Программный комплекс «Web - Смета»

Инструкция пользователя по настройке и использованию электронной подписи

Версия 1.01

2019 г.

Оглавление

1. Аннотация

Настоящий документ «Инструкция пользователя по настройке и использованию электронной подписи» (далее - Инструкция) предназначен для администраторов безопасности и операторов, осуществляющих работу с предметными решениями, разработанными ООО «НПО «Криста» на основе Web-Сметы (далее, Платформа).

В документе описывается порядок действий пользователя направленный на формирование окружения и обеспечение условий работы модуля «Электронная подпись» (далее, МЭП) в предметных решениях (далее, Система).

Функционал МЭП позволяет:

- Создавать/проверять электронную подпись данных в Системе;
- Аутентифицировать пользователей Системы по сертификату ключа электронной подписи.

Для работы с МЭП в общем случае потребуется выполнение следующих действий:

- Скачивание и установка СКЗИ КриптоПро CSP 4.0;
- Скачивание и установка в соответствующие хранилища корневых и промежуточных сертификатов удостоверяющего центра, где была получена подпись;
- Подключение ключевого носителя к компьютеру и установка личного сертификата;
- Скачивание и установка плагина WorkspaceCrypto;
- Установка приложения WorkspaceCryptoHost.

МЭП функционирует в среде Windows/Linux и поддерживается работа в следующих браузерах: применим в следующих браузерах: Mozilla Firefox, Opera, Google Chrome.

2. Установка средств криптографической защиты информации

Для использования МЭП, на рабочем месте должно быть установлено средство криптографической защиты информации (далее, СКЗИ).

Платформа поддерживает работу СКЗИ КриптоПро CSP (см. Установка КриптоПро CSP).

СКЗИ обеспечивает выполнение следующих функций:

- авторизация и обеспечение юридической значимости электронных документов при обмене ими между пользователями посредством использования процедур формирования и проверки электронной подписи;
- обеспечение конфиденциальности и контроля целостности информации;
- создание и управление ключевой информацией.

2.1. Установка КриптоПро CSP

2.1.1. Загрузка дистрибутива программы КриптоПро CSP

1. Открыть главную страницу сайта ООО КРИПТО-ПРО - https://www.cryptopro.ru/;
2. Авторизоваться на сайте, введя в форму аутентификации e-mail (логин) и пароль пользователя (См. Рисунок 1):

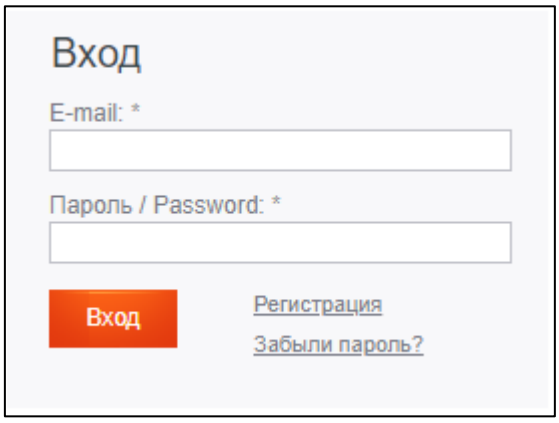


Рисунок 1. Форма аутентификации КриптоПро

Если пользователь не зарегистрирован, то необходимо выполнить процедуру регистрации на сайте ООО КРИПТО-ПРО.

3. Открыть «Центр загрузки КриптоПро».

Примечание. *Страница «Центра загрузки КриптоПро» находится на сайте ООО КРИПТО-ПРО, доступна по адресу: https://www.cryptopro.ru/downloads*

Примечание. *Функционал работы с «Центром загрузки КриптоПро» доступен после авторизации на сайте ООО КРИПТО-ПРО - https://www.cryptopro.ru/.*

---

4. Выбрать пункт «*КриптоПро CSP*»

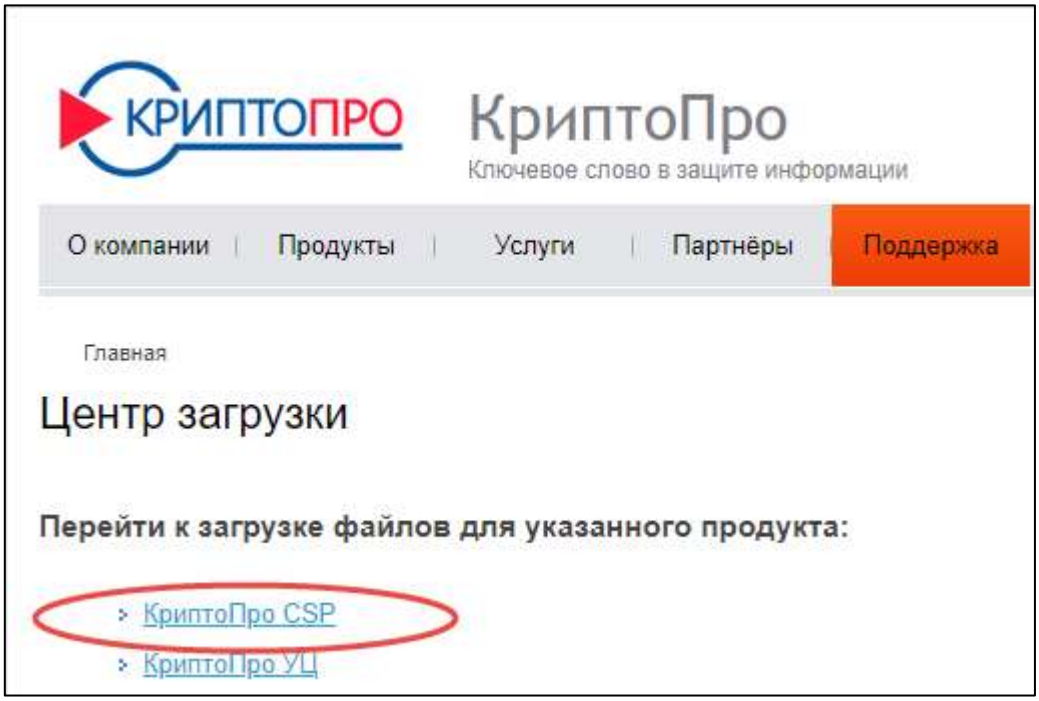


Рисунок 2. Страница «Центр загрузки»

Будет выполнен переход на страницу с лицензионным соглашением для продукта КриптоПро CSP.

5. После ознакомления с лицензионным соглашением для продолжения загрузки дистрибутива необходимо нажать кнопку «*Я согласен с Лицензионным соглашением. Перейти к загрузке*»:

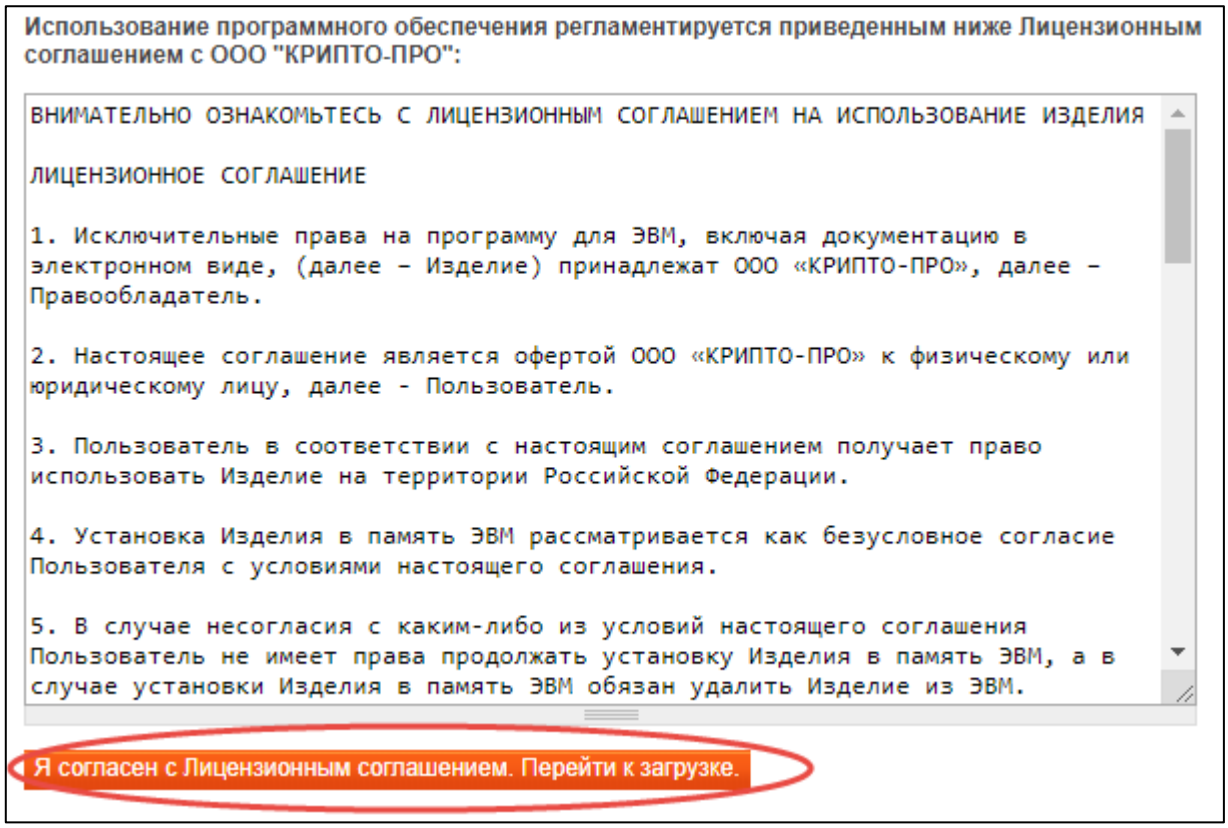


Рисунок 3. Лицензионное соглашение продукта КриптоПро CSP

6. После нажатия на кнопку «*Я согласен с Лицензионным соглашением. Перейти к загрузке*» будет осуществлен переход на страницу с перечнем дистрибутивов доступных для загрузки:

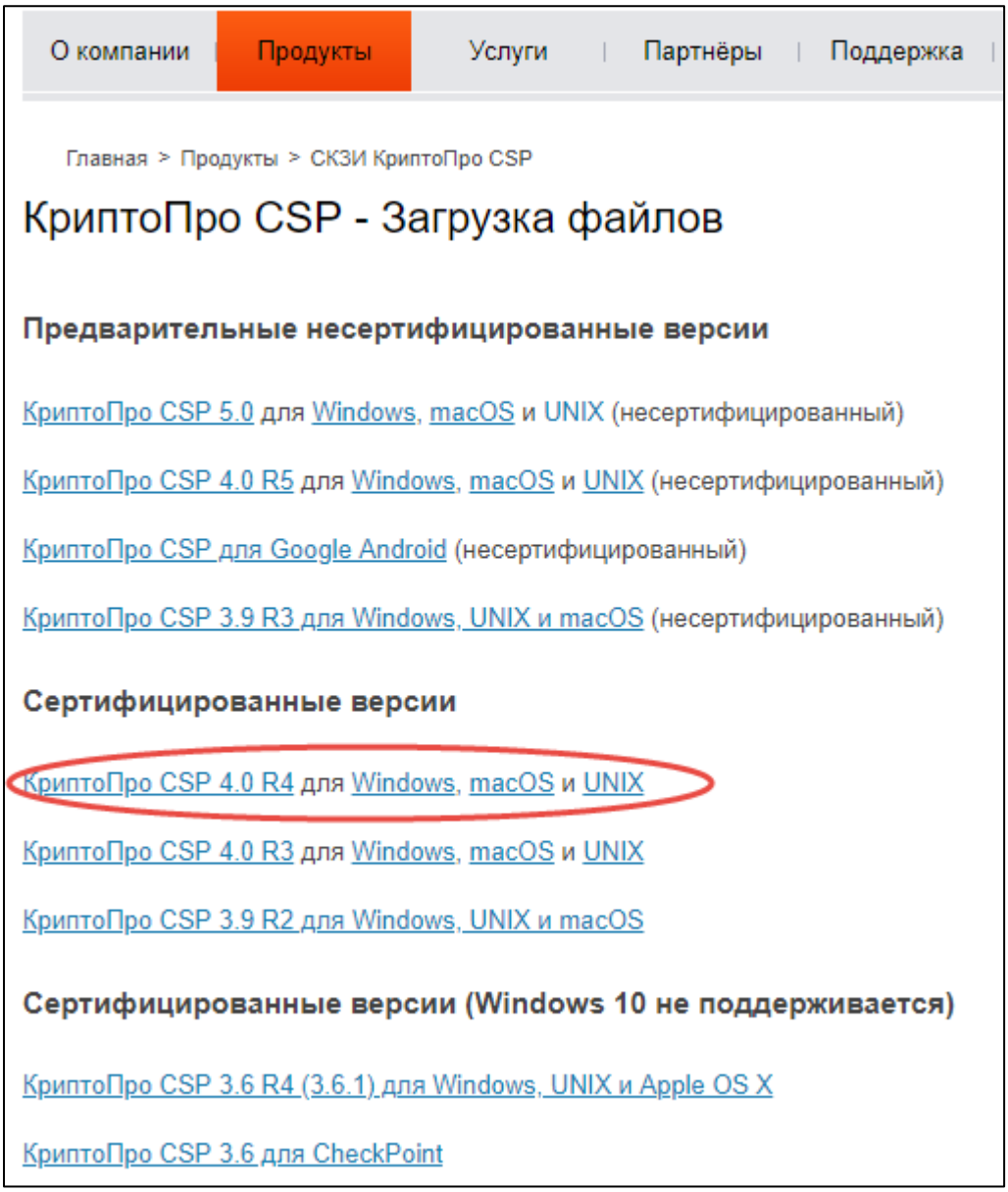


Рисунок 4. Страница с перечнем дистрибутивов для загрузки

7. Необходимо выбрать последнюю сертифицированную версию КриптоПро CSP, соответствующую операционной системе установленной на рабочем месте пользователя (Windows, либо Linux). После выбора версии дистрибутив программы будет загружен на компьютер пользователя.

Примечание. *При выборе ссылки «Windows» будет загружен исполняемый файл «CSPSetup.exe». При выборе Linux в зависимости от установленного менеджера пакетов и разрядности ОС (32-разрядная или 64-разрядная) необходимо загрузить либо *.deb (x86/x64) либо *.rpm (x86/x64). После выбора установочного пакета будет загружен архив. Пример загружаемого файла 64-разрядной системы с менеджером пакетов dpkg: linux-amd64_deb.tgz*

2.1.2. Установка КриптоПро CSP

Примечание. *Установка дистрибутива КриптоПро CSP должна производиться пользователем, имеющим права администратора.*

1. Установка КриптоПро CSP начинается с запуска, скачанного на предыдущем шаге дистрибутива программы. Перед запуском мастера установки выводится диалоговое окно, в котором доступен выбор уровня защищенности (параметр *Дополнительные опции*):

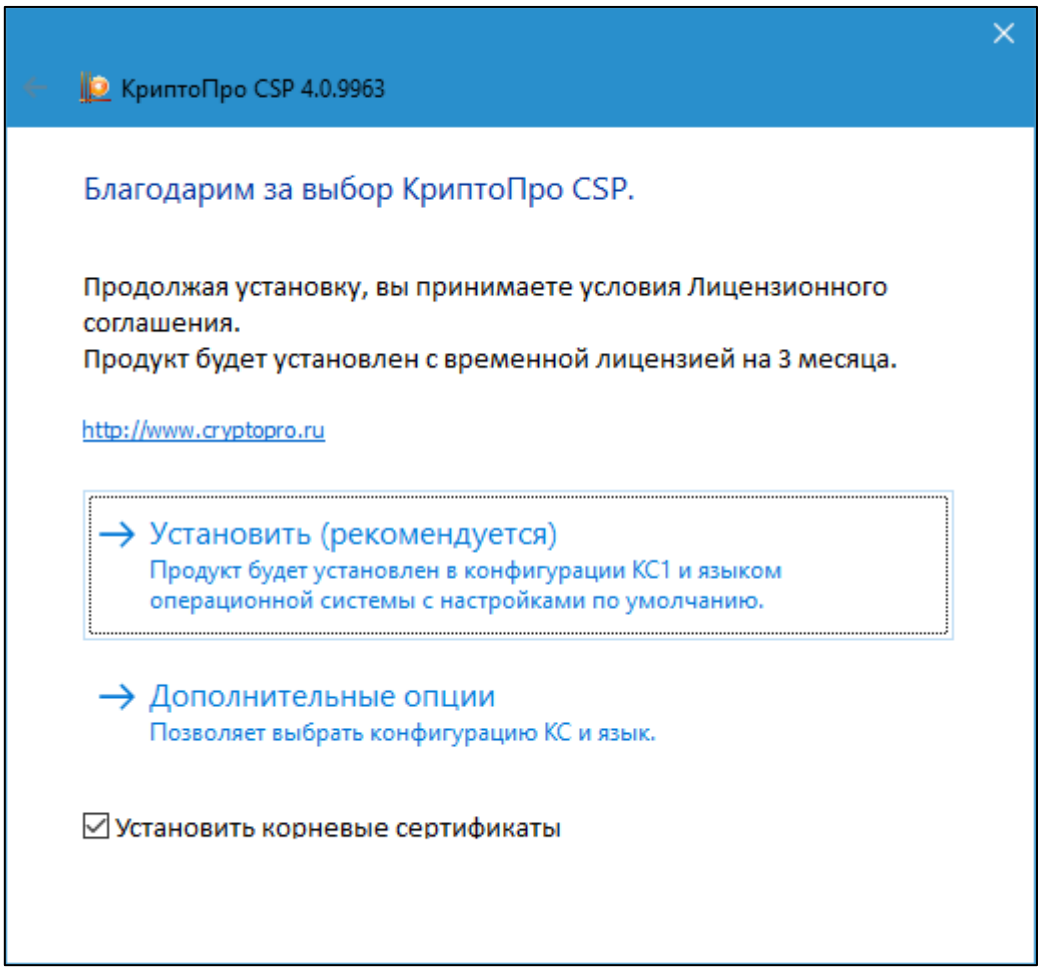


Рисунок 5. Страница мастера установки в ОС Windows 10

Укажите требуемый уровень безопасности, если он отличается от значения по умолчанию.

Для Linux необходимо распаковать архив и установить компоненты. Пример порядка установки для Ubuntu:

```
sudo dpkg -i ./lsb-cprocsp-base_4.0.9963-5_all.deb
sudo dpkg -i ./lsb-cprocsp-rdr-64_4.0.9963-5_amd64.deb
sudo dpkg -i ./lsb-cprocsp-kc1-64_4.0.9963-5_amd64.deb
sudo dpkg -i ./lsb-cprocsp-capilite-64_4.0.9963-5_amd64.deb
sudo dpkg -i ./lsb-cprocsp-kc2-64_4.0.9963-5_amd64.deb
sudo dpkg -i ./cprocsp-rdr-gui-gtk-64_4.0.9963-5_amd64.deb
```

Подробно процесс установки дистрибутива описан в документации КриптоПро CSP:

- ЖТЯИ.00087-03 92 01. КриптоПро CSP. Инструкция по использованию СКЗИ под управлением ОС Windows. 2018. С. 5;
- ЖТЯИ.00087-03 91 03. СКЗИ КриптоПро CSP. Руководство администратора безопасности. Использование СКЗИ под управлением ОС Linux. 2018. С. 7.

Примечание. *Документация КриптоПро CSP доступна по адресу: https://www.cryptopro.ru/products/csp/downloads и содержится в разделе соответствующей версии приложения выбранного пользователем.*

Примечание. *При установке программного обеспечения «КриптоПро CSP» без ввода лицензии пользователю предоставляется лицензия с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).*

Пример. *Установка лицензии в Linux:*
Перейти в рабочий каталог программы: `cd /opt/cprocsp/sbin/amd64/`
Установить лицензию: `./cpconfig -license -set XXXXX-XXXXX- XXXXX- XXXXX-XXXXX`

2.1.3. Установка корневого сертификата

В зависимости от принятой в организации политики безопасности в целях обеспечения контроля доверенности сертификатов открытых ключей, при использовании СКЗИ под управлением ОС Windows/Linux, может потребоваться установка корневого сертификата в доверенное хранилище.

Корневой сертификат предоставляется соответствующим удостоверяющим центром, выбранным для формирования электронной подписи.

Для Windows установка сертификатов осуществляется с помощью мастера импорта сертификатов.

Для Linux пример установки корневого сертификата, промежуточных сертификатов и списка отзывов:

```
Переходим в рабочий каталог: cd /opt/cprocsp/bin/amd64
./certmgr -inst -file [path_to_file]/certnew.cer -store uRoot
./certmgr -inst -all -file [path_to_file]/certnew.p7b -store uRoot
./certmgr -inst -crl -store uRoot -file [path_to_file]/certcrl.crl
```

Подробнее порядок установки корневого сертификата описан в документе:

- Для ОС Windows ЖТЯИ.00087-03 92 01. КриптоПро CSP. Инструкция по использованию, ч. 4.3., С. 56;
- Для ОС Linux ЖТЯИ.00087-03 93 02. Приложение командной строки для работы с сертификатами, ч. 2., С. 7.

Примечание. *Корневые и промежуточные сертификаты устанавливаются автоматически в соответствующие хранилища, если на этапе «Установка личного сертификата» сертификат устанавливается с помощью панели управления СКЗИ КриптоПро CSP, при условии что они содержатся в контейнере закрытого ключа.*

2.1.4. Установка личного сертификата

Для работы с МЭП необходимо установить пользовательский сертификат в локальное хранилище и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

Для Windows установка личного сертификата осуществляется через панель управления СКЗИ КриптоПро CSP.

Для Linux пример установки личного сертификата:

Пример для тестового контейнера и HDIMAGE:
Скачиваем тестовый контейнер и сертификат с тестового УЦ (https://www.cryptopro.ru/certsrv/) и распаковываем.
Копируем контейнер с закрытым ключем в HDIMAGE: cp ./le-820ae.000 -R /var/opt/cprocsp/keys/$USER/
Переходим в рабочий каталог: cd /opt/cprocsp/bin/amd64
Связываем сертификат и контейнер (пароль для контейнера 12345678): ./certmgr -inst -store uMy -file [path_to_file]/And.cer -cont '\\.\HDIMAGE\le-820aed1b-8eb2-4d3b-a02e-9b65f7682ac5'
Смотрим список сертификатов хранилища My: ./certmgr -list -store uMy

Порядок установки личного сертификата описан в документе:

- Для ОС Windows ЖТЯИ.00087-03 92 01. КриптоПро CSP. Инструкция по использованию, ч. 2.5.2., С. 33;
- Для ОС Linux ЖТЯИ.00087-03 93 02. Приложение командной строки для работы с сертификатами, ч. 2., С. 7.

3. Установка плагина WorkspaceCrypto

WorkspaceCrypto является плагином для веб-браузера, благодаря которому у пользователя появляется возможность подписывать документы электронной подписью. Плагин обеспечивает возможность аутентифицироваться в приложении по сертификату ключа электронной подписи.

Плагин WorkspaceCrypto применим в следующих браузерах:

- Mozilla Firefox
- Opera
- Google Chrome

Плагин WorkspaceCrypto загружается из интернет-магазина соответствующего браузера. В исключительных ситуациях, когда плагин не доступен в интернет-магазине, загрузка осуществляется: https://www.ssksoft.ru/public/WorkspaceCrypto/latest/browser-extensions.zip.

Установка плагина будет выполнена на примере браузера Google Chrome. Установка плагина на других браузерах происходит аналогичным образом с учетом специфики этих браузеров.

WorkspaceCrypto использует нативное приложение WorkspaceCryptoHost для взаимодействия для Windows CryptoAPI. WorkspaceCryptoHost – это хост-приложение, которое обеспечивает подписание ЭП посредством провайдеров Крипто-про CSP и VipNet CSP. Реализует поддержку алгоритмов цифровой подписи «XMLDSig» и «CMS detached». Для корректной работы приложения необходимо наличие установленного в системе крипто-провайдера (КриптоПро).

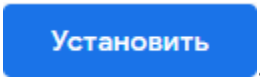
Примечание. *Если плагин WorkspaceCrypto и приложение WorkspaceCryptoHost установлено, то необходимо перейти в раздел 4. Наличие установленных плагинов проверяется в браузере на странице «Расширения». Наличие установленных приложений в «Параметры Windows» в разделе «Приложения и возможности» для ОС Windows 8+*

или в меню «Программы и компоненты» для более ранних версий ОС Windows.

3.1. Установка плагина WorkspaceCrypto и приложения WorkspaceCryptoHost

3.1.1. Установка из интернет-магазина

Для установки плагина необходимо выполнить следующие шаги:

1. Запустить браузер.
2. Открыть интернет-магазин:
   a. для Google Chrome - https://chrome.google.com/webstore/
   b. для Mozilla Firefox - https://addons.mozilla.org/ru/firefox/
   c. для Opera - https://addons.opera.com/ru/
3. В строке поиска расширений ввести название плагина – WorkspaceCrypto. Выполнить поиск. В результате поиска будет найдено расширение WorkspaceCrypto.
4. На странице будет доступна кнопка добавления расширений в браузер 

. Для установки плагина нажимаем кнопку «Установить», далее браузер без участия пользователя установит расширение. После установки в меню браузера будет добавлена кнопка . Восклицательный знак в красном треугольнике означает, что на РМ не установлено приложение WorkspaceCryptoHost. Порядок установки приложения описан в разделе 3.2. Установка приложения WorkspaceCryptoHost.

3.1.2. Оффлайн установка

Примечание. *Для плагина WorkspaceCrypto установленного оффлайн не доступно автоматическое обновление. В таком случае обновление производится пользователем вручную, в соответствии с инструкциями, описанными в текущем разделе.*

Для установки плагина необходимо выполнить следующие шаги:

1. Скачать архив с дистрибутивами плагина: https://www.ssksoft.ru/public/WorkspaceCrypto/latest/browser-extensions.zip.

Примечание. *В архиве содержится несколько файлов:*

workspacecrypto-1.0-chrome.crx *– файл установки для браузера Chrome*
workspacecrypto-1.0-firefox.zip *– архив с файлами установки для браузера FireFox*
workspacecrypto-1.0-opera.crx *- файл установки для браузера Chrome*

2. Запустить браузер.
3. Открыть страницу «*Расширения*» (*chrome://extensions/*).
4. Включить «*Режим разработчика*»:

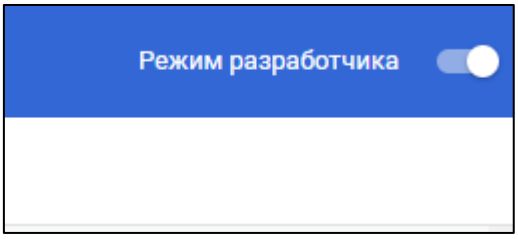


Рисунок 6. Флаг-галка включения параметра «Режим разработчика»

5. Распаковать архив browser-extensions.zip полученный на шаге 1.
6. Перетащить файл workspacecrypto-1.0-chrome.crx на страницу расширений браузера и подтвердить установку приложения:

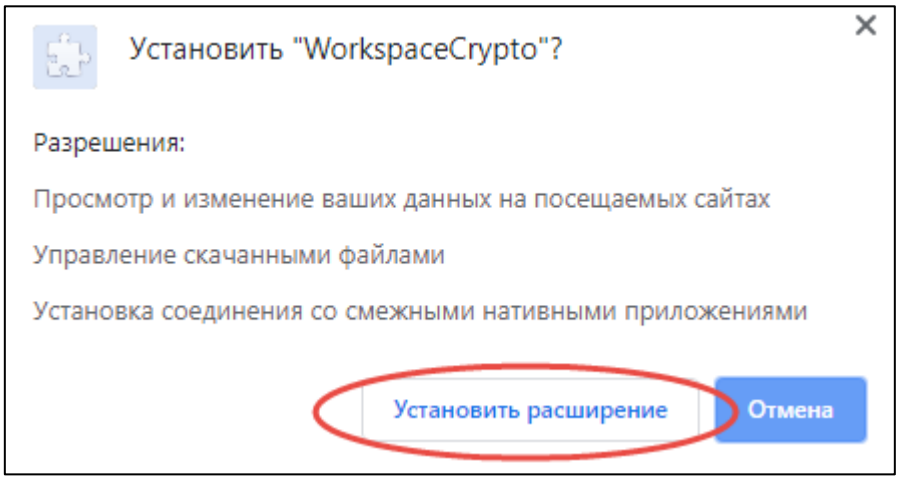


Рисунок 7. Окно подтверждения установки приложения

После установки в меню браузера будет добавлена кнопка «». Восклицательный знак в красном треугольнике означает, что на РМ не установлено приложение WorkspaceCryptoHost. Порядок установки приложения описан в разделе 3.2. Установка приложения WorkspaceCryptoHost.

3.2. Установка приложения WorkspaceCryptoHost

1. После установки плагина осуществляется автоматическая проверка на наличие установленного приложения WorkspaceCryptoHost. Если приложение не установлено, то пользователю будет предложено установить его:

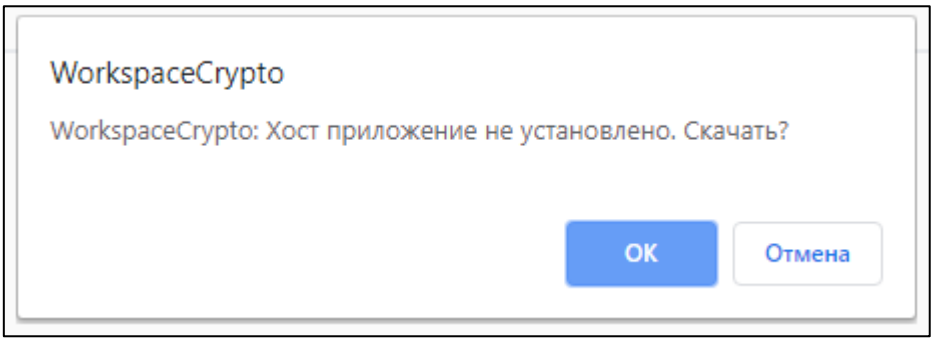


Рисунок 8. Ссылка на дистрибутив приложения WorkspaceCryptoHost

2. Далее, в окне уведомления необходимо нажать кнопку OK, после чего будет загружена последняя версия приложения WorkspaceCryptoHost.
3. Запустить загруженный инсталлятор WorkspaceCryptoHost.exe. Откроется окно мастера установки:

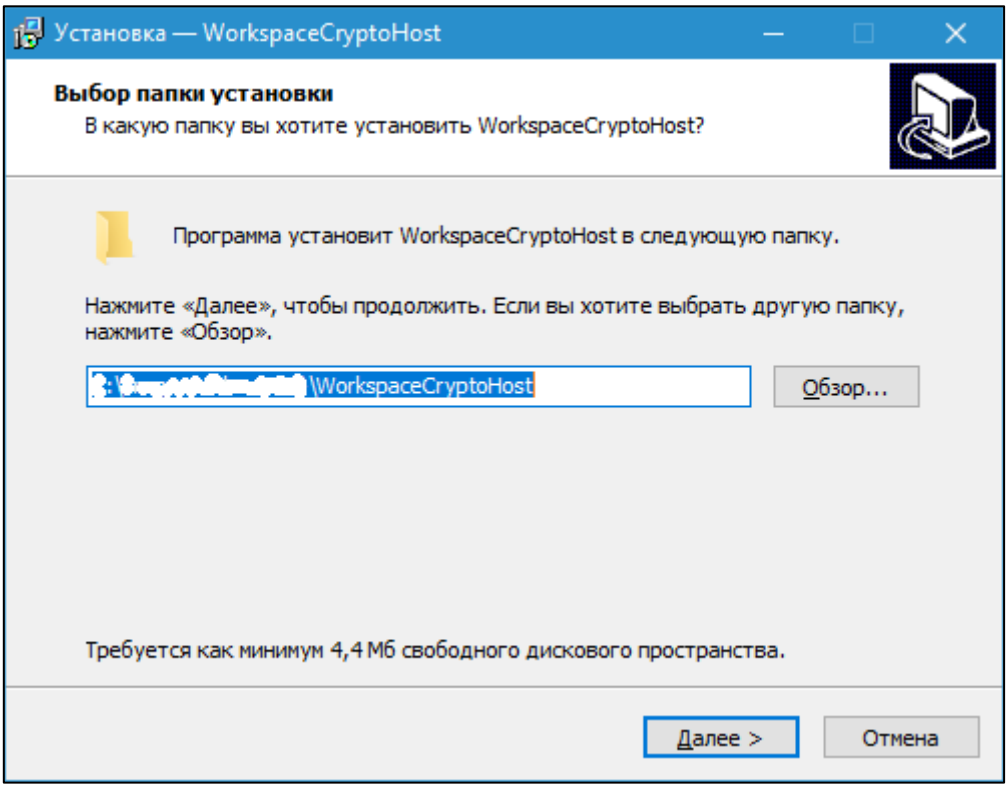


Рисунок 9. Окно мастера установки приложения WorkspaceCryptoHost

В мастере установки все параметры принимаются по умолчанию. После установки приложения WorkspaceCryptoHost кнопка приложения в меню браузера должна принять следующий вид «».

3.3. Обновление приложения WorkspaceCryptoHost

Для обновления установленного приложения WorkspaceCryptoHost необходимо выполнить следующие шаги:

1. Удалить хост-приложение с компьютера через панель управления: *Панель управления\Программы\Программы и компоненты*:

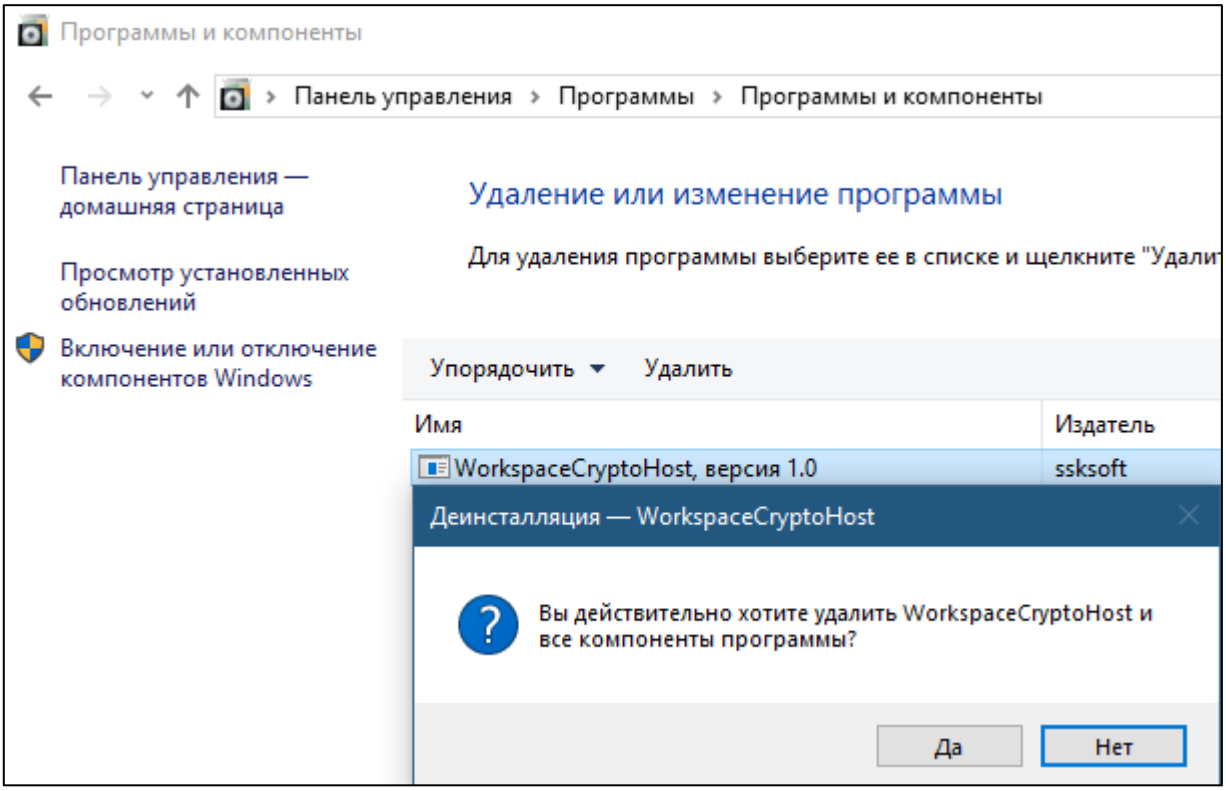


Рисунок 10. Программы и компоненты. Удаление хост-приложения.

2. Выбрать в контекстном меню плагина пункт «*Скачать хост-приложение*»:

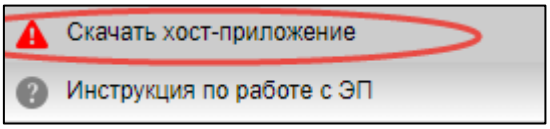


Рисунок 11. Контекстное меню плагина

Выполнится автоматическая загрузка инсталлятора последней версии приложения WorkspaceCryptoHost.

3. После того как будет выгружен инсталлятор приложения WorkspaceCryptoHost необходимо вернуться к шагу «3» пункта «3.2. *Установка приложения WorkspaceCryptoHost*» Инструкции.

4. Проверка функционирования механизмов электронной подписи

Проверить корректную установку окружения необходимого для работы электронной подписи можно на тестовой странице: https://www.ssksoft.ru/workspacecryptotest/

На странице отображается следующая информация:

- Сведения о плагине: установлен/не установлен/версия плагина.
- Установлено или нет хост-приложение и его версию.
- Установлен или нет СКЗИ.
- Какие установлены сертификаты.

Реализована возможность подписания данных с помощью личного сертификата.

Если все настройки были выполнены корректно, то результат проверки на странице будет следующий:

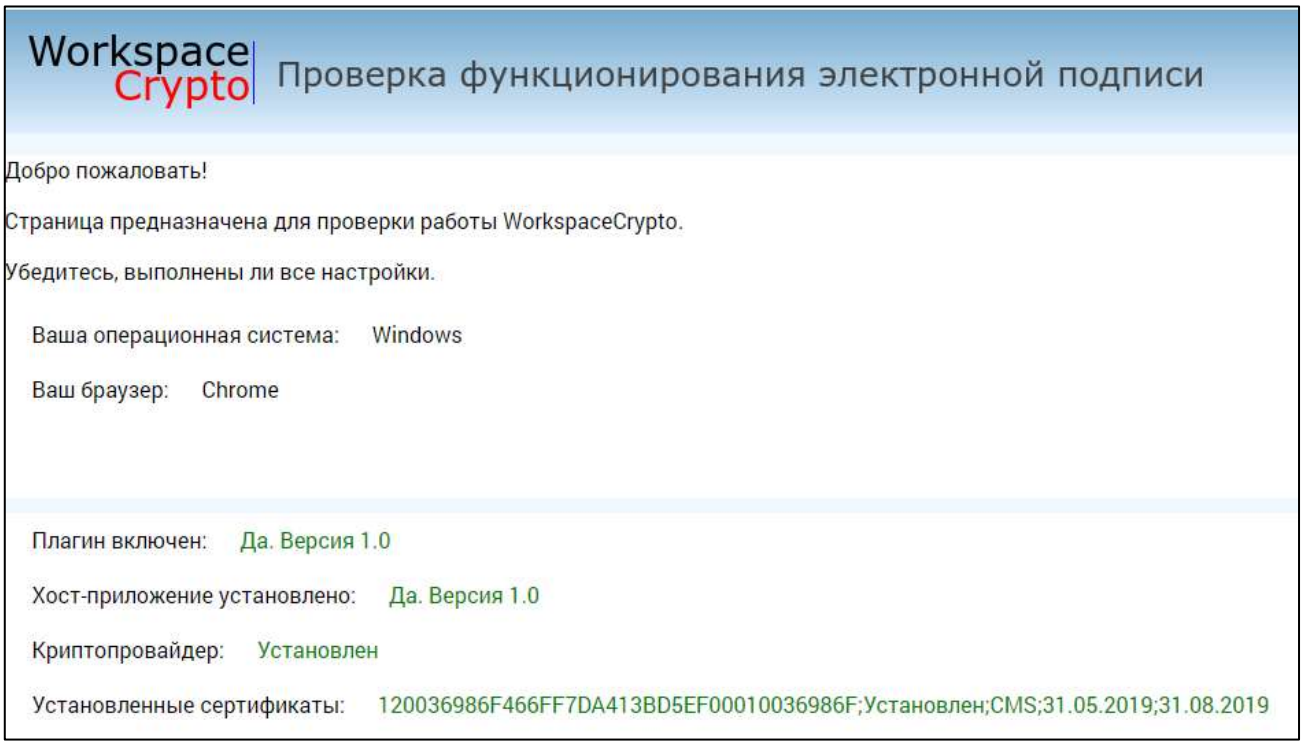


Рисунок 12. Успешное прохождение проверок на тестовой странице

Тестовая страница позволяет определить, на каком этапе возникли проблемы с настройкой окружения.

Пример интерфейса страницы, если плагин не установлен:

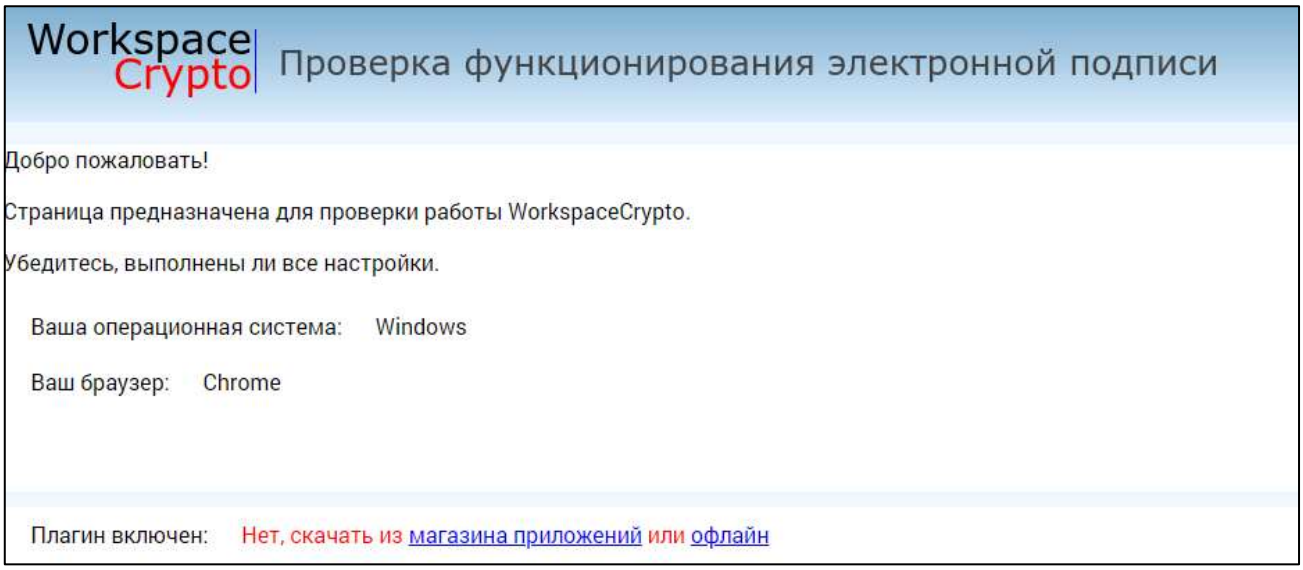


Рисунок 13. Интерфейс тестовой страницы: плагин не установлен.

5. Использование электронной подписи

5.1. Формирование электронной подписи

Формирование электронной подписи осуществляется на запущенном экземпляре Системы. Необходимо открыть интерфейс, для которого включен параметр «Использовать цифровую подпись».

Примечание. *Интерфейсы, для которых включен параметр «Использовать цифровую подпись» выделяются от остальных тем, что у таких интерфейсов на панели кнопок будет доступна кнопка*  *«Цифровая подпись».*

Для наложения электронной подписи необходимо выполнить следующие шаги:

1. Для вызова интерфейса «Подпись» необходимо нажать на кнопку  «Цифровая подпись».

2. Откроется интерфейс «Новая подпись», на котором отображается информация о подписываемом документе в xml-формате. Для формирования электронной подписи необходимо нажать кнопку Подписать.

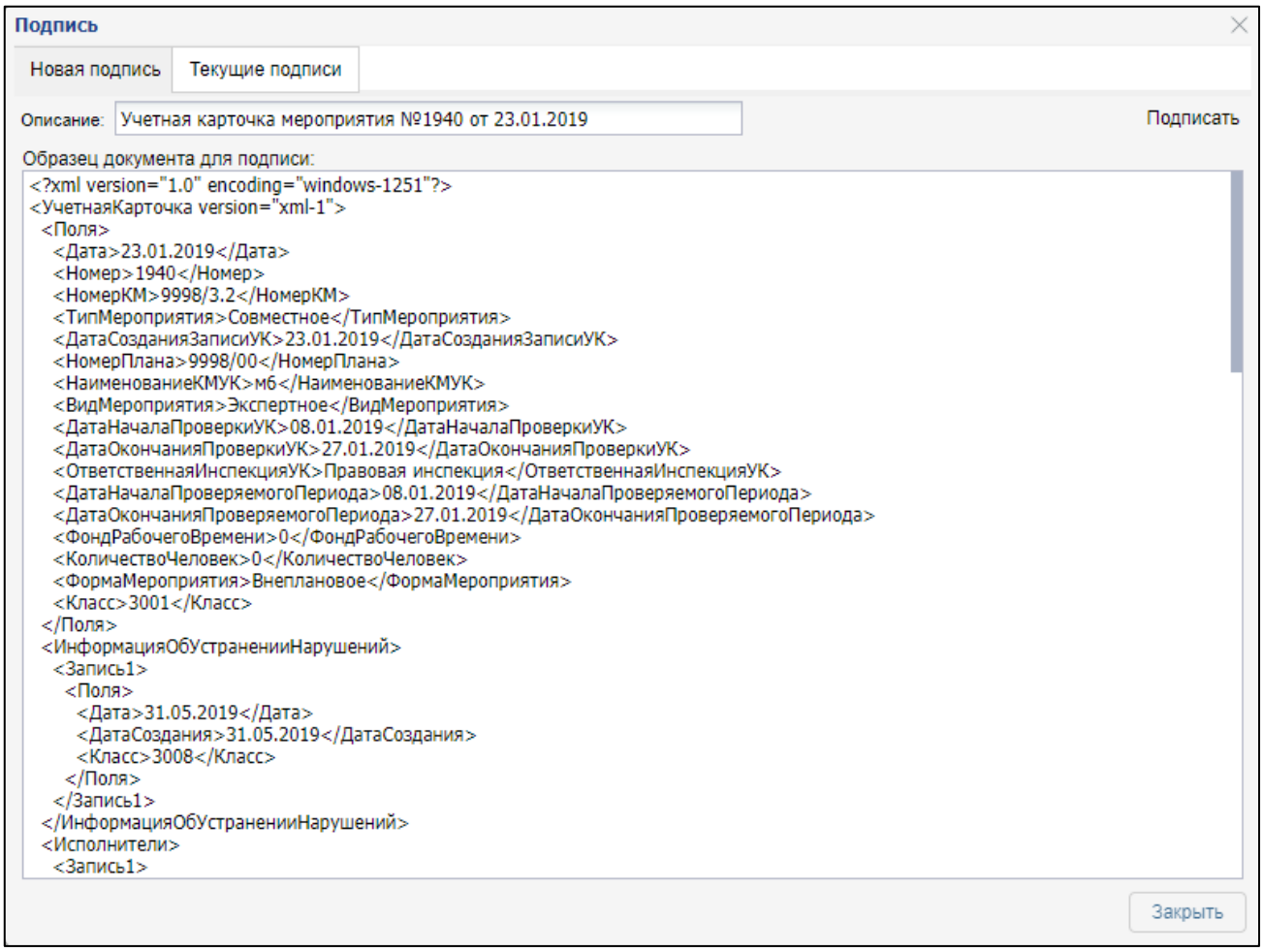


Рисунок 14. Интерфейс «Новая подпись»

3. В окне выбора сертификата для подписи документа необходимо выбрать соответствующий пользователю сертификат.

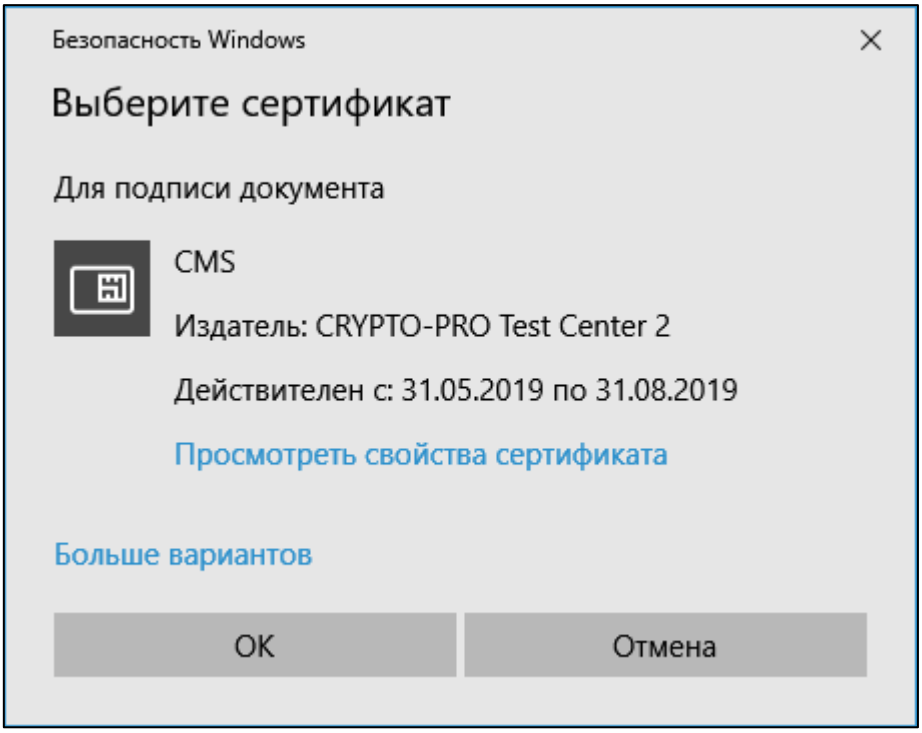


Рисунок 15. Модальное окно выбора сертификата для подписи документа

4. После выбора сертификата для подписи документа будет выведено диалоговое окно, в котором необходимо указать пароль от контейнера с закрытым ключом:

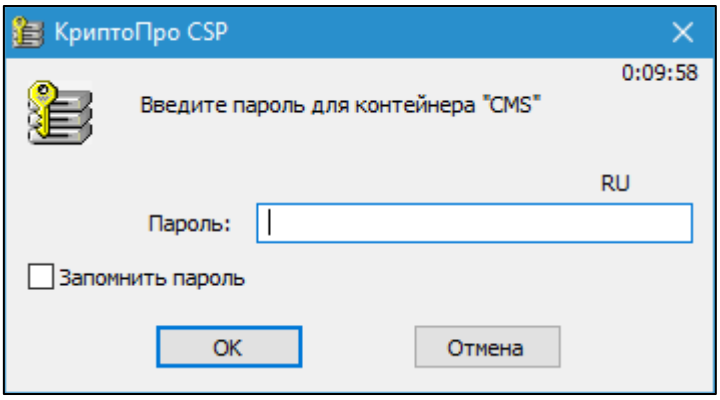


Рисунок 16. Диалоговое окно КриптоПро CSP для ввода пароля от контейнера с закрытым ключом

Для просмотра сведений о подписи документа необходимо открыть закладку «Текущие подписи»:

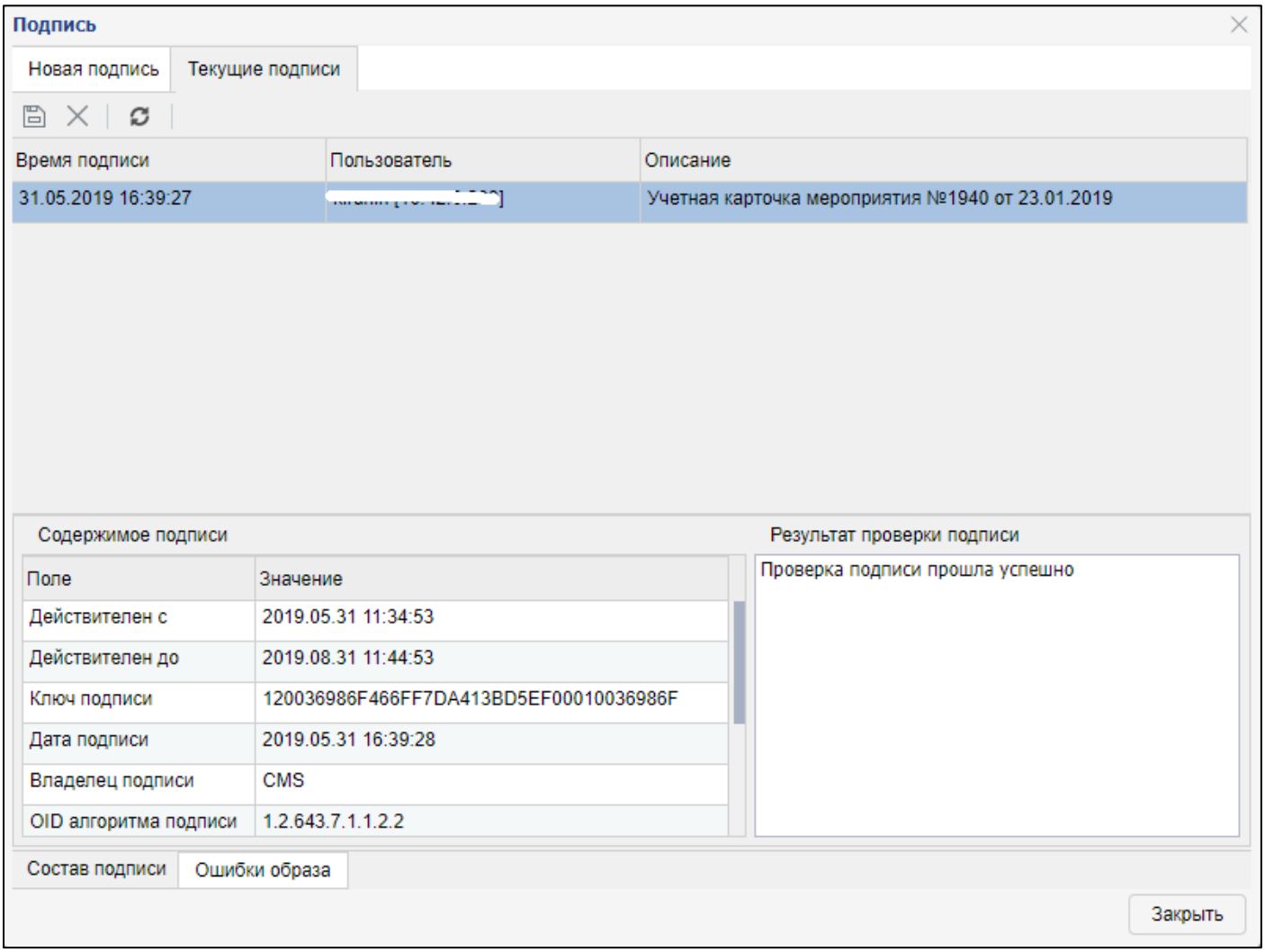


Рисунок 17. Интерфейс «Текущие подписи» положительный результат проверки ЭП

В заголовке окна отображается список подписей. Для каждой подписи выводятся сведения о времени подписи, о пользователе Системы выполнившем операцию «Подписать» и сведения о подписанном документе. В детализации «Состав подписи» отображаются сведения о содержимом подписи и результат проверки подписи. В случае успешного подписания документа в параметре «Результат проверки подписи»: «*Проверка подписи прошла успешно*». Если в результате проверки подписи будут возвращены ошибки, то появится соответствующее сообщение:

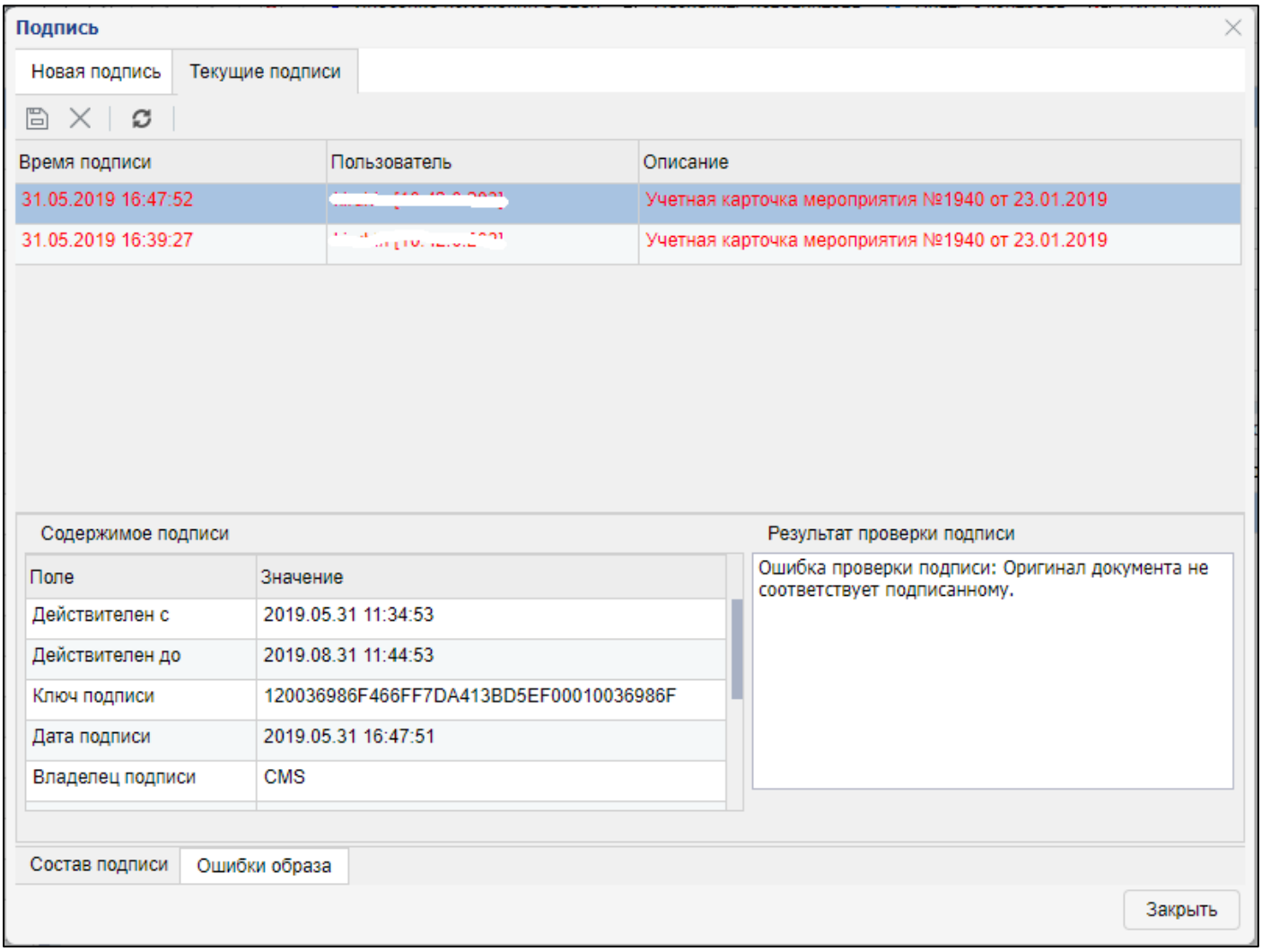


Рисунок 18. Интерфейс «Текущие подписи» ЭП не прошла проверку

Детальная информация об ошибке содержится в детализации «Ошибки образа»:

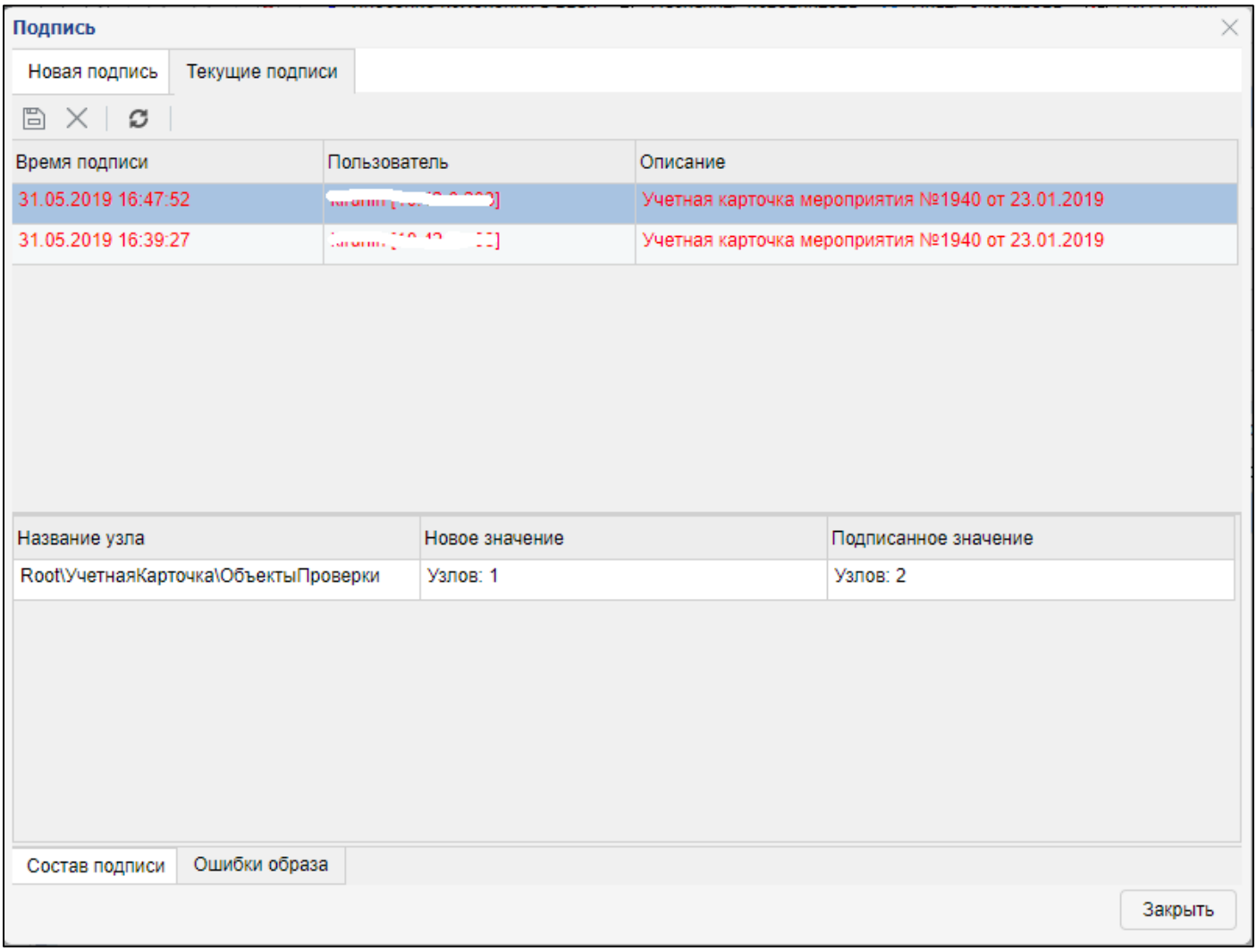


Рисунок 19. Детализация «Ошибки образа»

5.2. Аутентификация с помощью электронной подписи

Для входа в Систему с помощью МЭП необходимо выполнить следующие шаги:

1. Загрузить страницу аутентификации Системы.
2. Нажать на кнопку «Войти по сертификату»:

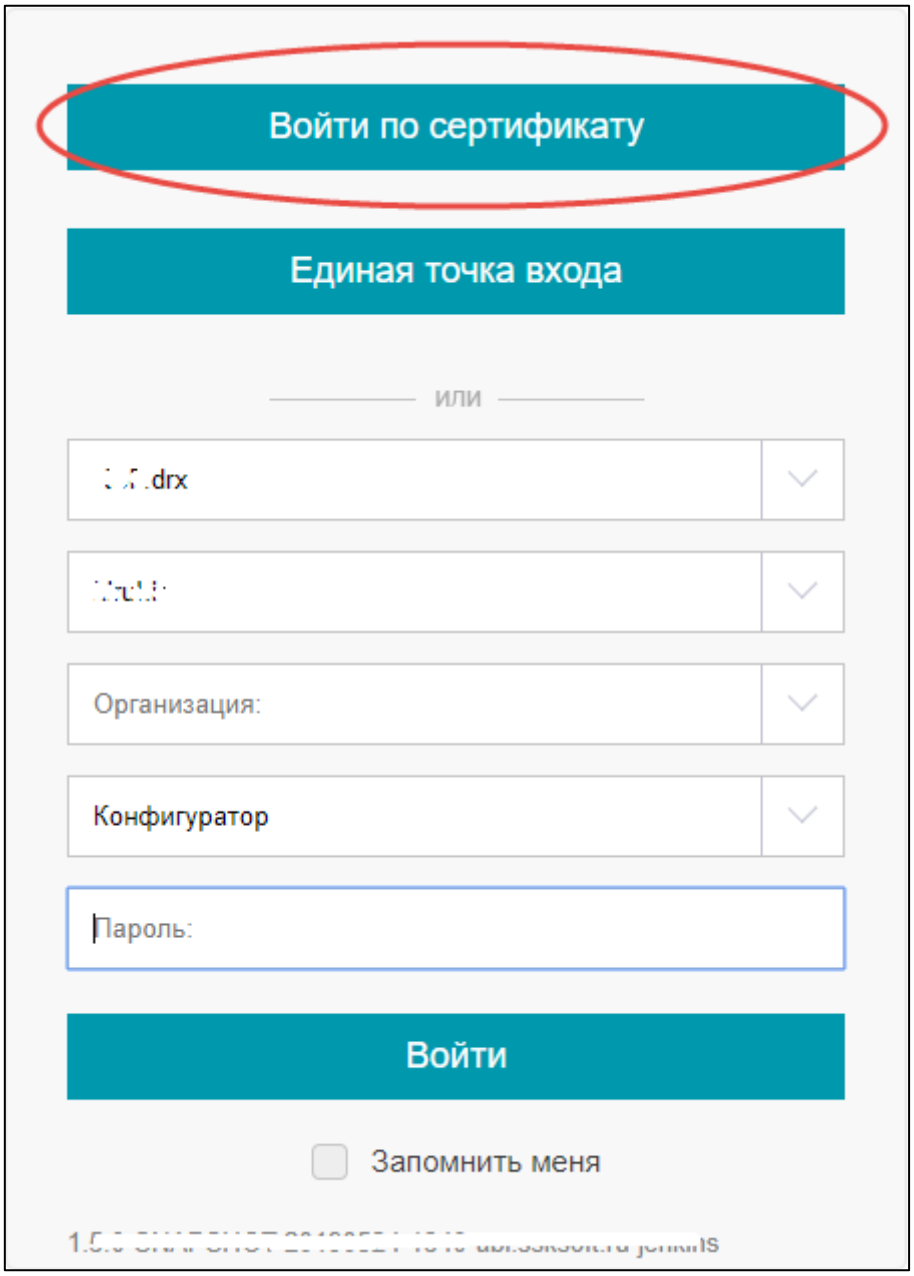


Рисунок 20. Страница аутентификации Системы

3. В окне выбора сертификата необходимо выбрать соответствующий пользователю сертификат.

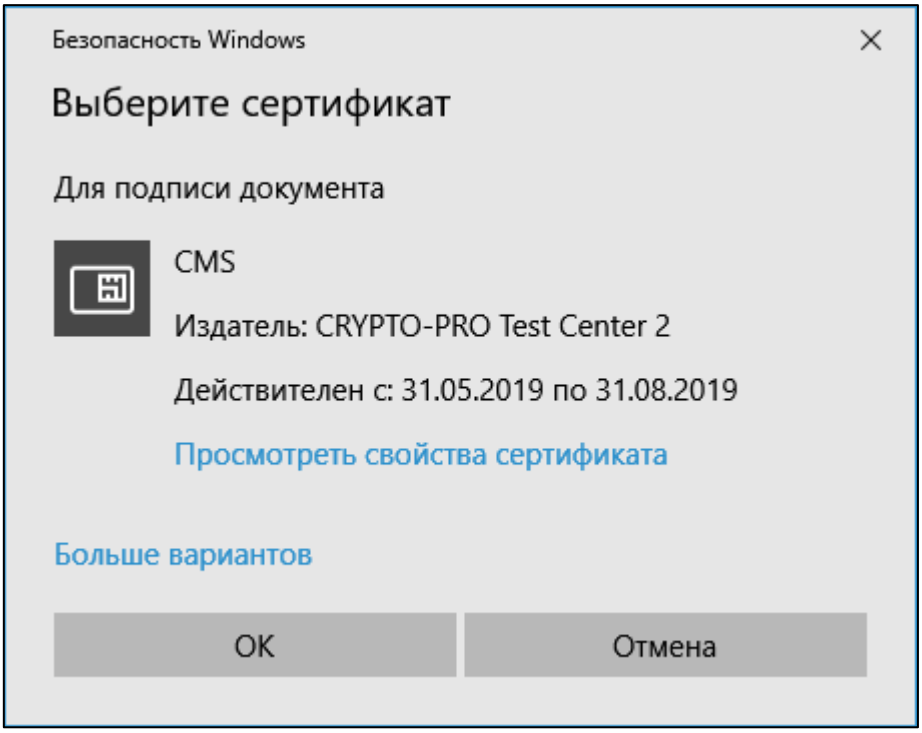


Рисунок 21. Модальное окно выбора сертификата для подписи документа

4. После выбора сертификата будет выведено диалоговое окно, в котором необходимо указать пароль от контейнера с закрытым ключом:

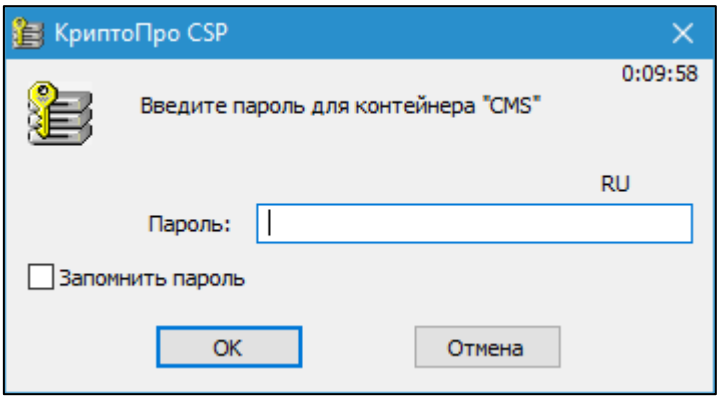


Рисунок 22. Диалоговое окно КриптоПро CSP для ввода пароля от контейнера с закрытым ключом

5. Далее Система выполняет проверку соответствия выбранного сертификата с данными модуля «Безопасность», в котором содержатся сведения о пользователе и его сертификате. После успешного завершения проверки будет открыт интерфейс Системы в соответствии с выбранным рабочим местом на странице аутентификации.

Примечание. *Для аутентификации в Системе с помощью ЭП необходимо, что бы на интерфейсе «Пользователи» в модуле «Безопасность» на закладке «Ключ ЭП» для соответствующего пользователя был загружен личный сертификат и включен флаг-галка «Доступ разрешен».*

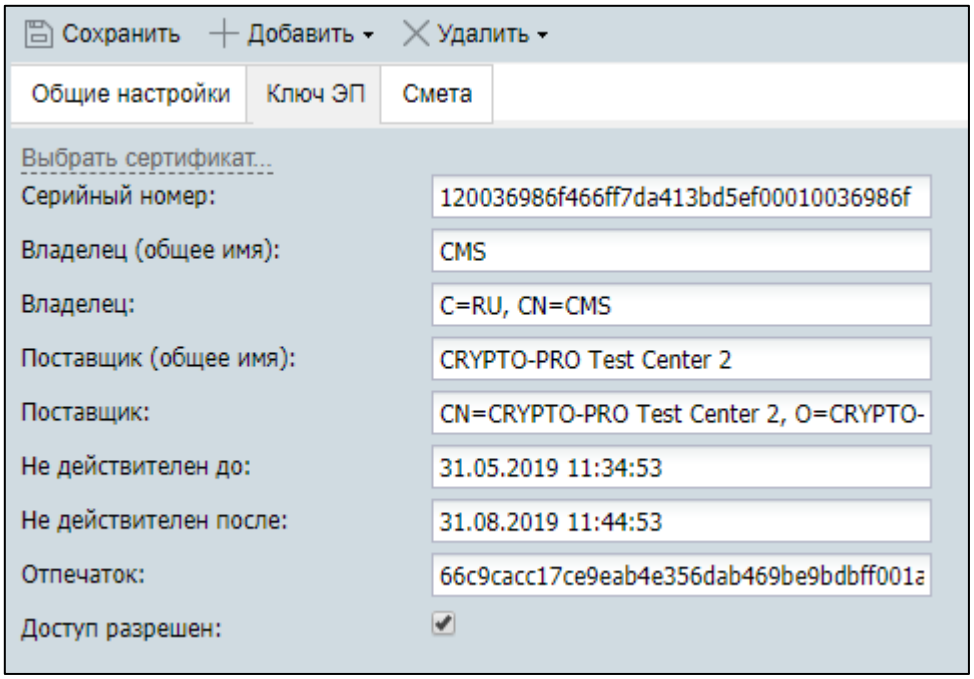


Рисунок 23. Настройка доступа к Системе по ЭП для пользователя в модуле «Безопасность»