Инструкция по настройке автоматизированного рабочего места пользователя на базе операционной системы семейства Linux для работы с сертификатом ключа проверки электронной подписи, выданным удостоверяющим центром АО «Крымтехнологии»

В настоящей Инструкции представлена схема общего алгоритма настройки автоматизированных рабочих мест на операционной системе CentOS 7 для работы с сертификатом ключа проверки электронной подписи и описан процесс установки и настройки сертифицированного средства криптографической защиты информации КриптоПро CSP и плагина КриптоПро ЭЦП Browser plugin.

Для работы с сертификатом ключа проверки электронной подписи на автоматизированном рабочем месте пользователя необходимо установить:

1) средство криптографической защиты информации (далее – СКЗИ) КриптоПро CSP.
2) корневые сертификаты Головного удостоверяющего центра (Минкомсвязь России) и удостоверяющего центра АО «Крымтехнологии».
3) плагин КриптоПро-ЭЦП-Browser-plugin.

1. Установка средства криптографической защиты информации КриптоПро CSP

Для установки СКЗИ КриптоПро CSP необходимо запустить имеющийся у Вас файл дистрибутива (например, linux-amd64.tgz). При отсутствии у Вас дистрибутива средства криптографической защиты информации, Вы можете приобрести дистрибутив КриптоПро CSP необходимой версии и лицензию к нему (годовую или бессрочную) в АО «Крымтехнологии».

В качестве примера в настоящей инструкции все дистрибутивы и сертификаты размещены в папке «Загрузки».

Перейдите в терминал операционной системы.

Установка программного обеспечения и различных компонентов должна осуществляться под учетной записью администратора. Авторизуйтесь под этой учетной записью (в примере учетная запись администратора имеет имя «root»), выполнив следующую команду:

```
su
```

Введите пароль администратора, после чего команды в терминале буду выполняться от имени администратора.

Распакуйте дистрибутив СКЗИ КриптоПро CSP для Linux, перейдя в директорию, в которую сохранился дистрибутив (в нашем случае папка «Загрузки»):

```
cd Загрузки
tar -xvf linux-amd64.tgz
```

Далее, необходимо установить lsb пакет. Lsb - стандартная базовая система, от которой могут зависеть программы, написанные для Linux. Пакет содержит только библиотеку функций инициализации оболочки, которая может быть использована сценариями инициализации из других пакетов для вывода сообщений в консоль и других целей. Для установки выполните команду:

```
yum install lsb -y
```

Для того, чтобы установить КриптоПро CSP необходима установка следующих пакетов[*] (строго в указанном порядке):

lsb-cprocsp-base
lsb-cprocsp-rdr
lsb-cprocsp-kc2 (или *kc1*, в зависимости какой класс СКЗИ Вам необходимо установить)
lsb-cprocsp-capilite

Для этого необходимо перейти в директорию распакованной папки и ввести следующие команды для установки:

```
cd linux-amd64
```

[*] Версии пакетов в настоящей Инструкции являются актуальными на момент её оформления и могут отличаться от версий пакетов, имеющихся у вас.

```
rpm -i lsb-cprocsp-base-4.0.9963-5.noarch.rpm
rpm -i lsb-cprocsp-rdr-64-4.0.9963-5.x86_64.rpm
rpm -i lsb-cprocsp-kc2-64-4.0.9963-5.x86_64.rpm
rpm -i lsb-cprocsp-capilite-64-4.0.9963-5.x86_64.rpm
```

КриптоПро CSP 4.0 КС2 установлено!!!

При установке СКЗИ КриптоПро CSP активируется временная лицензия на пользование им, срок действия которой 3 месяца. Для более долгой работы СКЗИ КриптоПро CSP необходимо её установить:

```
cd /opt/cprocsp/sbin/amd64/cpconfig -license -set лицензия_КриптоПро
```

2. Настройка работы со смарт-картами (токенами)

Для работы смарт-карт (токенов) дополнительно необходимо установить библиотеку *libusb* и пакеты, входящие в состав дистрибутива КриптоПро CSP для Linux («linux-amd64.tgz»), выполнив команды:

```
rpm -Uhv cprocsp-rdr-pcsc-64-4.0.9963-5.x86_64.rpm
yum -y install libusb
```

Для работы Рутокен дополнительно необходимо установить следующие пакеты:

```
rpm -Uvh ifd-rutokens-1.0.1-1.x86_64.rpm
rpm -Uhv cprocsp-rdr-rutoken-64-4.0.9963-5.x86_64.rpm
```

Для работы eТокен, JaCarta дополнительно необходимо установить следующие пакеты:

```
yum -y install pcsc-lite
rpm -Uhv cprocsp-rdr-jacarta-64-3.6.408.695-4.x86_64.rpm
```

Добавляем в автозагрузку демон Pcscd для доступа к смарт-картам и устройствам для их считывания:

```
systemctl enable pcscd
```

Убеждаемся, что демон считывания смарт-карт добавлен в автозагрузку:

```
systemctl list-units |grep pcscd
```

Система выдала данные:

```
  pcscd.service                 loaded active running   PC/SC Smart Card Daemon
  pcscd.socket                  loaded active running   PC/SC Smart Card Daemon Activation Socket
```

Настройка работы со смарт-картами (токенами) закончена!!!

3. Установка плагина КриптоПро-ЭЦП-Browser-plugin

Для работы с ключом электронной подписи необходимо установить плагин КриптоПро-ЭЦП-Browser-plugin. Для этого необходимо скачать его с сайта КриптоПро https://www.cryptopro.ru/ (только для авторизованных пользователей), пройдя по пунктам меню:

Загрузка / КриптоПро CSP / КриптоПро ЭЦП Browser plug-in / КриптоПро ЭЦП Browser plug-in 2.0/Linux 64 бита . В настоящей инструкции настраивается 64-битная система (рис. 1)

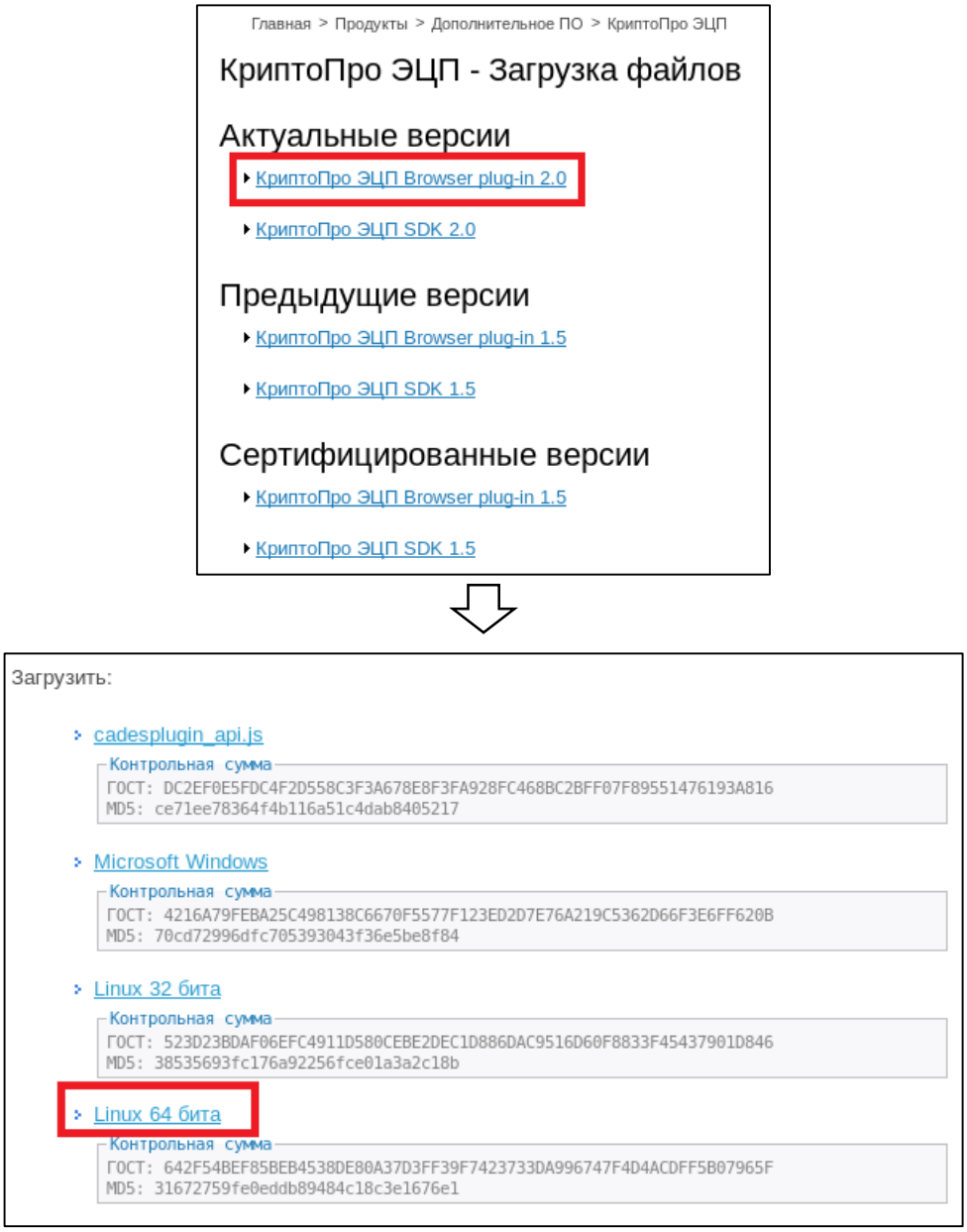

Рис. 1 – Скачивание КриптоПро-ЭЦП-Browser-plugin с сайта.

В результате скачается установочный архив «cades_linux_amd64.tar.gz».

Распакуйте архив плагина КриптоПро ЭЦП Browser plug-in, перейдя в директорию, в которой сохранен скаченный архив (в нашем случае папка «Загрузки»):

```
cd Загрузки
tar -xvf  cades_linux_amd64.tar.gz
```

И, перейдя в директорию распакованной папки, установите следующие пакеты (соблюдая порядок):

```
cd cades_linux_amd64
rpm -i cprocsp-pki-2.0.0-amd64-cades.rpm
rpm -i cprocsp-pki-2.0.0-amd64-plugin.rpm
```

Дополнительно установите пакет «cprocsp-rdr-gui-gtk» из дистрибутива КриптоПро CSP, перейдя в директорию распакованного дистрибутива КриптоПро CSP («linux-amd64»):

```
cd -
cd linux-amd64
```

rpm -i cprocsp-rdr-gui-gtk-64-4.0.9963-5.x86_64.rpm

Обращаем Ваше внимание на то, что пакет «cprocsp-rdr-gui» не должен быть установлен. Если Вы сомневаетесь устанавливали ли Вы его ранее удалите его, выполнив следующую команду:

rpm -e cprocsp-rdr-gui

Установка плагина КриптоПро ЭЦП Browser plug-in завершена!!!

4. Установка корневых сертификатов

Необходимо установить корневые сертификаты головного удостоверяющего центра и удостоверяющего центра АО «Крымтехнологии».

Установка любых сертификатов, в том числе корневых сертификатов, должна выполняться под учетной записью владельца сертификата ключа проверки электронной подписи, чтобы сертификаты поместились в хранилища сертификатов пользователя.

Для установки корневых сертификатов используется команда:

/opt/cprocsp/bin/amd64/certmgr -inst -store user -file имя.cer

Необходимо скачать корневые сертификаты Минкомсвязи России и Удостоверяющего центра АО «Крымтехнологии», перейдя по следующим ссылкам:

https://krtech.ru/wp-content/uploads/uc_soft/uc_guc.cer

https://krtech.ru/wp-content/uploads/uc_soft/uc_ao_krtech.cer

Выполните вход в Терминале под учетной записью пользователя (в нашем случае «user»):

su user -

Установите скачанные корневые сертификаты в хранилища корневых сертификатов:

/opt/cprocsp/bin/amd64/certmgr -inst -store user -file /home/user/Загрузки/UC_GUC.cer

/opt/cprocsp/bin/amd64/certmgr -inst -store user -file /home/user/Загрузки/UC_AO_KRTECH.cer

5. Работа с сертификатом ключа проверки электронной подписи

Ранее для работы со смарт-картами (токенами) уже установили нужные драйвера. Теперь необходимо распознать ту или иную смарт-карту (токен), распознать контейнер на ней и установить корневой сертификат удостоверяющего центра, выдавшего сертификат ключа проверки электронной подписи пользователю для подписания электронных документов.

В настоящей инструкции контейнер с ключом электронной подписи размещен на токене типа eToken Java 72k (при работе с другими ключевыми носителями (ruToken, JaCarta, flash-карта) действия аналогичны).

Нижеуказанные команды необходимо выполнять под учетной записью пользователя:

su user

Для начала удостоверьтесь, что система видит токен, выполнив команду:

/opt/cprocsp/bin/amd64/list_pcsc

В нашем случае токен распознался, как:

SafeNet eToken 5100 [Main Interface] 00 00

На вставленном в usb-порт компьютера токене размещен контейнер «le-33bccdb9-c122-4a95-b194-741483d6cf88» с ключом электронной подписи.

Убедимся, что система видит контейнер, для этого выполним команду:

/opt/cprocsp/bin/amd64/csptest -keyset -enum_cont -fqcn -verifyc

Ответ системы:

CSP (Type:80) v4.0.9019 KC2 Release Ver:4.0.9963 OS:Linux CPU:AMD64 FastCode:READY:SSSE3.

AcquireContext: OK. HCRYPTPROV: 25417651

\\.\SafeNet eToken 5100 [Main Interface] 00 00\le-33bccdb9-c122-4a95-b194-123123123123

OK.

```
Total: SYS: 0,010 sec USR: 0,010 sec UTC: 2,160 sec
[ErrorCode: 0x00000000]
```

Контейнер с ключом электронной подписи виден. Теперь установим этот ключевой контейнер, выполнив команду:

```
/opt/cprocsp/bin/amd64/certmgr -inst -cont '\\.\SafeNet eToken 5100 [Main Interface] 00 00\le-33bccdb9-c122-4a95-b194-123123123123'
```

Ответом система выдаст информацию о сертификате ключа проверки электронной подписи, соответствующем ключу электронной подписи, размещенному в контейнере на токене.

На этом настройка автоматизированного рабочего места завершена.