

# Работа с КриптоПро CSP в linux

Опубликовано Данзан Лиджиев on 2022-02-15 20:48

В данной статье мы описываем процесс установки и настройки КриптоПро CSP на ОС Linux (на примере Debian 11).

Она будет полезна вам, если вы получили ключ и сертификат в ФНС и используете ОС Linux для работы.

Рассматриваемая конфигурация:

- Debian 11
- КриптоПро CSP 5.0
- КриптоПро ЭЦП Browser plug-in 2.0

## Порядок настройки:

### 1) Установка КриптоПро CSP 5.0:

1.1. Выполните [регистрацию](#) на сайте нашей компании. Если Вы уже зарегистрированы – выполните вход (необходимо ввести адрес электронной почты и пароль, которые Вы указывали при регистрации)

1.2. Перейдите на страницу загрузки [дистрибутивов КриптоПро CSP](#)

1.3. Ознакомьтесь с условиями лицензионного соглашения и нажмите кнопку «Я согласен с лицензионным соглашением. Перейти к загрузке»

1.4. Нажмите кнопку «**Скачать для Linux**», для загрузки дистрибутива актуальной версии КриптоПро CSP

1.5. Распакуйте загруженный архив: **tar -xvf linux-amd64\_deb.tgz && cd linux-amd64\_deb**

1.6. Запустите установку в графическом интерфейсе посредством запуска скрипта

**sudo ./install\_gui.sh**

При установке дополнительно нужно отметить пакеты

- Smart Card and Token support modules

1.7. Для корректной работы с некоторыми ключевыми носителями необходима установка дополнительного программного обеспечения:

- **pcscd** (sudo apt-get install pcscd)
- **libccid** (sudo apt-get install libccid)
- Рутокен ЭЦП 2.0 - [библиотека для работы через PKCS#11 интерфейс](#)
- JaCarta-2 ГОСТ - [Единый клиент JaCarta](#)
- ESMART Token ГОСТ - [ESMART PKI Client](#)
- Рутокен S - пакет ifd-rutokens\_1.0.4 расположен в архиве с ПО

установка скаченных выше библиотек PKCS#11 выполняется командой

**sudo dpkg -i путь до скаченной библиотеки**

убедитесь, что служба pcscd запущена **sudo systemctl status pcscd**

если нет запустите ее **sudo systemctl enable --now pcscd**

2) Установка КриптоПро ЭЦП BrowserPlug-in 2.0:

Скачайте [КриптоПроЭЦП Browser plug-in 2.0](#)

Распакуйте загруженный архив: **tar -xvf cades-linux-amd64.tar.gz**

Выполните установку

**sudo dpkg -i cprocsp-pki-cades**

**sudo dpkg -i cprocsp-pki-plugin**

3) Установка личного сертификата:

Установка личного сертификата с привязкой к ключевому контейнеру на ключевом носителе (при подключенном ключевом носителе):

Обзор  
Показать приложения  
Инструменты КриптоПро  
Контейнеры  
Выбрать нужный ключевой носитель  
Установить сертификат

Установка облачного сертификата описана в инструкции по [ссылке](#)

4) Проверить правильность настройки можно на [тестовой странице проверки плагина](#).

Если настройка произведена корректно, то в поле **Сертификат** появится строка, соответствующая сертификату.

После выбора сертификата и нажатия кнопки **Подписать** появится надпись **Подпись сформирована успешно**.

5) Проверка статуса лицензии КриптоПро CSP 5.0:

Обзор  
Показать приложения  
Инструменты КриптоПро  
Общее

6) Активация лицензии КриптоПро CSP 5.0:

Обзор  
Показать приложения  
Инструменты КриптоПро

[Общее](#)[Ввести лицензию для меня](#)

Дополнительная информация по работе с лицензиями доступна по [ссылке](#).

**Примечания:**

**а)** При необходимости отдельной установки сертификатов

корневых удостоверяющих центров (например, в случае использования неквалифицированного сертификата) или промежуточных удостоверяющих центров (например, в случае с проблемами автоматического построения цепочки сертификатов по ссылкам из сертификатов) эти сертификаты можно установить следующим образом:

[Обзор](#)[Показать приложения](#)[Инструменты КриптоПро](#)[Сертификаты](#)[Установить сертификаты](#)[выбрать файл с нужным сертификатом](#)