



# **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:

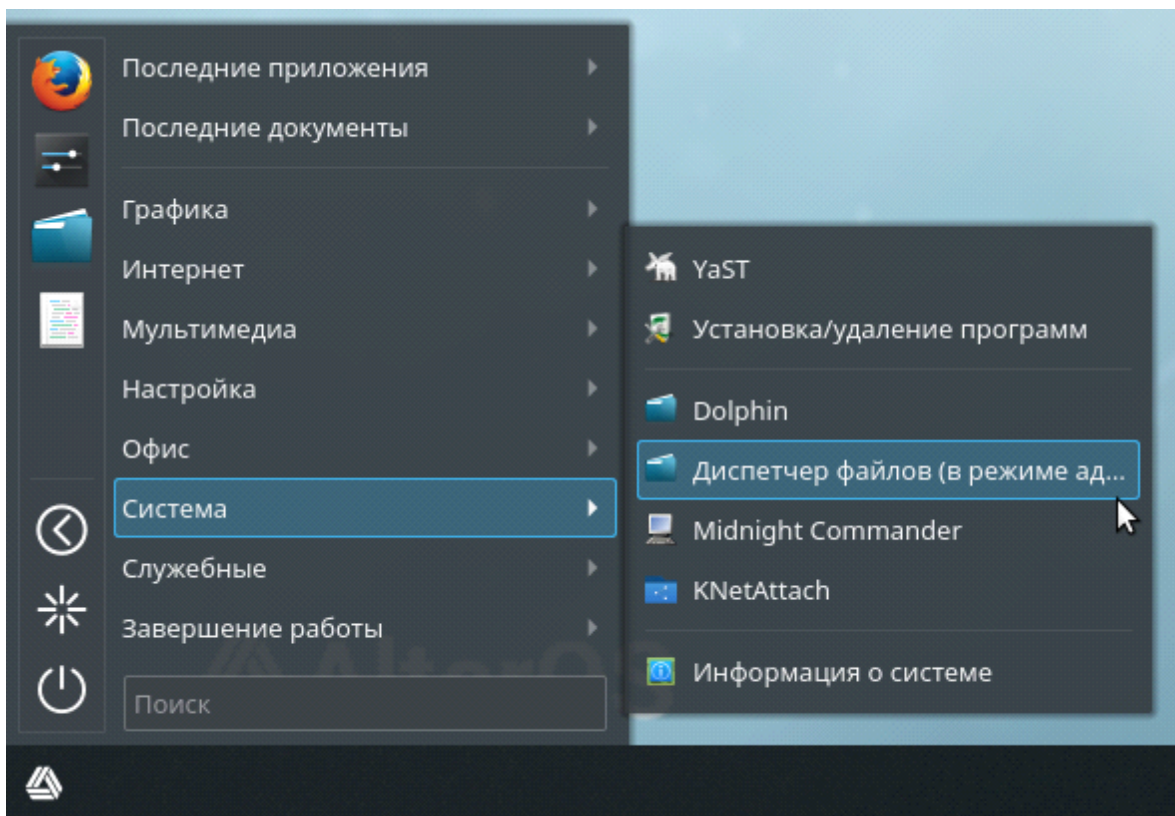
**<https://www.cryptopro.ru/products/cpfox>**

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 *srfox*.

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

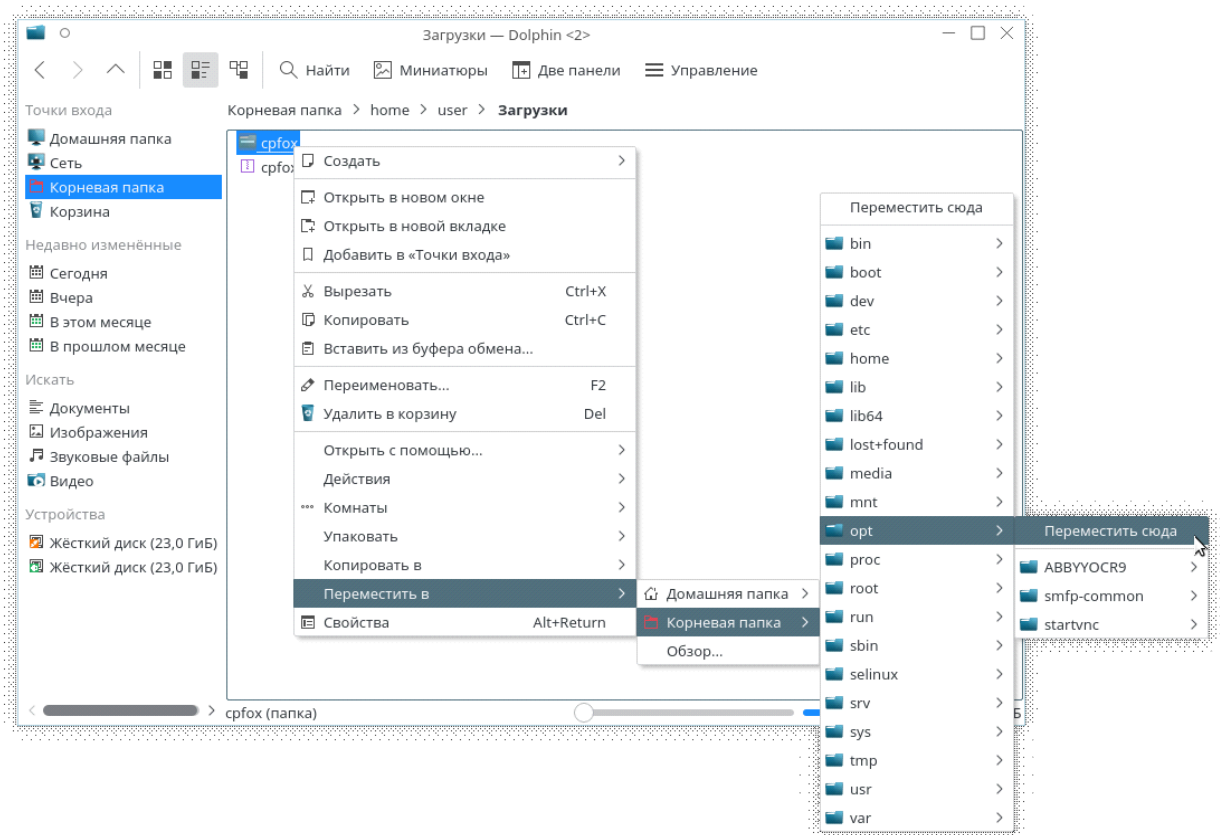
Нужно переместить полученную папку в каталог */opt/\** для этого необходимо обладать правами суперпользователя, по-другому называемыми правами администратора или root-правами.



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.

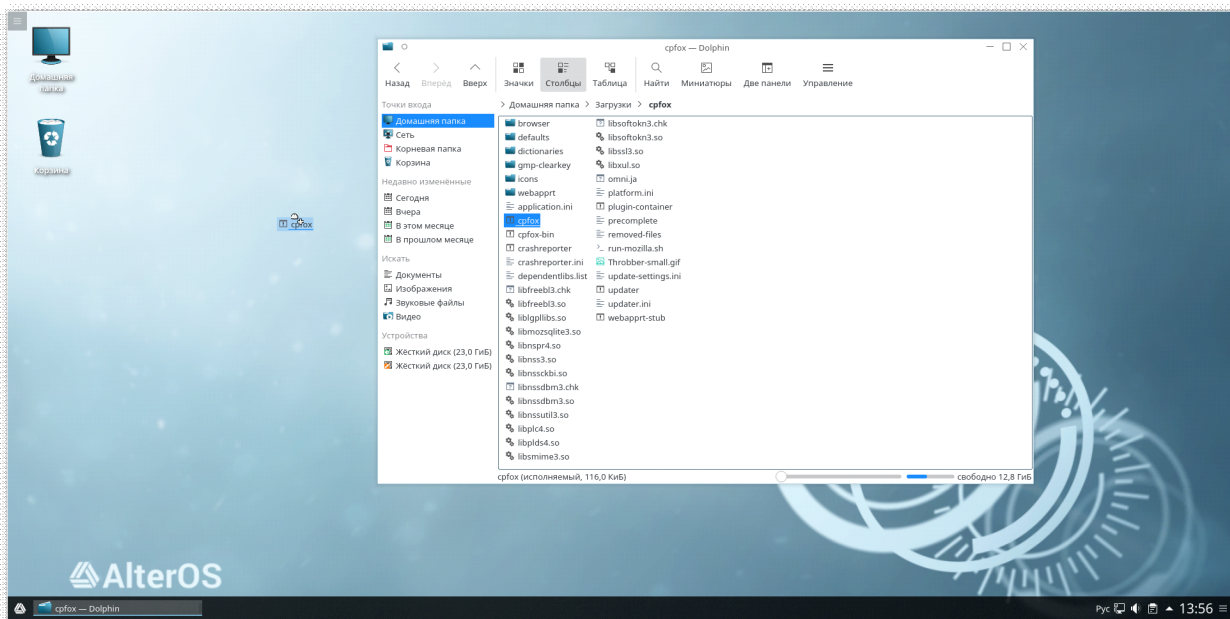
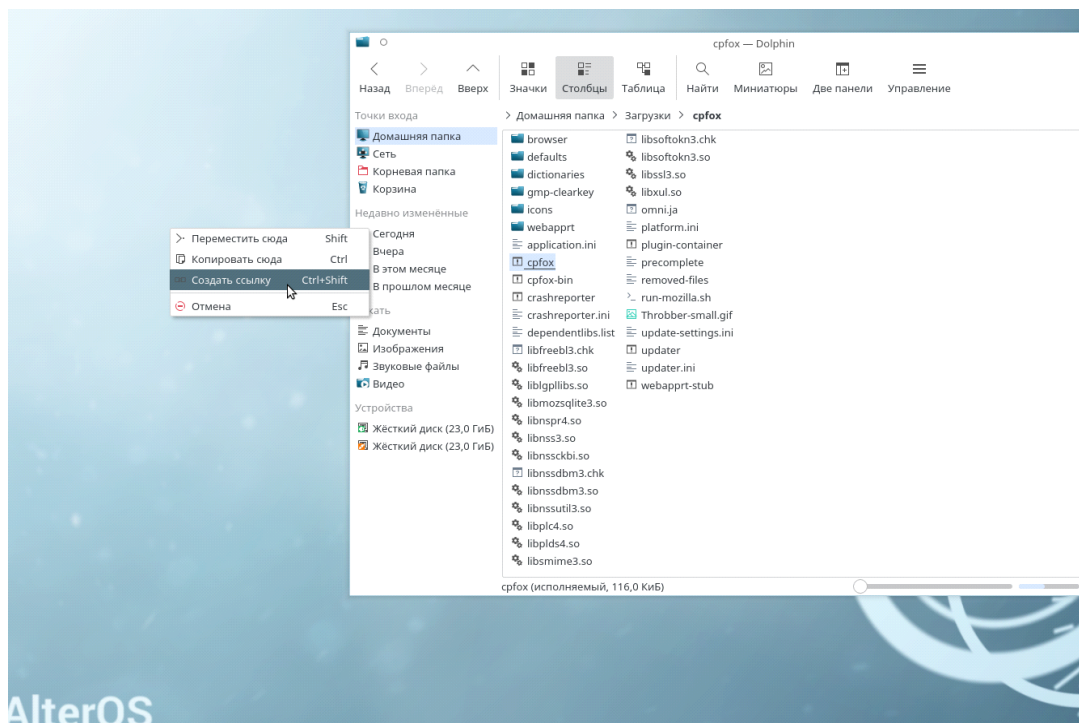
Необходимо будет ввести пароль суперпользователя.

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

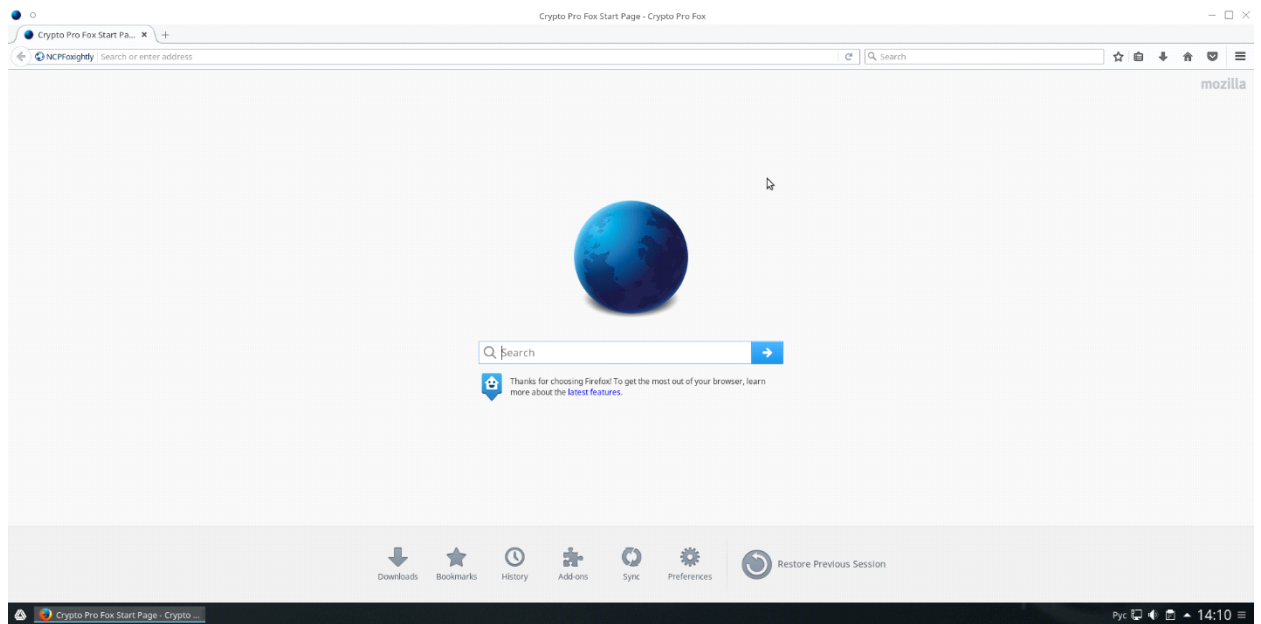


Переместим папку `srfox` нажав правой кнопкой мыши, и выбрав "Переместить в > Корневая папка > opt > Переместить сюда".

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.



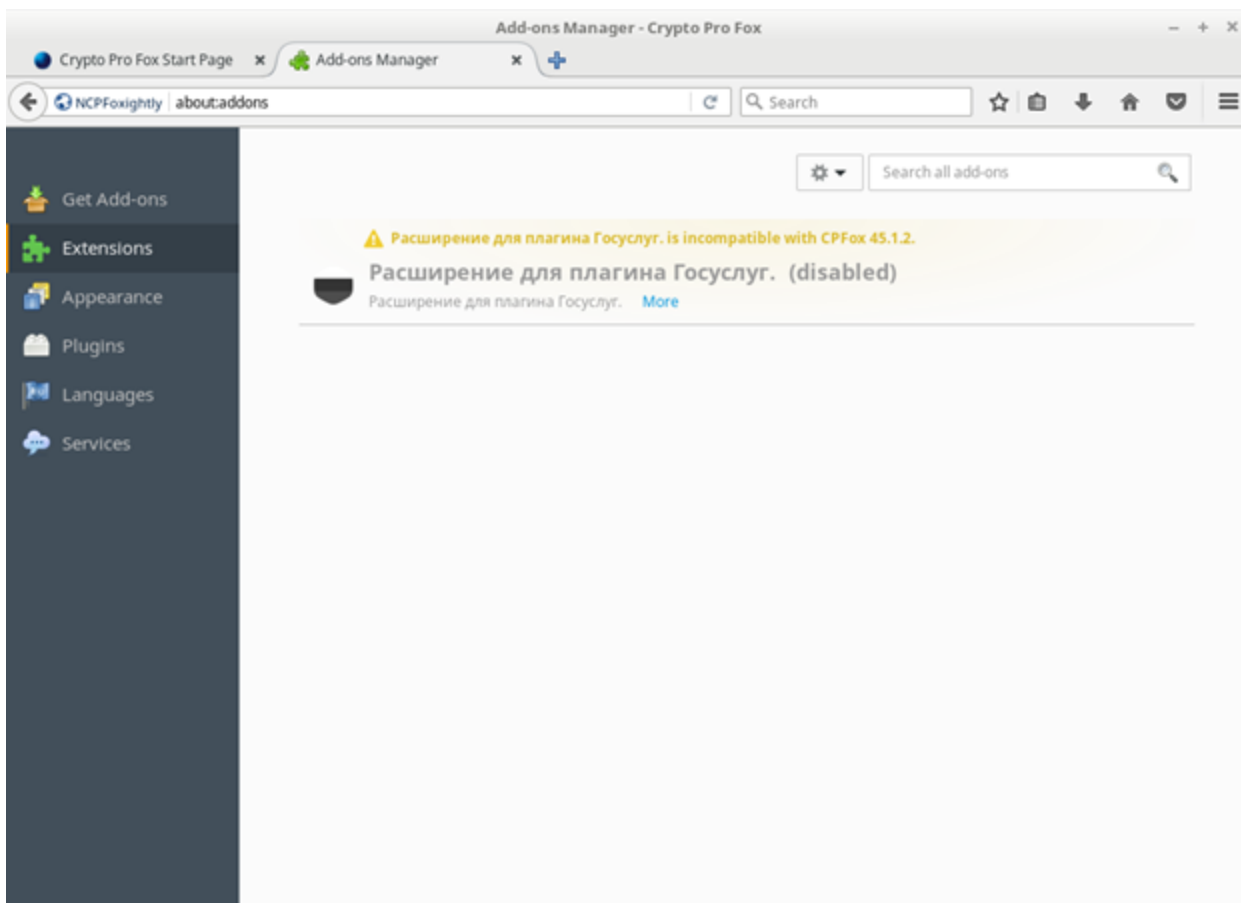
Запустим с помощью ссылки.

КриптоПро Fox готов к работе.

Установка плагина *IFCPlugin* в *CryptoFox*:



**Внимание!** Если Вы установили дополнение с сайта госуслуги (*IFCPlugin*) то его необходимо отключить в настройках *CryptoFox*:



Для входа в закрытую часть сайта *zakupki.gov.ru* необходимо 2 условия:

- 1) Браузер поддерживает TLS
- 2) Браузер умеет работать с ЭЦП через дополнения и плагины.

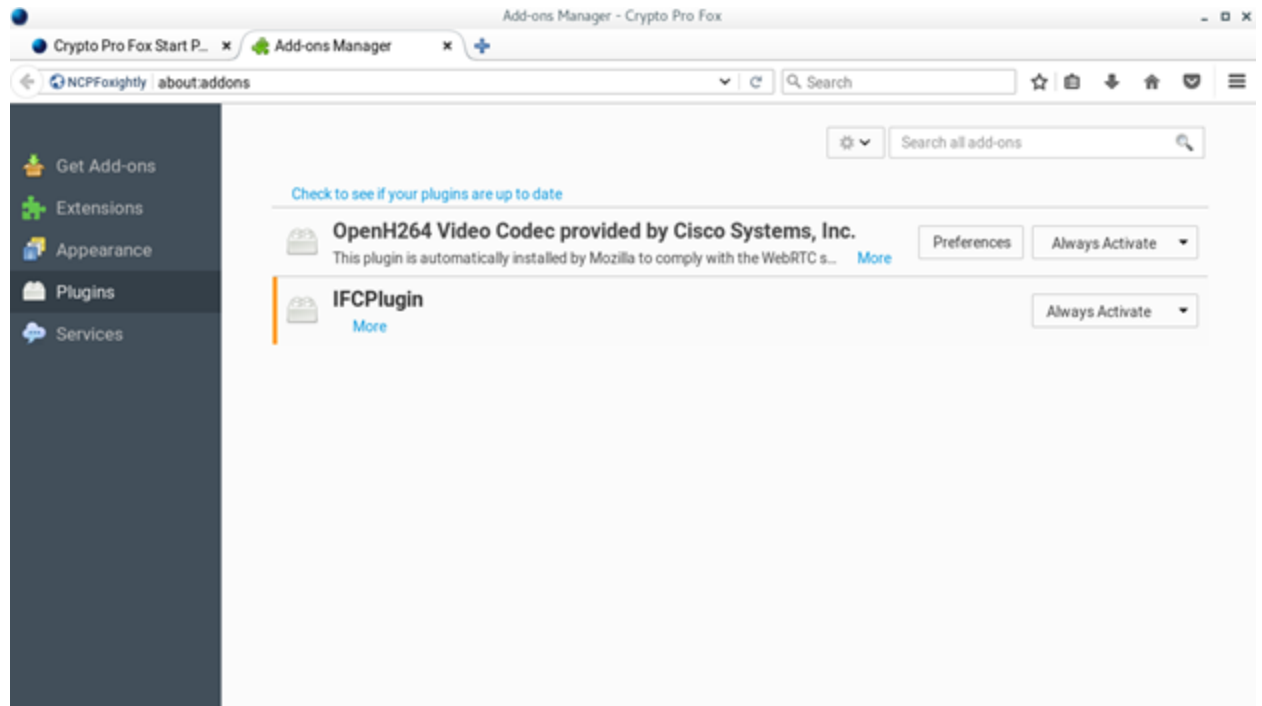
Перейдя на вкладку Plugins (Плагины) мы должны увидеть плагин IFCPlugin. Для того что бы браузер увидел дополнительный плагин необходимо:

- а) запустить терминал `konsole`
- б) в терминале ввести и выполнить команду от имени текущего пользователя (или заменить символ `~` на путь к домашней папке пользователя ):



```
In -s /usr/lib64/mozilla/plugins ~/.mozilla/firefox/*.default/
```

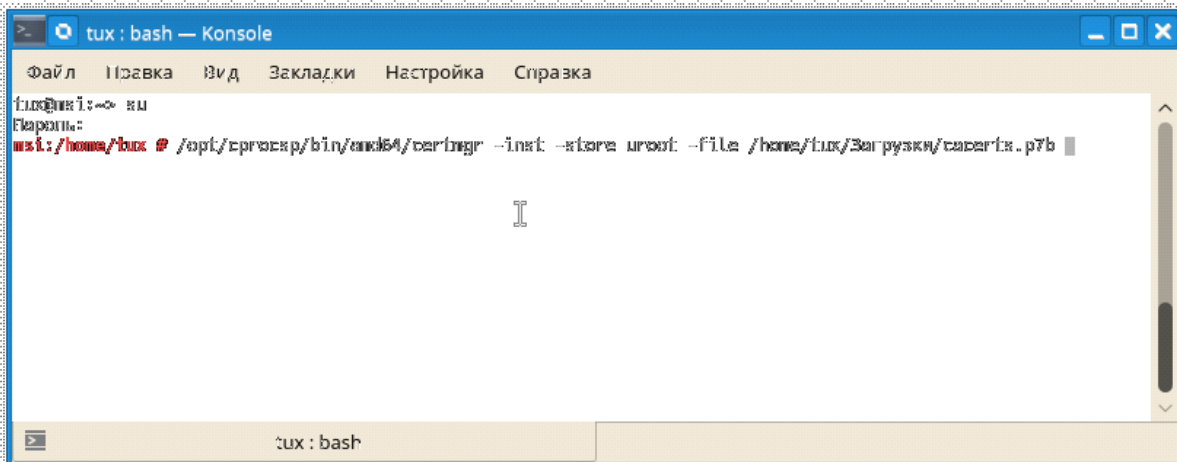
в) запустить *cryptofox* и включить дополнение на вкладке *Plugins* (установить статус Always Activate).



## Установка корневого сертификата

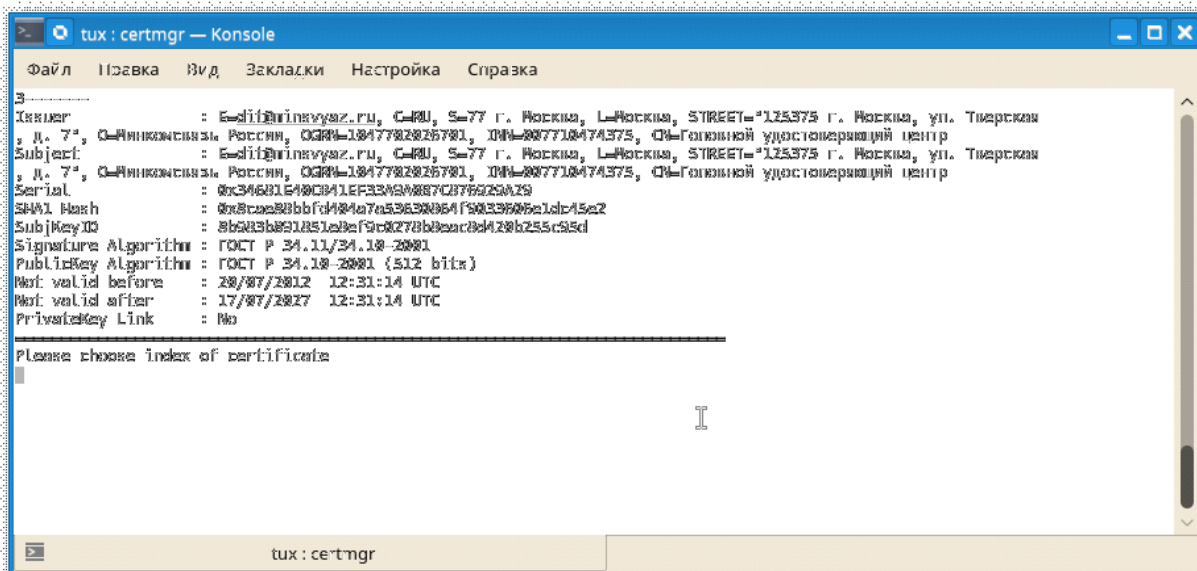
Для установки корневого сертификата удостоверяющего центра, необходимо в консоли, в режиме суперпользователя, выполнить команду:

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



```
tux : bash — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка
tux@tux:~$ certmgr -init -store urcert -file /home/tux/Загрузки/cacertfx.p7b
tux : bash
```

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 — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка
-----
Issuer          : E=ii@ipkuyuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тiersкая
, д. 7", O=Имянкэскыз. Россия, ODN=1847782826781, DN=887718474375, CN=Голыной удостоверный центр
Subject        : E=ii@ipkuyuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET="125375 г. Москва, ул. Тiersкая
, д. 7", O=Имянкэскыз. Россия, ODN=1847782826781, DN=887718474375, CN=Голыной удостоверный центр
Serial         : 0x34631648041EF33A9887C878825A19
SHA1 Hash      : 0x8c5e28bbfd484a7a53630054f583360fe1dc45a2
SubjectID      : 8b823b891851e8ef9c8278bbeac8a428b255c95d
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 — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка
-----
1-----
Issuer       : E=efi@tinivuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET=125375 г. Москва, ул. Тверская
, д. 7, O=Минкомсвязь, Россия, ODN=1847782826781, INN=887718474375, CN=Головной удостоверяющий центр
Subject     : E=efi@tinivuz.ru, C=RU, S=77 г. Москва, L=Москва, STREET=125375 г. Москва, ул. Тверская
, д. 7, O=Минкомсвязь, Россия, ODN=1847782826781, INN=887718474375, CN=Головной удостоверяющий центр
Serial      : 0x346816480b41ef3346a887c879925a29
SHA1 Hash   : 0x82eae8bbf6f44a7a53628064f98239606e1dca45e2
SubjKeyID   : 8b283b891851e9ef9c8278bb9eac8d428b235c55d
Signature Algorithm : ГОСТ P 34.11/34.10-2001
PublicKey Algorithm : ГОСТ P 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       : INN=887718474375, ODN=1847782826781, E=efi@tinivuz.ru, STREET=125375 г. Москва ул. Тверская д.7, O=Минкомсвязь, Россия, L=Москва, S=77 г. Москва, C=RU, CN=11 ИС ГСЛ
Subject     : E=efi@tinivuz.ru, ODN=1885262223444, C=RU, S=52 Нижегородская область, L=Нижегородский Новогород, STREET=Городской д.1, O=Удостоверяющий центр, O=C=OAO "Нижегородский территориальный центр информатизации", CN=ИТ ИТ ЛМ
Serial      : 0x044816480549185c82e61181e7198437c2
SHA1 Hash   : 0x66814887d671d24a37d692067396c4ba27e9eb3
SubjKeyID   : 5b0ca427c4040e4508c87f1a23b3c0e183f1d625
Signature Algorithm : ГОСТ P 34.11/34.10-2001
PublicKey Algorithm : ГОСТ P 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://reestr.cca.ru/csp/vgucl_5.crt
CA cert URL   : http://reestr-pki.ru/csp/vgucl_5.crt
CSP           : http://reestr.cca.ru/csp/vgucl_5.crt
CSP           : http://reestr-pki.ru/csp/vgucl_5.crt

[ErrorCode: 0x00000000]
msi:/home/tux #

```

Чтобы проверить установку сертификата, можно выполнить команду:

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

```
tux : bash — Konsole
Файл  Правка  Вид  Закладки  Настройка  Справка
tux@tux:~$ cd
Пароль:
tux@tux:~$ /opt/cproccsp/bin/amd64/cryptcp --inpk --store urcert --file /home/tux/Загрузки/cacert1.p7b
Cryptcp 1.0 (c) "CryptcpPro", 2007-2010.
программ для managing certificates, CRLs and stores

-----
1-----
Issuer          : O=RU-087718474375, O=DNI=1847702026701, E=efi@nikayaz.ru, STREET=125375 г. Москва ул. Твер
ская д.7, С=Янтарный, Россия, L=Москва, S=77 г. Москва, C=RU, CN=31 1 MC GSI
Subject        : E=uc@nic.ru, O=DNI=1885260001801, O=RU-08526221344, C=RU, S=52 Нижегородская область
, L=Нижегород, STREET=Генералов д.1, O=Удостоверяющий центр, С=ОАО "Нижегородский территориальный центр
информатизации", CN=31 HTML
Serial         : 00044816400549185C82E61181E7150437C2
SHA1 Hash      : 00666014007de77ed24a37cd692e6736ec4ba27a6eb3
SubjKeyID      : 5bce6427c404a6e55a3c87f1a23b3c8e103f1de25
Signature Algorithm : ГОСТ P 34.11/34.10-2001
PublicKey Algorithm : ГОСТ P 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://rextelcom.ru/csp/vguc1_5.crl
CA cert URL     : http://rextel-pki.ru/csp/vguc1_5.crl
CSP             : http://rextelcom.ru/csp/vguc1_5.crl
```

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

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

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