УЦСБ

КАК ПОДГОТОВИТЬСЯ К ПРОХОЖДЕНИЮ ГОСКОНТРОЛЯ В ОБЛАСТИ ЗАЩИТЫ КИИ

VIII вебинар цикла «Обеспечение безопасности объектов КИИ в рамках 187-ФЗ»

УЦСБ

ПЛАН ВЕБИНАРА

01 Что такое госконтроль?

02 Типовое прохождение госконтроля

03 Подготовка к госконтролю

04 Прохождение госконтроля

05 Работа с нарушениями

06 Типовые нарушения, выявляемые при госконтроле

07 Решения для подготовки к госконтролю

УЦСБ

ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ

Проверка соблюдения субъектами КИИ требований 187-ФЗ и подзаконных актов

№248-ФЗ

О государственном контроле (надзоре)
и муниципальном контроле
в Российской Федерации

№294-ФЗ

О защите прав юридических лиц и индивидуальных предпринимателей при осуществлении государственного контроля (надзора) и муниципального контроля

Постановление Правительства РФ от 17.02.2018 №162

Об утверждении Правил осуществления государственного контроля в области обеспечения безопасности значимых объектов критической информационной инфраструктуры Российской Федерации

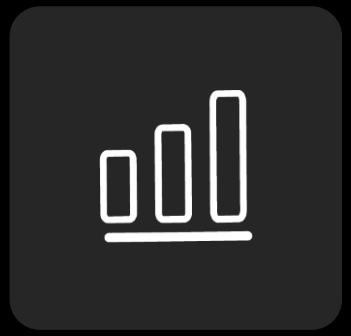
УЦСБ

ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ

ФЕДЕРАЛЬНЫЕ ЗАКОНЫ	УКАЗЫ ПРЕЗИДЕНТА РФ, ПОСТАНОВЛЕНИЯ И РАСПОРЯЖЕНИЯ ПРАВИТЕЛЬСТВА РФ	НОРМАТИВНЫЕ ПРАВОВЫЕ АКТЫ ФОИВ
Федеральный закон 187-ФЗ	**Постановление Правительства РФ №127** Правила категорирования	**Приказы ФСТЭК России**
▪ Ч. 1, 2, 4, 5, 9, 12 статьи 7 ▪ Категорирование объектов КИИ ▪ Статья 9 ▪ Права и обязанности субъектов КИИ ▪ Статья 10 ▪ Система безопасности значимого объекта КИИ	▪ Пункты 1-18 ▪ Порядок категорирования объектов КИИ ▪ Пункт 20 ▪ Порядок изменения категории значимости объекта КИИ ▪ Пункт 21 ▪ Порядок пересмотра категорий значимости объектов КИИ или решений об отсутствии категории	▪ Приказ ФСТЭК №235 ▪ Требования к созданию систем безопасности значимых объектов КИИ и обеспечению их функционирования ▪ Приказ ФСТЭК №239 ▪ Требования по обеспечению безопасности значимых объектов КИИ

ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ

Направления



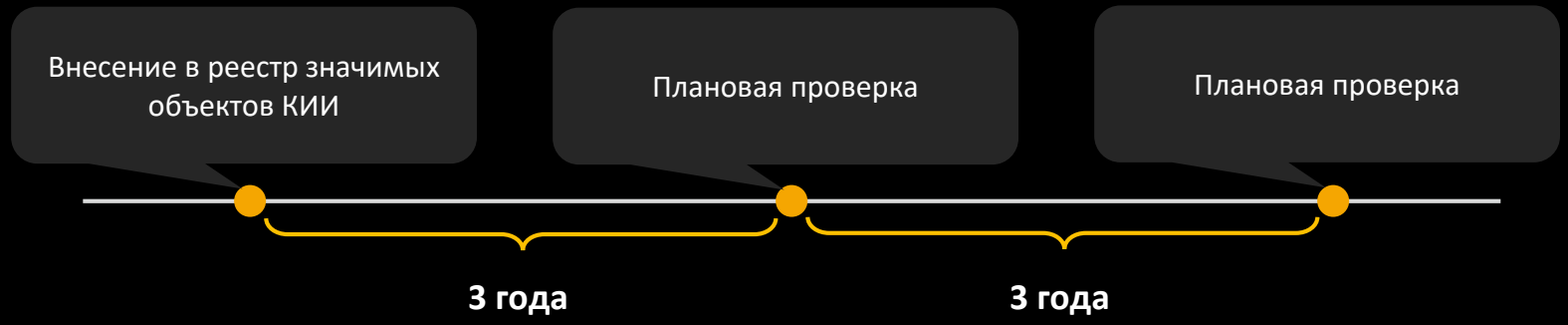
категорирование объектов КИИ

создание систем безопасности значимых объектов КИИ

обеспечение безопасности значимых объектов КИИ

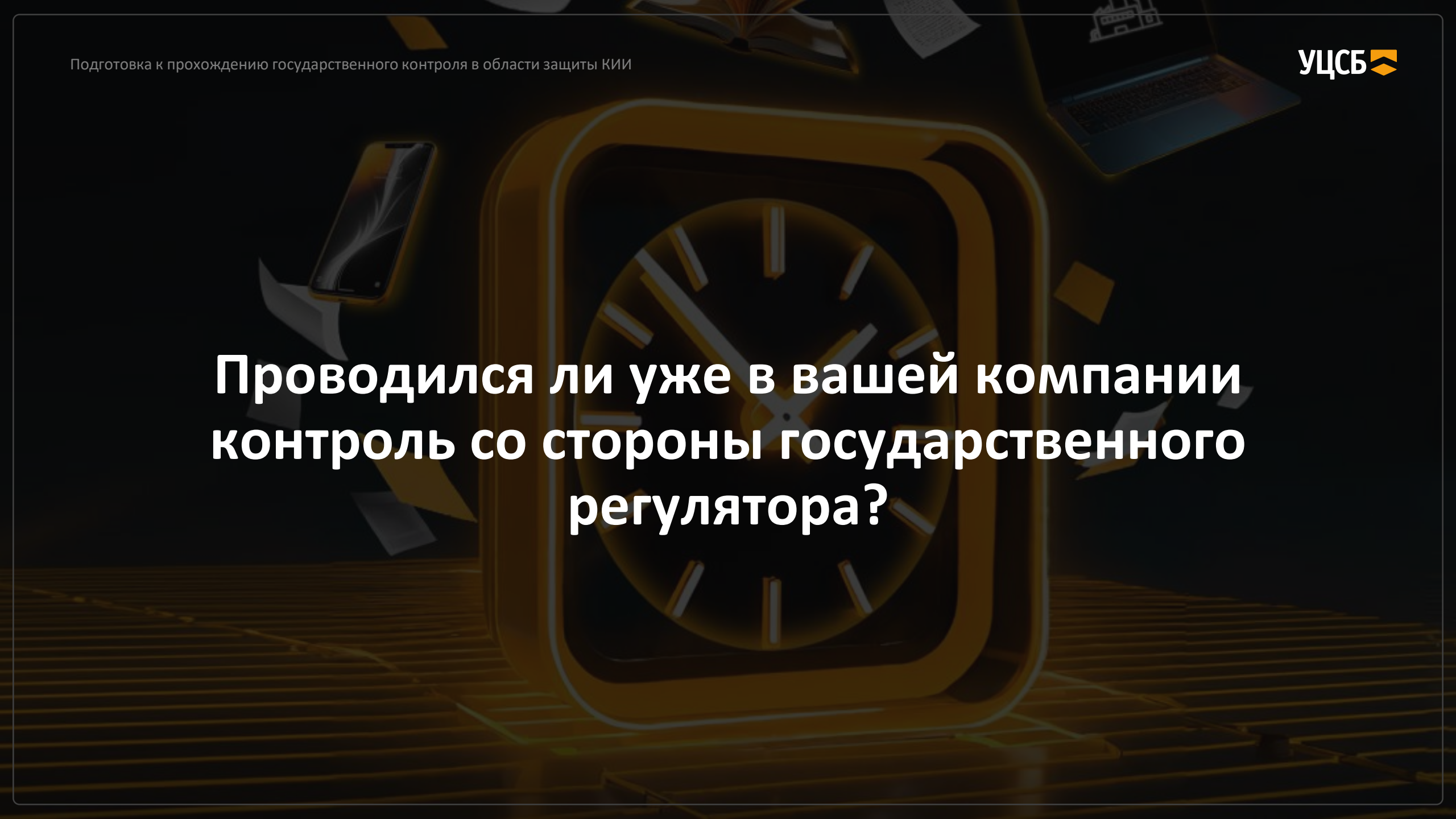
ГОСУДАРСТВЕННЫЙ КОНТРОЛЬ

Плановые



Внеплановые

- Истечение срока выполнения предписаний
- Компьютерный инцидент
- Поручение Президента / Правительства РФ или требование прокурора



Проводился ли уже в вашей компании контроль со стороны государственного регулятора?

ФОРМИРОВАНИЕ ПЛАНА КОНТРОЛЯ

До **20 декабря** ФСТЭК России утверждает ежегодный план проведения проверок

До **1 января** года проведения проверки ФСТЭК России направляет выписку из плана организациям, попадающим в план

План и выписки включают:

- сведения о субъекте КИИ
- сведения о лице, эксплуатирующем значимый объект КИИ
- дату окончания последней плановой проверки (если проводилась)
- месяц и срок проведения проверки
- основание проведения проверки
- наименование органа государственного контроля

ПОДГОТОВКА ПО ПЕРЕЧНЮ ВОПРОСОВ

Перечень вопросов при проведении плановой проверки направляется Обществу для подготовки к госконтролю.

Направления

Категорирование объектов КИИ

- Подтверждение субъектности Общества
- Требования к комиссии по категорированию
- Требования к процедуре категорирования

Создание систем безопасности значимых объектов КИИ

- Наличие СОИБ ЗОКИИ
- Организационное обеспечение функционирования СОИБ
- Наличие документации по созданию СОИБ, протоколы приемочных испытаний, акты ввода в эксплуатацию
- Наличие СрЗИ, сертифицированных / оцененных в формате приемки, достаточных для реализации технических мер

Обеспечение безопасности значимых объектов КИИ

- Наличие контроля доступа на территорию и к ЗОКИИ
- Организационное и техническое обеспечение ИБ
- Наличие технической документации на системы
- Выполнение требований Указа Президента РФ №250 и постановления Правительства РФ №1272

ПОДГОТОВКА ПО ПЕРЕЧНЮ ВОПРОСОВ

Рекомендуем подготовить **справочную информацию** по реализации организационных и технических мер по ИБ ЗОКИИ в соответствии с приказом ФСТЭК России №239:

АСУ ТП «1»

Мера	Статус	Способ реализации / причина отсутствия реализации
ИАФ.1 Идентификация и аутентификация пользователей и инициируемых ими процессов	Реализована	Реализована техническими средствами с использованием встроенных средств SCADA для разделения полномочий оператора и администратора. Принадлежность действий конкретному оператору устанавливается на основании Журнала смены операторов

СОСТАВ ГРУППЫ ФСТЭК РОССИИ

Технические специалисты

Осуществляют проверку реализации технических мер, правильности настройки СрЗИ, организации сети и т. д.

Аудиторы

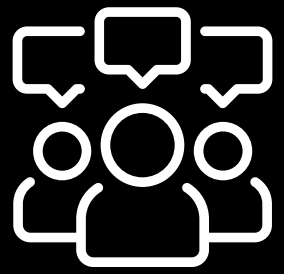
Осуществляют проверку реализации организационных мер, корректности и достаточности разработанной документации

Руководитель группы

Координирует действия группы, выносит решения по итогам госконтроля

ЭТАПЫ ПРОВЕРКИ

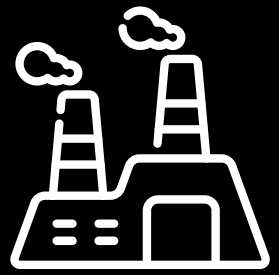
1



Обсуждение СОИБ в головном офисе

Проверка организационных мер, формирование предварительных замечаний

2



Выездная проверка производственных площадок

Проверка реализации технических мер

ОСНОВНЫЕ РЕКОМЕНДАЦИИ

1 **Своевременная подготовка к госконтролю**

В том числе – привлечение / оповещение подрядчиков, внедрение необходимых решений

2 **Проработка перечня вопросов при проведении плановой проверки**

Подготовка справочной ведомости для ФСТЭК России, приведение в порядок ОРД, инвентаризация договоров

3 **Планирование маршрута проверки**

Формирование маршрута, позволяющего охватить все ЗОКИИ в области проверки

4 **Разработка тактики поведения**

Если СОИБ введен в эксплуатацию – готовим всю документацию, связанную с СОИБ и реализованными мерами

Если СОИБ не введен в эксплуатацию – обсуждаем с ФСТЭК России детали реализации, просим рекомендации по построению СОИБ

УЦСБ

ПОДГОТОВКА К ГОСКОНТРОЛЮ

Обсуждение с ФСТЭК России

Планирование сопровождения проверки

Подготовка документации

- Порядок проведения проверки
- Допуски на территорию
- Трансфер проверяющих
- Рабочие места для проверяющих
- Внос / вынос технических средств
- Средства индивидуальной защиты *(при необходимости)*
- Перенос сроков *(при необходимости)*

ПОДГОТОВКА К ГОСКОНТРОЛЮ

Обсуждение с ФСТЭК России | **Планирование сопровождения проверки** | Подготовка документации

Подготовка к установочному совещанию

- Сведения о субъекте КИИ
- Информация о технологических процессах
- Информация об объектах КИИ
- Информация об обеспечении безопасности ЗОКИИ
- Информация о результатах внутренних и внешних проверок

Планирование мероприятий на различных площадках

- Программа мероприятий по дням

УЦСБ

ПОДГОТОВКА К ГОСКОНТРОЛЮ

Обсуждение с ФСТЭК России

Планирование сопровождения проверки

Подготовка документации

- Учредительные документы
- Документы, определяющие деятельность сил обеспечения безопасности
- Релевантные договоры со сторонними организациями
- Перечень ОРД, предназначенных для ознакомления персонала и работников сторонних организаций, допускаемых к работам на технологическом объекте
- Техническая и рабочая документация на объекты КИИ
- Программы и планы по модернизации и дооснащению ЗОКИИ
- Приказы о назначении администраторов объектов КИИ, администраторов безопасности объектов КИИ
- План реагирования на компьютерные инциденты
- Сведения об объектах КИИ
- Документация, регламентирующая вопросы обеспечения ИБ АСУ ТП
- Иные…

УЦСБ

ДЕЙСТВИЯ ПРИ ГОСКОНТРОЛЕ

Встреча с проверяющими

1

Проверка легитимности

***Приказ о проведении проверки**, удостоверения проверяющих*

2

Проведение установочного совещания

3

Прохождение инструктажа по технике безопасности

4

Предоставление индивидуальных СЗ

*Средства должен предоставить **субъект КИИ***

ДЕЙСТВИЯ ПРИ ГОСКОНТРОЛЕ

Сопровождение должностных лиц

Подготовьте к проверке документы, работников, помещения и компоненты систем

Спланируйте маршрут проверки и обеспечьте служебный транспорт

Оказывайте содействие проверяющим

Не стесняйтесь задавать вопросы комиссии

Руководитель субъекта КИИ (уполномоченное лицо)
обязан присутствовать на месте проведения проверки

ДЕЙСТВИЯ ПРИ ГОСКОНТРОЛЕ

Подтверждение выполнения требований

- Копии документов, предоставленных субъектом КИИ
- Протоколы / заключения по результатам контрольных мероприятий
- Отчеты, формируемые средствами контроля
- Фото- и видеоматериалы, отснятые проверяющими
- Устные свидетельства работников субъекта КИИ

- Орган госконтроля может направить субъекту КИИ мотивированный запрос на предоставление документов
- Собранные свидетельства прикладываются к акту проверки

ДЕЙСТВИЯ ПРИ ГОСКОНТРОЛЕ

Подписание акта проверки

Акт оформляется по окончании проверки. Форма утверждена приказом №229 ФСТЭК России

Руководитель субъекта КИИ или уполномоченное лицо должен быть ознакомлен с результатами под подпись

*В ином случае ставится пометка об **отказе** в ознакомлении с актом*

К акту проверки прилагаются **предписания** об устранении нарушений и ***рекомендации*** по устранению недостатков

Что делать при наличии возражений к акту проверки или предписаниям?

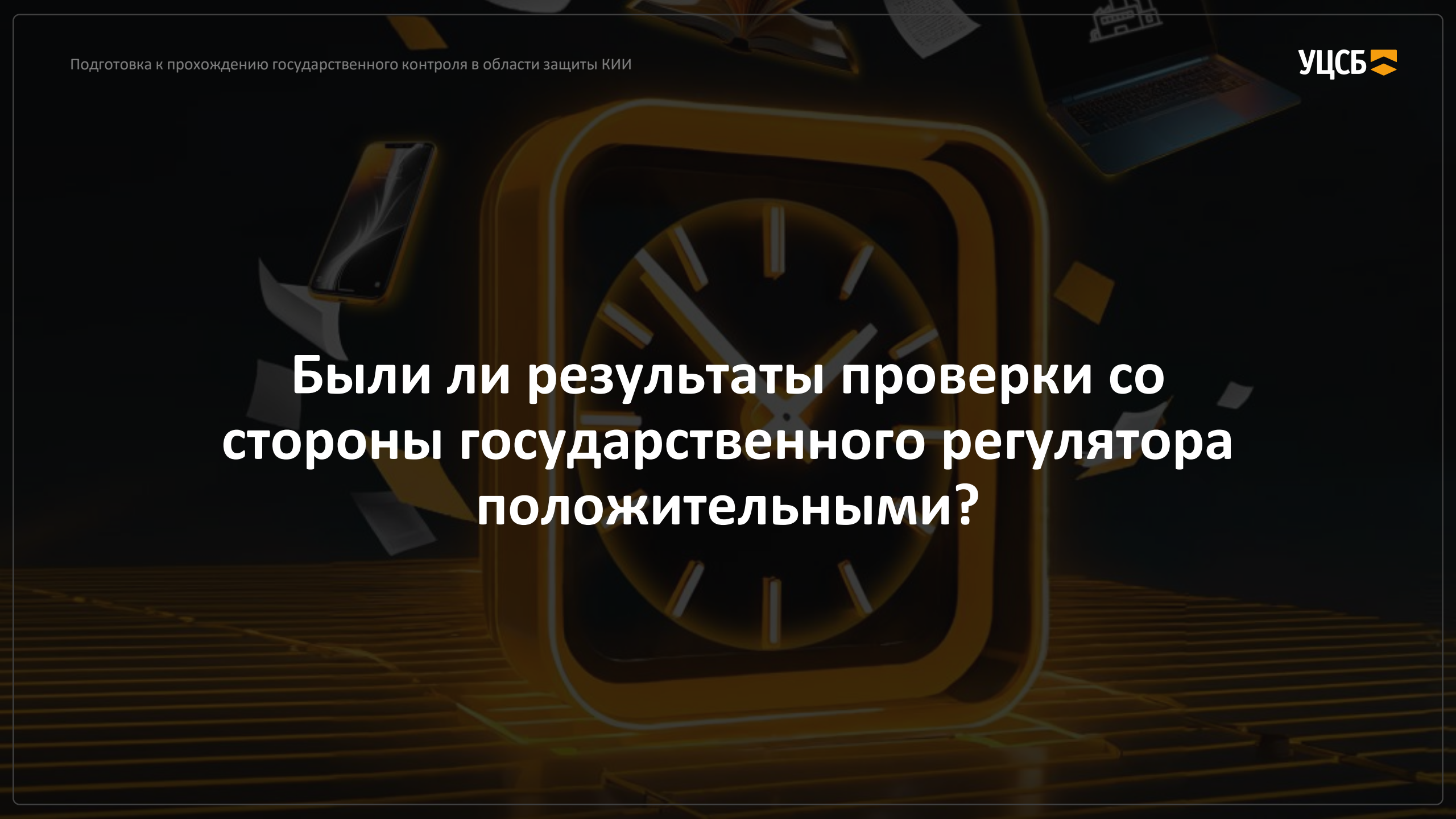
- Указать несогласие руководителя субъекта КИИ или уполномоченного лица в акте

  *В течение **15 дней** с даты получения акта*

- Представить в орган госконтроля возражения в письменной форме

  Желательно приложить документы, подтверждающие обоснованность возражений

- Дальнейшая работа с органом госконтроля



Были ли результаты проверки со стороны государственного регулятора положительными?

РАБОТА С НАРУШЕНИЯМИ

Что делать?

- Руководитель субъекта КИИ издает **приказ об устранении** несоответствий, в котором определяются ответственные
- Ответственные разрабатывают **план мероприятий** по устранению несоответствий

  Подлежит согласованию со ФСТЭК России до начала реализации
- По результатам реализации плана составляем **отчет о выполнении предписаний**

В какие сроки?

Срок фиксируется **в предписании** об устранении нарушения,
с учетом планов по модернизации объекта КИИ

!

Неполучение отчета об устранении нарушений в срок **является поводом для проведения внеплановой проверки со стороны ФСТЭК России**

В случае выявления неустраненных нарушений к субъекту КИИ
могут применяться **меры административного наказания**

НАРУШЕНИЯ И НЕДОСТАТКИ: КАТЕГОРИРОВАНИЕ КИИ

- В перечне ОКИИ указана **неточная дата** категорирования
- В перечень ОКИИ включены **не все объекты**, подлежащие категорированию
- При определении ОКИИ объекты были **разделены неверно** (разделение АСУ на верхний и нижний уровень)
- В сведениях об ОКИИ **не конкретизирована информация** о программно-аппаратных средствах, общесистемном и прикладном ПО
- Сведения о результатах категорирования содержат **противоречивую информацию** об ОКИИ в части его архитектуры, назначения и т. д.
- В составе ОКИИ **не были учтены** СЗИ, а также инфраструктура для обслуживания (АРМ администратора и др.)

НАРУШЕНИЯ И НЕДОСТАТКИ: КАТЕГОРИРОВАНИЕ КИИ

- При категорировании **не были рассмотрены** все виды нарушителей
- При категорировании **не был учтен** худший сценарий при нарушении функционирования ОКИИ
- В сведениях **не указаны** рассчитанные значения по показателем и сведения о применимости показателей
- В сведения **не внесены изменения** в соответствии с последними изменениями в показатели критериев значимости
- Перечни подлежащих категорированию объектов КИИ были предоставлены **в неутвержденном виде**
- Фактический состав ОКИИ **не соответствует** реальному

УЦСБ

НАРУШЕНИЯ И НЕДОСТАТКИ: СИЛЫ ИБ

- **Недостаточная подготовка** сил в части эксплуатации СЗИ
- **Невыполнение** СКИИ принятых политик/регламентов по безопасности
- **Недостаточные контроль и координация действий**, осуществляемых иными силами, по ОБ ЗОКИИ со стороны подразделения по ОБ КИИ
- Состав комиссии по контролю состояния безопасности ЗОКИИ **не соответствует требованиям** регуляторов
- **Отсутствие вопросов** ОБ ЗОКИИ в договорах с подрядными организациями или **неознакомление** подрядных организаций с ОРД по ОБ ЗОКИИ
- Персонал СКИИ и подрядных организаций **не осведомлен** об УБИ и правилах безопасной работы
- **Отсутствие контроля** за работниками подрядчика при осуществлении работ на компонентах ЗОКИИ

УЦСБ

НАРУШЕНИЯ И НЕДОСТАТКИ: ОРД

- ОРД **не утверждены** и (или) **не введены** в действие
- Персонал **не ознакомлен** с ОРД в части ОБ ОКИИ; инструкции персоналу перегружены
- **Не регламентированы** отдельные вопросы ОБ ЗОКИИ
- Имеются **противоречия** в различных ОРД
- **Недостатки** обеспечения физической защиты компонентов ЗОКИИ
- **Отсутствие организационных мер** по обеспечению безопасности ЗОКИИ при работе на их компонентах сотрудников подрядных организаций
- Планы выполняются **частично и (или) несвоевременно**, свидетельства о выполнении отсутствуют

НАРУШЕНИЯ И НЕДОСТАТКИ: ПОСТРОЕНИЕ СОИБ

- **Не создана** СОИБ ЗОКИИ
- **Не определен** состав и структура СОИБ, функции ее участников, задачи по обеспечению ИБ ЗОКИИ
- **Не проводятся** мероприятия по повышению уровня знаний работников по вопросам обеспечения безопасности КИИ
- На заместителя руководителя субъекта КИИ **не возложены полномочия** по обеспечению ИБ, не определено структурное подразделение по вопросам ИБ

НАРУШЕНИЯ И НЕДОСТАТКИ: ТЕХНИЧЕСКИЕ МЕРЫ

- Выполняются не все положения требований регуляторов
- Нарушения в части управления доступом (избыточный состав административных учетных записей)
- Незащищенное двустороннее сетевое взаимодействие между компонентами ЗОКИИ и внешними системами
- Незапущенные на компонентах ЗОКИИ СЗИ
- Актуальные уязвимости на компонентах ЗОКИИ
- Несоответствие декларируемых в ОРД мер реализации в отдельных компонентах ОКИИ

РАНЖИРОВАНИЕ НАРУШЕНИЙ И НЕДОСТАТКОВ: ОПЫТ ЗАКАЗЧИКОВ

Высокий уровень критичности

- Необеспечение функционирования ОКИИ в выделенном сегменте сети
- Подключение к ОКИИ сторонних компонентов, а также использование в ОКИИ ПО, не предусмотренных РД
- Организация каналов доступа к Интернету, использование электронной почты
- Организация удаленного управления ОКИИ, удаленного администрирования программно-технических средств ОКИИ
- Наделение учетных записей избыточными правами, а также необоснованное предоставление прав доступа к компонентам ОКИИ

Средний уровень критичности

- Неактуальность документированных сведений о составе программных и программно-технических средств ОКИИ
- Отсутствие своевременного обновления ПО
- Несоответствие настроек программно-технических средств действующим политикам безопасности
- Небезопасное хранение парольной информации, неперсонифициро-ванные учетные записи, отсутствие матриц доступа и заявок на доступ
- Отсутствие проведения резервного копирования
- Недостатки в обеспечении безопасности физического доступа к компонентам ОКИИ

Низкий уровень критичности

- Недостатки, связанные с оформлением или ведением ОРД, журналов, заявок
- Недостатки, связанные с непроведением актуализации или недостаточной проработкой ОРД
- Недостатки, связанные с опечатыванием компонентов ЗОКИИ
- Недостатки, связанные с использованием неучтенных / немаркированных носителей информации при проведении резервного копирования компонентов ЗОКИИ

РЕАЛЬНАЯ ИБ

ЧТО ДЕЛАТЬ ДЛЯ ПОВЫШЕНИЯ УРОВНЯ ИБ?

«Самооценка»

CL DATAPK Audit

Мобильный комплекс для оперативного или периодического контроля состояния сетей АСУ ТП

ссылка на описание продукта

ePlat4m

Платформа автоматизации процессов системы управления информационной безопасностью

ссылка на описание продукта

R-Vision

Система автоматизации процесса управления уязвимостями

ссылка на описание продукта

Обучение сотрудников

Программа «Подготовка к госконтролю по КИИ»

- 2 дня обучения
- 8 теоретических занятий по темам:
  - Обзор законодательства по КИИ
  - Категорирование объектов КИИ
  - Обеспечение безопасности объектов КИИ
  - Государственный контроль
  - Подготовка к прохождению госконтроля
  - Действия при прохождении госконтроля (+практическое занятие)
  - Работа с нарушениями и недостатками, выявленными в результате государственного контроля
  - Типовые проблемы, возникающие при прохождении госконтроля
- онлайн-формат

Подписывайтесь на наш канал в Телеграме

- Ежемесячные обзоры изменения законодательства
- Разбор часто задаваемых вопросов по теме КИИ
- Экспертные статьи и кейсы

Кибербезопасность с УЦСБ

УЦСБ

СПАСИБО ЗА ВНИМАНИЕ!
ВОПРОСЫ?

Светлана Мадина

Аналитик направления аудитов и соответствия требованиям ИБ

2024

sec@ussc.ru

sec.ussc.ru

УЦСБ

СЕРИЯ ВЕБИНАРОВ

19.03	Обеспечение безопасности объектов КИИ в рамках 187-ФЗ
09.04	Как построить эффективную систему обеспечения ИБ объектов КИИ
25.04	Практика построения СОИБ: проблемы, решения, кейсы
28.05	Мониторинг инцидентов ИБ ОКИИ
04.06	Как обеспечить эффективное управление привилегированным доступом для защиты КИИ
09.07	Безопасная разработка ПО для значимых объектов КИИ
01.08	Как оценить защищенность ЗОКИИ и почему пентесты — эффективный инструмент
28.08	Как подготовиться к прохождению госконтроля в области защиты КИИ