127018, Москва, Сущёвский Вал, 18
Телефон: (495) 995 4820
Факс: (495) 995 4820
https://CryptoPro.ru
E-mail: info@CryptoPro.ru

Средство
Криптографической
Защиты
Информации

КриптоПро CSP
Версия 5.0 R2 KC1
Исполнение 1-Base
Инструкция по использованию
графического приложения
Инструменты КриптоПро (cptools)

ЖТЯИ.00101-02 92 06
Листов 32

2021 г

Содержание

Аннотация

Инструменты КриптоПро (CryptoPro Tools, cptools) — кроссплатформенное графическое приложение, функционирующее под управлением ОС Windows, Linux и macOS, поддерживаемых СКЗИ «КриптоПро CSP» версия 5.0 R2 КС1 исполнение 1-Base (см. п. 3.2 ЖТЯИ.00101-02 30 01. КриптоПро CSP. Формуляр).

Утилита предоставляет доступ к основным функциям и настройкам СКЗИ КриптоПро CSP, включая:

- просмотр сведений о лицензии на использование КриптоПро CSP;
- установку параметров облачного провайдера;
- создание и проверку ЭП;
- шифрование и расшифрование файлов;
- управление ключевыми контейнерами;
- управление сертификатами ЭП и связанными с ними ключами подписи;
- управление носителями.

1 Установка и доступ к приложению Инструменты КриптоПро

1.1 Windows

При использовании СКЗИ КриптоПро CSP под управлением ОС Windows утилита Инструменты КриптоПро устанавливается автоматически с основными файлами.

В ОС Windows приложение Инструменты КриптоПро доступно как отдельный пункт в группе программ «КРИПТО-ПРО» (меню **Пуск** ⇒ **КРИПТО-ПРО** ⇒ **Инструменты КриптоПро**) (см. Рисунок 1).

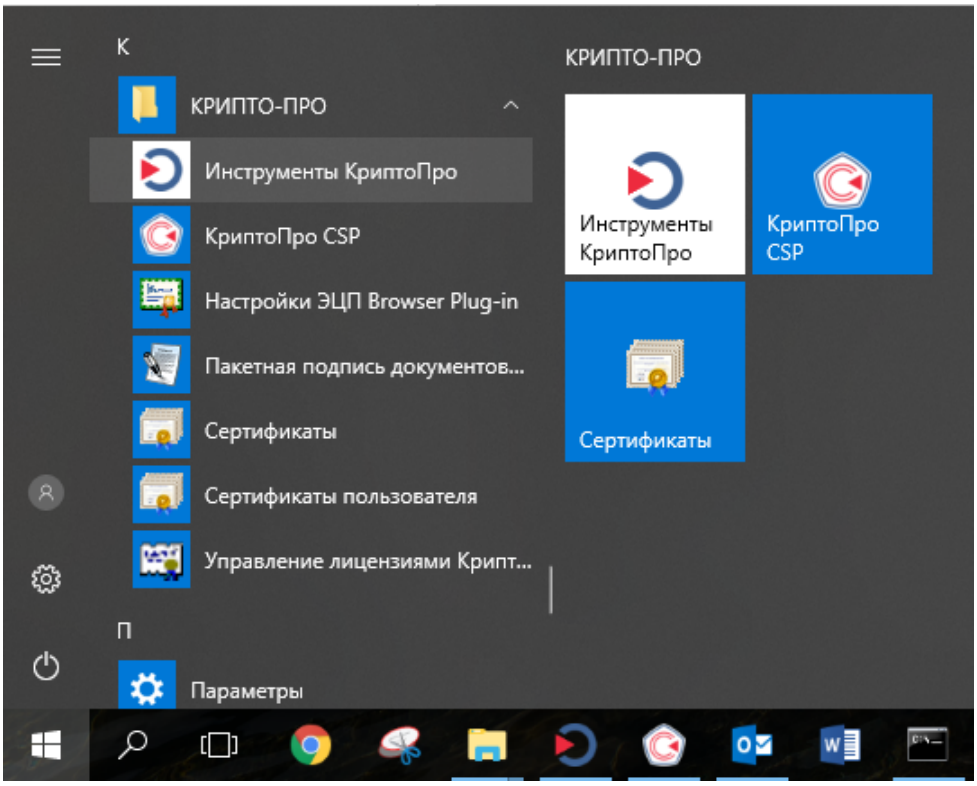

Рисунок 1. Доступ к приложению Инструменты КриптоПро под управлением ОС Windows

1.2 macOS

Для использования cptools под управлением ОС macOS необходимо выбрать для установки компонент **cptools** в Мастере установки КриптоПро CSP (см. Рисунок 2) или установить пакет **CPROcptools** из архива дистрибутива:

```
installer -pkg CPROcptools.pkg -target "/"
```

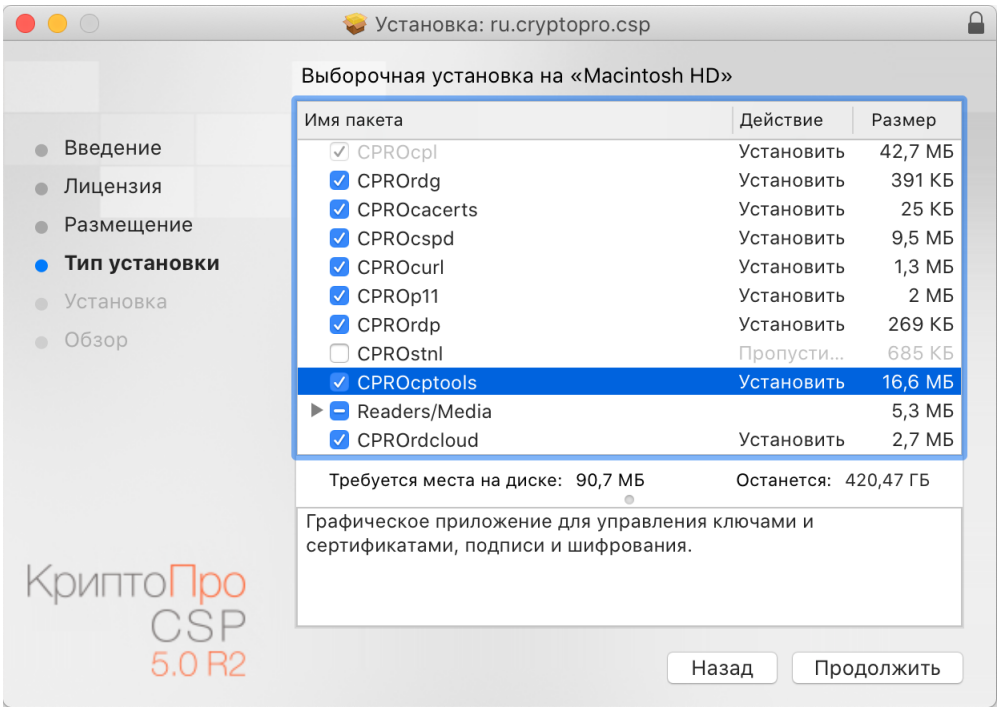

Рисунок 2. Установка cptools в ОС macOS

Утилита устанавливается в директорию `/opt/cprocsp/bin`.

Запуск приложения осуществляется из Launchpad (см. Рисунок 3) или из консоли с помощью команды `cptools`.

Рисунок 3. Доступ к приложению Инструменты КриптоПро под управлением macOS

1.3 Linux

Для использования cptools под управлением ОС семейства Linux необходимо выбрать компонент **cptools** в Мастере установки КриптоПро CSP (см. Рисунок 4) или установить пакет **cprocsp-cptools-gtk** с помощью соответствующей платформе команды установки пакета, указанной в разделе 2 «ЖТЯИ.00101-02 91 03. Руководство администратора безопасности. Linux».

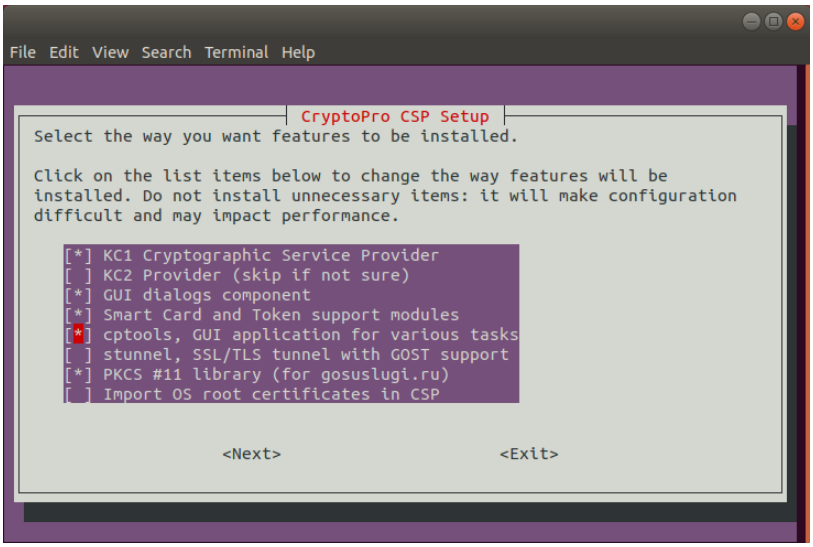

Рисунок 4. Установка cptools в ОС семейства Linux

Утилита устанавливается в директорию `/opt/cprocsp/bin/<название архитектуры>`.

Запуск приложения осуществляется из штатного меню приложений (внешний вид зависит от используемой ОС) (см. Рисунок 5) или из консоли с помощью команды `cptools`.

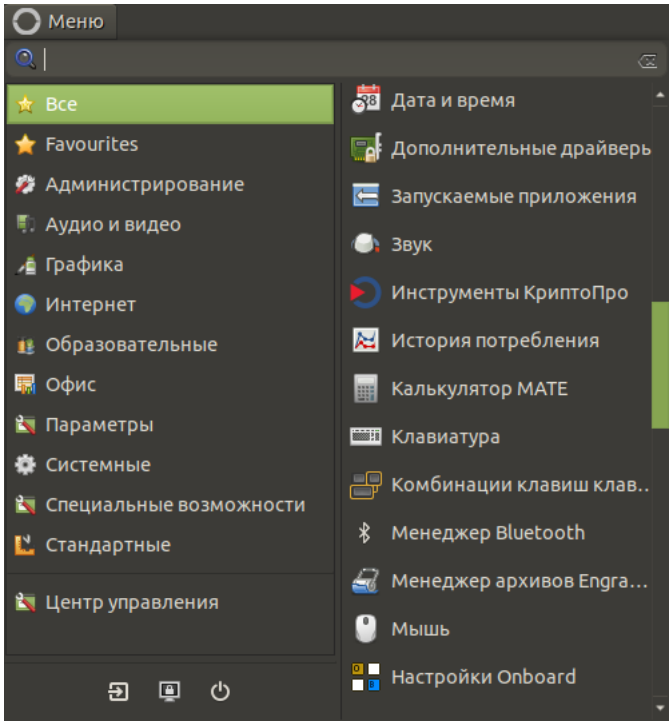

Рисунок 5. Доступ к приложению Инструменты КриптоПро под управлением ОС семейства Linux

2 Интерфейс приложения Инструменты КриптоПро

С помощью Инструментов КриптоПро решаются задачи управления контейнерами, сертификатами, носителями, настройками криптопровайдеров, создания и проверки электронной подписи PKCS #7.

Функции приложения сгруппированы по вкладкам в соответствии с назначением и позволяют пользователям удобно решать типовые задачи. Дополнительные функции по настройке провайдера доступны в расширенном режиме (кнопка **Показать расширенные**).

Панель приложения Инструменты КриптоПро содержит следующие вкладки (см. Рисунок 7):
- **Общее**;
- **Облачный провайдер**;
- **Контейнеры**;
- **Сертификаты**;
- **Создание подписи**;
- **Проверка подписи**;
- **Зашифровать файл**;
- **Расшифровать файл**;
- **Управление носителями** (доступна в расширенном режиме);
- **Настройки** (доступна в расширенном режиме).

2.1 Расширенный режим

Расширенный режим панели приложения рассчитан для опытных пользователей и открывает дополнительные возможности настройки параметров провайдера и операций с контейнерами, носителями, создания и проверки подписи.

Для отображения расширенных опций нажмите кнопку **Показать расширенные**. В расширенном режиме работы доступны дополнительные опции и настройки на вкладках.

Чтобы скрыть расширенные опции, нажмите кнопку **Скрыть расширенные**. Если при этом была открыта вкладка, доступная только в расширенном режиме (**Управление носителями** или **Настройки**), то будет отображена вкладка **Общее**.

Примечание. Некоторые опции в расширенном режиме (например, использование локального хранилища компьютера при выборе контейнера) доступны только при запуске панели с правами администратора (суперпользователя).

2.2 Поиск по панели

С помощью глобального поиска по панели можно быстро найти инструмент или настройки, соответствующие искомому слову. Поиск выполняется по значениям всех полей панели. Например, при поиске по слову «пароль» (см. Рисунок 6) для выбора доступны вкладки **Контейнеры** и **Управление носителями**, т.к. они содержат функции «Сменить **пароль** контейнера» и «Вернуть **пароль** по умолчанию» носителя соответственно.

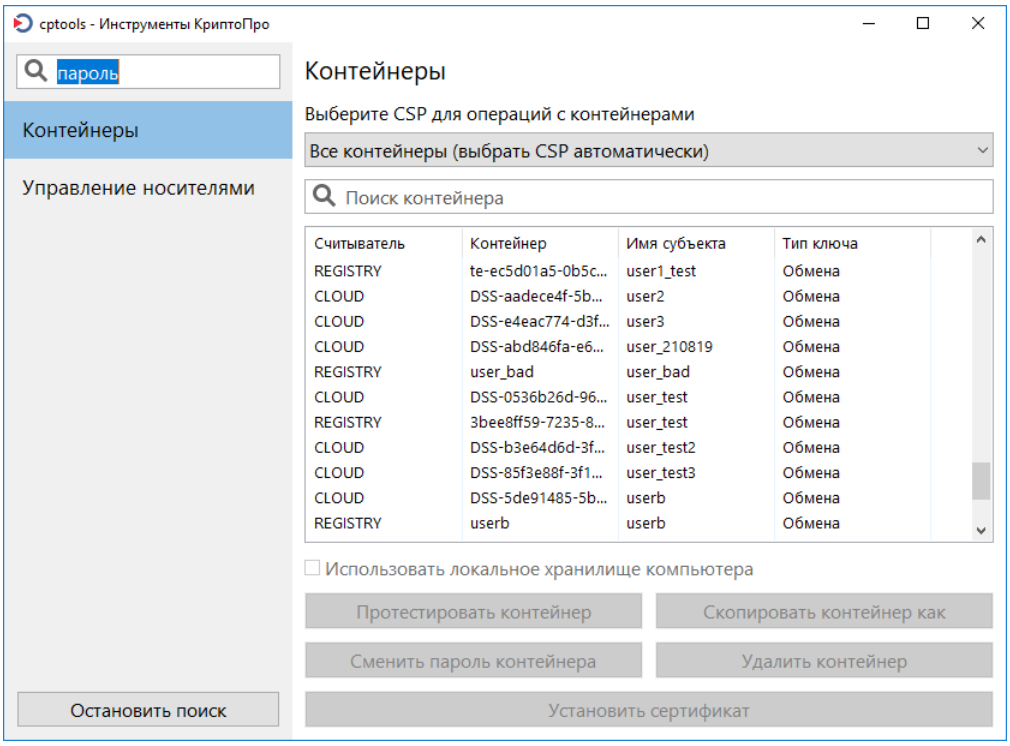

Рисунок 6. Поиск по панели

2.3 Общая информация о СКЗИ

Вкладка **Общее** панели Инструментов КриптоПро содержит информацию о версии установленного СКЗИ КриптоПро CSP, сведения о лицензии, а также позволяет выбрать язык провайдера для текущего пользователя.

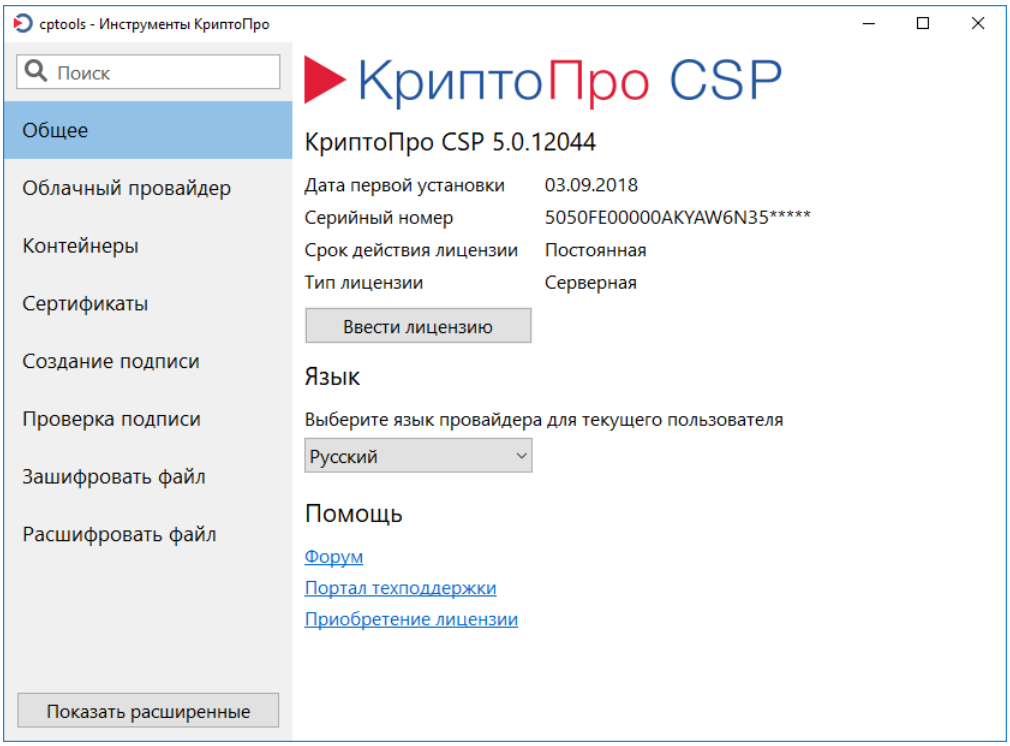

Рисунок 7. Вкладка **Общее**

2.4 Настройка параметров облачного провайдера

СКЗИ КриптоПро CSP поддерживает работу с ключами, хранящимися на облачном сервисе КриптоПро DSS. Инструменты вкладки **Облачный провайдер** позволяют настроить взаимодействие криптопровайдера с «облачными» ключами.

Интерфейс взаимодействия с ключами в облаке в КриптоПро CSP не отличается от работы с ключами на классических ключевых носителях. Для того, чтобы операции с облачными ключами в КриптоПро CSP стали доступны, необходимо настроить подключение к серверу DSS и установить сертификаты из личного кабинета пользователя сервиса электронной подписи (СЭП).

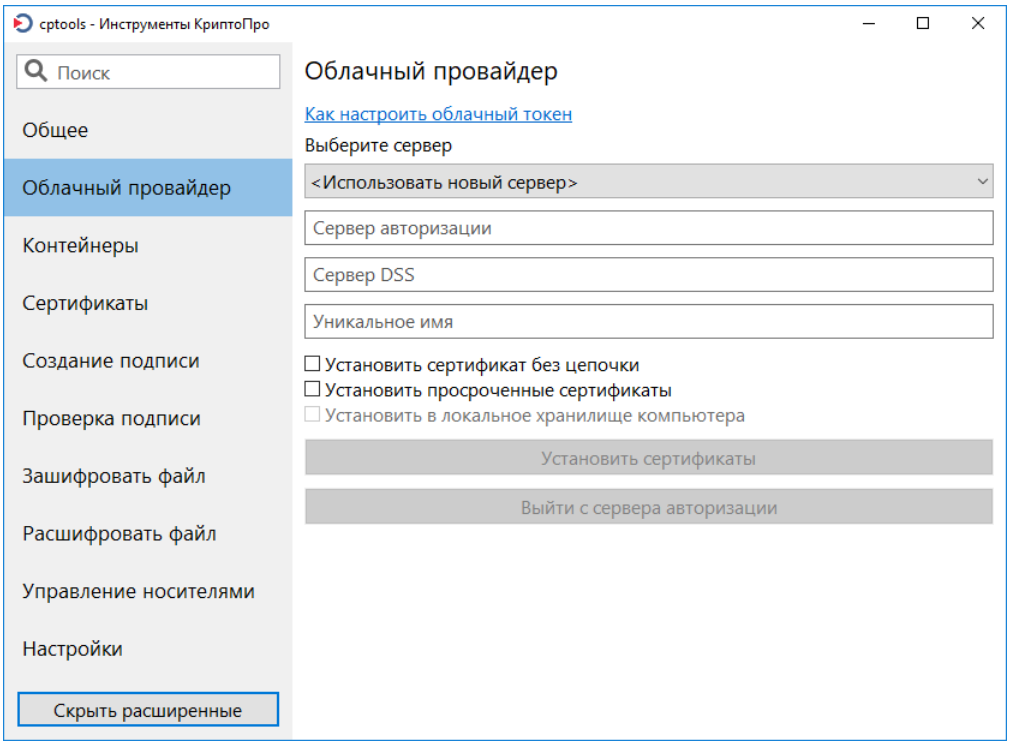

Рисунок 8. Вкладка **Облачный провайдер**

При использовании приложения под управлением ОС семейства Linux/macOS для возможности настройки параметров облачного провайдера необходимо дополнительно установить модуль поддержки cloud (инструкцию по установке см. в руководстве администратора безопасности для используемой платформы). Если модуль не установлен, кнопки на вкладке **Облачный провайдер** неактивны, внизу панели отображается соответствующее сообщение (см. Рисунок 9).

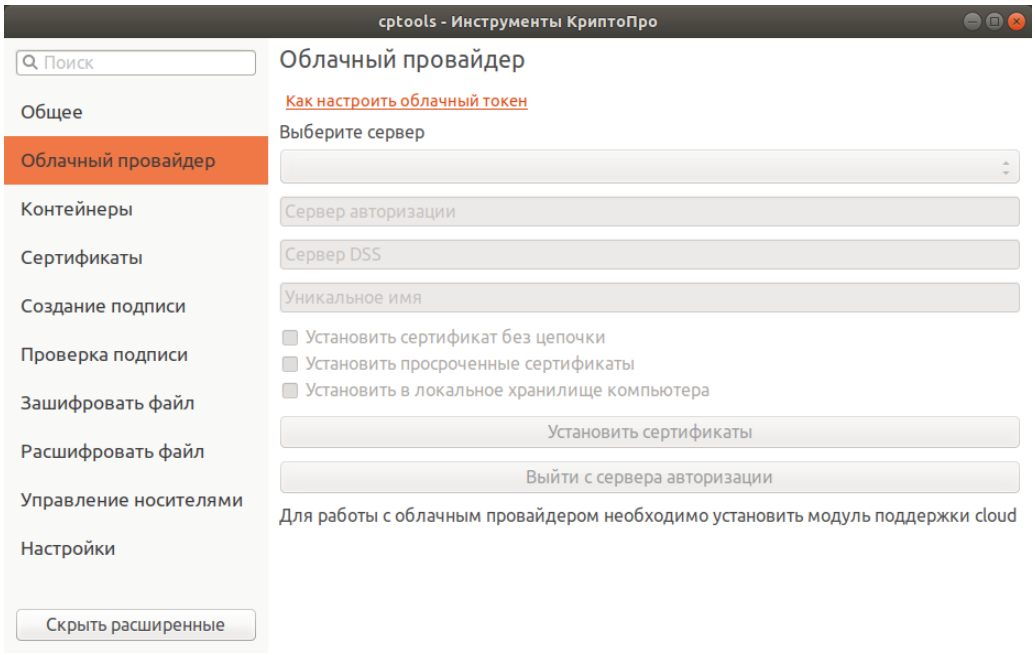

Рисунок 9. Вкладка **Облачный провайдер** для КС2 под управлением ОС семейства Linux/macOS

Для настройки соединения с необходимым СЭП КриптоПро DSS в выпадающем списке выберите <Использовать новый сервер> и укажите адреса сервера авторизации и сервера DSS в соответствующих полях. При необходимости измените автоматически назначенное уникальное имя.

Для установки сертификатов в хранилище текущего пользователя нажмите кнопку **Установить сертификаты**.

Если вход в СЭП ранее не был выполнен, откроется окно входа в веб-интерфейс СЭП. Вид интерфейса зависит от используемой ОС (см. Рисунок 10). Дальнейшие действия пользователя для осуществления аутентификации в СЭП зависят от используемой программно-аппаратной платформы, настроек сервера, метода аутентификации пользователя и регламента работы с указанным СЭП (подробнее см. эксплуатационную документацию на компонент Сервер электронной подписи «КриптоПро DSS»).

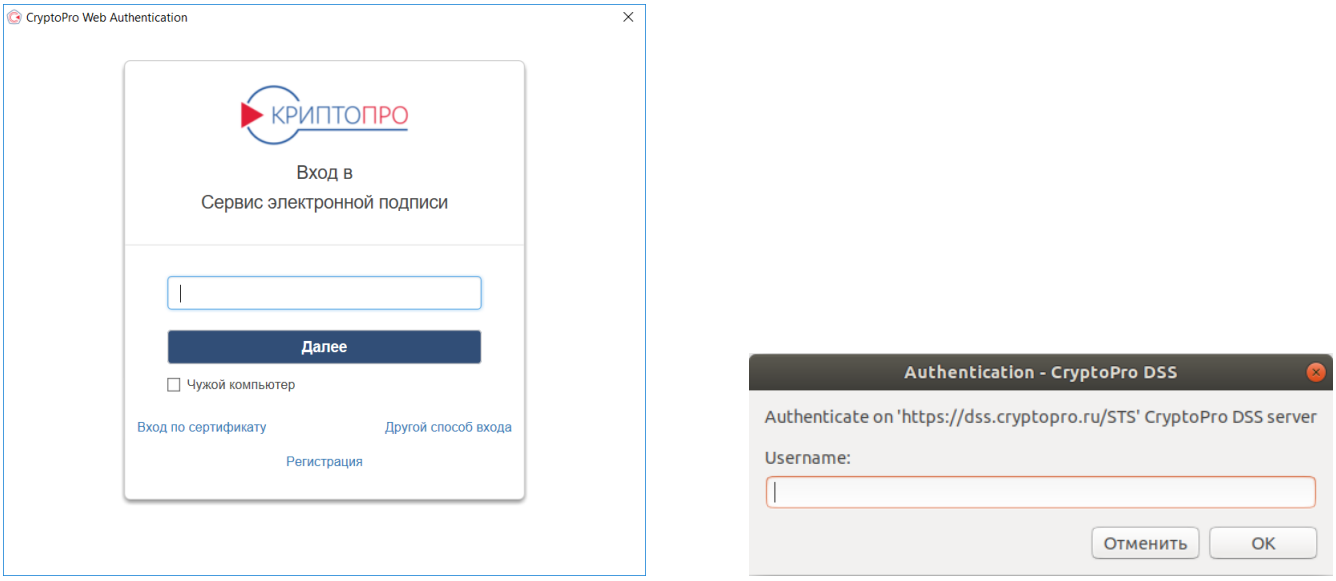

Рисунок 10. Вход в СЭП КриптоПро DSS

Примечание. Если в ОС Linux окно входа в веб-интерфейс СЭП отображается в консольном виде без графического интерфейса (см. Рисунок 11), установите пакет zenity для корректного отображения.

Рисунок 11. Отображение окна входа в СЭП без графического интерфейса в ОС Linux

После того, как выполнен вход в СЭП, сертификаты пользователя СЭП будут установлены в локальное хранилище сертификатов текущего пользователя (см. Рисунок 12).

Примечание. При установке сертификатов ключи подписи не покидают сервер DSS.

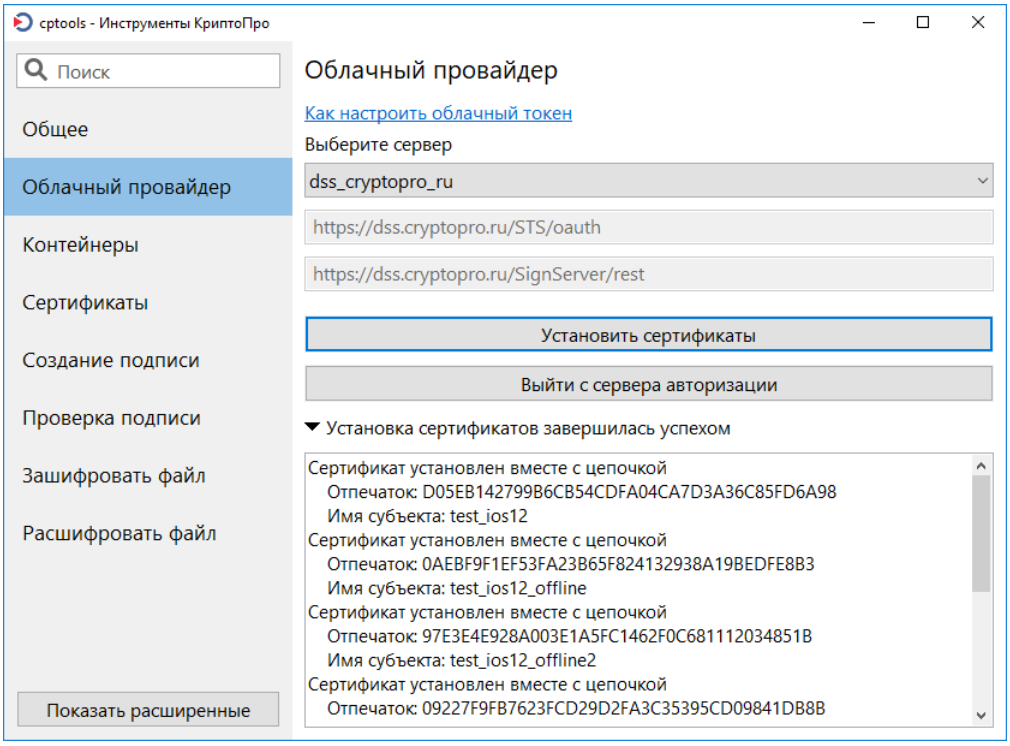

Рисунок 12. Установка сертификатов в хранилище текущего пользователя

По кнопке **Выйти с сервера авторизации** можно выйти из личного кабинета пользователя СЭП. В случае успешного выхода с сервера будет отображено окно с соответствующим сообщением (см. Рисунок 13).

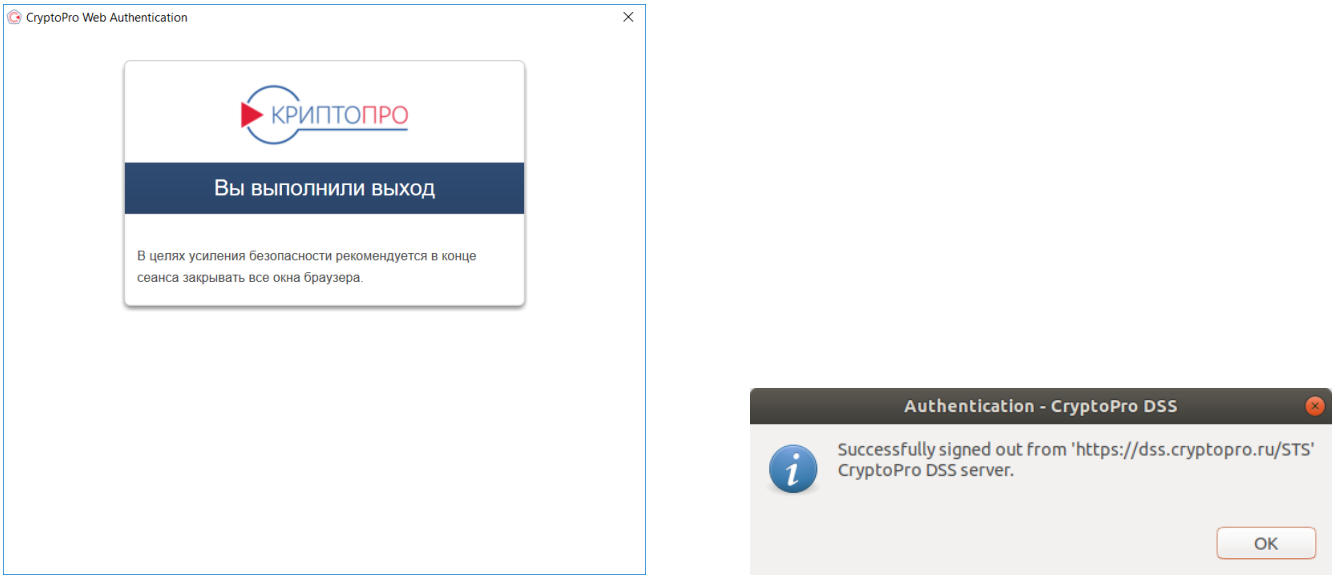

Рисунок 13. Выход из СЭП КриптоПро DSS

В расширенном режиме использования панели доступны следующие дополнительные опции установки сертификатов:

- **Установить сертификат без цепочки** (по умолчанию выключена) — будет установлен только конечный сертификат без цепочки корневого и промежуточных сертификатов УЦ.
- **Установить просроченные сертификаты** (по умолчанию выключена) — будет установлены сертификаты с истекшим сроком действия. Если опция выключена, при наличии у пользователя СЭП недействительных сертификатов при попытке их установки будет отображена ошибка и сертификаты не будут установлены (см. Рисунок 14).
- **Установить в локальное хранилище компьютера** (по умолчанию выключена) — сертификаты будут установлены в локальное хранилище сертификатов (при выключенной опции устанавливаются в хранилище текущего пользователя). Опция доступна для выбора только при запуске приложения с правами администратора (суперпользователя).

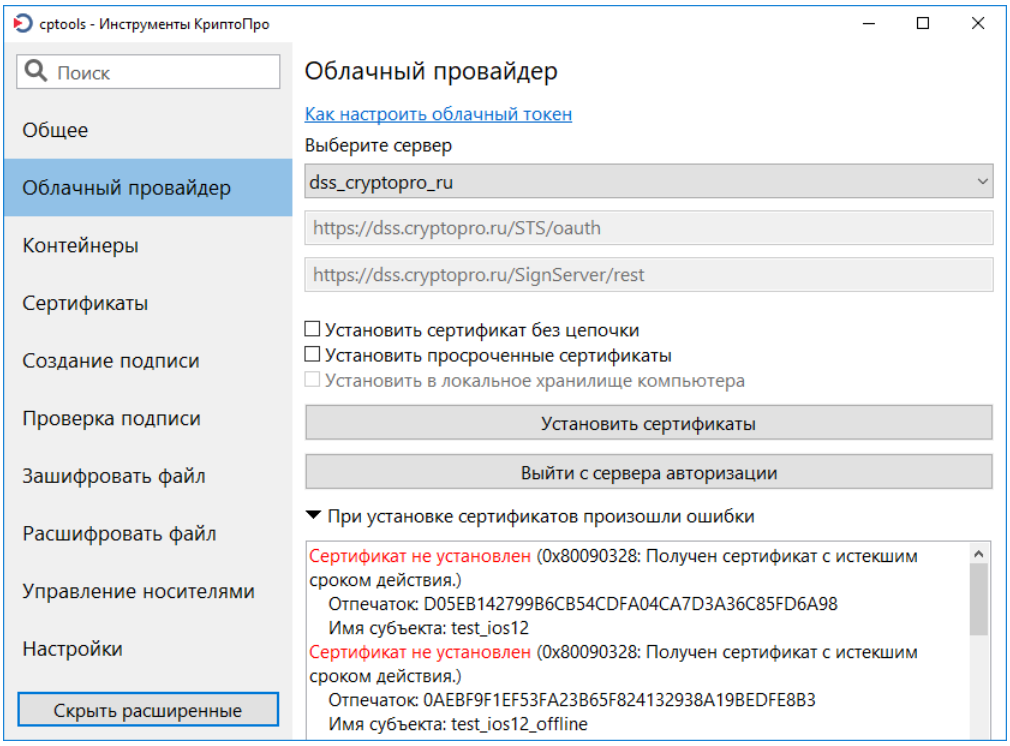

Рисунок 14. Опции установки сертификатов

2.5 Операции с контейнерами

На вкладке **Контейнеры** отображается перечень контейнеров, доступных пользователю, от имени которого запущено приложение, на подключенных в настоящий момент носителях. По умолчанию для каждого ключа в контейнере указаны соответствующий считыватель, имя субъекта (CN) сертификата (в случае наличия сертификата в контейнере) и тип ключа в контейнере.

Управление колонками таблицы. В таблице можно изменить перечень отображаемых свойств контейнера (и соответствующих колонок). Для этого нажмите правой кнопкой мыши на название любой колонки и в выпадающем списке укажите те колонки, которые необходимо отобразить в таблице.

Для изменения порядка отображения колонок левой кнопкой мыши зажмите название колонки и перетяните ее на необходимое место в таблице.

Сортировка контейнеров. В таблице доступна сортировка контейнеров по одной из колонок таблицы. По умолчанию контейнеры отсортированы по имени считывателя. Чтобы отсортировать контейнеры, нажмите на название необходимой колонки. По умолчанию выполняется сортировка по алфавиту. Чтобы изменить направление сортировки, повторно нажмите на название колонки.

Поиск контейнера. Для быстрого поиска необходимого контейнера воспользуйтесь поисковой строкой «Поиск контейнера». Поиск осуществляется по всем полям одновременно.

Вкладка предоставляет доступ к следующим функциям:

- тестирование контейнера;
- копирование контейнера;
- установка сертификата.

В расширенном режиме использования панели доступны следующие дополнительные операции с контейнерами:

- фильтрация контейнеров по провайдеру (CSP);
- использование локального хранилища компьютера для поиска контейнера (функция доступна при запуске панели с правами администратора (суперпользователя));
- изменение пароля контейнера;
- удаление контейнера.

В случае возникновения ошибки во время выполнения какой-либо операции с контейнером, внизу окна красным цветом отображаются код и информация об ошибке. Если операция с контейнером завершена успешно, отображается соответствующее сообщение.

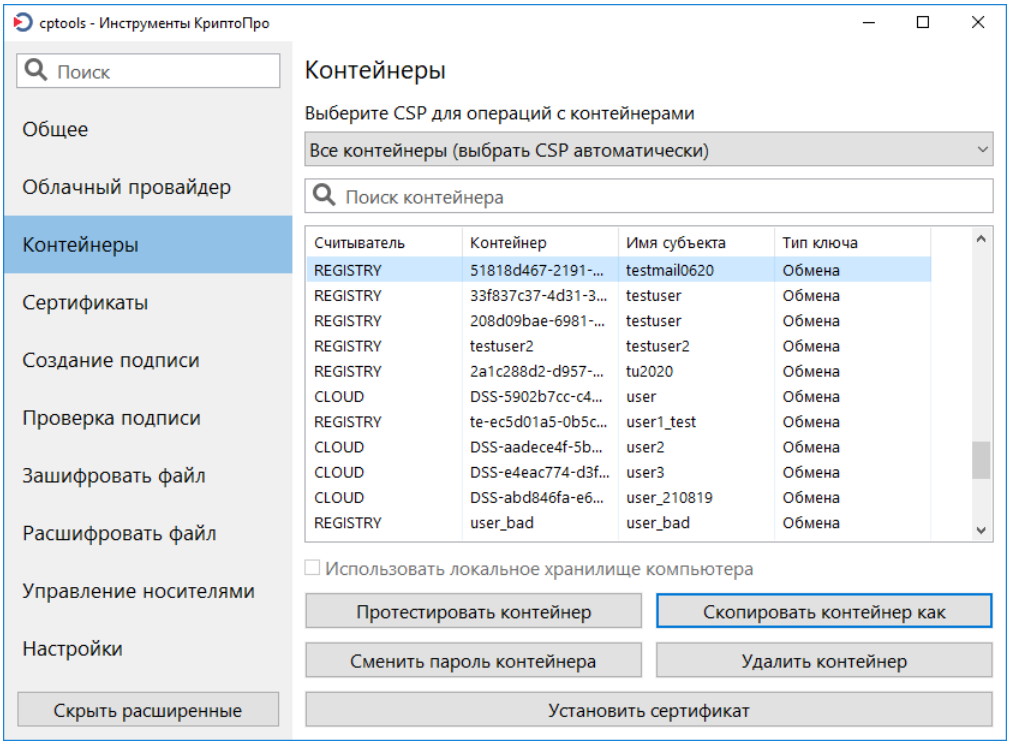

Рисунок 15. Вкладка **Контейнеры**

Примечание. Если на контейнер установлен пароль, он будет запрашиваться в окне аутентификации в контейнере всякий раз при выполнении операций с закрытым ключом. Для удобства в случае необходимости многократного обращения к закрытому ключу возможно сохранить пароль контейнера в специальном хранилище локального компьютера. Для этого установите флаг **Сохранить пароль в системе** в окне аутентификации в контейнере (см. Рисунок 16).

Для удаления ранее сохраненных паролей воспользуйтесь функцией **Удалить сохраненные пароли** вкладки **Настройки**.

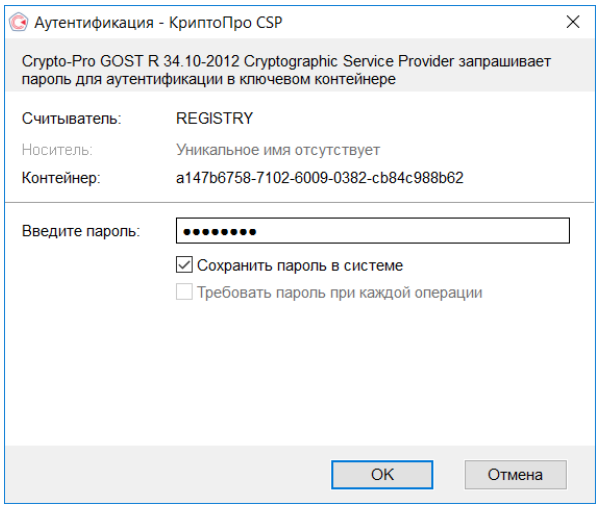

Рисунок 16. Сохранение пароля контейнера

2.5.1 Тестирование контейнера

Тестирование контейнера позволяет проверить его работоспособность, а также отобразить свойства ключа (ключей) и сертификата (сертификатов) в контейнере. Чтобы протестировать контейнер:

1) на вкладке **Контейнеры** выберите необходимый контейнер;
2) нажмите кнопку **Протестировать контейнер**;
3) если на доступ к ключу установлен пароль, введите его в окне аутентификации в контейнере.

Результаты тестирования отображаются в новом окне, информацию о контейнере можно скопировать или сохранить в файл. Если в процессе тестирования контейнера были обнаружены ошибки, информация о них выделяется красным цветом в окне с результатами проверки (см. Рисунок 17).

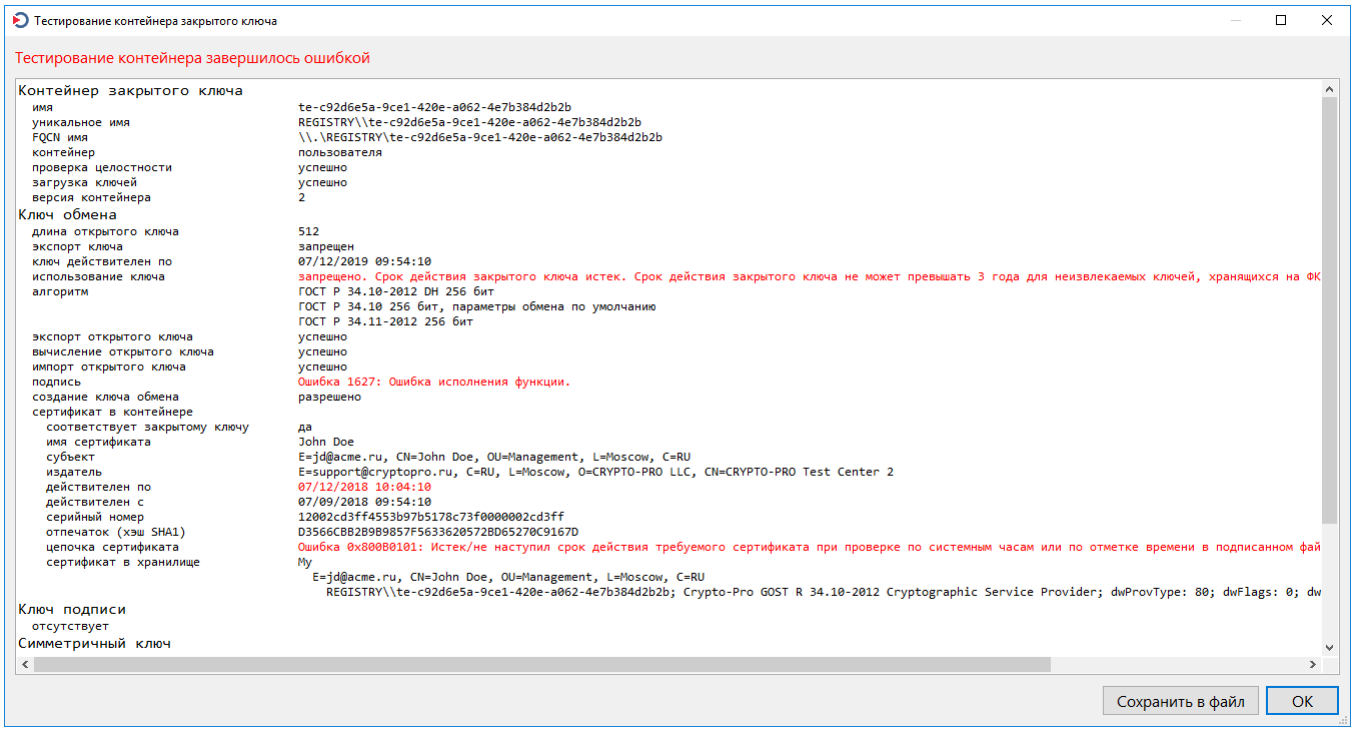

Рисунок 17. Результаты тестирования контейнера

2.5.2 Копирование контейнера

Примечание. При использовании функции **Скопировать контейнер** новому контейнеру по умолчанию присваивается имя вида contname_copy. Для самостоятельного назначения имени скопированного контейнера и выбора некоторых других параметров воспользуйтесь функцией **Скопировать контейнер как** расширенного режима панели.

Копирование контейнера закрытого ключа доступно только для ключей, при генерации которых был установлен признак экспортируемого. Чтобы скопировать контейнер:

1) на вкладке **Контейнеры** выберите необходимый контейнер;
2) нажмите кнопку **Скопировать контейнер**;
3) выберите доступный ключевой носитель для нового контейнера;
4) если на доступ к ключу в копируемом контейнере установлен пароль, введите его в окне аутентификации в контейнере;
5) установите пароль для нового контейнера в окне аутентификации.

Если при копировании контейнера необходимо изменить его параметры по умолчанию, воспользуйтесь функцией **Скопировать контейнер как**:

1) перейдите в расширенный режим использования панели, нажав кнопку **Показать расширенные**;
2) на вкладке **Контейнеры** выберите необходимый контейнер;
3) нажмите кнопку **Скопировать контейнер как**;
4) укажите следующие параметры для нового контейнера:
   - имя контейнера
   - провайдер (доступен для выбора, если на машине зарегистрированы несколько провайдеров одного типа)
   - установите флаг, если новый контейнер должен находиться в локальном хранилище компьютера (доступен при запуске панели с правами администратора (суперпользователя))
5) выберите доступный ключевой носитель для нового контейнера;
6) если на доступ к ключу в копируемом контейнере установлен пароль, введите его в окне аутентификации в контейнере;
7) установите пароль для нового контейнера в окне аутентификации.

2.5.3 Установка сертификата из контейнера

Примечание. По умолчанию установка сертификата производится в хранилище текущего пользователя. Чтобы установить сертификат хранилище локального компьютера, установите флаг **Использовать локальное хранилище компьютера**, доступный в расширенном режиме.

При установке сертификата из контейнера в хранилище формируется ссылка на закрытый ключ, соответствующий данному сертификату.

Для установки сертификата, хранящегося в контейнере закрытого ключа, в хранилище сертификатов:

1) на вкладке **Контейнеры** выберите контейнер, из которого необходимо установить сертификат;
2) нажмите кнопку **Установить сертификат**.

2.5.4 Изменение пароля контейнера

Чтобы сменить пароль контейнера:

1) перейдите в расширенный режим использования панели, нажав кнопку **Показать расширенные**;
2) на вкладке **Контейнеры** выберите необходимый контейнер;

3) нажмите кнопку **Сменить пароль контейнера**;
4) в окне аутентификации в контейнере введите текущий пароль и дважды новый пароль.

Примечание. Если пароль контейнера сохранен в хранилище (был установлен флаг **Сохранить пароль в системе**), в окне смены пароля текущий пароль вводить не требуется. После смены пароля новый пароль также будет сохранен.

2.5.5 Удаление контейнера

Чтобы удалить контейнер:
1) перейдите в расширенный режим использования панели, нажав кнопку **Показать расширенные**;
2) на вкладке **Контейнеры** выберите необходимый контейнер;
3) нажмите кнопку **Удалить контейнер**;
4) подтвердите удаление контейнера.

Примечание. При удалении контейнера описанным способом связанные с контейнером сертификаты в системных хранилищах не удаляются. Чтобы удалить соответствующие сертификаты, воспользуйтесь функцией Удаление сертификата.

2.6 Операции с ключами и сертификатами

Вкладка **Сертификаты** содержит функции управления сертификатами ЭП и связанными с ними ключами подписи.

Управление колонками таблицы. По умолчанию для каждого сертификата указаны имя субъекта, имя издателя, срок действия и отпечаток. В таблице можно изменить перечень отображаемых свойств сертификата (и соответствующих колонок). Для этого нажмите правой кнопкой мыши на название любой колонки и в выпадающем списке укажите те колонки, которые необходимо отобразить в таблице.

Для изменения порядка отображения колонок левой кнопкой мыши зажмите название колонки и перетяните ее на необходимое место в таблице.

Сортировка сертификатов. В таблице доступна сортировка сертификатов по одной из колонок таблицы. По умолчанию сертификаты отсортированы по значению отпечатка. Чтобы отсортировать сертификаты, нажмите на название необходимой колонки. По умолчанию выполняется сортировка по алфавиту. Чтобы изменить направление сортировки, повторно нажмите на название колонки.

Поиск сертификата. Для быстрого поиска необходимого сертификата воспользуйтесь поисковой строкой «Поиск сертификата». Поиск осуществляется по всем полям одновременно.

Отображение сертификатов в хранилище. По умолчанию в таблице отображаются сертификаты хранилища Личное пользователя, от имени которого запущено приложение. Чтобы отобразить перечень сертификатов в необходимом хранилище, выберите его из выпадающего списка над строкой поиска.

Вкладка предоставляет доступ к следующим функциям:
- установка сертификатов в хранилище из файла;
- удаление сертификата из хранилища;
- просмотр свойств сертификата в хранилище;
- экспорт сертификата в файл;
- импорт ключей из файла;
- экспорт ключей в файл или QR-код.

В расширенном режиме использования панели доступны следующие дополнительные опции:

- использование локального хранилища компьютера для поиска или установки сертификата (функция доступна при запуске панели с правами администратора (суперпользователя));
- отключение автоматического выбора хранилища для установки сертификата.

В случае возникновения ошибки во время выполнения какой-либо операции с сертификатом или соответствующим ключом, внизу окна красным цветом отображаются код и информация об ошибке. Если операция завершена успешно, отображается соответствующее сообщение.

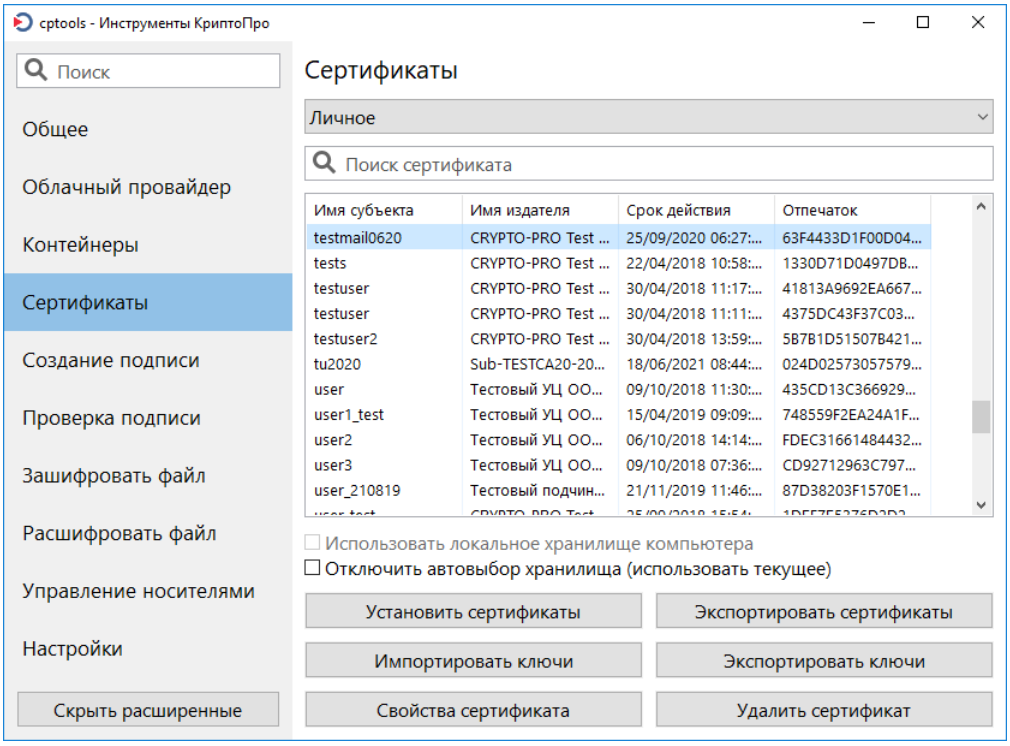

Рисунок 18. Вкладка **Сертификаты**

2.6.1 Установка сертификатов из файла

Функция **Установить сертификаты** позволяет установить сертификаты из файлов различных форматов в соответствующие хранилища сертификатов.

По умолчанию выбор хранилища для сертификата осуществляется автоматически. Если при установке сертификата контейнер соответствующего закрытого ключа доступен, сертификат помещается в хранилище Личное. В других случаях сертификаты распределяются по хранилищам согласно своему назначению.

Чтобы отключить автоматический выбор хранилища и установить сертификат в текущее хранилище (название указано в поле над строкой поиска), установите флаг **Отключить автовыбор хранилища (использовать текущее)**.

Файлы некоторые форматов могут содержать более одного сертификата. При установке они будут автоматически размещены по соответствующим хранилищам.

Примечание. Для установки сертификатов в хранилище локального компьютера необходимо предварительно установить флаг **Использовать локальное хранилище компьютера.** Поле доступно только при запуске панели с правами администратора (суперпользователя).

Чтобы установить сертификат из файла в хранилище:
1) нажмите кнопку **Установить сертификат**;
2) в открывшемся окне выберите файл сертификата для установки.

В случае успешного выполнения операции перечень установленных сертификатов в соответствующих хранилищах можно развернуть по кнопке с сообщением об успешной установке внизу окна (см. Рисунок 19).

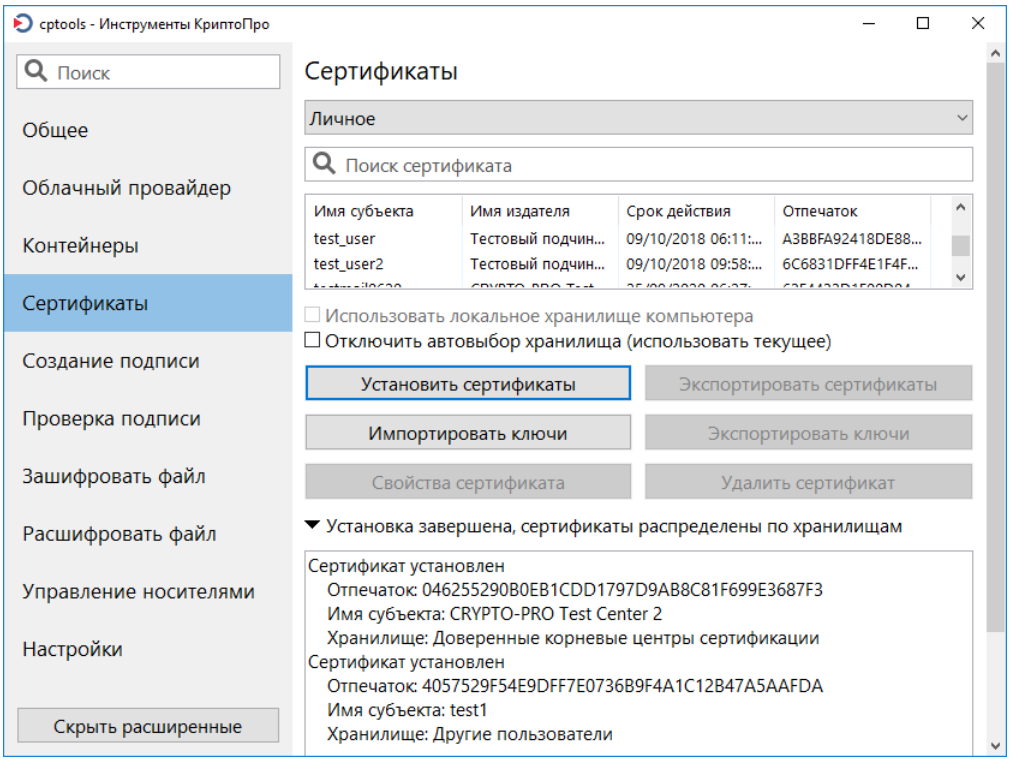

Рисунок 19. Установка сертификатов из файла

2.6.2 Удаление сертификата из хранилища

Чтобы удалить сертификат из хранилища:
1) на вкладке **Сертификаты** выберите необходимый сертификат;
2) нажмите кнопку **Удалить сертификат**;
3) подтвердите удаление сертификата.

Примечание. При удалении сертификата из хранилища описанным выше способом связанный с сертификатом ключ подписи не удаляется. Чтобы удалить соответствующий сертификату ключ, воспользуйтесь функцией Удаление контейнера.

2.6.3 Просмотр свойств сертификата

Чтобы просмотреть свойства сертификата:
1) на вкладке **Сертификаты** выберите необходимый сертификат;
2) нажмите кнопку **Свойства сертификата**.

Откроется окно, содержащее перечень полей сертификата (см. Рисунок 20). Текст в окне доступен для копирования.

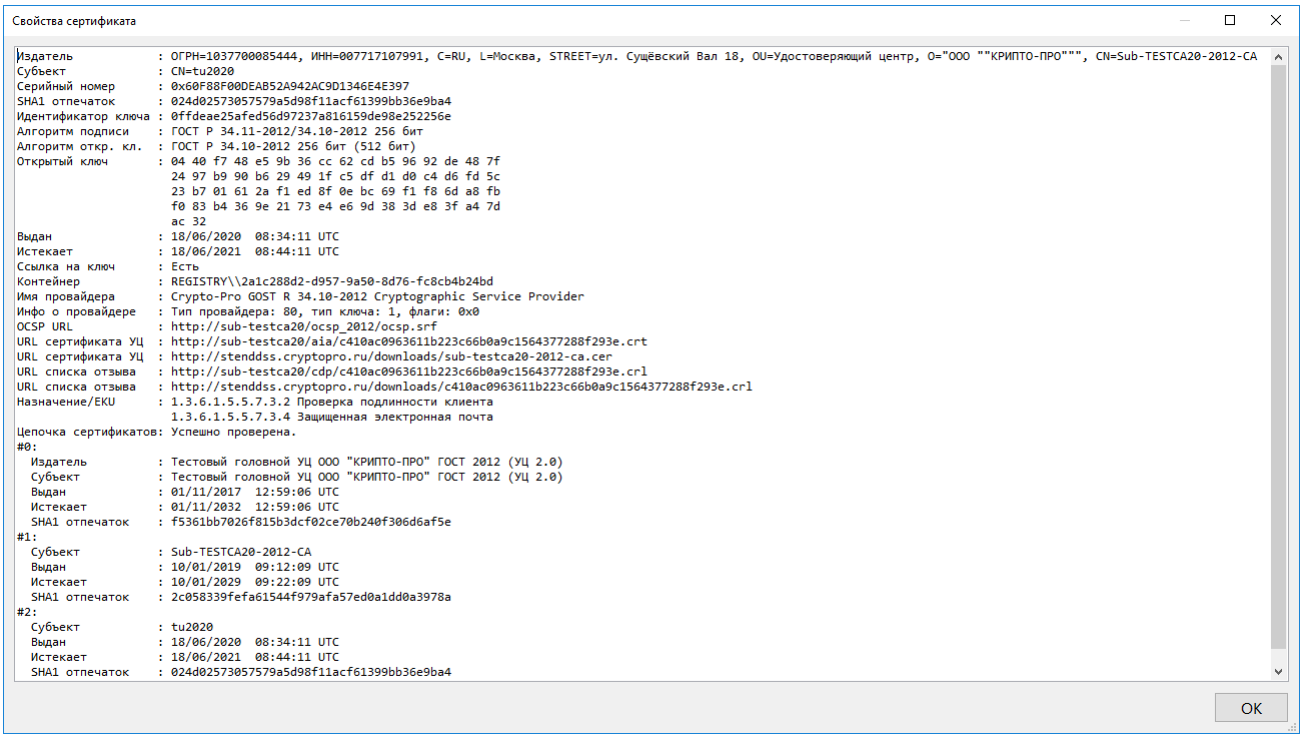

Рисунок 20. Свойства сертификата

2.6.4 Экспорт сертификатов в файл

Чтобы экспортировать сертификат в файл:

1) на вкладке **Сертификаты** выберите один или несколько сертификатов;
2) нажмите кнопку **Экспортировать сертификаты**;
3) в открывшемся окне укажите путь, имя и тип файла и нажмите кнопку **Сохранить**.

Примечание. При экспорте сертификата в файл описанным выше способом связанный с сертификатом ключ подписи (закрытый ключ) не экспортируется. Чтобы экспортировать соответствующий ключ, воспользуйтесь функцией Экспорт ключей.

2.6.5 Импорт ключей

Импорт ключей выполняется из файла обмена личной информацией формата PKCS #12 (.PFX). При импорте ключей сертификаты из файла автоматически устанавливаются в соответствующие хранилища.

Чтобы импортировать ключ:

1) на вкладке **Сертификаты** нажмите кнопку **Импортировать ключи**;
2) в открывшемся окне выберите файл PFX для импорта ключей; если указанный файл защищен с помощью пароля, введите его в соответствующем окне;
3) в окне выбора ключевого носителя укажите носитель для создания контейнера;
4) установите пароль для нового ключевого контейнера в окне аутентификации;
5) для установки соответствующего закрытому ключу сертификата введите пароль в окне аутентификации в контейнере (если он был установлен на предыдущем шаге).

В случае успешного выполнения операции перечень установленных сертификатов в соответствующих хранилищах можно развернуть по кнопке с сообщением об успешной установке внизу окна (см. Рисунок 19).

2.6.6 Экспорт ключей

Примечание. Экспорт ключей доступен только для ключей, имеющих признак экспортируемых.

Экспорт ключей и соответствующего сертификата выполняется в формате файла обмена личной информацией PKCS#12 (.PFX). Также возможно экспортировать PFX в QR-код для последующего импорта ключа с помощью СКЗИ, поддерживающих данную функцию (например, «КриптоПро NGate» или «КриптоАРМ ГОСТ»).

Чтобы экспортировать ключ:

1) на вкладке **Сертификаты** выберите сертификат, соответствующий ключу, который необходимо экспортировать;
2) нажмите кнопку **Экспортировать ключи**;
3) откроется окно экспорта ключей (см. Рисунок 21);
4) в открывшемся окне установите пароль на создаваемый файл PFX и выберите способ экспорта ключа:
   - экспортировать PFX в файл — ключ и соответствующий сертификат будут сохранены в формате файла .pfx на компьютере. В следующем окне укажите путь и имя для создаваемого файла.
   - экспортировать PFX в QR-код — PFX будет выведен на экран в формате QR-кода для последующего импорта в СКЗИ, указанное в поле «Выберите приложение». Для импорта ключей в не поддерживаемые по умолчанию приложения возможно указать префикс Deep Link вручную в поле ниже.
5) если на контейнер экспортируемого ключа установлен пароль, введите его в окне аутентификации в контейнере.

В результате операции, если был выбран способ экспорта PFX в виде QR-кода, откроется окно с сформированным QR-кодом (см. Рисунок 22), который можно отсканировать на мобильным устройстве с установленным СКЗИ для импорта ключа и сертификата.

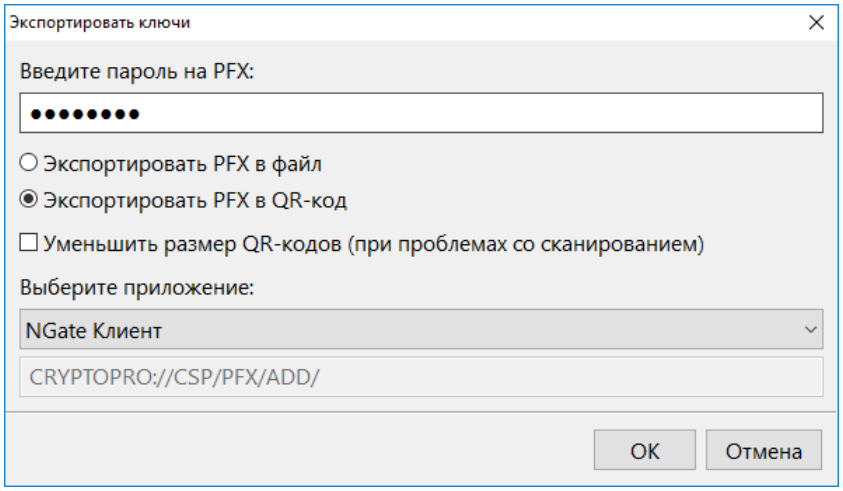

Рисунок 21. Экспорт ключей

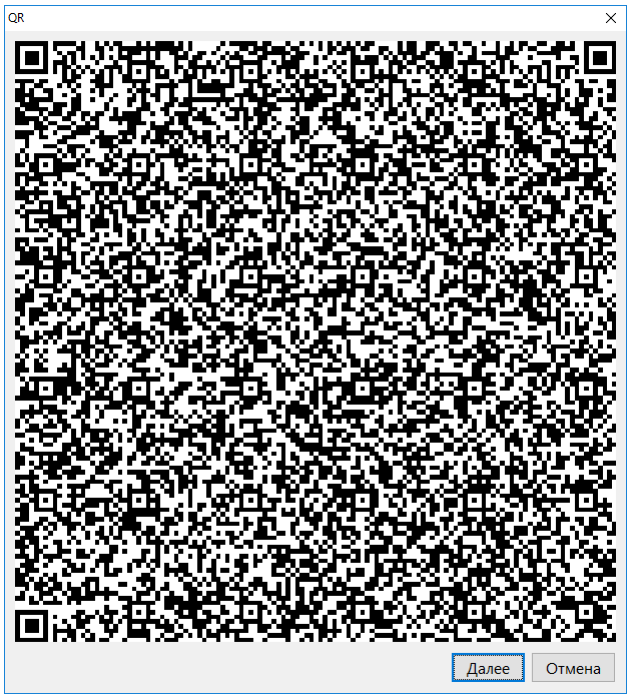

Рисунок 22. Экспорт PFX в QR-код

2.7 Создание подписи

Вкладка **Создание подписи** предназначена для создания подписи файла и сохранение ее в виде CMS-файла.

Подпись файла создается с использованием ключа, соответствующего выбранному в окне сертификату. Можно создать присоединенную подпись (подписываемый документ и подпись содержатся в одном файле) и отсоединенную подпись (создается в отдельном от подписываемого документа файле).

Управление колонками таблицы. По умолчанию для каждого сертификата указаны имя субъекта, имя издателя, срок действия и отпечаток. В таблице можно изменить перечень отображаемых свойств сертификата (и соответствующих колонок). Для этого нажмите правой кнопкой мыши на название любой колонки и в выпадающем списке укажите те колонки, которые необходимо отобразить в таблице.

Для изменения порядка отображения колонок левой кнопкой мыши зажмите название колонки и перетяните ее на необходимое место в таблице.

Сортировка сертификатов. В таблице доступна сортировка сертификатов по одной из колонок таблицы. По умолчанию сертификаты отсортированы по значению отпечатка. Чтобы отсортировать сертификаты, нажмите на название необходимой колонки. По умолчанию выполняется сортировка по алфавиту. Чтобы изменить направление сортировки, повторно нажмите на название колонки.

Поиск сертификата. Для быстрого поиска необходимого сертификата воспользуйтесь поисковой строкой «Поиск сертификата». Поиск осуществляется по всем полям одновременно.

В расширенном режиме использования панели доступны дополнительные опции создания подписи:

- выбор сертификата из хранилища сертификатов локального компьютера (функция доступна при запуске панели с правами администратора (суперпользователя));
- создание отсоединенной подписи.

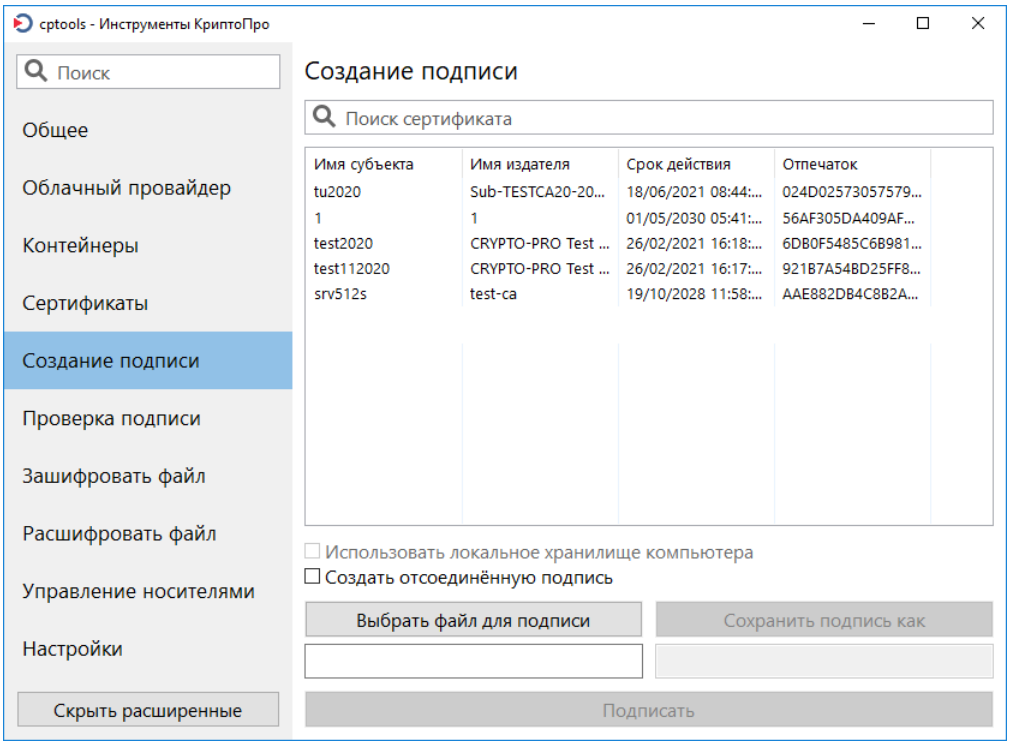

Рисунок 23. Вкладка **Создание подписи**

Для создания подписи файла:

1) на вкладке **Создание подписи** выберите сертификат, соответствующий ключу подписи, который будет использоваться для создания подписи;

2) нажмите кнопку **Выбрать файл для подписи** и выберите файл, который необходимо подписать (или введите адрес файла вручную в поле под кнопкой);

3) поле с адресом файла подписи заполнится автоматически; при необходимости измените адрес или имя файла вручную или с помощью кнопки **Сохранить подпись как**;

4) нажмите кнопку **Подписать**;

5) если на контейнер установлен пароль, введите его в окне аутентификации в контейнере.

Для проверки корректности созданной подписи воспользуйтесь вкладкой Проверка подписи.

2.8 Проверка подписи

На вкладке **Проверка подписи** можно проверить действительность присоединенной и отсоединенной подписи.

Примечание. Для проверки отсоединенной подписи потребуются 2 файла — исходный подписываемый документ и файл с подписью.

В расширенном режиме использования панели возможно сохранить исходный файл после проверки присоединенной подписи.

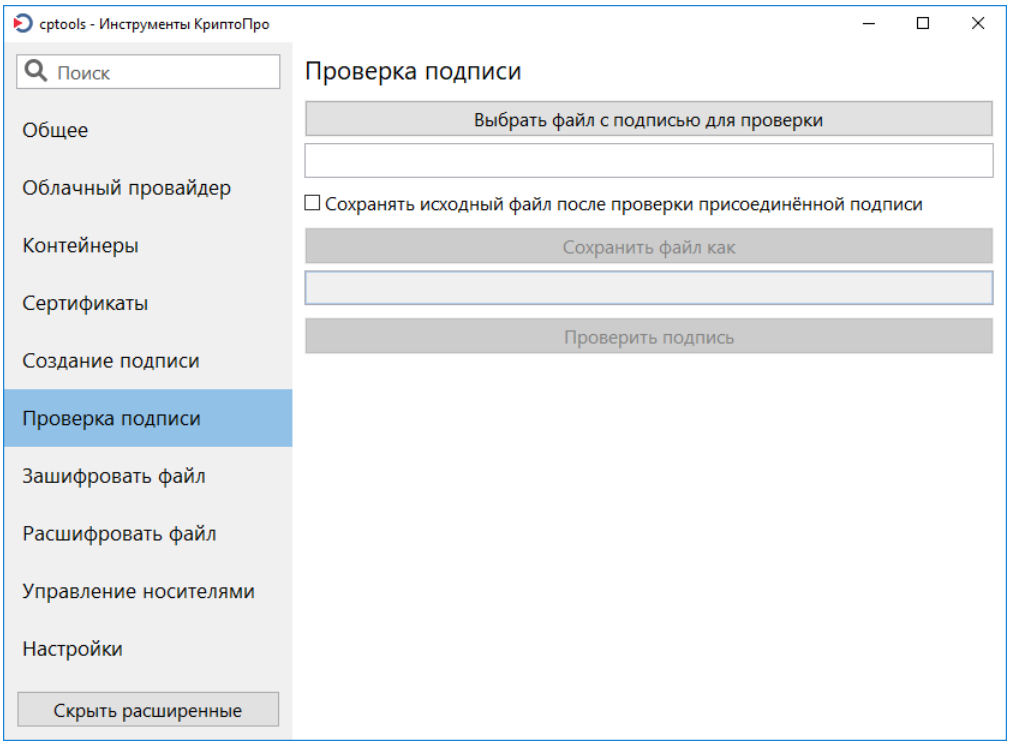

Рисунок 24. Вкладка **Проверка подписи**

Для проверки присоединенной подписи:

1) нажмите кнопку **Выбрать файл с подписью для проверки** и выберите файл с подписью (или введите адрес файла вручную в поле под кнопкой);

2) если после проверки подписи необходимо сохранить исходный файл:

- перейдите в расширенный режим использования панели по кнопке **Показать расширенные**;
- установите флаг **Сохранять исходный файл после проверки присоединенной подписи**;
- выберите путь к сохраняемому файлу по кнопке **Сохранить файл как** (или введите его вручную в поле под кнопкой);

3) нажмите кнопку **Проверить подпись**.

Для проверки отсоединенной подписи:

1) нажмите кнопку **Выбрать файл с подписью для проверки** и выберите файл с подписью (или введите адрес файла вручную в поле под кнопкой);

2) нажмите кнопку **Проверить подпись**;

3) если исходный файл и файл с подписью расположены в разных директориях или имеют несоответствующие друг другу имена (например, test и sign.sig вместо test и test.sig), откроется окно для выбора исходного файла. В открывшемся окне выберите исходный файл, подпись которого проверяется.

Если в результате проверки подписи возникла ошибка, внизу окна красным цветом отобразится соответствующее сообщение. Нажмите на сообщение, чтобы открыть подробную информацию об ошибке (см. Рисунок 25).

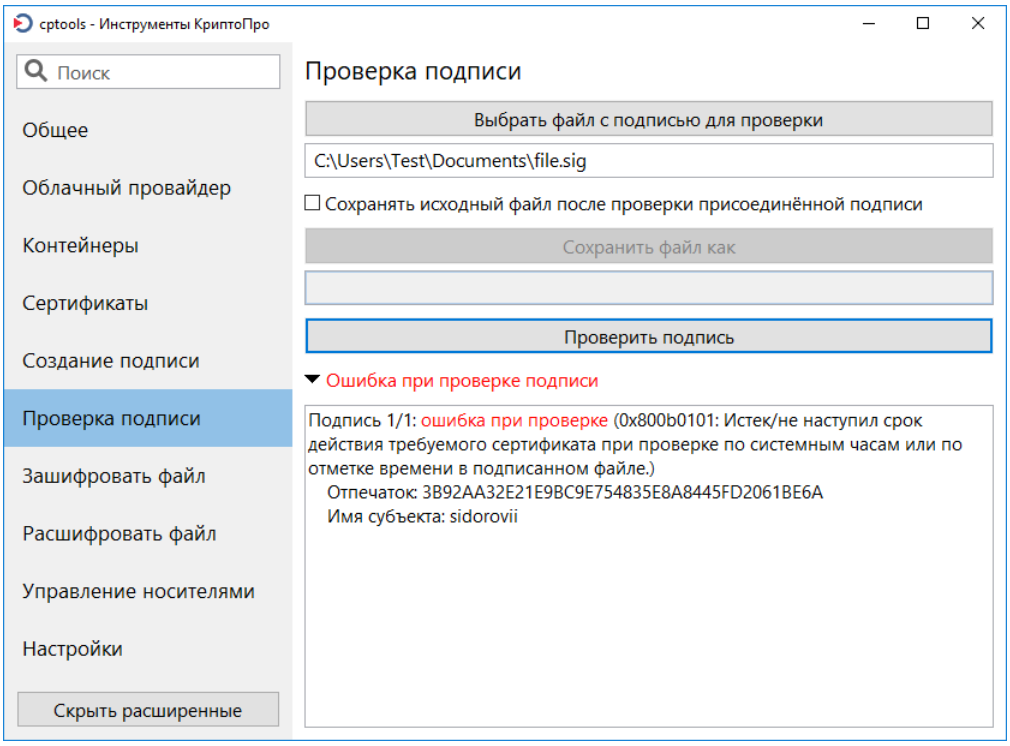

Рисунок 25. Ошибка при проверке подписи файла

2.9 Шифрование файла

Вкладка **Зашифровать файл** предназначена для шифрования файла и сохранения результата в виде CMS-файла.

Шифрование файла выполняется с использованием выбранного в окне сертификата.

Управление колонками таблицы. По умолчанию для каждого сертификата указаны имя субъекта, имя издателя, срок действия и отпечаток. В таблице можно изменить перечень отображаемых свойств сертификата (и соответствующих колонок). Для этого нажмите правой кнопкой мыши на название любой колонки и в выпадающем списке укажите те колонки, которые необходимо отобразить в таблице.

Для изменения порядка отображения колонок левой кнопкой мыши зажмите название колонки и перетяните ее на необходимое место в таблице.

Сортировка сертификатов. В таблице доступна сортировка сертификатов по одной из колонок таблицы. По умолчанию сертификаты отсортированы по значению отпечатка. Чтобы отсортировать сертификаты, нажмите на название необходимой колонки. По умолчанию выполняется сортировка по алфавиту. Чтобы изменить направление сортировки, повторно нажмите на название колонки.

Поиск сертификата. Для быстрого поиска необходимого сертификата воспользуйтесь поисковой строкой «Поиск сертификата». Поиск осуществляется по всем полям одновременно.

В расширенном режиме использования панели доступна дополнительная опция — выбор сертификата из хранилища сертификатов локального компьютера (функция доступна при запуске панели с правами администратора (суперпользователя)).

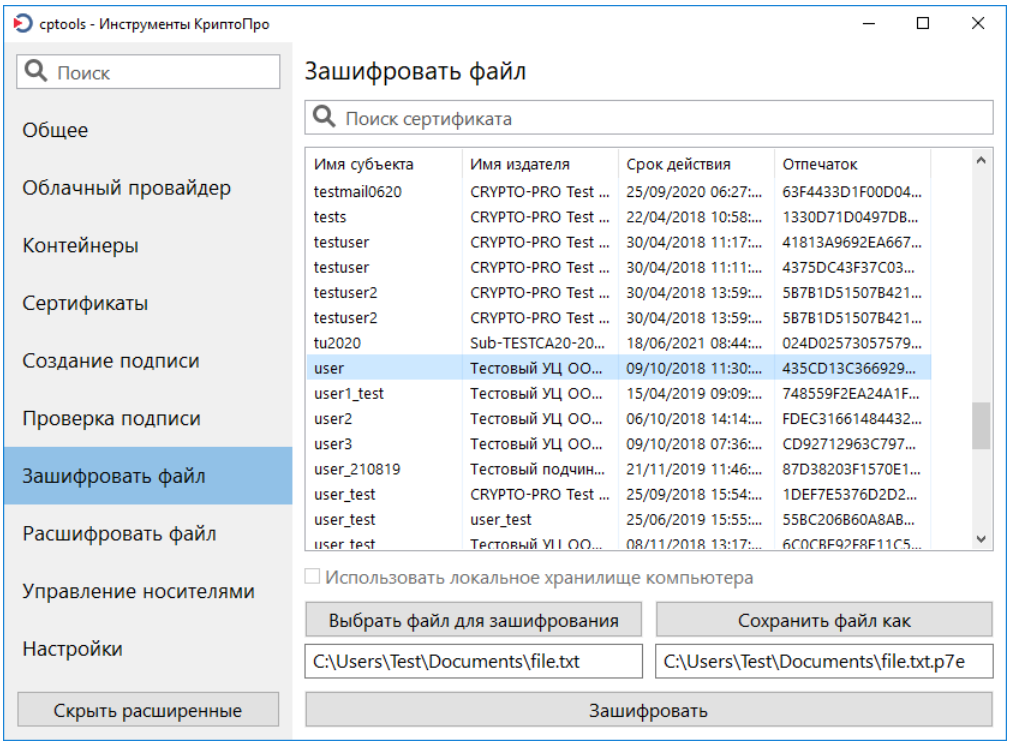

Рисунок 26. Вкладка **Зашифровать файл**

Для шифрования файла:

1) на вкладке **Зашифровать файл** выберите сертификат, который будет использоваться для шифрования файла;

2) нажмите кнопку **Выбрать файл для зашифрования** и выберите файл, который необходимо зашифровать (или введите адрес файла вручную в поле под кнопкой);

3) поле с адресом зашифрованного файла заполнится автоматически; при необходимости измените адрес или имя файла вручную или с помощью кнопки **Сохранить файл как**;

4) нажмите кнопку **Зашифровать**.

Если в результате шифрования файла возникла ошибка, внизу окна красным цветом отобразится соответствующее сообщение.

2.10 Расшифрование файла

Вкладка **Расшифровать файл** предназначена для расшифрования полученного зашифрованного файла.

Примечание. Для успешного расшифрования файла на компьютере должен быть установлен сертификат, который использовался для зашифрования, с соответствующим закрытым ключом.

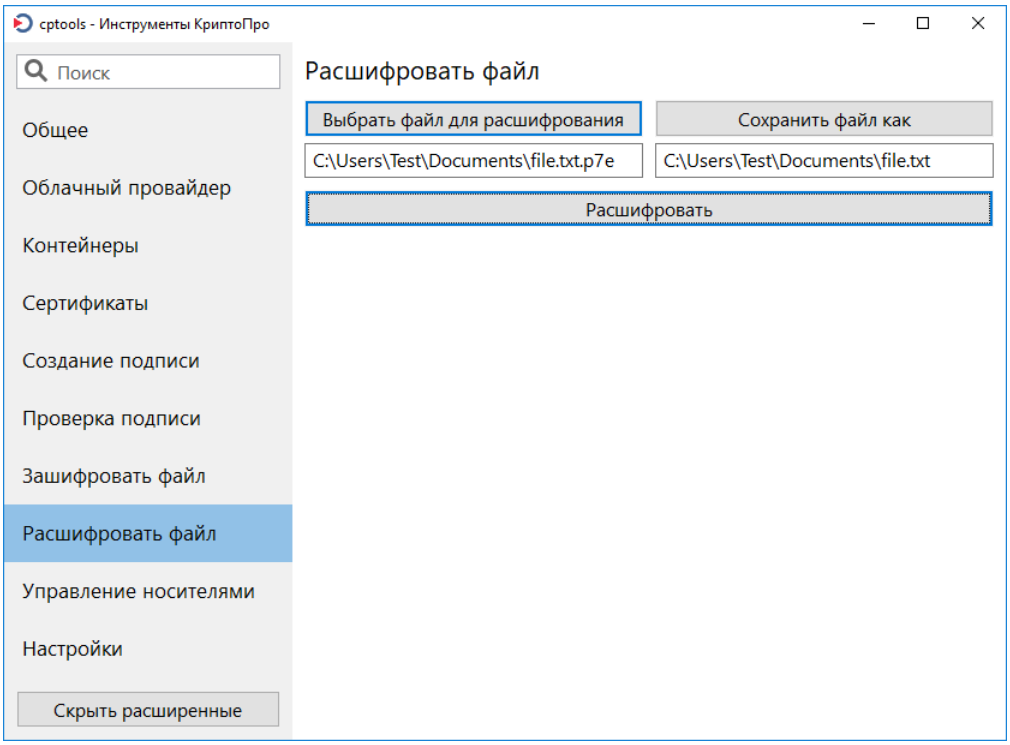

Рисунок 27. Вкладка **Расшифровать файл**

Для расшифрования файла:

1) нажмите кнопку **Выбрать файл для расшифрования** и выберите зашифрованный файл (или введите адрес файла вручную в поле под кнопкой);

2) поле с адресом расшифрованного файла заполнится автоматически; при необходимости измените адрес или имя файла вручную или с помощью кнопки **Сохранить файл как**;

3) нажмите кнопку **Расшифровать**;

4) если на контейнер ключа установлен пароль, введите его в окне аутентификации в контейнере.

Если в результате расшифрования файла возникла ошибка, внизу окна красным цветом отобразится соответствующее сообщение.

2.11 Управление носителями

Инструменты КриптоПро предоставляет интерфейс управления некоторыми параметрами подключенных съемных ключевых носителей.

Примечание. Некоторые функции управления паролями недоступны для ряда носителей. В таких случаях соответствующие кнопки на вкладке неактивны. Для выполнения этих действий воспользуйтесь ПО производителя ключевого носителя.

Вкладка **Управление носителями** доступна в расширенном режиме использования панели.

Для установки параметров носителя выберите его из выпадающего списка **Выберите считыватель**. Поле **Выберите приложение (режим работы)** позволяет указать один из поддерживаемых носителем режимов работы:

- работа в режиме пассивного хранилища ключевой информации;
- работа в режиме активного вычислителя без защиты канала между носителем и СКЗИ;
- работа в режиме активного вычислителя с защитой канала между носителем и СКЗИ по протоколу

SESPAKE.

Если носитель поддерживает лишь один режим работы, поле **Выберите приложение (режим работы)** неактивно.

Примечание. На некоторых носителях установлены счетчики неправильных попыток ввода пароля носителя. При вводе неверного пароля значение счетчика уменьшается на 1. Если в поле «Осталось попыток» указано значение 1, при следующей неудачной попытке ввода пароля носитель заблокируется. Действия, необходимые для разблокировки носителя, зависят от модели используемого носителя. Для выполнения этих действий воспользуйтесь инструкциями производителя ключевого носителя.

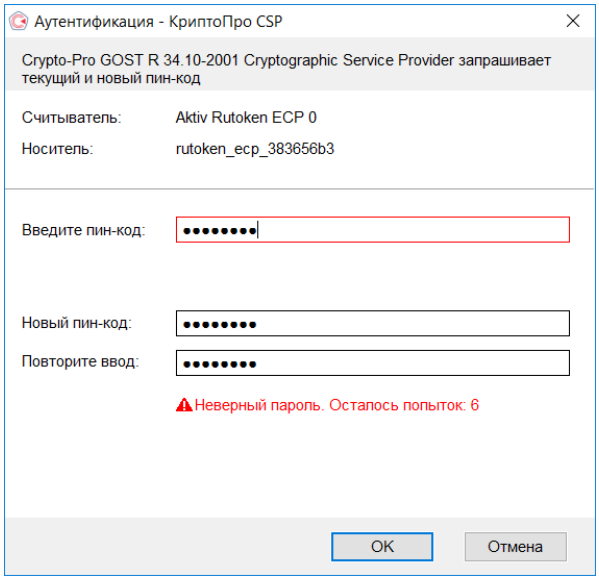

Рисунок 28. Ввод неверного пароля носителя

Доступны следующие функции управления носителями:

1) **Сменить пароль носителя** — позволяет установить новый пароль носителя. Для изменения пароля введите текущий пароль и дважды новый в окне аутентификации.

2) **Сменить PUK** — позволяет установить новый пароль администратора (PUK). Для изменения пароля введите текущий PUK и дважды новый в окне аутентификации.

3) **Вернуть пароль по умолчанию** — позволяет установить на носитель пароль, заданный производителем устройства по умолчанию. Для установки пароля по умолчанию введите текущий пароль в окне аутентификации.

4) **Вернуть заводские настройки** — позволяет вернуть устройство к заводскому состоянию. **При этом все данные, хранящиеся на носителе, будут удалены!**

5) **Сбросить счетчик попыток** — позволяет обнулить значение счетчика неправильных попыток ввода пароля носителя. Для сброса значения счетчика введите пароль администратора (PUK) в окне аутентификации.

6) **Забыть пароль** — позволяет удалить все пароли, хранящиеся в кэше провайдера или носителя.

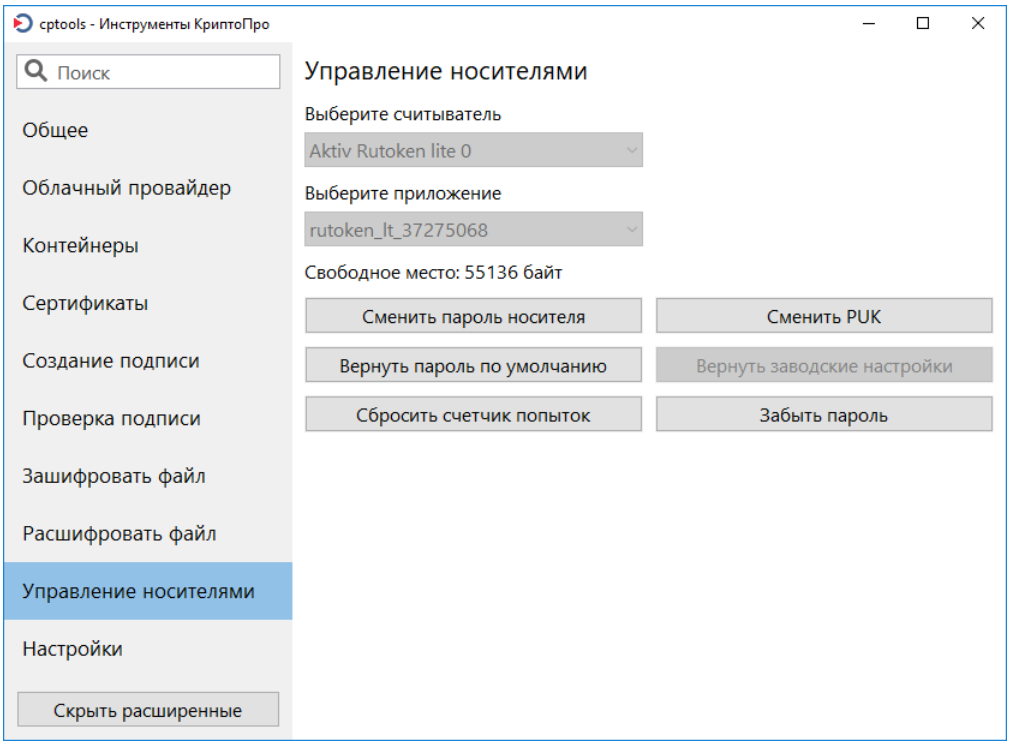

Рисунок 29. Вкладка **Управление носителями**

2.12 Дополнительные настройки провайдера

Вкладка **Настройки** доступна в расширенном режиме использования панели.

Доступны следующие дополнительные настройки КриптоПро CSP:

• **Настройки облачного провайдера** — позволяет установить значение тайм-аута при подключении к серверу DSS. По умолчанию значение не установлено. Опция доступна только при запуске панели с правами администратора (суперпользователя).

• **Удаление сохраненных паролей** — позволяет удалить все сохраненные пароли контейнеров текущего пользователя. Для удаления сохраненных паролей контейнеров в локальном хранилище компьютера необходимо запустить приложение с правами администратора (суперпользователя).

• **Настройки по умолчанию** — восстанавливает настройки приложения по умолчанию, приложение будет перезапущено.

• **Поддержка средств подтверждения подписи** — позволяет включить поддержку и принудительное использование средств подтверждения подписи. Опции доступны только при запуске панели с правами администратора (суперпользователя).

2.12.1 Подтверждение подписи

Флаг **Включить поддержку средств подтверждения подписи** включает механизм СКЗИ, позволяющий передавать содержимое подписываемого документа средствам визуализации подписываемых данных, таким как Рутокен PINPad, SafeTouch PRO и КриптоПро DSS.

Флаг **Принудительно использовать устройства подтверждения подписи** позволяет обеспечить поддержку подписи данных ТОЛЬКО с использованием устройств подтверждения подписи. Данная опция позволяет использовать указанные устройства в старых приложениях без разработки специального API.

Флаг доступен для установки только при включении поддержки средств подтверждения подписи.

Для применения изменений после установки флагов требуется перезапуск приложения.

Примечание. Опция отключает возможность выполнения операции подписи без устройства подтверждения. Данная особенность может быть полезной для ограничения использования других ключевых носителей с целью повышения общего уровня безопасности. Чтобы вернуть возможность использования любых поддерживаемых ключевых носителей, отключите флаг **Принудительно использовать устройства подтверждения подписи** и перезапустите приложение.

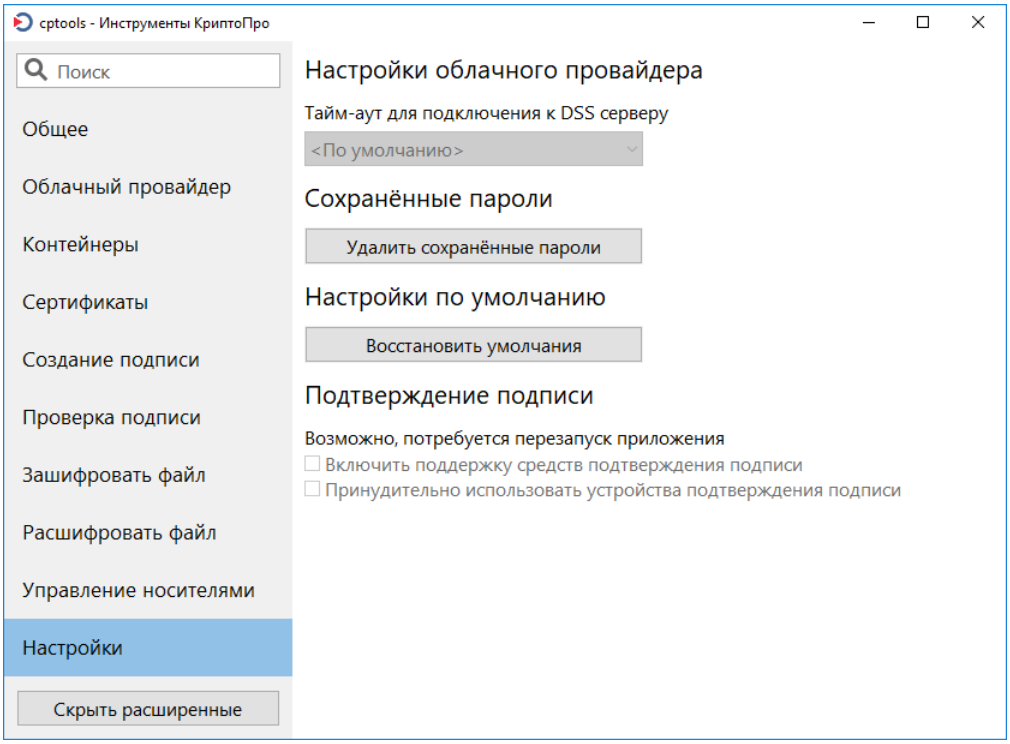

Рисунок 30. Вкладка **Настройки**