Инструкция по настройке рабочего места на базе операционной системы семейства Linux для работы в СЭД «Диалог» через ViPNet TLS Gateway

СЭД «Диалог» является Web-приложением, для доступа к которому на рабочем месте пользователя необходимо наличие браузера и криптопровайдера с поддержкой российских алгоритмов ГОСТ, а также наличие специального плагина для осуществления процесса подписания документа электронной подписью.

Далее в инструкции будет описан процесс установки и настройки КриптоПро CSP, Chromium ГОСТ и КриптоПро ЭЦП Browser plugin на примере CentOS 7.

Использование всех команд в инструкции подразумевает наличие прав ***суперпользователя***.

Ниже представлена схема общего алгоритма настройки АРМ на ОС CentOS 7 для работы в СЭД «Диалог» через ViPNet TLS Gateway.

1. Установка пакета lsb

Для работы со СКЗИ КриптоПро CSP необходим пакет *lsb*, который устанавливается командой:

```
# yum install lsb
```

*Вместе с пакетом *lsb* надо установить все зависимые пакеты, что нужно будет подтвердить.

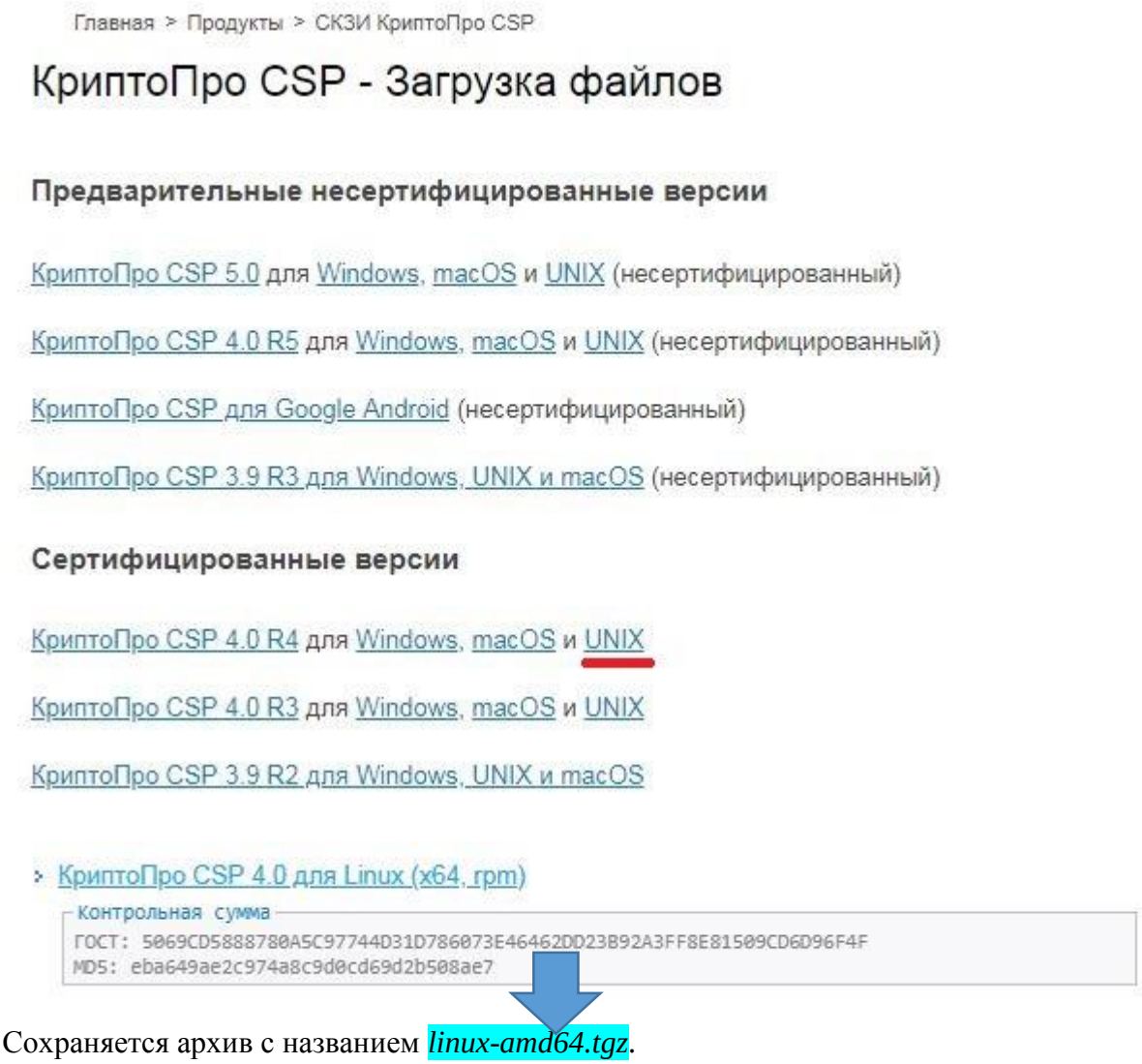
```
Установить  1 пакет (+75 зависимых)

Объем загрузки: 26 M
Объем изменений: 77 M
Is this ok [y/d/N]: y
```

2. Загрузка установочных файлов

Актуальные версии дистрибутивов скачиваем с сайта КриптоПро. Скачать нужно два архива: *linux-amd64.tgz, cades_linux_amd64.tar.gz.*

2.1 Скачивание файлов КриптоПро CSP

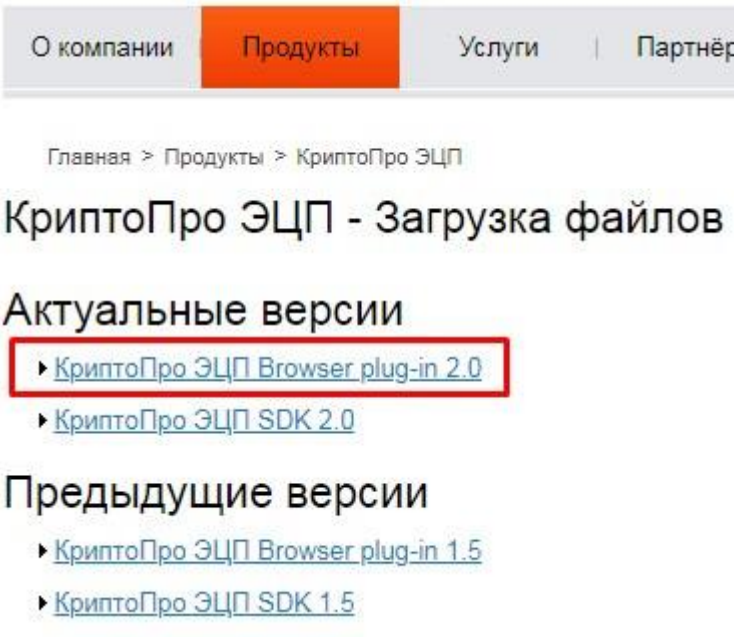
Для начала надо зарегистрироваться на сайте https://www.cryptopro.ru/ и со страницы загрузки https://www.cryptopro.ru/downloads скачать сертифицированную версию КриптоПро CSP 4.0 R4 для UNIX в формате rpm.



Сохраняется архив с названием *linux-amd64.tgz*.

2.2 Скачивание файлов КриптоПро Browser Plug-in

Скачать КриптоПРО Browser Plug-in можно на странице https://www.cryptopro.ru/downloads



Архив с файлами плагина называется *cades_linux_amd64.tar.gz*.

* Плагин необходим для подписания документов квалифицированной электронной подписью в СЭД «Диалог». В данный момент, при установке, КриптоПро ЭЦП Browser-Plugin требует установленного несертифицированного КриптоПро CSP 5.0

3. Установка пакетов КриптоПро CSP

Ранее скачанный архив с файлами КриптоПро CSP с именем *linux-amd64.tgz* следует распаковать командой:

```
# tar –xvf linux-amd64.tgz
```

*Команду следует выполнять из директории, в которой находится архив.

При наличии графической оболочки распаковку можно провести средствами GUI.

Перед установкой СКЗИ КриптоПро CSP перейдите в директорию с распакованными из архива файлами командой:

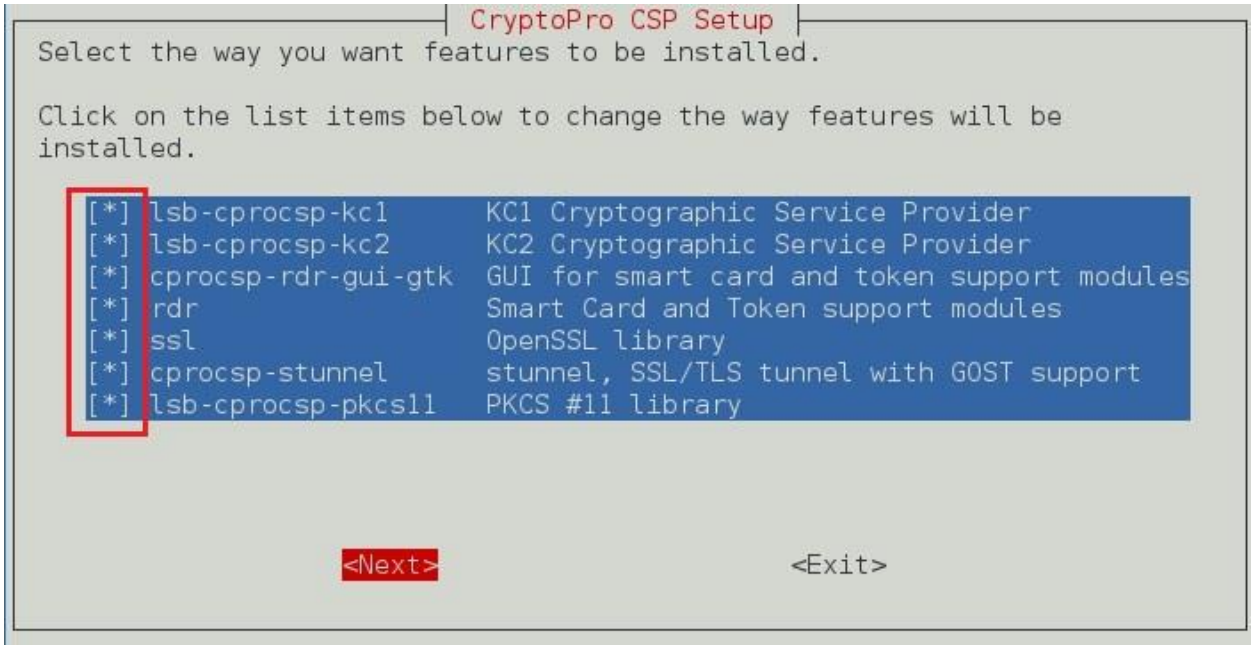
```
# cd /home/<имя пользователя>/Загрузки/linux-amd64
```

*Вместо *<имя пользователя>* указать надо имя Вашей учётной записи в операционной системе.

Для установки КриптоПро CSP требуется запустить скрипт **install_gui.sh**. Этот скрипт запустит графическую оболочку установки. Скрипт запускается командой:

```
# ./install_gui.sh
```

Выбираем (пробелом) все представленные пункты для установки полного комплекта КриптоПРО CSP:



По завершению установки нужно ввести серийный номер лицензии. В противном случае будет установлена пробная версия КриптоПро CSP на 3 месяца.

Минимальный набор пакетов для работы с электронной подписью в СЭД «Диалог» включает следующие пакеты из набора, используя скрипт **install.sh** установите:

lsb-cprocsp-pkcs11

lsb-cprocsp-kc2

cprocsp-rdr-pcsc

cprocsp-rdr-gui

В этом случае может понадобиться установить так же отдельно пакеты драйверов для носителей/считывателей из набора CSP.

Далее следует добавить в автозагрузку демон считывателя смарт-карт:

```
# systemctl enable pcscd
```

*После выполнения данной команды перезагрузите операционную систему.

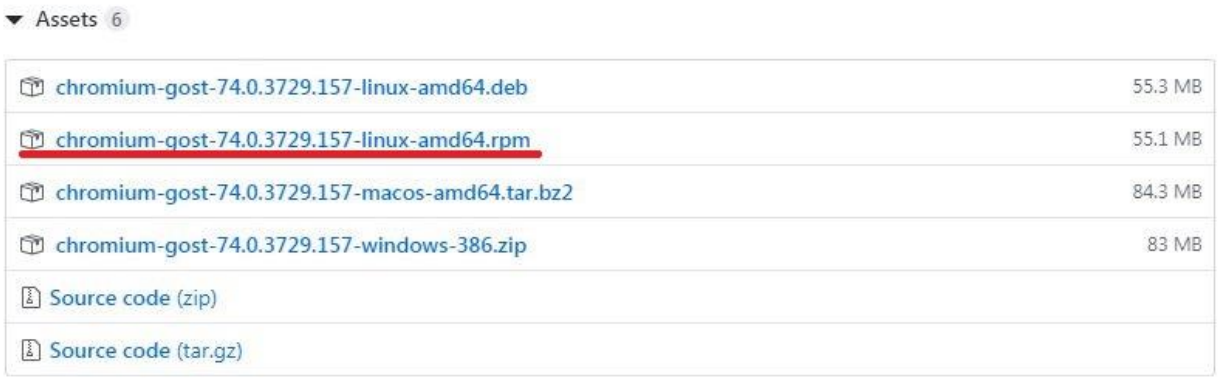
Если команда выдает ошибку *«Failed to execute operation: No such file or directory»*, тогда следует установить пакеты: *libusb, ccid, pcsc-lite*. Также убедитесь установили ли вы все пакеты на предыдущем этапе.

4. Установка Chromium ГОСТ

Дистрибутив браузера скачивается по ссылке:

https://github.com/deemru/chromium-gost/releases/tag/74.0.3729.157

Для CentOS 7 скачивается дистрибутив «chromium-gost-74.0.3729.157-linux-amd64.rpm»



Скачается файл с именем *chromium-gost-74.0.3729.157-linux-amd64.rpm*. Для установки браузера используйте команду:

```
# rpm –ivh chromium-gost-74.0.3729.157-linux-amd64.rpm
```

*Команду следует выполнять из директории, в которой находится файл.

Запуск браузера возможен только из учетной записи **пользователя**.

5. Установка сертификатов удостоверяющего центра

Далее требуется установить корневые сертификаты удостоверяющего центра и списки отозванных сертификатов. Скачать их можно по ссылкам:

1. Корневой сертификат головного удостоверяющего центра (http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=4BC6DC14D97010C41A26E058AD851F81C842415A);

2. Корневой сертификат «ИнфоТеКС Интернет Траст» (http://uc1.iitrust.ru/uc/CA-IIT-(K3)-2018.cer)

3. Список отозванных сертификатов Головного удостоверяющего центра (http://reestr-pki.ru/cdp/guc_gost12.crl);

4. Список отозванных сертификатов «ИнфоТеКС Интернет Траст» (http://uc1.iitrust.ru/uc/CA-IIT-(K3)-2018.crl).

Основной утилитой для работы с сертификатами является **certmgr** (лежит в папке /opt/cprocsp/bin/amd64/).

Установка корневого сертификата:

```
certmgr -inst -store uroot -file <путь к файлу с сертификатом>.cer
```

Установка промежуточного сертификата:

```
certmgr -inst -store uca -file <путь к файлу с сертификатом>.cer
```

Пример использования команды установки корневого сертификата:

```
$ /opt/cprocsp/bin/amd64/certmgr -inst -store uroot -f /home/user/Загрузки/rootca.cer
```

```
[root@localhost user]# /opt/cprocsp/bin/amd64/certmgr -inst -store uroot -f /home/user/Загрузки/rootca.cer

Certmgr 1.1 (c) "CryptoPro",  2007-2010.
program for managing certificates, CRLs and stores

Installing:
================================================================================
1-------
Issuer             : E=" info@cryptopro.ru", OGRN=1037700085444, INN=007717107991, C=RU, S=77 Москва, L=M
осква, STREET=ул. Сущёвский вал д. 18, O="ООО ""КРИПТО-ПРО""", CN="Тестовый головной УЦ ООО ""КРИПТО-ПРО""
 ГОСТ 2012 (УЦ 2.0)"
Subject            : E=" info@cryptopro.ru", OGRN=1037700085444, INN=007717107991, C=RU, S=77 Москва, L=M
осква, STREET=ул. Сущёвский вал д. 18, O="ООО ""КРИПТО-ПРО""", CN="Тестовый головной УЦ ООО ""КРИПТО-ПРО""
 ГОСТ 2012 (УЦ 2.0)"
Serial             : 0x01BAD8001EA8179F4EF889B80ECB8DF4
SHA1 Hash          : f5361bb7026f815b3dcf02ce70b240f306d6af5e
SubjKeyID          : d00fb90e68827687ffd4e50c15aaa2dedb6a79f7
Signature Algorithm : ГОСТ Р 34.11-2012/34.10-2012 256 bit
PublicKey Algorithm : ГОСТ Р 34.10-2012 (512 bits)
Not valid before   : 01/11/2017  12:59:06 UTC
Not valid after    : 01/11/2032  12:59:06 UTC
PrivateKey Link    : No
================================================================================

[ErrorCode: 0x00000000]
[root@localhost user]#
```

6. Установка списка отозванных сертификатов

Далее требуется установить список отозванных сертификатов(СОС).

Установка СОС осуществляется командой:

```
certmgr -inst -crl -file <путь к файлу с сертификатом>.crl
```

Пример установки списка отозванных сертификатов:

```
$ /opt/cprocsp/bin/amd64/certmgr -inst -crl -f /home/user/Загрузки/sos.cer
```

```
[root@localhost user]# /opt/cprocsp/bin/amd64/certmgr -inst -crl -f /home/user/Загрузки/sos.crl
Certmgr 1.1 (c) "CryptoPro",  2007-2010.
program for managing certificates, CRLs and stores

Installing:
================================================================================
1-------
Issuer    : E=" info@cryptopro.ru", OGRN=1037700085444, INN=007717107991, C=RU, S=77 Москва, L=Москва, STR
EET=ул. Сущёвский вал д. 18, O="ООО ""КРИПТО-ПРО""", CN="Тестовый головной УЦ ООО ""КРИПТО-ПРО"" ГОСТ 2012
 (УЦ 2.0)"
ThisUpdate: 25/07/2018  14:50:01 UTC
NextUpdate: 01/08/2018  23:10:00 UTC
AuthKeyID : d00fb90e68827687ffd4e50c15aaa2dedb6a79f7
================================================================================

[ErrorCode: 0x00000000]
[root@localhost user]#
```

7. Настройка файла hosts

Для получения доступа к https://tls.krtech.ru необходимо внести изменения в файл hosts. Для этого необходимо выполнить команду:

```
# vim /etc/hosts
```

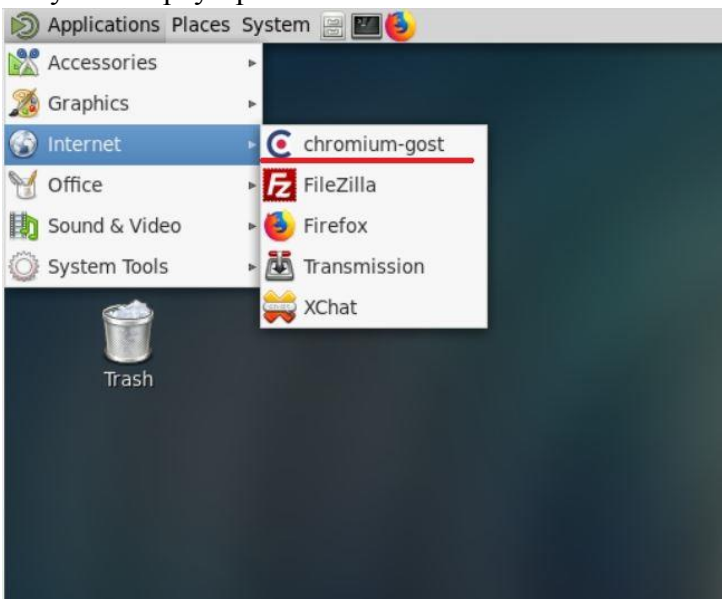
Затем нажмите на клавишу «i», чтобы войти в режим редактирования. И введите

212.110.158.225 tls.krtech.ru

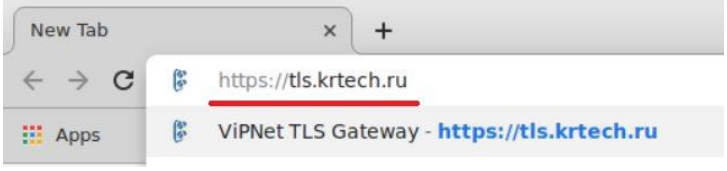
Нажмите клавишу Enter, а потом Esc. После этого введите «:wq».

8. Проверка защищенного соединения

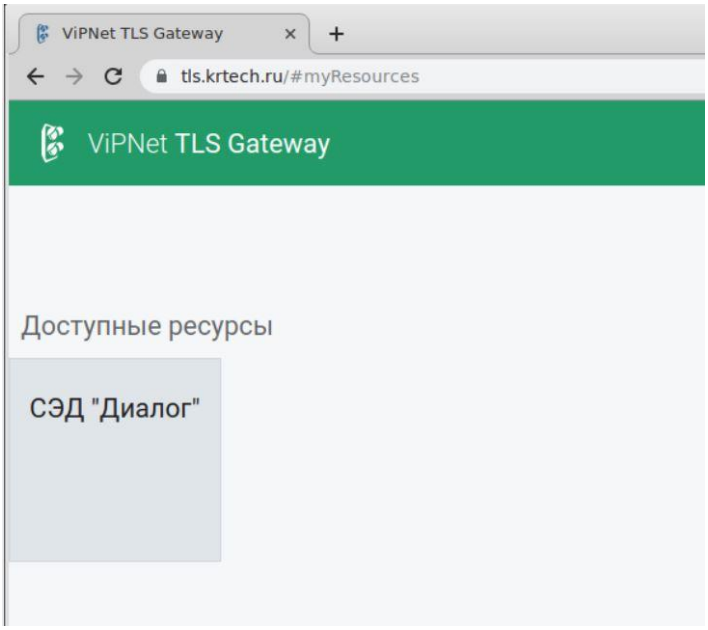
Запустите браузер Chromium ГОСТ



Введите в адресной строке: https://tls.krtech.ru



Дождитесь загрузки интерфейса ViPNet TLS Gateway и нажмите на кнопку СЭД «Диалог»



9. Установка пакетов КриптоПро Browser Plug-in

Распаковываем ранее скачанный архив *cades_linux_amd64.tar.gz* с файлами плагина:

```
# tar –xvf cades_linux_amd64.tar.gz
```

*Команду следует выполнять из директории, в которой находится архив.

После распаковки архива в директории появятся файлы (версии файлов могут отличаться, на момент составления инструкции актуальные версии файлов представлены ниже):

cprocsp-pki-2.0.0-amd64-cades.rpm

cprocsp-pki-2.0.0-amd64-plugin.rpm

* *lsb-cprocsp-devel-5.0.11438-4.noarch.rpm*

(именно этот файл требует установки КриптоПро CSP5.0)

cprocsp-pki-2.0.0-amd64-phpcades.rpm

Перед установкой данных пакетов следует закрыть все открытые браузеры.

Установка данных пакетов выполняется командами в следующем порядке:

```
# rpm -i lsb-cprocsp-devel-5.0.11438-4.noarch.rpm
# rpm -i cprocsp-pki-2.0.0-amd64-cades.rpm
# rpm -i cprocsp-pki-2.0.0-amd64-phpcades.rpm
# rpm -i cprocsp-pki-2.0.0-amd64-plugin.rpm
```