

# Инструкция по настройке рабочего места для ОС Linux

В документе описан порядок установки и настройки программ, необходимых для работы с системой обмена юридически значимыми документами Synerdocs (далее система ЭДО Synerdocs) в ОС Linux.

## ОСНОВНЫЕ ПОНЯТИЯ

### **Закрытый ключ**

Ключ, известный только своему владельцу. Сохранение пользователем в тайне своего закрытого ключа гарантирует невозможность подделки злоумышленником документа и цифровой подписи от имени заверяющего.

### **Ключ электронной подписи**

Набор уникальных данных, который используется криптографическим алгоритмом при шифровании и расшифровке сообщений, постановке и проверке цифровой подписи. При асимметричном алгоритме шифрования различают закрытый и открытый ключ.

### **Корневой сертификат**

Начальный сертификат в цепочке доверия. Как правило, корневым сертификатом является сертификат удостоверяющего центра.

### **КриптоПро FOX**

Веб-браузер на основе Mozilla FireFox, поддерживающий установку защищённых соединений (Transport Layer Security, TLS) с использованием российских криптографических алгоритмов. Поддерживается работа TLS как с односторонней, так и с двухсторонней аутентификацией.

### **Открытый ключ**

Ключ, который может быть опубликован и используется для проверки подлинности подписанного документа, а также для предупреждения мошенничества со стороны заверяющего лица в виде отказа его от подписи документа. Открытый ключ подписи вычисляется как значение некоторой функции от закрытого ключа, но знание открытого ключа не дает возможности определить закрытый ключ.

### **Промежуточный сертификат**

Сертификат в цепочке доверия, подписанный на другом сертификате УЦ.

**Сертификат пользователя (сертификат ключа проверки электронной подписи, сертификат открытого ключа)**

Цифровой или бумажный документ, подтверждающий соответствие между открытым ключом и информацией, идентифицирующей владельца ключа. Содержит информацию о владельце ключа, сведения об открытом ключе, его назначении и области применения, название центра сертификации и т.д.

**Токен**

Уникальный идентификатор сессии, который выдается пользователю после успешной авторизации и обеспечивает доступ к объектам сервиса Synerdocs.

**Цепочка доверия**

Механизм проверки, при котором происходит построение пути от текущего сертификата до любого из доверенных корневых центров, причем каждый сертификат проверяется последующим.

**Электронная подпись (ЭП)**

Реквизит электронного документа, удостоверяющий автора подписи и гарантирующий неизменность документа после его подписания.

## Системные требования

К компьютеру, на котором будут работать с системой ЭДО Synerdocs, предъявляются требования:

- |                   |   |
|-------------------|---|
| <b>ОС</b>         | <ul style="list-style-type: none"> <li>• CentOS 5/6 (ia32, x64)</li> <li>• Fedora 16/17 (ia32, x64)</li> <li>• Linpus Lite 1.3 (ia32)</li> <li>• Mandriva Server 5 (ia32, x64)</li> <li>• Oracle Enterprise Linux 5/6 (ia32, x64)</li> <li>• Open SUSE 12 (ia32, x64)</li> <li>• Red Hat Enterprise Linux 5/6 (ia32, x64)</li> <li>• SUSE Linux Enterprise 11 (ia32, x64)</li> <li>• Ubuntu 8.04/10.04/11.04/11.10/12.04 (ia32, x64)</li> <li>• ALT Linux 5/6 (ia32, x64)</li> <li>• Red Hat Enterprise Linux Version 3 Update 3 (ia32, x64)</li> <li>• Debian 6 (ia32, x64)</li> </ul> |
| <b>Браузер</b>    | <ul style="list-style-type: none"> <li>• КриптоПро Fox 17 и выше</li> </ul>   |
| <b>Сертификат</b> | <ul style="list-style-type: none"> <li>• Сертификат пользователя ЭП</li> </ul>  |
| <b>СКЗИ</b>       | <ul style="list-style-type: none"> <li>• СКЗИ КриптоПро CSP 3.6 R3 и выше<br/>(<a href="http://www.cryptopro.ru/products/csp/overview">http://www.cryptopro.ru/products/csp/overview</a>)</li> <li>• КриптоПро ЭЦП Browser Plug-in версии 1.05.0946 и выше</li> </ul>   |

# Настройка рабочего места

1. [Установите КриптоПро CSP](#)
2. [Настройте КриптоПРО CSP](#)
3. [Установите сертификаты](#)
4. [Установите браузер КриптоПро Fox](#)
5. [Установите КриптоПро ЭП Browser plug-in](#)

## Установка КриптоПро CSP

Программа КриптоПро CSP предназначена для интеграции криптографических функций в клиентское приложение. Посредством криптографических функций осуществляется расшифрование токена авторизации и работа с электронной подписью.

По вопросам получения лицензии на КриптоПро CSP обратитесь в службу поддержки системы ЭДО Synerdocs: [support@synerdocs.ru](mailto:support@synerdocs.ru).

Чтобы установить КриптоПро CSP:

1. Зарегистрируйтесь на сайте <http://cryptopro.ru/products/csp/downloads>, скачайте программу установки и разархивируйте ее.
2. Установите пакеты в указанной последовательности:
  - ./lsb-cproscsp-base-3.6.4-4.noarch.rpm
  - ./lsb-cproscsp-rdr-3.6.4-4.i486.rpm
  - ./lsb-cproscsp-kc1-3.6.4-4.i486.rpm
  - ./lsb-cproscsp-capilite-3.6.4-4.i486.rpm

Версии пакетов могут отличаться.

Для установки пакетов используйте соответствующую команду из таблицы:

ОС	Действие	Команда	Пример
ОС семейства Linux, основанные на Debian (например, Debian, Ubuntu)	Установка	<ul style="list-style-type: none"><li>• <code>alien -kci &lt;файл_пакета&gt;</code></li><li>• <code>dpkg-architecture -ai386 -c alien -kci &lt;файл_пакета&gt;</code> - для установки 32-битных пакетов на 64-битную ОС</li></ul>	<code>alien -kci ./lsb-cproscsp-base-3.6.1-4.noarch.rpm</code>
	Удаление	<code>dpkg -P &lt;имя_пакета_без_версии&gt;</code>	<code>dpkg -P lsb-cproscsp-base</code>
Прочие ОС семейства Linux	Установка	<code>rpm -i &lt;файл_пакета&gt;</code>	<code>rpm -i ./lsb-cproscsp-base-3.6.1-4.noarch.rpm</code>
	Удаление	<code>rpm -e &lt;имя_пакета&gt;</code>	<code>rpm -e lsb-cproscsp-base-3.6.1-4</code>

Имя пакета может не включать версию.

Файлы КриптоПРО CSP устанавливаются в каталог `/opt/cproscsp`.

## Настройка КриптоПРО CSP

Настройка СКЗИ КриптоПРО CSP осуществляется с помощью утилиты **cpconfig**, которая входит в состав дистрибутива и расположена в каталоге /opt/cproscsp/sbin/<название\_архитектуры>.

Чтобы настроить СКЗИ КриптоПРО CSP:

1. Введите серийный номер лицензии. Для этого выполните команду:

```
cpconfig -license -set <серийный_номер>
```

Просмотреть лицензию можно с помощью команды:

```
cpconfig -license -view
```

2. По умолчанию в качестве носителей закрытых ключей используется flash-носители. Если необходимо использовать другой носитель, например дискету, выполните команду:

```
cpconfig -hardware reader -add FAT12_0 -name "Floppy Drive"
```

---

### Примечание

Более подробную информацию об использовании утилиты **cpconfig** можно получить на странице «map 8 certmgr».

---

## Установка сертификатов

Если у пользователя нет сертификата открытого ключа, выданного аккредитованным удостоверяющим центром, то необходимо оформить заявку на получение. Для этого обратитесь в службу поддержки системы ЭДО Synerdocs [support@synerdocs.ru](mailto:support@synerdocs.ru).

Для работы с сертификатами используется утилита **certmgr**, которая входит в состав дистрибутива и расположена в каталоге /opt/cproscsp/bin/<название\_архитектуры>.

Чтобы установить корневой сертификат, выполните команду:

```
certmgr -inst -store root -file <путь к файлу с сертификатом>
```

Чтобы установить промежуточный сертификат, выполните команду:

```
certmgr -inst -store CA -file <путь к промежуточному сертификату>
```

Чтобы установить личный сертификат и привязать его к закрытому ключу, выполните команду:

```
certmgr -inst -cert -file <путь к личному сертификату> -store uMy -cont <путь к контейнеру закрытого ключа>
```

---

### Примечание

При привязке сертификата к закрытому ключу убедитесь, что носитель с контейнером подключен к компьютеру.

---

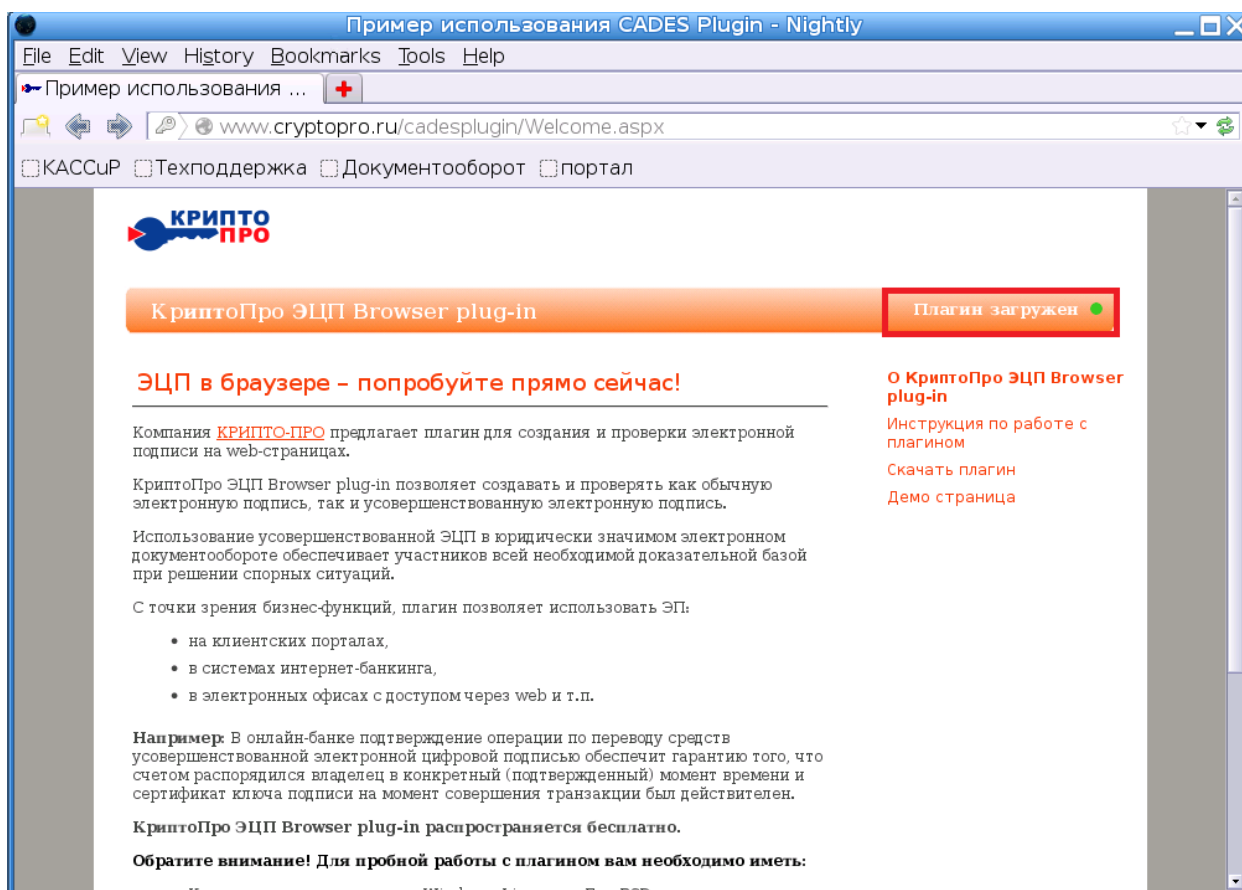
# Установка КриптоПро FOX

Программа КриптоПро Fox представляет собой веб-браузер на основе Mozilla FireFox, поддерживающий установку защищённых соединений, таких как Transport Layer Security, TLS, с использованием российских криптографических алгоритмов.

Чтобы установить КриптоПро FOX:

1. Скачайте архив с пакетом установки и пакет PKCS11 с сайта <http://www.cryptopro.ru/products/cpfox>.
2. Разархивируйте архив с помощью команды:  
tar xvjf <имя архива>
3. Установите последнюю версию пакета библиотек libgtk2.0-0 из репозитория.
4. Установите пакет PKCS11.
5. Запустите файл firefox. Чтобы проверить работоспособность плагина в браузере КриптоПро FOX, перейдите по ссылке <http://www.cryptopro.ru/cadesplugin/Welcome.aspx>.

В правой части открывшейся страницы должна появиться надпись «Плагин загружен»:



## Установка и настройка КриптоПро ЭП Browser plug-in

Программа КриптоПро ЭЦП Browser plug-in предназначена для создания и проверки электронной подписи на веб-страницах.

Чтобы установить КриптоПро ЭЦП Browser plug-in:

1. Скачайте необходимый архив с пакетами установки, в зависимости от разрядности и версии используемой ОС, с сайта <http://www.cryptopro.ru/products/cades/plugin/downloads>.

2. Разархивируйте пакеты с помощью команды:

```
tar xvzf <имя архива>
```

3. Установите пакеты с помощью соответствующей команды:

- Isb-cproscsp-tsp-util
- Isb-cproscsp-ocsp-util
- Isb-cproscsp-cades
- cproscsp-ncades

4. Скопируйте файл libnrcades.so\*:

- из /opt/cproscsp/lib/ia32/ в /usr/lib32/mozilla/plugins/ – для 32-битных платформ;
- из /opt/cproscsp/lib/amd64/ в /usr/lib64/mozilla/plugins/ – для 64-битных платформ.

Переименуйте файл в libnrcades.so.

5. Выполните от пользователя root команду:

```
/sbin/ldconfig
```