Средство криптографической защиты информации «Криптографический сетевой программный комплекс "КриптоПро NGate"». Руководство пользователя. ОС Linux

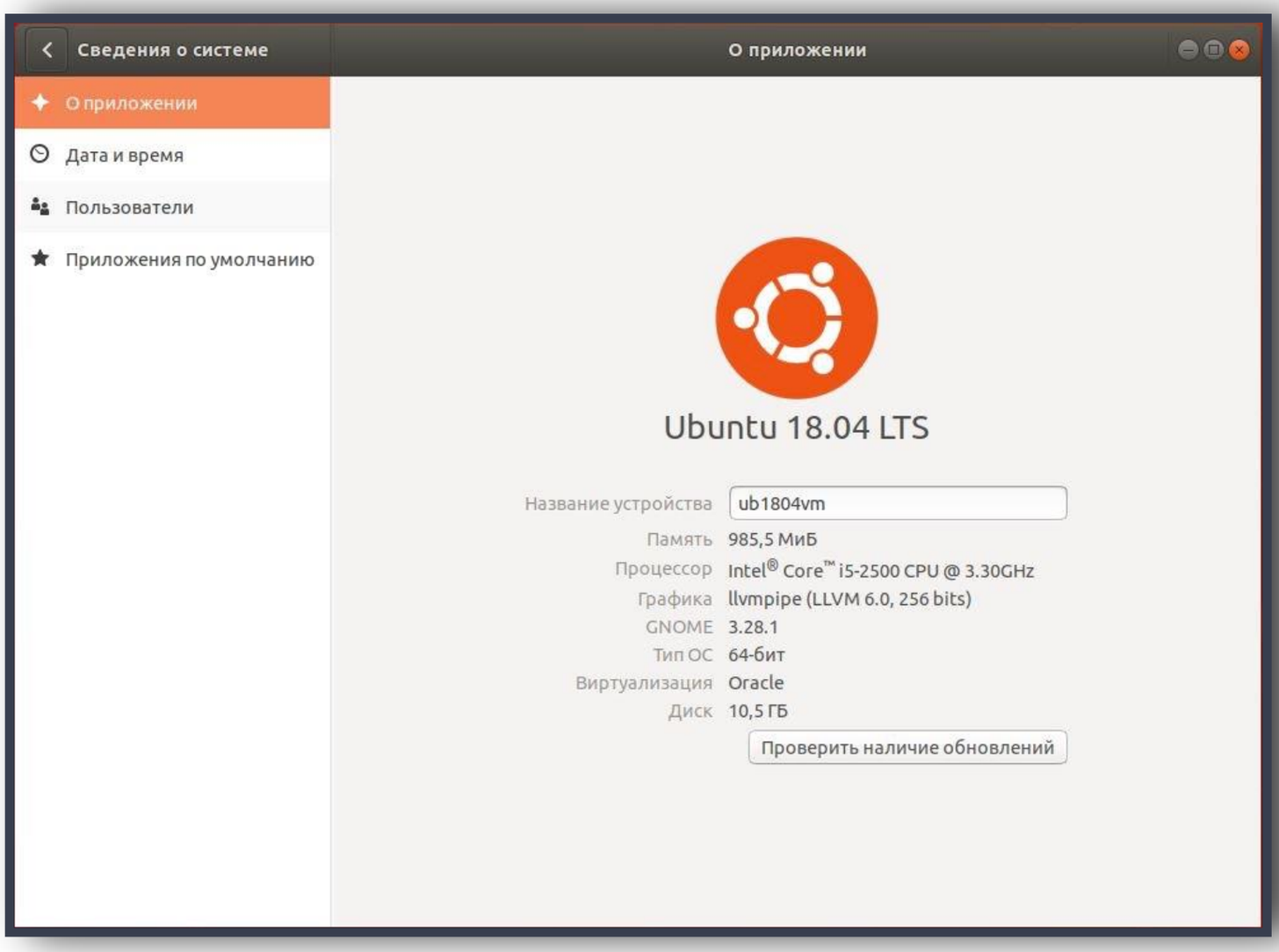
ЖТЯИ.00104-01 91 02

КриптоПро NGate – это высокопроизводительный шлюз на базе протокола TLS, который позволяет безопасно и быстро организовать защищённый доступ удалённых пользователей к корпоративным ресурсам через незащищённые сети, например, сеть Интернет.

В документе будет описан процесс установки и подготовка к работе клиентского программного обеспечения КриптоПро NGate : КриптоПро CSP и «КриптоПро NGate Клиент».

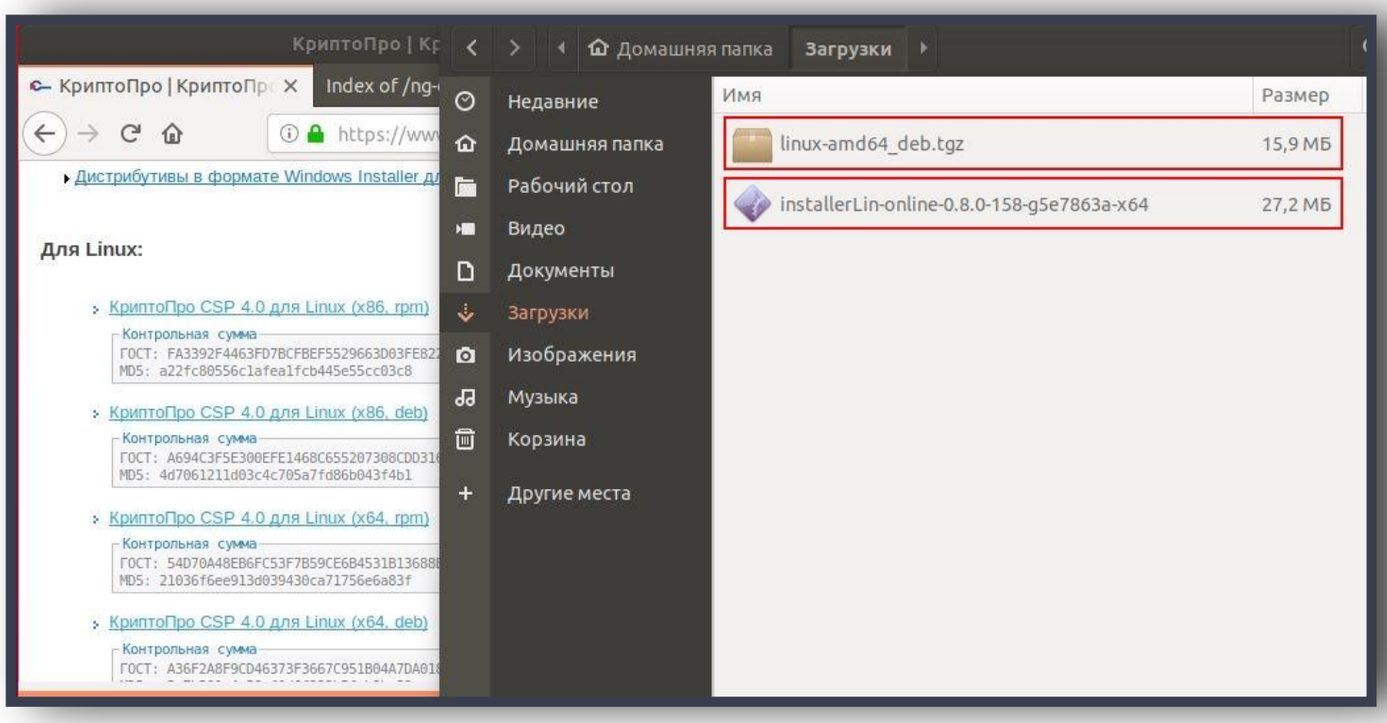
ПО «КриптоПро NGate Клиент» является частью КСПК NGate, и должен эксплуатироваться в соответствии с требованиями Формуляра ЖТЯИ.00104-01 30 01.

В качестве ОС будет использоваться Ubuntu 18.04 LTS



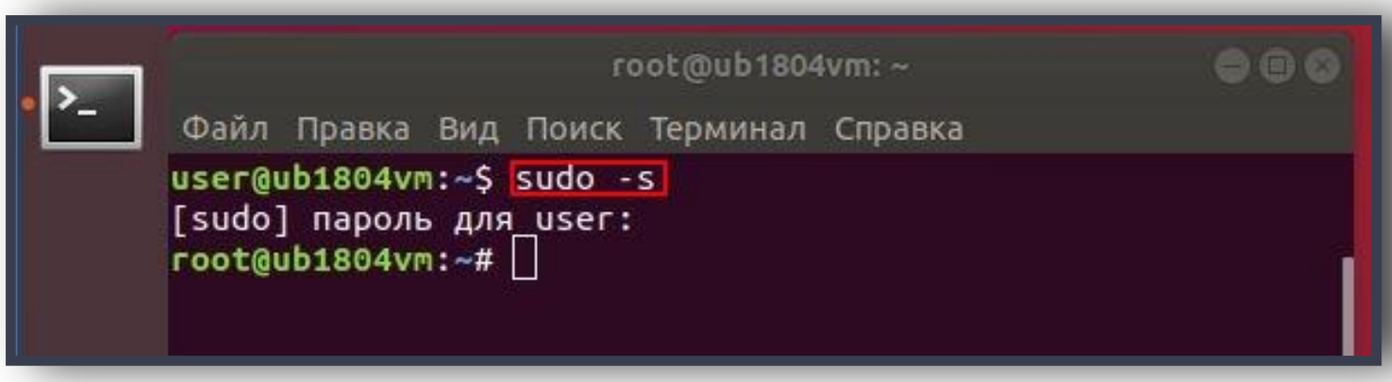
Окно сведений о системе ОС Ubuntu

Потребуется архив КриптоПро CSP, который можно скачать с сайта *cryptopro.ru* после предварительной свободой регистрации. В примере будет использоваться версия 4.0R4 (4.0.9948). Также потребуется установочный пакет клиентского ПО КриптоПро NGate.



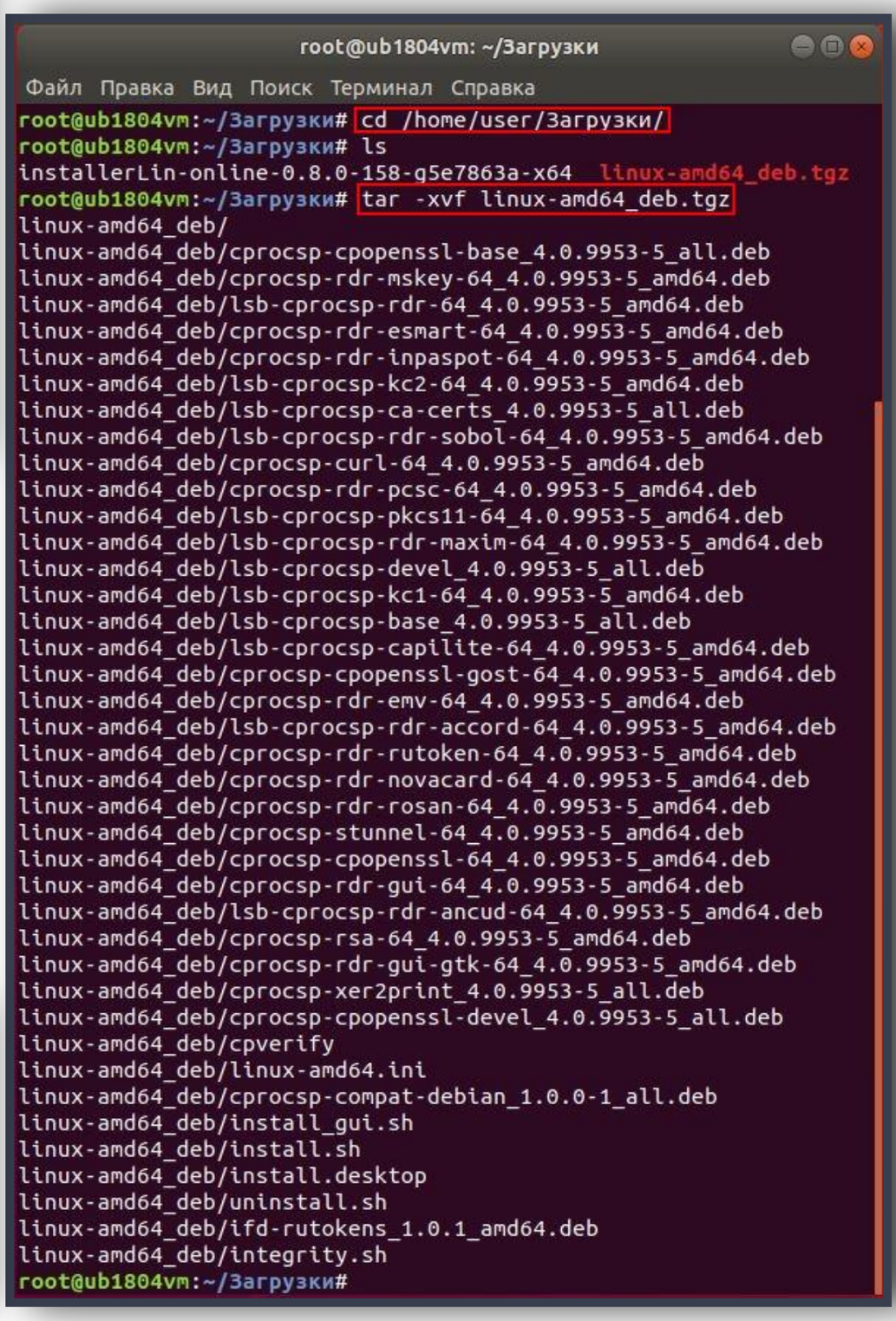
Архив с пакетами криптопровайдера КриптоПро CSP, скачанный с официального сайта КриптоПро, и инсталляционный пакет клиентского ПО КриптоПро NGate Клиент

Произведем установку криптопровайдера КриптоПро CSP. Для этого следует запустить терминал и получить права суперпользователя.

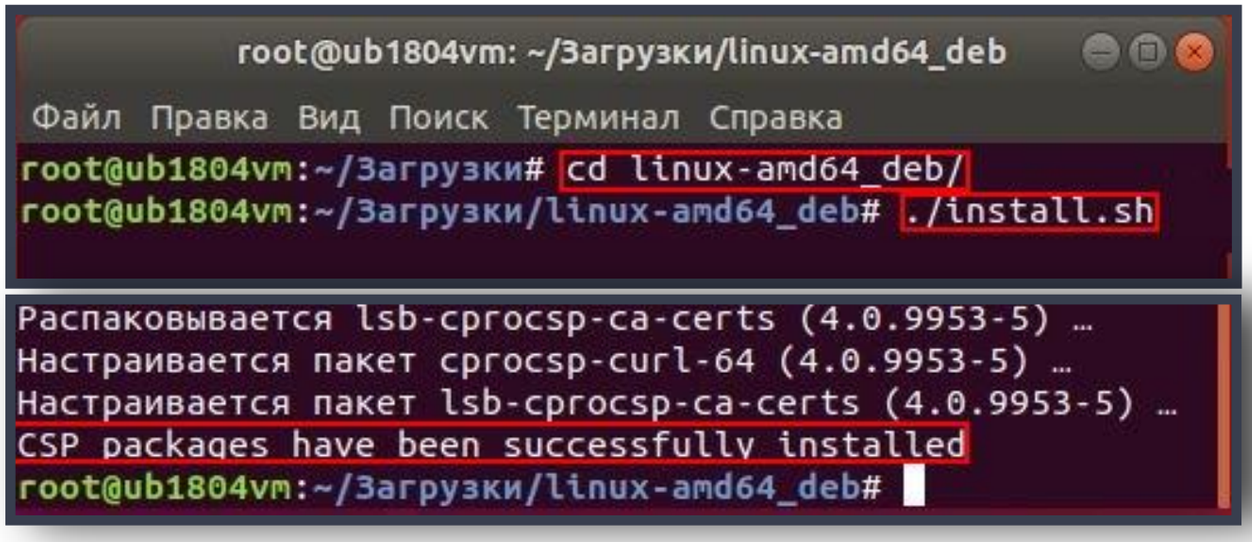


Получение прав суперпользователя

Следует зайти в папку с архивом и произвести его распаковку.

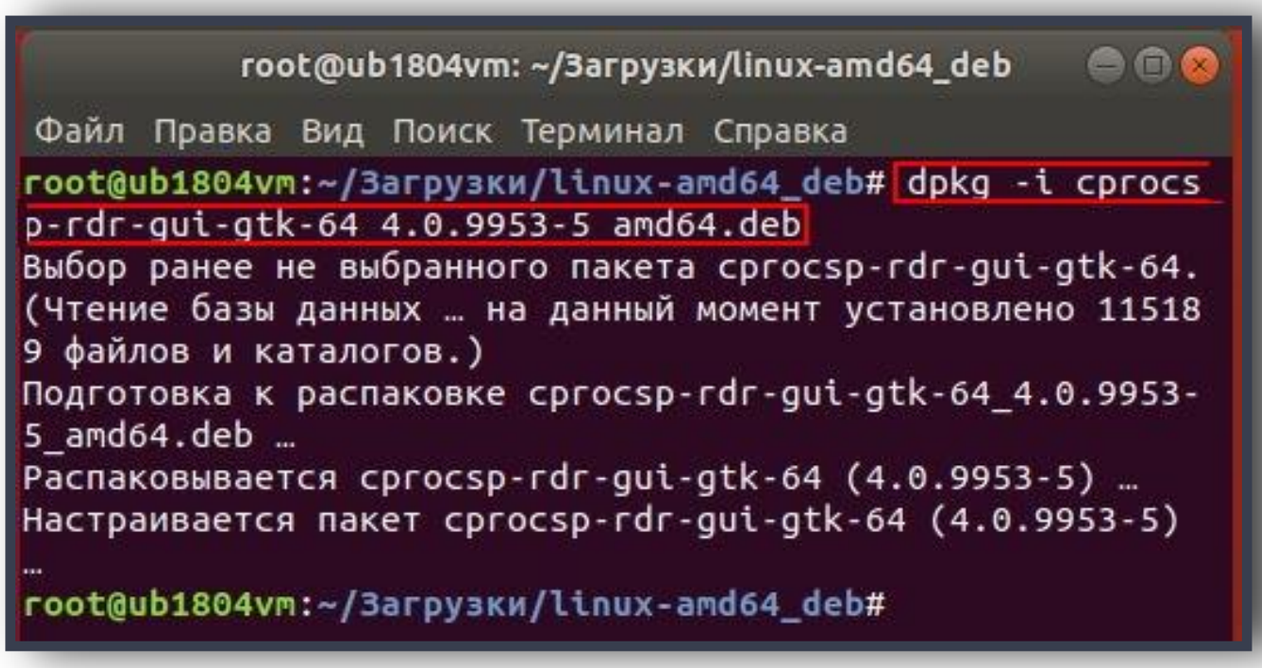


Распаковка архива криптопровайдера

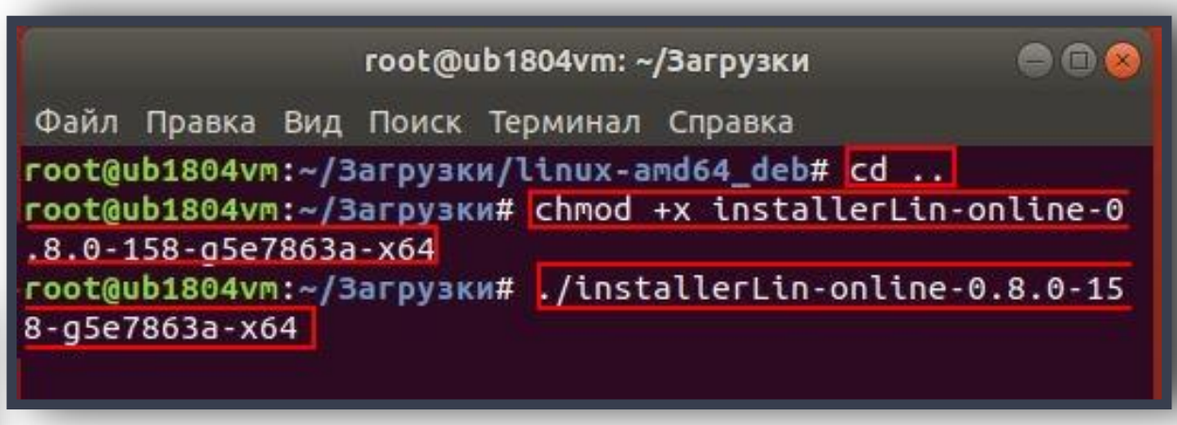


Успешное завершение работы скрипта установки базовых пакетов криптопровайдера

Перейдя в папку с распакованным содержимым архива, следует запустить скрипт установки базовых пакетов криптопровайдера ./install.sh После, следует дополнительно установить еще один пакет вручную.

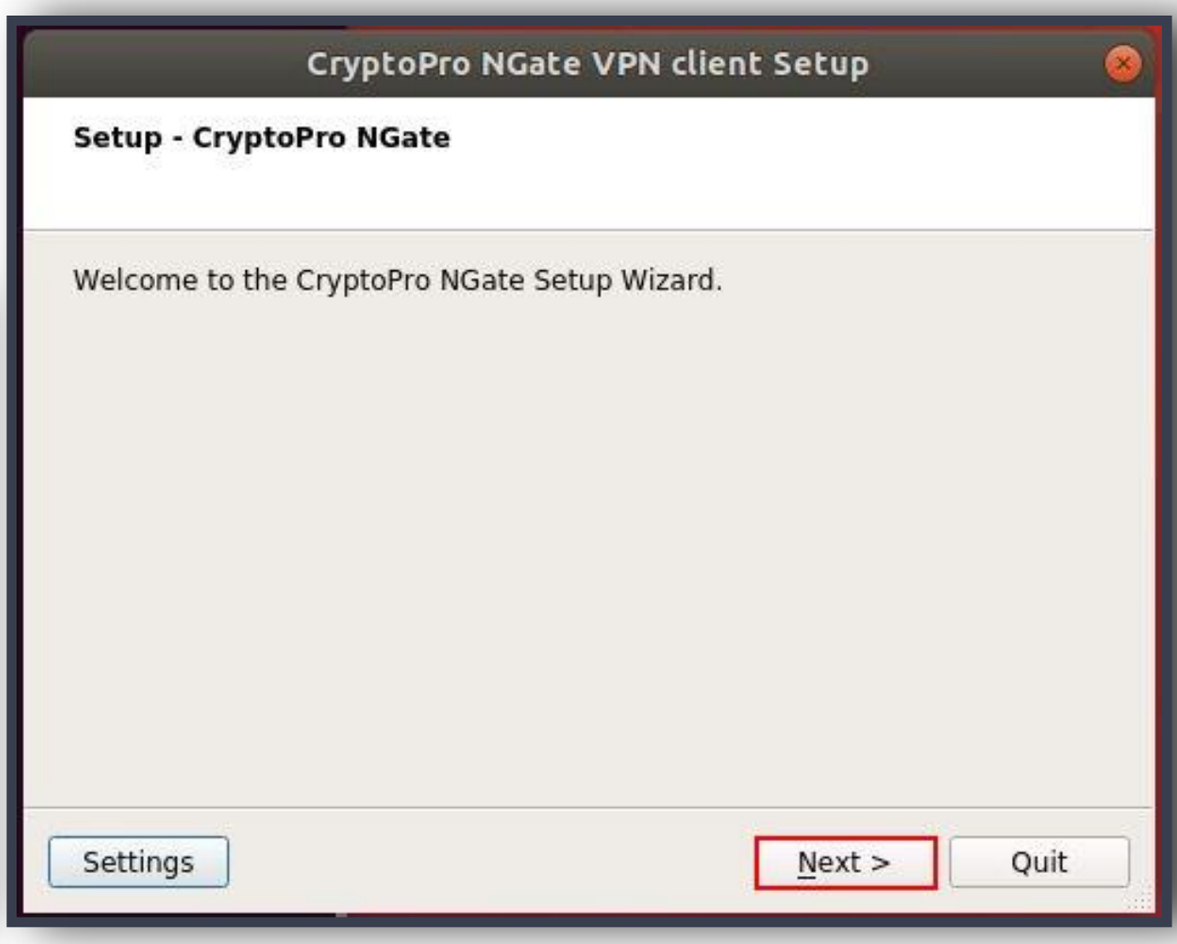


Установка требуемого пакета вручную

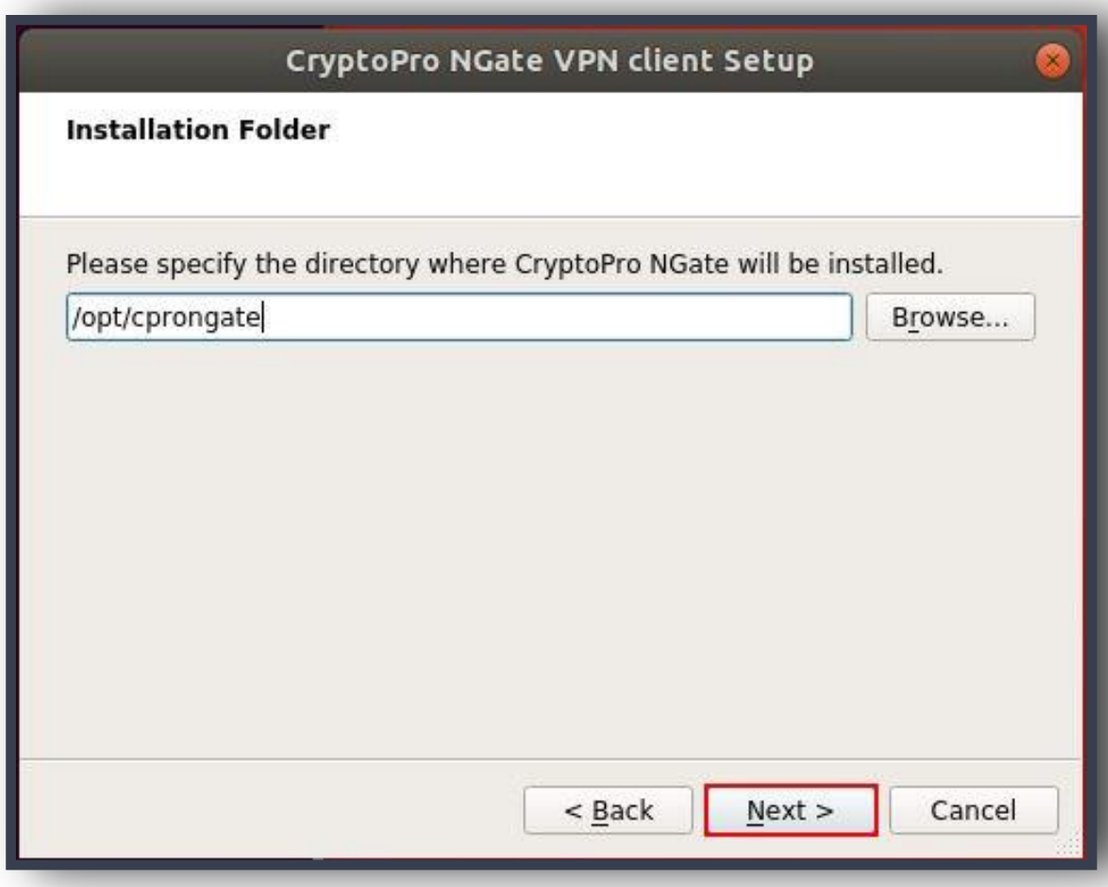


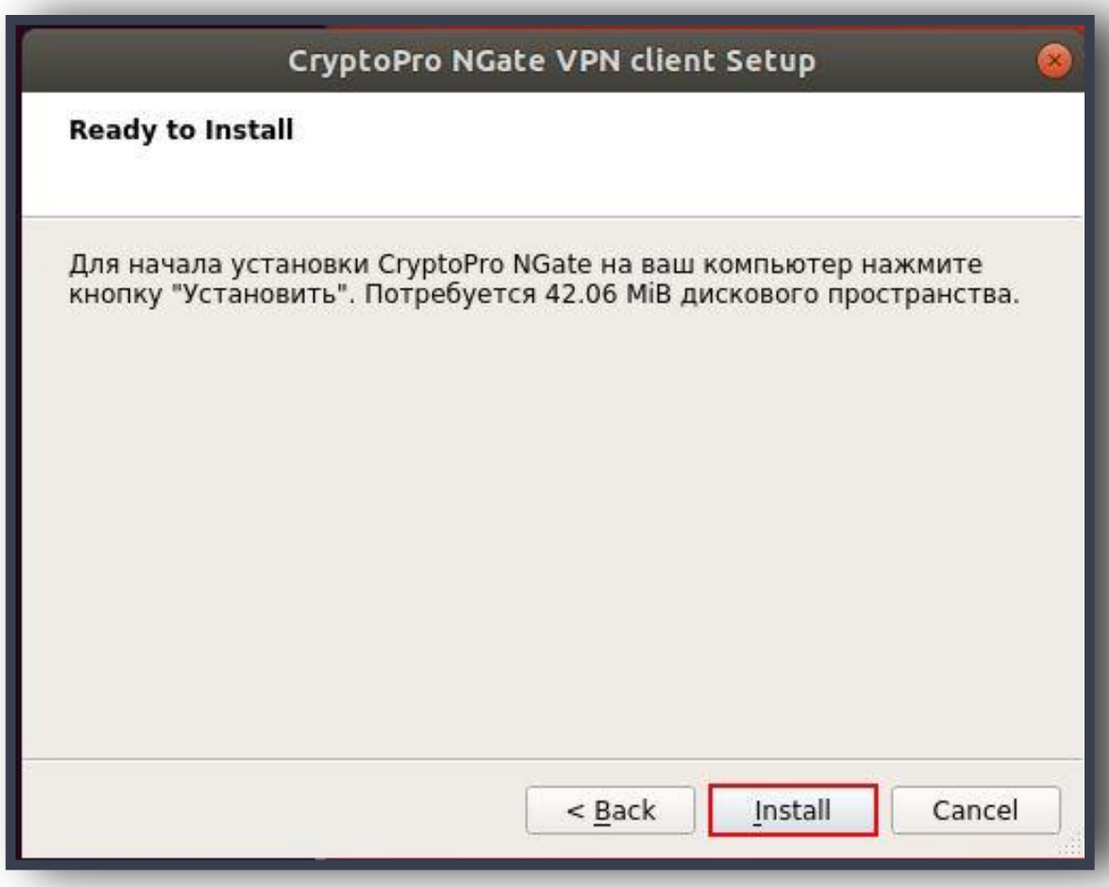
Присваивание свойства исполняемости и запуск установочного файла

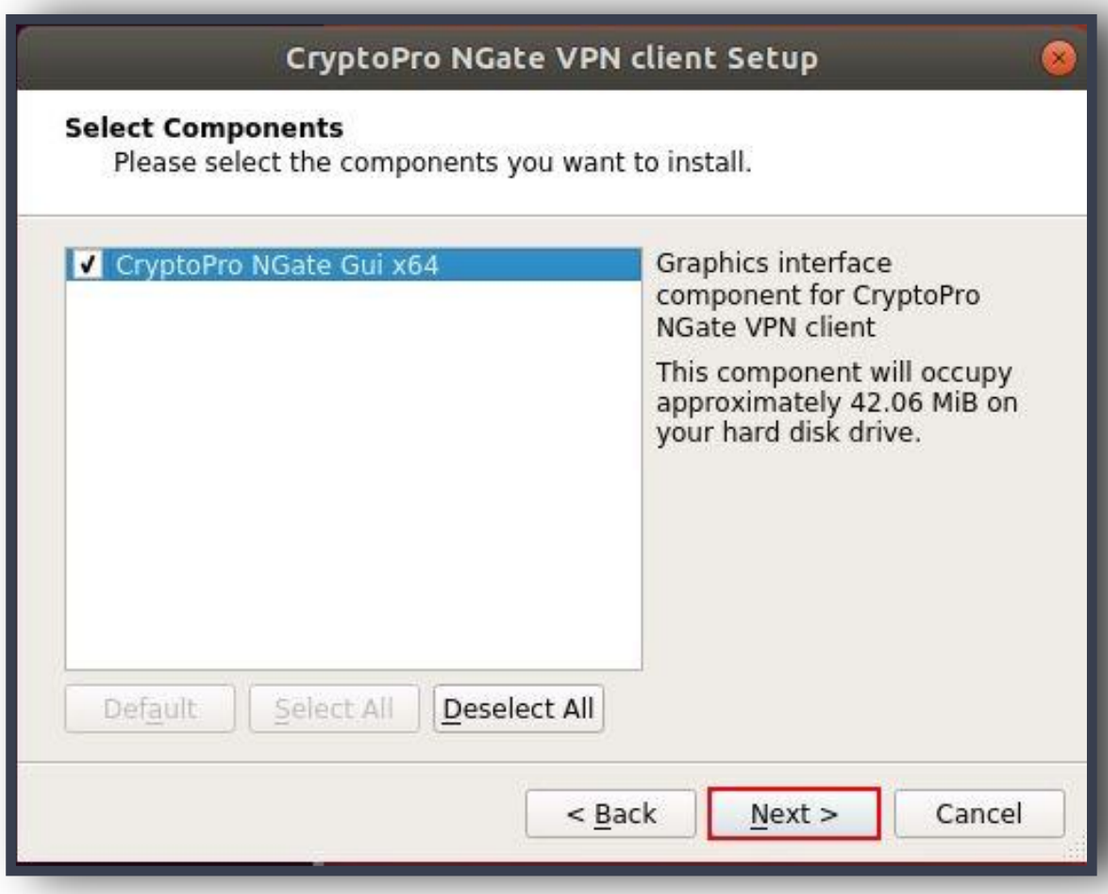
Далее следует перейти в папку с дистрибутивом ПО КриптоПро NGate Клиент, сделать его исполняемым и произвести запуск. Отобразиться окно приветствия мастера установки.

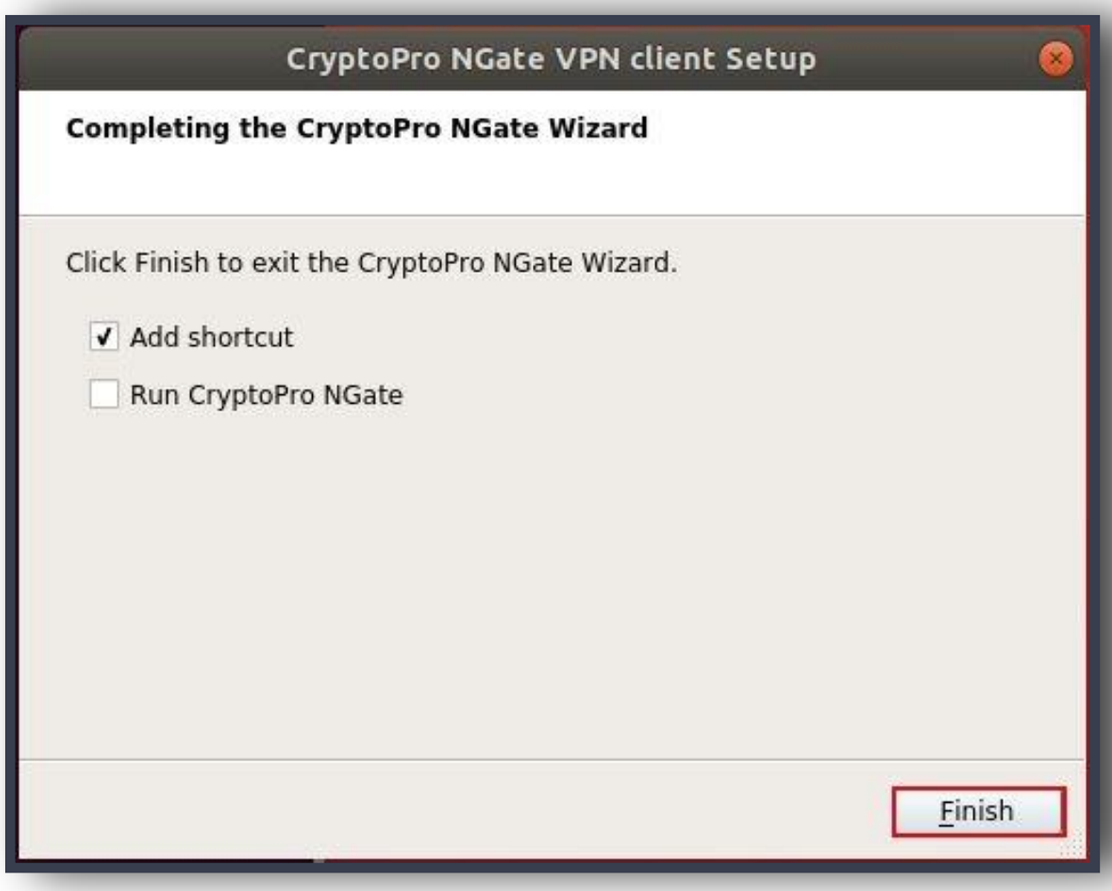


Начало процесса графического мастера установки







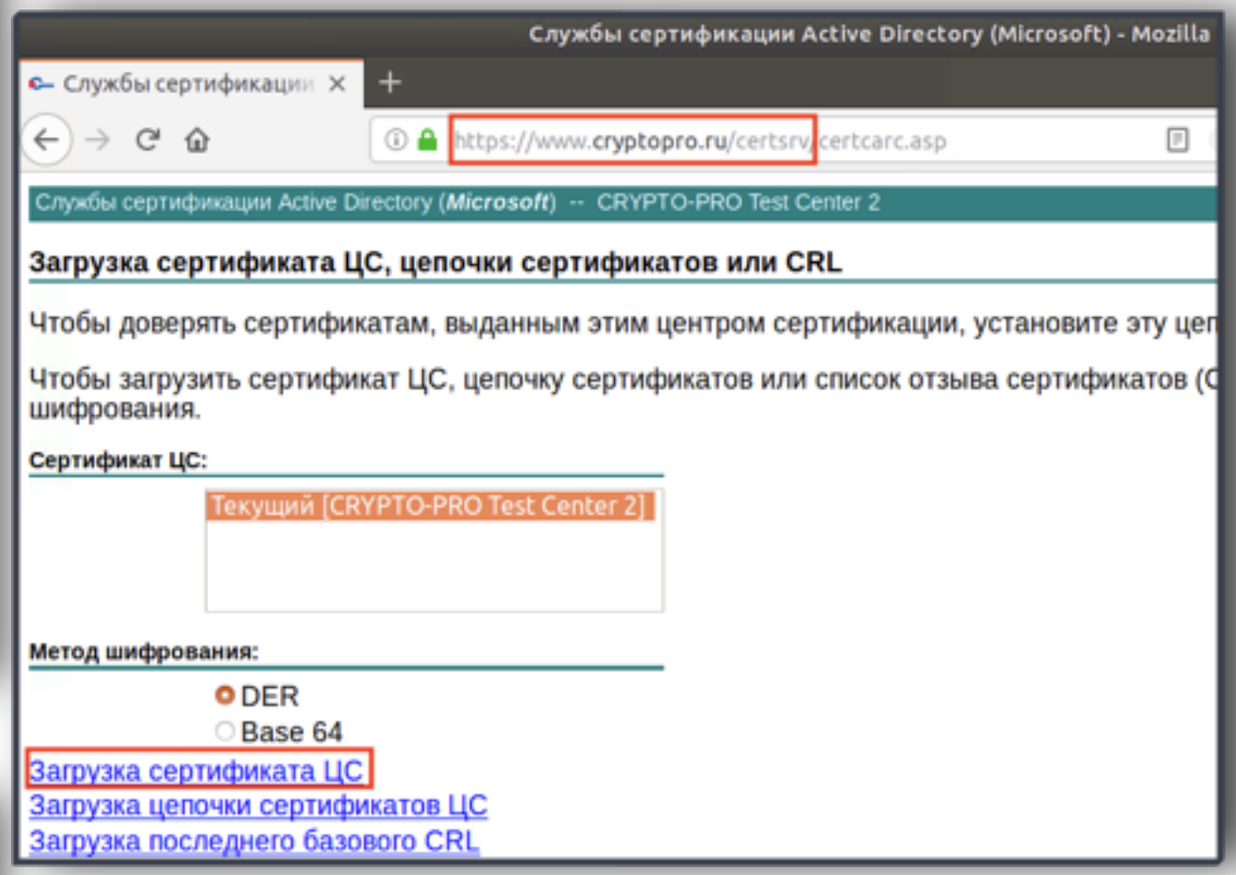


Последовательность шагов мастера установки КриптоПро NGate Клиент

Ярлык установленной программы в перечне доступного ПО Ubuntu

Главное окно программы

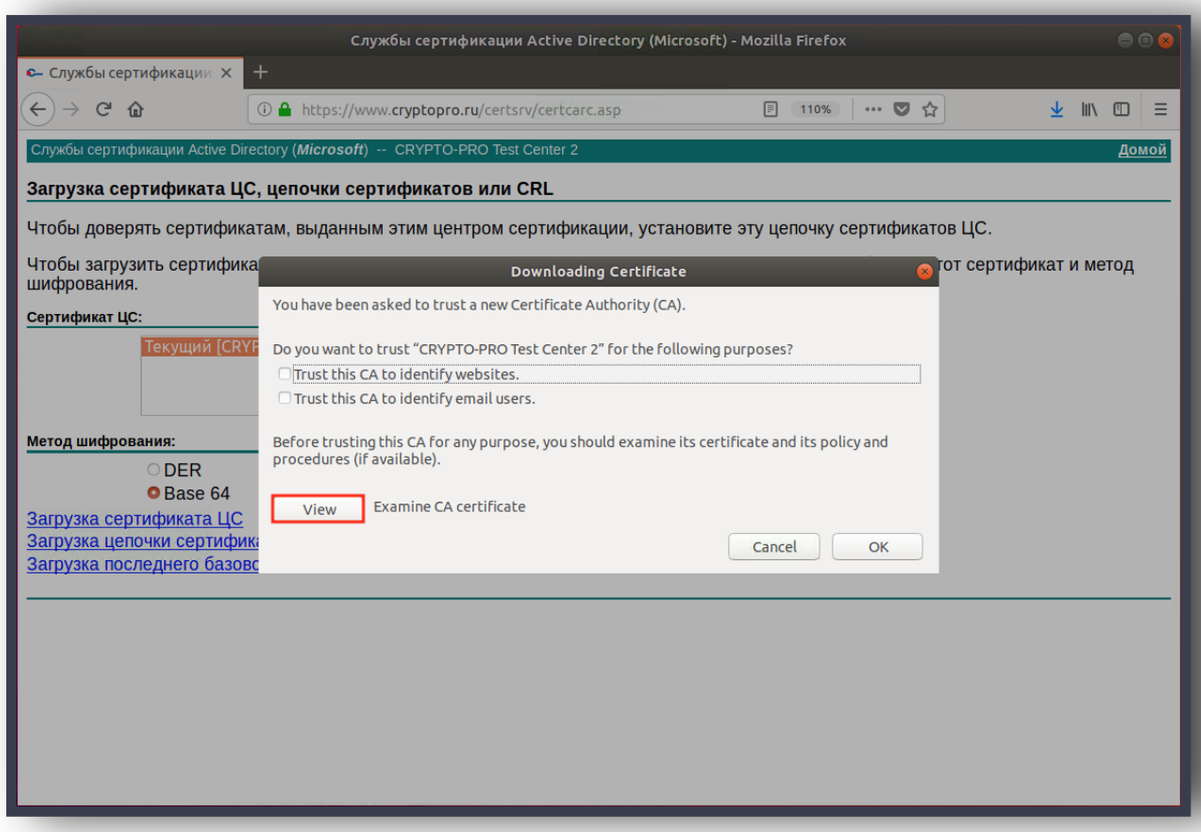
После успешного завершения установки, программа может быть запущена посредством ярлыка в перечне ПО Ubuntu.



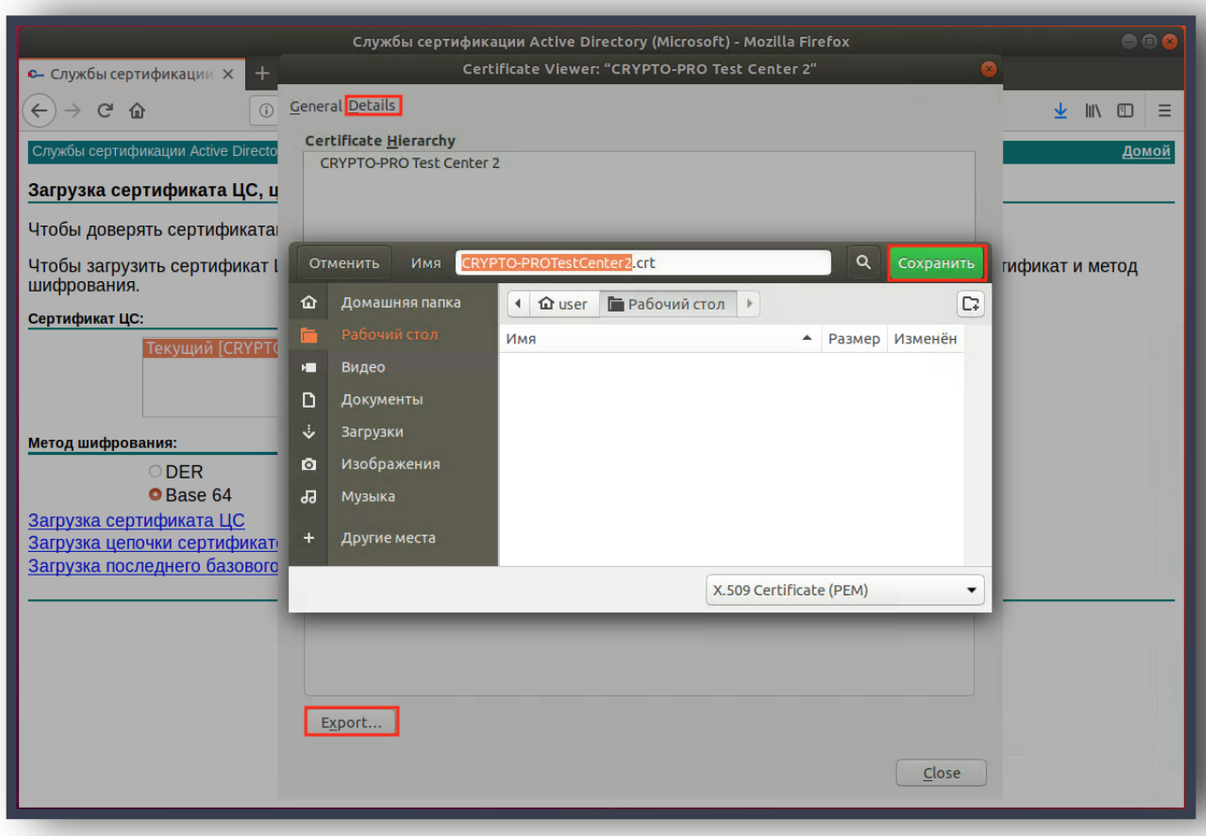
Загрузка корневого сертификата тестового УЦ КриптоПро

Клиентское ПО будет производить подключение к шлюзу. Для установления отношений доверия потребуется скачать и установить корневой сертификат удостоверяющего центра [УЦ], выпустившего серверный мандат данного шлюза. В нашем случае данным УЦ является один из тестовых центров КриптоПро.

При попытке скачать сертификат посредством браузера Firefox, будет предложено произвести сохранение в собственное хранилище сертификатов браузера. Нам же требуется получить сертификат в виде файла для его последующей установки средствами криптопровайдера, так что выполним процедуру экспорта.

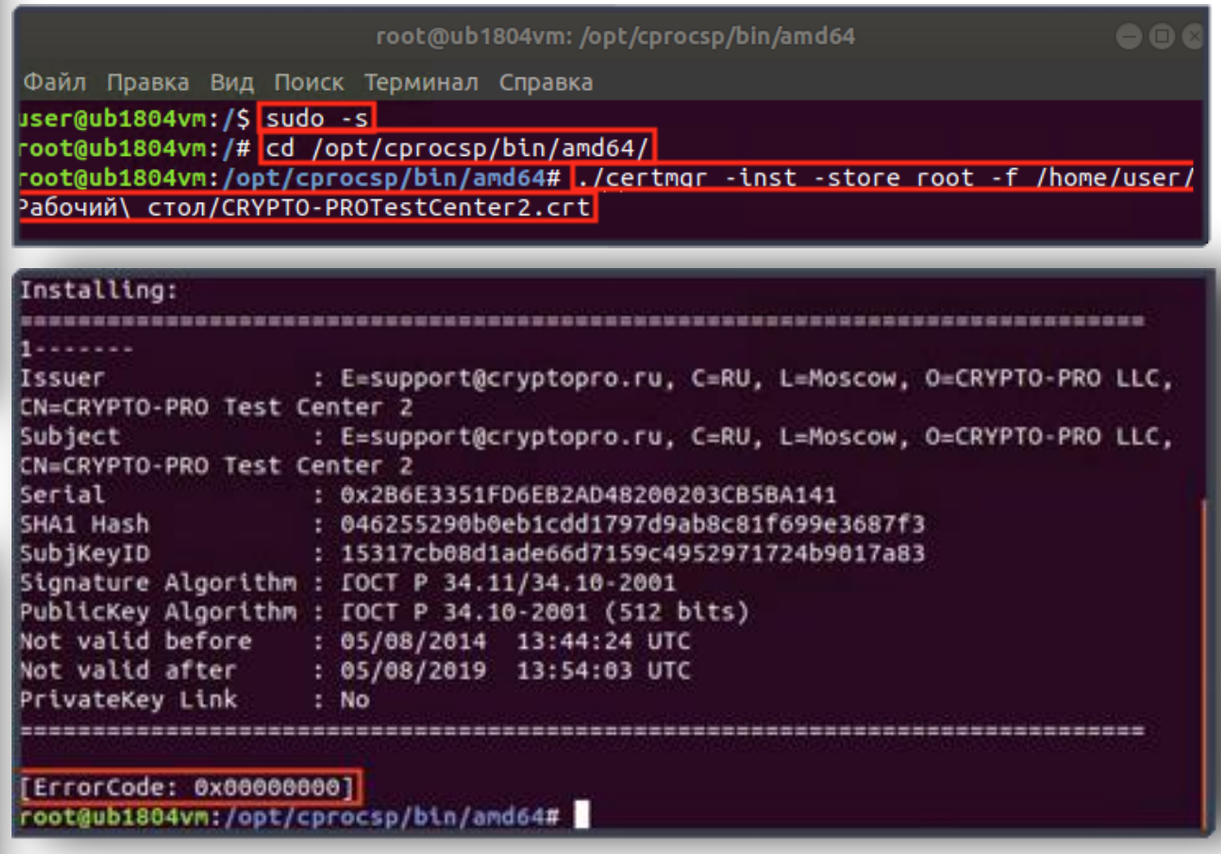


Диалоговое окно добавления сертификата в хранилище браузера



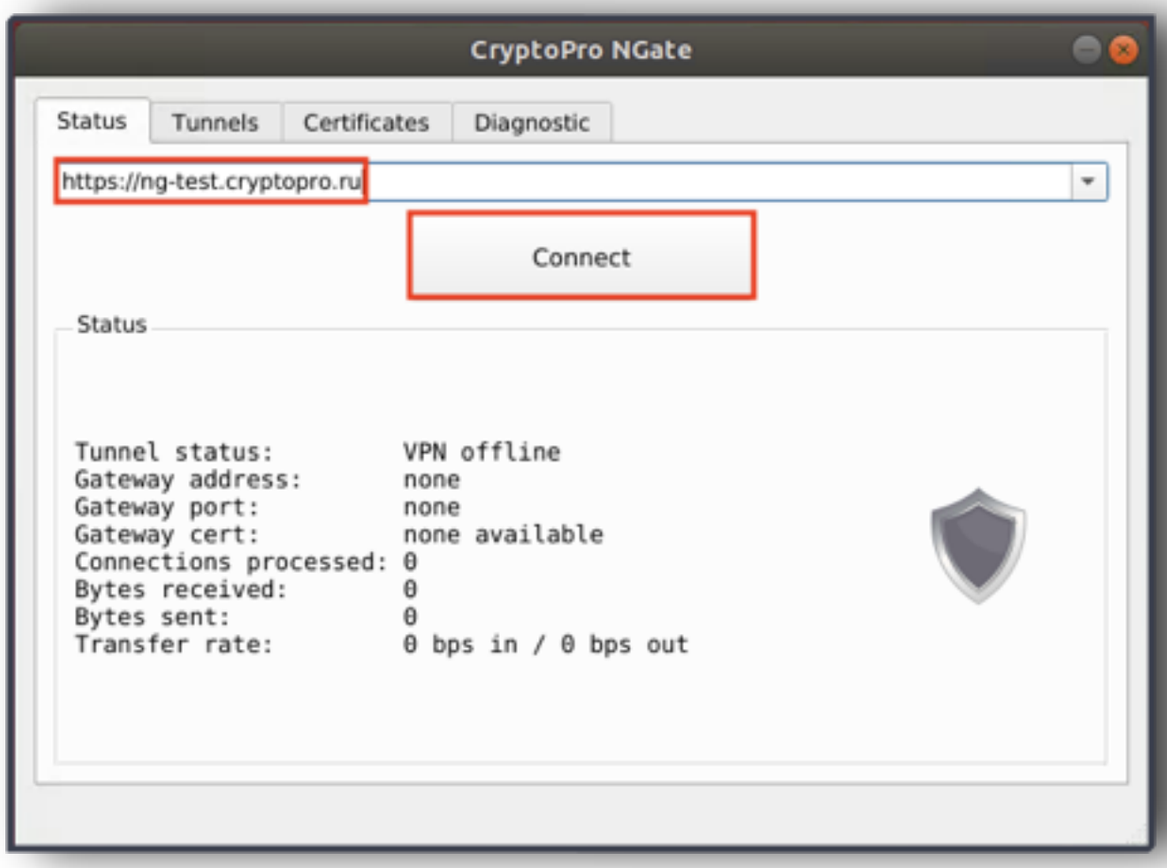
Процедура экспорта сертификата в файл

Для установки сертификата снова терминал и перейдем в папку с утилитами криптопровайдера. Затем выполним команду установки файла в хранилище доверенных корневых центров сертификации [root]. Понадобятся права суперпользователя.

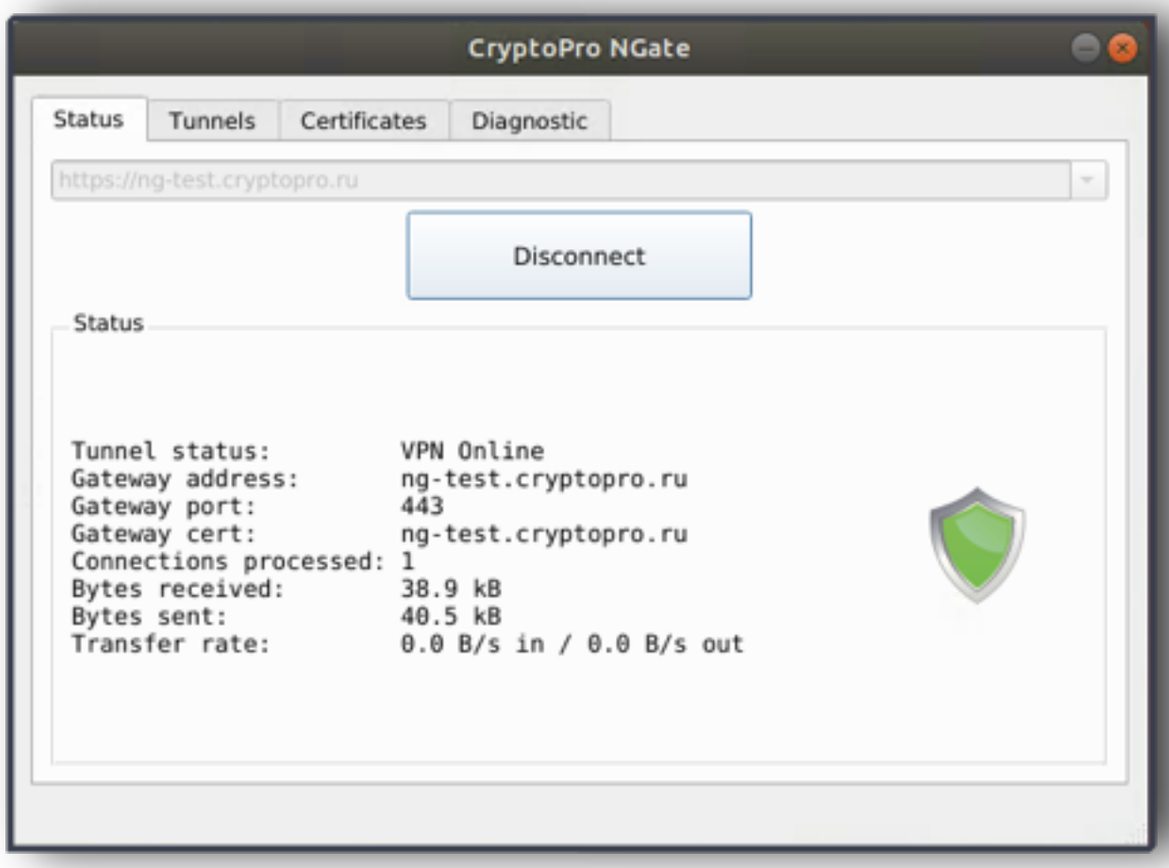


Установка сертификата в хранилище доверенных сертификатов

Установка сертификата успешно завершена и теперь, для проверки работоспособности, можно подключится к одному из тестовых шлюзов КриптоПро. Данный шлюз [https://ng-test.cryptopro.ru] реализует аутентификацию пользователей по логину/пароль [test/test]



Ввод адреса шлюза и попытка подключения



Подключение успешно установлено

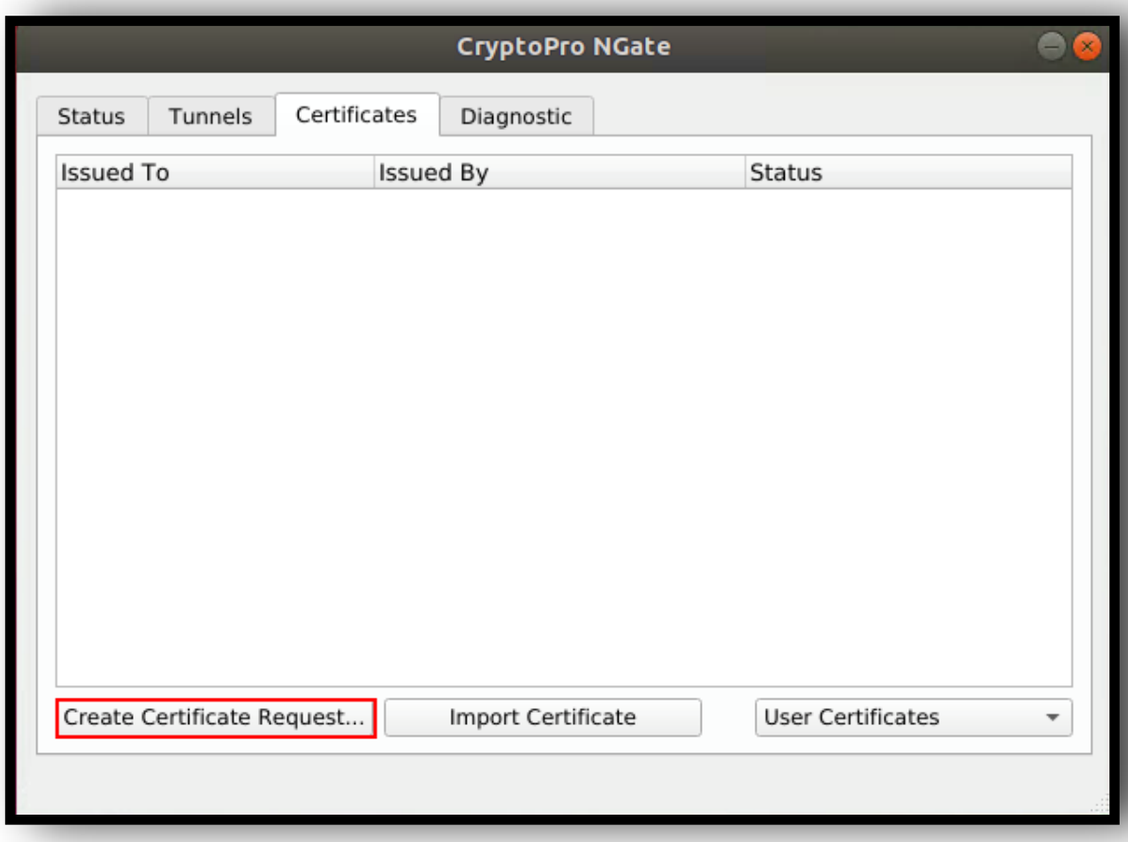
Запрос ввода логина/пароля.

Автоматическое открытие демо-странички ресурса из защищаемого сегмента сети

После успешной установки защищенного соединения автоматически откроется страничка демо-ресурса, находящегося в защищаемом сегменте сети, к которой производилось подключение.

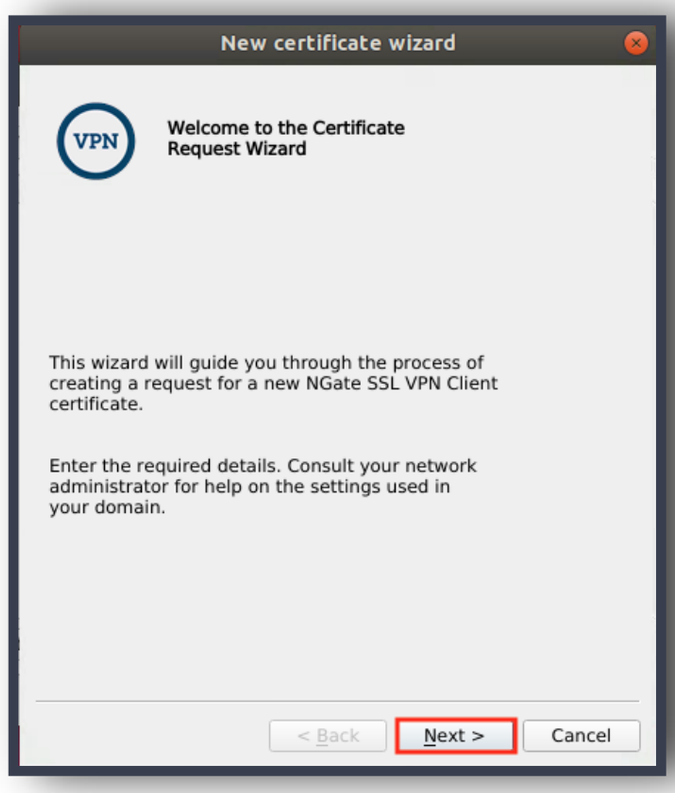
Теперь получим ключи и сертификат пользователя, для аутентификации на другом тестовом шлюзе [https://ng-test-cert.cryptopro.ru]. Данный шлюз аутентифицирует пользователей исключительно по сертификатам, выпущенным упомянутым ранее УЦ, и содержащим значение test в компонентах имени сертификата O/OU.

Запустим мастер генерации запроса на сертификат.

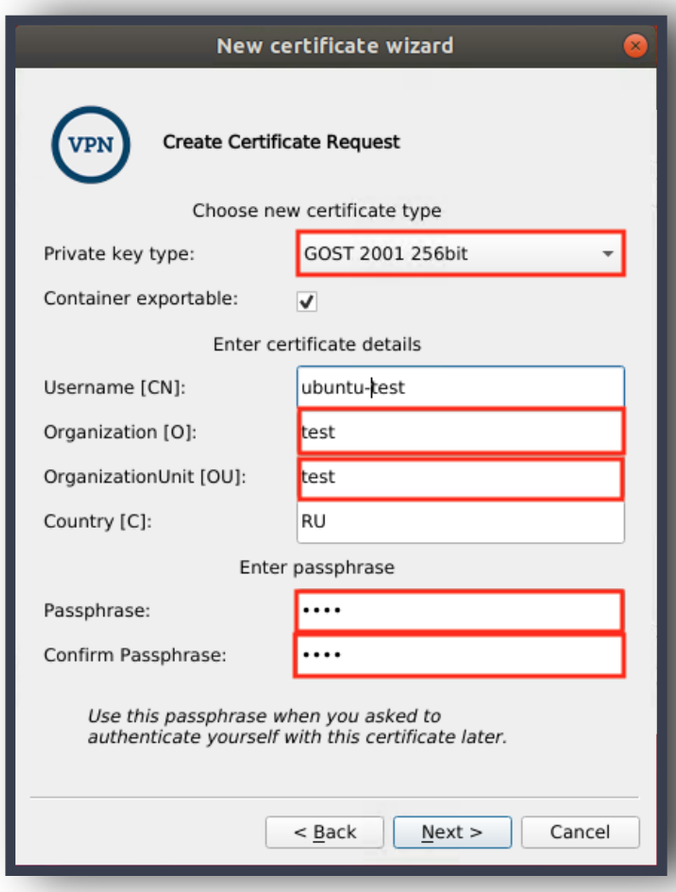


Инициализация мастера создания запроса на сертификат

Пройдя первое диалоговое окно мастера, в следующем, нужно указать значение алгоритма ключа на GOST 2001 256bit, Username [CN] можно задать произвольное. Поля Organsation [O] и OrganisationUnit [OU] должны обязательно иметь значения test. Страна – RU. Также потребуется задать т.н. passphrase - пароль для создаваемого контейнера с ключами. Жмём “Next”.

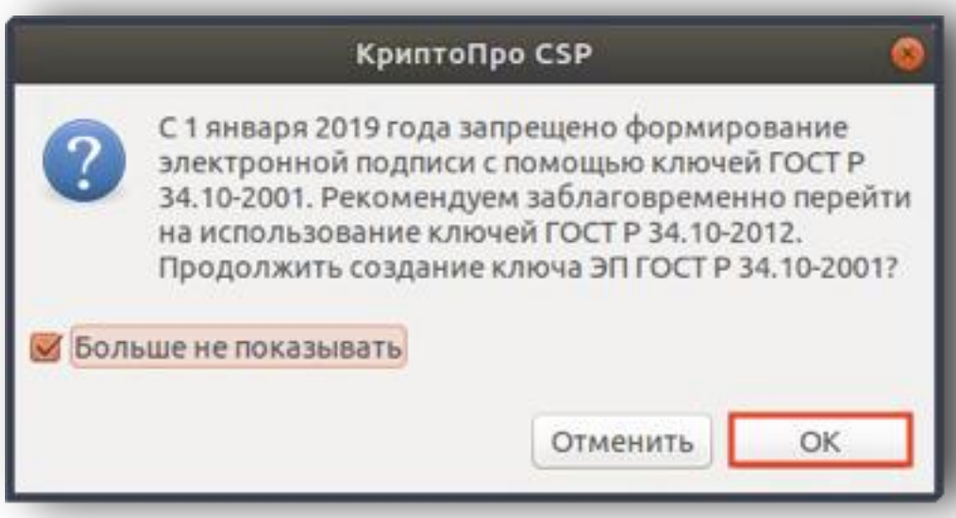


Диалоговое окно мастера создания запроса на сертификат



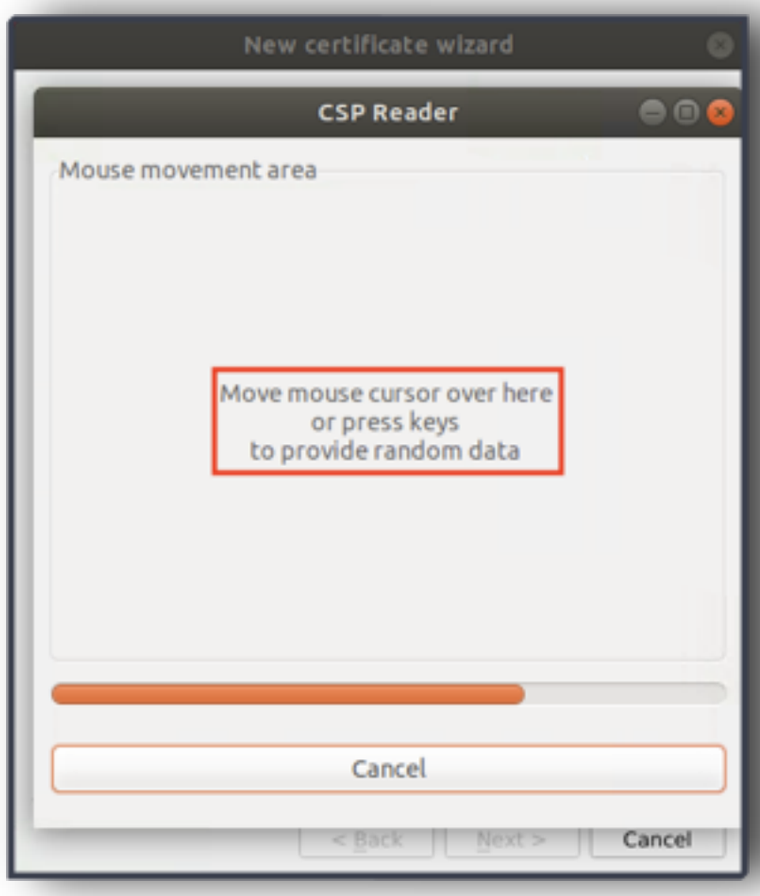
Окно ввода данных формируемого запроса

Может появиться уведомление. Соглашаемся.



Уведомление касаемо правового аспекта использования криптографических алгоритмов

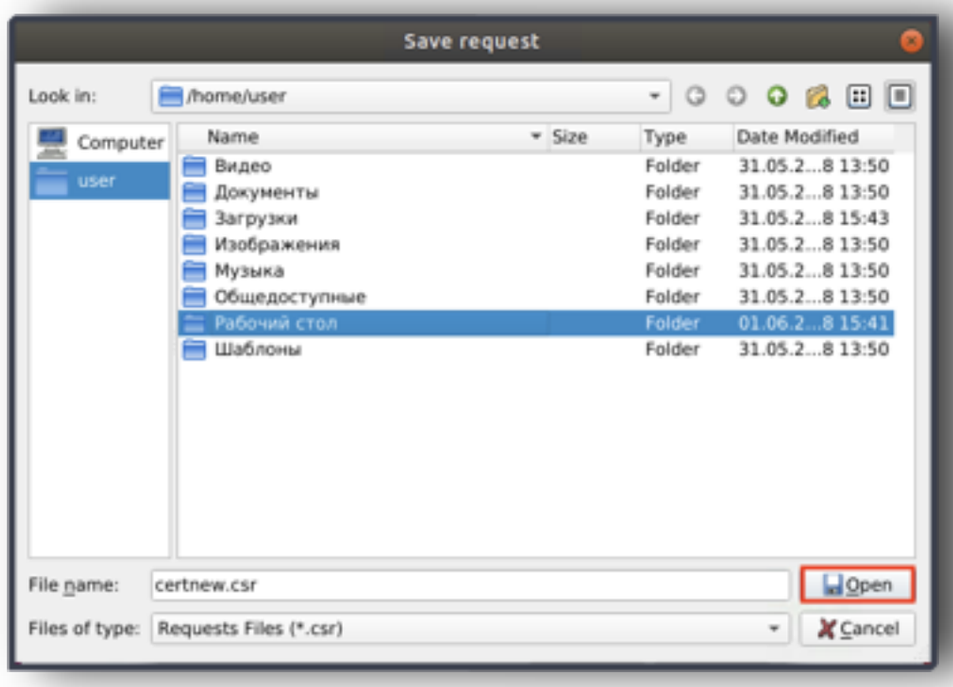
Далее запуститься окно датчика случайных чисел. Потребуется перемещать курсор мыши до окончания процесса формирования ключей.



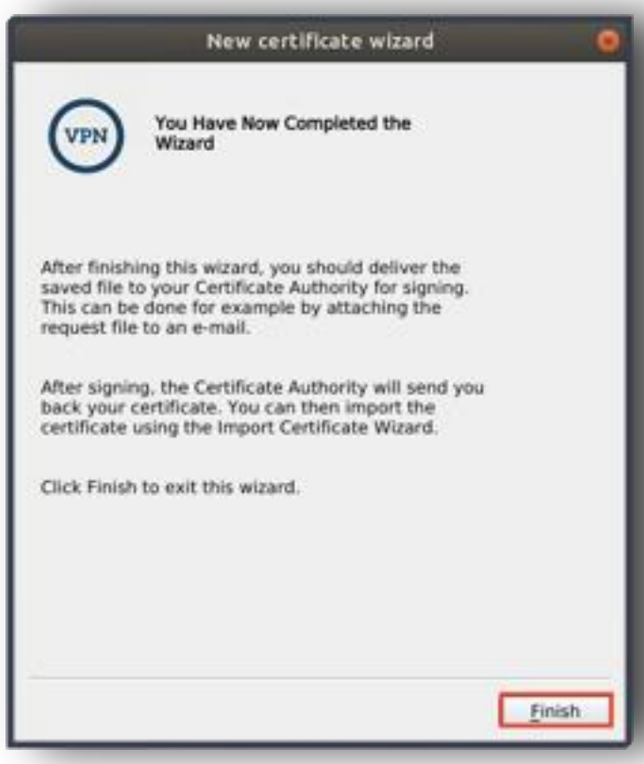
Окно работы БИО-датчика случайных чисел

Будет предложено произвести сохранение полученного запроса на сертификат в файл.

Диалоговое окно, предваряющее сохранение запроса на сертификат

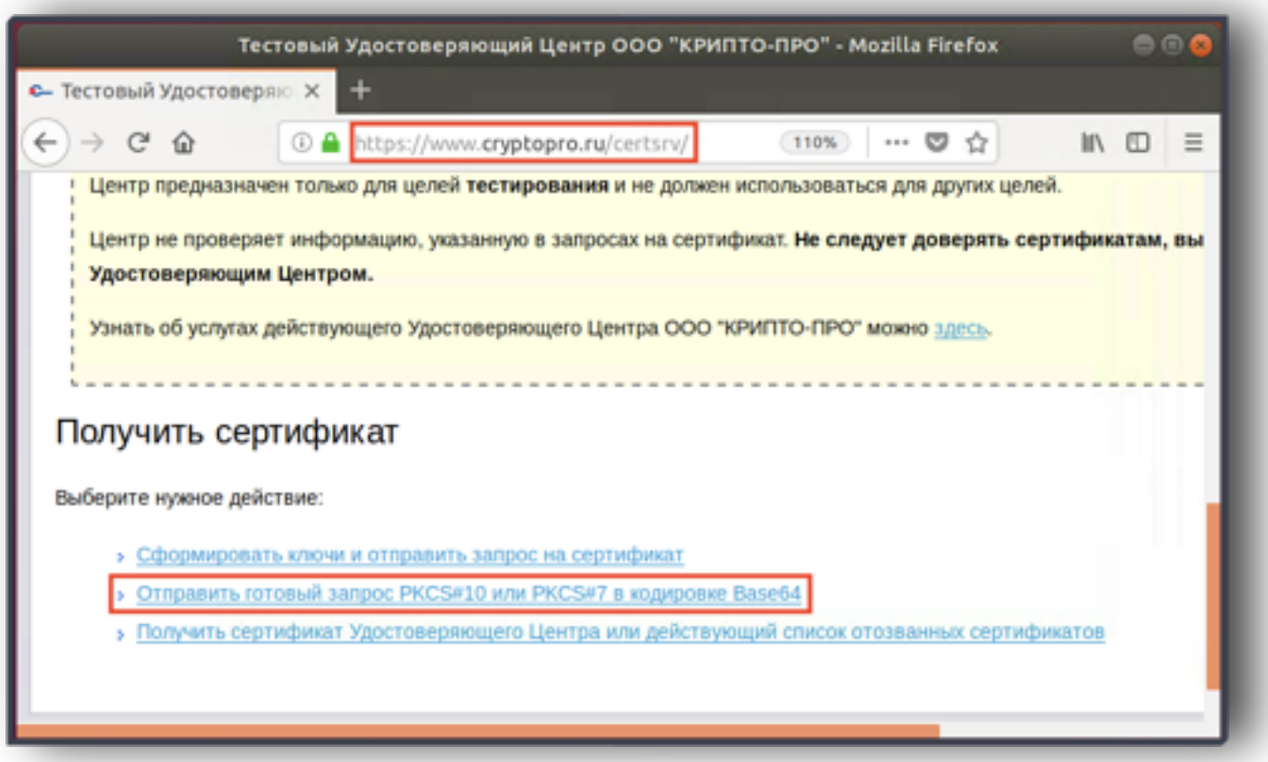


Окно сохранения запроса на сертификат

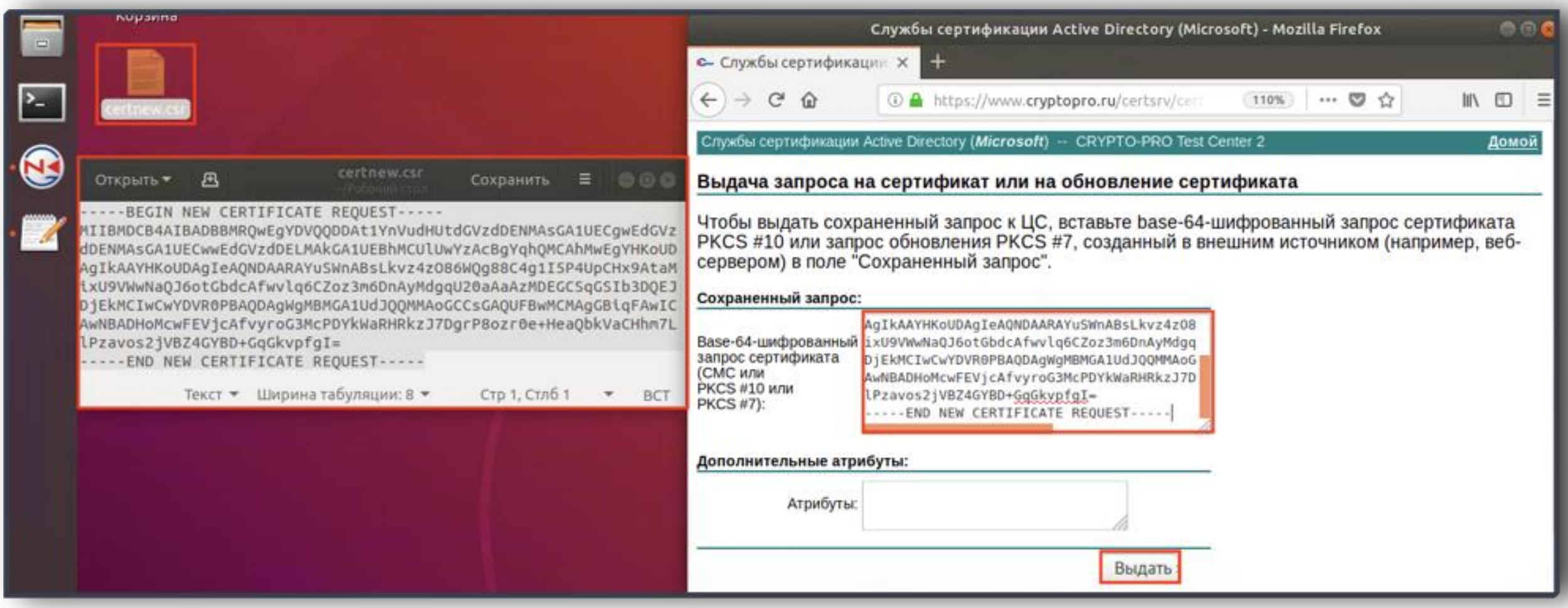


Работа мастера завершена и теперь нужно направить созданный запрос в УЦ для выпуска клиентского сертификата. Перейдем в соответствующий раздел веб-интерфейса УЦ. Затем откроем любым текстовым редактором файл запроса и скопируем содержимое в соответствующую форму. Далее “Выдать” .

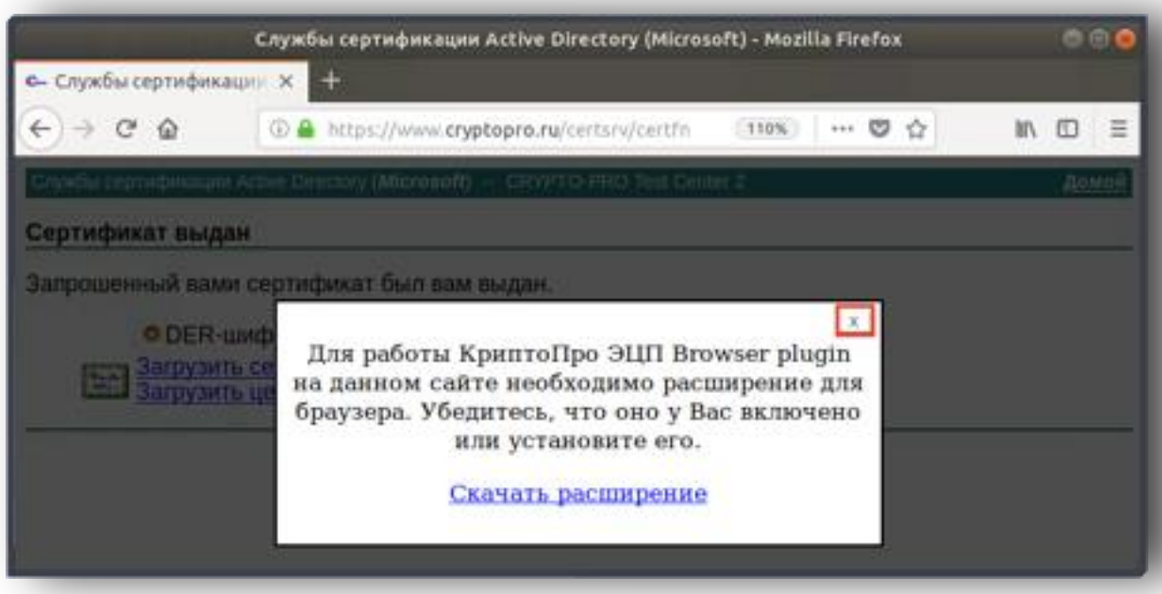
Завершение работы мастера



Выбор соответствующего пункта в окне веб-интерфеса тестового УЦ.

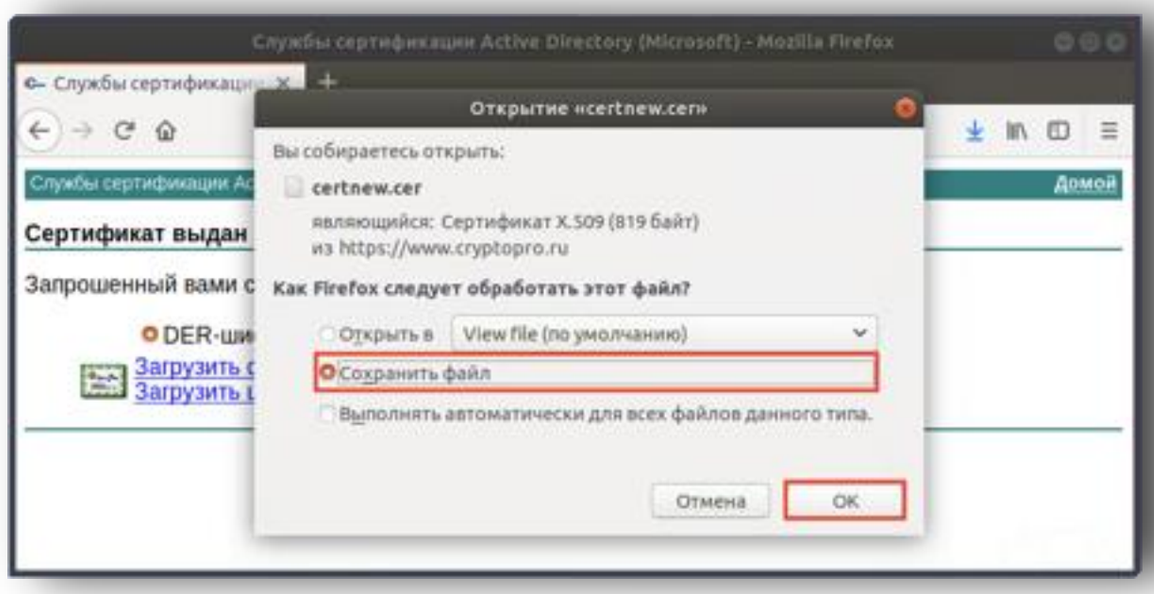


Импорт запроса из файла в соответсвующее поле окна веб-интерфеса тестового УЦ.



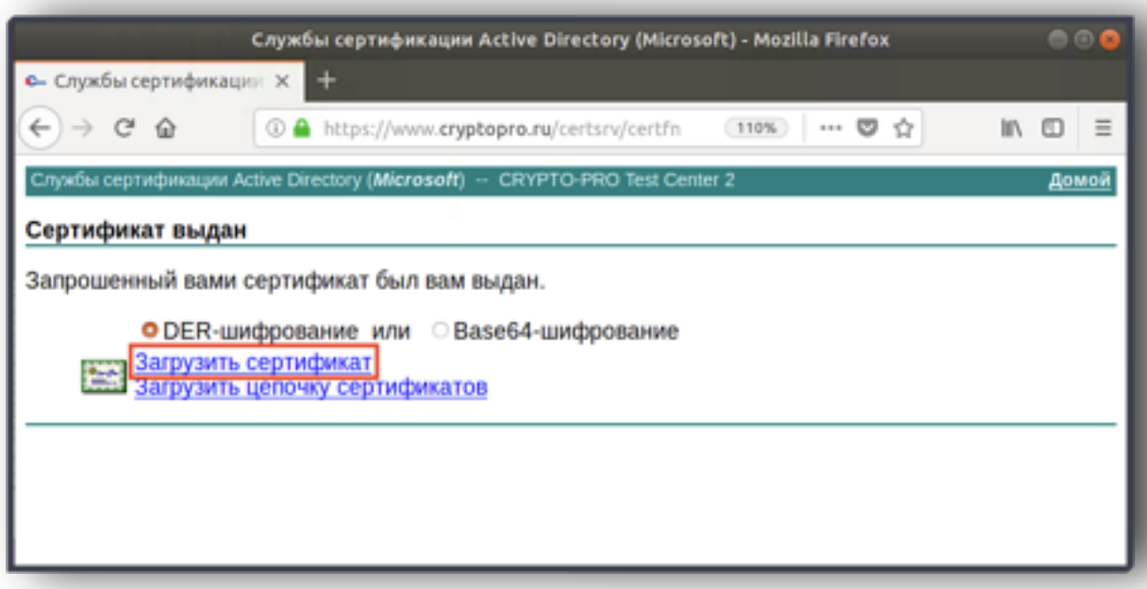
Уведомление

На возможные сообщения о необходимости использования расширения для браузера при работе с УЦ не обращаем внимания. Сохраняем полученный сертификат в файл.

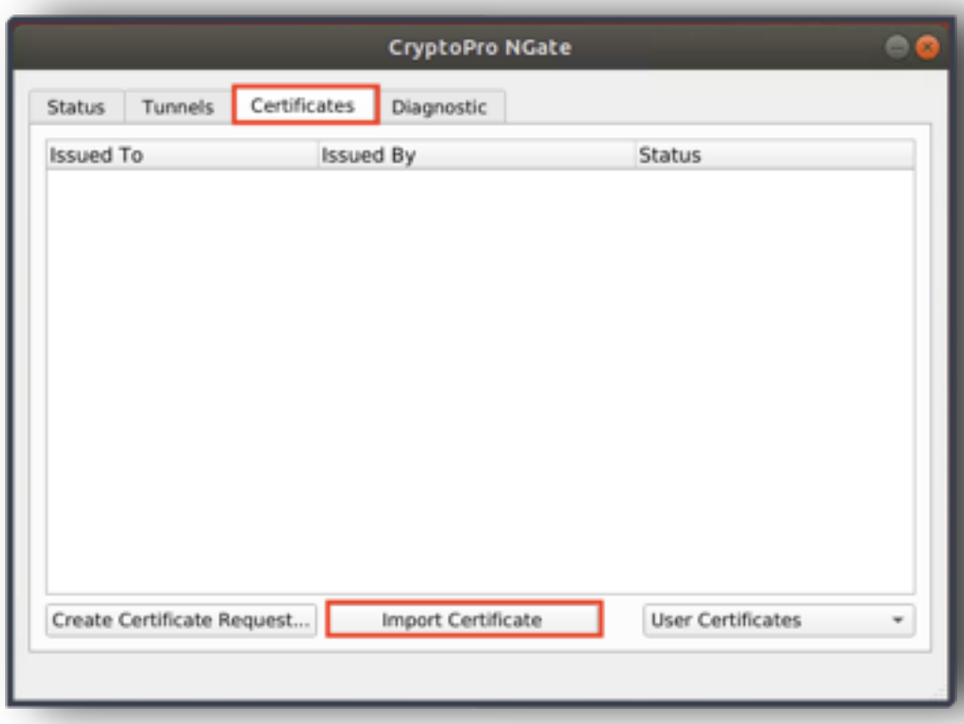


Диалоговое окно сохранение сертификата в файл

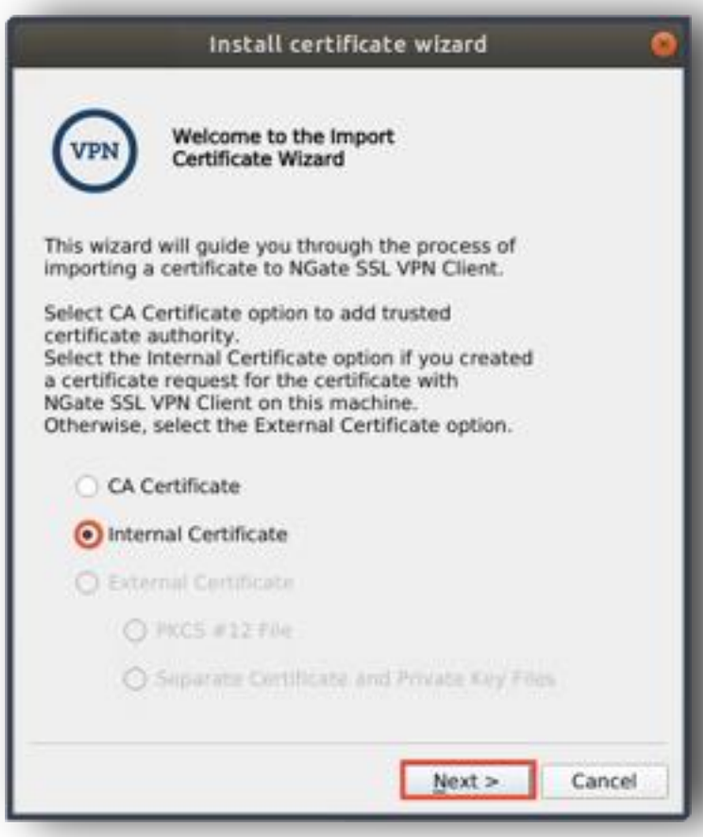
После успешного сохранения сертификата в файл его нужно импортировать в созданный ранее контейнер с ключами. Для этого снова потребуется запустить КриптоПро NGate Клиента и соответствующий мастер в нём.



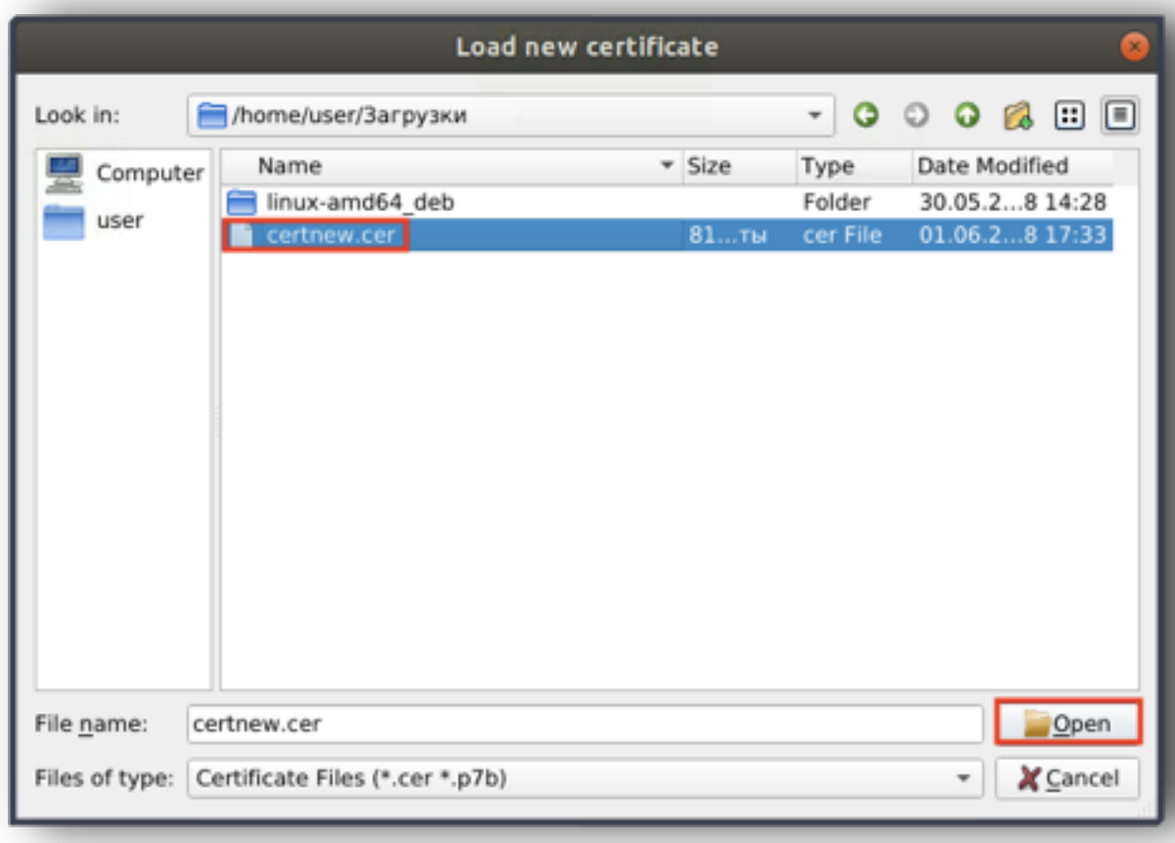
Выбор параметров сохранения свойств сертификата



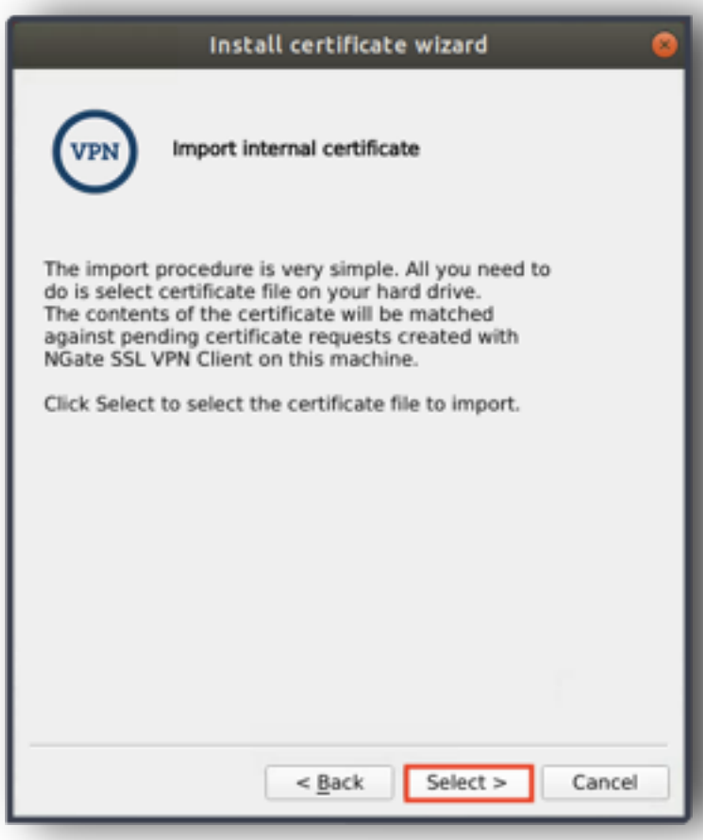
Запуск мастера импорта сертификата



Выбор опции импорта клиентского сертификата



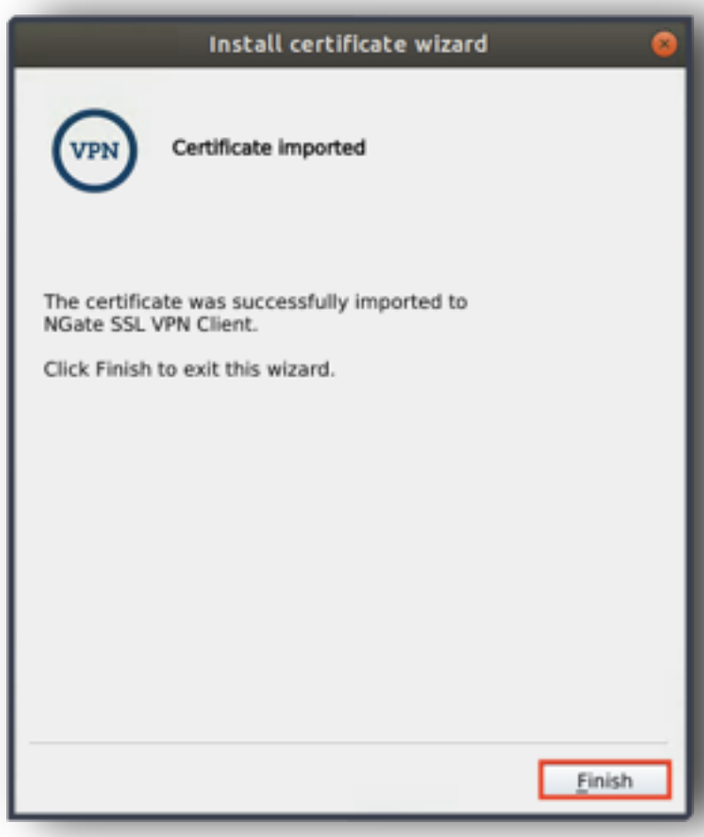
Диалоговое окно выбора файла сертификата



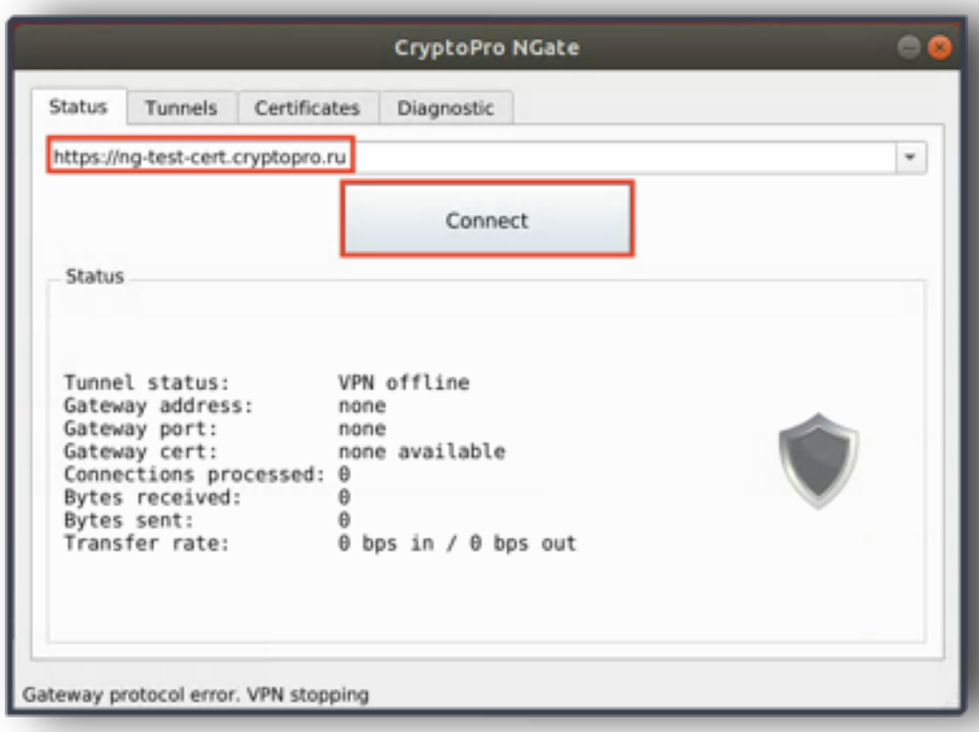
Диалоговое окно, предваряющее выбор сертификата

Следует выбрать и открыть файл сертификата, а затем ввести заданный ранее пароль на контейнер с ключами (passphrase)

Диалоговое окно ввода пароля для контейнера

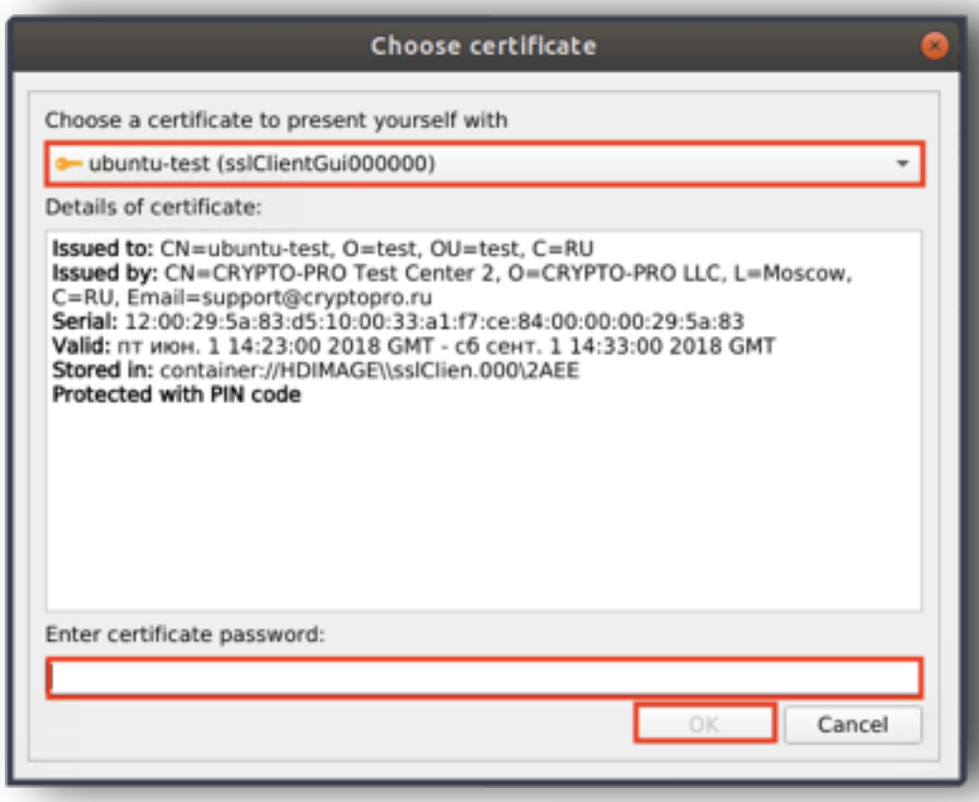


Завершение работы мастера



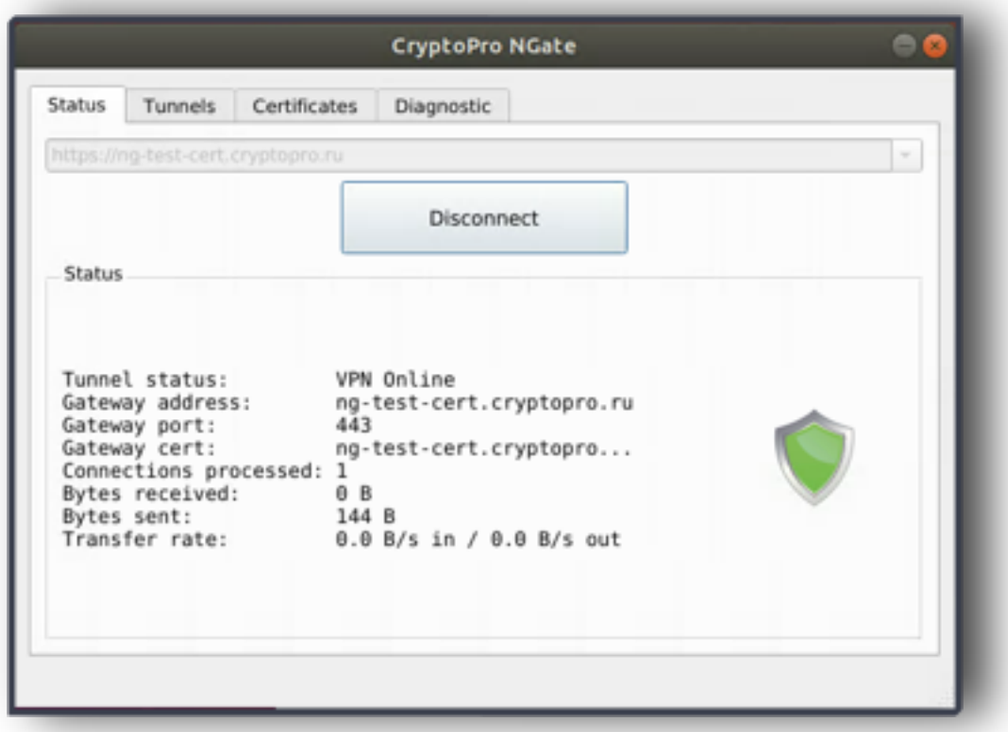
Указание корректного имени шлюза

Работа мастера импорта завершена и можно попробовать подключиться к тестовому шлюзу, указав корректное имя, и нажать “Connect”.



Выбор сертификата и ввод пароля на контейнер

В появившемся окне следует выбрать клиентский сертификат из перечня доступных (у нас он единственный) и ввести пароль (passphrase).



Окно клиентского ПО при успешном подключении к

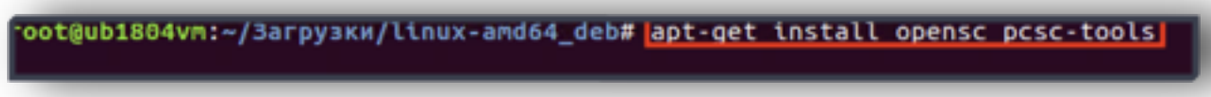
Тестовая страничка веб-сервера, развернутого на ресурсе в защищаемого сегменте сети открывается автоматически при установлении соединения.

При описанной выше процедуре генерации клиентского сертификата и ключей - контейнер создается на диске ПК. Для работы с контейнерами на защищенных ключевых носителях (токенах) потребуется произвести некоторые действия и установить требуемые пакеты. Полный перечень поддерживаемых носителей можно узнать из документации к КриптоПро CSP. В текущем примере будет продемонстрирован процесс настройки системы для работы с usb-ключевыми носителями ESMART token usb 64k и Рутокен ЭЦП. В общем случае потребуется установить пакеты для работы со смарткартами из системных репозитариев ОС, затем пакет для той же цели, но уже из архива криптопровайдера и далее - пакет с модулем поддержки для конкретного защищенного ключевого носителя.

ESMART token usb 64k

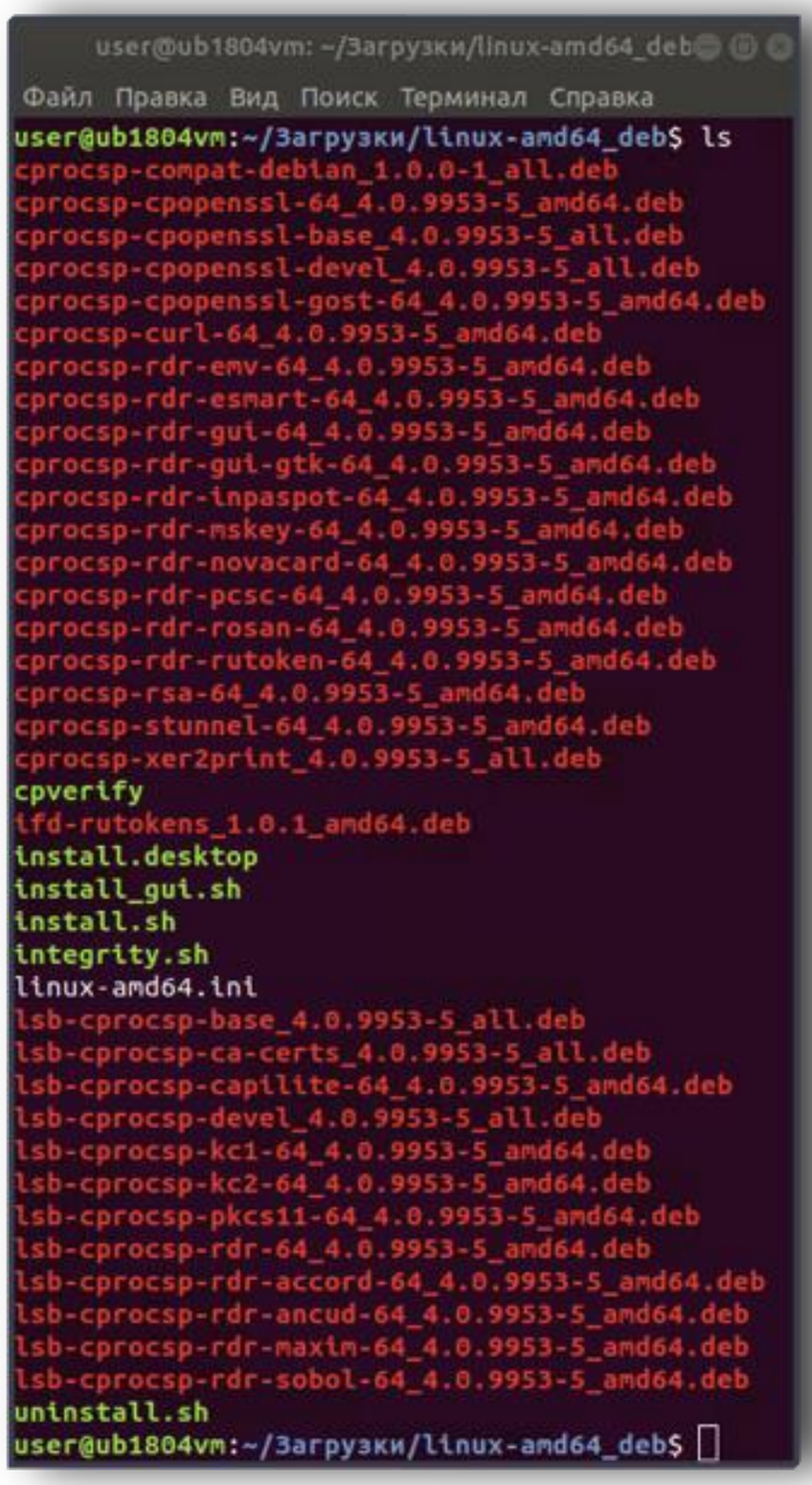
Рутокен ЭЦП

Итак, сперва следует установить недостающие пакеты из системных репозитариев ОС. Потребуются права суперпользователя.



Установка пакетов из репозитариев ОС

Далее потребуется зайти в папку с пакетами криптопровайдера, перечень которых отображен на скриншоте ниже.



Перечень пакетов архива криптопровайдера

Теперь произведем установку недостающего пакета для работы со смарткартами из состава криптопровайдера.

```
root@ub1804vm:~/Загрузки/linux-amd64_deb# dpkg -i cprocsp-rdr-pcsc-64_4.0.9953-5_amd64.deb
```

Установка требуемого пакета для работы со смарткартами из состава криптопровайдера.

Далее будет произведена установка модуля поддержки Рутокен ЭЦП.

```
root@ub1804vm:~/Загрузки/linux-amd64_deb# dpkg -i cprocsp-rdr-rutoken-64_4.0.9953-5_amd64.
deb
Выбор ранее не выбранного пакета cprocsp-rdr-rutoken-64.
(Чтение базы данных … на данный момент установлено 151127 файлов и каталогов.)
Подготовка к распаковке cprocsp-rdr-rutoken-64_4.0.9953-5_amd64.deb …
Распаковывается cprocsp-rdr-rutoken-64 (4.0.9953-5) …
Настраивается пакет cprocsp-rdr-rutoken-64 (4.0.9953-5) …
root@ub1804vm:~/Загрузки/linux-amd64_deb#
```

Установка требуемого пакета для работы с носителем Рутокен из состава криптопровайдера.

Убедиться в корректности произведенной настройки можно, к примеру, произведя опрос контейнеров на всех доступных в системе считывателях посредством утилиты csptest из состава КриптоПро CSP. Следует перейти в папку с утилитами КриптоПро CSP и запустить утилиту с соответствующими параметрами (скриншот). В выводе видно наличие двух контейнеров с ключами на защищенном носителе Рутокен ЭЦП.

```
root@ub1804vm:~/Загрузки/linux-amd64_deb# cd /opt/cprocsp/bin/amd64/
root@ub1804vm:/opt/cprocsp/bin/amd64# ./csptest -keys -enum_c -verifyc -fqcn
CSP (Type:80) v4.0.9018 KC1 Release Ver:4.0.9953 OS:Linux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 24568627
\\.\Aktiv Rutoken ECP (123456 600 600 600) 00 00\vpn
\\.\Aktiv Rutoken ECP (123456 600 600 600) 00 00\qnew
OK.
Total: SYS: 0,080 sec USR: 0,060 sec UTC: 1,500 sec
[ErrorCode: 0x00000000]
root@ub1804vm:/opt/cprocsp/bin/amd64#
```

Проверка возможности работы с Рутокен ЭЦП средствами КриптоПро CSP

```
dpkg -i cprocsp-rdr-esmart-64_4.0.9953-5_amd64.deb
```

Установка требуемого пакета для работы с носителем ESMART из состава криптопровайдера.

Далее установим модуль поддержки для ESMART из архива криптопровайдера. Затем снова произведем опрос контейнеров утилитой csptest из состава КриптоПро CSP. На этот раз вывод показал, в дополнение к уже имеющимся на Рутокен, наличие еще пяти контейнеров, которые расположены на защищенном носителе ESMART.

```
root@ub1804vm:/opt/cprocsp/bin/amd64# ./csptest -keys
 -enum_c -verifyc -fqcn
CSP (Type:80) v4.0.9018 KC1 Release Ver:4.0.9953 OS:L
inux CPU:AMD64 FastCode:READY:AVX.
AcquireContext: OK. HCRYPTPROV: 28164915
\\.\ACS Token - CP 01 00\test915
\\.\ACS Token - CP 01 00\testb
\\.\ACS Token - CP 01 00\testy1
\\.\ACS Token - CP 01 00\test53
\\.\ACS Token - CP 01 00\123456
\\.\Aktiv Rutoken ECP (123456 600 600 600) 00 00\vpn
\\.\Aktiv Rutoken ECP (123456 600 600 600) 00 00\qnew
OK.
Total: SYS: 0,070 sec USR: 0,110 sec UTC: 4,340 sec
[ErrorCode: 0x00000000]
root@ub1804vm:/opt/cprocsp/bin/amd64#
```

Проверка возможности работы с Рутокен ЭЦП ESMART token usb 64k средствами КриптоПро CSP

Настройка произведена успешно и теперь данные токены можно использовать при работе с КриптоПро NGate Клиентом.