SOLAR
Rostelecom

Ростелеком

В соответствии с Федеральным законом от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» и Указа Президента РФ от 15.01.2013 № 31с (ред. от 22.12.2017) «О создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы РФ» задача защиты критической информационной инфраструктуры (КИИ) выводится на качественно новый, государственный уровень.

По данным объективного контроля сервиса мониторинга Solar JSOC объекты КИИ государства подвержены огромному числу киберугроз, источниками которых являются преступные группировки, политически или социально мотивированные «хактивисты», а подчас и отдельные государства.

- Собственный SOC дорого и долго?
- Нет специалистов для отражения таргетированных атак?
- ИБ-специалисты перегружены эксплуатацией средств защиты?

В соответствии с Федеральным законом

187-ФЗ

Решение по созданию центров ГосСОПКА от Solar JSOC

SOLAR
JSOC
Rostelecom

Чтобы эффективно противодействовать такого рода ударам и обеспечивать штатное функционирования объектов КИИ в условиях возникновения компьютерных инцидентов, создается государственная система обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации — ГосСОПКА.

Функции центров ГосСОПКА

Согласно указу президента № 31с и концепции ГосСОПКА она включает в себя главный, ведомственные, региональные и корпоративные центры. Они решают задачи сбора и анализа информации о компьютерных атаках и компьютерных инцидентах, обеспечивают оперативное реагирование на угрозы, а также осуществляют мероприятия по ликвидации последствий компьютерных инцидентов в информационных ресурсах с использованием специализированных программных решений и построенных процессов эксплуатации данных систем.

В соответствии с методическими рекомендациями ФСБ России ведомственные и корпоративные центры ГосСОПКА призваны осуществлять мониторинг, анализ и расследование инцидентов, анализ защищенности и целый ряд других функций.

Информационное взаимодействие с ГЦ ГосСОПКА

УПРАВЛЕНИЕ ЦЕНТРОМ

- Оценка и контроль эффективности мер безопасности инфраструктуры объекта
- Прогнозирование угроз

УПРАВЛЕНИЕ ИНЦИДЕНТАМИ

- Обнаружение атак
- Регистрация инцидентов
- Анализ событий и инцидентов

КОНТРОЛЬ ЗАЩИЩЕННОСТИ

- Инвентаризация ресурсов
- Выявление уязвимостей
- Анализ угроз

ПРОТИВОДЕЙСТВИЕ АТАКАМ

- Реагирование на инциденты
- Ликвидация последствий
- Анализ причин возникновения

Таким образом, каждая организация, владеющая объектом КИИ, встает перед выбором путей решения указанных задач внутренними ресурсами:

Подбором и обучением специалистов	Разработкой регламентной базы	Запуском процессов, обеспечивающих функции ГосСОПКА

или с привлечением внешней компании

Правила создания и эксплуатации центров ГосСОПКА

Деятельность центров ГосСОПКА может обеспечиваться услугами аккредитованного корпоративного центра. Согласно пункту 7.3.3 Методических рекомендаций по созданию ведомственных и корпоративных центров, деятельность центра ГосСОПКА может обеспечиваться:

Путем заключения договоров на выполнение сторонними организациями, осуществляющими лицензируемую деятельность в области защиты информации

Функции центра ГосСОПКА, реализуемые в рамках оказания услуги

Контроль защищенности инфраструктуры компании/государственной организации

Взаимодействие с главным центром ГосСОПКА

Мониторинг и реагирование на компьютерные атаки

Готовые к использованию сервисы позволяют органам исполнительной власти передать функции обнаружения компьютерных атак, реагирования и анализа инцидентов, а также двустороннему взаимодействию с Главным центром ГосСОПКА в центре мониторинга и реагирования на компьютерные инциденты компании Ростелеком-Solar.

Создание и эксплуатация центра ГосСОПКА силами Solar JSOC помогает организациям:

- построить программно-аппаратную платформу и методическую базу, требуемую для функционирования ведомственного/корпоративного центра ГосСОПКА;
- привести компанию в соответствие с требованиями федерального закона о КИИ и методических рекомендаций о создании ведомственных и корпоративных центров ГосСОПКА;
- качественно повысить уровень реальной защищенности и обеспечить непрерывный мониторинг и реагирование на возникающие компьютерные атаки.

Преимущества решения Solar JSOC

Компания Ростелеком-Solar обладает экспертизой и опытом эксплуатации Центров мониторинга и управления инцидентами ИБ, включая создание и эксплуатацию центров ГосСОПКА. К таким проектам можно отнести: информационное и техническое взаимодействие в вопросах мониторинга и реагирования на инциденты с ДИТ Самары, ведомственным центром ГосСОПКА, обеспечение функций мониторинга киберугроз в КИИ финансового сектора (НСПК, Почта Банк, ТКС, МТС-Банк), энергетических, транспортных и государственных заказчиков.

ГосСОПКА за 2 месяца	Экономия бюджетов	Реальная экспертиза
Запустите базовые функции своего ведомственного или корпоративного сегмента ГосСОПКА менее чем за 2 месяца	Сэкономьте значительные средства на персонале благодаря передаче части функций в Solar JSOC	Используйте весь накопленный опыт проектов и наработок Solar JSOC для построения инфраструктуры и процессов ГосСОПКА

Центр мониторинга безопасности Solar JSOC позволит избежать распространенных сложностей при построении центров ГосСОПКА:

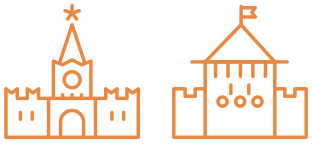
- отсутствие или неэффективность существующих инструментов ИБ для реализации задач корпоративного или ведомственного центра;
- невозможность своевременно выявлять и анализировать возникающие инциденты ИБ силами малочисленного и высоконагруженного подразделения ИБ;
- недостаток уровня экспертизы для поддержания необходимого уровня актуальных сценариев выявления, реагирования и расследования инцидентов ИБ;
- отсутствие опыта, методических наработок создания центров мониторинга ИБ в организации.

В распоряжении наших клиентов ежедневно пополняемые базы актуальных угроз (Threat Intelligence), собственные команды мониторинга, вирусной аналитики, тестирования на проникновения, расследования инцидентов ИБ.

Почему Solar JSOC

- Solar JSOC — первый в России коммерческий центр мониторинга и реагирования на инциденты ИБ.
- К Solar JSOC подключено более 100 клиентов: государственные организации, предприятия энергетики, крупные финансовые организации, транспортные компании.
- Solar JSOC обеспечивает мониторинг кибератак и внутренних нарушений, реагирование на инциденты, противодействие атакам, проведение расследований, контроль защищенности и устранение выявляемых уязвимостей в режиме 24×7.
- Налажено взаимодействие с Центром реагирования на компьютерные инциденты в информационных системах органов государственной власти Российской Федерации (GOV-CERT.RU), а также с другими ключевыми SOCами и CERTами России — Банком России (FinCERT), Министерством обороны Российской Федерации, операторами связи и др.
- Все работы проводятся в соответствии с требованиями законодательства и методическими рекомендациями ФСБ России.

1-я линия дежурной смены в режиме 24×7 обрабатывает свыше 280 000 событий с подозрением на инциденты в год.



Две площадки в Москве и Нижнем Новгороде обеспечивают катастрофоустойчивую инфраструктуру сервисов.

Более 90 специалистов дежурной смены — аналитики, эксперты.

SOLAR Rostelecom

Ростелеком

Компания Ростелеком-Solar, входящая в группу ПАО «Ростелеком», — национальный провайдер сервисов и технологий кибербезопасности.

rt-solar.ru
info@rt-solar.ru
+7 (499) 755-07-70