



# Единая платформа сервисов кибербезопасности

Набор сервисов для защиты ИТ-инфраструктуры  
и приложений от сетевых угроз и вредоносного ПО

**Ростелеком**

# Ростелеком-Solar — провайдер сервисов кибербезопасности

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

В основе наших технологий лежит понимание, что настоящая информационная безопасность (ИБ) возможна только через непрерывный мониторинг и удобное управление системами ИБ. Этот принцип реализован в продуктах и сервисах Ростелеком-Solar.

Все сервисы кибербезопасности оказываются на основе SLA с четко прописанными условиями.

## Единая платформа сервисов кибербезопасности

Единая платформа сервисов кибербезопасности (ЕПСК) — набор сервисов для защиты ИТ-инфраструктуры и приложений от различных сетевых угроз и вредоносного ПО. Применение ЕПСК позволяет идентифицировать и закрыть слепые зоны в сетевом периметре организации, обеспечить применение лучших практик по защите информации и круглосуточное реагирование на инциденты безопасности, а также привести процессы защиты информации в соответствие с требованиями регуляторов и законодательством РФ.

Помимо повышения уровня защищенности ЕПСК позволяет перевести капитальные затраты в операционные, что приводит к снижению издержек на кибербезопасность и повышает точность их прогнозирования. Параметры ЕПСК можно гибко настраивать под текущие потребности бизнеса — быстро уменьшать или увеличивать производительность, расширять функциональность, а также подключать новые филиалы или точки продаж.

Одной из главных ценностей, предоставляемых ЕПСК, является переход от фрагментарной защиты информации, когда мониторинг и реагирование на инциденты ИБ осуществляются только в будние дни (режим 8×5), к непрерывной защите от кибератак в режиме 24×7.

Таким образом, переход на ЕПСК приводит к повышению уровня защищенности сетевого периметра организации при одновременном снижении издержек на кибербезопасность, позволяя сконцентрироваться на решении первоочередных бизнес-задач.

## Ростелеком-Solar в цифрах

**№1**

на рынке сервисов ИБ

**350+**

экспертов кибербезопасности

**5**

филиалов SOC в России

**50+**

клиентов из топ-100 российского бизнеса

**№1**

на рынке SOC

**10**

минут на обнаружение атаки

**30**

минут на реагирование и защиту

**14,4+**

миллиардов событий в сутки

# Схема функционирования ЕПСК



## Преимущества сервисной модели

### 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

#### СООТВЕТВИЕ ТРЕБОВАНИЯМ

Выполнение требований законодательства и регуляторов РФ.

#### ПОДХОДЯЩИЕ СРЕДСТВА ЗАЩИТЫ

Эксплуатация сертифицированных решений от 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.

# Сервис защиты веб-приложений

## На базе решения класса Web Application Firewall (WAF)

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, DoS-атаки уровня приложений (L7) и атаки нулевого дня (0-day).

Сервис размещается в облачной платформе Ростелеком-Solar и эксплуатируется высококлассными специалистами Центра мониторинга и реагирования Solar JSOC.

### Решаемые задачи



Защита от атак из списка OWASP Top-10



Защита от DoS-атак уровня приложений



Защита от уязвимостей веб-приложений



Защита от атак в режиме 24×7

### Состав сервиса

ОПЕРАТИВНАЯ АКТУАЛИЗАЦИЯ ПОЛИТИК И СИГНАТУР

КОНСУЛЬТАЦИИ ПО ПРИМЕНЕНИЮ СЕРВИСА

ВЫЯВЛЕНИЕ, АНАЛИЗ И РЕАГИРОВАНИЕ НА ИНЦИДЕНТЫ ИБ

ПОДДЕРЖКА В РЕЖИМЕ 24×7

### Схема функционирования сервиса



### Преимущества сервиса

- Комплексная защита веб-приложений
- Защита от атак нулевого дня и атак OWASP Top-10
- Поиск и блокирование уязвимостей веб-приложений
- Применение актуальных настроек и сигнатур
- Снижение затрат на ИБ-персонал и оборудование
- Переход к контролируемым операционным затратам
- Подключение новых точек за 24 часа
- Мониторинг и реагирование в режиме 24×7

# Сервис по защите от сетевых угроз

## На базе решения класса Unified Threat Management (UTM)

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.

Сервис размещается в облачной платформе Ростелеком-Solar и эксплуатируется высококлассными специалистами Центра мониторинга и реагирования Solar JSOC.

### Решаемые задачи



Комплексная борьба с сетевыми угрозами



Централизация доступа в сеть для филиалов



Применение единых политик безопасности



Защита от атак в режиме 24×7

### Состав сервиса

- МЕЖСЕТЕВОЕ ЭКРАНИРОВАНИЕ
- ФИЛЬТРАЦИЯ ТРАФИКА ВЕБ-ПРИЛОЖЕНИЙ
- ЗАЩИТА ОТ ВРЕДОНОСНОГО ПО
- ОБНАРУЖЕНИЕ И ПРЕДОТВРАЩЕНИЕ ВТОРЖЕНИЙ
- КОНТРОЛЬ ИСПОЛЬЗОВАНИЯ ПРИЛОЖЕНИЙ В СЕТИ
- КОНСУЛЬТАЦИИ ПО ПРИМЕНЕНИЮ СЕРВИСА
- ПОДДЕРЖКА В РЕЖИМЕ 24×7

### Схема функционирования сервиса



### Преимущества сервиса

- Объединение разрозненных функций защиты сети
- Централизация точек выхода в Интернет
- Мгновенное применение единых ИБ-политик
- Снижение затрат на ИБ-персонал и оборудование
- Применение актуальных настроек и сигнатур
- Единая система статистики по ИБ
- Подключение новых точек за 24 часа
- Мониторинг и реагирование в режиме 24×7

# Сервис по защите электронной почты

## На базе решения класса Secure Email Gateway (SEG)

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.

Сервис размещается в облачной платформе Ростелеком-Solar и эксплуатируется высококлассными специалистами Центра мониторинга и реагирования Solar JSOC.

### Решаемые задачи



Борьба со спамом



Борьба с фишингом



Борьба с вредоносным ПО



Защита от атак в режиме 24×7

### Состав сервиса

ЗАЩИТА ОТ СПАМА, ФИШИНГА И ВРЕДОНОСНОГО ПО

МОНИТОРИНГ СОБЫТИЙ ИБ

EMAIL-АУТЕНТИФИКАЦИЯ

ПОДДЕРЖКА В РЕЖИМЕ 24×7

ПОДДЕРЖКА ЧЕРНЫХ И БЕЛЫХ СПИСКОВ

ФИЛЬТРАЦИЯ URL

КОНСУЛЬТАЦИИ ПО ПРИМЕНЕНИЮ СЕРВИСА

### Схема функционирования сервиса



### Преимущества

- Комплексная защита электронной почты
- Производительность — до 1 000 000 писем в час
- Снижение затрат на ИБ-персонал и оборудование
- Снижение нагрузки на почтовые серверы
- Повышение производительности труда сотрудников
- Быстрое изменение параметров услуги
- Подключение новых точек за 24 часа
- Мониторинг и реагирование в режиме 24×7

# Сервисы Ростелекома по кибербезопасности



## Комплекс сервисов защиты каналов связи

- Сервис защиты от DDoS-атак (**Anti-DDoS**)
- Сервис по шифрованию каналов связи (**ГОСТ VPN**)
- Сервис по контентной фильтрации трафика



## Единая платформа сервисов кибербезопасности

- Сервис по защите от сетевых угроз (**UTM**)
- Сервис защиты веб-приложений (**WAF**)
- Сервис по защите электронной почты (**SEG**)



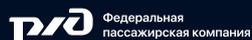
## Мониторинг и управление ИБ

- Мониторинг, реагирование и анализ инцидентов
- Контроль защищенности и управление уязвимостями
- Анализ безопасности состояния конфигураций систем ИБ
- Техническое расследование инцидентов
- Специальные сервисы **ГосСОПКА**

Узнать подробнее или заказать сервис

[presale@rt-solar.ru](mailto:presale@rt-solar.ru)

## Нас выбрали



Федеральная пассажирская компания



МСП Банк



РоссельхозБанк



Таможенная Карта  
Платежная система



РОСНЕФТЬ



ЭНЕРГОБАНК



Банк России



МИНИСТЕРСТВО ОБОРОНЫ  
РОССИЙСКОЙ ФЕДЕРАЦИИ



ВЕРХОВНЫЙ  
СУД РОССИИ

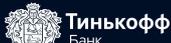
Яндекс Деньги



МТС Банк



БАШКОМСНАББАНК



Тинькофф  
Банк



Росфинмониторинг



ПОЧТА  
БАНК



CARTREK  
innovative cars sharing platform



РОСБАНК  
SOCIETE GENERALE GROUP



EXANTE



СТС



ГТТК-1



S7 AIRLINES



Уральский Банк  
реконструкции и развития



ВСЕРОССИЙСКИЙ БАНК  
РАЗВИТИЯ РЕГИОНОВ



LEROY MERLIN



ГАЗПРОМ  
НЕФТЬ



ISBC  
RFID



Compliance Control



БИНБАНК



ЮНИ  
ПРО



БАНК  
САНКТ-ПЕТЕРБУРГ



Корпорация  
Тактическое  
Ракетное  
Вооружение



МАЛАХИТ  
ИНДУСТРИАЛЬНЫЕ ТЕХНОЛОГИИ  
КОМПЛЕКСНОГО РЕШЕНИЯ ПРОБЛЕМ



ФСК  
ЕЭС



ИРКУТ  
ИПКУТ



MSOFT



Открытое Акционерное Общество  
ПРОМЫСЛОВЫЙ ЗАВОД



+7 (499) 755-07-70

[info@rt-solar.ru](mailto:info@rt-solar.ru) [rt.ru](http://rt.ru) [rt-solar.ru](http://rt-solar.ru)