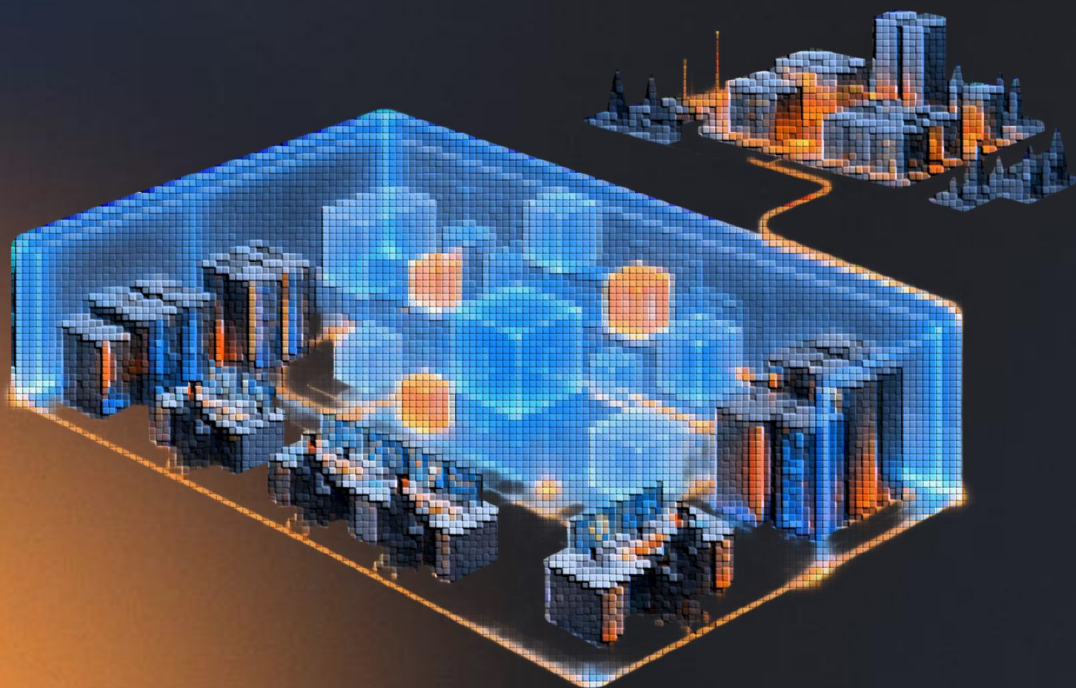


Киберучения и киберполигоны

Требования и мировая практика



Документы: нормы и рекомендации

Обязательность зависит от юрисдикции и категории организации

Юрисдикция	Документ	Статус	Назначение
Россия	ФСБ № 547, п. 10	Обязательная норма для указанной КИИ	Тренировки плана реагирования
ЕС	Регламент 2024/2690 Приложение 3.5	Обязателен для перечисленных категорий	Проверка процедур реагирования
Франция	ANSSI/CCA, 2020	Рекомендации	Кризисный штаб и разбор
Великобритания	NCSC CIE v1.4	Условия схемы для провайдеров	Качество услуг по учениям
США	NICE Guide NIST SP 800-84	Руководства	Критерии полигона и программа
ЕС / ENISA	Методика v1.0, 2026	Рекомендации	Практические учения и оценка

Обязательные нормы определяют обязанности; ТЗ и сценарий уточняют реализацию

Россия: обязательные тренировки



Приказ ФСБ России от 25.12.2025 № 547 · Порядок, пункт 10

Не реже 1 раза в год

Для субъектов КИИ, которым
принадлежат значимые объекты КИИ

Действует с 30 января 2026 года

Что требуется

- 01** Отработать мероприятия плана реагирования
- 02** Назначить ответственных за организацию тренировки
- 03** Изменить план при выявлении недостатков мероприятий

ЕС: проверка процедур реагирования

Регламент Комиссии (ЕУ) 2024/2690 от 17.10.2024 · Приложение, раздел 3.5

ОБЯЗАТЕЛЬНЫЙ РЕГЛАМЕНТ

Область применения

Определённые поставщики цифровых услуг: облака и центры обработки данных, управляемые сервисы, DNS и другие категории, перечисленные в акте

Периодичность: запланированные интервалы, без единого годового срока

3.5.1–2

Документированные процедуры

Сдерживание, устранение, восстановление

3.5.3

Планы коммуникаций

CSIRT, сотрудники и внешние стороны

3.5.4

Фиксация действий

Журналирование и доказательства

3.5.5

Проверка процедур

Тестирование через плановые интервалы

Официальные документы по организации учений: разные статусы и аудитории

Франция · ANSSI/CCA

Руководство по кризисным киберучениям, 2020

Методические рекомендации

Цели, роли и сценарий
Хронология вводных и наблюдение
Разбор и письменный отчёт

С. 24–44, 50–82, 106–112, 121
Уровень кризисного штаба

Великобритания · NCSC

CIE Technical Standard
v1.4, сентябрь 2023

Условия участия провайдеров в схеме NCSC Assured CIE

Согласованные цели и границы
Достоверный сценарий и вводные
Наблюдение, разбор и отчёт

Разделы 2.3, 3.4, 6.4–6.11
Форматы: tabletop и live play

Эти документы не устанавливают общую обязанность организаций строить полигон

США: полигон и программа учений

NICE и NIST: технические и методические руководства

The Cyber Range: A Guide

NICE · сентябрь 2023

Критерии полигона

Оркестрация и учебная среда
Виртуализация и масштабирование
Настройка сценариев
Запись действий и оценка работы

С. 6–10; приложение А, с. 14–15
Основа для критериев ТЗ

NIST SP 800-84

Сентябрь 2006

Программа учений

Проектирование и разработка
Проведение и оценка
Материалы ведущего и участников
Формы разбора и итогового отчёта

Разделы 4–5 и приложения
Штабные и функциональные учения

Руководства: перечисленные возможности не обязательны для любого полигона

ENISA: методика учений на полигоне

The ENISA Cybersecurity Exercise Methodology · v1.0 · февраль 2026

ОФИЦИАЛЬНАЯ МЕТОДИКА, РЕКОМЕНДАТЕЛЬНЫЙ СТАТУС

Подготовка

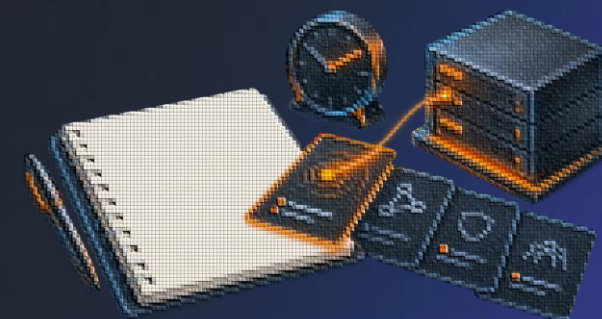
- Измеримые цели и границы
- Роли участников и наблюдателей
- Реалистичный сценарий
- План оценки до начала учений

Техническая практика

- Контролируемая виртуальная среда
- Выдача вводных и фиксация действий
- Журналы и мониторинг
- Разбор и реализация улучшений

Комплект документов · приложение В, с. 61–62

План учений, план оценки, план коммуникаций,
перечень событий и вводных (MSEL), итоговый отчёт (AAR)



Европа: управление киберкризисом

Германия и Франция: работа организаций при масштабном отказе ИТ

LÜKEX 23 · Германия

27–28 сентября 2023

> 2 500

участников, свыше 60 организаций

Отказ государственных ИТ
и нарушение критичных процессов

Приоритеты процессов,
непрерывность
и общая картина кризиса

REMPAR25 · Франция

18 сентября 2025

≈ 5 680

участников из 1 263 организаций

Массовый отказ цифровых
сервисов
и информационное давление
50% участников работали
вне ИТ и кибербезопасности



Штабные и сценарные учения; технический полигон в этих источниках не заявлен

Европа: техника и координация

Два формата комплексной подготовки к масштабным киберинцидентам

Cyber Europe 2024

Европейские страны · июнь 2024

≈ 5 000

участников

Кризис в энергетике
Уведомления и трансграничная
эскалация

Ограничения в оценке
трансграничных последствий

Locked Shields 2025

Эстония · международное участие

> 4 000

участников, 41 страна, 17 команд

Защита виртуализированных
систем
Право, коммуникации и решения

Техническая среда сочетается
с управленческими заданиями



Техническое реагирование
и работа кризисного штаба

Самооценка участников и рейтинг команд не измеряют готовность к реальной атаке

Россия: киберучения Банка России

2025 год: проверка реакции на угрозы и взаимодействия с ФинЦЕРТ

> 320 

финансовых организаций

25 работников

в 21 организации
условно скомпрометированы

Сценарии

Фишинг

Эксплуатация уязвимостей

Хищение денежных средств

Что проверяли

Корректность реагирования

Скорость исправления уязвимостей

Оперативный обмен с ФинЦЕРТ



Региональный киберполигон Кузбасса

Ampire 360°

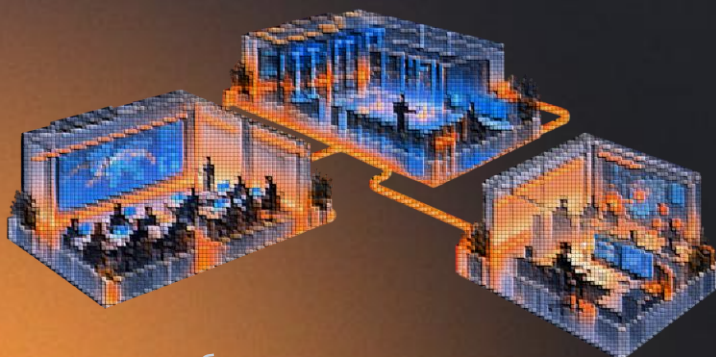
Общая среда для органов власти и образовательных организаций

193

тренировки за год

10

для сотрудников
органов власти



По данным разработчика

[Перспективный мониторинг · Киберполигон Кузбасса](#)

Органы власти

КемГУ
КузГТУ



Ampire

региональный полигон



Другие
учебные
организации

Регион самостоятельно
планирует график учений

Россия: региональные практики

Подготовка специалистов органов власти и совместная работа команд

Учения РОИВов · 2023

29

РОИВов

300

сотрудников

Полигон «Солар Кибермир»

Выявлена неравномерность подготовки
Результаты для планов развития

Кемерово · январь 2025

4 команды

Органы власти, госорганизации
и бизнес

CSIRT: «Защита сервера
автоматизации»

Оценки команд и развёртывание
полигона в публикации не раскрыты

Количественный прирост готовности по этим публикациям установить нельзя

Россия: учения на киберполигоне

Ampire 360°

IV Международный киберчемпионат · ЦИПР-2025 · Нижний Новгород

117 команд

из 26 стран

Solar CyberMir

Финал: Defence Challenge

Изучение инфраструктуры, настройка защиты и устранение уязвимостей

Результаты финала

Беларусь	6 149
----------	-------

Россия	5 588
--------	-------

Вьетнам	5 280
---------	-------

баллы в учебном сценарии

Рейтинг соревнования не подтверждает готовность руководства к кризису

Программа комплексных киберучений

Ampire 360°

Сценарий, роли, критерии и контроль улучшений

- 01** Сценарий
Инфраструктура и критичные сервисы
- 02** Участники
ИБ, ИТ, руководители и коммуникации
- 03** Критерии
Проверяемые задачи и наблюдения
- 04** Разбор
Недостатки и ответственные за улучшения
- 05** Повторная проверка
Контроль выполнения плана



Как читать результаты

Участники: масштаб
Задачи: учебный результат
Замеры: изменение готовности

Спасибо

Гуревич Алексей

ЦК «КИБЕРБЕЗОПАСНОСТЬ»

EnergyNet

Объединяем компетенции и формируем системный подход к обеспечению кибербезопасности

EnergyNetCS@ya.ru

