СберБизнес

Установка компонентов для работы с электронной подписью на VPN-KEY-TLS для версий после 550 прошивки или Рутокен TLS для версий после 531 прошивки

Для настройки рабочего места необходимо, чтобы на компьютере локального пользователя было установлено следующее программное обеспечение:

- Windows 7, Windows 8, Windows 8.1, Windows 10, Windows Server 2003 и выше, Windows Server 2008 и выше, Windows Server 2012 и выше;
- интернет-браузер Chrome, Firefox, Opera, Yandex или Internet Explorer;

Дополнительные требования к браузеру или системе зависят от электронного сервиса или портала для работы с электронной подписью.

- СКЗИ КриптоПро СЅР версии 5.0 и выше. Работа токена с электронной подписью во внешних системах на других версиях невозможна;
- КриптоПро ЭЦП Browser plug-in;
- наличие USB-порта и доступ в интернет.

Для установки вышеуказанных компонентов необходимы права администратора локального пользователя на рабочем месте.

Установите средство криптографической защиты информации КриптоПро CSP 5.0

Скачайте и запустите <u>файл</u> для установки КриптоПро CSP, имя которого начинается с CSPSetup. В открывшемся окне нажмите кнопку **Установить.** После этого начнётся установка КриптоПро CSP, и компьютер перезагрузится.



Если на компьютере уже есть КриптоПро CSP, то программа установки предложит обновить его. Для этого в открывшемся окне нажмите кнопку **Да**, чтобы установить последнюю версию. В процессе установки компьютер будет перезагружен.

📀 Обновление	×
Будет произведено обновление КриптоПро CSP Обновить?	(тек)щая до версии 5.0.12000 версия)
	Да Нет

По клику ОК подтвердите завершение установки.

КриптоПро CSP	\times
КриптоПро CSP успешно установлен. Для корректной работы КриптоПро CSP может потребоваться перезапустить браузер.	
ОК	

При первой установке КриптоПро CSP устанавливается временная лицензия КриптоПро CSP. По истечении лицензии и (или) при её отсутствии необходимо приобрести постоянную лицензию в удостоверяющем центре, в т. ч. <u>СберКОРУС</u>.

2 Установите КриптоПро ЭЦП Browser Plug-in

Скачайте <u>КриптоПро ЭЦП Browser Plug-in</u> и запустите скачанный файл cadesplugin.exe, нажав **Да**.

КриптоПро ЭЦП Browser plug-in	\times
Установить КриптоПро ЭЦП Browser plug-in?	
<u>Д</u> а <u>Н</u> ет	

Если на компьютере уже установлен КриптоПро ЭЦП Browser Plug-in, то установщик предложит переустановить программу. Нажмите кнопку **Да**.



По клику ОК начните перезапуск браузера, закрыв браузер и открыв его снова.



Установите сертификат хранилища «Личное»

Подключите носитель с электронной подписью к компьютеру. По клику **Пуск** найдите приложение «Инструменты КриптоПро» и запустите его. Если приложения нет, то установите <u>КриптоПро CSP</u>.

В приложении перейдите в раздел **Контейнеры** и найдите контейнер закрытого ключа, затем нажмите кнопку **Установить сертификат**.

Ð	сptools - Инструменты КриптоПро 🛛 🗕 🗖 🗙					
Q Поиск	Контейнеры					
Общее	Q Поиск контейнера					
	Считыватель	Контейнер	Имя субъекта	Тип ключа		
Облачный провайдер	Infocrypt HWDSSL	2badeb507-10d6	DOO TECT	Обмена		
Контейнеры						
Сертификаты						
Создание подписи						
Проверка подписи						
Зашифровать файл						
Расшифровать файл						
	Протестиро	вать контейнер	Скоп	ировать контейн	ер	
Показать расширенные	Установить сертификат					

По завершении в окне информации о сертификате проверьте, что сертификат установлен.

4 Установите корневой сертификат удостоверяющего центра в хранилище

Скачайте и откройте <u>файл</u>. В открывшемся окне нажмите **Установить сертификат**. Запустится «Мастер импорта сертификатов».

8	Сертификат	×
0	бщие Состав Путь сертификации	
	Сведения о сертификате	
	Этот сертификат предназначается для: • Все политики выдачи • Все политики применения	
	Кому выдан: Минкомсвязь России	
	Кем выдан: Минкомсвязь России	
	Действителен с 06.07.2018 по 01.07.2036	
	Установить сертификат Заявление поставщика	
	ОК	

Для продолжения установки выберите расположение хранилища **Локальный** компьютер и нажмите **Далее**.

	×
📀 🍠 Мастер импорта сертификатов	
Мастер импорта сертификатов	
Этот настер помогает копировать сертификаты, списки доверия и списки отзыва сертификатов с локального диска в хранилище сертификатов.	
Сертификат, выданный центром сертификации, является подтверждением вашей личности и содержит информацию, необходимую для защиты данных или установления защищенных сетевых подключений. Хранимице сертификатов — это область системы, предназначенная для хранения сертификатов с	
Расположение хранилища О Текущий пользователь Покальный компьютер	
Для продолжения нажните кнопку "Далее".	
Отмен	13

В открывшемся окне установите флажок **Поместить все сертификаты в следующее хранилище** и нажмите **Обзор.**



В списке хранилищ выберите **Доверенные корневые центры сертификации** и нажмите кнопку **ОК.**



Для завершения установки сертификата нажмите Готово.

Zapanulauta tractana trupanza
Завершение мастера импорта
сертификатов
Сертификат будет импортирован после нажатия
кнопки "Готово".
Были указаны следующие параметры:
Хранилище сертификатов, выбранное пользователем
Содержание
< >
۲ <u>ــــــــــــــــــــــــــــــــــــ</u>
4 <u> </u>
4 <u> </u>
< <u> </u>
< <u>m</u> >

При запросе системы подтвердите доверие издателю сертификата.



Подтвердите завершение импорта, нажав **ОК** в окне информации, которое откроется после успешного импорта сертификата в хранилище.

Мастер им	порта сертификатов	8
i	Импорт успешно выполи	нен.
		ок

Установка <u>сертификата</u> Федеральной налоговой службы производится аналогично пунктам 2-7, но сертификат устанавливается в хранилище **Промежуточные центры** сертификации.

5 Включите «CryptoPro Extension for CAdES Browser Plug-in» для браузера

При установке КриптоПро ЭЦП Browser Plug-in установите расширение для любого браузера. Для Internet Explorer данное программное обеспечение не доступно. Убедитесь, что расширение есть и включено.

Перейдите в расширения вашего браузера. Для этого в новой вкладке введите соответствующий браузеру адрес и нажмите на кнопку **Enter**:

- Chrome chrome://extensions/;
- Firefox about:addons;
- Opera opera://extensions;
- Yandex browser://tune/.

Найдите расширение **CryptoPro Extension for CAdES Browser Plug-in** и убедитесь, что оно включено. Если расширения нет, то перейдите на его страницу и установите расширение для браузера:

- <u>Chrome;</u>
- <u>Firefox;</u>
- <u>Opera;</u>
- <u>Yandex.</u>

Чтобы проверить работу электронной подписи, перейдите на <u>сайт КриптоПро</u> и нажмите кнопку **Да**.

•	Подтверждение доступа	×
<u>^</u>	Этот веб-сайт пытается выполнить операцию с ключами или сертификатами от имени пользователя.	
	'https://www.cryptopro.ru/sites/default/files/products/cades/demopag e/cades_bes_sample.html'	
	Выполнение таких операций следует разрешать только для веб-сайтов, которым вы доверяете.	
	Чтобы отключить данное подтверждение для конкретного веб-сайта, его можно добавить в список доверенных веб-сайтов, доступный на странице настроек через меню Пуск->КРИПТО-ПРО->Настройки ЭЦП Browser plug-in.	
	Разрешить эту операцию?	
	Да Нет	

Затем выберите сертификат и нажмите Подписать.

Данные для подписи:	
Hello World	
Подписать	

6 Экспорт сертификата с ключевого носителя для загрузки во внешнюю систему

Если в системе есть требования по экспорту сертификата, то необходимо запустить **КриптоПро CSP.** Для этого перейдите в меню **Пуск,** далее **Панель управления** и выберите **КриптоПро CSP.**

Затем на вкладке Сервис нажмите кнопку Просмотреть сертификаты в контейнере.

G	КриптоПро CSP ×						x
Безопасн	юсть	Winlogon	Настр	ойки TLS	Крипто	провайдер	ы
Общие	Общие Оборудование Сервис Дополнительно Алгоритмы						
Контей Эти ма удалит	Контейнер закрытого ключа Эти мастера позволяют протестировать, скопировать или удалить контейнер закрытого ключа с носителя.						
Проте	естиров	ать	Скопирова	ть	Удалі	ить	
в конт сертиф Личны Этот м контей	Этот мастер позволяет просмотреть сертификаты, находящиеся в контейнере закрытого ключа, и установить их в хранилище сертификатов. Просмотреть сертификаты в контейнере Личный сертификат Этот мастер позволяет связать сертификат из файла с контейнерен тако ключа, установия этот сертификат в						
хранил	хранилище. Установить личный сертификат						
Пароли	Пароли закрытых ключей						
Эти ма ключе	Эти мастера позволяют изменить пароли (ПИН-коды) закрытых ключей или удалить запомненные ранее пароли.						
V	Изменить пароль Удалить запомненные пароли						
Портал т	ехподд	ержки	ОК	0	тмена	Примени	пь

В открывшемся окне нажмите кнопку Обзор.

😟 Сертификаты в контей	інере закрытого і	ключа ×
Контейнер закрытого ключа Введите или укажите контейнер закры сертификатов в этом контейнере	того ключа для просмо	тра
Имя ключевого контейнера:		,
		Обзор
Введенное имя задает ключевой контейнер: Пользователя Компьютера		По сертификату
Выберите CSP для поиска ключевых контейн	еров:	
Все поддерживаемые криптопровайдеры		/
	< Назад Дале	ее > Отмена

В списке ключевых носителей выберите личный сертификат и нажмите ОК.

Выбор контейнера - КриптоПро CSP
Выбор ключевого контейнера В списке показывать:
 Дружественные имена Уникальные имена Список ключевых контейнеров пользователя:
Считыватель Имя контейнера
InfoCrypt V 2badeb 507-10d6-c281-9cd4-b6fd61b0d68
ОК Отмена ".:

В окне с информацией о выбранном сертификате нажмите кнопку Свойства.

😟 Cep	отификаты в контейнере закрытого ключа 🛛 🔍
Сертификат для Просмотрите и	а просмотра и выберите сертификат
Сертификат: Субъект: Поставщик: Действителен с: Действителен по: Серийный номер:	E= ИНН=, ИНН=, С=RU,
	Установить Свойства Обзор
	< Назад Готово Отмена

На вкладке Состав нажмите кнопку Копировать в файл.

	Ce	ртификат	
Общие Со	став Путь сертифи	икации	
Показать:	<bce></bce>	¥	
Поле		Значение	^
Версия		V3	
Серийн	ный номер		
Алгори	ттм подписи	FOCT P 34.11-2012/34.10-20	
(Хэш-ал	горитм подписи	ТОСТ Р 34, 11-2012 256 бит	
Лейсте	сль вителен с		
Дейста	зителен по		
Субъе	кт		\mathbf{v}
1		Свойства Копировать в фай.	л
		0	к

После этого запустится «Мастер экспорта сертификатов». Для продолжения установки нажмите **Далее**.



В окне экспортирования закрытого ключа выберите вариант **«Нет, не экспортировать** закрытый ключ» и нажмите Далее.



Выберите формат файла сертификата – **Файлы X.509 (.CER) в кодировке DER** – и нажмите **Далее**.

	×
Эмастер экспорта сертификатов	
Формат экспортируемого файла	
Сертификаты могут быть экспортированы в различных форматах.	
	_
Выберите формат, который вы хотите использовать:	
🖲 Файлы Х.509 (.CER) в кодировке DER	
🔵 Файлы Х.509 (.CER) в кодировке Base-64	
🔘 Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)	
Включить по возможности все сертификаты в путь сертификации	
Файл обмена личной информацией - PKCS #12 (.PFX)	
Включить по возможности все сертификаты в путь сертификации	
Удалить закрытый ключ после успешного экспорта	
Экспортировать все расширенные свойства	
 Хранилище сериализованных сертификатов (.SST) 	
Далее Отм	ена

Чтобы добавить место для хранения экспортируемого файла, нажмите **Обзор** и выберите место для хранения. Задайте имя произвольно и нажмите **Сохранить**.

		×
0		
	Имя экспортируемого файла Укажите имя файла, который вы хотите экспортировать	
		_
	Имя файла:	
	Обзор	
	Далее Отме	на

Для продолжения работы мастера нажмите Далее.

	^
С Мастер экспорта сертификатов	
Имя экспортируемого файла	
Укажите имя файла, который вы хотите экспортировать	
	—
Имя файла:	
C:\Users\Desktop\cepтификат.cer Обзор	
Далее Отме	на

Завершите работу мастера экспорта сертификатов по клику Готово.

	×
📀 🍜 Мастер экспорта сертифика	тов
Завершение работы ма	стера экспорта сертификатов
Вы успешно завершили работу с маст	гером экспорта сертификатов.
Были указаны следующие параметре	ы:
Файл	C:\Users Desktop\ceртификат.cer
Экспорт ключей	Нет
Включить в путь все сертификаты	Нет
Формат файлов	Двоичные файлы X.509 (*.cer) в кодировке
<	>
	Готово Отмена

Появится сообщение о том, что экспорт выполнен. Нажмите ОК.

