Инструкция по настройке автоматизированного рабочего места пользователя на базе операционной системы семейства Linux для подключения посредством ViPNet TLS Gateway к СЭД «Диалог» и подписания электронных документов в нем ключом электронной подписи

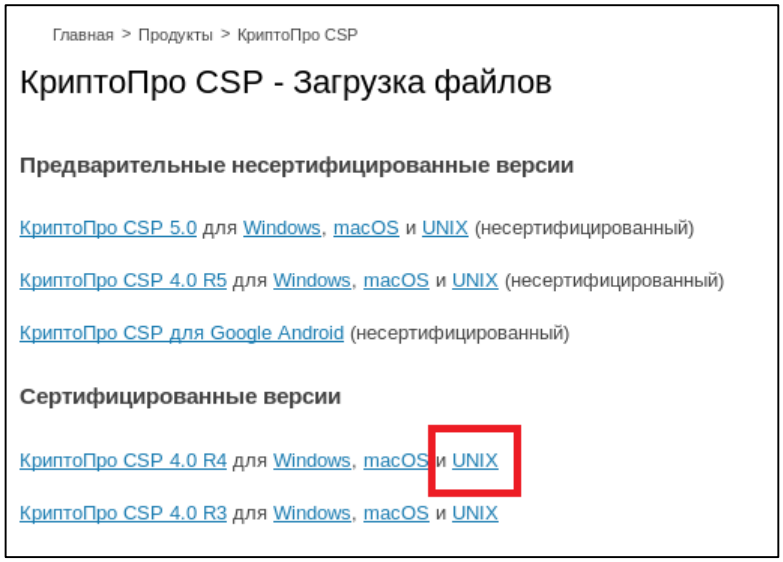
СЭД «Диалог» является Web-приложением, для доступа к которому на автоматизированном рабочем месте пользователя должны быть установлены браузер и средство криптографической защиты информации (криптопровайдер) с поддержкой российских ГОСТ-алгоритмов, а также специальный плагин для осуществления функции подписания электронных документов ключом электронной подписи.

В настоящей Инструкции представлена схема общего алгоритма настройки автоматизированных рабочих мест на операционной системе CentOS 7 для подключения посредством ViPNet TLS Gateway к СЭД «Диалог» и описан процесс установки и настройки сертифицированного средства криптографической защиты информации КриптоПро CSP 4.0, плагина КриптоПро ЭЦП Browser plugin и браузера Chromium ГОСТ.

1. **Установка средства криптографической защиты информации КриптоПро CSP**

При отсутствии в Вашей организации дистрибутива КриптоПро CSP 4.0 для Linux скачайте его с официального сайта КриптоПро https://www.cryptopro.ru/ (только для авторизованных пользователей), пройдя по пунктам меню:

Загрузка / КриптоПро CSP / КриптоПро CSP 4.0 для UNIX / КриптоПро CSP 4.0 для Linux (x64, rpm) (в качестве примера в настоящей инструкции устанавливается КриптоПро CSP 4.0 R4).



В результате скачается установочный архив «linux-amd64.tgz».

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 4.0 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
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 KC2 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 приобрести лицензию на СКЗИ и её установить.

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
```

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

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:

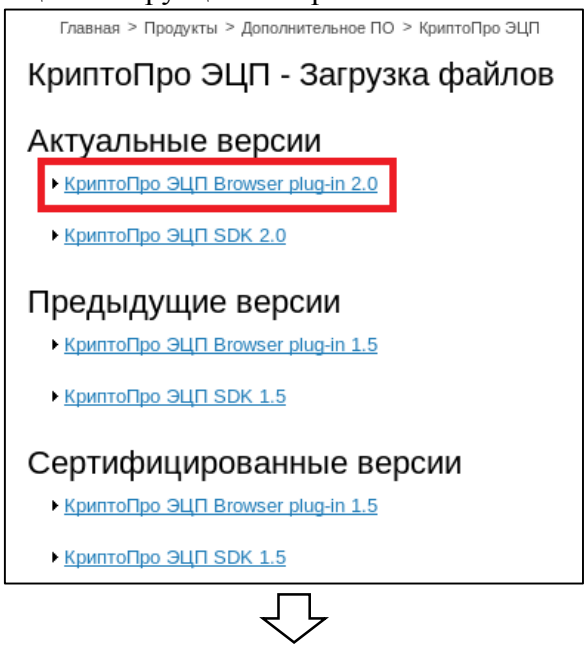
pcscd.service loaded active running PC/SC Smart Card Daemon
pcscd.socket loaded active running PC/SC Smart Card Daemon Activation Socket

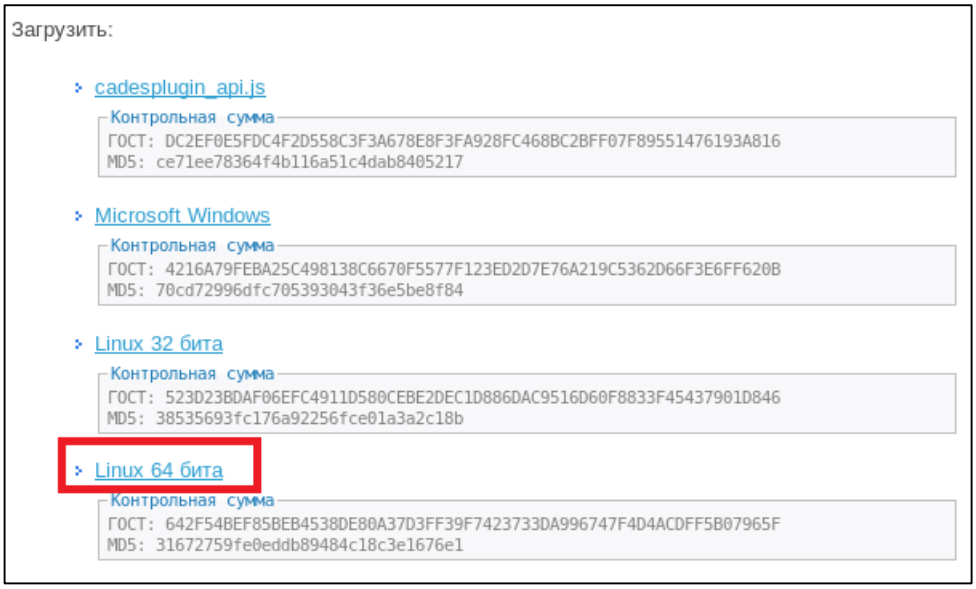
Настройка работы со смарт-картами (токенами) закончена!!!

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)





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 и списков отозванных сертификатов для работы TLS

Необходимо установить корневые сертификаты и списки отозванных сертификатов удостоверяющего центра, выпустившего сертификат ключа проверки электронной подписи, обеспечивающий работу защищенного TLS соединения.

Установка любых сертификатов, в том числе корневых сертификатов, и списков отозванных сертификатов должна выполняться под учетной записью пользователя СЭД «Диалог», чтобы сертификаты поместились в хранилища сертификатов пользователя.

Для установки корневых сертификатов используется команда:

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

Для установки списка отозванных сертификатов используется команда:

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

1) Необходимо скачать корневые сертификаты Минкомсвязи России и Удостоверяющего центра ООО «ИИТ», перейдя по следующим ссылкам:

http://e-trust.gosuslugi.ru/Shared/DownloadCert?thumbprint=4BC6DC14D97010C41A26E058AD851F81C842415A

http://uc1.iitrust.ru/uc/CA-IIT-(K3)-2018.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/4BC6DC14D97010C41A26E058AD851F81C842415A.cer
/opt/cprocsp/bin/amd64/certmgr -inst -store user -file /home/user/Загрузки/'CA-IIT-(K3)-2018.cer'
```

2) Необходимо скачать списки отозванных сертификатов, перейдя по следующим ссылкам:

http://reestr-pki.ru/cdp/guc_gost12.crl
http://uc1.iitrust.ru/uc/CA-IIT-(K3)-2018.crl

Далее, под учетной записью пользователя установите их:

```
/opt/cprocsp/bin/amd64/certmgr -inst -crl -store user -file /home/user/Загрузки/guc_gost12.crl
/opt/cprocsp/bin/amd64/certmgr -inst -crl -store user -file /home/user/Загрузки/'CA-IIT-(K3)-2018.crl'
```

5. Работа с сертификатом ключа проверки электронной подписи пользователя СЭД «Диалог»

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 и списки отозванных сертификатов удостоверяющего центра, выдавшего сертификат ключа проверки электронной подписи пользователю СЭД «Диалог» 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-b194-741483d6cf88
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-b194-741483d6cf88'
```

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

Дополнительно необходимо установить корневой сертификат и списки отозванных сертификатов удостоверяющего центра, выдавшего личный сертификат пользователя СЭД «Диалог». Для этого выполним уже известные команды (см. п. 5 Инструкции). Для начала их необходимо скачать с сайта удостоверяющего центра.

В нашем случае сертификат ключа проверки электронной подписи был сгенерирован Тестовым удостоверяющим центром ООО КриптоПро. Устанавливаем ранее скаченные корневые сертификаты Тестового удостоверяющего центра ООО КриптоПро, выполнив команды:

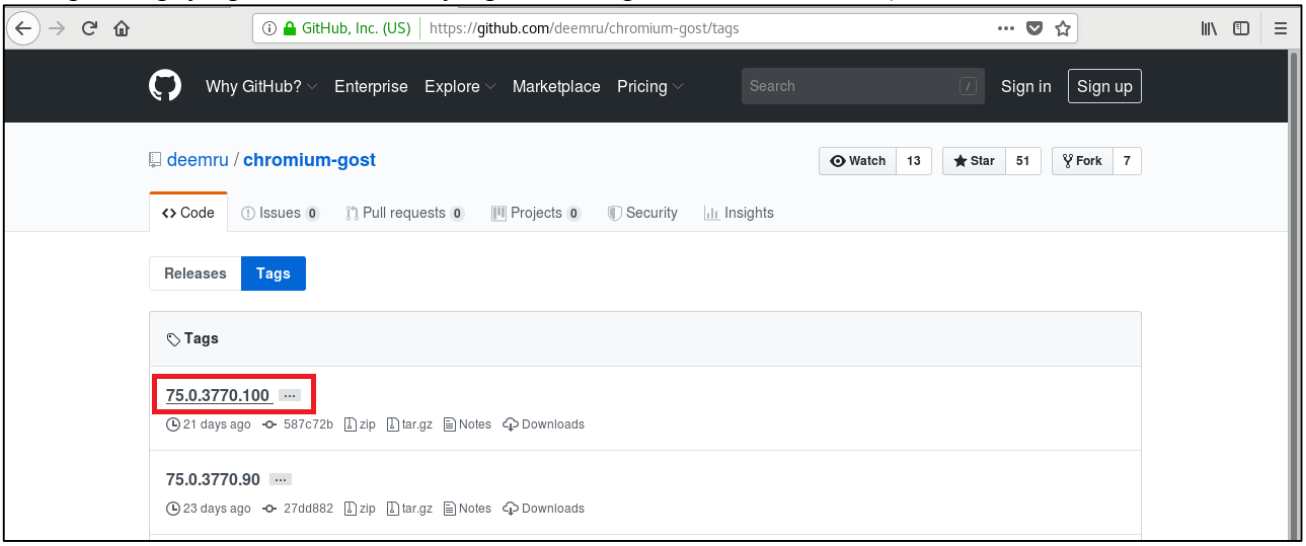
```
su user
/opt/cprocsp/bin/amd64/certmgr -inst -store user -file /home/user/Загрузки/UC1.cer
/opt/cprocsp/bin/amd64/certmgr -inst -store user -file /home/user/Загрузки/UC2.cer
```

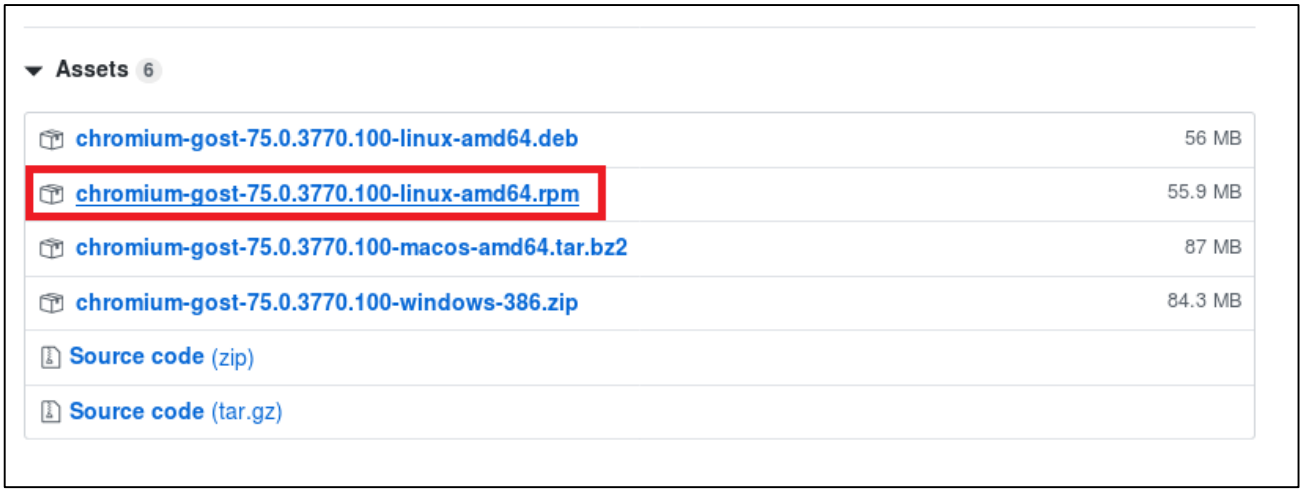
Система выведет в терминале информацию об установленных корневых сертификатах.

Также командой /opt/cprocsp/bin/amd64/certmgr -inst -crl -store user -file имя.crl необходимо установить списки отозванных сертификатов. У тестового удостоверяющего центра ООО КриптоПро их нет, поэтому в настоящей инструкции их установка не указана.

6. Установка браузера Chromium GOST

Для начала необходимо скачать браузер Chromium GOST. Перейдя по ссылке https://github.com/deemru/chromium-gost/tags, необходимо выбрать версию Chromium GOST и скачать её. Для составления инструкции скачивалась версия 75.0.3770.100 (можно придерживаться этой версии браузера, чтобы быть уверенным в работоспособности).





В результате скачается установочный файл «chromium-gost-75.0.3770.100-linux-amd64.rpm».

Браузер Chromium GOST необходимо устанавливать под учетной записью администратора, выполнив следующую команду:

```
rpm -i chromium-gost-75.0.3770.100-linux-amd64.rpm
```

Однако, при попытке установить браузер система может выдать ошибку «Неудовлетворенные зависимости», потребовать установки дополнительных пакетов, например, «libappindicator3.so.1», «liberation-fonts» или др..

Для libappindicator3.so.1 устанавливаем следующий пакет, выполнив команду:

```
yum install libappindicator-gtk3
```

Для liberation-fonts устанавливаем следующий пакет, выполнив команду:

```
yum -y install liberation-fonts
```

Установка плагина браузера Chromium GOST завершена!!!

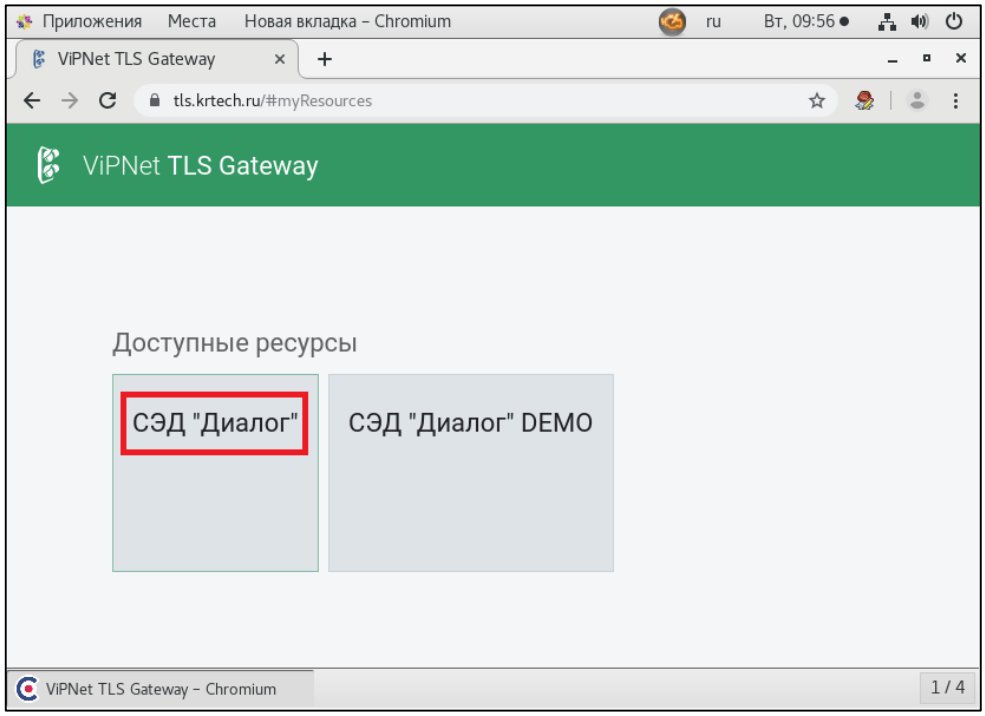
7. Внесение изменений в файл hosts

Для осуществления доступа к СЭД «Диалог» необходимо внести изменения в файл hosts, для этого вводим команду:

```
vim /etc/hosts
```

Нажмите клавишу "i" на клавиатуре, чтобы войти в режим редактирования, и введите:
212.110.158.225 tls.krtech.ru
Нажмите клавишу Esc, после введите ":wq", нажмите клавишу Enter.

После этого Вы можете зайти через браузер Chromium GOST на ресурс ТЛС по ссылке https://tls.krtech.ru и выбрать пункт «СЭД «Диалог».



На этом настройка автоматизированного рабочего места завершена.

Пользователь может осуществлять вход в СЭД «Диалог» через браузер Chromium GOST по TLS-каналу.

После сохранения карточки документа для подписания электронного документа ключом электронной подписи необходимо нажать на кнопку «Подписать», выбрать пункт выпадающего меню «Квалифицированная электронная подпись», разрешить КриптоПро CSP выполнить операцию с ключами и сертификатами от имени пользователя и выбрать в выпадающем пункте меню ключ электронной подписи, которым пользователь хочет подписать электронный документ (в СЭД «Диалог» в качестве идентификатора ключа указывается отпечаток сертификата ключа проверки электронной подписи).