

Краткий обзор функционирования
ГосСОПКА и вектора дальнейшего
развития. Отраслевые центры
ГосСОПКА



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ

Текущее состояние нормативной правовой базы в области ГосСОПКА



ФЗ от 26.07.2017 № 187-ФЗ
«О безопасности КИИ РФ»

ФЗ от 26.07.2017 № 194-ФЗ
«О внесении изменений в УК РФ»

ФЗ от 26.07.2017 № 193-ФЗ
«О внесении изменений отдельные
законодательные акты РФ»

Указ Президента РФ, утв.
22.12.2017 № 620

Приказ ФСБ России «Положение
о НКЦКИ» от 24.07.2018 № 366

Приказ ФСБ России «Перечень
информации, предоставляемой
в ГосСОПКА» от 24.07.2018 № 367

Приказ ФСБ России «Порядок
обмена информацией о КИ»
от 24.07.2018 № 368

Приказ ФСБ России «Требования
к средствам ГосСОПКА»
от 06.05.2019 № 196

Приказ ФСБ России «Порядок информирования
ФСБ России, о КИ, реагирования
на них, принятия мер по ликвидации последствий
КА, проведенных в отношении
значимых объектов КИИ РФ» от 19.06.2019 г. № 282

Приказ ФСБ России
«Порядок
и ТУ уст. и экспл.
средств ГосСОПКА»
от 19.06.2019 № 281

Методические документы НКЦКИ

Приказ ФСБ России «Перечень
информации, предоставляемой
в ГосСОПКА» от 13.02.2023 № 77

Указ Президента РФ «О дополнительных мерах
по обеспечению безопасности Российской Федерации»
от 01.05.2022 № 250

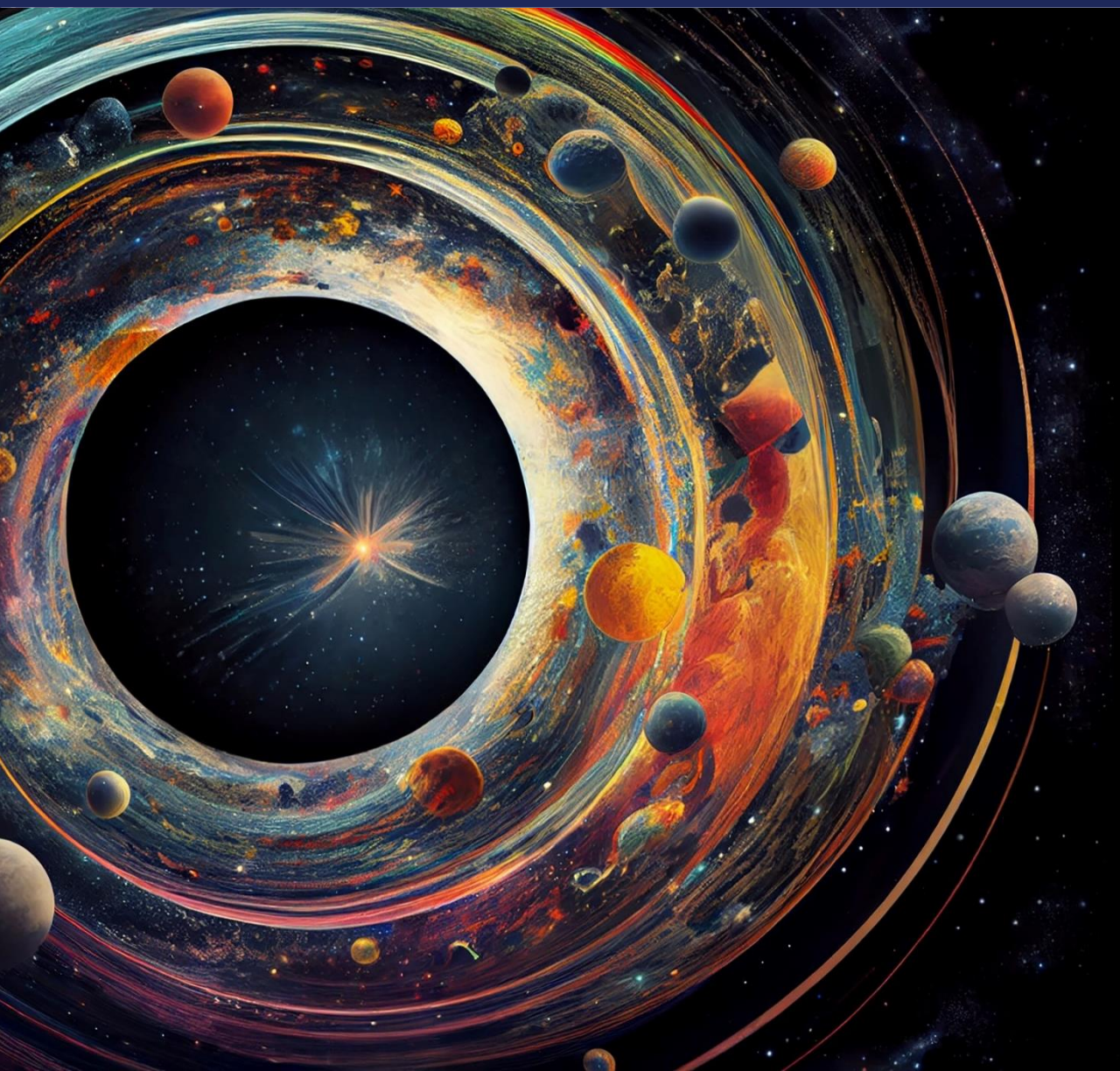
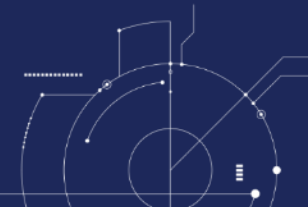
Приказ ФСБ России «Об
осуществлении мониторинга»
от 11.05.2023 № 213

Цель Указа Президента РФ № 250

Указ направлен на устранение пробелов, которыми пользовались недобросовестные руководители



Расширение орбиты ГосСОПКА



Требования по обеспечению ИБ теперь необходимо выполнять:

- государственным органам
- государственным фондам
- государственным корпорациям
- стратегическим предприятиям
- системообразующим организациям

Основные тезисы Указа Президента РФ № 250



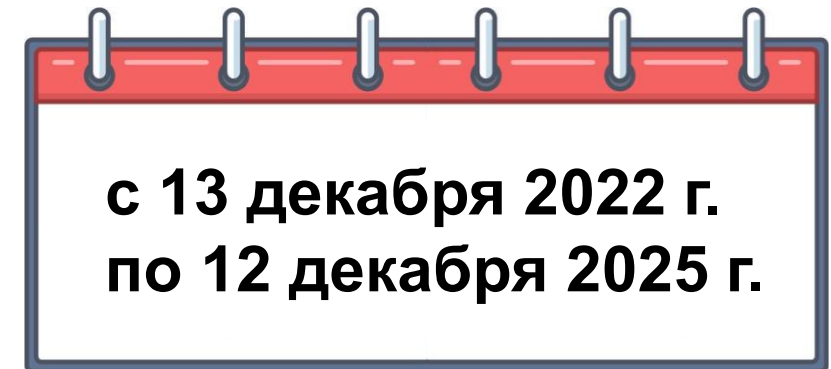
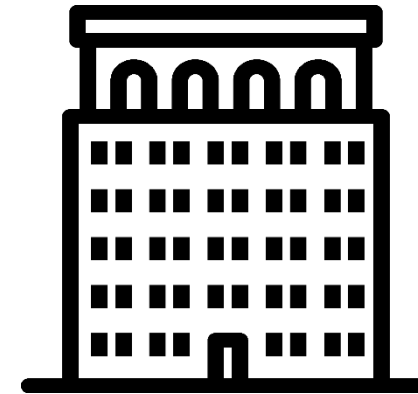
Заместители руководителей теперь будут отвечать за ИБ и мероприятия по обнаружению компьютерных атак и реагированию на компьютерные инциденты

Необходимо определить структурное подразделение, ответственное за ИБ

Вопросы аккредитации центров ГосСОПКА

К деятельности в рамках ГосСОПКА могут привлекаться только организации, являющиеся аккредитованными центрами ГосСОПКА

Переходный период, в рамках которого возможна реализация мероприятий силами организаций, имеющих соглашения с ФСБ России и (или) НКЦКИ



Порядок аккредитации центров ГосСОПКА, определяет:

- порядок подачи заявки и её рассмотрения, прохождения документарной проверки, проверки знаний и навыков специалистов центра, сроки действия аккредитации, порядок её отзыва

Требования к аккредитуемым центрам ГосСОПКА

- действующие требования к подразделениям и должностным лицам субъектов ГосСОПКА будут переработаны с учетом текущих реалий



Процедура проверки в рамках аккредитации

- проверка документов и сведений, представленных соискателем
- проверка знаний и навыков сотрудников центра ГосСОПКА
- проверка достоверности представленных сведений



Аккредитация центров ГосСОПКА. Ограничения

- срок аккредитации – **5** лет
- досрочное приостановление аккредитации
- отзыв аккредитации



Основные причины приостановления и отзыва аккредитации

Не соответствие требованиям:

- сокрытие информации от НКЦКИ о компьютерных инцидентах
- невыполнение запросов НКЦКИ в части деятельности в рамках ГосСОПКА

Не устранение выявленных несоответствий



**И ТАК,
СОЙДЕТ!**

Требования к центрам ГосСОПКА



- проведение мероприятий по обнаружению компьютерных атак и регистрации компьютерных инцидентов
- проведение мероприятий по реагированию на компьютерные инциденты и ликвидации их последствий
- проведение мероприятий по оценке защищенности информационных ресурсов от компьютерных атак
- координация подразделений субъектов ГосСОПКА, анализ и выработка рекомендаций по обеспечению защищенности информационных ресурсов

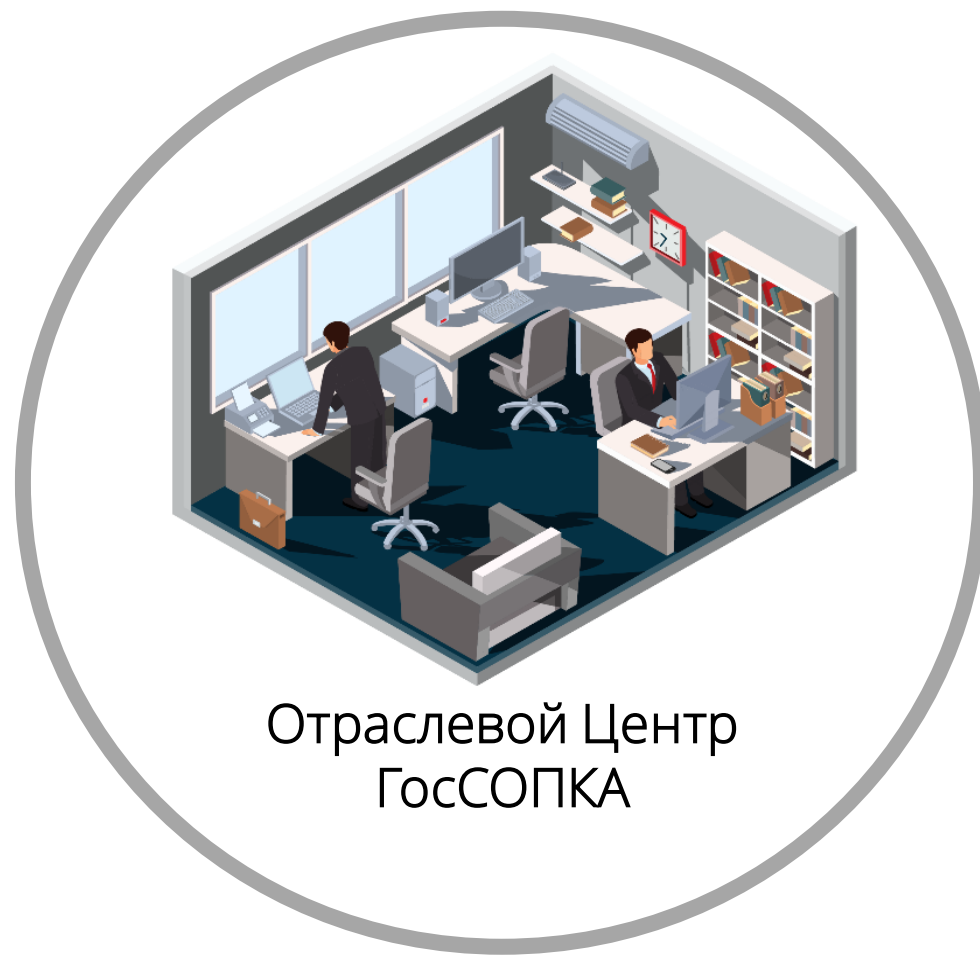
Как стать отраслевым центром ГосСОПКА?

Пройти аккредитацию как Центр ГосСОПКА с обязательным выполнением функций координации подразделений субъекта ГосСОПКА при проведении мероприятий, анализа и выработки рекомендаций по обеспечению защищенности информационных ресурсов **с учетом отраслевых особенностей**



Отраслевые центры ГосСОПКА должны стать своего рода НКЦКИ отрасли:

- Координация мероприятий по реагированию на КИ в отрасли
- Анализ возникающих угроз и выработка соответствующих мер
- Оказание помощи субъектам ГосСОПКА с учетом отраслевой специфики
- Взаимодействие с НКЦКИ





Спасибо за внимание!



НАЦИОНАЛЬНЫЙ КООРДИНАЦИОННЫЙ ЦЕНТР
ПО КОМПЬЮТЕРНЫМ ИНЦИДЕНТАМ