ООО «Цифровые документы»

Организация защищенного TLS соединения с использованием ГОСТ алгоритмов шифрования

Версия редакции: 1.0.0 Дата редакции 11.12.2023

Калуга, 2023

Условия доступа к сайту lk.152doc.ru по протоколу TLS с использованием криптоалгоритмов ГОСТ

- 1. Для организации TLS ГОСТ на APM пользователя должен быть установлен криптопровайдер с поддержкой криптоалгоритмов ГОСТ (плагин КриптоПро ЭЦП Browser plug-in).
- 2. Защищенный TLS-ГОСТ канал со стороны пользователя можно организовать с помощью установки сертифицированного средства защиты информации (СКЗИ КриптоПро CSP) и совместимый с ним интернет обозреватель (браузеры Яндекс Браузер, Chromium ГОСТ)
- 3. Для проверки используемого сайтом lk.152doc.ru сертификата должен быть установлен сертификат Удостоверяющего Центра «Астрал-Софт» (скачать сертификат) в хранилище сертификатов «Доверенные корневые центры». Сертификаты Удостоверяющего Центра «Астрал-Софт» устанавливаются вручную.

Инструкция по установке КриптоПро ЭЦП Browser plug-in в различные ОС

Инструкция по установке КриптоПро ЭЦП Browser plug-in в Windows представлена по <u>ссылке</u>.

Инструкция по установке КриптоПро ЭЦП Browser plug-in в *nix представлена по <u>ссылке</u>.

Инструкция по установке КриптоПро ЭЦП Browser plug-in в Apple macOS представлена по <u>ссылке</u>.

Подключение к сайту lk.152doc.ru по TLS ГОСТ в Windows

- 1. Установить КриптоПро ЭЦП Browser plug-in и один из совместимых браузеров.
- 2. Установить корневой сертификат Удостоверяющего Центра.
- 3. Перейти на <u>страницу</u> личного кабинета 152doc.ru.
- 4. Удостовериться, что соединение защищено по ГОСТ.

Рисунки, демонстрирующие, что соединение защищено по ГОСТ (рис. 1):

· ← ③ Ĉ ▲ https://lk.152doc.ru	· ← ③ Ċ ▲ https://lk.152doc.ru
Protect ?	← Protect
Вы на сайте https://lk.152doc.ru	соединение
Соединение безопасно. Данные зашифрованы согласно ГОСТу. Подробнее	Яндекс Браузер проверил, что ООО "АСТРАЛ-СОФТ" действительно выпустил этот сертификат. Сервер не предоставил информацию публичного аудита этого сертификата. Данные сертификата
Оставить отзыв о сайте 🔸 Нет отзывов	Соединение с lk.152doc.ru защищено с помощью современных методов шифрования.
Блокировка рекламы и трекеров	Для передачи данных используется протокол TLS 1.2.
ОБЩИЕ НАСТРОЙКИ БЕЗОПАСНОСТИ Предупреждать о вводе номера банковской карты на опасных сайтах Вкл.	Соединение зашифровано с помощью GOST_KUZNYECHIK_CTR, для аутентификации сообщений используется GOST_KUZNYECHIK_OMAC, для обмена ключами — GOSTR341112. Подробнее
Блокировать рекламу с шокирующими или	РАЗРЕШЕНИЯ
Рис	.1

Приложение 1. Пример установки КриптоПро ЭЦП Browser plug-in в Windows

Для корректного функционирования веб-страниц, использующих КриптоПро ЭЦП Browser plug-in, недостаточно расширения для браузера. Сначала необходимо скачать установочный файл и установить его, соблюдая настоящую Инструкцию.

Для работы плагина требуется установленный КриптоПро CSP версии 4.0 и выше.

Дистрибутив и инструкцию по установке можно получить по ссылке.

1. Скачайте программу установки. КриптоПро ЭЦП Browser plug-in доступен по <u>ссылке</u>.

2. Запустите исполняемый файл cadesplugin.exe.



Рис. 2

3. Подтвердите установку КриптоПро ЭЦП Browser plug-in.



Рис. 3

4. Если потребуется, разрешите КриптоПро ЭЦП Browser plug-in внести изменения путем нажатия кнопки "Да".

Вы хотите разрешить следующей программе внести изменения на этом компьютере? Имя программы: КриптоПро ЭЦП Browser plug-in Проверенный издатель: СКУРТО-РКО Источник файла: Жесткий диск компьютера	0	Ko	онтроль учетных запис	ей пользователей 🛛 🗙
Имя программы: КриптоПро ЭЦП Browser plug-in Проверенный издатель: Источник файла: СКҮРТО-РКО Источник файла: Да Нет	?	Вы хо измен	тите разрешить следу іения на этом компью	ющей программе внести тере?
🕑 Показать подробности Да Нет		×	Имя программы: Проверенный издатель: Источник файла:	КриптоПро ЭЦП Browser plug-in CRYPTO-PRO Жесткий диск компьютера
Настройка выдачи таких уведомлений	⊙ п	Іоказать г	подробности На	Да Нет Тройка выдачи таких уведомлений

Рис. 4

5. Дождитесь окончания установки КриптоПро ЭЦП Browser plug-in.

КриптоПро ЭЦП Browser plug-in	
идет настройка КриптоПро ЭЦП Browser plug-in	
Оставшееся время: 31 сек	
	Отмена

Рис. 5

6. После окончания установки КриптоПро ЭЦП Browser plug-in нажмите ОК.

КриптоПро ЭЦП Browser plug-in	×	
КриптоПро ЭЦП Browser plug-in успешно установлен. Для корректной работы КриптоПро ЭЦП Browser plug-in может потребоваться перезапустить браузер.		
ок		

Рис. 6

Приложение 2. Пример настройки для Яндекс.Браузера

Выполните загрузку и установку Яндекс Браузер. <u>Инструкция по</u> <u>установке</u> браузера и <u>ссылка на установочный файл</u>. После установки КриптоПро CSP по инструкции (<u>приложение 1</u>) браузер автоматически проверит наличие и работоспособность КриптоПро CSP.

Убедитесь, что в Яндекс Браузере включена поддержка КриптоПро CSP. Для этого зайдите в настройки Яндекс Браузера нажав <u>Настройки</u> (рис. 7)



Рис. 7

Откройте раздел Системные (рис. 8).

Избранное	Загрузки История Дополнения Настро	ойки Безопасность Яндекс ID Другие устройства
Поиск	Системные	
Общие настройки Интерфейс Инструменты Сайты Системные	Автозапуск и фоновый режим Открывать окно Браузера при старте Windows Никогда ✓ Разрешить открывать в Яндекс Браузере ссылки на сервисы Яндекса П Разрешить работу в фоне (при запуске браузер открывается быстрее, регулярно	
	обновляются компоненты без Подробнее	зопасности)

Рис. 8

Убедитесь, что в блоке Сеть включена опция «Подключаться к сайтам, использующим шифрование по ГОСТ. Требуется КриптоПро CSP» (рис. 9)

Сеть Подключаться к сайтам, использующим шифрование по ГОСТ. Требуется КриптоПро CSP. Автоматически открывать сайты по протоколу HTTPS, если они его поддерживают Предупреждать, если у сайта должна быть HTTPS-версия, но её нет Настройки прокси-сервера Управление сертификатами

Рис. 9