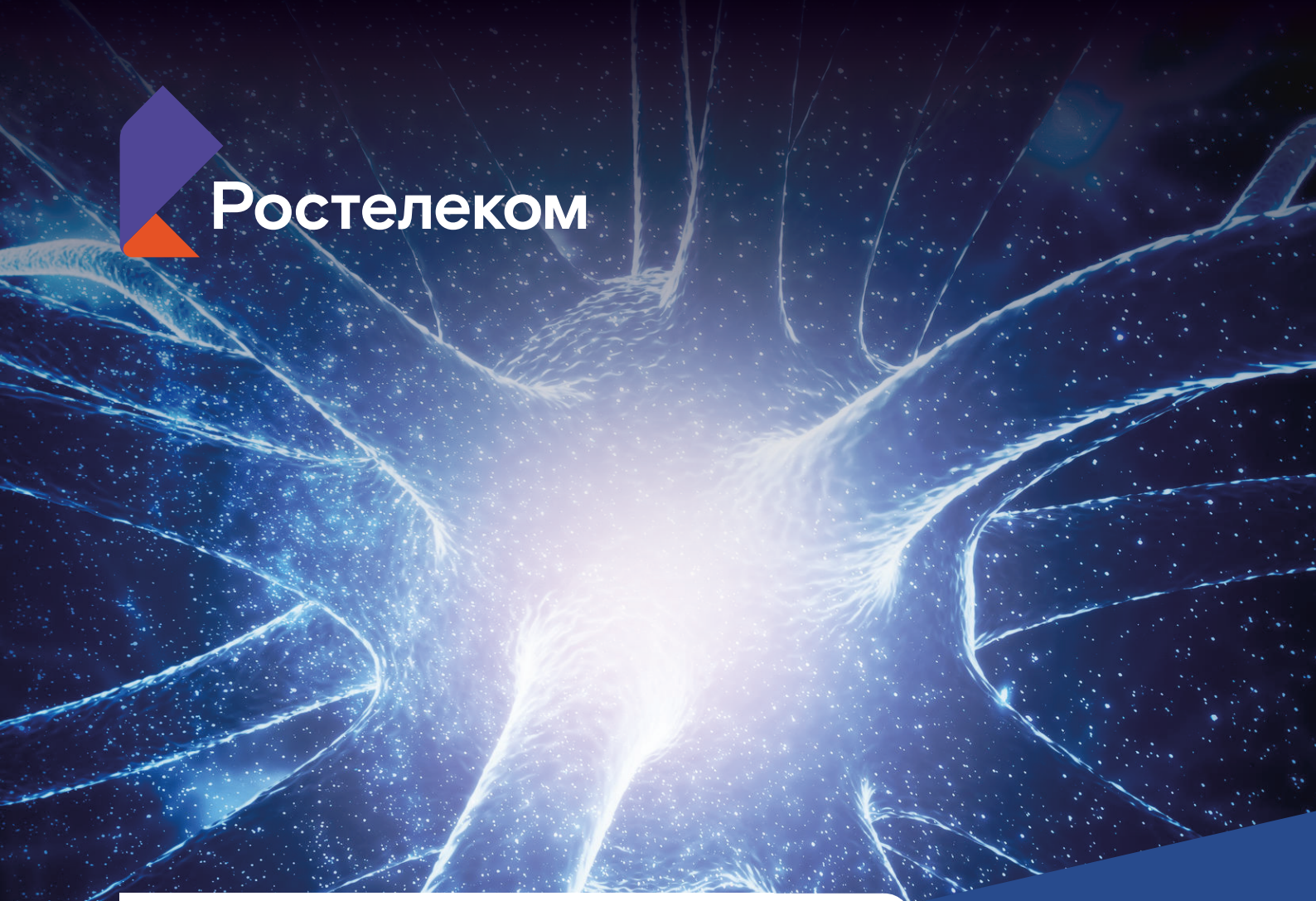


Ростелеком

# Solar MSS

## Кибербезопасность как сервис

- rt-solar.ru
- rt.ru

# Solar MSS

Solar MSS — экосистема управляемых сервисов кибербезопасности (Managed Security Services, MSS), которые призваны защитить российские организации от киберугроз в процессе цифровой трансформации.

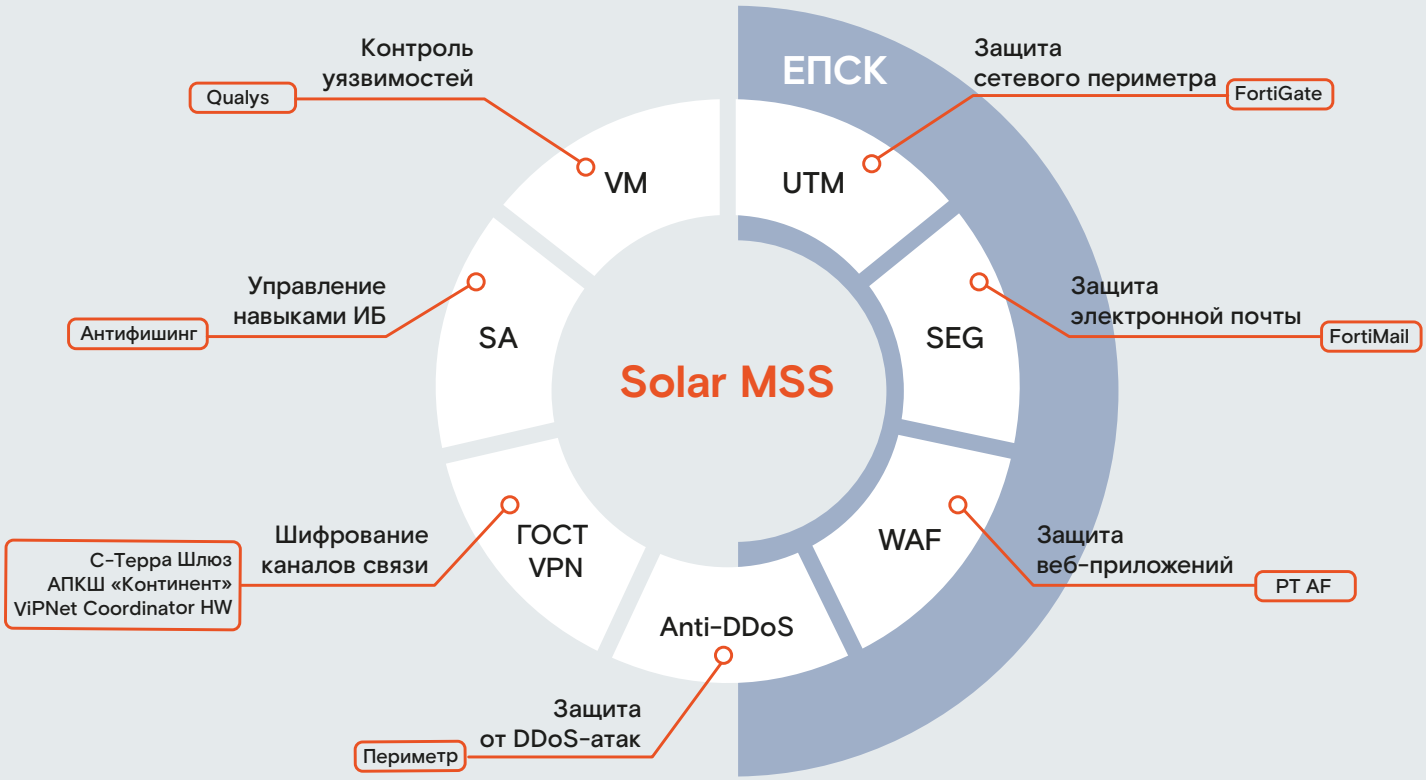
В основе Solar MSS — опыт оказания сервисов, накопленный с момента запуска Единой платформы сервисов кибербезопасности (ЕПСК) в ноябре 2018 года.

**Solar MSS**

- Технологии
  - SD-WAN — Программно-определяемые сети
  - NFV — Виртуализация сетевых функций
  - ZTP — Автоматическая настройка устройств
- Опыт экспертов
- Реализованные проекты
- Обратная связь клиентов

**Решения для бизнеса**

Сегодня экосистема Solar MSS является лидером российского рынка по количеству технологий защиты от киберугроз. Между сервисами налажен взаимный обмен телеметрией по угрозам и атакам. Технологии Solar MSS способны обеспечить защиту от всех основных типов атак, сфокусировавшись на сегментах, наиболее критичных для каждой отдельной организации.




## Технологическая основа

POSITIVE TECHNOLOGIES · infotecs · NOKIA · FORTINET · ГАРДА ТЕХНОЛОГИИ · Qualys. · КОД БЕЗОПАСНОСТИ · s•terra

# Сервисная модель

## Экономия и эффективность

**Снижение стоимости владения**
Совокупная стоимость владения сервисами дешевле покупки, внедрения и последующей поддержки ИБ-решений.

**Устранение дефицита кадров**
Отсутствие необходимости создания отдела из высококвалифицированных ИБ-специалистов.

**Экономия**
Снижение затрат на оборудование и персонал, перевод капитальных издержек в операционные.

**Профессиональная команда**
Настройка, обслуживание и разбор инцидентов безопасности лучшими специалистами отрасли.

## Технологичность и надежность

**Доступность**
Защита и мониторинг 24 часа в сутки без перерывов и выходных.

**Надежность**
Эксплуатация распределенной отказоустойчивой инфраструктуры.

**Гибкость**
Простая масштабируемость и быстрое изменение параметров услуги.

**Скорость**
Быстрое подключение к сервисам и оперативное реагирование на инциденты.

## Соблюдение законодательства

**Соответствие требованиям**
Выполнение требований законодательства и регуляторов РФ.

**Подходящие средства защиты**
Эксплуатация сертифицированных решений лидирующих вендоров.

**Лицензии регуляторов**
Компания является лицензиатом ФСТЭК России, ФСБ России и Минобороны России.

**Отслеживание изменений**
Меры защиты всегда соответствуют всем новым законам и регламентам.

# Преимущества Solar MSS

## Экосистема

Все сервисы дополняют друг друга

## Удобное управление

Все параметры гибко настраиваются в личном кабинете

## Опыт

Готовые решения для каждого сегмента

## Мониторинг и реагирование

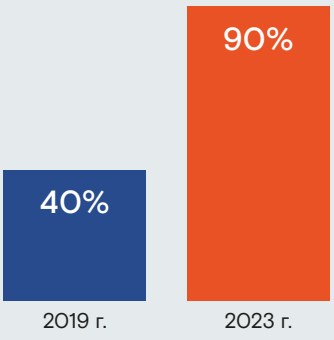
Solar JSOC обогащает сервисы экспертной аналитикой, индикаторами угроз и методами противодействия злоумышленникам

## Фокус на бизнесе

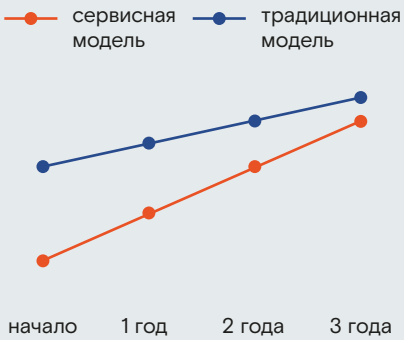
Решение не отдельных проблем ИБ, а комплексная защита бизнес-активов

## Проверенные технологии

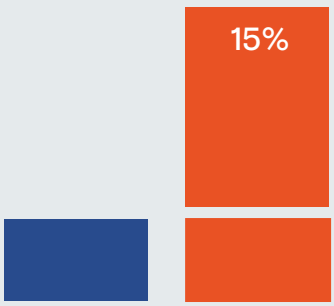
Сервисы Solar MSS используют только проверенные решения лидирующих вендоров




Распространение технологии SD-WAN согласно прогнозу Gartner




Сравнение платежей сервисной и традиционной моделей




Среднегодовой темп распространения сервисной модели в мире согласно отчету MSSP Alert

# Сервисы Solar MSS на базе ЕПСК

В состав ЕПСК входят три сервиса: сервис защиты от сетевых угроз (UTM), сервис защиты электронной почты (SEG) и сервис защиты веб-приложений (WAF). Они могут использоваться как одновременно, так и по отдельности. Для подключения сервисов на стороне клиента устанавливается CPE (Customer Premises Equipment).

С помощью ЕПСК также может предоставляться сервис защиты от DDoS-атак (Anti-DDoS), что делает его доступным клиентам любых интернет-провайдеров. При одновременном подключении сервисов Anti-DDoS и WAF клиенты получают комплексную защиту веб-ресурсов от уровня канала до бизнес-логики приложения.


# Customer Premises Equipment

CPE — телекоммуникационное оборудование, которое устанавливается на стороне клиента и предназначено для передачи трафика между ЦОД «Ростелекома» и инфраструктурой клиента. Клиентский трафик может передаваться в зашифрованном виде. В качестве каналов связи можно использовать как фиксированную, так и мобильную сеть.

## Технологии

### SOFTWARE DEFINED WIDE AREA NETWORK

Создает единую точку управления всей инфраструктурой: достаточно изменить настройки одного устройства, и обновления распространятся на все CPE сети. Это дает возможность оперативно изменять конфигурацию оказываемых сервисов кибербезопасности.

### NETWORK FUNCTIONS VIRTUALIZATION

Позволяет исполнять сетевые функции и функции сетевой безопасности программными модулями, работающими на стандартных серверах и виртуальных машинах. Программные модули могут взаимодействовать между собой для предоставления услуг связи, что позволяет отказаться от менее гибких аппаратных платформ.

### ZERO TOUCH PROVISIONING

Обеспечивает автоматическую настройку CPE без участия пользователя. Это позволяет максимально быстро развертывать сервисы кибербезопасности.

# Сервис защиты от сетевых угроз (UTM)

ЕПСК

Сервис обеспечивает комплексную безопасность сетевого периметра организации с помощью нескольких взаимосвязанных средств защиты: межсетевого экрана, системы предотвращения вторжений, антивирусного ПО, а также спам- и веб-фильтров.

Комплексная борьба с сетевыми угрозами

Централизация доступа в сеть для филиалов

Применение единых политик безопасности


Защита от атак в режиме 24×7

# Сервис защиты веб-приложений (WAF)

ЕПСК

Сервис обеспечивает обнаружение и блокировку атак на веб-приложения, которые пропускают традиционные межсетевые экраны. В их число входят атаки из списка OWASP Top 10 и классификации WASC, DDoS-атаки уровня приложений (L7) и атаки нулевого дня (0-day).


Защита от атак из списка OWASP Top 10

Защита от DDoS-атак уровня приложений

Защита от уязвимостей веб-приложений


Защита от атак в режиме 24×7

# Сервис защиты от DDoS-атак (Anti-DDoS)

ЕПСК

Сервис нейтрализует атаки, выводящие из строя сайты, онлайн-приложения и сервисы (DDoS-атаки), гарантируя их доступность для легитимных пользователей. Он защищает каналы, сетевую инфраструктуру и веб-ресурсы компании, многоступенчато фильтруя атаки на всех уровнях модели OSI. Сервис доступен организациям со сложной инфраструктурой, подключенной к любым интернет-провайдерам.

Доступность всех интернет-сервисов и приложений

Защита распределенной интернет-инфраструктуры на уровнях L3-L4 модели OSI

Защита веб-сайта компании, в том числе от атак уровня приложений

# Сервис защиты электронной почты (SEG)

ЕПСК

Сервис обеспечивает многоуровневую проверку электронной почты до того, как она достигнет почтовых серверов организации и будет доставлена конечному пользователю. Основой сервиса является шлюз защиты электронной почты (SEG), обладающий специализированными механизмами защиты от спама, фишинга и вредоносного ПО.


Борьба со спамом

Борьба с фишингом

Борьба с вредоносным ПО


Защита от атак в режиме 24×7

# Сервис шифрования каналов связи (ГОСТ VPN)

Сервис защищает информацию при передаче по открытым каналам связи, обеспечивая конфиденциальность и целостность данных. Архитектура и используемые СКЗИ позволяют реализовывать проекты любого масштаба по построению защищенных сетей.

Для подключения сервиса необязательно использовать услуги связи ПАО «Ростелеком» — сервис доступен как вместе с ними, так и отдельно.

Быстрое подключение сервиса шифрования каналов связи

Перемещение ответственности за систему криптозащиты на сторону компании «Ростелеком»


Мониторинг и реагирование в режиме 24×7

# Сервис управления навыками информационной безопасности (SA)

Сервис предоставляет платформу для тестирования и обучения сотрудников практической кибербезопасности. Имитируя фишинговые атаки, сервис выявляет сотрудников с недостаточным уровнем знаний и предоставляет необходимые курсы для повышения квалификации.

Вся необходимая для работы сервиса инфраструктура — личный кабинет пользователя и автоматизированная система дистанционного обучения и тестирования — размещается на вычислительных мощностях ПАО «Ростелеком».

Обучение выявлению фишинга

Определение опасных сайтов

Защита данных на мобильных устройствах


Соблюдение парольной политики

# Сервис контроля уязвимостей (VM)

Сервис проверяет соблюдение политик, упрощает управление уязвимостями и мониторинг информационной безопасности. Настраиваемые отчеты, интеграция с другими системами и набор модулей снижают затраты на оборудование и нагрузку на ИТ-отдел компании.

Мониторинг внешнего периметра для защиты от киберугроз

Контроль уровня защищенности удаленных сотрудников

Контроль соблюдения внутренних политик и требований регуляторов


Точная информация об уровне защищенности в любой момент

# «Ростелеком-Солар» — провайдер сервисов кибербезопасности

«Ростелеком-Солар», компания группы ПАО «Ростелеком», — национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления кибербезопасностью.

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами защиты. Этот принцип реализован в продуктах и сервисах «Ростелеком-Солар».

**№1**
на рынке сервисов ИБ

**600+**
экспертов кибербезопасности

**70+**
клиентов из топ-100 российского бизнеса

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)

### 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
- Сервисы ГосСОПКА

*Единая платформа сервисов кибербезопасности

## Нас выбрали

Банк России · Верховный Суд России · БИНБАНК · МТС Банк · РоссельхозБанк · МИР · Яндекс Деньги · Росфинмониторинг · Почта Банк · CARTREK · РОСБАНК · EXANTE · СТС · Роснефть · S7 Airlines · Уральский Банк реконструкции и развития · Тинькофф Банк · Leroy Merlin · Газпром нефть · Compliance Control · Министерство обороны Российской Федерации · Таможенная Карта · Юнипро · Банк Санкт-Петербург · Корпорация Тактическое Ракетное Вооружение · Малахит · ФСК ЕЭС · Иркут · РЖД · Федеральная пассажирская компания

Ростелеком

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

+7 (499) 755-07-70