



Руководство пользователя AlterOS Desktop Edition

2018 г.

Содержание

Часть I Работа с КриптоПро

3

1 Работа с КриптоПро

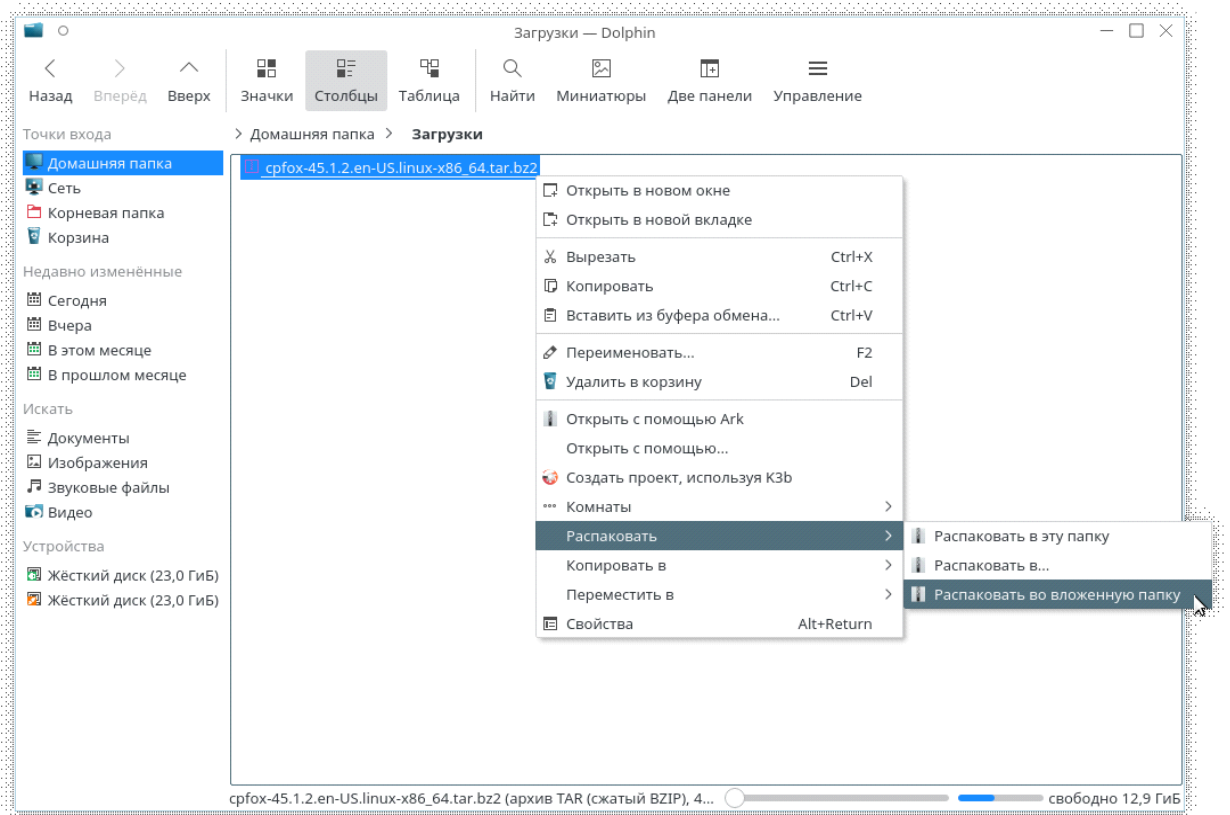
Установка CryptoFox

Данное руководство поможет Вам установить браузер КриптоПро Fox для Firefox.

CryptoFox скачиваем с официального сайта по ссылке:

<https://www.cryptopro.ru/products/cpfox>

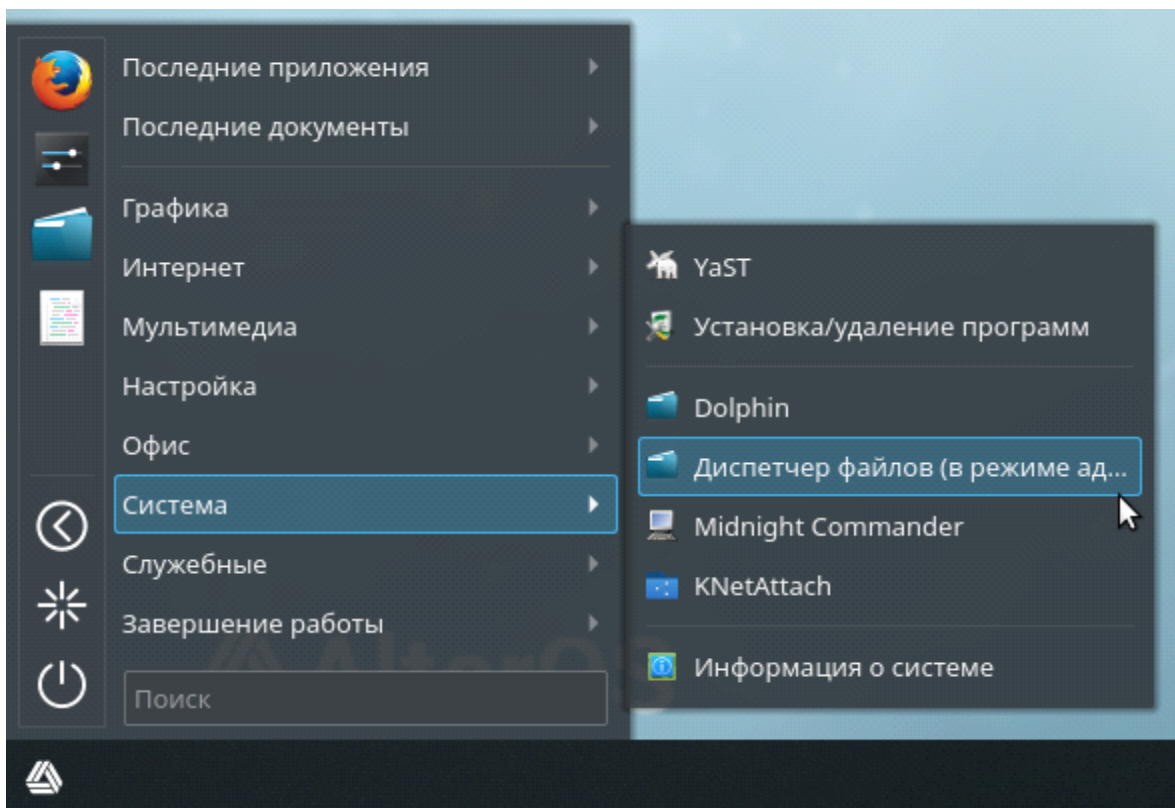
Находим «Установка КриптоПро Fox на Linux» Дистрибутив КриптоПро Fox...» и скачиваем архив кликнув Скачать КриптоПро Fox 45 для 64-разрядных Linux (CentOS 6.6+).



Распаковать скачанный архив можно кликнув по нему правой кнопкой мыши, навести курсор на «Распаковать» и в выпадающем меню кликнуть левой кнопкой мыши на «Распаковать во вложенную папку». Появится новый каталог в том же разделе где и архив с именем *crfox*.

Архив содержит Portable версию, то есть не требующую установки. Начать работу можно прямо сейчас запустив файл *crfox*, но для удобства распакованный каталог необходимо переместить, иначе в дальнейшем могут возникнуть некоторые проблемы.

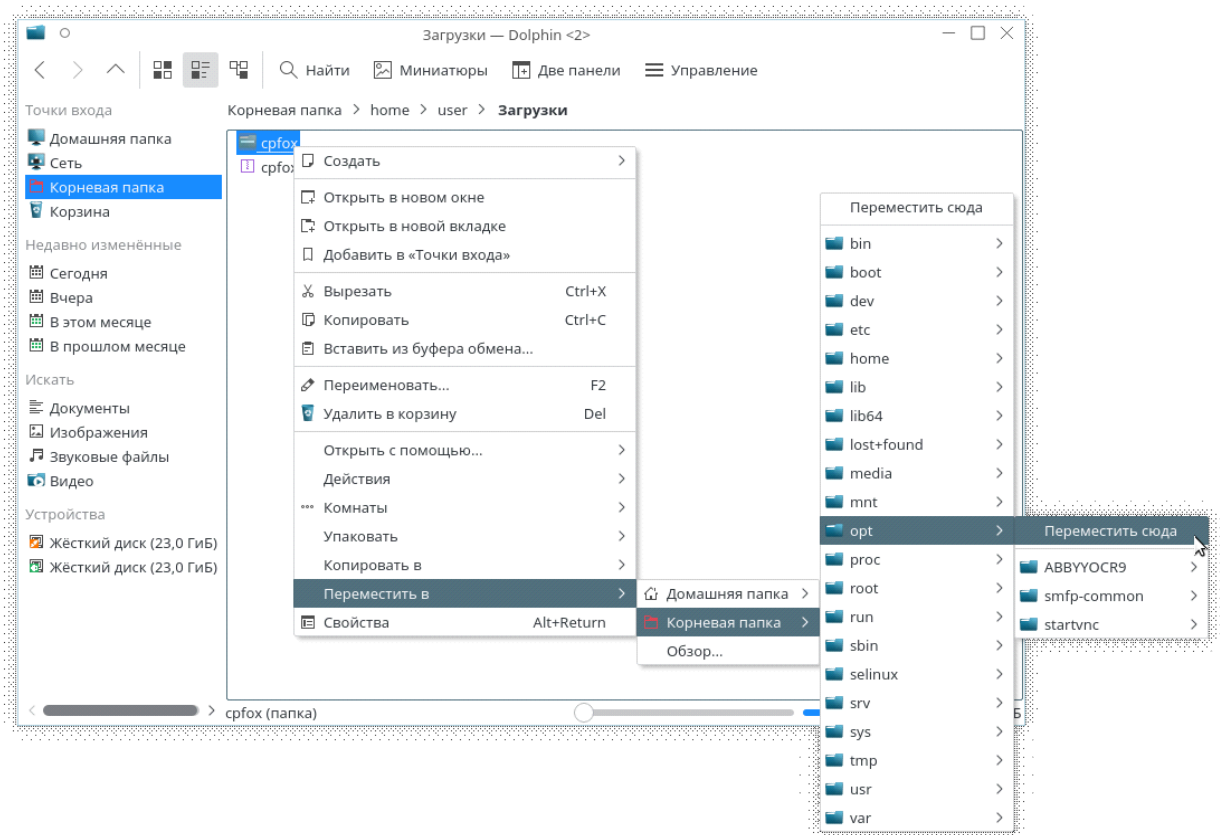
Нужно переместить полученную папку в каталог `/opt/*` для этого необходимо обладать правами суперпользователя, по-другому называемыми правами администратора или root-правами.



В нашем случае необходимо запустить Диспетчер файлов (в режиме администратора). Для этого переходим в «*Меню приложений*» *Система*» *Диспетчер файлов (в режиме администратора)*» и щёлкаем левой кнопкой мыши.

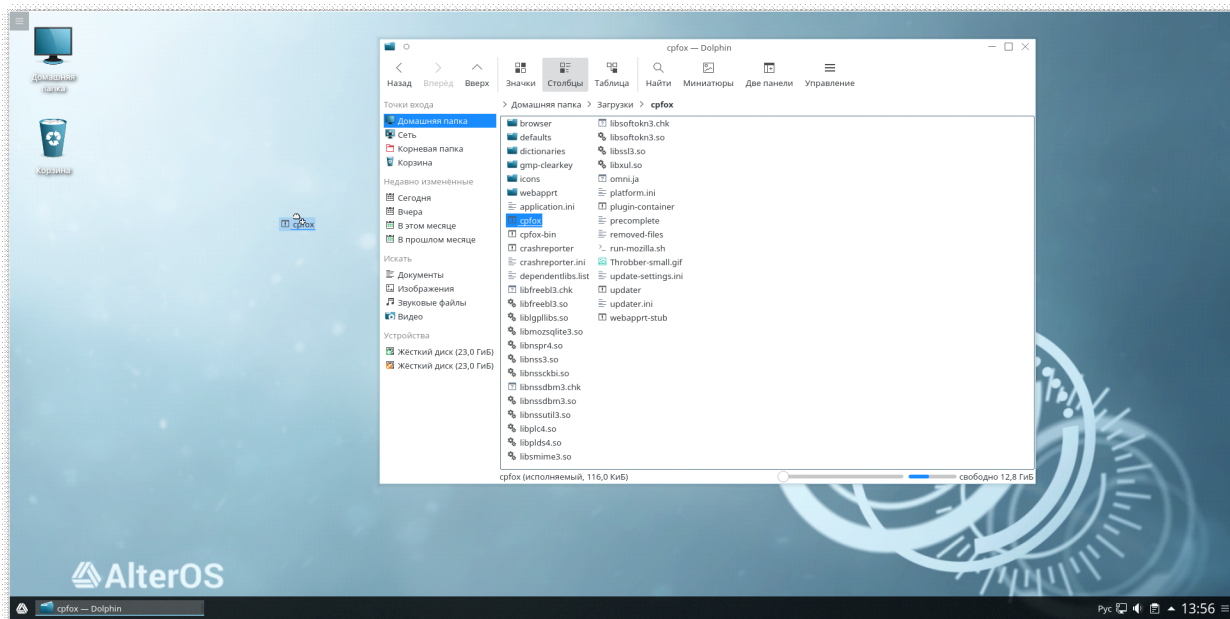
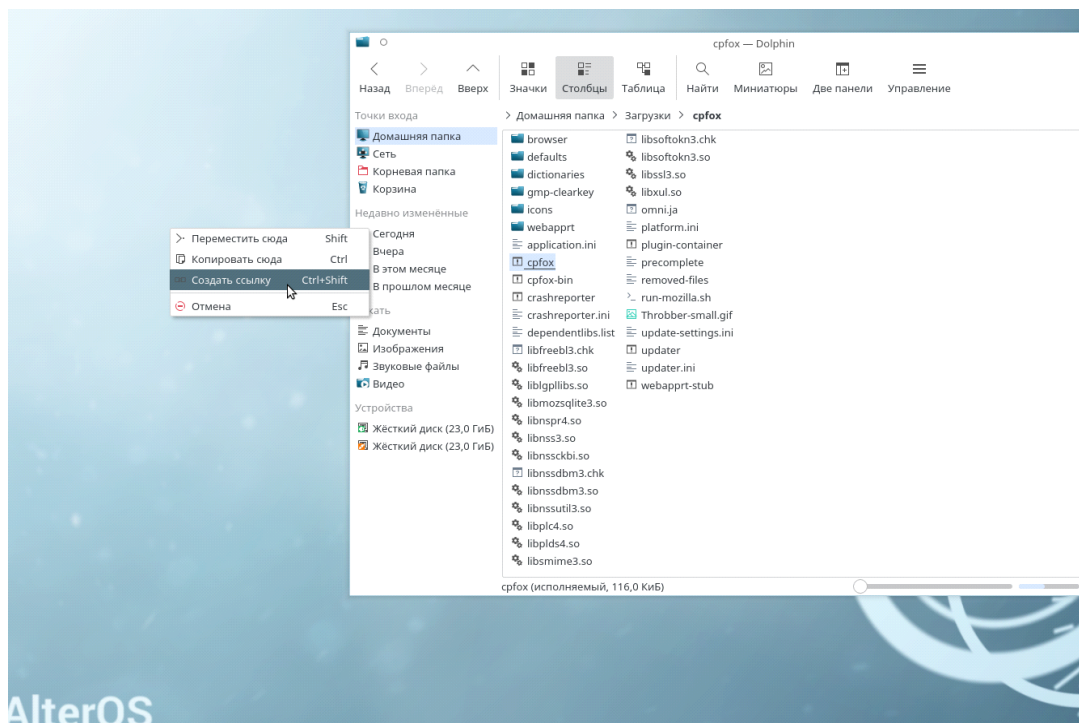
Необходимо будет ввести пароль суперпользователя.

Путь к папке `"/home/<ваше имя пользователя>/Загрузки/"`

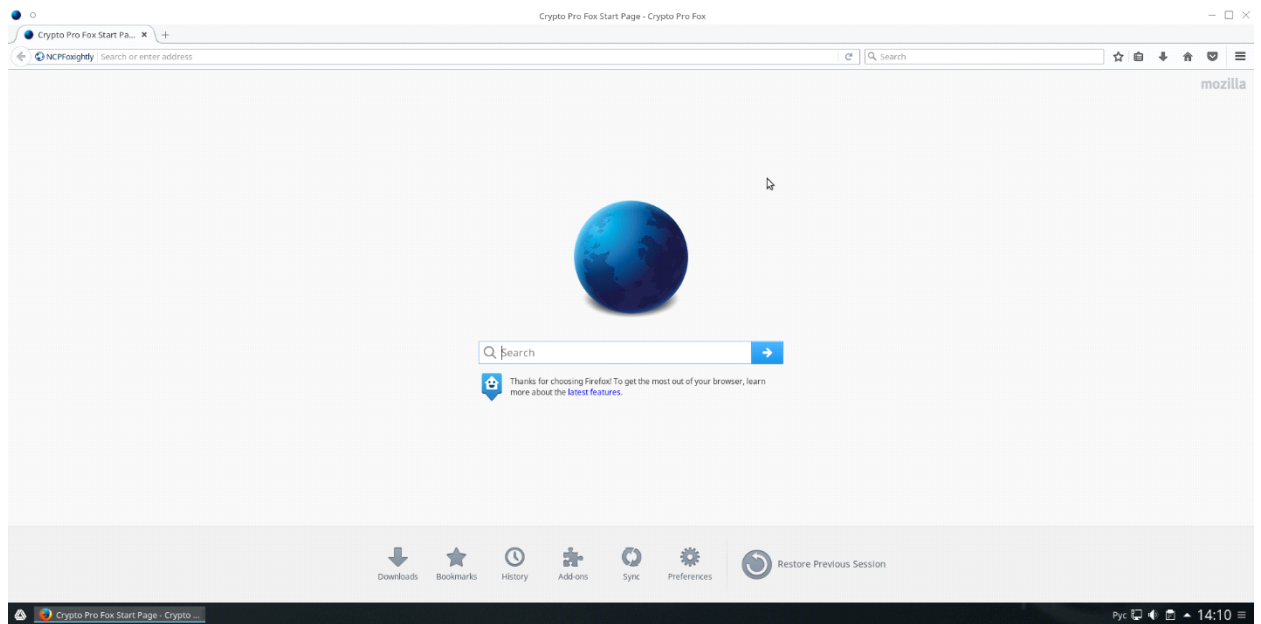


Переместим папку `srfox` нажав правой кнопкой мыши, и выбрав "Переместить в > Корневая папка > opt > Переместить сюда".

Откроем папку `srfox`. В ней находится файл с таким же именем `srfox`, это и есть файл запуска КриптоПро Fox. Для запуска необходимо кликнуть два раза по этому файлу, при этом Mozilla Firefox не должна быть запущена. Выполнять запуск из папки будет не удобно. Создадим ссылку на рабочем столе, для этого зажмём левую кнопку мыши на файле `srfox` и переместим за область окна диспетчера файлов на рабочий стол. В Lite версии нужно зажать Alt+Левая кнопка мыши, чтобы появилось меню после перетаскивания.



Появится меню, выберем «Создать ссылку». Ссылка окажется на рабочем столе.



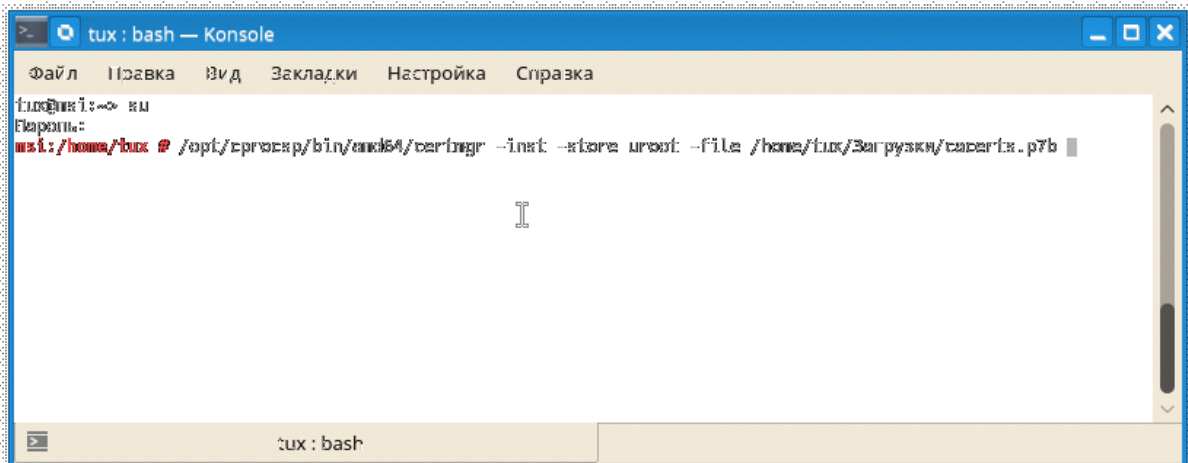
Запустим с помощью ссылки.

КриптоПро Fox готов к работе.

Установка корневого сертификата

Для установки корневого сертификата удостоверяющего центра, необходимо в консоли, в режиме суперпользователя, выполнить команду:

```
/opt/cprosp/bin/amd64/certmgr -inst -store uroot -file <путь к файлу с  
сертификатом>/<сертификат
```



После выполнения команды, поступит запрос на выбор индекса сертификата: "Please choose index of certificate". Необходимо набрать 1, 2 или 3 и нажать Enter.

```

tux : certmgr — Console
Файл Правка Вид Закладки Настройка Справка
-----
Issuer       : E=dif@tinkeyuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тварская
, д. 7", O=Минкомсвязь. Россия, O=DN=1847782826781, DN=887718474375, CN=Главный удостоверяющий центр
Subject     : E=dif@tinkeyuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тварская
, д. 7", O=Минкомсвязь. Россия, O=DN=1847782826781, DN=887718474375, CN=Главный удостоверяющий центр
Serial      : 0x34681E49D41EF3346A887C879925A29
SHA1 Hash  : 0x82e82bbf4444a7a53629064f9839f06e1dca15e2
SubjKeyID   : 8b283b891851e2ef9c8278bb8eac8d428b255c55d
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 34.10-2001 (512 bits)
Not valid before : 28/07/2012 12:31:14 UTC
Not valid after  : 17/07/2027 12:31:14 UTC
PrivateKey Link : No
-----
Please choose index of certificate

```

```

tux : certmgr — Console
Файл Правка Вид Закладки Настройка Справка
-----
Issuer       : E=dif@tinkeyuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тварская
, д. 7", O=Минкомсвязь. Россия, O=DN=1847782826781, DN=887718474375, CN=Главный удостоверяющий центр
Subject     : E=dif@tinkeyuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тварская
, д. 7", O=Минкомсвязь. Россия, O=DN=1847782826781, DN=887718474375, CN=Главный удостоверяющий центр
Serial      : 0x34681E49D41EF3346A887C879925A29
SHA1 Hash  : 0x82e82bbf4444a7a53629064f9839f06e1dca15e2
SubjKeyID   : 8b283b891851e2ef9c8278bb8eac8d428b255c55d
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 34.10-2001 (512 bits)
Not valid before : 28/07/2012 12:31:14 UTC
Not valid after  : 17/07/2027 12:31:14 UTC
PrivateKey Link : No
-----
Please choose index of certificate
1

```

Если появилось сообщение [ErrorCode: 0x00000000] значит установка прошла успешно.


```
tux : bash — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка
-----
Install:
-----
1-----
Issuer          : O=ИП-087718474375, OU=1847702026701, E=it@itnkvuz.ru, STREET=125375 г. Москва ул. Тверская д.7, CN=Ит
Инженерия, Россия, L=Москва, S=77 г. Москва, C=RU, OU=ИТ ИК ГИИ
Subject         : E=it@itnkvuz.ru, OU=1885262223444, IPN=085262223444, C=RU, S=52 Нижегородская область, L=Нижегород
Город, STREET=Генералов д.1, OU=Центральный центр, O="ОАО "Нижегородский территориальный центр информатизации"", CN=ИТ
LN
Serial          : 0004A81E4005A9185CE2E61181E7198437C2
SHA1 Hash       : 0066014807de71cd24a37cd592e6736ec4ba27aebb3
SubjKeyID       : 5b0c0427c4040ed5a3c97f1a23b3c0e103f1de25
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 34.10-2001 (512 bits)
Not valid before : 31/01/2017 06:41:59 UTC
Not valid after  : 07/12/2026 10:51:11 UTC
PrivateKey Link  : No
CA cert URL     : http://roxiatacom.ru/cdp/vguc1_5.crl
CA cert URL     : http://reaxtr-pk1.ru/cdp/vguc1_5.crl
CSP             : http://roxiatacom.ru/cdp/vguc1_5.crl
CSP             : http://reaxtr-pk1.ru/cdp/vguc1_5.crl

[ErrorCode: 0x00000000]
msl:/home/tux #
```

Чтобы проверить установку сертификата, можно выполнить команду:

```
/opt/cproscsp/bin/amd64/certmgr -list
```

```
tux : bash — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка
-----
tux@itnkvuz:~$ cd
Пароль:
msl:/home/tux # /opt/cproscsp/bin/amd64/certmgr -list -store myroot -file /home/tux/Загрузки/cacert1x.p7b
Certmgr 1.0 (c) "CryptoPro", 2007-2010.
program for managing certificates, CRLs and stores
-----
1-----
Issuer          : O=ИП-087718474375, OU=1847702026701, E=it@itnkvuz.ru, STREET=125375 г. Москва ул. Твер
ская д.7, CN=ИтИнженерия, Россия, L=Москва, S=77 г. Москва, C=RU, OU=ИТ ИК ГИИ
Subject         : E=it@itnkvuz.ru, OU=1885262223444, IPN=085262223444, C=RU, S=52 Нижегородская область
, L=НижегородГород, STREET=Генералов д.1, OU=Центральный центр, O="ОАО "Нижегородский территориальный центр
информатизации"", CN=ИТ HTML
Serial          : 0004A81E4005A9185CE2E61181E7198437C2
SHA1 Hash       : 0066014807de71cd24a37cd592e6736ec4ba27aebb3
SubjKeyID       : 5b0c0427c4040ed5a3c97f1a23b3c0e103f1de25
Signature Algorithm : ГОСТ Р 34.11/34.10-2001
PublicKey Algorithm : ГОСТ Р 34.10-2001 (512 bits)
Not valid before : 31/01/2017 06:41:59 UTC
Not valid after  : 07/12/2026 10:51:11 UTC
PrivateKey Link  : No
CA cert URL     : http://roxiatacom.ru/cdp/vguc1_5.crl
CA cert URL     : http://reaxtr-pk1.ru/cdp/vguc1_5.crl
CSP             : http://roxiatacom.ru/cdp/vguc1_5.crl
CSP             : http://reaxtr-pk1.ru/cdp/vguc1_5.crl

msl:/home/tux #
```

Подписать сертификатом с e-мэйлом указанным в нем (из предыдущей команды)

```
/opt/cproscsp/bin/amd64/cryptcp -sign -dn E=test@alteros.ru Path_to_file/file.pdf
```

```
/opt/cprosp/bin/amd64/cryptcp -verify Path_to_file/file.pdf.sig
```

Ключ "-verify" у утилиты cryptcp предназначен для проверки attached подписи, если она detached, проверять надо так:

```
/opt/cprosp/bin/amd64/cryptcp -vsignf -f file.pdf.sig file.pdf1
```