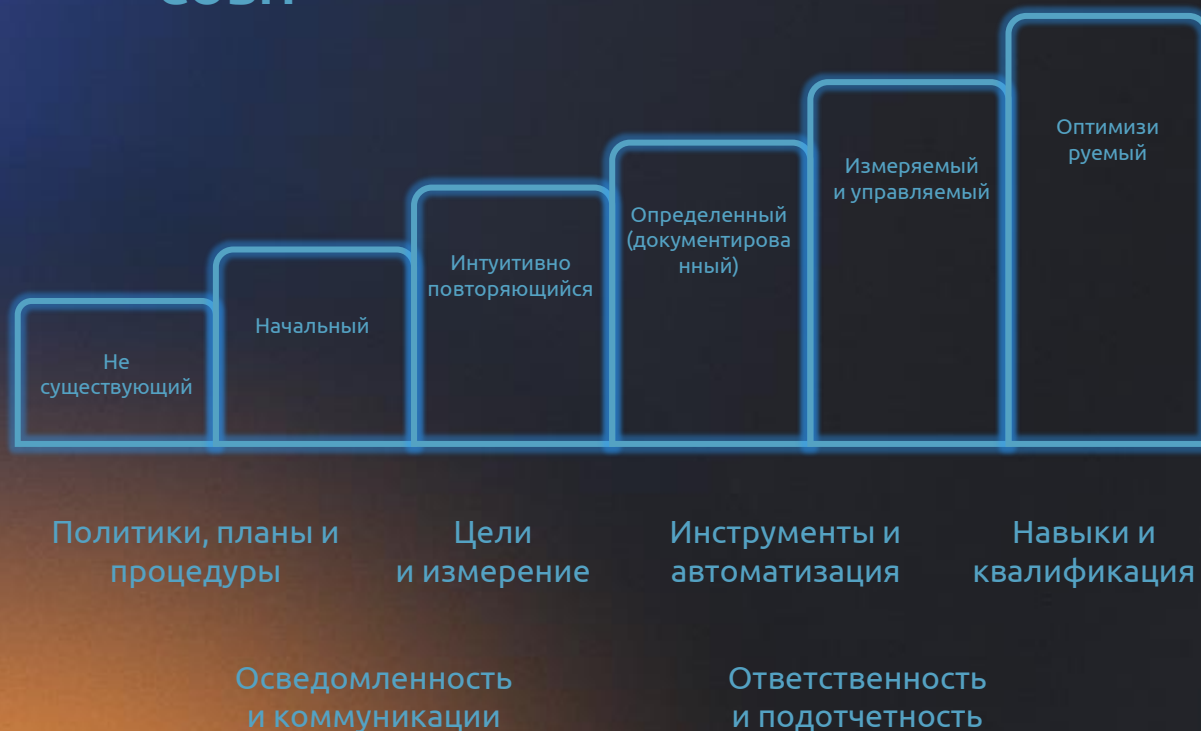
- ▶ Распространяется на области 117, 31, 239, 21 Приказов
- ▶ Определяет состав исходных данных для оценки показателя защищенности
- ▶ Устанавливает требования к квалификации специалистов, принимающих участие в сборе исходных данных и их анализе
- ▶ Устанавливает методику вычисления показателя защищенности
- ▶ Устанавливает целевое значение показателя защищенности
- ▶ Базируется на оценке 4-х групповых показателей: Организация и управление, Защита пользователей, Защита информационных систем, Мониторинг информационной безопасности и реагирование

Методика оценки уровня зрелости

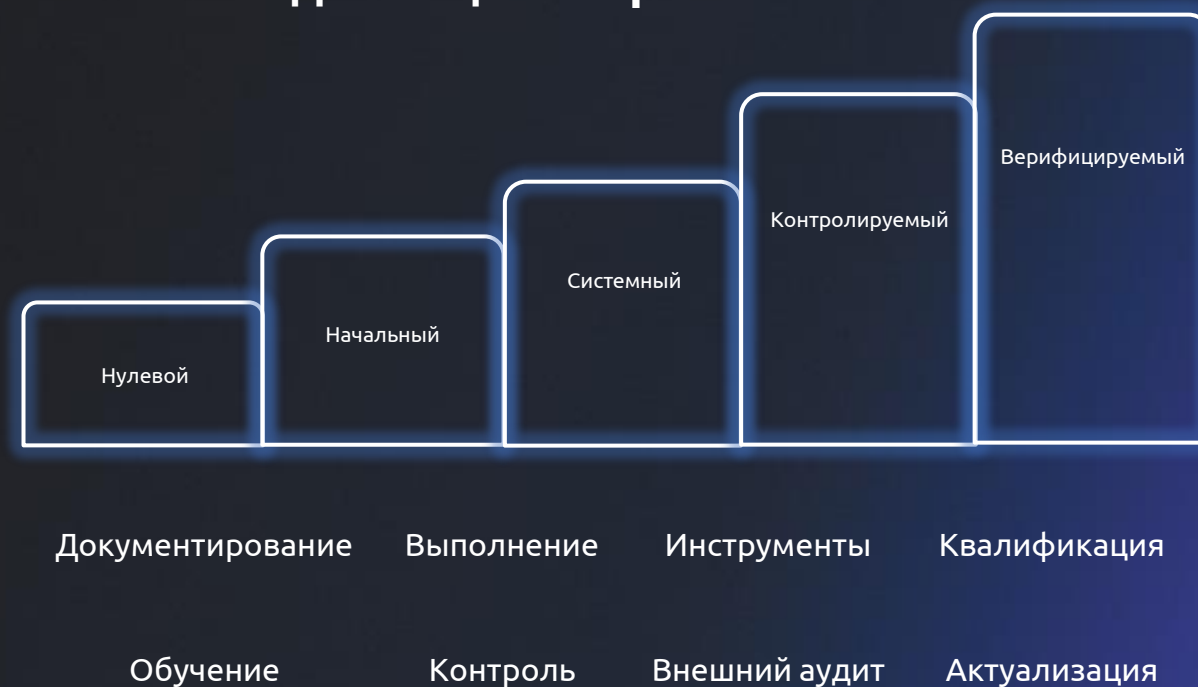
- ▶ Распространяется на области 117, 31, 239, 21 Приказов
- ▶ Устанавливает 5 уровней зрелости и количественные значения для каждого из них
- ▶ Устанавливает методику вычисления количественного значения уровня зрелости
- ▶ Устанавливает целевое значение уровня зрелости
- ▶ Определяет состав исходных данных
- ▶ Устанавливает требования к квалификации специалистов, принимающих участие в сборе свидетельств и их анализе
- ▶ Устанавливает требования к документированию результатов оценки

Как соотносится с международной практикой

COBIT



Методика оценки зрелости



Целевые значения уровня зрелости

Текущий уровень зрелости направления, ($y_{зит_i}$)	Степень выполнения вида требования, (D_{ij})								Значение уровня зрелости направления, (P_i)
	Документирование (ВК = 0,15)	Выполнение (ВК = 0,2)	Инструменты (ВК = 0,1)	Квалификация (ВК = 0,1)	Контроль (ВК = 0,15)	Обучение (ВК = 0,1)	Внешний аудит (ВК = 0,1)	Актуализация (ВК = 0,1)	
0									$P_{3H} < 0,2$
1	$D_{i_1} \geq 0,075$	$D_{i_2} \geq 0,1$	$D_{i_3} \geq 0,05$						$P_{3H} \geq 0,225$
2	$D_{i_1} \geq 0,075$	$D_{i_2} \geq 0,1$	$D_{i_3} \geq 0,05$	$D_{i_4} \geq 0,05$	$D_{i_5} \geq 0,075$				$P_{3H} \geq 0,35$
3	$D_{i_1} = 0,15$	$D_{i_2} = 0,2$	$D_{i_3} \geq 0,05$	$D_{i_4} \geq 0,05$	$D_{i_5} = 0,15$	$D_{i_6} \geq 0,05$			$P_{3H} \geq 0,65$
4	$D_{i_1} = 0,15$	$D_{i_2} = 0,2$	$D_{i_3} \geq 0,05$	$D_{i_4} \geq 0,05$	$D_{i_5} = 0,15$	$D_{i_6} = 0,1$	$D_{i_7} = 0,1$	$D_{i_8} = 0,1$	$P_{3H} \geq 0,9$

ГОС ИС: 3 КЗ
ИСПДН: 4 и 3 УЗ
ЗО КИИ: 3 КЗ

ГОС ИС: 2 КЗ
ИСПДН: 2 УЗ
ЗО КИИ: 2 КЗ

ГОС ИС: 1 КЗ
ИСПДН: 1 УЗ
ЗО КИИ: 1 КЗ

Как достичь третьего уровня зрелости?

- ▶ Утвердить ВНД по всем областям деятельности, внедрить процесс их пересмотра и довести их требования до заинтересованных лиц
- ▶ Реализовать все процессы по всем областям деятельности
- ▶ Допускается частичное внедрение инструментальных средств поддержки области деятельности
- ▶ Допускается использование специалистов прошедших обучение, но не имеющих опыта реализации меры ЗИ
- ▶ Внедрить контрольные процедуры как на плановой, так и ситуационной основе
- ▶ Организовать обучение персонала, при этом допускается не проводить контроль знаний

Что надо сделать?

- Разработка внутренних нормативных документов
- Внедрение процессов, реализующих направления деятельности
- Моделирование угроз (оценка риска)
- Дооснащение – закупка, внедрение, эксплуатация средств ЗИ
- Дополнительные трудовые ресурсы (включая подрядчиков)
- Тренинги персонала по реагированию на инциденты ЗИ
- Подключение к ГосСОПКА
- Внешний аудит
- Отчетность перед Регулятором
- Выделение бюджета на ЗИ

Спасибо за внимание!

Алексей Глазков

Начальник отдела аудита ИБ и консалтинга

Aleksey.Glazkov@amonitoring.ru

