# Работа с КриптоПро ЭЦП Browser plug-in и КриптоПро CSP в среде macOS Sierra

В данном документе будет пошагово описан процесс подготовки к работе и функционирования СКЗИ КриптоПро CSP совместно с КриптоПро ЭЦП Browser plug-in в среде macOS Sierra (10.12.2) + браузер Safari.

ВАЖНО!

На момент написания данного руководства, какая-либо стандартизация в требованиях электронных площадок (госуслуги, налог, сбербанк АСТ и тд) к клиентскому программному обеспечению фактически отсутствует. Это означает, что в каждом конкретном случае нужно выяснять, поддерживается ли операционная система данной площадкой в принципе, какой браузер предпочтителен, какой криптопровайдер и какое расширение для реализации подписи в браузере требуется. По опыту – если в требованиях к клиентскому программному обеспечению имеется СКЗИ КриптоПро CSP и КриптоПро ЭЦП Browser plug-in (вне зависимости от ОС и браузера) возможность работы на macOS\linux существует. Необходимо также упомянуть, что на некоторых порталах для авторизации\подписи может использоваться несколько расширений (криптокомпонентов) разных разработчиков, и далеко не все из них (расширений) существуют для платформ, отличных от Windows. Т.е. к примеру, произведя авторизацию по личному сертификату посредством КриптоПро ЭЦП Browser plug-in, в момент подписания некоего документа на портале может обнаружиться необходимость дополнительного ПО (криптокомпонента), установка которого на macOS невозможна. Изучать требования порталов следует крайне тщательно.

КриптоПро ЭЦП Browser plug-in бесплатен, а СКЗИ КриптоПро CSP имеет пробный 90-дневный период, в который ПО является полностью функциональным и ни каких ограничений не накладывается. Решение о покупке продукта можно принять, предварительно прояснив работоспособность того или иного предполагаемого сценария использования.

## Замечания

Из замечаний (актуальных на момент публикации), возникших при анализе обращений пользователей, следует перечислить следующие:

- Следует использовать **исключительно** “связку” КриптоПро CSP 4.0 с КриптоПро ЭЦП Browser plug-in 2.0
- В КриптоПро CSP 4.0 для macOS **отсутствует поддержка** ключевых носителей **etoken/jacarta**
- В сборках КриптоПро CSP 4.0 до 9842 включительно присутствует **проблема работы с контейнерами, в названии которых присутствуют кириллические символы.** Обходным вариантом может быть копирование контейнера средствами КриптоПро CSP на Windows-ПК с присвоением копии имени, состоящего из латиницы.
- При подготовке к работе ключевого носителя **Рутокен S** следует установить соответствующее ПО производителя, а затем обязательно перезагрузить компьютер.

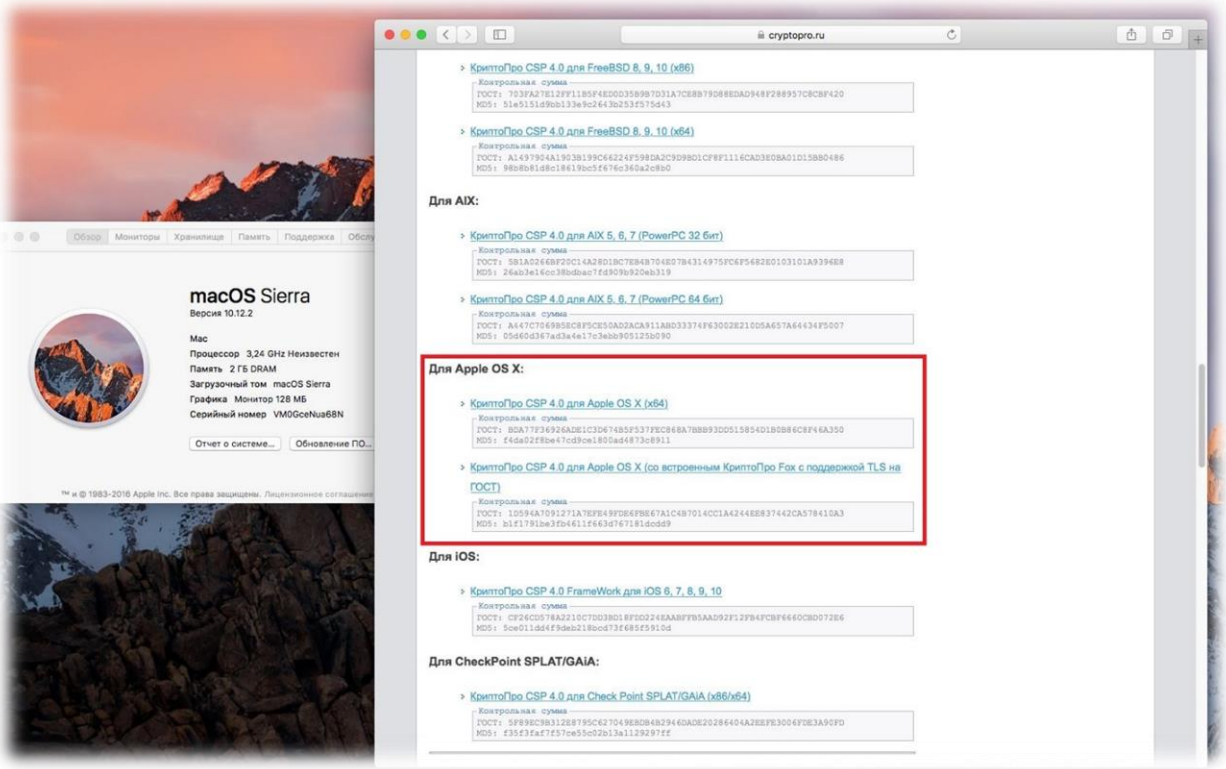
# Установка ПО

Для работы с личной подписью в общем случае потребуется выполнение следующих действий:

- Скачивание и установка СКЗИ КриптоПро CSP 4.0
- Скачивание и установка КриптоПро ЭЦП Browser plug-in 2.0
- Установка расширения в chrome-подобных браузерах из магазина расширений
- Подключение ключевого носителя к компьютеру и установка личного сертификата
- Скачивание и установка в соответствующие хранилища корневых и промежуточных сертификатов удостоверяющего центра, где была получена подпись.
- Добавление адреса электронной площадки в локальный перечень доверенных сайтов.

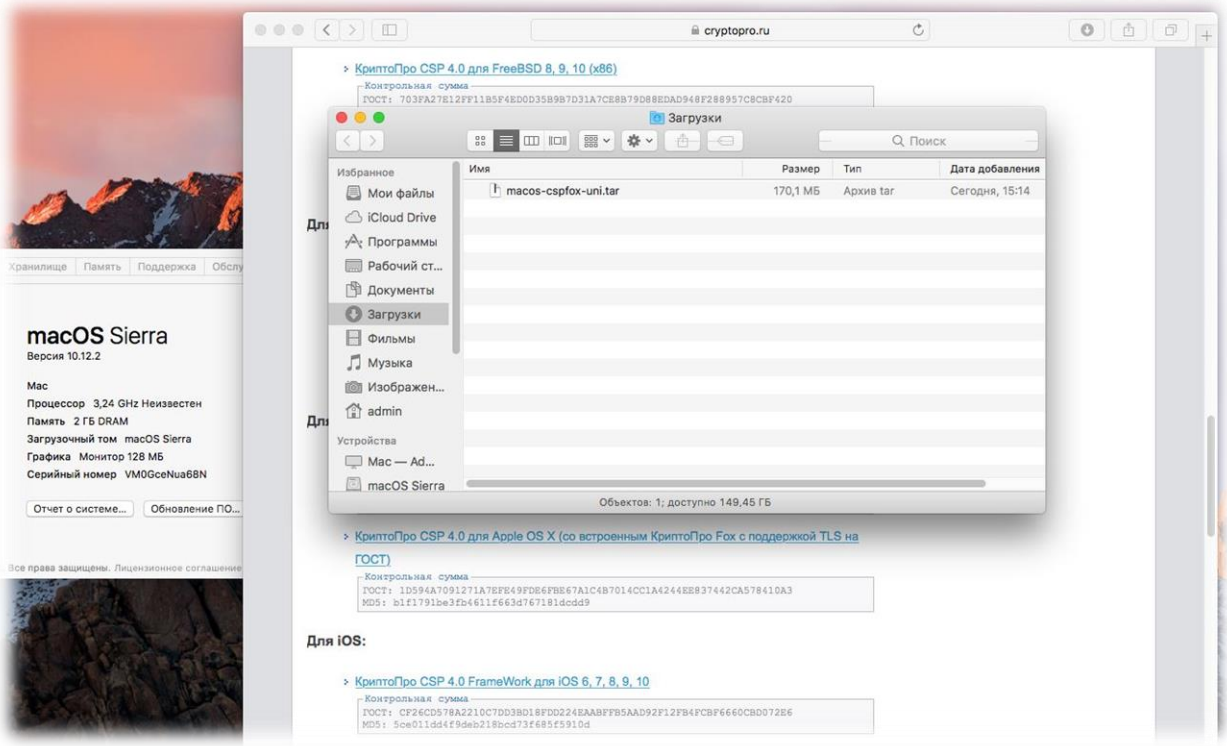
# Скачивание и установка СКЗИ КриптоПро CSP

Дистрибутив криптопровайдера доступен для скачивания после свободной регистрации на сайте.

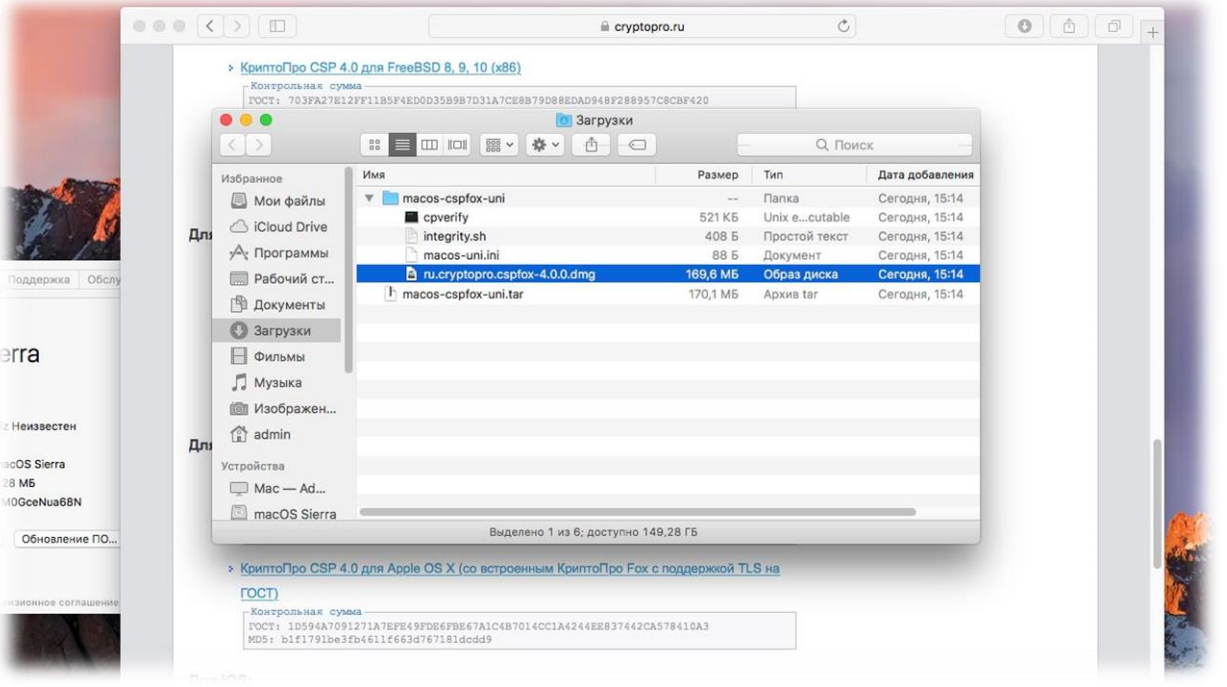



Желательно скачивать архив, содержащий браузер КриптоПро Fox, который позволит работать на площадках, требующих организации соединения, защищенного по ГОСТ. К примеру nalog.ru. Подробнее можно ознакомиться здесь.

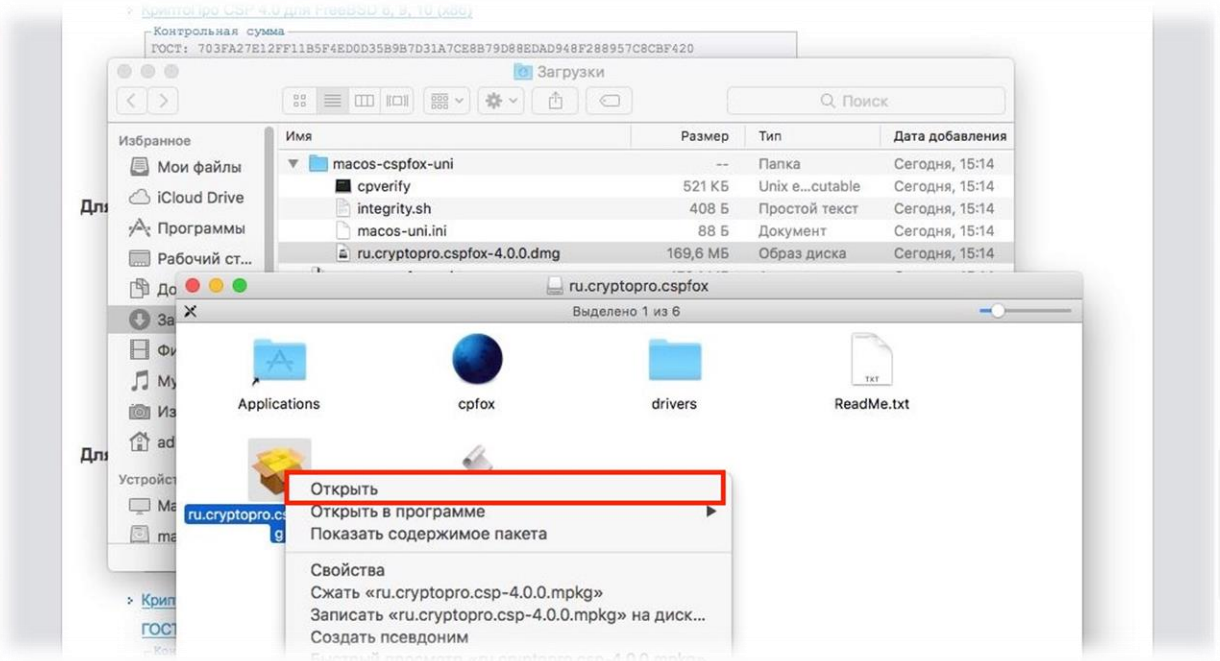
Распакуйте скачанный архив.



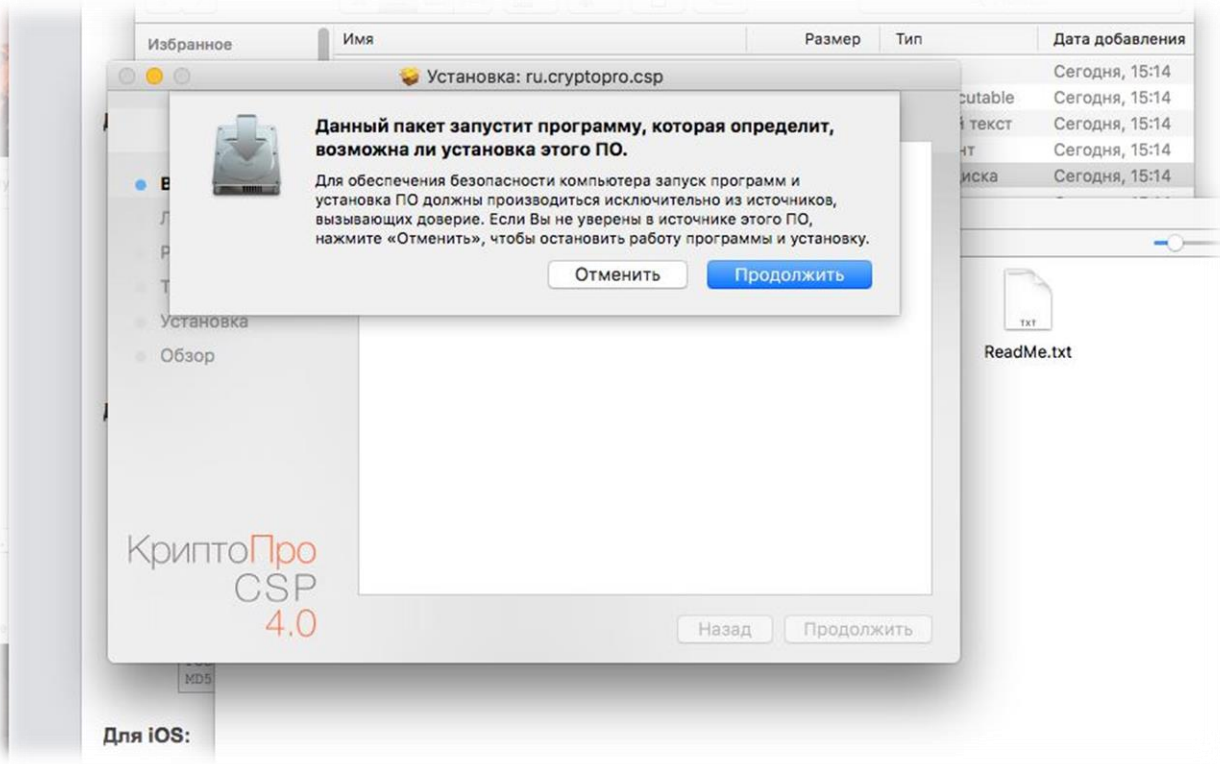

Откройте файл образа ru.cryptopro.cpfox-4.0.0.dmg



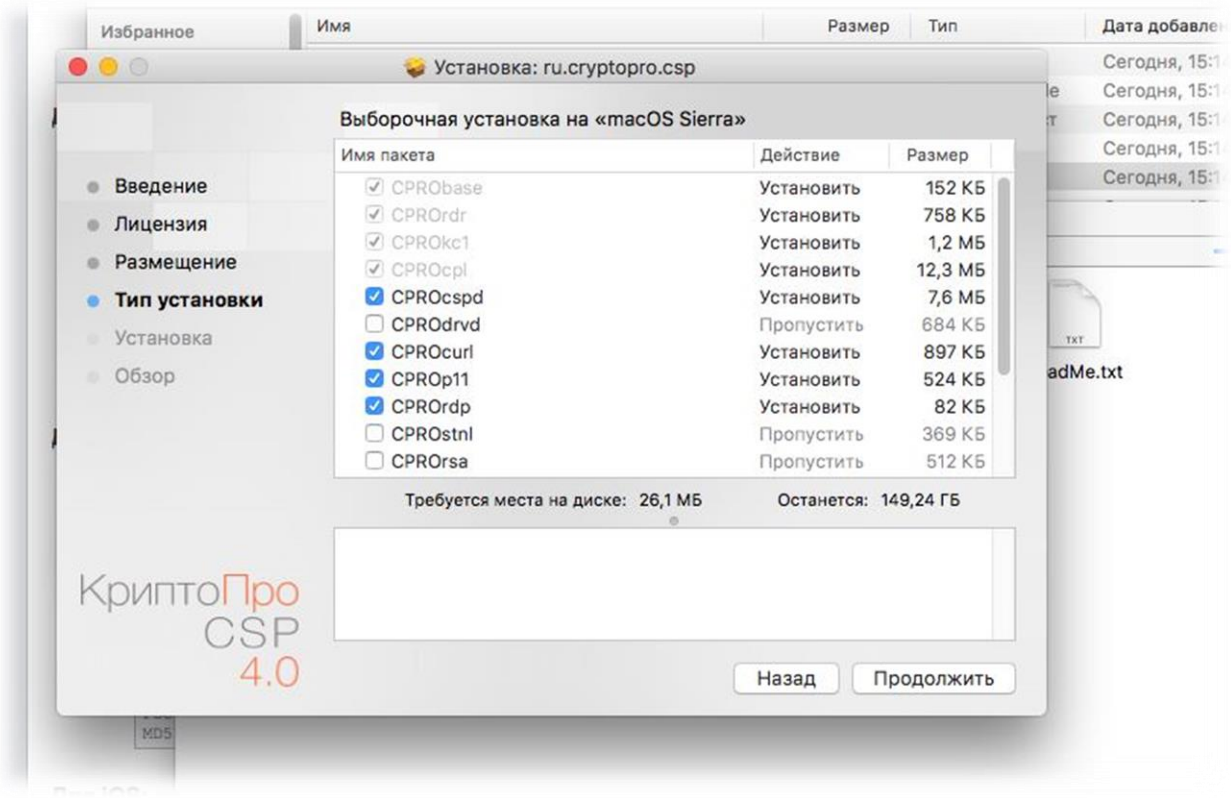

В открывшемся окне запустите ru.cryptopro.csp-4.0.0.mpkg Может потребоваться произвести запуск, нажав ПКМ, а затем “Открыть”, т.к. в системе может быть отключена возможность установки ПО не из App Store (“Защита и безопасность” – вкладка ”Основные”)



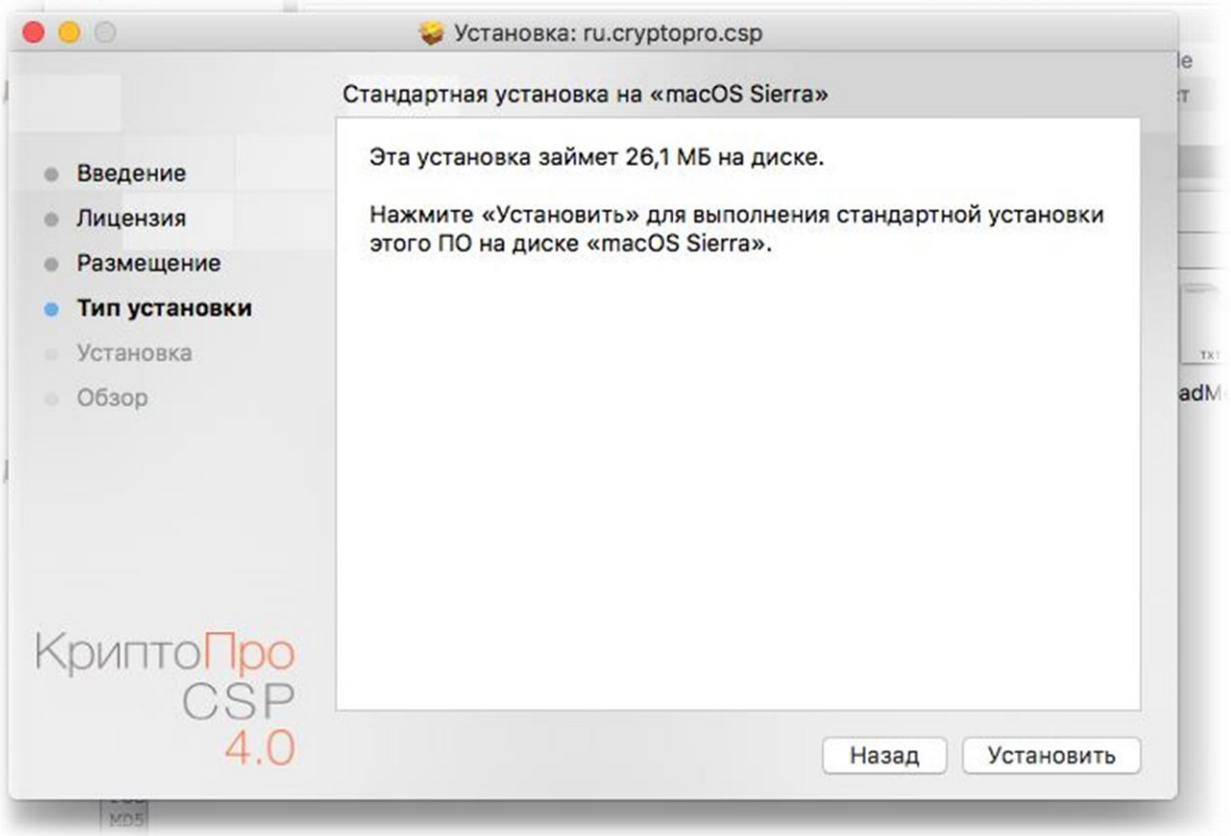

Далее запустится программа установки



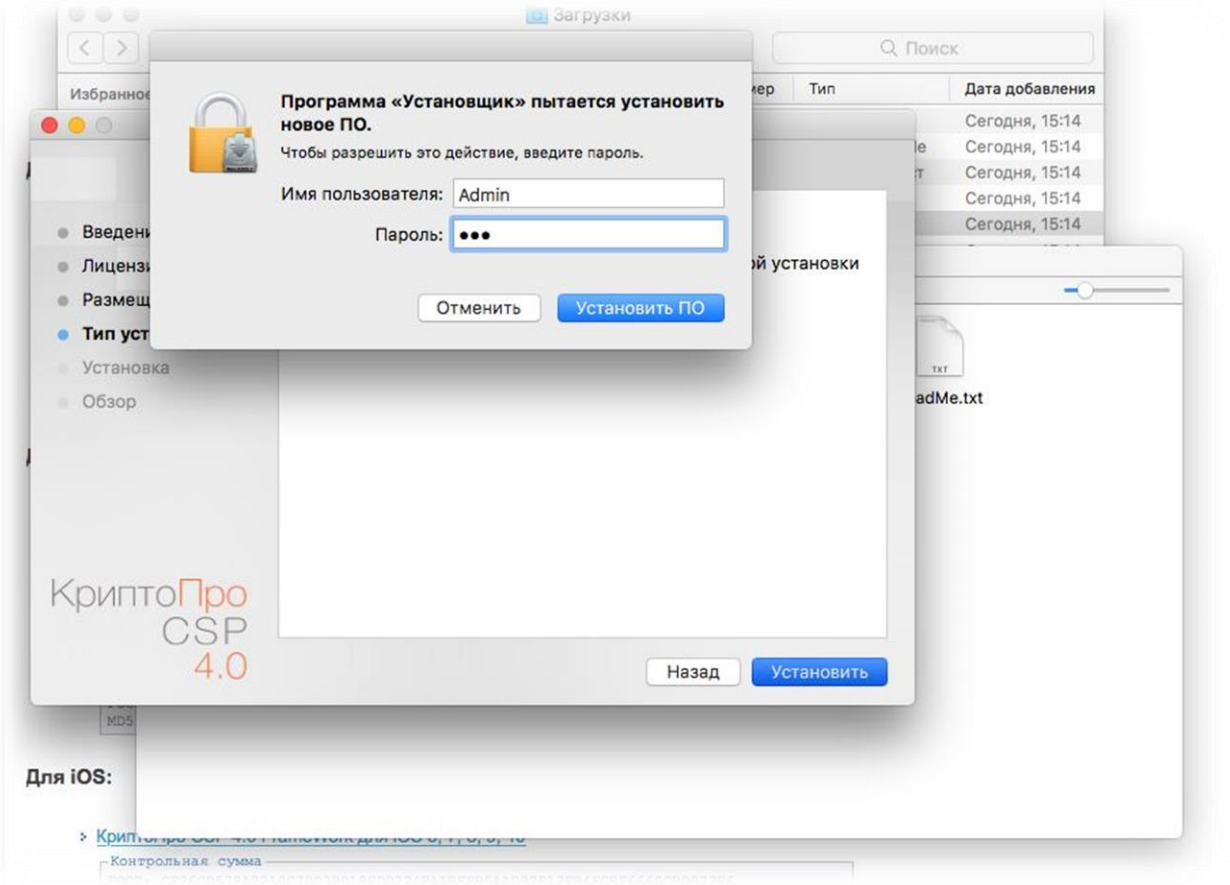

При необходимости можно выбрать дополнительные пакеты, но в нашем случае оставляем все, как есть и нажимаем «Продолжить».



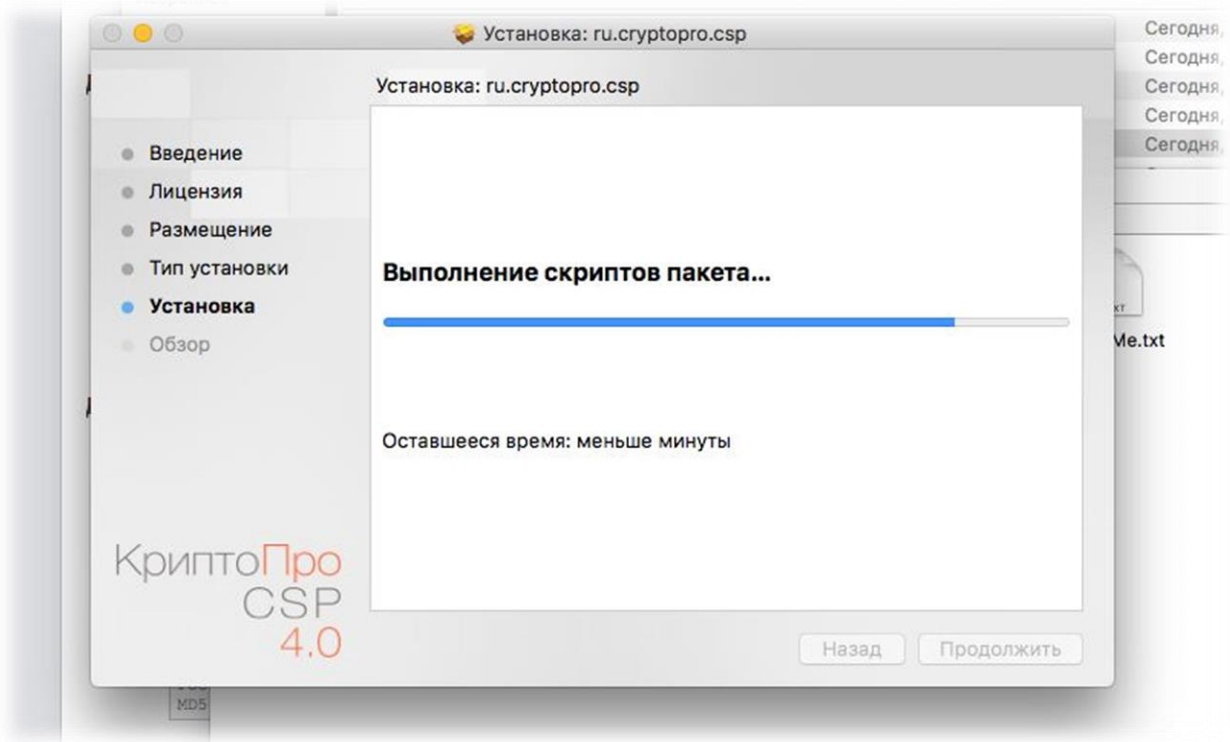

Продолжаем установку

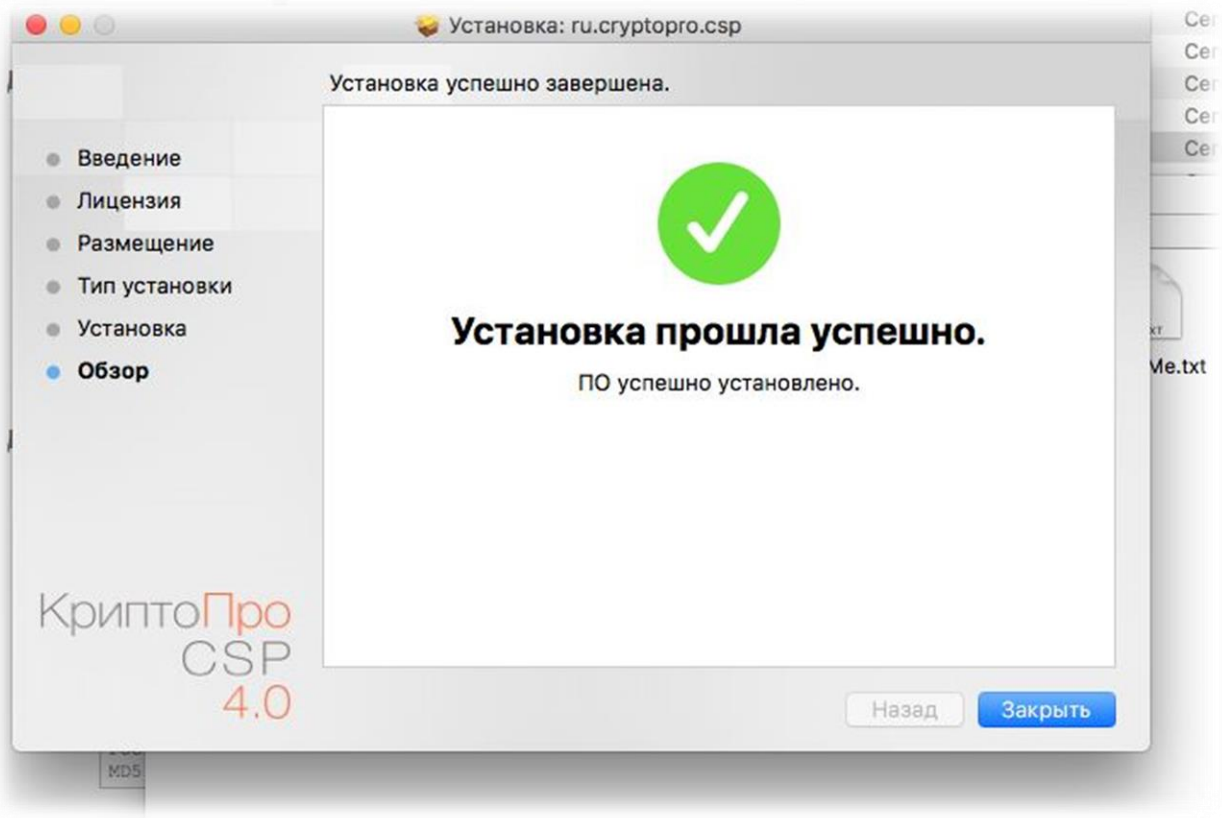



Вводим пароль от учетной записи в системе.



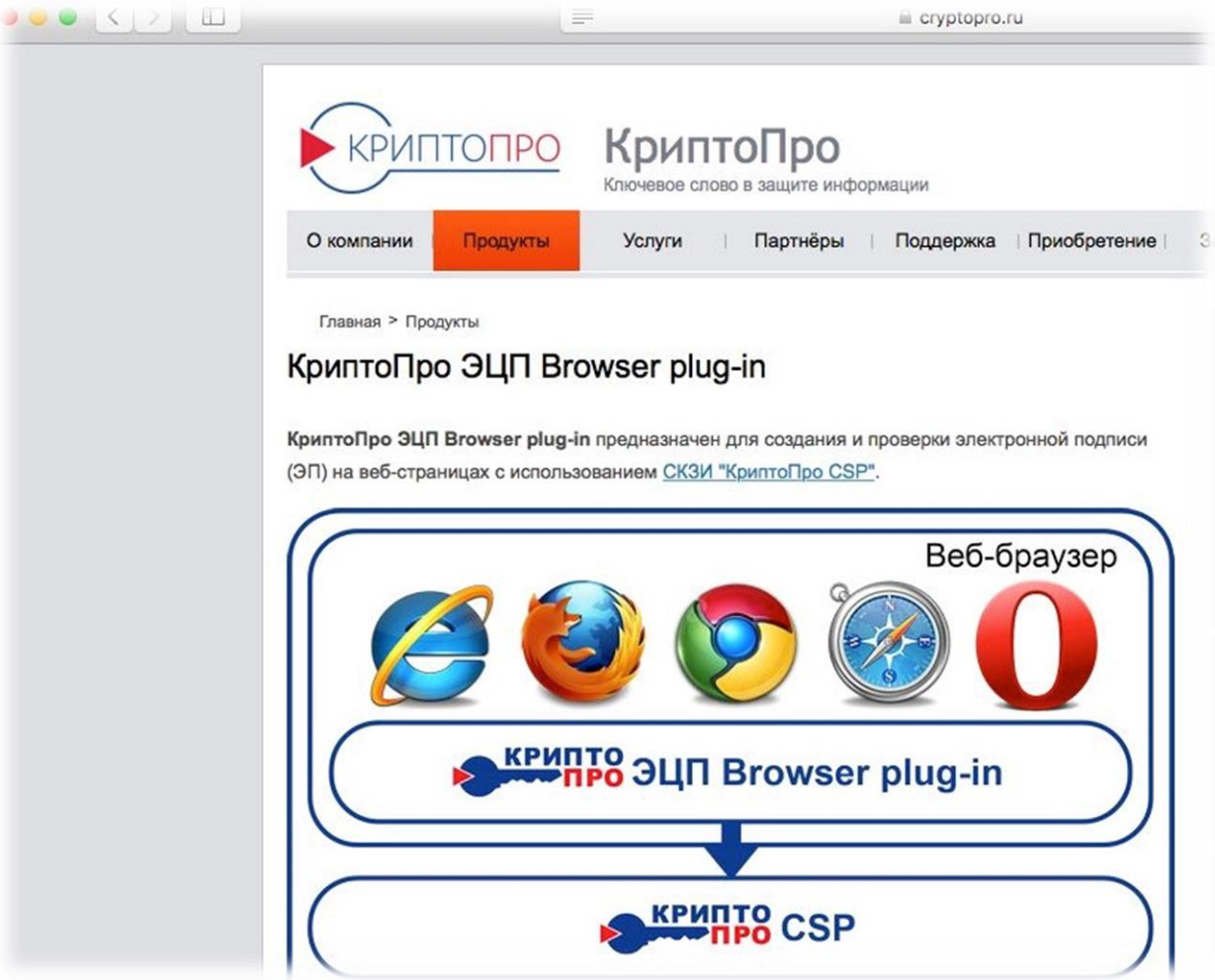

Завершение установки СКЗИ КриптоПро CSP



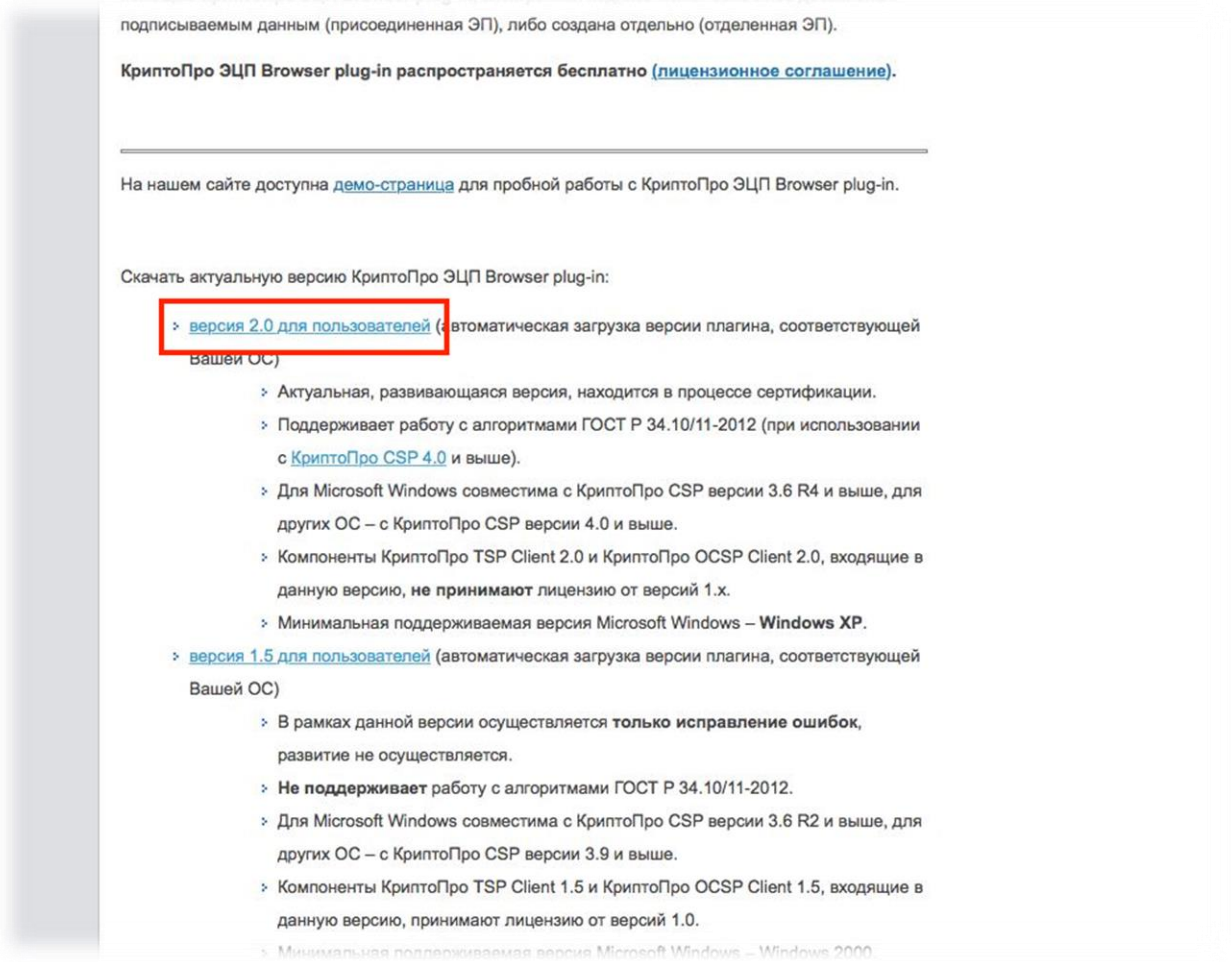

Установка: ru.cryptopro.csp
Установка успешно завершена.
Введение
Лицензия
Размещение
Тип установки
Установка
Обзор
Установка прошла успешно.
ПО успешно установлено.
КриптоПро CSP 4.0
Назад
Закрыть

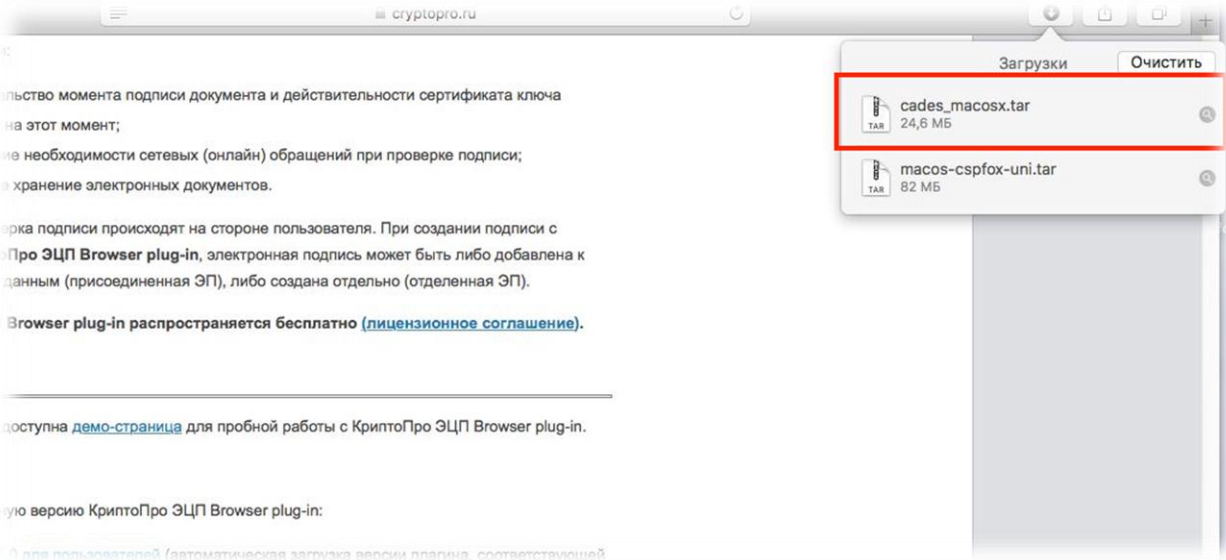
# Скачивание и установка дистрибутива КриптоПро ЭЦП Browser plug-in

Дистрибутив КриптоПро ЭЦП Browser plug-in предназначен для создания и проверки ЭП на веб-страницах с использованием СКЗИ КриптоПро CSP. Используемая клиентом ОС при скачивании дистрибутива плагина определяется сайтом автоматически – скачивается версия подходящая именно для данной ОС.

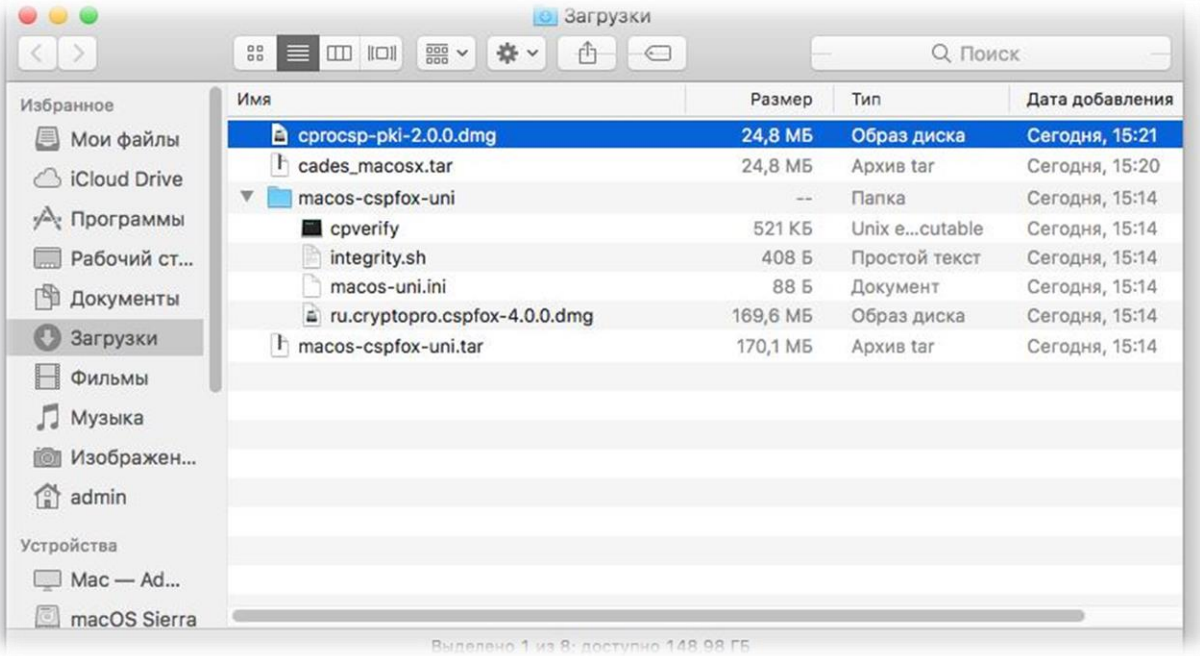


Производится скачивание дистрибутива КриптоПро ЭЦП Browser plug-in

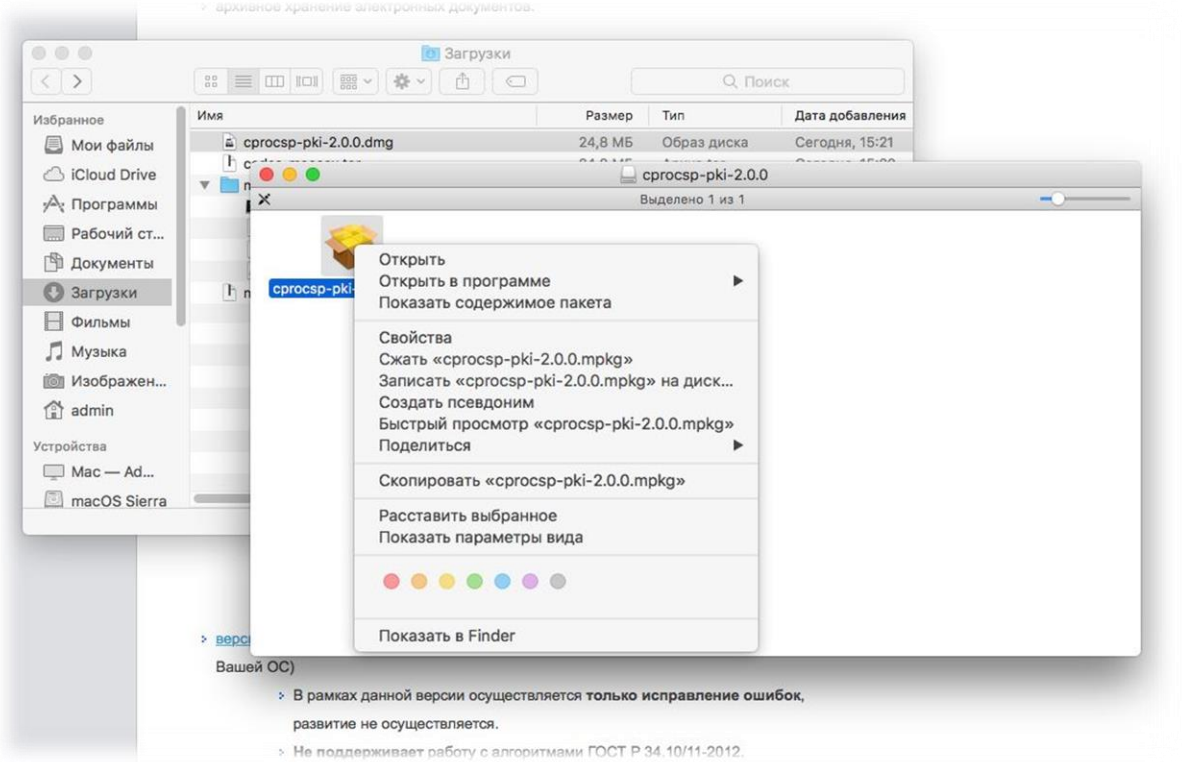


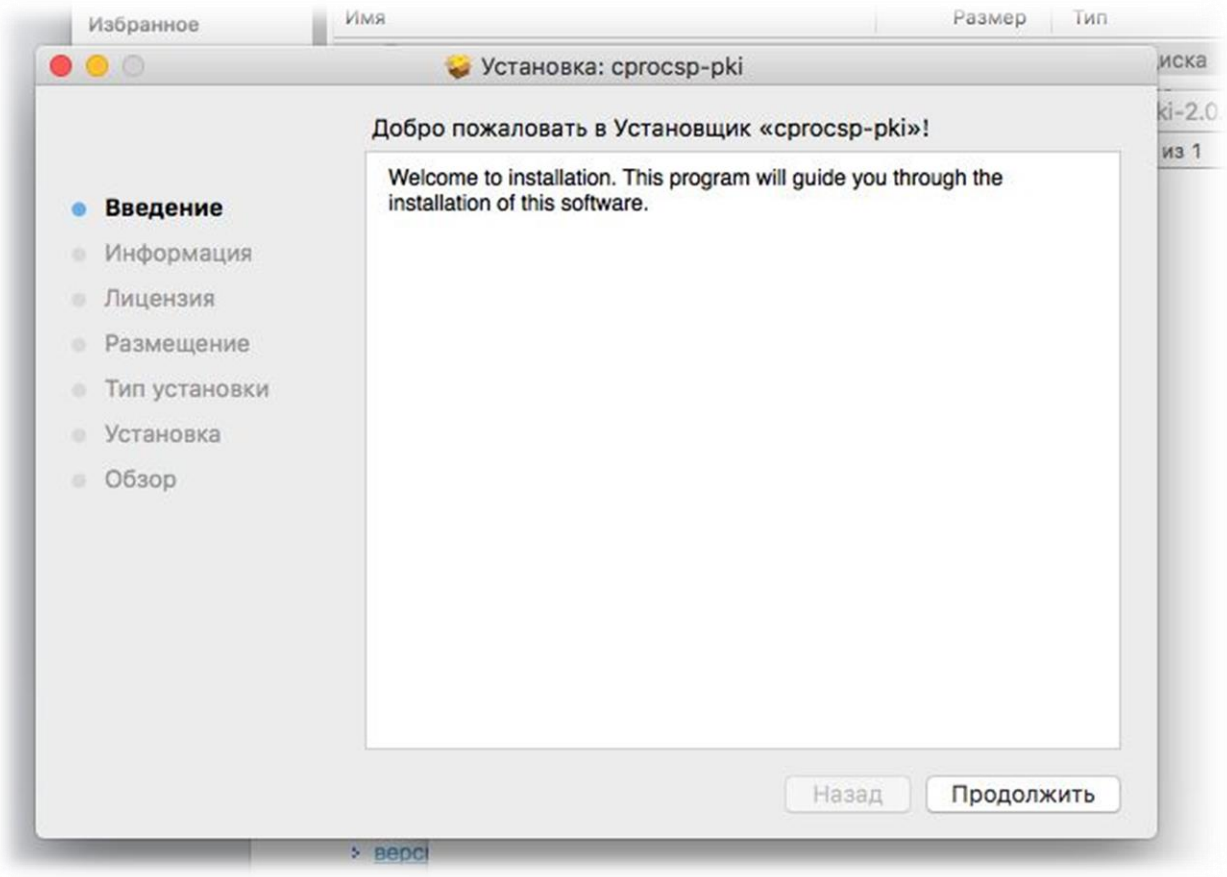
Далее следует открыть файл образа cprocsp-pki-2.0.0.dmg

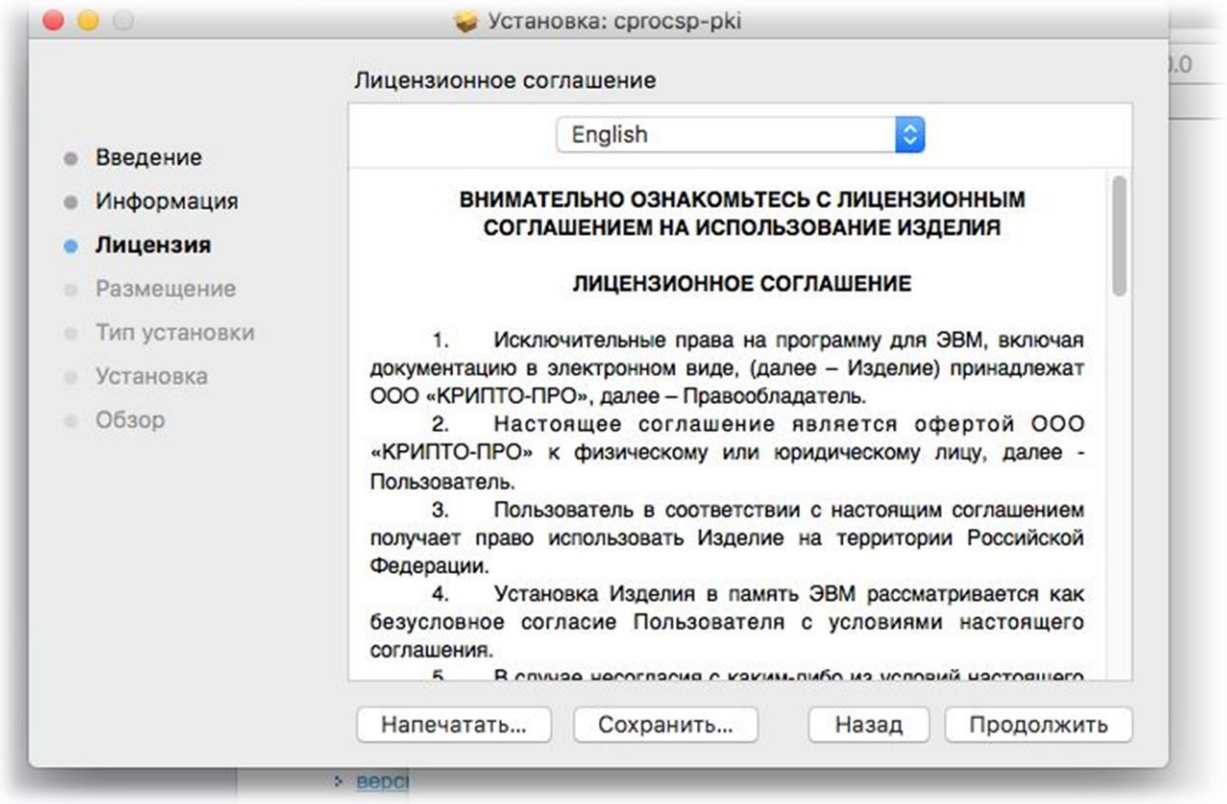



В открывшемся окне запустить cprocsp-pki-2.0.0.mpkg Может потребоваться произвести запуск, нажав ПКМ, а затем “Открыть”, т.к. в системе может быть отключена возможность установки ПО не из App Store (“Защита и безопасность” – вкладка ”Основные”)

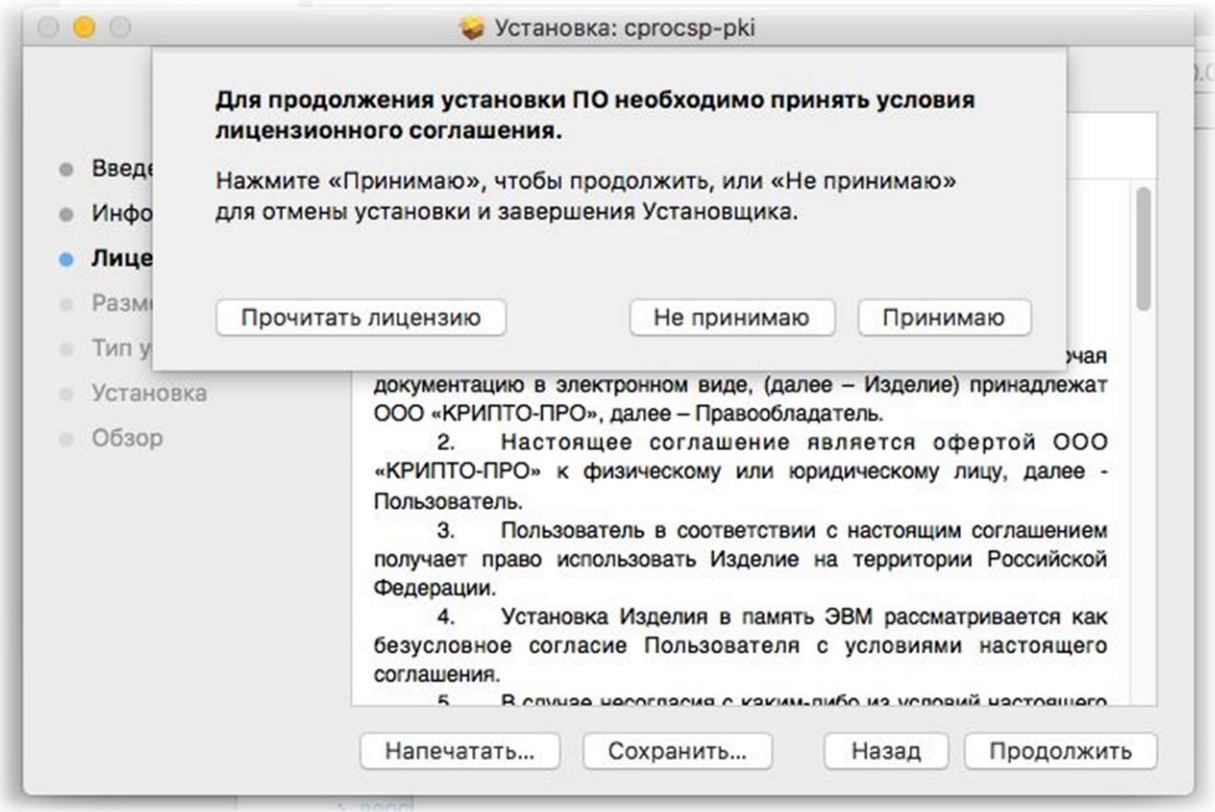


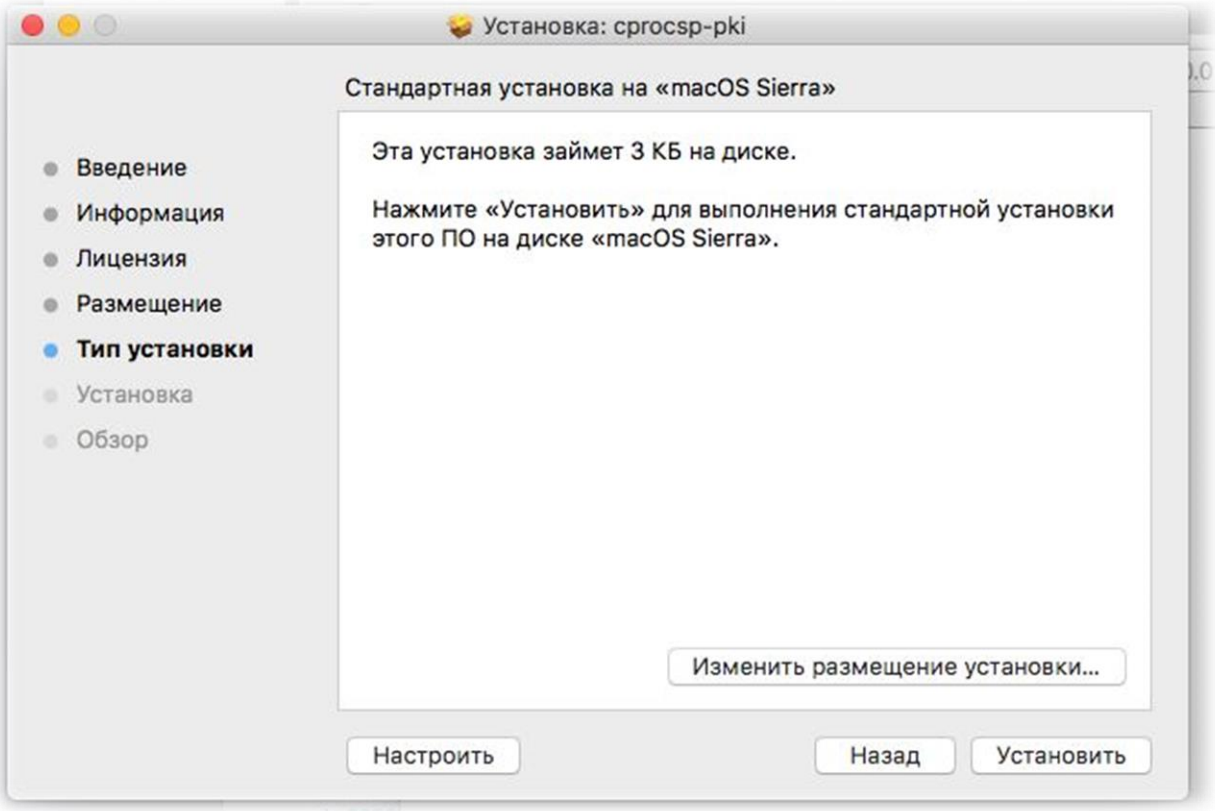
Далее установка производится стандартным способом.



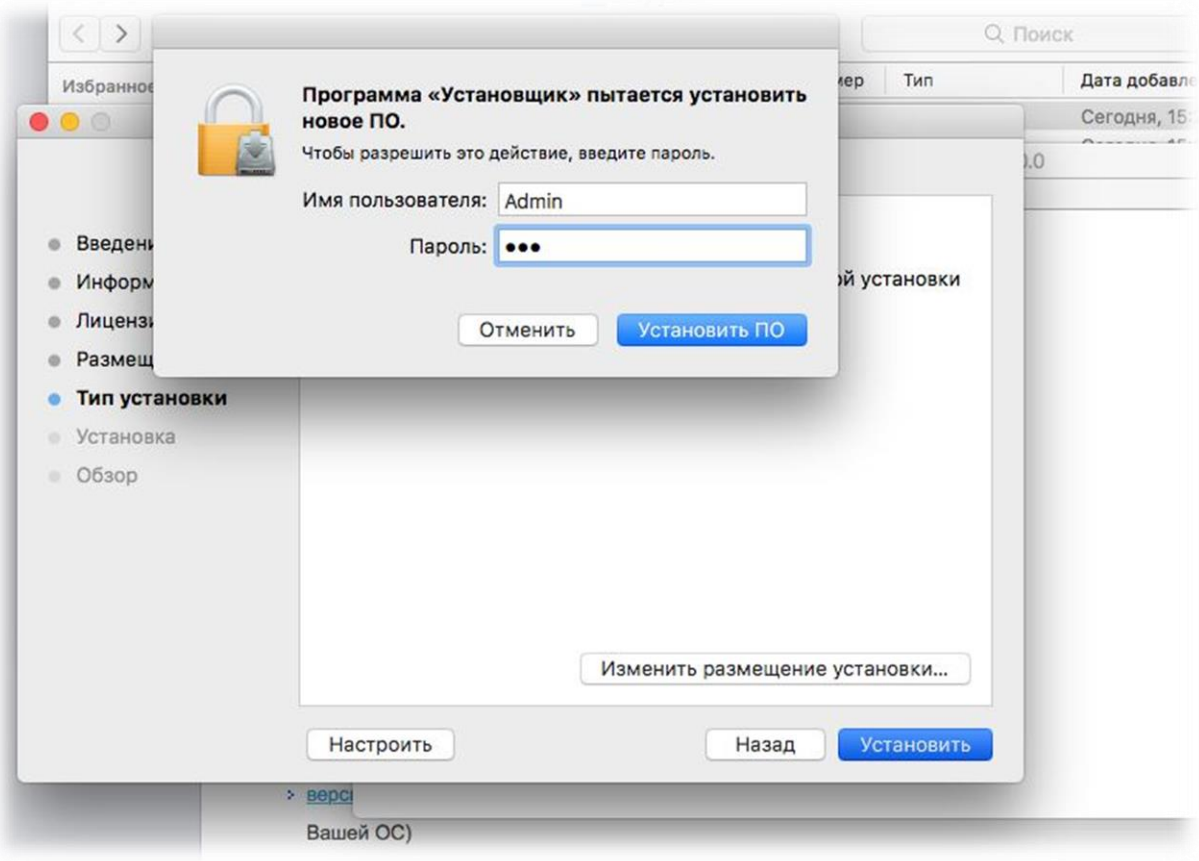



Принятие условий лицензионного соглашения.

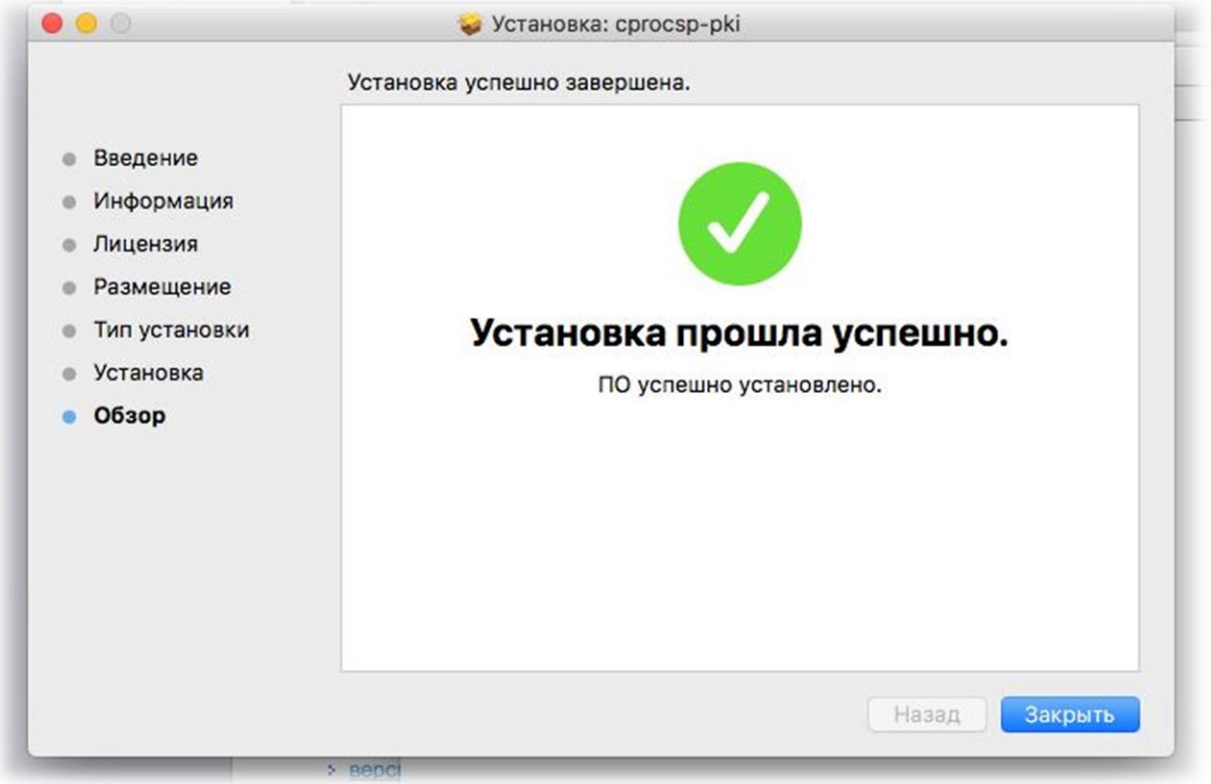


Ввод пароля учетной записи.

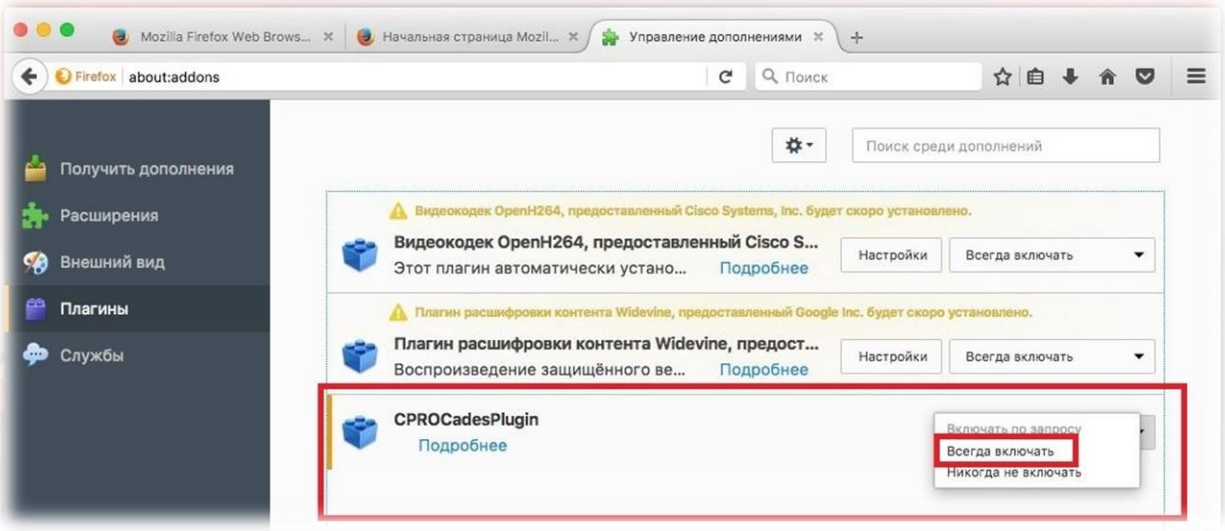


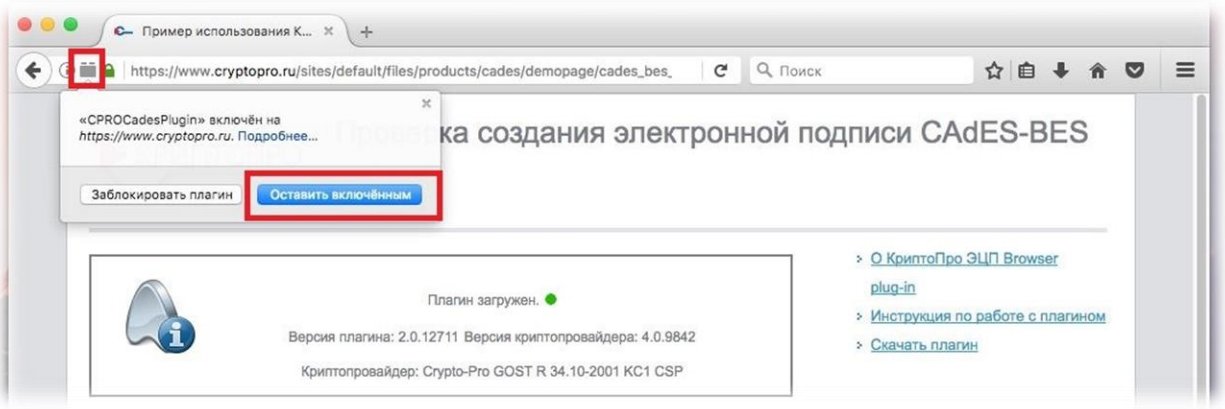

Завершение процесса установки КриптоПро ЭЦП Browser plug-in.



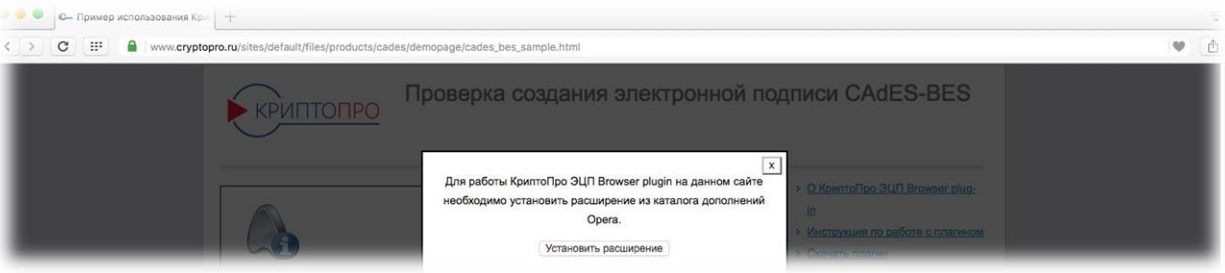

Браузер(ы) следует перезапустить.

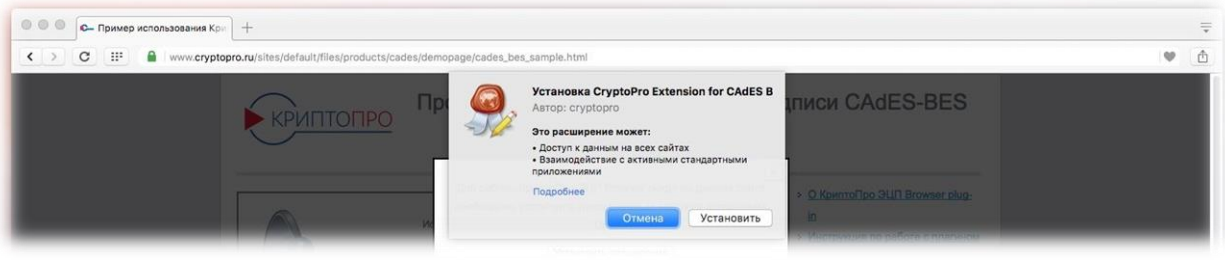
В случае Safari и Firefox этого будет достаточно. Разве что в FF может потребоваться разрешить работу плагина



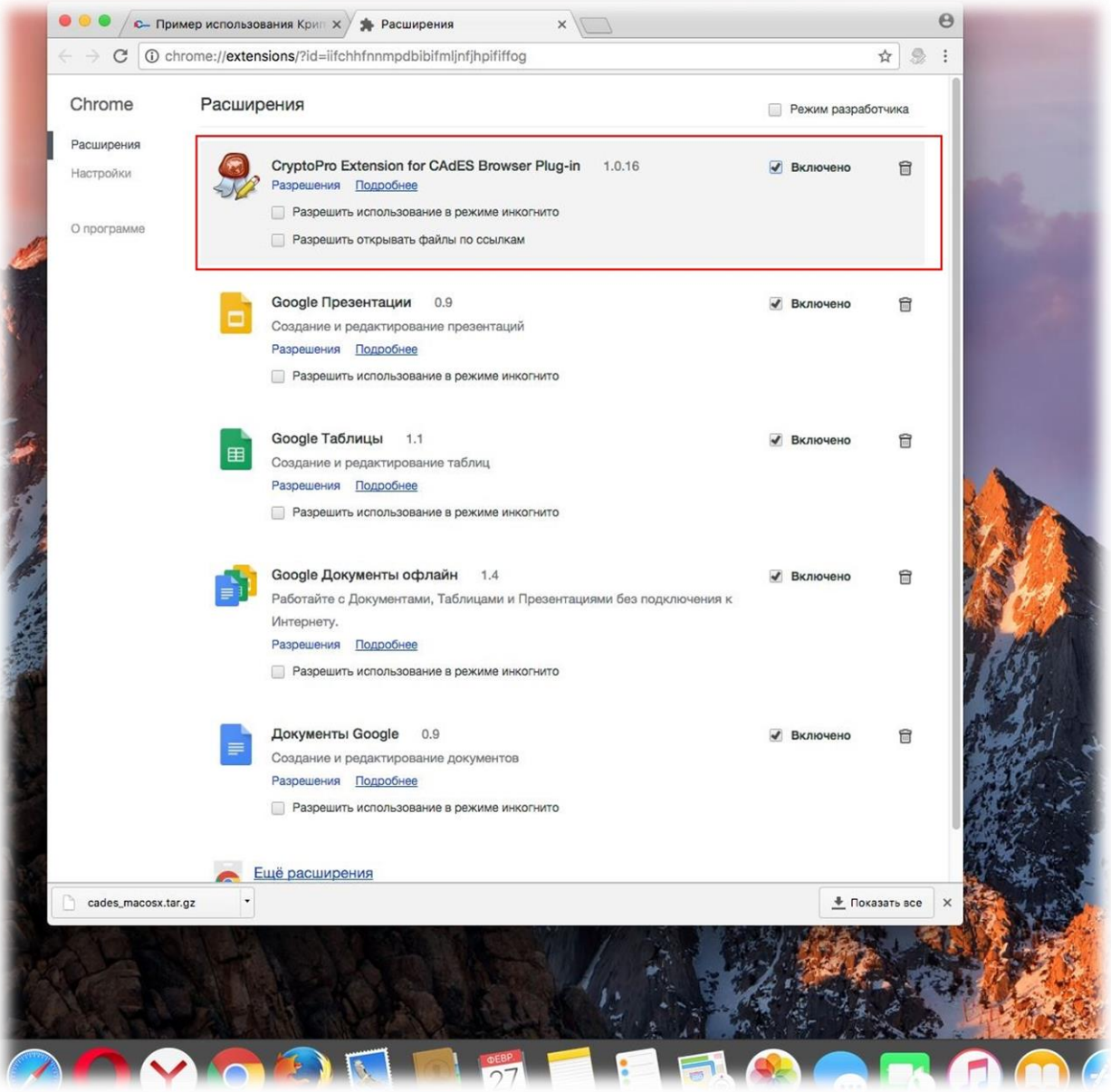




В Opera предложение установить расширение отобразится автоматически



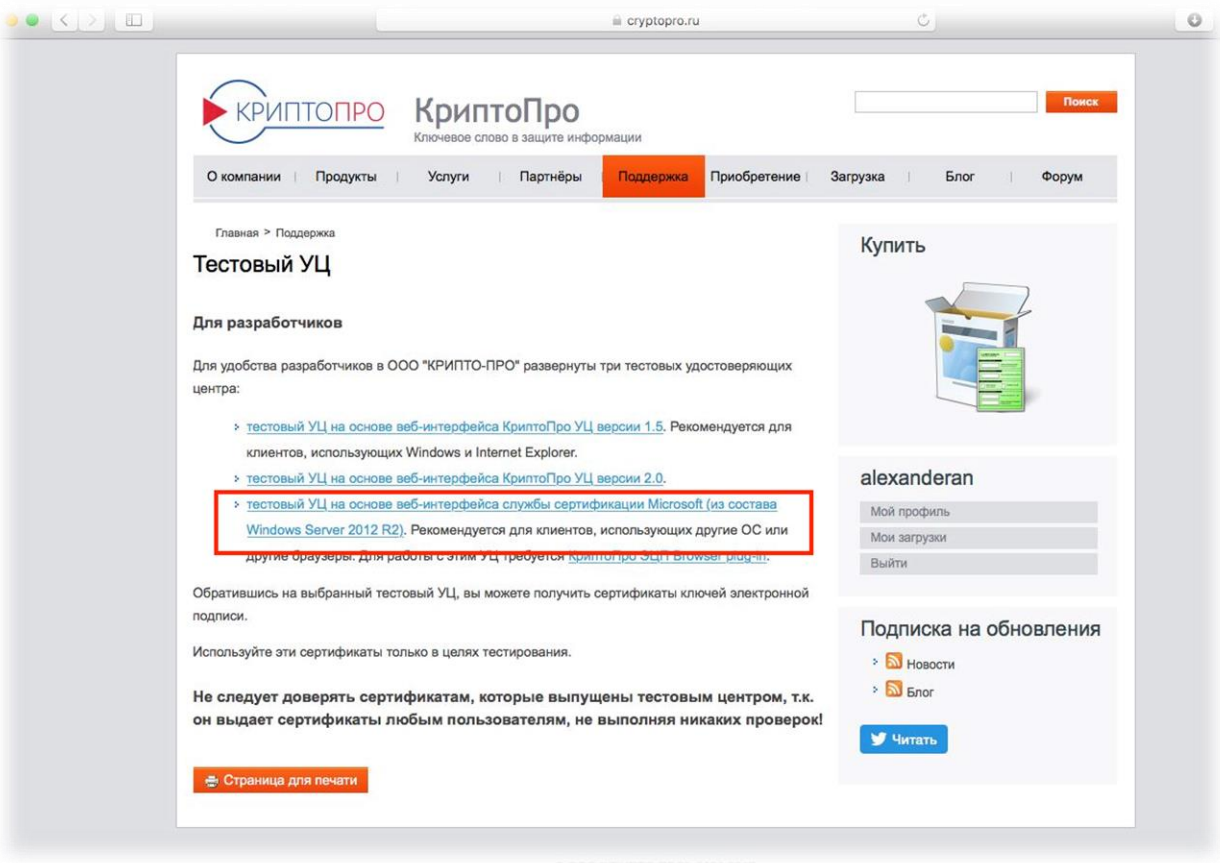



В Google Chrome и Яндекс Браузере может потребоваться установить расширение вручную из магазина расширений.

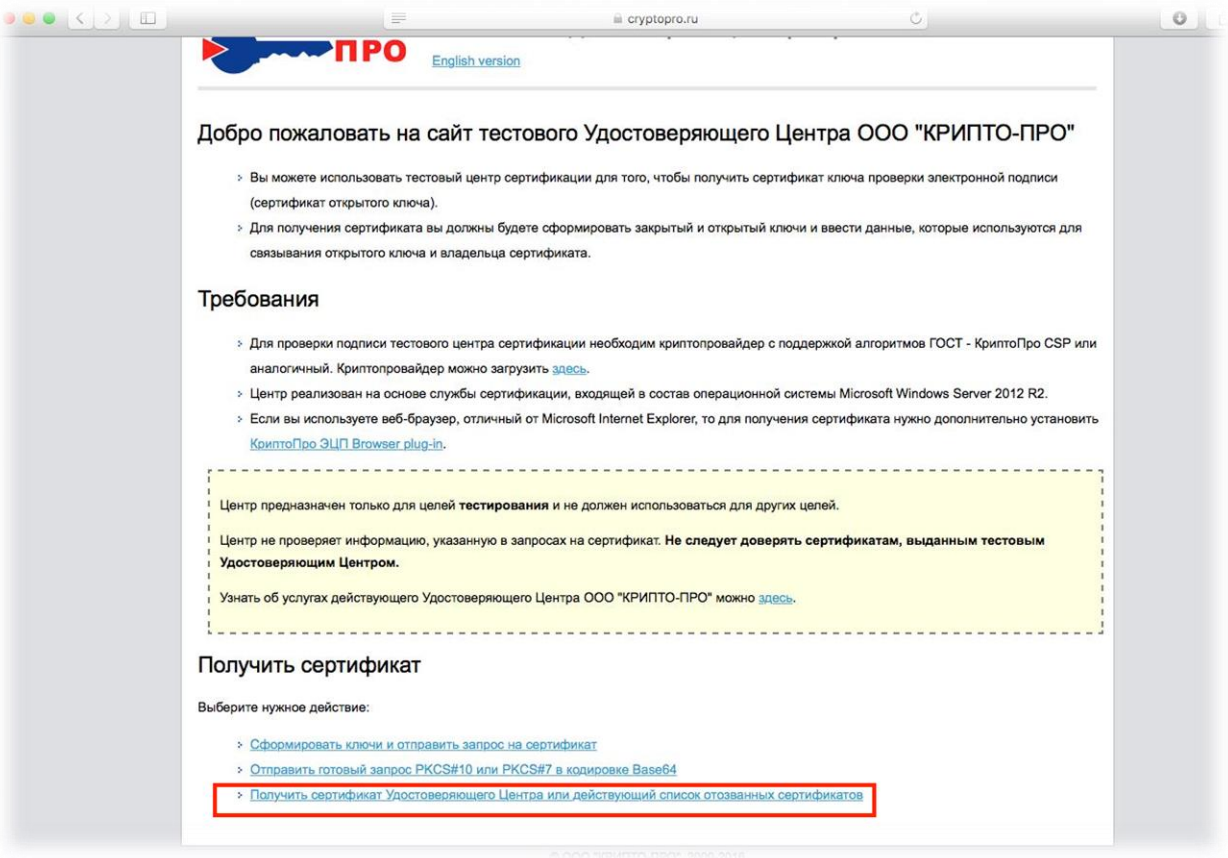


# Работа с тестовым удостоверяющим центром

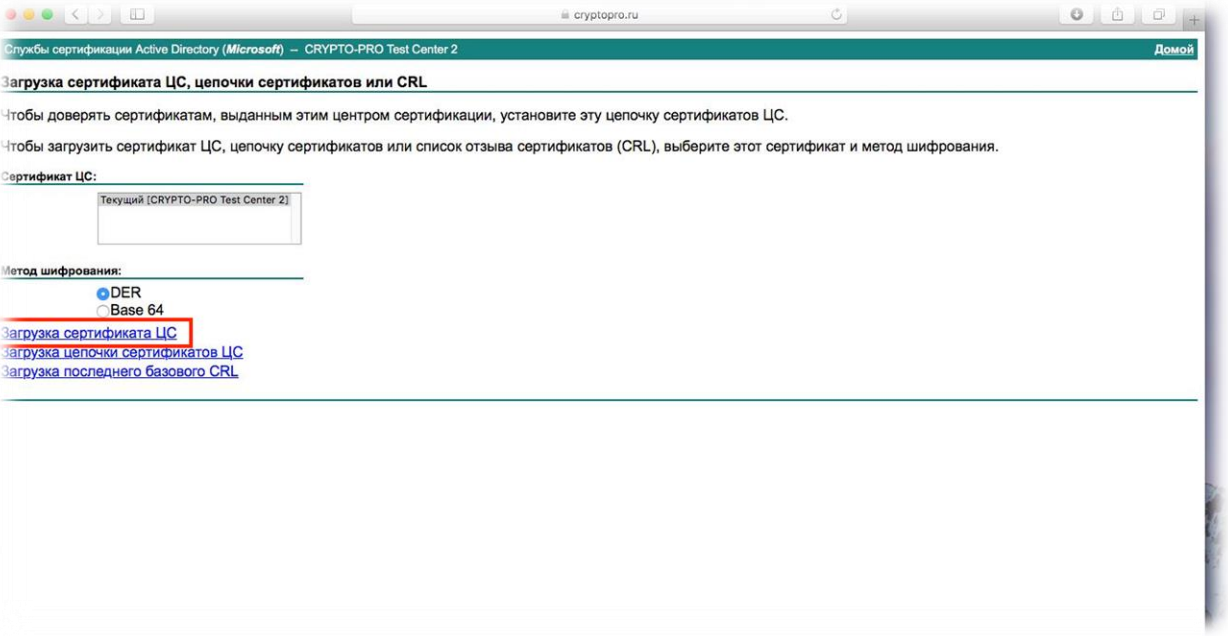
Произведя установку ПО можно сформировать ключи и выпустить сертификат для тестовых целей. Будет использоваться один из доступных тестовых удостоверяющих центров

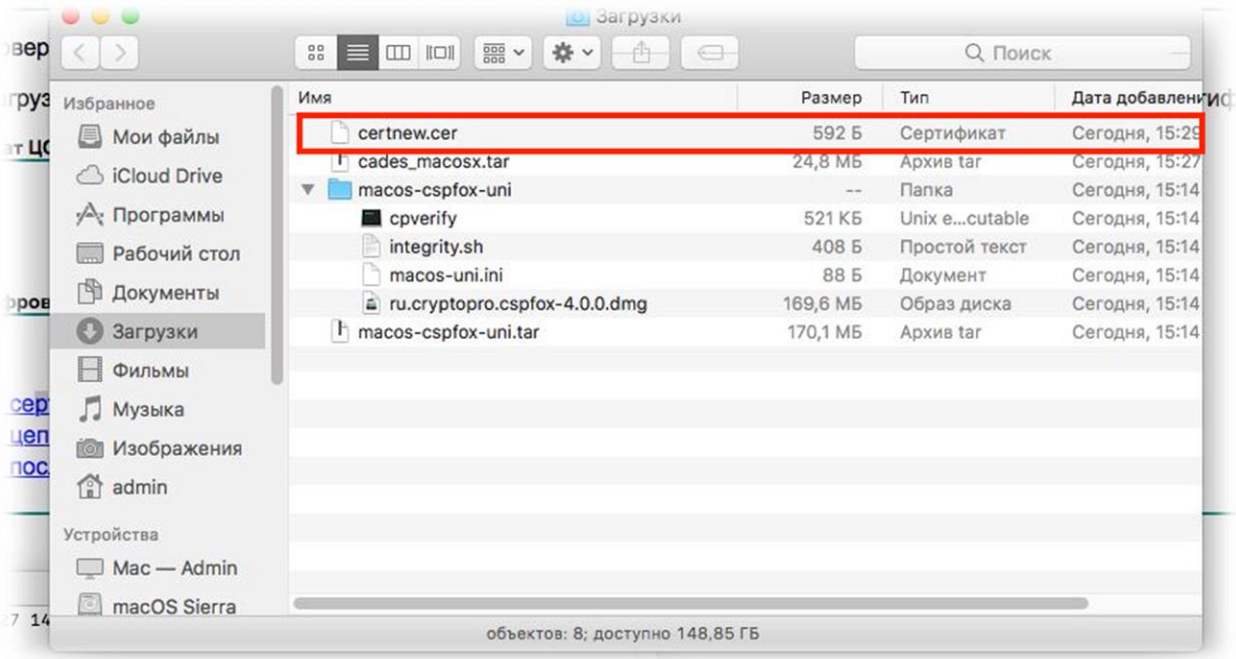


Сперва следует скачать и установить в соответствующее хранилище (root – доверенные корневые центры сертификации) корневой сертификат данного УЦ.

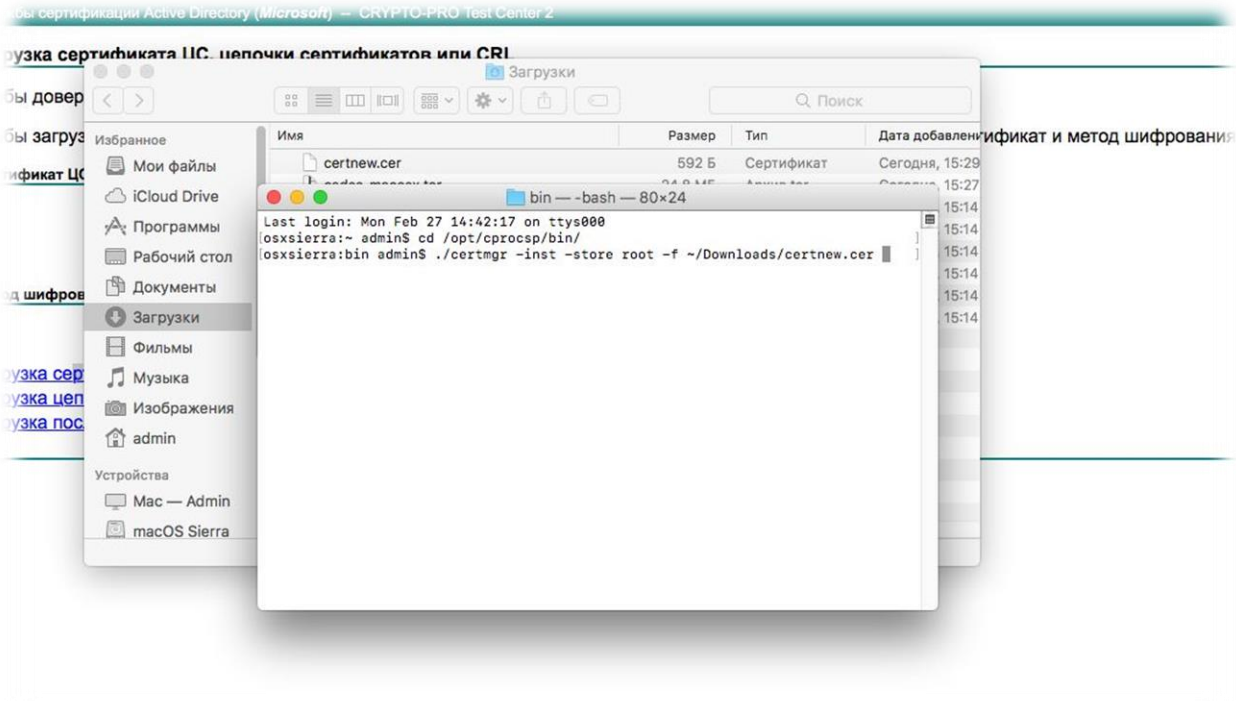



Производится скачивание файла сертификата.

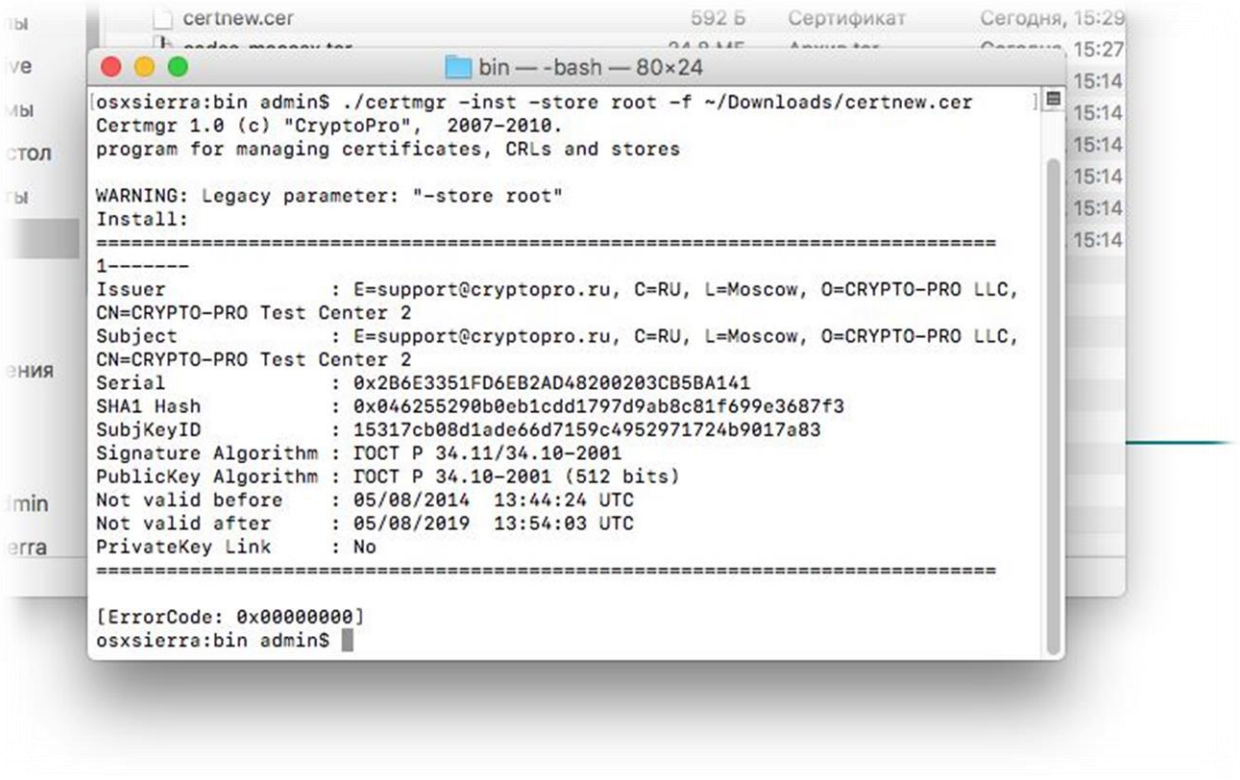




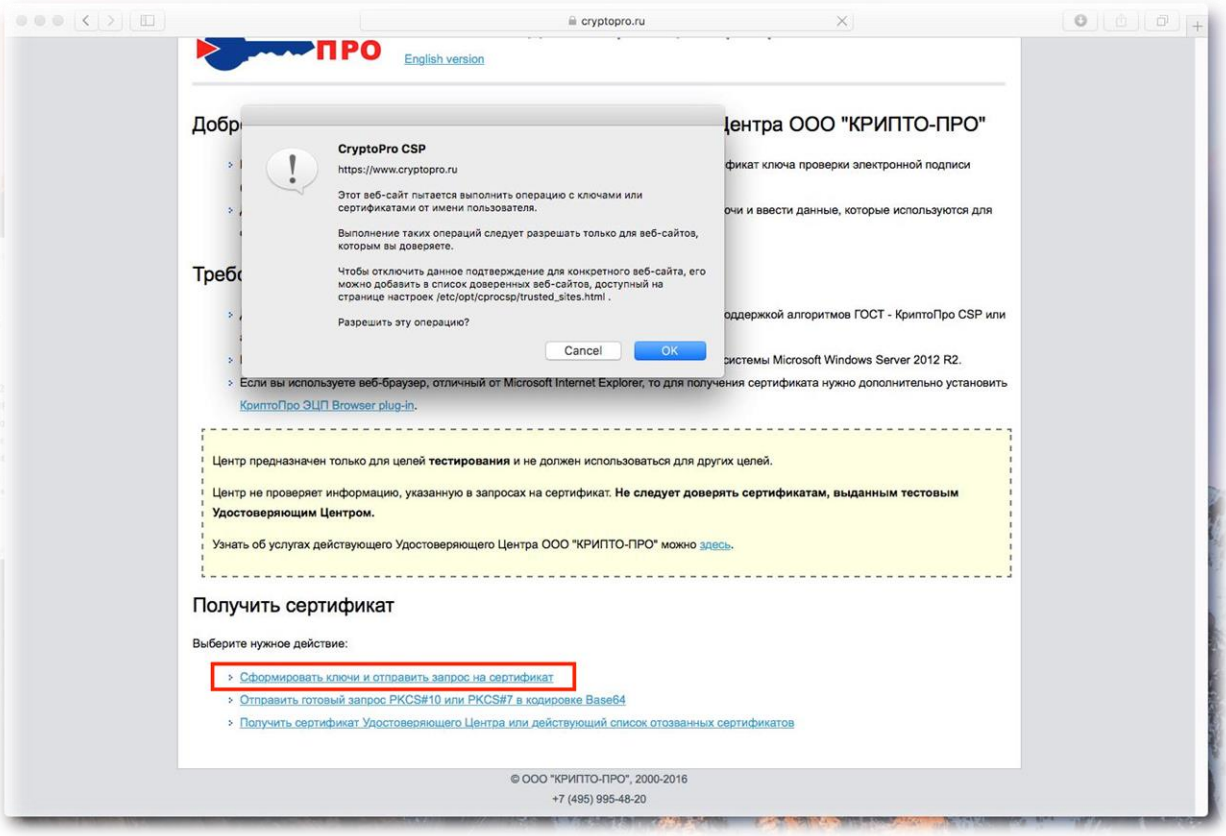

Далее следует открыть Терминал (Утилиты - Терминал) и произвести установку сертификата утилитой certmgr.



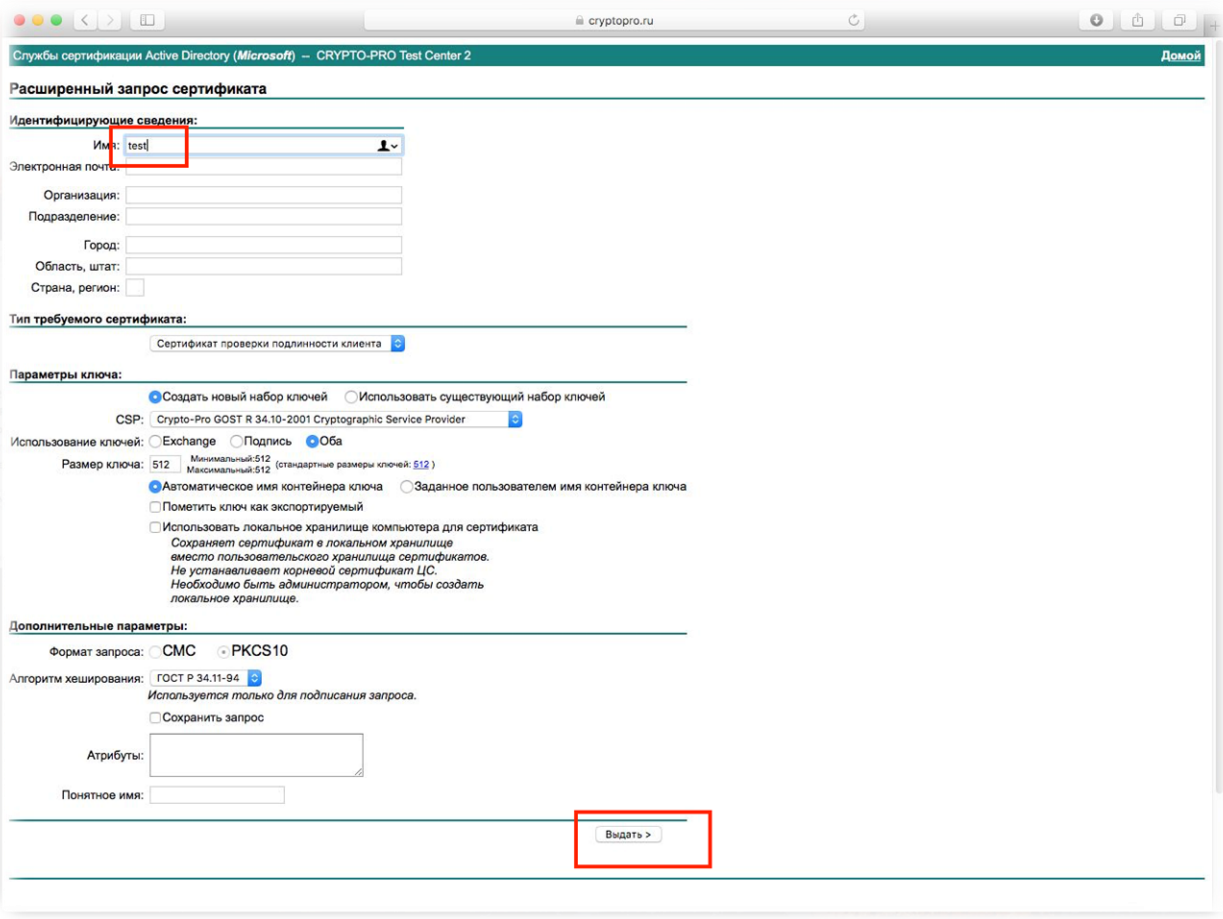
Установка корневого сертификата произведена успешно.



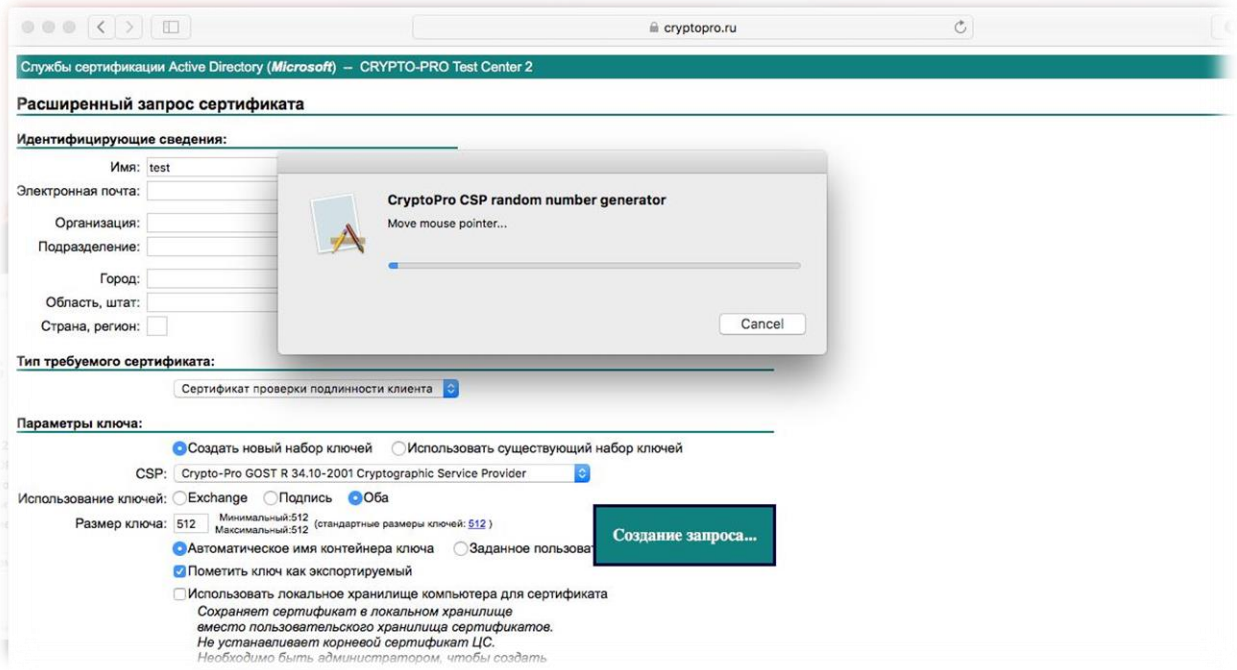

Далее можно приступить к формированию тестовых ключей и выпуску личного сертификата. При попытке перехода по выделенной красным ссылке отобразится окно с уведомлением о необходимости подтверждения на выполнение операции с ключами и сертификатами. Уведомление вызвано отсутствием сайта (https://www.cryptopro.ru) в перечне доверенных. Механизм добавления сайтов в данный перечень будет проиллюстрирован несколько позднее. Нажать ОК.



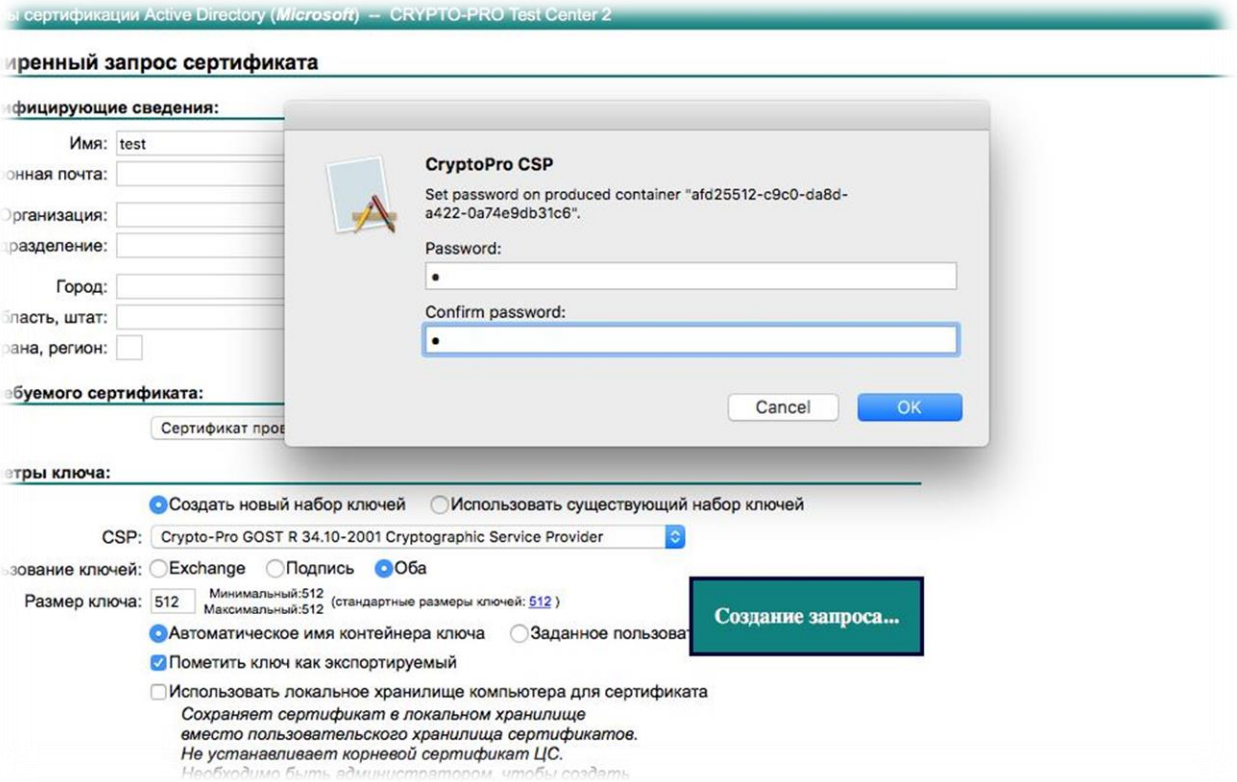

В следующем окне для простоты следует указать произвольное имя и нажать кнопку “Выдать >”



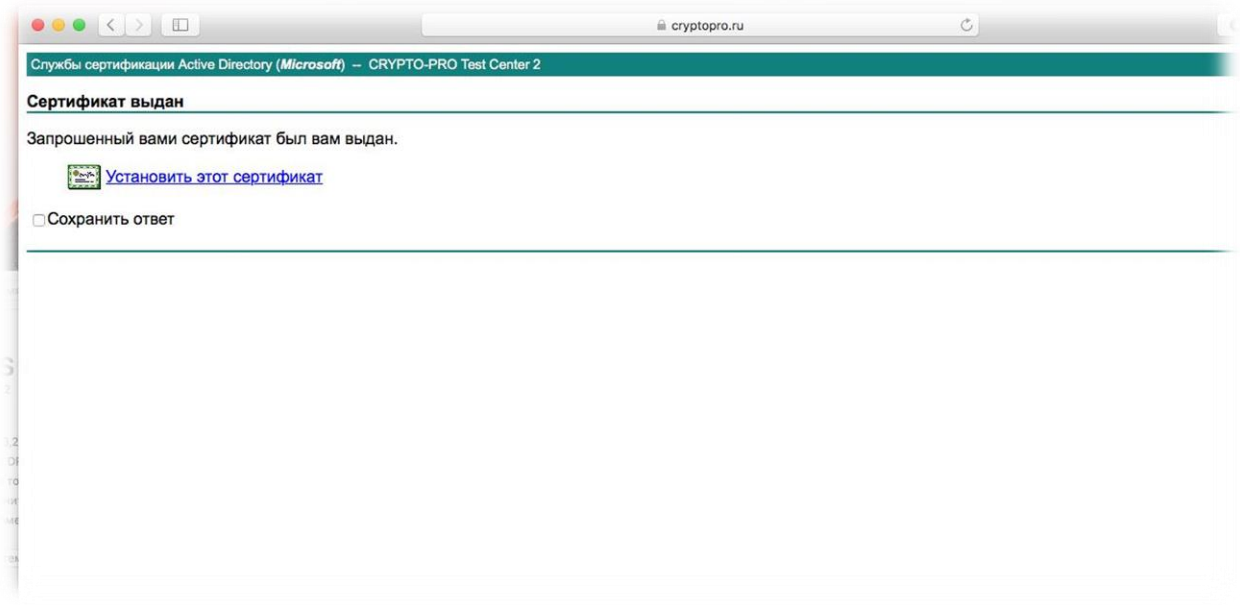
Отобразится датчик случайных чисел (био-ДСЧ). Потребуется передвигать курсор мыши до окончания процесса формирования ключей.



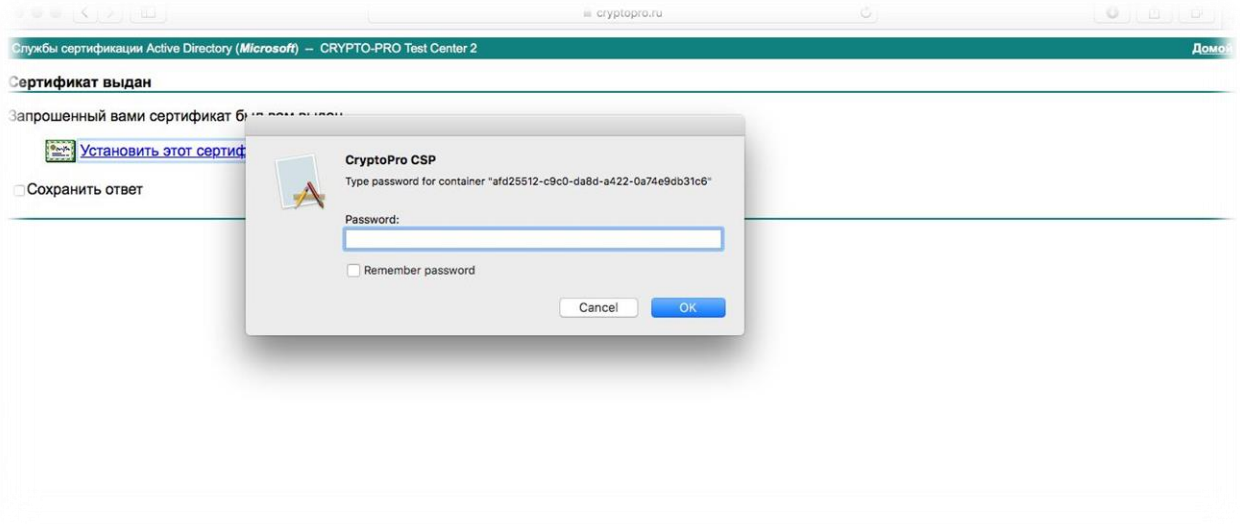

Предложение задать пароль на созданный контейнер



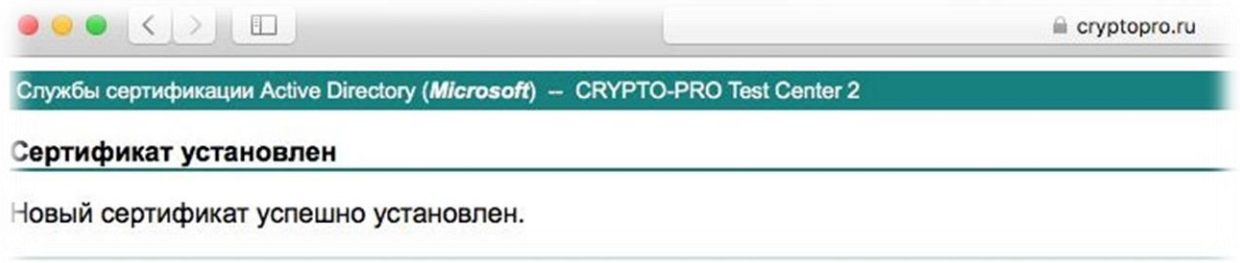
Далее производится установка сертификата



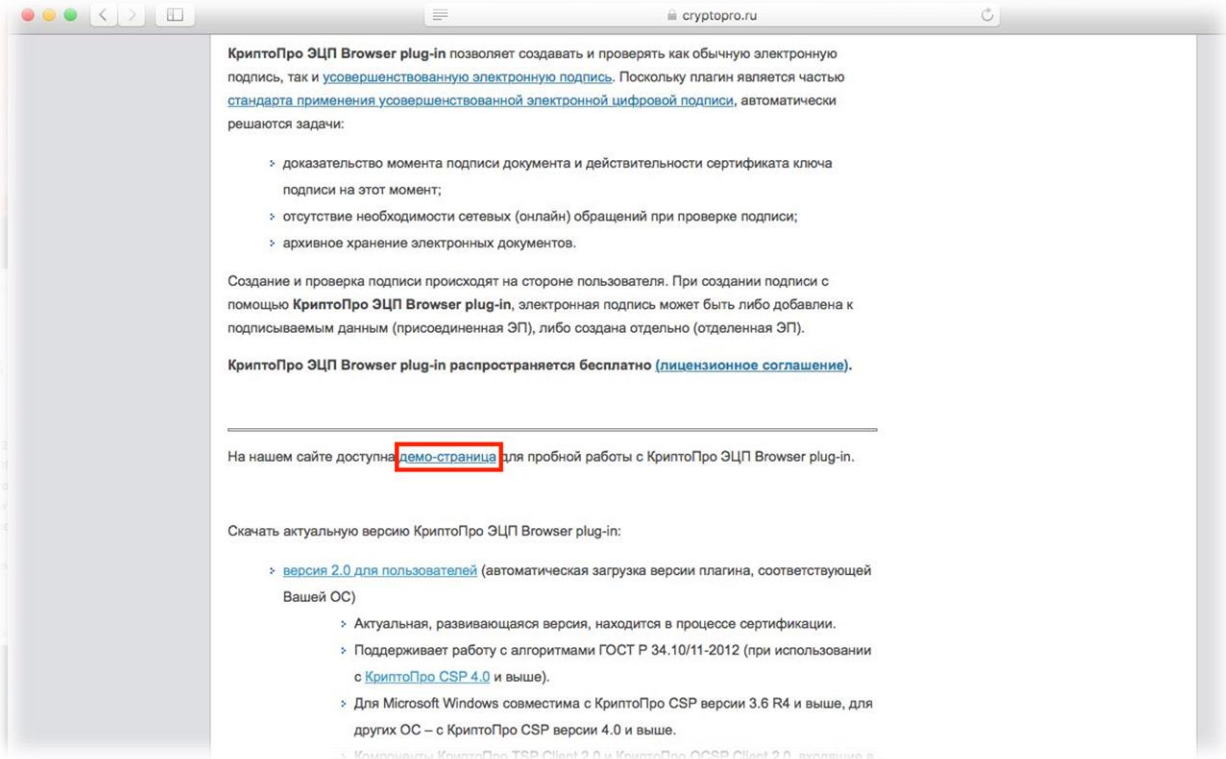

Потребуется ввести ранее придуманный пароль на контейнер



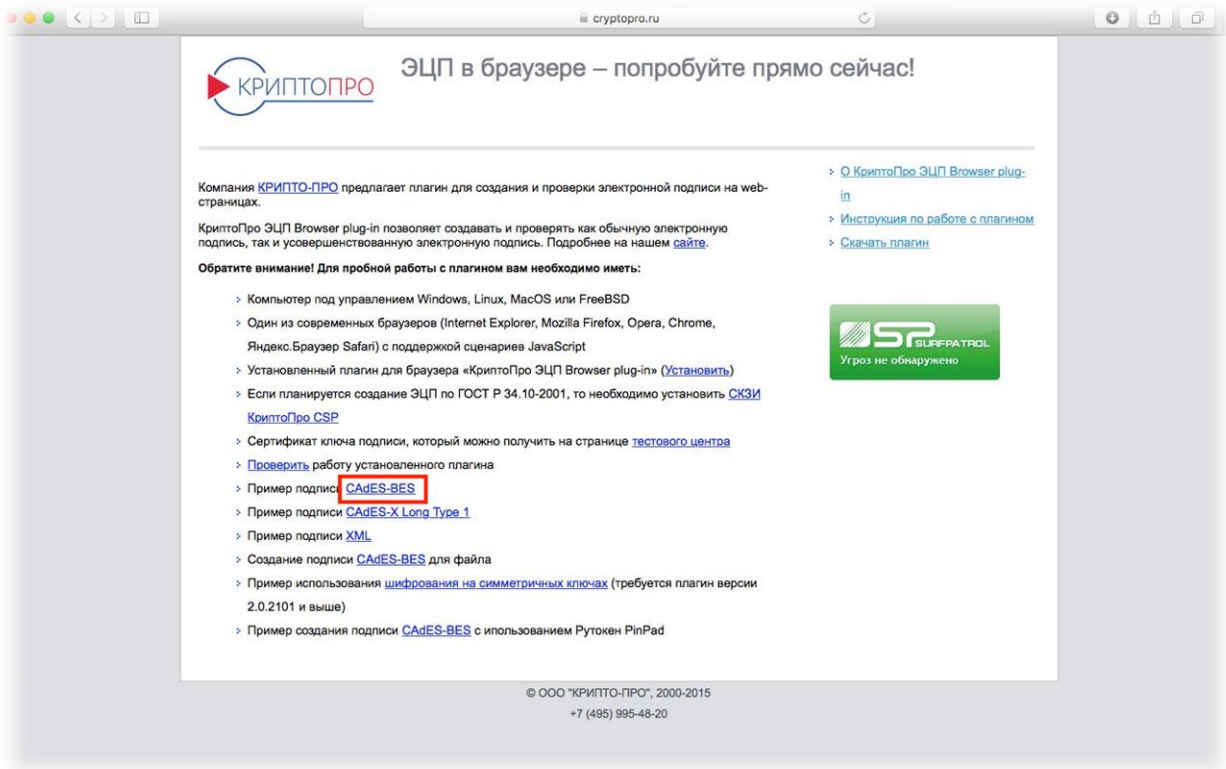

Установка личного сертификата прошла успешно.



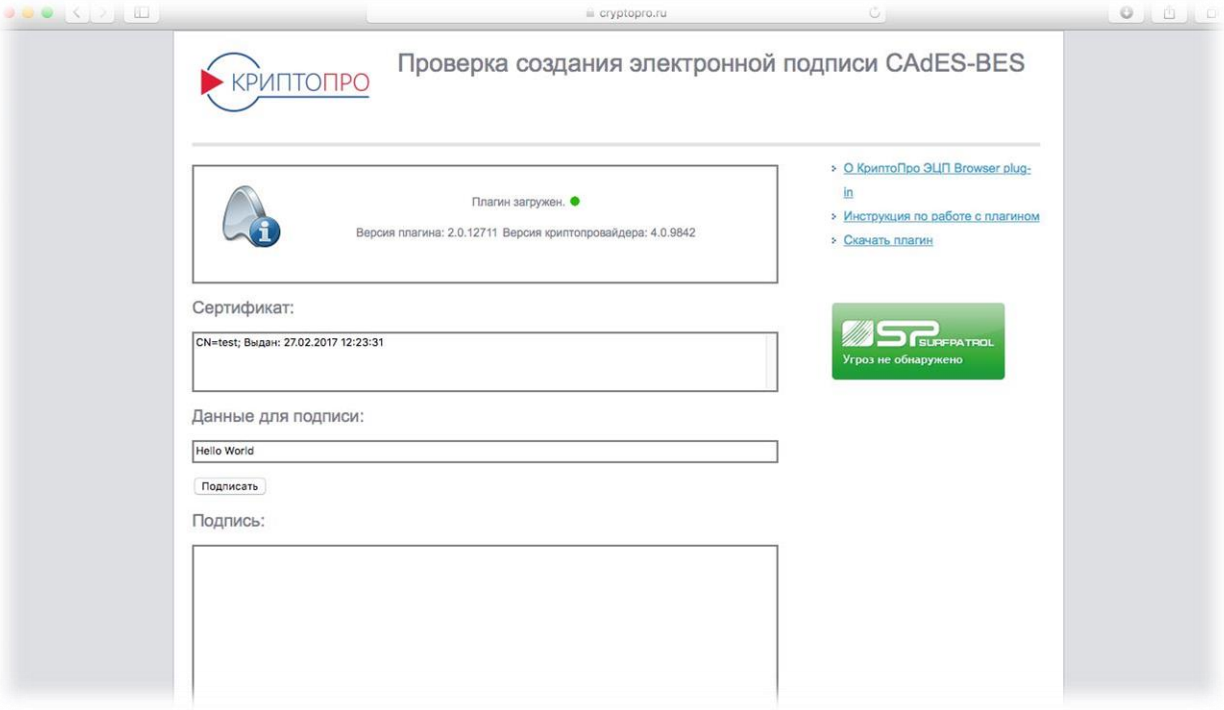
Для проверки работоспособности можно произвести подпись выпущенным сертификатом. Для этого следует воспользоваться функционалом демо-страницы для пробной работы с КриптоПро ЭЦП Browser plug-in.



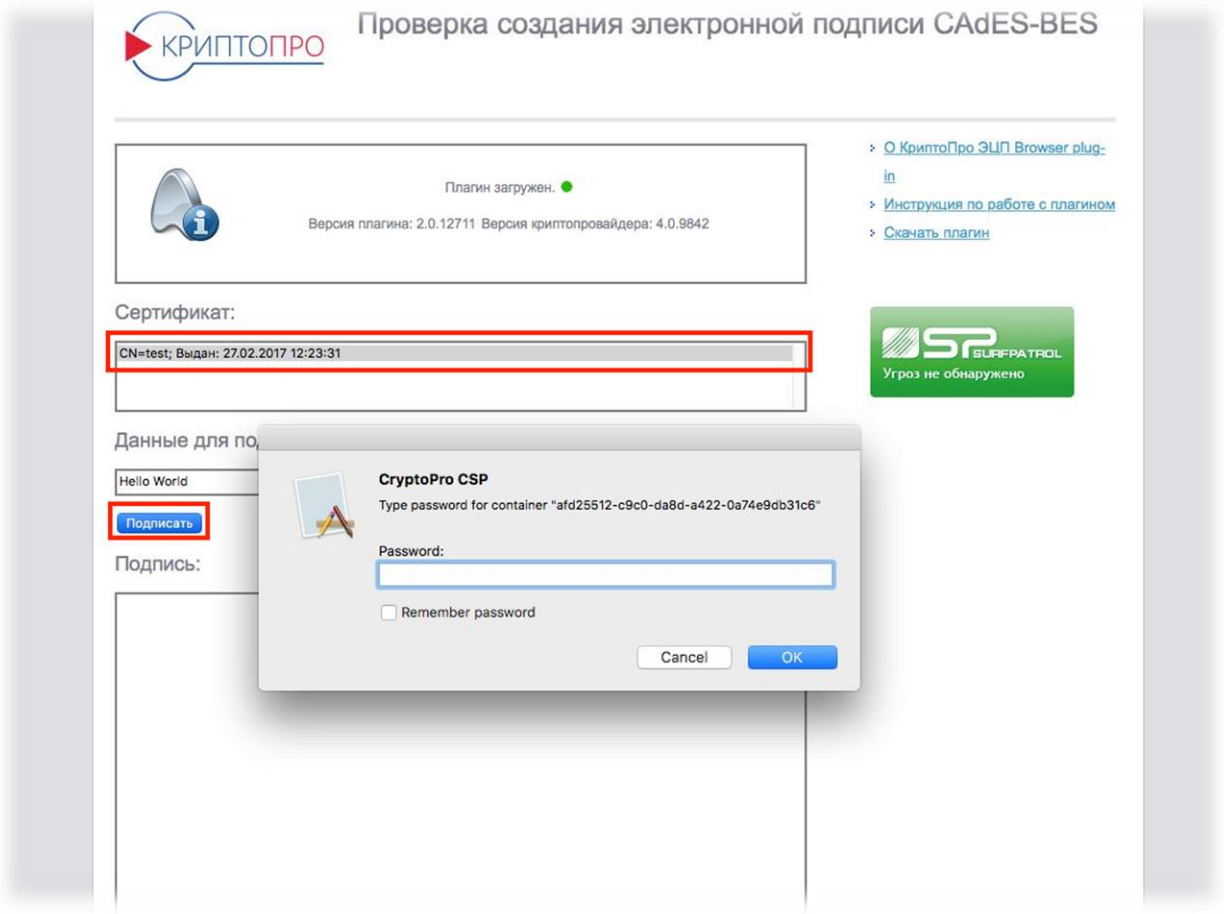

Выбор типа подписи. Используется пример CAdES-BES



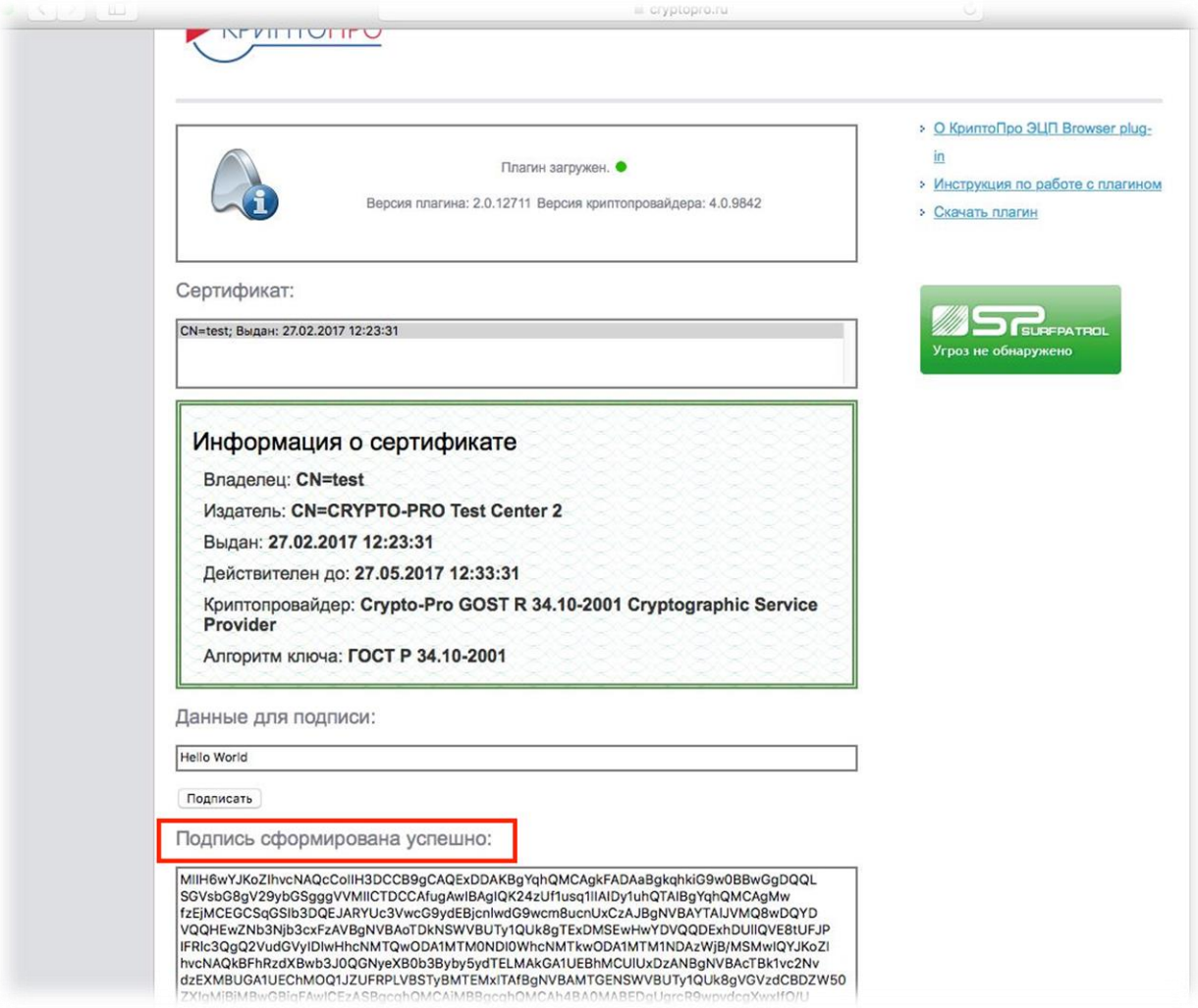
В появившемся окне будет отображено состояние и версия плагина, версия и сборка криптопровайдера, а также доступный для использования сертификат.




Выбрав сертификат, следует нажать на кнопку «Подписать», а затем ввести пароль от контейнера с ключами.

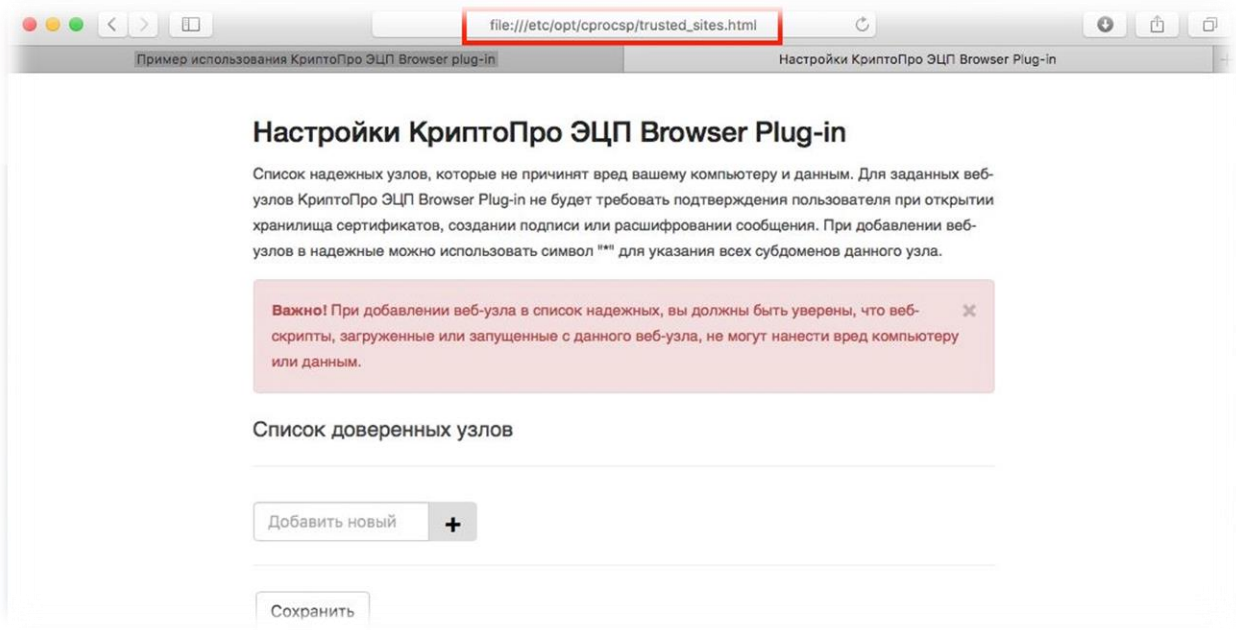


Подпись была успешно сформирована.

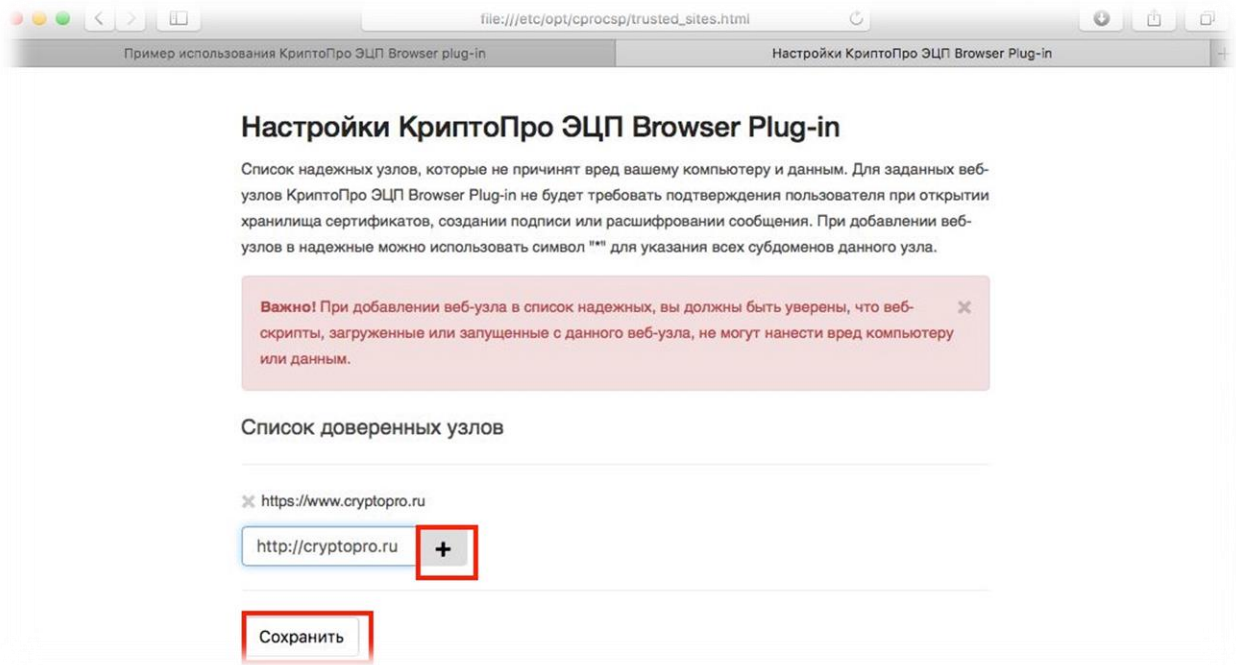


# Внесение сайтов в перечень доверенных

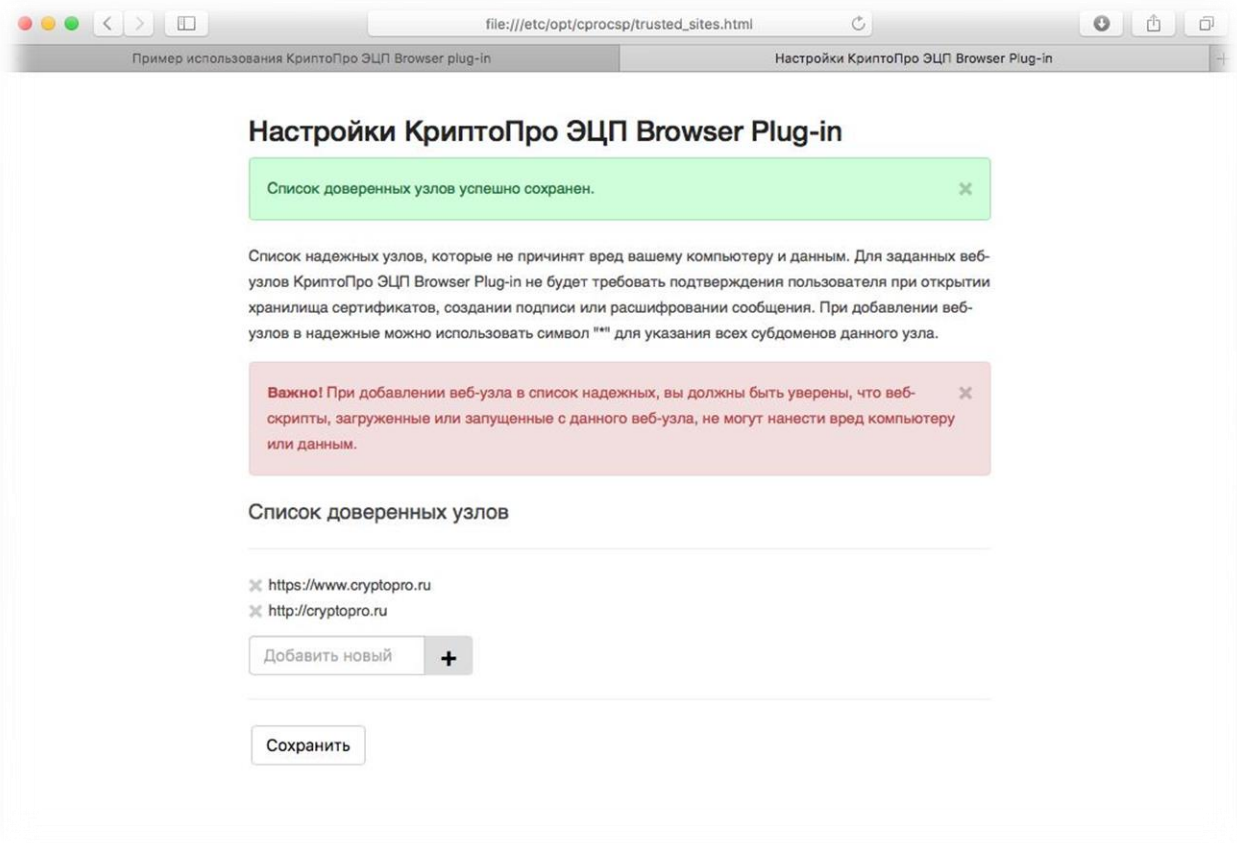
Перечень доверенных сайтов содержится в файле /etc/opt/cprocsp/trusted_sites.html




Следует ввести адрес сайта в соответствующее поле, затем нажать **+** и кнопку «Сохранить»



Отобразиться уведомление об успешном сохранении.

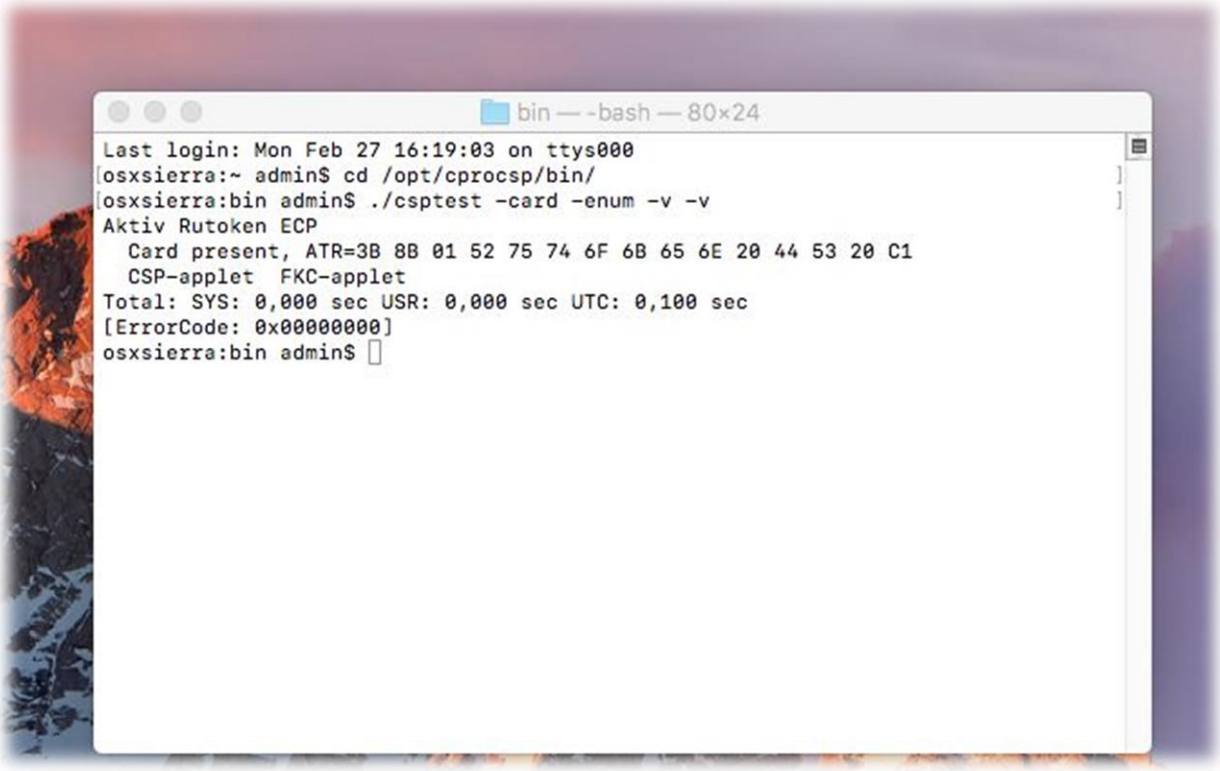


## Работа с ключевым носителем Рутокен ЭЦП

В описанном выше примере контейнер формировался на жестком диске ПК. В качестве ключевых носителей на macOS поддерживаются различные токены и смарт-карты. С полным перечнем можно ознакомиться в руководстве администратора безопасности macOS из архива документации к криптопровайдеру. В данном примере будет использоваться Рутокен ЭЦП.

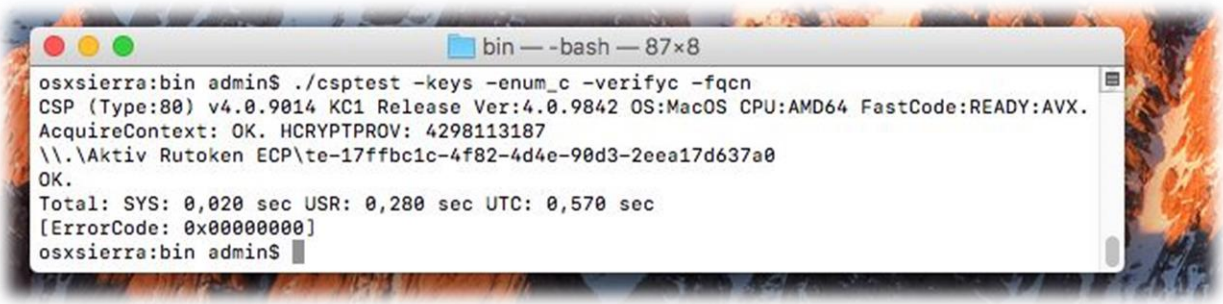
Подключив токен к ПК, убедиться в доступности ключевого носителя можно командой

./csptest –card –enum –v –v




Просмотреть доступные контейнеры можно командой

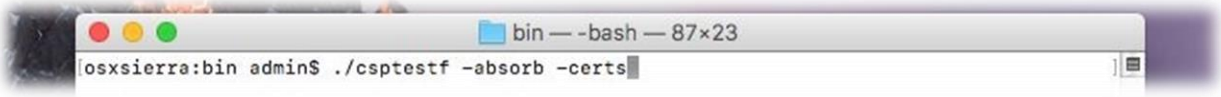
./csptest –keys –enum_c –verifyc –fqcn

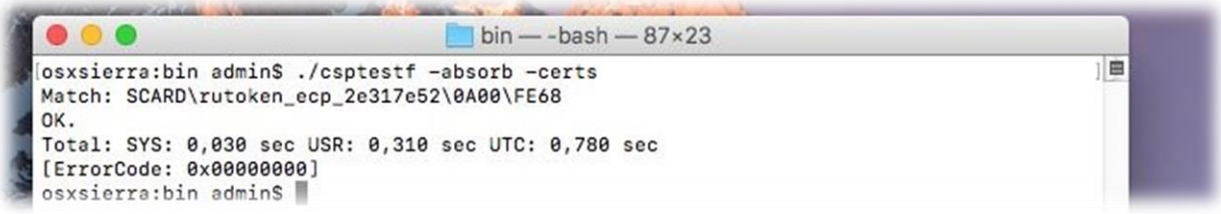


Установить личный сертификат с привязкой к закрытому ключу можно командой

./csptestf –absorb –certs

Будет произведена установка сертификатов из всех доступных контейнеров

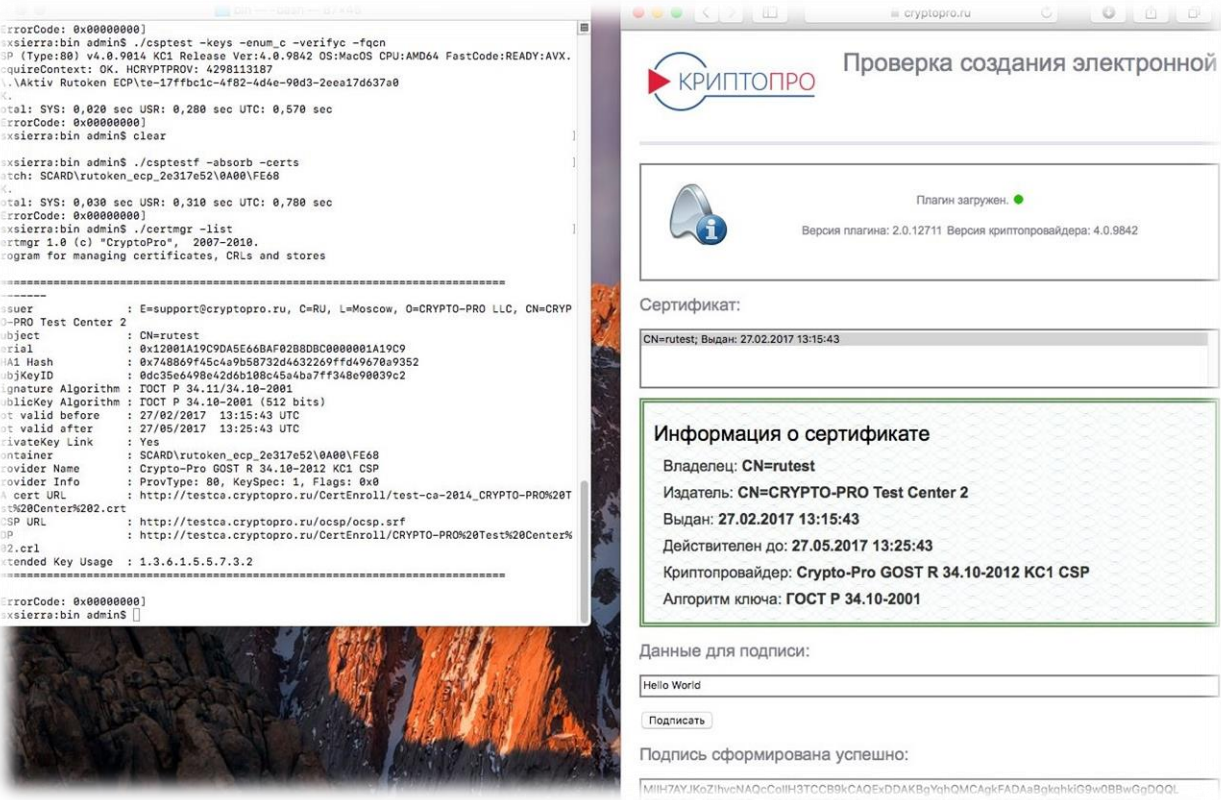



Либо же можно использовать команду ./certmgr –inst –cont ‘имя_контейнера’

Проверить правильность установки можно командой ./certmgr –list

Далее можно снова открыть страницу проверки работы плагина, убедиться, что установленный сертификат присутствует в перечне доступных и осуществить подпись.



В данном примере корневой сертификат удостоверяющего центра был установлен ранее. Если цепочка доверия не строится (отсутствует корневой, или промежуточные сертификаты ) личный сертификат в перечне доступных на странице проверки работы КриптоПро ЭЦП Browser plug-in отображен не будет.