Выполнение функций центра ГосСОПКА силами Solar JSOC

Соблюдение требований к субъектам КИИ в соответствии с 187-ФЗ, требованиями и методическими рекомендациями ФСБ России

rt-solar.ru

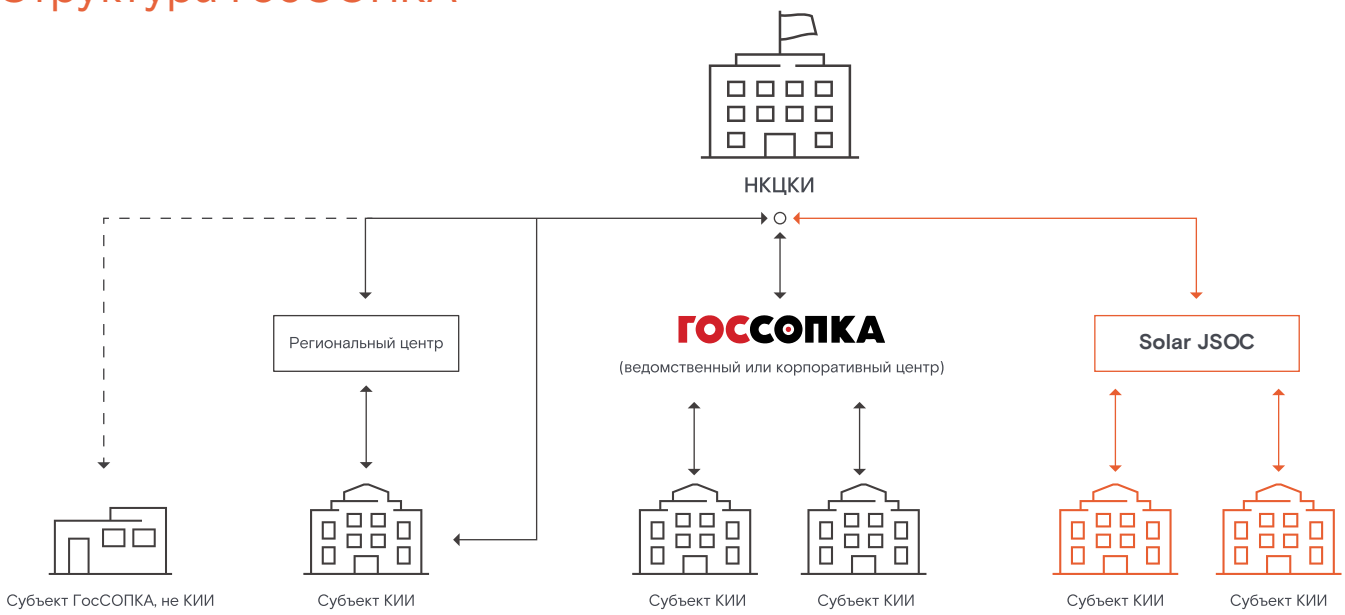
rt.ru

Ростелеком

Что такое ГосСОПКА

ГосСОПКА — государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации. Во главе ГосСОПКА стоит Национальный координационный центр по компьютерным инцидентам (НКЦКИ) — субъекты критической информационной инфраструктуры (КИИ) обязаны сообщать ему о произошедших компьютерных инцидентах.

Структура ГосСОПКА



Законодательные требования

- **187-ФЗ «О безопасности КИИ».** Все субъекты КИИ сообщают о компьютерных инцидентах в НКЦКИ
- **Приказы ФСТЭК России №235 и №239.** Значимые объекты КИИ создают системы защиты и обеспечивают непрерывное взаимодействие с НКЦКИ
- **Приказ ФСБ России №367.** Субъект КИИ отправляет информацию о компьютерном инциденте в НКЦКИ не позднее 24 часов с момента обнаружения
- **Приказ ФСБ России №282.** Субъекты КИИ — владельцы значимых объектов КИИ — отправляют информацию о компьютерном инциденте не позднее 3-х часов с момента обнаружения КИ
- Субъекты КИИ реализуют требования к персоналу, должностным лицам, налаживают выполнение функций ГосСОПКА
- **Статья 274.1 УК РФ.** Нарушение правил хранения, обработки или передачи охраняемой компьютерной информации, повлекшее тяжелые последствия, грозит лишением свободы до 10 лет

Субъекты КИИ, владеющие значимыми объектами КИИ, могут создать Центр ГосСОПКА и выполнять эти функции самостоятельно. Для этого необходимо:

Нанять специалистов

Установить средства защиты информации

Запустить процессы

Получить лицензии ФСТЭК и ФСБ России

Функции Центра ГосСОПКА

В соответствии методическими рекомендациями ФСБ России Центр ГосСОПКА должен выполнять следующие функции:

Взаимодействие с НКЦКИ

- Предоставление сведений о компьютерных инцидентах в течение 24 часов (3 для значимых объектов)
- Отправка результатов прогнозирования угроз ИБ
- Предоставление сведений о состоянии защищенности
- Направление предложений по совершенствованию средств ГосСОПКА
- Реагирование на запросы от НКЦКИ

Управление центром

- Разработка документов, регламентирующих процессы работы Центра
- Анализ угроз ИБ и прогнозирование их развития

Управление инцидентами

- Анализ событий ИБ
- Регистрация компьютерных атак и инцидентов
- Составление перечня компьютерных инцидентов

Контроль защищенности

- Составление и актуализация перечня угроз ИБ
- Инвентаризация уязвимостей
- Выявление уязвимостей

Противодействие атакам

- Эксплуатация средств ГосСОПКА
- Прием сообщений об инцидентах от пользователей
- Формирование предложений по повышению уровня защищенности информационных ресурсов
- Ликвидация последствий компьютерных инцидентов и анализ ее результатов
- Установление причин компьютерных инцидентов

В соответствии с п. 7.3 методических рекомендаций ФСБ России субъекты КИИ могут передать выполнение функций Центра ГосСОПКА сторонним организациям, осуществляющими лицензируемую деятельность в области защиты информации, — например Solar JSOC.

50,4 млн

минимум стоит самостоятельное построение Центра ГосСОПКА

1,5 года

уходит на создание Центра ГосСОПКА своими силами

20 человек

средняя численность персонала Центра ГосСОПКА

Преимущества

Solar JSOC берет на себя задачу выполнения функций Центра ГосСОПКА.

Обнаружение, предотвращение и ликвидация последствий компьютерных атак силами Центра ГосСОПКА Solar JSOC позволит:

- Запустить технический процесс мониторинга и реагирования на компьютерные атаки без долгосрочного интеграционного проекта
- Качественно повысить уровень реальной защищенности информационной инфраструктуры
- Привести организацию в соответствие с требованиями нормативных документов

«Ростелеком-Солар», компания группы ПАО «Ростелеком», обладает экспертизой и опытом мониторинга и управления инцидентами ИБ, включая создание и эксплуатацию Центров ГосСОПКА. В распоряжении наших клиентов ежедневно пополняемые базы актуальных угроз, собственные команды мониторинга, вирусной аналитики, тестирования на проникновения и расследования инцидентов ИБ.

ГосСОПКА за 2 месяца	Экономия бюджетов	Реальная экспертиза
Запустите базовые функции Центра ГосСОПКА менее чем за 2 месяца	Сэкономьте на персонале и техническом обеспечении благодаря передаче части функций в Solar JSOC	Используйте весь накопленный опыт Solar JSOC для защиты объектов КИИ

Узнать подробнее или заказать сервис presale@rt-solar.ru

Сервисы кибербезопасности «Ростелекома»

Solar MSS — кибербезопасность как сервис

- Защита от сетевых угроз (UTM)
- Защита веб-приложений (WAF)
- Защита электронной почты (SEG)
- Защита от DDoS-атак (Anti-DDoS)

ЕПСК*

- Шифрование каналов связи (ГОСТ VPN)
- Управление навыками ИБ (SA)
- Контроль уязвимостей (VM)
- Управление мобильными устройствами (EMM)

Solar JSOC — сервисы мониторинга и реагирования

- Мониторинг, реагирование и анализ инцидентов ИБ
- Контроль защищенности и управление уязвимостями
- Техническое расследование инцидентов
- Эксплуатация систем ИБ и реагирование на атаки
- Подготовка аналитики для бизнеса и поддержки принятия решения
- Сервисы ГосСОПКА

*Единая платформа сервисов кибербезопасности

О компании

ПАО «Ростелеком» — крупнейший в России провайдер цифровых услуг и решений, присутствующий во всех сегментах ИКТ-рынка. Компания — признанный технологический лидер в инновационных решениях в области электронного правительства, кибербезопасности, облачных вычислений, здравоохранения, образования, безопасности, жилищно-коммунальных услуг.

Ростелеком

info@rt-solar.ru rt.ru rt-solar.ru

+7 (499) 755-07-70

9.08.BR.SJ.GOS.01