



Кибербезопасность

Коммерческое предложение

Ростелеком

Ключевые особенности Solar MSS

Solar MSS компании ПАО «Ростелеком» — экосистема управляемых сервисов кибербезопасности (MSS), решающих задачи по защите от киберугроз в процессе цифровой трансформации российских организаций.

Между сервисами налажен процесс обогащения телеметрией по угрозам и атакам, что позволяет непрерывно совершенствовать технологии и политики безопасности каждого из них.

Защита от всех основных типов атак

Сервисы Solar MSS защищают от сетевых и веб-атак, фишинга, спама, DDoS-атак, позволяют шифровать каналы связи, выявлять уязвимости в ИТ-инфраструктуре и обучать сотрудников навыкам кибербезопасности

Команда экспертов

За эксплуатацию и обновление средств защиты отвечают специалисты «Ростелеком» и Solar JSOC, обеспечивающие клиентам непрерывную защиту от кибератак в режиме 24/7

Преимущества Solar MSS

1

Быстрое подключение и простая масштабируемость

2

Возможность подключения дополнительных сервисов

3

Просчитываемые ежемесячные платежи

4

Мониторинг и реагирование 24 часа в сутки

5

Перевод капитальных издержек на ИБ в операционные

6

Устранение дефицита ИБ-специалистов

7

Отсутствие дополнительных затрат

8

Соответствие законодательству РФ

Ценообразование Solar MSS

Сервисы	Стоимость	Срок
Защита от сетевых угроз	20-200 тыс. рублей	в месяц за одну площадку
Защита электронной почты	от 30 тыс. рублей	
Защита от атак на веб-сайты и веб-приложения	80-300 тыс. рублей	
Защита каналов связи	10-30 тыс. рублей	
Управление навыками кибербезопасности	от 133 рублей	в год за одного сотрудника
Контроль уязвимостей	от 10 тыс. рублей	за одно сканирование или в месяц в зависимости от варианта сканирования

Ключевые особенности Solar JSOC

Solar JSOC компании ПАО «Ростелеком» — первый и крупнейший коммерческий центр мониторинга и реагирования на инциденты кибербезопасности (SOC) в России.

Solar JSOC активно сотрудничает с ФинЦЕРТ Банка России и НКЦКИ ФСБ России. Организованы информационный обмен и сотрудничество с ведущими мировыми аналитическими центрами для оперативного противодействия киберпреступности.

Высокий уровень обслуживания

Каждые сутки в Solar JSOC анализируется более 72 млрд. событий ИБ. Жесткие соглашения по уровню обслуживания отводят не более 10 минут на обнаружение кибератаки и не более 30 минут на реагирование и защиту

Команда экспертов

Более 170 специалистов Solar JSOC противодействуют сложным целенаправленным кибератакам и устраняют причины возникновения инцидентов, проводят расследования и проверяют устойчивость организаций к кибератакам

Преимущества Solar JSOC

1 Самая опытная команда на рынке

2 Филиалы в Москве, Нижнем Новгороде, Самаре и Хабаровске

3 Работа во всех часовых поясах страны

4 Опыт защиты крупнейших клиентов и мероприятий

5 Крупнейший коммерческий SOC страны

6 Круглосуточный мониторинг и реагирование

7 Сотрудничество с ФинЦЕРТ Банка России и НКЦКИ ФСБ России

8 Все требуемые лицензии и соглашения

Ценообразование Solar JSOC

Сервисы Solar JSOC

Мониторинг, анализ и реагирование на инциденты

Специальные сервисы ГосСОПКА

Техническое расследование инцидентов

Консалтинг по построению SOC

от 500 000 ₽ в месяц

Защита АСУ ТП и КИИ. Ключевые особенности

Специалисты «Ростелекома» предоставляют полный комплекс услуг в области защиты АСУ ТП и КИИ, начиная от категорирования объектов КИИ в соответствии с 187-ФЗ и заканчивая проведением киберучений и исследований ПО АСУ ТП и IIoT на наличие уязвимостей и недекларированных возможностей.

Возможно подключение АСУ ТП к сервисам мониторинга и реагирования Solar JSOC компании ПАО «Ростелеком».

Всесторонняя защита АСУ ТП

Полный комплекс услуг по защите АСУ ТП: от тестирования на проникновение и проведения киберучений до круглосуточного мониторинга и выявления уязвимостей и недекларированных возможностей в компонентах АСУ ТП и IIoT

Лаборатория кибербезопасности

«Лаборатория кибербезопасности АСУ ТП» — центр компетенций «Ростелекома». Собственные методики, сотрудничество с мировыми вендорами и команда экспертов международного уровня позволяют решать даже самые сложные задачи

Защита АСУ ТП и КИИ. Преимущества

1

Одни из лидеров в рейтинге БДУ ФСТЭК России по количеству выявленных уязвимостей

4

Большой опыт совместной работы с производителями компонентов АСУ ТП, регуляторами и CERT

2

Реальный опыт разработки и внедрения

5

Перекрестная экспертиза со специалистами Solar JSOC

3

Шоурум и тестовые полигоны для заказчиков

6

Собственные методики и лабораторная база

Защита АСУ ТП и КИИ. Ценообразование

Сервисы	Стоимость
Приведение в соответствие 187-ФЗ «О безопасности КИИ»	
Категорирование объекта КИИ	от 500 000 ₹
Проектирование подсистемы безопасности объекта КИИ	от 500 000 ₹
Построение подсистемы безопасности объекта КИИ (без поставки СЗИ)	от 1 000 000 ₹
Solar JSOC. Мониторинг и реагирование для систем промышленной автоматизации	от 500 000 ₹
Киберучения для владельцев АСУ ТП и субъектов КИИ	от 1 000 000 ₹
Тестирование на проникновение для АСУ ТП (одна средняя площадка)	от 500 000 ₹
Выявление уязвимостей и НДВ в компонентах АСУ ТП и IIoT (одна средняя площадка)	от 800 000 ₹
Комплексный анализ (аудит) защищенности АСУ ТП (одна средняя площадка)	от 1 000 000 ₹