SOLAR

ЗАЩИЩЕННЫЙ ДОСТУП К ВЕБ-РЕСУРСАМ

ГОСТ TLS

МОСКВА, 2024

W: RT-SOLAR.RU

ЗАЧЕМ НУЖЕН ПРОТОКОЛ TLS

Для безопасного взаимодействия между веб-ресурсом и пользователем используется протокол https («s» – secure), который обеспечивает:

- Конфиденциальность и целостность передаваемой информации. Трафик между веб-ресурсом и пользователем шифруется, злоумышленник не может получить доступ к передаваемым данным, а также произвести их подмену.

- Подлинность веб-ресурса, к которому обращается пользователь. Это повышает доверие посетителей к сайту. Кроме того, поисковые системы, такие как Yandex, Google, также отдают предпочтение защищенным сайтам при ранжировании результатов поиска, что способствует повышению видимости и рейтинга веб-ресурса.

Работа протокола основана на использовании SSL/TLS-сертификатов.

Сертификаты можно разделить на три условные группы по месту получения:

1) Западные центры сертификации, использующие зарубежную криптографию: DigiCert, Sectigo, GlobalSign. Сертификаты данных центров могут быть отозваны или не продлены из-за санкций. С такой ситуацией столкнулась Торгово-промышленная палата РФ в 2018 году, а в марте 2022 года – Банк ВТБ, Промсвязьбанк и Банк России.

2) Национальный удостоверяющий центр (НУЦ) Минцифры России, использующий зарубежную криптографию. Данный вариант сейчас активно используется как промежуточный/переходный, поскольку решение нужно здесь и сейчас, а вариант с полностью российской криптографией пока недоступен для массового применения.

3) Национальный удостоверяющий центр (НУЦ) Минцифры России или другие отечественные УЦ, использующие российскую криптографию. Целевой вариант, поскольку осуществляется на базе российских криптоалгоритмов и российской инфраструктуры.

В сервисе защищенного доступа к веб-ресурсам (ГОСТ TLS) используется полностью российская инфраструктура с отечественными криптоалгоритмами.

ОПИСАНИЕ СЕРВИСА

О СЕРВИСЕ

Сервис ГОСТ TLS располагается в облачной инфраструктуре ГК «Солар» и управляется командой квалифицированных специалистов по кибербезопасности Solar MSS. Это позволяет гарантировать высокую доступность веб-ресурса и безопасную передачу трафика до него.

В рамках сервиса ГОСТ TLS для подключения к веб-ресурсу используются средства криптографической защиты информации (далее – СКЗИ), сертифицированные ФСБ России. Дополнительно возможно применение сервиса защиты веб-приложений (WAF).

ЗАДАЧИ

Архитектура и технические возможности сервиса позволяют решить основные задачи, связанные с защитой веб-ресурсов:

- защита трафика от клиента до веб-сервиса;
- обеспечение работоспособности на RSA- и ГОСТ-сертификатах.

ОПИСАНИЕ ТЕХНОЛОГИЙ

Предоставляемые в составе сервиса СКЗИ поддерживают:

- актуальные российские криптоалгоритмы ГОСТ 28147-89, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012;
- возможность одновременной работы с ГОСТ- и RSA-сертификатами;
- различные версии протокола – TLS 1.1 и TLS 1.2.

Продукты, на базе которых предоставляется сервис, сертифицированы ФСБ России на соответствие требованиям к СКЗИ класса КС1 и допустимость применения для криптографической защиты информации, не содержащей сведений, составляющих государственную тайну.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ СЕРВИСА ГОСТ TLS

Сервис защищенного доступа к веб-ресурсам ГОСТ TLS ГК «Солар» имеет ряд существенных преимуществ как перед проектными решениями интеграторов, так и сервисами других операторов связи:

- Быстрое подключение без существенных затрат.
- Класс криптографической защиты – КС1, оптимальный для веб-трафика.
- Масштабируемость.
- Возможность подключения дополнительных сервисов ИБ.
- Эксплуатация силами экспертов ГК «Солар».
- Соответствие требованиям регуляторов.

Мониторинг и эксплуатацию оборудования, а также реагирование на инциденты, связанные с СКЗИ, осуществляют специалисты Solar MSS.

АРХИТЕКТУРА СЕРВИСА

При подключении сервиса происходит изменение DNS-A-записи веб-ресурса на IP-адрес, выделяемый ГК «Солар». Облачная инфраструктура защищена от DDoS-атак мощностью до 5 Тбит/с.

На устройства конечных пользователей устанавливается браузер и совместимое с ним СКЗИ. Возможные варианты:

СКЗИ	БРАУЗЕР
КриптоПро CSP	Яндекс Браузер, Chromium-Gost
ViPNet PKI Client (TLS Unit)	Любой
Континент ZTNA	Любой

Таблица 1. Варианты совместимости браузера и СКЗИ

При подключении к TLS-шлюзу приоритетно используются ГОСТ-алгоритмы. Если на рабочей станции пользователя ГОСТ не поддерживается, то происходит подключение через RSA.

После TLS-шлюза трафик опционально проходит очистку с помощью сервиса WAF, а далее отправляется из облачной инфраструктуры непосредственно на веб-сервер клиента.

Доступны следующие варианты защиты канала между облачной инфраструктурой и веб-сервером клиента:

1) ГОСТ VPN с организацией межсетевого взаимодействия с оборудованием клиента;
2) https RSA;
3) ГОСТ VPN с предоставлением оборудования ГК «Солар» клиенту;
4) https ГОСТ.

Общая схема подключения к сервису ГОСТ TLS для первого и второго варианта защиты представлена на рисунке 1.

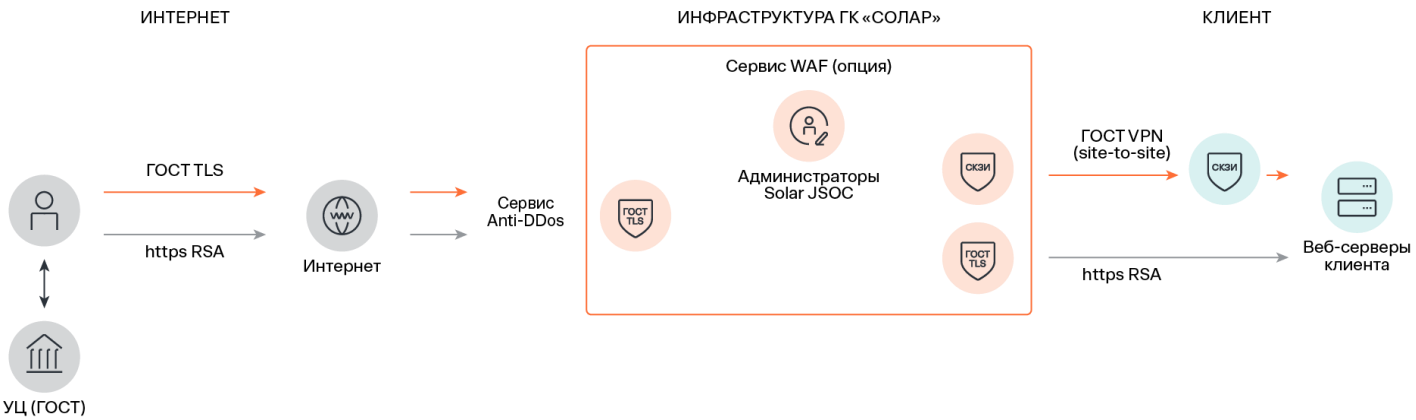

Рисунок 1. Вариант подключения сервиса к инфраструктуре клиента

ПОДКЛЮЧЕНИЕ, ЗАПУСК И ЭКСПЛУАТАЦИЯ

ПОРЯДОК ПОДКЛЮЧЕНИЯ СЕРВИСА

Для подключения к сервису ГОСТ TLS клиенту необходимо заполнить опросный лист, указав ряд параметров:

- URL и публичный IP-адрес веб-ресурса.
- Необходимость формирования сертификата ГОСТ.
- Максимальное количество запросов (RPS) RSA и ГОСТ в нормальном и пиковом режиме.
- Пропускная способность (Мбит/с) в нормальном и пиковом режиме.
- Необходимость подключения к сервису WAF.
- Вариант защиты трафика между облачной инфраструктурой и веб-ресурсом.

На основе полученной информации формируется ТКП и договор.

ЗАПУСК СЕРВИСА

Объем работ может варьироваться в зависимости от размера инфраструктуры.

Список работ в рамках запуска сервиса:

1. Формирование технического решения.
2. Подготовка облачной инфраструктуры.
3. Формирование (или предоставление клиентом) TLS-сертификатов.
4. Тестирование связи облачной инфраструктуры и веб-ресурса.
5. Подключение к системе мониторинга.
6. Настройка резервного копирования.
7. Переключение клиентом DNS-A-записи и проверка работоспособности.
8. Запуск сервиса.

ЭКСПЛУАТАЦИЯ СЕРВИСА

Эксплуатация сервиса осуществляется в режиме 24/7 и включает в себя:

1. Выполнение работ по администрированию системы, в том числе:
    - техническую консультацию по вопросам СКЗИ;
    - обеспечение работоспособности TLS-шлюза на платформе;
    - обеспечение защищенного канала от платформы до веб-ресурса;
    - изменение конфигурации TLS-шлюза при обращении клиента;
    - замену сертификатов на TLS-шлюзе;

- проведение регламентных и неотложных работ;
- мониторинг согласно модели здоровья;
- корректировку инструкций для подключения пользователей при появлении новых способов подключения.

2. Выявление и анализ инцидентов кибербезопасности, связанных с СКЗИ, и реагирование на них.
3. Назначение сервис-менеджера для административного контроля работ.
4. Изменение параметров сервиса по дополнительному соглашению с клиентом.
5. Предоставление подробных отчетов для технических специалистов по запросу.

ОГРАНИЧЕНИЯ

- На этапе подключения сервиса клиент обеспечивает выделение необходимых временных ресурсов для настройки и сопряжения оборудования со смежными системами своими техническими специалистами.
- Для реализации защищенного канала передачи данных между облачной инфраструктурой и веб-ресурсом через межсетевое взаимодействие клиент самостоятельно настраивает оборудование на своей площадке. При получении оборудования ГК «Солар» клиент обеспечивает его размещение на площадке в соответствии с техническими условиями (электропитание, охлаждение).
- Работы и услуги, не прописанные в договоре, такие как разработка и предоставление дополнительной документации, отчетов, дополнительные консультации и т. д., оцениваются отдельно и могут быть выполнены в рамках дополнительных работ.
- СКЗИ для пользователей в рамках оказания сервиса не предоставляются.
- Для пользователей, которые подключаются к веб-ресурсу, первой линией технической поддержки является сам клиент. При необходимости сотрудники клиента обращаются в техническую поддержку ГК «Солар».

ДОПОЛНИТЕЛЬНЫЕ ВАРИАНТЫ ПРЕДОСТАВЛЕНИЯ СЕРВИСА

РАЗМЕЩЕНИЕ TLS-СЕРВЕРА В ЦОД

Если веб-ресурс клиента расположен в ЦОД ПАО «Ростелеком», в том числе на базе Национальной облачной платформы (НОП), или на Yandex Cloud, то возможно размещение TLS-шлюза в облаке клиента.

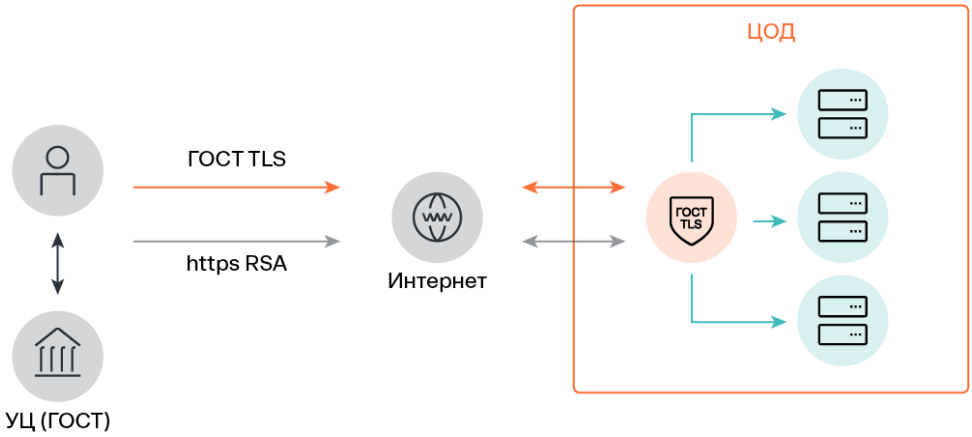

Рисунок 2. Схема расположения TLS-шлюза в ЦОД

РАЗМЕЩЕНИЕ TLS-СЕРВЕРА У КЛИЕНТА

Если веб-ресурс клиента размещен на его площадке, то возможен вариант установки выделенного оборудования на площадку клиента. Зоны ответственности и работа с балансировщиком нагрузки в таком варианте реализации обсуждается индивидуально. В данной схеме возможно применение продуктов, сертифицированных ФСБ России на соответствие требованиям к СКЗИ класса КС3.

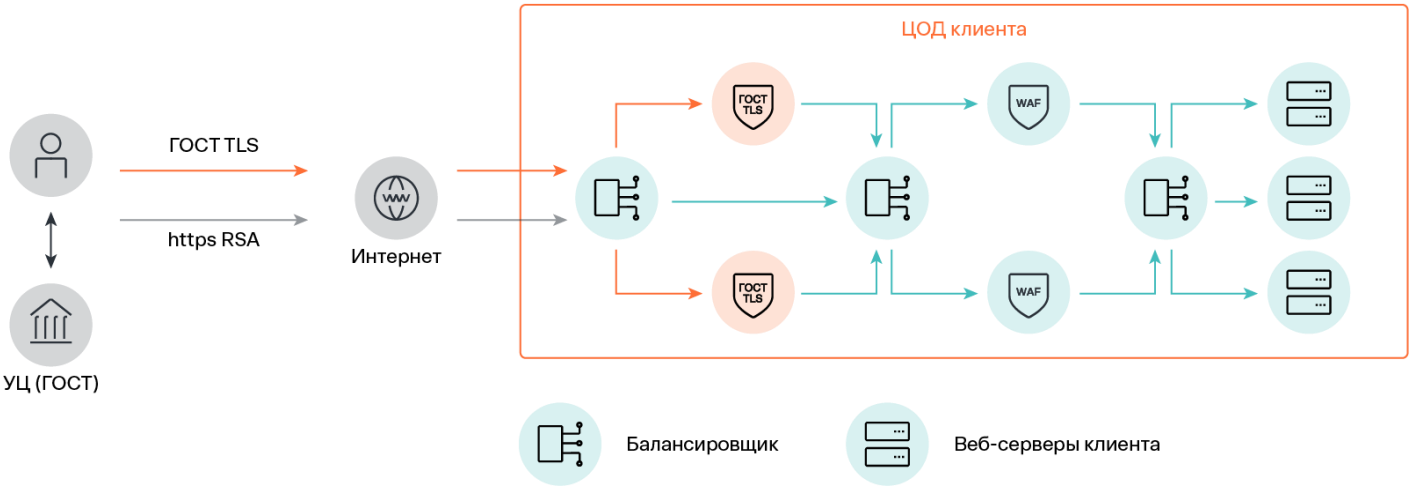

Рисунок 3. Схема расположения TLS-шлюза у клиента

РЕГЛАМЕНТ ТЕХНИЧЕСКОЙ ПОДДЕРЖКИ

Параметры предоставления сервиса:

- Режим предоставления сервиса – круглосуточно.
- Обеспечение регистрации инцидентов и запросов – круглосуточно.
- Решение инцидентов критического приоритета – круглосуточно.

Доступность сервиса для объектов с резервированием СКЗИ составляет 99,5% за квартал.

Типы приоритетов инцидентов:

1. Критический приоритет – авария. Перерыв в предоставлении сервиса, вызванный неисправностью в зоне ответственности ГК «Солар».
2. Высокий приоритет – предаварийное состояние. Периодически возникающие прерывания связи или существенные изменения показателей качества сервиса, которые могут привести к аварии.
3. Стандартный приоритет – любые возникающие проблемы, не приводящие к прерыванию оказания сервиса, но влияющие на его качество. Параметры оказания сервиса не соответствуют требуемым показателям.
4. Низкий приоритет – любые обращения клиента, связанные с оказанием сервиса, за исключением обращений по проблемам первого, второго и третьего приоритетов.

Таблица 2. Параметры оказания сервиса

№	ПРИОРИТЕТ ИНЦИДЕНТА	ВРЕМЯ РЕАКЦИИ	ВРЕМЯ РЕШЕНИЯ (БЕЗ ВЫЕЗДА)
1	Критический	до 15 минут	до 4 астроном. часов
2	Высокий	до 30 минут	до 8 астроном. часов
3	Стандартный	до 30 минут	до 48 астроном. часов
4	Низкий	до 30 минут	до 240 рабочих часов

Для проведения регламентных мероприятий, сопряженных с риском возникновения перебоев в работе сервиса, выделяется технологическое окно в удобное для клиента время.

Минимальное время уведомления клиента о регламентных мероприятиях, приводящих к перебоям в работе основного функционала сервиса, – 72 часа до начала работ.

Минимальное время уведомления клиента о неотложных ремонтных мероприятиях – 4 часа до начала работ.

О КОМПАНИИ

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

В основе подходов и технологий ГК «Солар» лежит понимание, что настоящая кибербезопасность возможна только через непрерывный мониторинг и удобное управление системами защиты.

№1
на рынке
сервисов ИБ

2000+
экспертов
по кибербезопасности

1000+
организаций под защитой

24/7
обеспечение
кибербезопасности

Топ-5
европейских MSSP*

1,5 млрд
отраженных атак в год

Продуктовый портфель ГК «Солар» делится на три основных направления: продукты на базе собственных технологий (DLP, SAST, SWG, IGA), сервисы кибербезопасности под брендами Solar MSS и Solar JSOC, а также услуги в области кибербезопасности, в том числе для защиты автоматизированных систем управления технологическими процессами (АСУ ТП) и Промышленного интернета вещей (IIoT).

*По данным рейтинга iKS-CONSULTING «MSSP в мире по итогам 2023 года».

КОНТАКТНАЯ ИНФОРМАЦИЯ

Телефоны:

+7 (499) 755-07-70 – продажи и общие вопросы

E-mail:

solar@rt-solar.ru – продажи и вопросы по сервису

info@rt-solar.ru – общие вопросы

Адреса:

- Москва, Никитский пер., 7, стр. 1
- Москва, Вятская ул., 35/4, БЦ «Вятка», 1-й подъезд
- Санкт-Петербург, ул. Савушкина, 126, БЦ «Атлантик Сити»
- Ижевск, ул. Ленина, 21, БЦ «Форум»
- Нижний Новгород, Казанское ш., 25, корп. 2
- Ростов-на-Дону, Доломановский пер., 70Д
- Самара, Молодогвардейская ул., 204
- Томск, Комсомольский просп., 70/1
- Хабаровск, ул. Серышева, 56