1424033, РМЭ, г. Йошкар-Ола, ул. Петрова, д.1
E-mail: info@trusted.ru

КриптоАРМ ГОСТ

Руководство пользователя

2020 год

Оглавление

1 Введение

КриптоАРМ ГОСТ — это универсальное приложение с графическим пользовательским интерфейсом для выполнения операций по созданию и проверке электронной подписи файлов, шифрования и расшифрования, управления сертификатами, размещенными в хранилищах криптопровайдеров.

Приложение КриптоАРМ ГОСТ является кроссплатформенным, и представлено различными установочными дистрибутивами под платформы: Microsoft Windows, Linux, OSX. На каждой из платформ реализована поддержка российских криптографических стандартов (в том числе ГОСТ Р 34.10-2012) посредством использования криптопровайдера КриптоПро CSP.

2 Функциональность версии 2.5

Приложение текущей версии рассчитано на выполнение операций:

Электронная подпись	– электронная подпись произвольных файлов размером до 2 Гб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память; – проверка электронной подписи файлов размером до 2 Гб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память; – добавление электронной подписи (функция создания соподписи) размером до 2 Гб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память; – создание присоединенной и отделенной электронной подписи; – поддержка стандарта электронной подписи ГОСТ Р 34.10-2012; – создание подписи со штампом времени на подпись и подписываемые данные; – создание усовершенствованной подписи; – подпись сертификатом DSS.
Шифрование	– шифрование и расшифрование файлов размером до 2 Гб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память; – удаление исходных файлов после шифрования; – шифрование по стандарту PKCS#7/CMS.
Управление сертификатами и ключами	– отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых криптопровайдеров; – проверка корректности выбранного сертификата с построением цепочки доверия и скачиванием актуального списка отзыва; – хранение закрытых ключей на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.), ESMART (ISBC) при условии использования криптопровайдера КриптоПро CSP; – создание запросов на сертификат; – импорт сертификатов с привязкой к закрытому ключу;

	– экспорт сертификатов; – удаление сертификатов; – импорт сертификатов из DSS.
Просмотр и управление журналом операций	– отображение результатов операций, которые производились в приложении.
Работа с файлами в каталоге Документы	– сохранение всех результатов выполнения операций с файлами в централизованном каталоге Документы
Работа с сервисам УЦ	– подключение и отправка запросов на сертификат через КриптоПро УЦ 2.0
Управление списком доверенных сервисов	– управление списком доменных имен сайтов, с которых разрешена обработка запросов приложением

3 Назначение и условия применения

Приложение КриптоАРМ ГОСТ предназначено для создания и проверки электронной подписи, шифрования и расшифрования файлов посредством использования криптопровайдера КриптоПро CSP.

Криптопровайдер (Cryptography Service Provider, CSP) — это независимый модуль, позволяющий осуществлять криптографические операции с помощью функций CryptoAPI.

3.1 Поддерживаемые криптопровайдеры

В приложении осуществляется поддержка криптопровайдера КриптоПро CSP версии 5.0 и выше.

3.2 Поддерживаемые ключевые носители

В приложении поддерживается работа с ключевыми носителями Рутокен, JaCarta, Esmart через криптопровайдер КриптоПро CSP.

3.3 Лицензия на программный продукт

При первой установке приложения активируется временная лицензия сроком на 14 дней. После истечения ознакомительного периода для полнофункциональной работы приложения требуется приобретение и установка лицензии. Без установки лицензии операции подписи, расшифрования, установления TLS соединения выполняться не будут.

Для приобретения лицензии на программный продукт КриптоАРМ ГОСТ можно обратиться в компанию разработчика приложения.

3.4 Системные требования

Для приложения сформулированы минимальные системные требования к конфигурации оборудования под платформами:

Windows

- Процессор Intel Core 2 Duo, Core i3, Core i5, Core i7 или Xeon (64 - бита), поддержка CMPXCHG16b, PrefetchW, LAHF/SAHF и SSE2;
- 4Gb оперативной памяти;
- 150 Mb дискового пространства для установки и работы приложения;
- Видеоадаптер DirectX версии не ниже 9 с драйвером WDDM 1. Должно поддерживаться минимальное разрешение 800x600.

Mac

- Процессор Intel Core 2 Duo, Core i3, Core i5, Core i7 или Xeon (64 - бита);
- 4Gb оперативной памяти;
- 150 Mb дискового пространства для установки и работы приложения;

- требование к видеоадаптеру не критично. Должно поддерживаться минимальное разрешение 800x600.

Linux

- Двухъядерный процессор с частотой 1,6GHz и мощнее - Unity, Gnome, KDE.
- 4Gb оперативной памяти;
- 150 Mb дискового пространства для установки и работы приложения;
- требование к видеоадаптеру не критично. Должно поддерживаться минимальное разрешение 800x600.

3.5 Поддерживаемые операционные системы

Каждая выпускаемая версия программного продукта тестируется на работоспособность заявленного функционала на операционных системах:

- Microsoft Windows 10 64bit/32bit.
- Ubuntu 19.10 64bit и выше.
- CentOS 7, 8 64bit.
- Rosa Fresh R11 64bit
- Rosa Enterprise Desktop
- ОС РОСА «КОБАЛЬТ» для клиентских систем
- ОС РОСА «КОБАЛЬТ» для серверных систем
- ROSA Enterprise Linux Server
- ОС на платформе Альт 64bit- Альт Рабочая Станция 8/9, Альт Рабочая Станция К 8/9, . Альт 8/9 СП, Альт Образование 8/9.
- Ось 2.1 64bit.
- Astra Linux Special Edition 1.6, релиз «Смоленск» 64bit
- РЕД ОС 7.1 МУРОМ 64bit
- РЕД ОС 7.2
- Mac OS X 10.12, 10.13, 10.15.

Не исключается возможность работы приложения на других платформах, не входящих в представленный выше перечень.

Но следует учесть, что для работы с ГОСТ алгоритмами необходима установка криптопровайдера КриптоПРО CSP на выбранную платформу.

Тестирование корректности работы приложения на иных платформах возлагается на самого пользователя. Для этих целей вместе с приложением устанавливается временный лицензионный ключ сроком на 14 дней.

3.6 Доля использования OpenSource проектов

При разработке программного продукта были использованы OpenSource проекты:

- Electron - MIT License
- archiver - MIT License
- history - MIT License
- immutable - MIT License
- request - Apache License 2.0
- reselect - MIT License
- sudo-prompt - MIT License
- winston - MIT License
- react - MIT License

4 Подготовка к работе

В данном разделе описана установка и настройка рабочего места для работы с приложением.

4.1 Установка КриптоАРМ ГОСТ

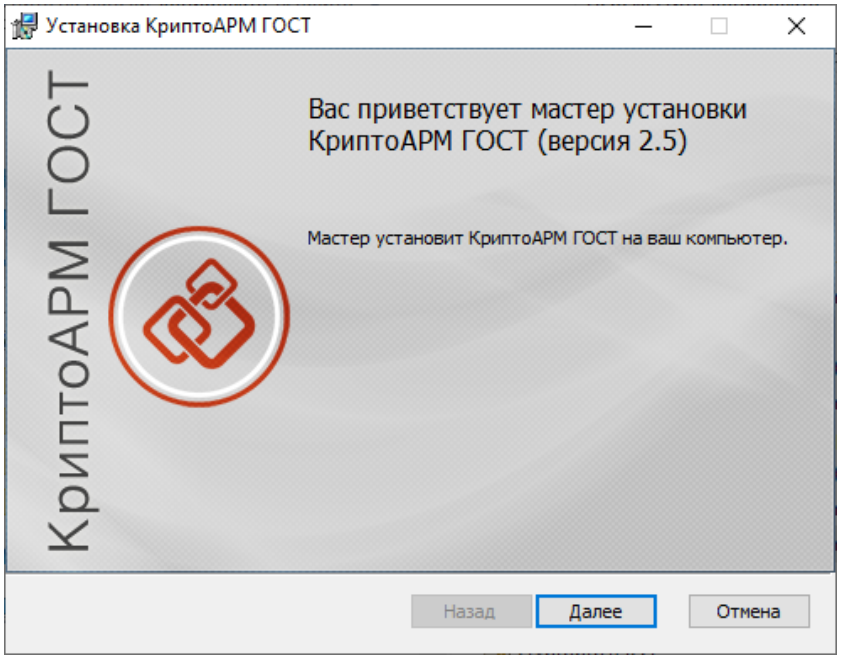
4.1.1 Установка на платформу Microsoft Windows

Для установки приложения КриптоАРМ ГОСТ на платформу Microsoft Windows предлагаются два дистрибутива – под 64-битную и 32-битную платформы:

cryptoarm-gost-vx.x.x-x64.msi (где x.x.x – номер версии) для 64-разрядной ОС;

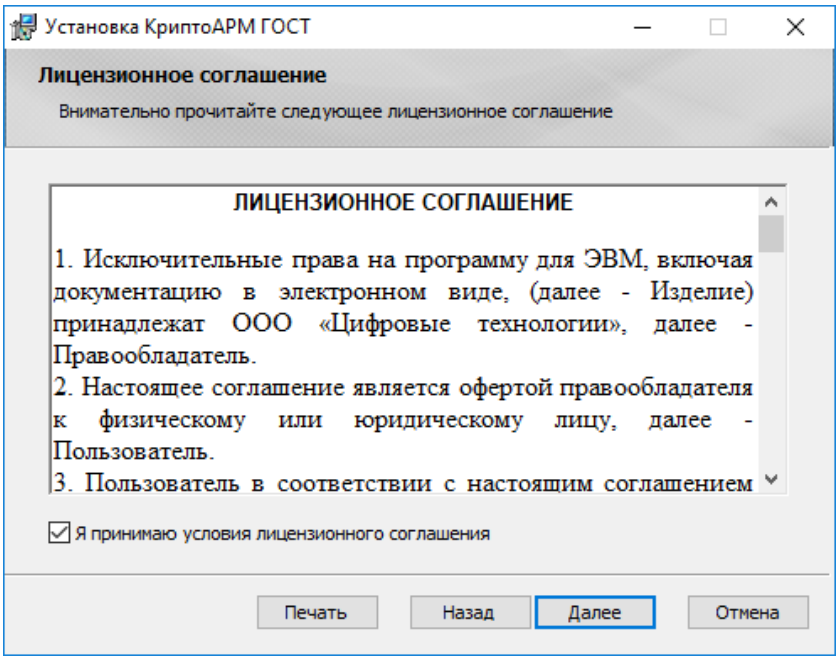
cryptoarm-gost-vx.x.x-x86.msi (где x.x.x – номер версии) для 32-разрядной ОС).

При запуске исполняемого файла, открывается мастер установки приложения КриптоАРМ ГОСТ.



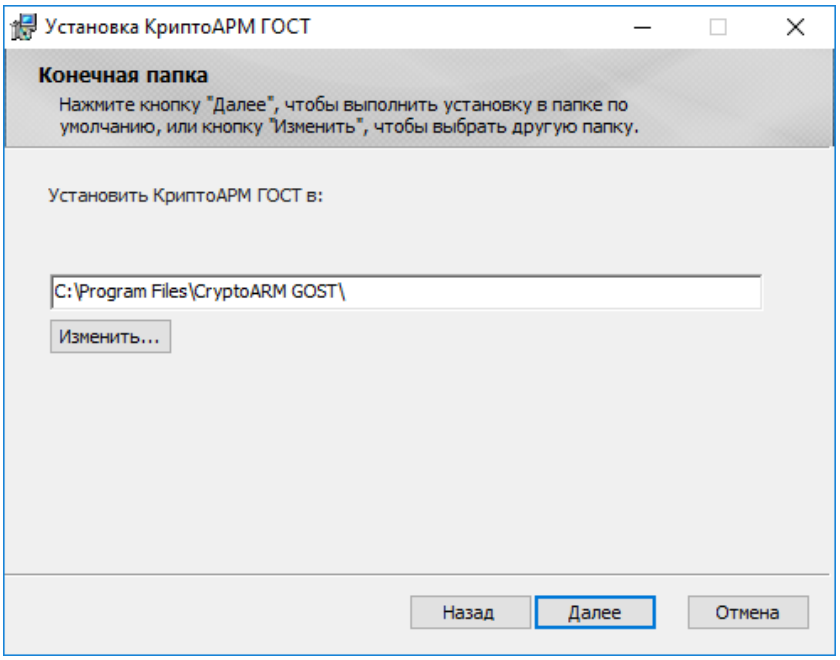
Первый шаг мастера установки приложения

По кнопке **Далее** происходит переход на следующий шаг, где предлагается ознакомиться с условиями лицензионного соглашения. В случае согласия, нужно принять условия и перейти к следующему шагу мастера, нажав кнопку **Далее**.



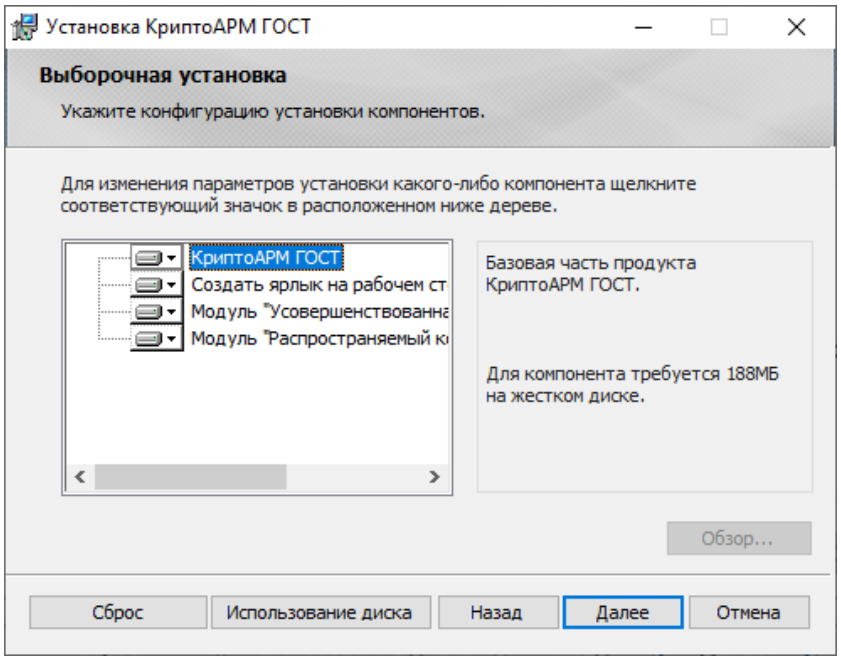
Условия лицензионного соглашения

На следующем шаге мастера можно выбрать каталог для установки КриптоАРМ ГОСТ (по умолчанию приложение устанавливается в каталог C:\Program Files\CryptoARM GOST\).



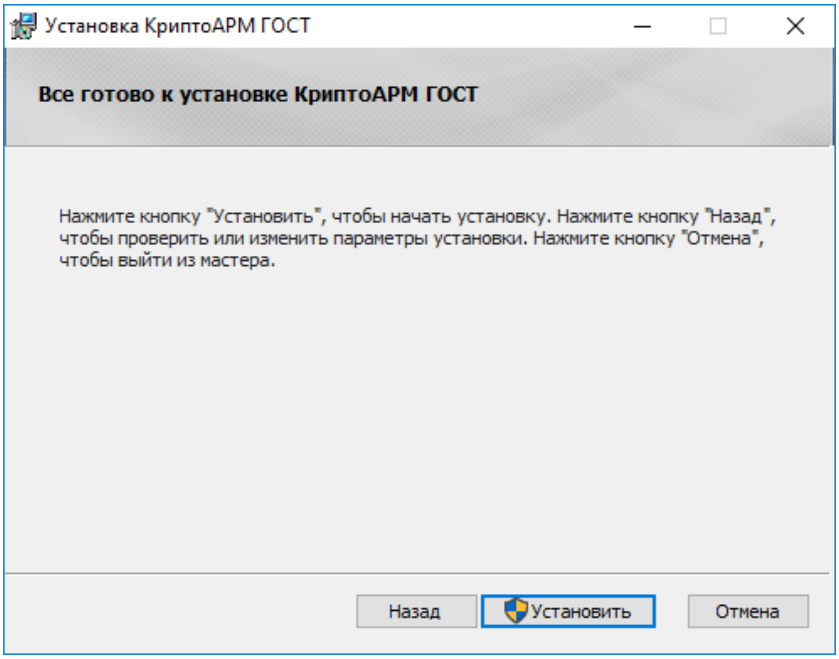
Выбор каталога установки приложения

На шаге выборочной установки можно отключить создание ярлыка на рабочем столе и установку модулей для создания усовершенствованной подписи.



Выбор компонент для установки

На заключительном шаге мастера нажмите кнопку **Установить**. Установка выполняется с правами администратора.



Установка приложения

После успешной установки приложения в главном меню появится новая группа КриптоАРМ ГОСТ, которая содержит ярлык запуска приложения КриптоАРМ ГОСТ и ярлык запуска мастера удаления программы. В указанном при установке каталоге (по умолчанию - каталог Program Files/CryptoARM GOST) будут размещаться файлы приложения КриптоАРМ ГОСТ.

4.1.2 Установка на платформу Linux

Установка приложения КриптоАРМ ГОСТ на операционную систему Linux может быть выполнена в графическом режиме (через мастер установки пакетов), через терминал в режиме командной строки и обычной распаковкой из архива.

По умолчанию приложение устанавливается в каталог /opt/cryptoarm_gost/.

- **В режиме графической установки** запустите на исполнение файл:

  cryptoarm-gost-vx.x.x-x64.rpm (где x.x.x – номер версии) для 64-разрядных ОС, основанных на RPM;

  cryptoarm-gost-vx.x.x-x64.deb (где x.x.x – номер версии) для 64-разрядных ОС, основанных на DEB.

Откроется пакетный менеджер, в котором нужно нажать **Установить**. Так как установка производится от имени администратора системы, то появится диалог ввода пароля администратора системы (Root).

- **С помощью командной строки** нужно запустить терминал и ввести команду:

  sudo dpkg -i cryptoarm-gost-vx.x.x-x64.deb - для ОС, основанных на Debian (Debian/Ubuntu);

  sudo rpm -i cryptoarm-gost-vx.x.x-x64.rpm - для ОС, основанных на RPM;

После установки приложения в меню появится ярлык КриптоАРМ ГОСТ.

В том случае, когда не поддерживается пакетный режим установки приложения, его можно установить из предоставленного архива, распаковав содержимое в каталог **/opt/cryptoarm_gost/**. Распаковку архива необходимо производить с правами администратора.

4.1.3 Настройка работы КриптоАРМ ГОСТ в режиме замкнутой программной среды на Astra Linux Special Edition Смоленск 1.6

Включение режима замкнутой программной среды описано по ссылке: https://wiki.astralinux.ru/pages/viewpage.action?pageId=41190634.

Для работы КриптоАРМ ГОСТ в режиме замкнутой программной среды надо:

- установить подписанный дистрибутив КриптоАРМ ГОСТ (если уже установлен, то переустанавливать не надо);
- скопировать ключ (https://github.com/TrustedRu/CryptoARMGOST/raw/master/trusted_pub_key.gpg) trusted_pub_key.gpg в папку /etc/digsig/keys (от имени учетной записи администратора через механизм sudo);
- выполнить команду:
  sudo update-initramfs -u -k all
- перезагрузить компьютер.

Для работы КриптоПро CSP в режиме замкнутой программной среды надо:

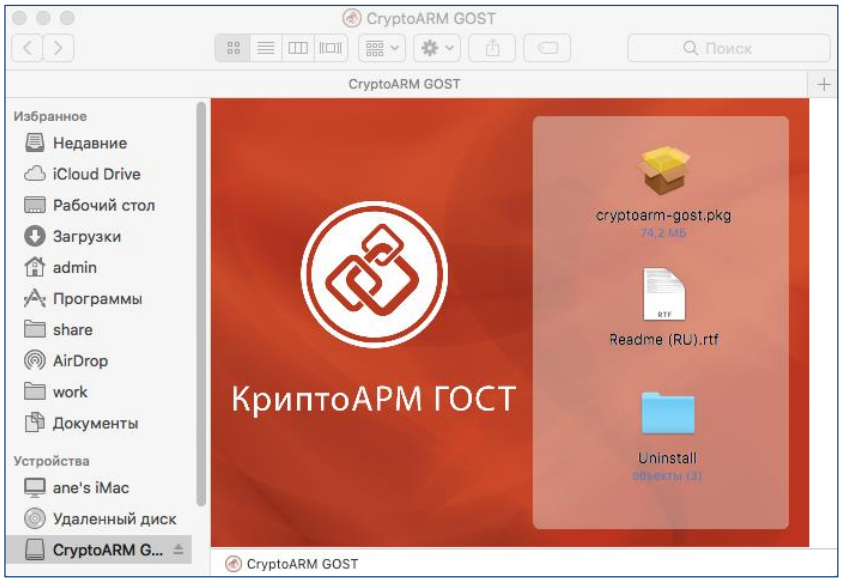
- установить КриптоПро CSP (если уже установлен, то переустанавливать не надо);

- скачать на сайте КриптоПро ключ для работы в режиме замкнутой программной среды Astra Linux SE (выложен рядом с дистрибутивом на КриптоПро CSP)
- установить пакет astra-digsig-oldkeys;
- поместить ключ в папку /etc/digsig/keys/legacy (нужно, чтобы с папке legacy обязательно были ещё 4 файла с ключами);
- выполнить команду:
  sudo update-initramfs -u -k all
- перезагрузить компьютер.

4.1.4 Установка на платформу OS X

Дистрибутив приложения КриптоАРМ ГОСТ поставляется в упакованном виде, имеет формат .dmg и представляет собой образ диска, содержащий пакет установки **cryptoarm-gost-vx.x.x-x64.pkg,** описание приложения, каталог со скриптами удаления приложения.

Для установки пакета через графический интерфейс откройте двойным щелчком образ диска с дистрибутивом **cryptoarm-gost-vx.x.x-x64.dmg** (где x.x.x – номер версии).

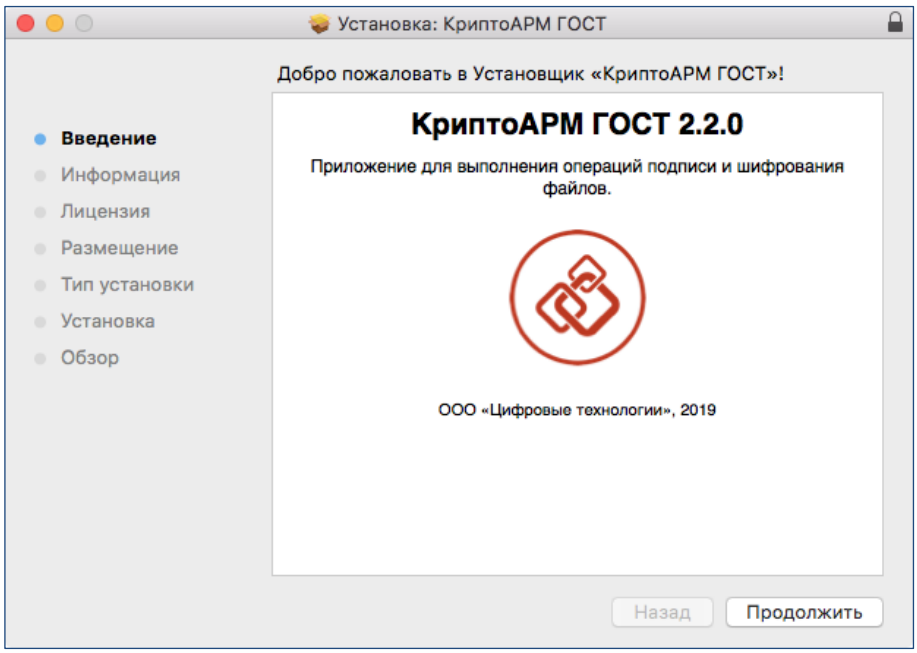


Состав образа диска

Для установки программы КриптоАРМ ГОСТ запустите на исполнение файл **cryptoarm-gost-vx.x.x-64.pkg** (где x.x.x – номер версии).

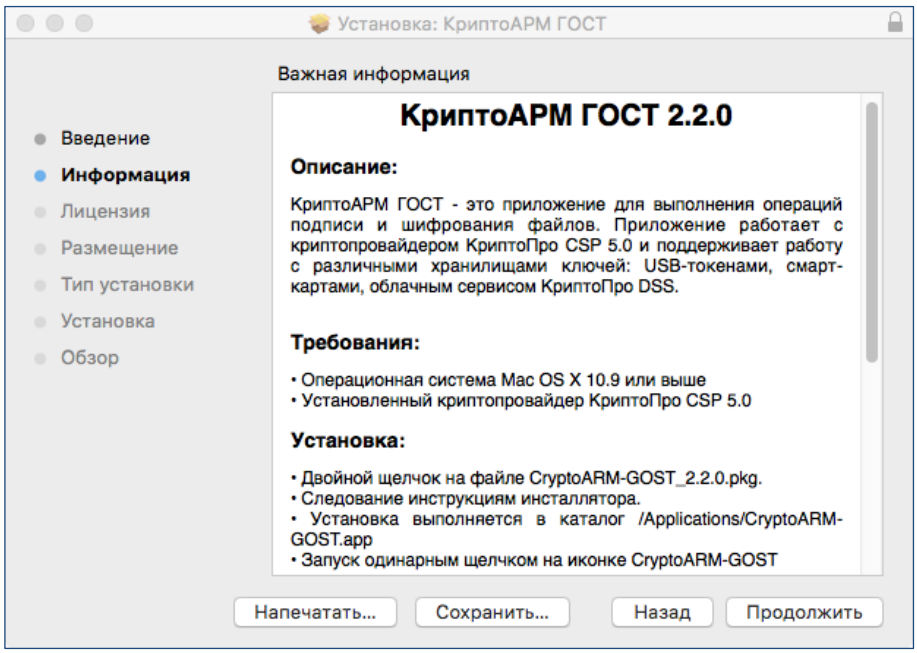
Установочный пакет для приложения КриптоАРМ ГОСТ может поставляться вне образа диска. В таком случае нужно сразу запустить файл **cryptoarm-gost-vx.x.x-64.pkg** (где x.x.x – номер версии).

Откроется мастер установки КриптоАРМ ГОСТ. Нажмите кнопку **Продолжить** для продолжения установки. На каждом шаге можно вернуться на предыдущий шаг нажатием **Назад**.



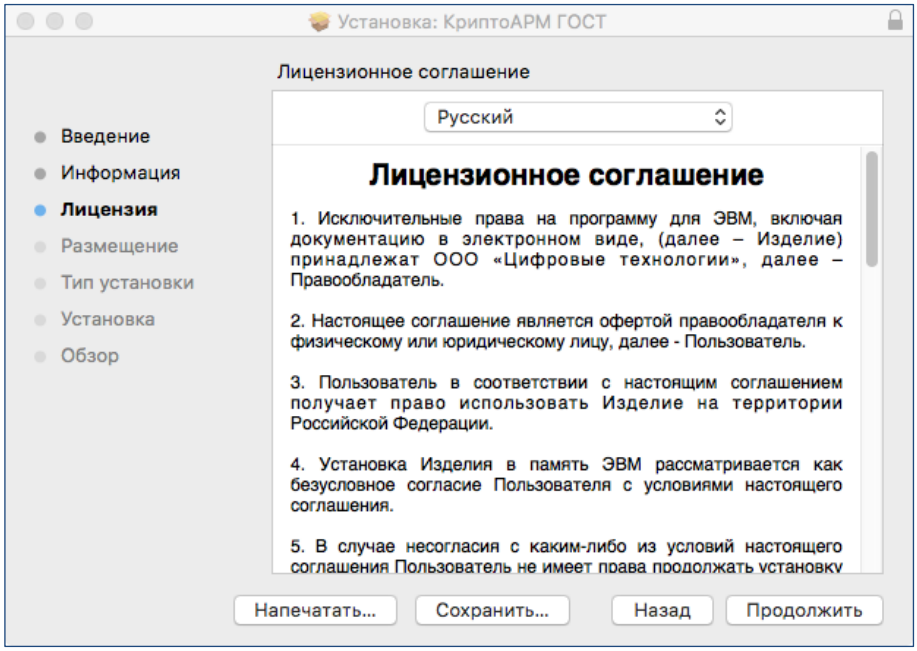
Начальный шаг мастера установки пакета приложения

Ознакомьтесь с описание программы и нажмите **Продолжить**. На данном этапе описание можно распечатать или сохранить в файл.



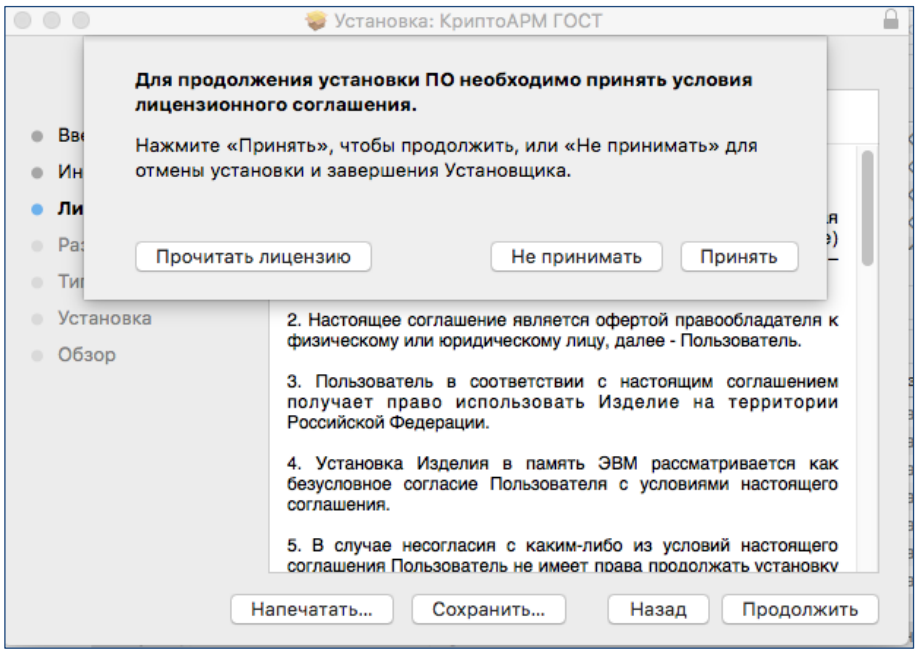
Просмотр информации о программном продукте

Ознакомьтесь с условиями лицензионного соглашения, нажмите **Продолжить**. На данном этапе лицензионное соглашение можно распечатать или сохранить в файл.



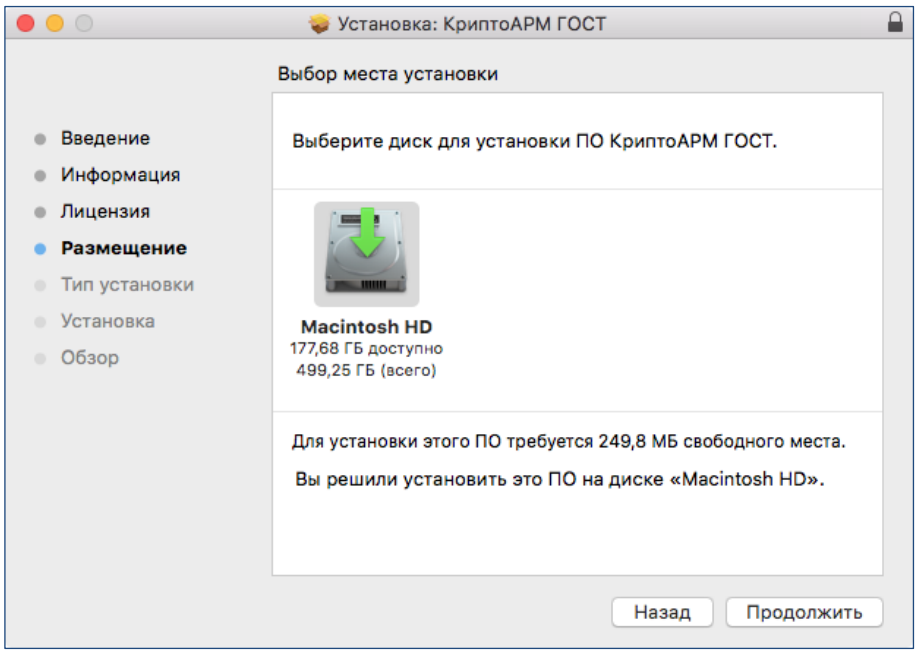
Просмотр информации о лицензии

Нажмите кнопку **Принимаю** для продолжения установки приложения или **Не принимаю** - для отмены установки.



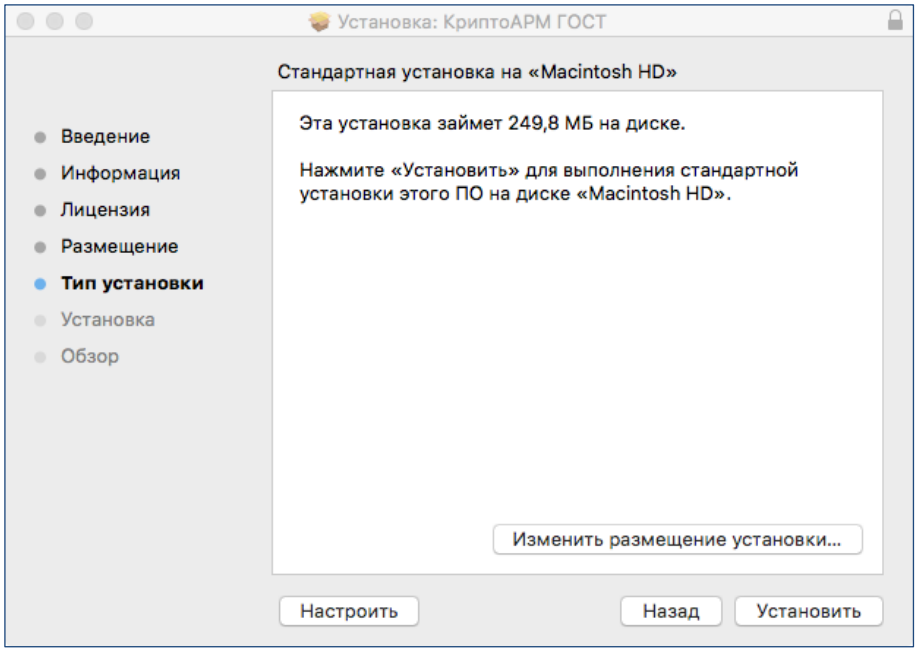
Соглашение с условиями лицензии

Выберете диск, на который будет установлено приложение и нажмите **Продолжить**.



Информация о размещении приложения на жестком диске

На следующем шаге мастера нажмите кнопку **Установить**.



Подтверждение установки на физический носитель

Введите пароль администратора и нажмите **Установить ПО.**

Начнется установка программы на компьютер. По окончании установки нажмите кнопку **Закрыть**.

После установки программы в Launchpad появится ярлык приложения КриптоАРМ ГОСТ и в каталоге Applications (Программы) будут созданы подкаталоги приложения.

После завершения установки можно отмонтировать диск стандартными средствами ОС.

4.2 Установка криптопровайдера КриптоПро CSP

Для работы приложения КриптоАРМ ГОСТ на рабочее место нужно установить СКЗИ КриптоПро CSP.

4.2.1 Установка криптопровайдера на платформу MS Windows

Для установки КриптоПро CSP на платформу Windows можно воспользоваться инструкцией установки КриптоПро CSP более ранних версий, доступной по адресу https://cryptostore.ru/article/instruktsii/kak_ustanovit_criptopro_csp/ .

4.2.2 Установка криптопровайдера на платформу Linux

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo.

4.2.2.1 Установка базовых пакетов скриптом

Установку провайдера можно осуществить, запустив файл из дистрибутива **install.sh или install_gui.sh**. Файлы из пакетов устанавливаются в **/opt/cprocsp**.

4.2.2.2 Установка пакета для модулей TSP и OCSP

Для создания подписи со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP.

Скачать архив **Linux 64 бита** по ссылке https://www.cryptopro.ru/products/cades/downloads (требуется предварительная регистрация).

Распаковать архив.

Установить пакет:

- **sudo dpkg –i cprocsp-pki-x.x.x-amd64-cades.deb – для ОС на основе ubuntu/debian**
- **sudo rpm –i cprocsp-pki-x.x.x-amd64-cades.rpm – для RPM ОС**

Для создания подписи со штампом времени или усовершенствованной подписи необходима установка лицензии на модули TSP и/или OCSP.

Для создания классической подписи без штампа времени лицензии на данные модули устанавливать не нужно.

4.2.2.3 Установка пакета для графического интерфейса ввода пароля

Для работы с контейнерами закрытых ключей требуется ввод пароля. Графический интерфейс диалога ввода пароля содержится в пакете **cprocsp-rdr-gui**, который можно установить командой:

sudo dpkg -i ./cprocsp-rdr-gui-<>.deb

4.2.2.4 Установка пакетов для работы с ключевыми носителями

Для работы электронных идентификаторов Рутокен или JaCarta в deb-based системе должны быть установлены: библиотека libccid не ниже 1.3.11, пакеты pcscd и libpcsclite1.

Для работы в RPM-based системе должны быть установлены библиотеки и пакеты ccid, pcscd и pcsc-lite

Пакеты и драйвера для работы с ключевыми носителями устанавливаются с помощью команд:

sudo dpkg -i ./cprocsp-rdr-pcsc-<...>.deb

Для ключевого носителя Рутокен:

sudo dpkg -i ./cprocsp-rdr-rutoken-<...>.deb
sudo dpkg -i ./ifd-rutokens_1.0.4_1.x86_64.deb

Для ключевого носителя JaCarta:

sudo dpkg -i ./cprocsp-rdr-jacarta -<...>.deb

Примечание. Директория расположения утилит КриптоПро CSP /opt/cprocsp/bin/<arch>/, где под <arch> подразумеваться один из следующих идентификаторов платформы: ia32 - для 32-разрядных систем; amd64 - для 64-разрядных систем.

4.2.3 Установка криптопровайдера на платформу OS X

Для установки КриптоПро CSP на платформу OS X можно воспользоваться инструкцией, доступной по адресу https://cryptoarm.ru/How-to-install-cryptopro-csp-4-on-mac-os-x .

4.2.3.1 Установка пакета для модулей TSP и OCSP

Для создания подписи со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP.

Скачать архив **Apple MacOS** по ссылке КриптоПро ЭЦП SDK 2.0 (требуется предварительная регистрация).

Установить пакет cprocsp-pki-x.x.x.pkg, следуя инструкциям на каждом шагу установщика.

Для создания подписи со штампом времени или усовершенствованной подписи необходима установка лицензии на модули TSP и/или OCSP.

Для создания классической подписи без штампа времени лицензии на данные модули устанавливать не нужно.

4.3 Установка лицензии на программный продукт КриптоАРМ ГОСТ

Для полноценной работы приложения КриптоАРМ ГОСТ необходима установка лицензионного ключа. Лицензионный ключ представляет собой файл, который необходимо расположить в специально созданном каталоге приложения.

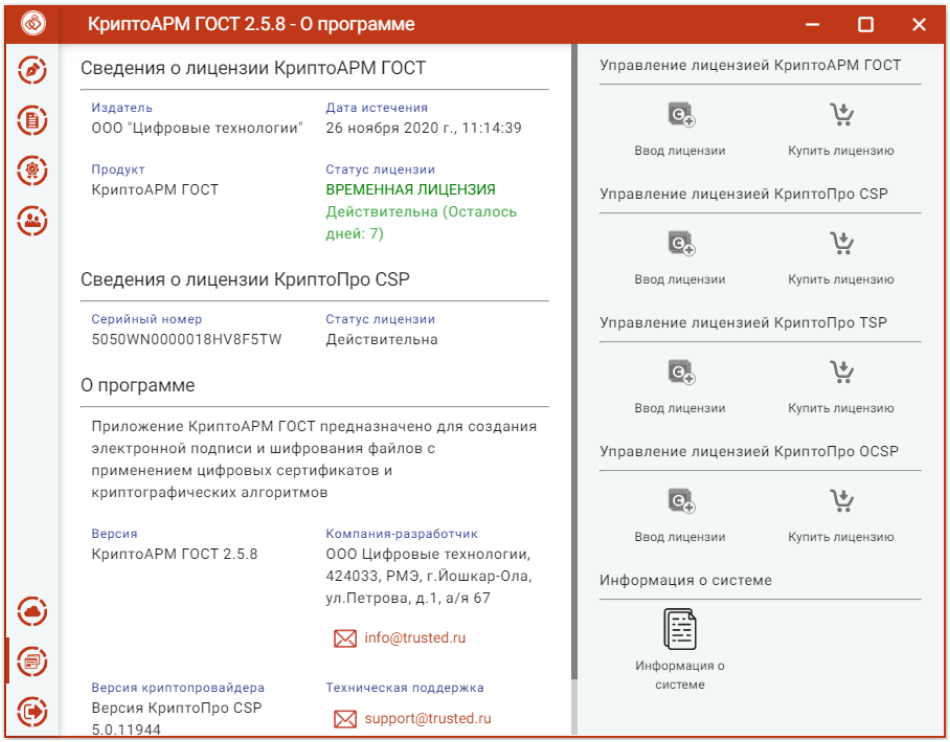
Существуют два вида лицензий – постоянная и временная. Временная лицензия предоставляется с ограниченным сроком действия. Для приобретения постоянной лицензии можно обратиться в компанию разработчика.

Установка лицензионного ключа может производиться как через пользовательский интерфейс, так и копированием файла лицензии в заданный каталог.

4.3.1 Установка лицензии через пользовательский интерфейс

4.3.1.1 Установка постоянной лицензии

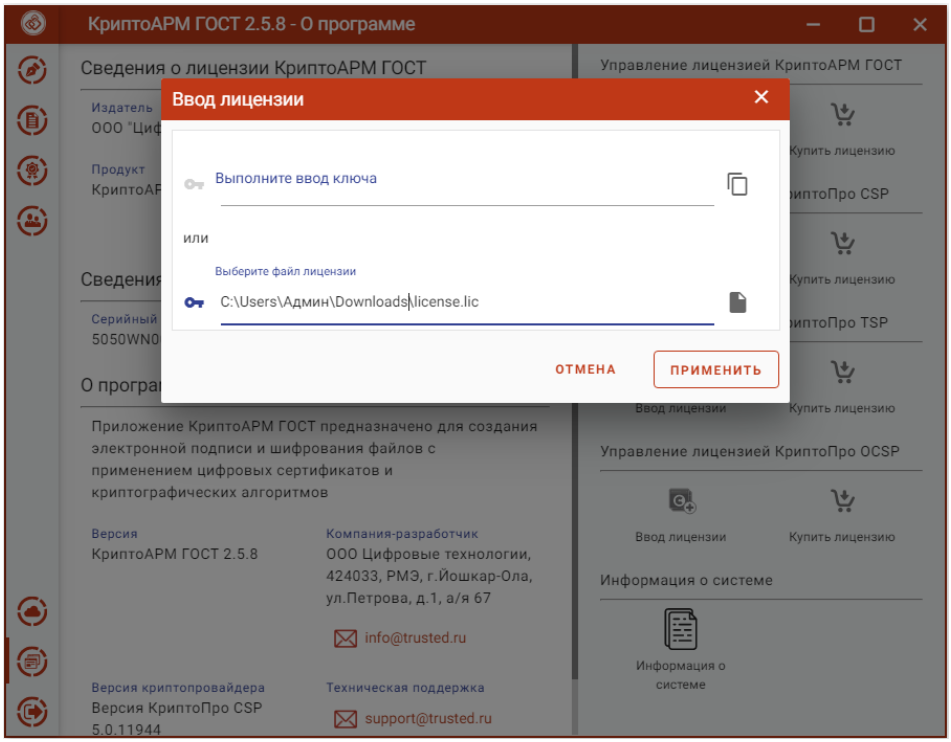
Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения. На открывшейся странице нажать на кнопку **Ввод лицензии** в разделе управления лицензией КриптоАРМ ГОСТ.



Страница ввода лицензионного ключа на программный продукт

В результате должно появиться всплывающее окно ввода лицензии, предполагающее выполнение действия одним из двух способов:

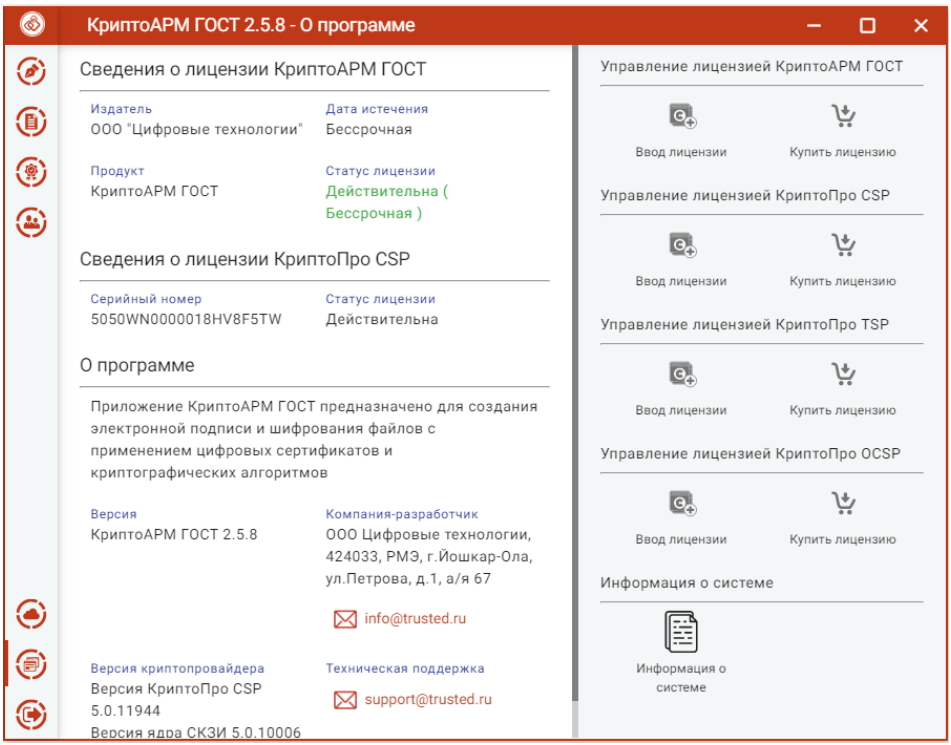
- вставить содержимое файла лицензии в текстовое поле;
- выбрать файл лицензии.



Диалоговое окно с выбором варианта ввода лицензионного ключа

Примечание. При установке лицензии будут запрошены права администратора (Root) на доступ к каталогу установки лицензии.

Если установка лицензионного ключа прошла успешно, то появляется всплывающее сообщение с информацией об этом. На странице **Лицензии** отображается информация о введенном лицензионном ключе на приложение с данными об издателе программного продукта, продукте, владельце лицензии, дате истечения лицензии, статусе лицензии.



Сведения о лицензии

В том случае, если лицензия на продукт не введена или не действительна при каждом запуске приложения будет появляться всплывающее сообщение с информацией об этом.

4.3.2 Установка лицензии копированием файла

Только для платформ **Linux** и **MacOS.**

Для установки лицензии необходимо скопировать файл лицензии license.lic в каталог /etc/opt/Trusted/CryptoARM GOST/. Если каталога нет, тосоздать.

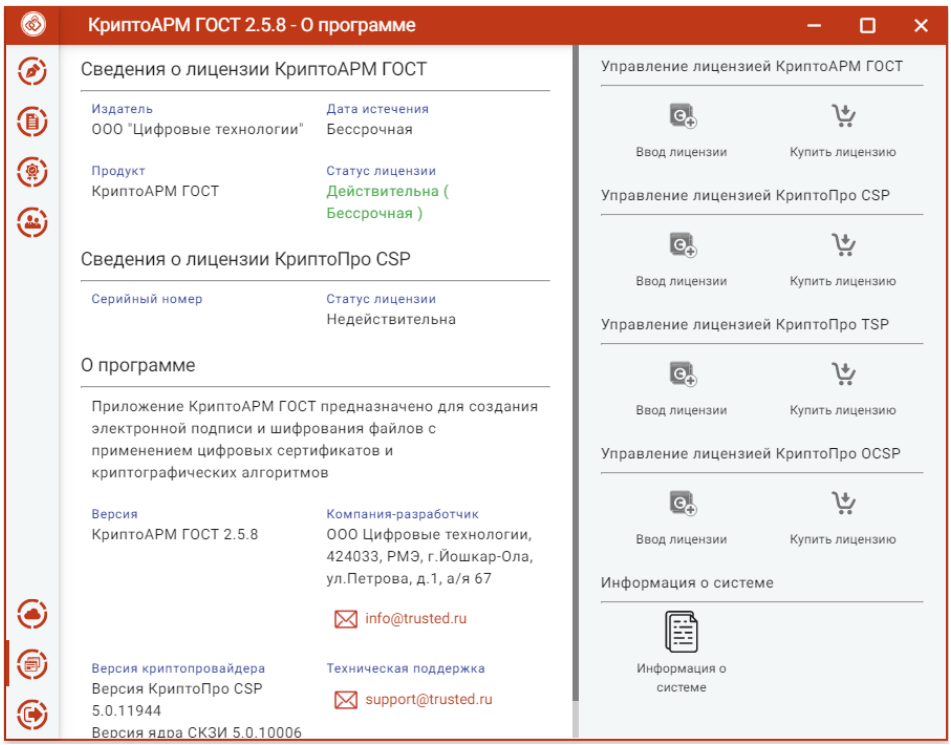
Примечание. Для последующей установки лицензии пользователями каталог КриптоАРМ ГОСТ должен иметь права на запись, а минимально необходимые права – права на чтение для пользователей на рабочем месте.

4.4 Установка лицензии на программный продукт КриптоПро CSP

Установка программного обеспечения КриптоПро CSP без ввода лицензии подразумевает использование временной лицензии 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).

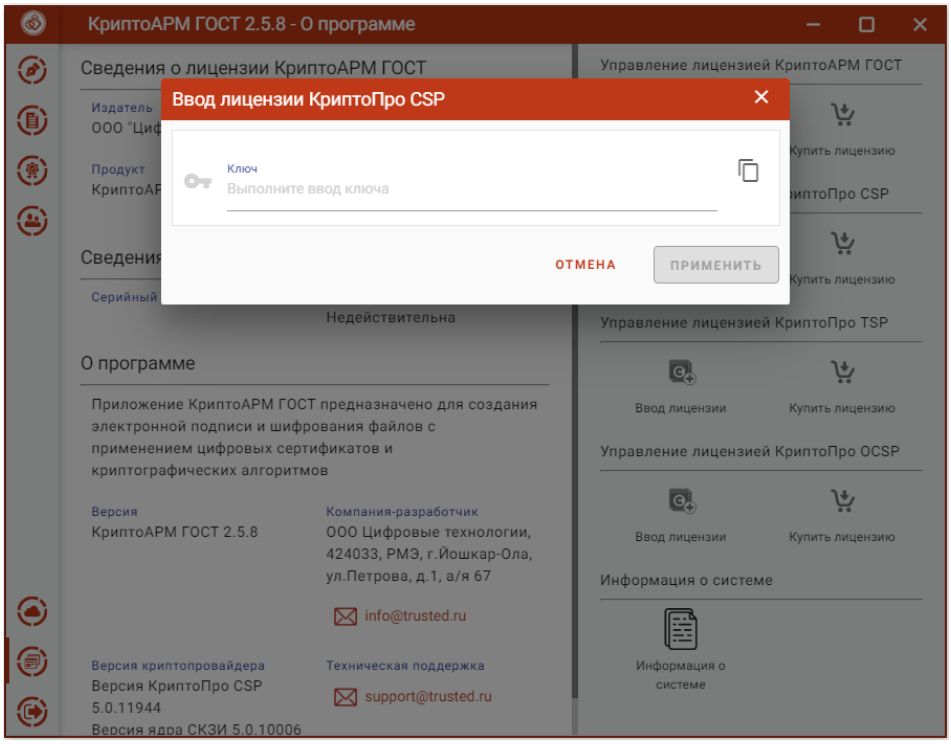
Установка лицензионного ключа может производиться как через пользовательский интерфейс приложения КриптоАРМ ГОСТ, так и с помощью консольных команд для ОС linux и MacOS, и через интерфейс программы КриптоПро CSP для ОС Windows.

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **О программе** главного меню приложения. На открывшейся странице нажать на кнопку **Ввод лицензии** в разделе управления лицензией КриптоПро CSP



Страница ввода лицензионного ключа на КриптоПРО CSP

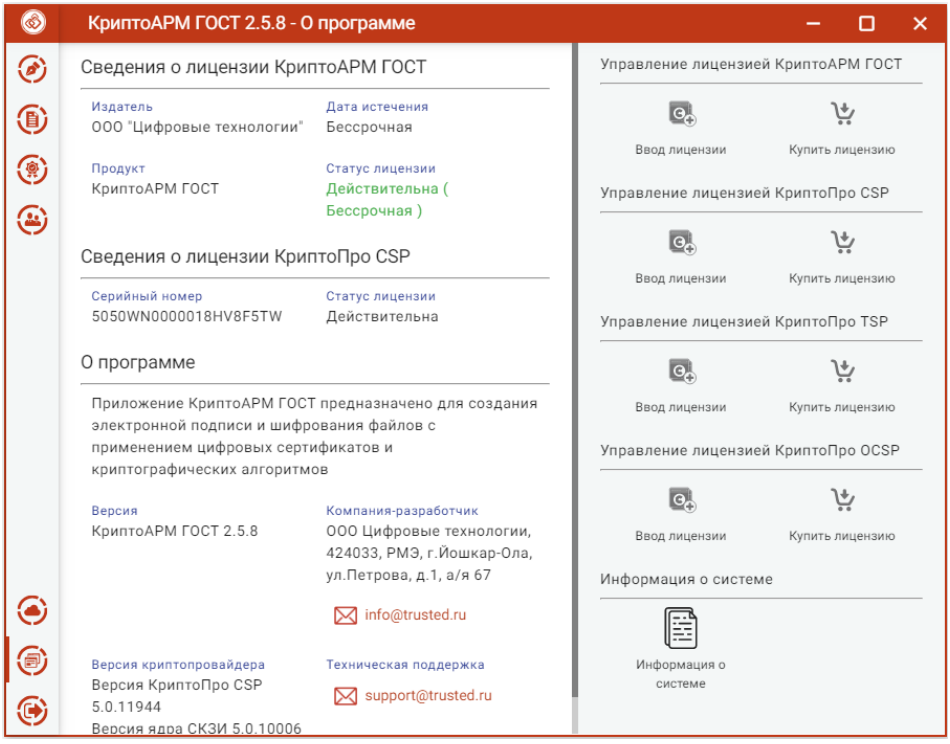
В результате появляется всплывающее окно ввода лицензии в текстовое поле.



Диалоговое окно ввода лицензионного ключа

Примечание. При установке лицензии будут запрошены права администратора (Root) на доступ к каталогу установки лицензии.

Если установка лицензионного ключа прошла успешно, то появляется всплывающее сообщение с информацией об этом. На странице **Лицензии** отображается серийный номер и статус лицензии.



Сведения о лицензии

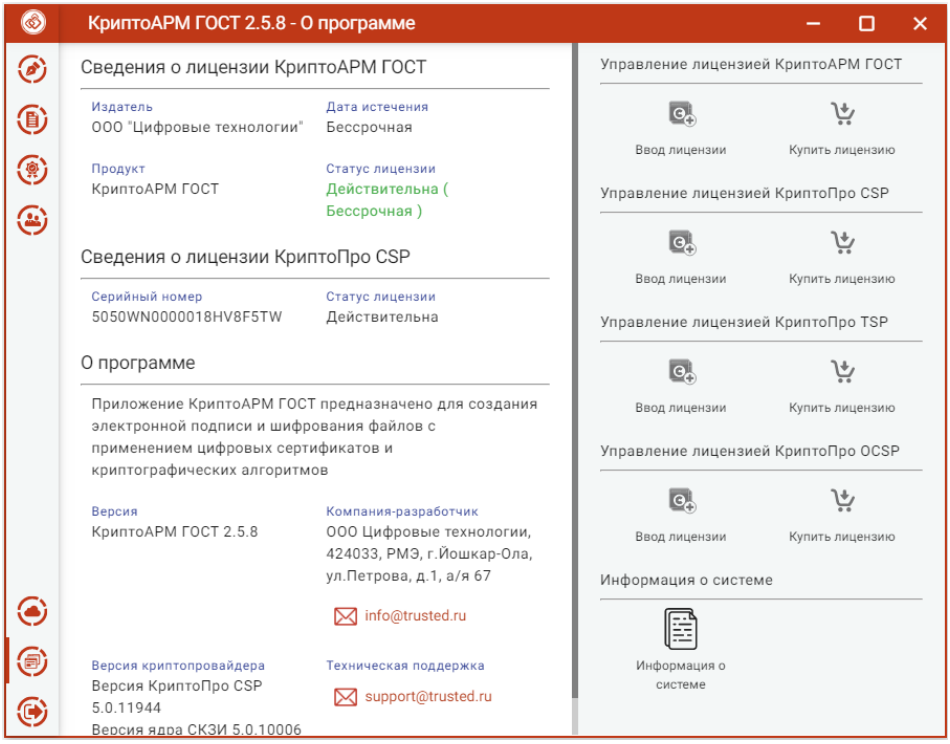
В том случае, если лицензия на продукт КриптоПро CSP не введена или не действительна при каждом запуске приложения будет появляться всплывающее сообщение с информацией об этом.

4.5 Установка лицензии на модуль TSP

Для создания подписи со штампом времени на подпись или данные необходима лицензия на модуль TSP.

Установка лицензионного ключа может производиться как через пользовательский интерфейс приложения КриптоАРМ ГОСТ, так и с помощью консольных команд для ОС linux и MacOS, и через интерфейс программы КриптоПро CSP для ОС Windows.

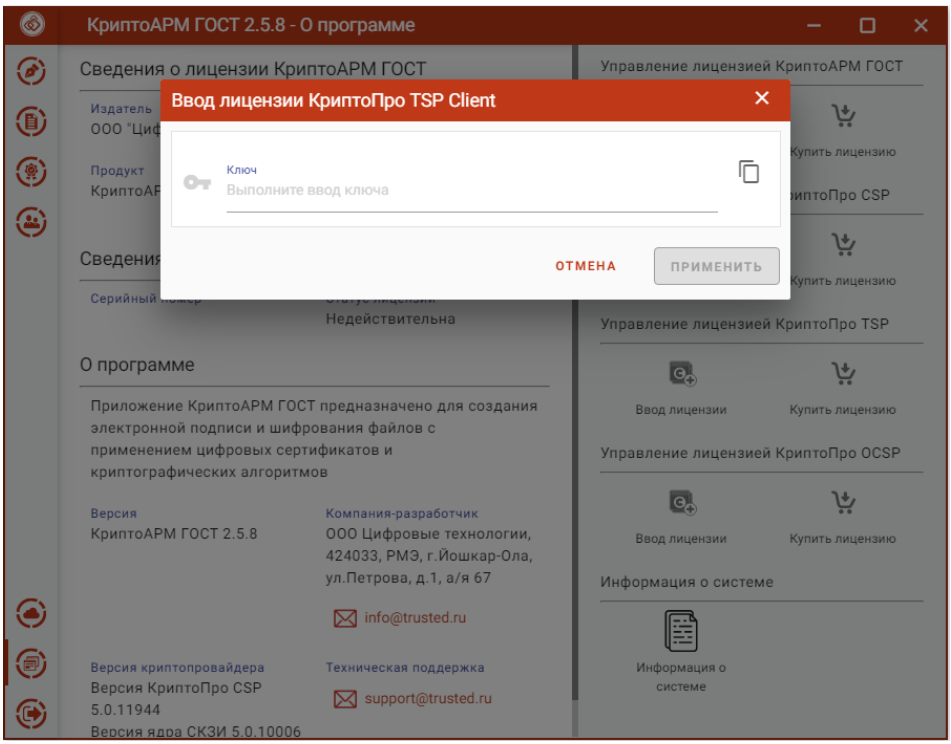
Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **О программе** главного меню приложения. На открывшейся странице нажать на кнопку **Ввод лицензии** в разделе управления лицензией модуля штампов времени (TSP).



Страница ввода лицензионного ключа на модуль TSP

Примечание: Если модуль TSP не установлен, то кнопка **Ввода лицензии** будет недоступна.

В результате должно появиться всплывающее окно ввода лицензии в текстовое поле.



Окно ввода лицензионного ключа на модуль TSP

Примечание. При установке лицензии будут запрошены права администратора (Root) на доступ к каталогу установки лицензии.

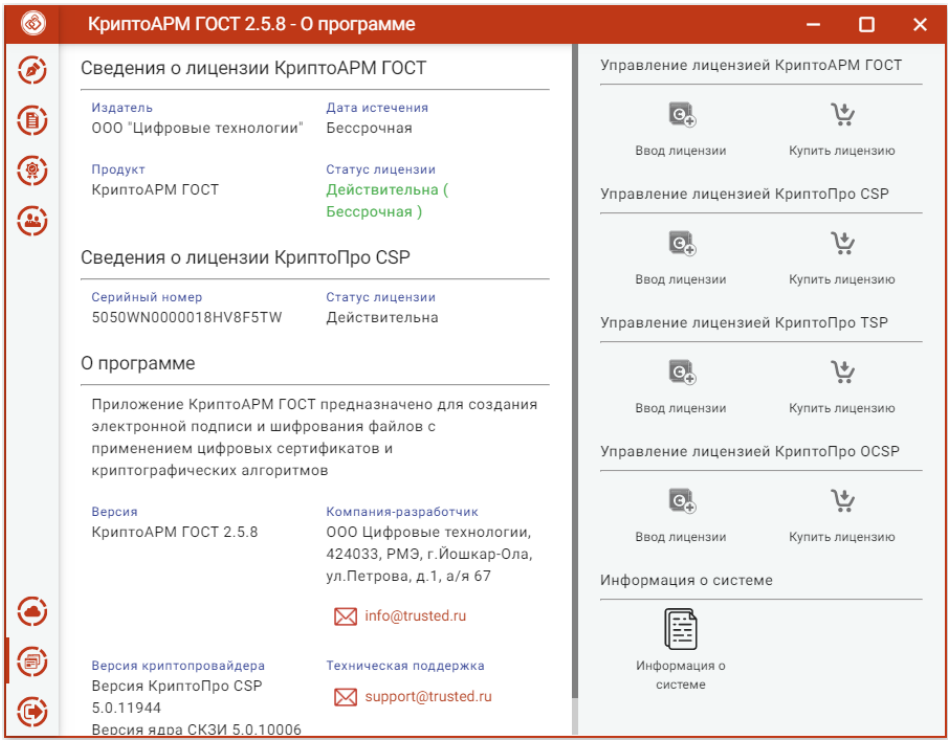
При успешной операции должно появиться информационное сообщение.

4.6 Установка лицензии на модуль OCSP

Для создания усовершенствованной подписи необходима установка лицензионного ключа на модули TSP и OCSP.

Установка лицензионного ключа на модуль OCSP может производиться как через пользовательский интерфейс приложения КриптоАРМ ГОСТ, так и с помощью консольных команд для ОС linux и MacOS, и через интерфейс программы КриптоПро CSP для ОС Windows.

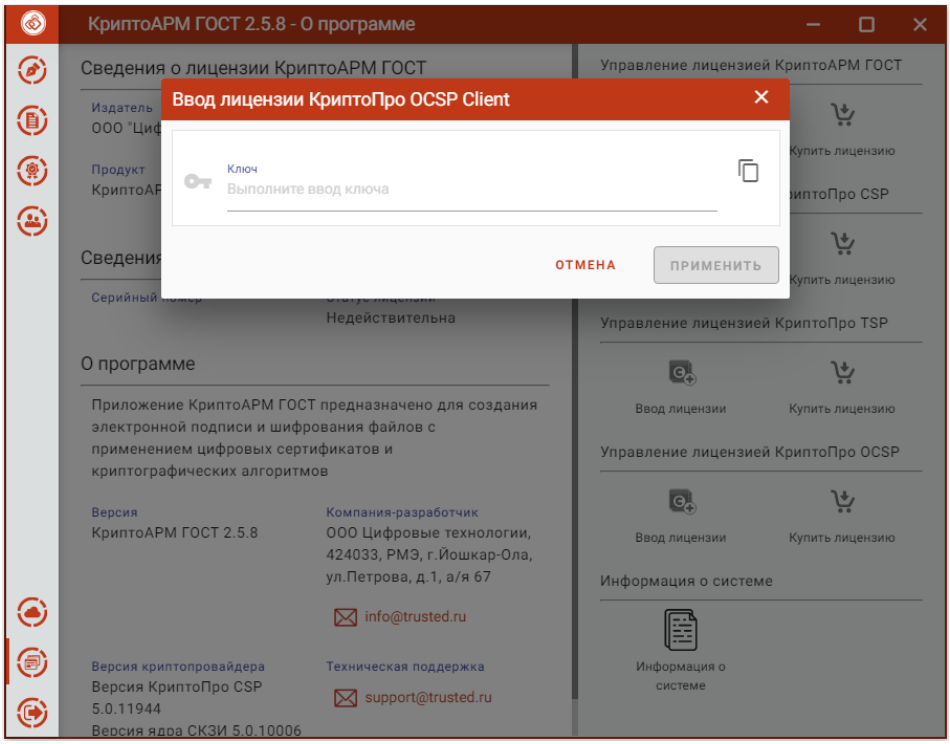
Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения. На открывшейся странице нажать на кнопку **Установить лицензию** в разделе управления лицензией модуля OCSP.



Страница ввода лицензионного ключа на модуль OCSP

Примечание: Если модуль TSP не установлен, то кнопка **Ввода лицензии** будет недоступна.

В результате должно появиться всплывающее окно ввода лицензии копированием содержимого файла лицензии в текстовое поле.



Окно ввода лицензионного ключа на модуль OCSP

Примечание. При установке лицензии будут запрошены права администратора (Root) на доступ к каталогу установки лицензии.

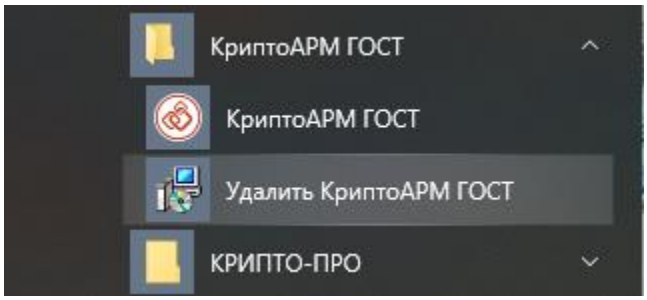
При успешной операции должно появиться информационное сообщение.

4.7 Удаление программного продукта

4.7.1 Удаление приложения на платформе MS Windows

Удалить приложение КриптоАРМ ГОСТ можно следующим образом:

1. Воспользоваться стандартными средствами удаление программ в операционной системе Windows. Через кнопку **Пуск** откройте **Панель управления**. В окне **Настройка параметров** компьютера активизируйте ярлык **Программы и компоненты**. Откроется одноименное окно, в котором перечислены программы, установленные на компьютере. Выберите в списке программу **КриптоАРМ ГОСТ**, нажмите на кнопку **Удалить**, и подтвердите решение об удалении. Выполнение процесса удаления будет отображаться в виде индикатора прогресса в специальном окне. По завершении процесса программа КриптоАРМ ГОСТ будет удалена с компьютера и из списка элементов **Установленные программы**.
2. Второй способ удаления доступен через главное меню операционной системы. В главном меню найдите раздел с приложением - **Пуск, Все программы, КриптоАРМ ГОСТ**. В списке найдите **Удалить КриптоАРМ ГОСТ** (Uninstall КриптоАРМ ГОСТ) и активизируйте команду.



Начнется процесс удаления приложения КриптоАРМ ГОСТ. Выполнение процесса отображается в виде индикатора прогресса. После завершения этого процесса приложение КриптоАРМ ГОСТ будет удалено из операционной системы.

4.7.2 Удаление приложения на платформе Linux

Удаление приложения КриптоАРМ ГОСТ на операционных системах Linux выполняется через графический интерфейс (пакетный менеджер), либо через терминал в режиме командной строки.

1. Удаление приложения КриптоАРМ ГОСТ через графический интерфейс выполняется следующим образом. Нужно открыть менеджер программ (пакетный менеджер) и найти приложение КриптоАРМ ГОСТ. Найденное приложение следует пометить для удаления и нажать на кнопку **Удалить**. После этого программа КриптоАРМ ГОСТ будет удалена с компьютера.
2. Второй способ удаления основан на запуске команд в терминале:

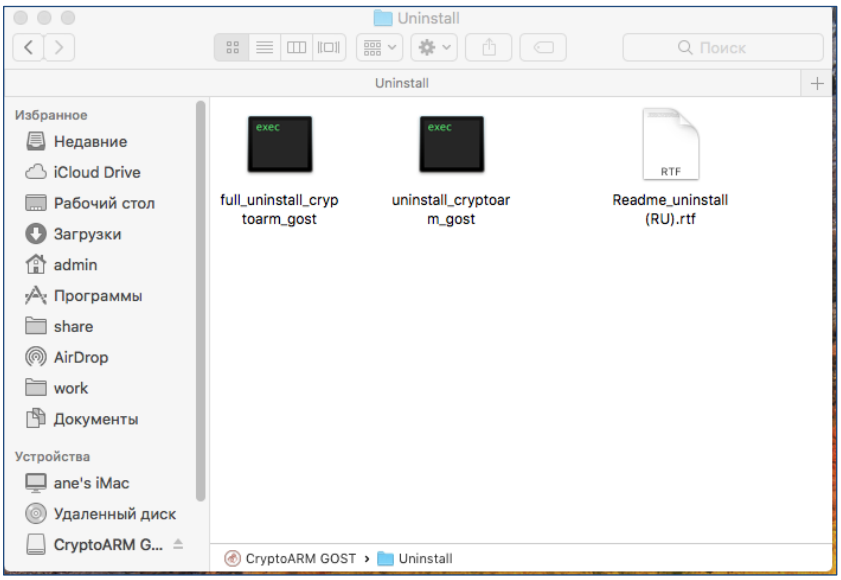
   sudo dpkg -P cryptoarm-gost - для ОС, основанных на Debian (Debian/Ubuntu);

   sudo rpm -e cryptoarm-gost - для ОС, основанных на RPM;

После выполнения команды приложение будет удалено из операционной системы.

4.7.3 Удаление приложения на платформе OS X

Для удаления пакета через графический интерфейс откройте двойным щелчком образ диска с дистрибутивом (dmg), а затем двойным щелчком по каталогу **Uninstall**, содержащему скрипты для удаления приложения. Для удаления приложения из каталога Application запускается **скрипт unistall_cryptoarm_gost**. Для полного удаления приложения (настроек, кэша) используется скрипт **full_uninstall_cryptoarm_gost**. Требуется ввод пароля администратора.



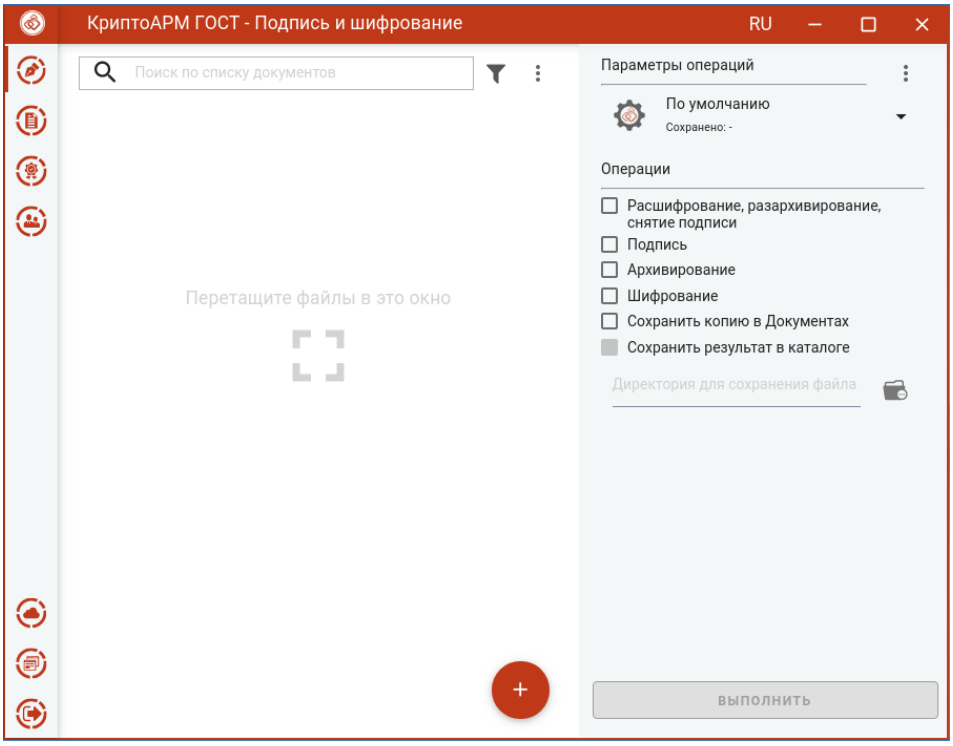
Каталог скриптов удаления приложения

Для удаления приложения КриптоАРМ ГОСТ на операционной системе OS X можно воспользоваться менеджером Finder. В менеджере выберете вкладку **Программы** и найдите приложение КриптоАРМ ГОСТ. Перетащите приложение КриптоАРМ ГОСТ в **Корзину**. Таким образом, приложение будет удалено из операционной системы.

5 Графический пользовательский интерфейс приложения

5.1 Начало работы с приложением

Работа с приложением КриптоАРМ ГОСТ начинается со страницы **Подпись и шифрование**.



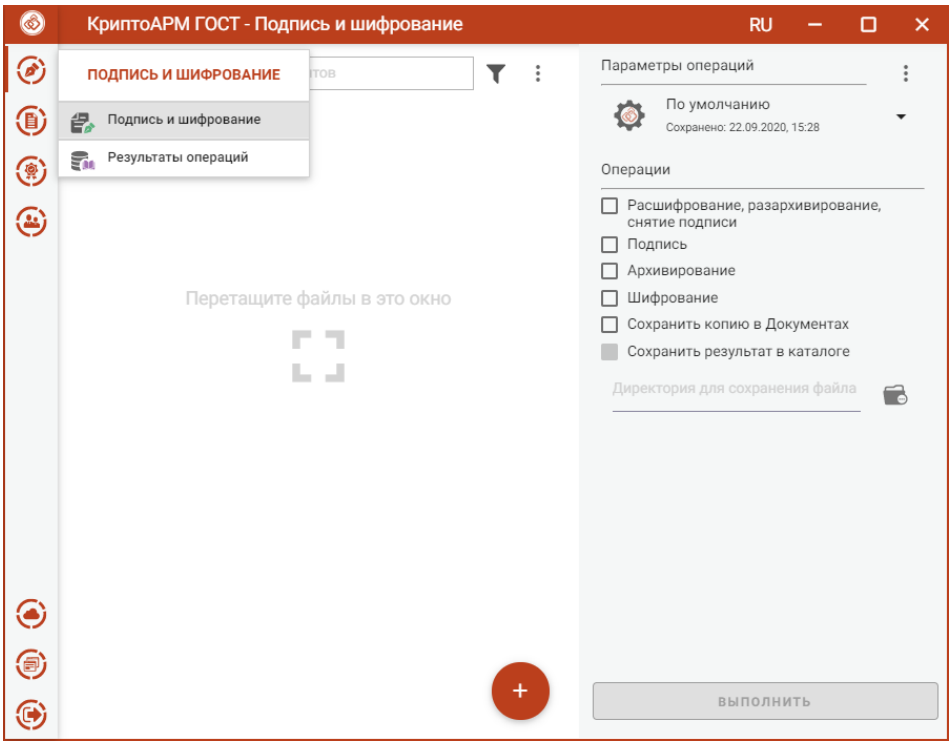
Стартовое окно приложения

Левая рабочая часть окна предназначена для управления списком файлов; в правой части располагается панель выбора **Параметров операций**, переключатель **Операций** и кнопка **Выполнить.**

Переключатель операций позволяет выбрать группу операций, которая будет выполняться над списком файлов:

- **Расшифрование, разархивирование, снятие подписи** – опция для выполнения обратных операций. Для выполнения обратных операций не требуется установка дополнительных параметров.
- **Подпись, архивирование, шифрование** – опция для выполнения прямых операций. Допускается выбор одной операции или группы операций. Для прямых операций требуется выбор дополнительных параметров подписи и шифрования.
- **Сохранить копию в Документах, Сохранить результат в каталоге** – для сохранения результатов прямых операций в заданные каталоги.

Слева на панели расположены кнопки выбора пунктов меню приложения, через которые можно выполнить переход ко всем представлениям.



Пункт меню Подпись и шифрование с подменю

При первом запуске приложения в домашней папке пользователя создается подкаталог с наименованием **.Trusted**, который содержит файловые объекты, необходимые для корректного функционирования приложения. В частности, в подкаталоге размещаются файлы журнала операций и каталог с документами. В файле **settings.json** сохраняются пользовательские настройки.

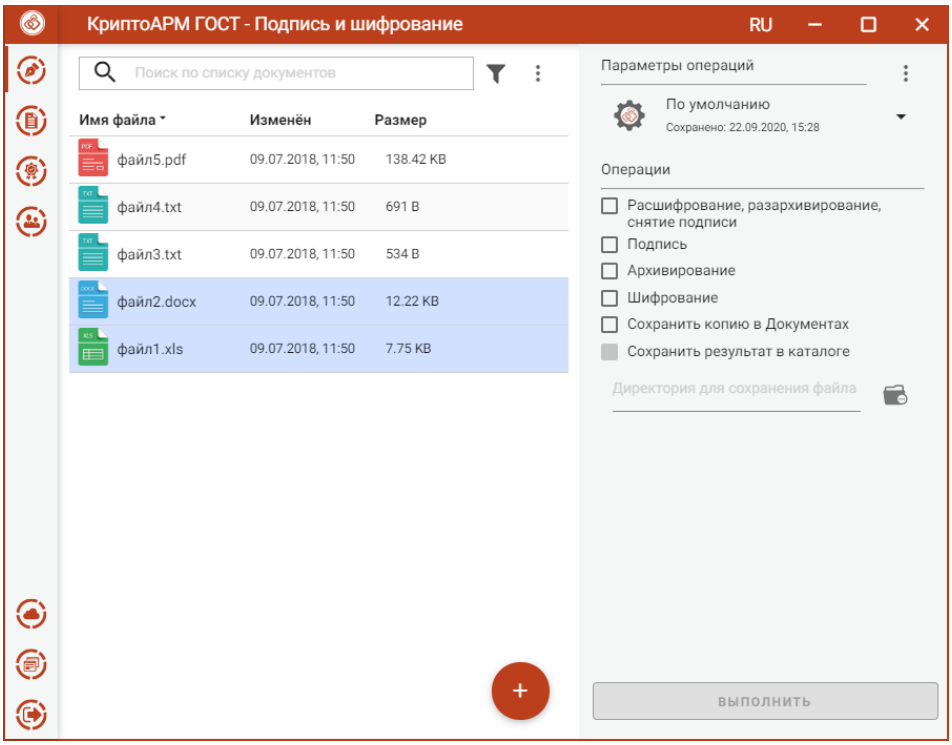
5.2 Создание электронной подписи

Подписать файлы можно на странице **Подпись и шифрование**. Для этого нужно выбрать подписываемые файлы, сертификат подписи и задать параметры подписи.

5.2.1 Выбор подписываемых файлов

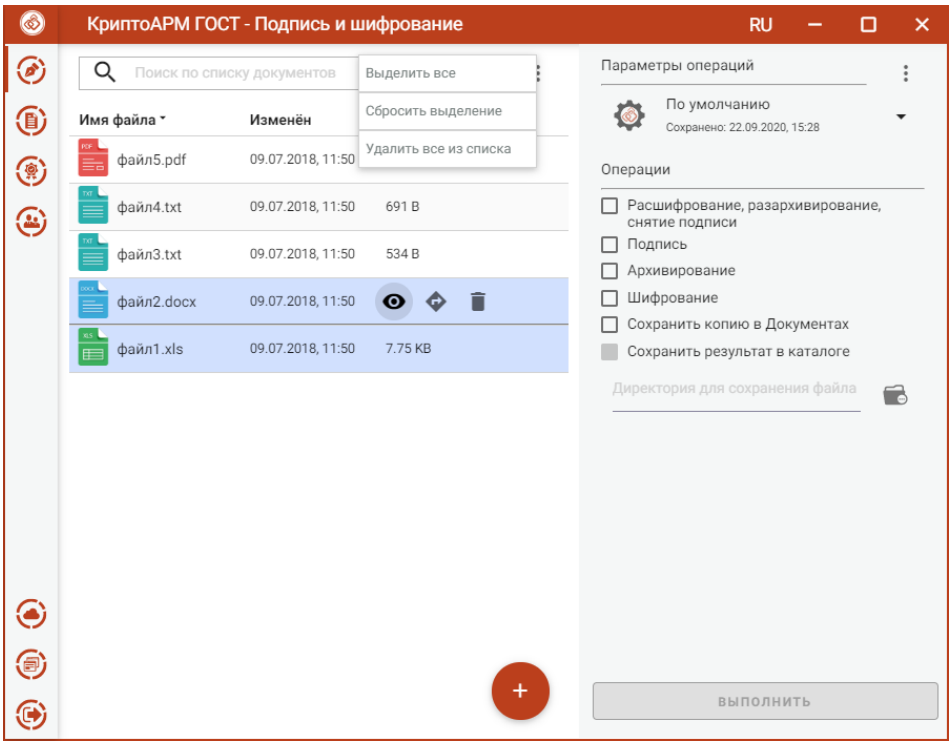
В приложении доступно создание подписи для одного или группы выбранных файлов. Файлы для подписи можно добавить двумя способами: через кнопку **Добавить** (+) или перетащив мышкой в область формирования списка файлов.

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список.



Список подписываемых файлов

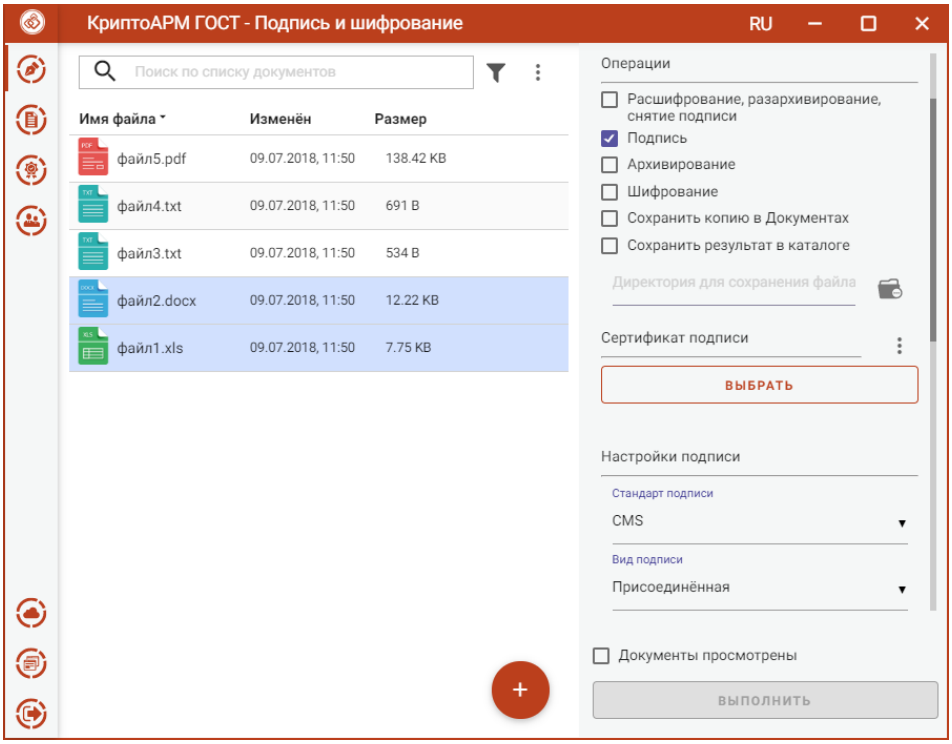
Для данного списка доступны поиск, фильтрация, управление файлами через контекстное меню и кнопки для каждого файла.



Контекстное меню управления списком файлов

5.2.2 Установка параметров подписи

Для подписи файлов в разделе **Операции** необходимо выбрать опцию **Подпись**, становятся доступны параметры подписи.



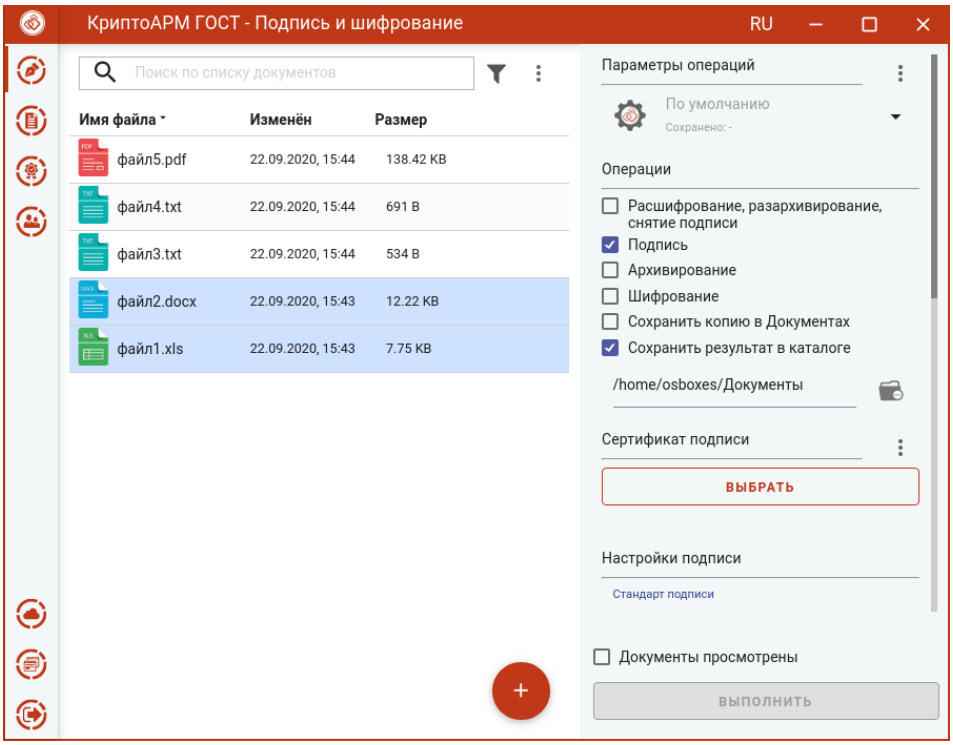
Настройка параметров подписи

В параметрах можно настроить:

- **Сертификат подписи** – личный сертификат с закрытым ключом.

- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 - для усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP) (**подробнее в пункте Создание усовершенствованной подписи). Стандарт подписи CAdES-X Long Type 1 доступен только при установленных модулях КриптоПро TSP Client и КриптоПро OCSP Client.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.

Можно задать каталог для сохранения подписанных документов, выбрав в операциях опцию **Сохранить результат в каталоге.** При установке флага становится доступно поле выбора каталога.



Выбор каталога для сохранения результата операции подписи

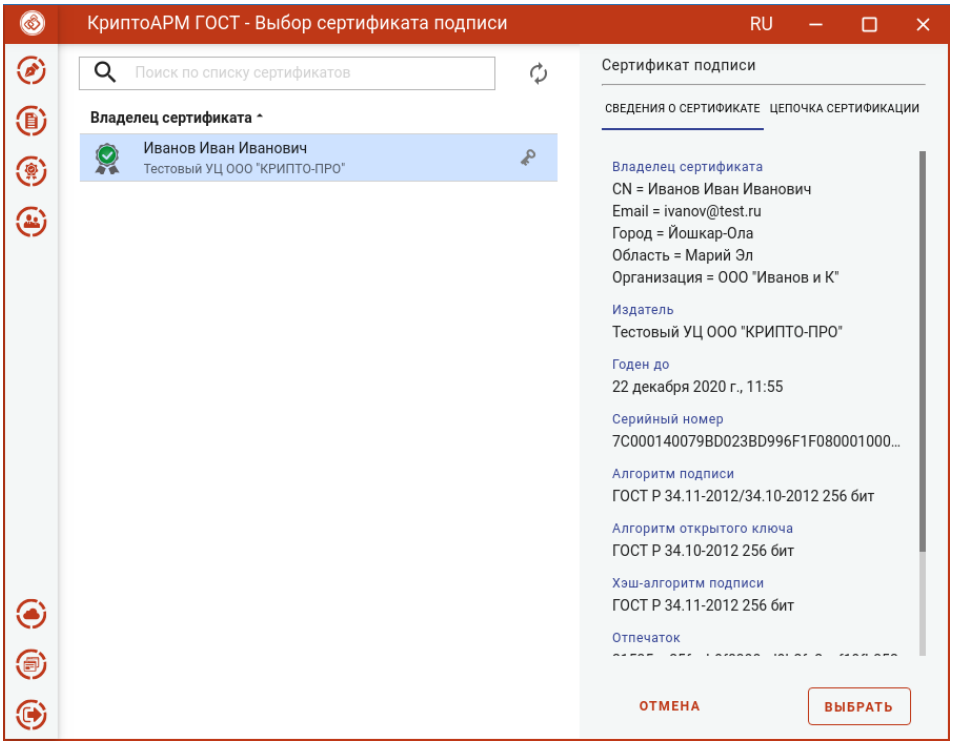
Если флаг не установлен, то файл сохраняется рядом с исходным файлом.

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Выбранные параметры подписи можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте Управление параметрами операции.

5.2.3 Выбор сертификата подписи

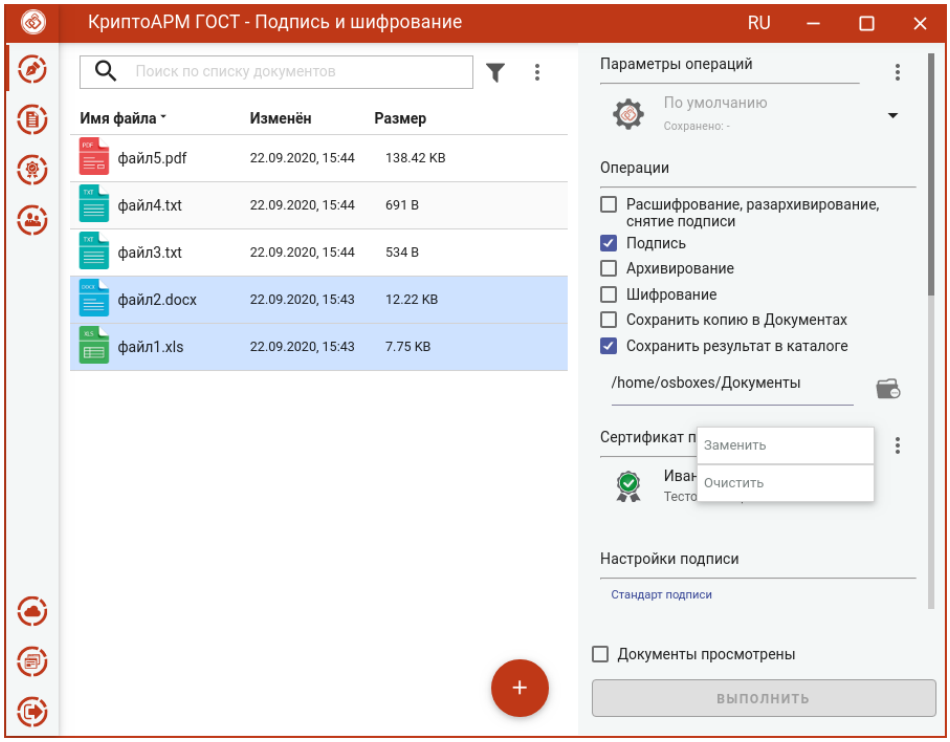
Для того, чтобы выполнить подпись необходимо выбрать сертификат, к которому привязан закрытый ключ. Эта операция производится нажатием кнопки **Выбрать** сертификат подписи. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи.



Выбор сертификата подписи

Выбор сертификата подписи осуществляется его выделением и нажатием на кнопку **Выбрать**.

Сертификат подписи можно изменить с помощью контекстного меню.

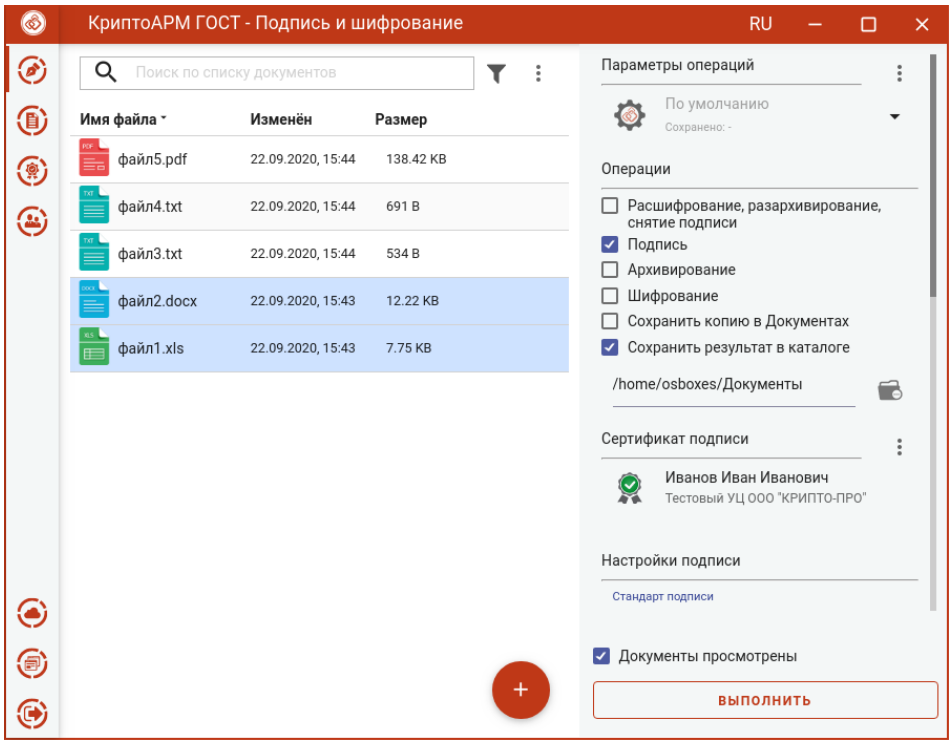


Изменение сертификата подписи

Если в хранилище личных сертификатов нет сертификата с закрытым ключом, то можно его создать или импортировать в разделе Сертификаты.

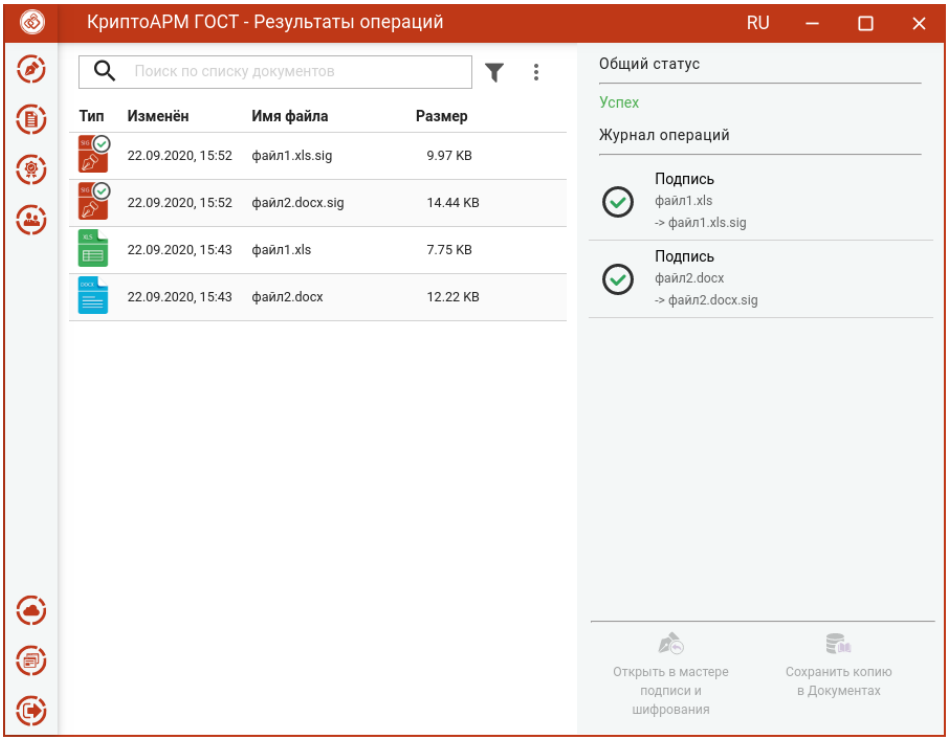
5.2.4 Подпись файлов

При условии выбора сертификата подписи, файлов и установленного флага, что **Документы просмотрены**, в мастере становится доступной кнопка **Выполнить**. Подписать можно любые файлы, кроме зашифрованных.



Подпись файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи. Исходные документы (оригиналы) и результаты операции отображаются в отдельном мастере **Результаты операций**.



Результаты операции подписи

Подписанные файлы сохраняются в заданном каталоге, если в операциях был выбран каталог для сохранения результатов. Или рядом с исходным файлом, если в операциях не был установлен флаг **Сохранить результат в каталоге**.

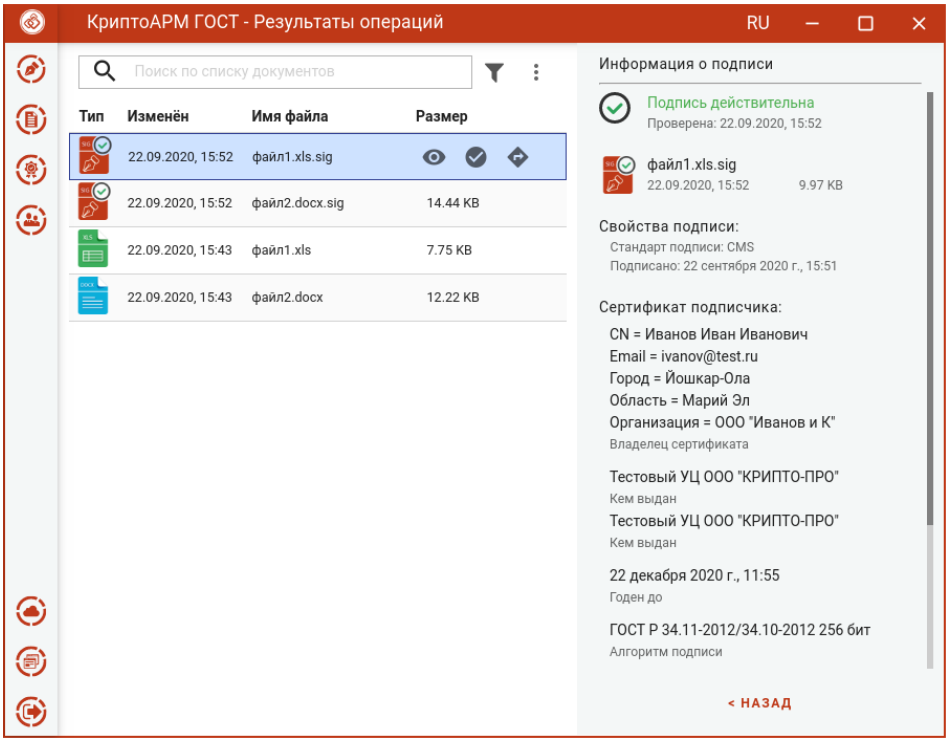
Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученного после операции файла сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Подпись проверяется автоматически.

Для просмотра информации о подписи нужно выделить один файл в списке.

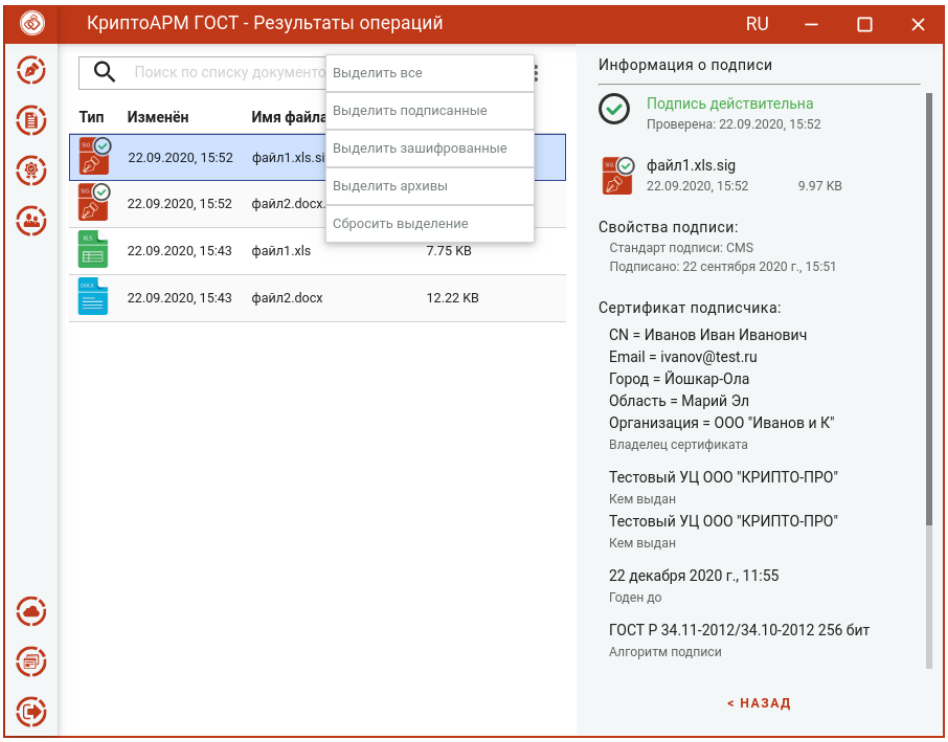
Для каждого документа доступны операции:

- **Просмотр** - выполняется открытие файла через приложение, которое ассоциировано с его расширением. Для подписанных файлов открывается оригинал документа;
- **Проверить подпись** – доступна только для подписанных файлов. Принудительно запускает процесс проверки подписи;
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл.



Операции для документа

Для списка документов доступно контекстное меню, позволяющее выделить файлы по типу операции.



Выделение группы файлов по типу файла

Документ из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций**.** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

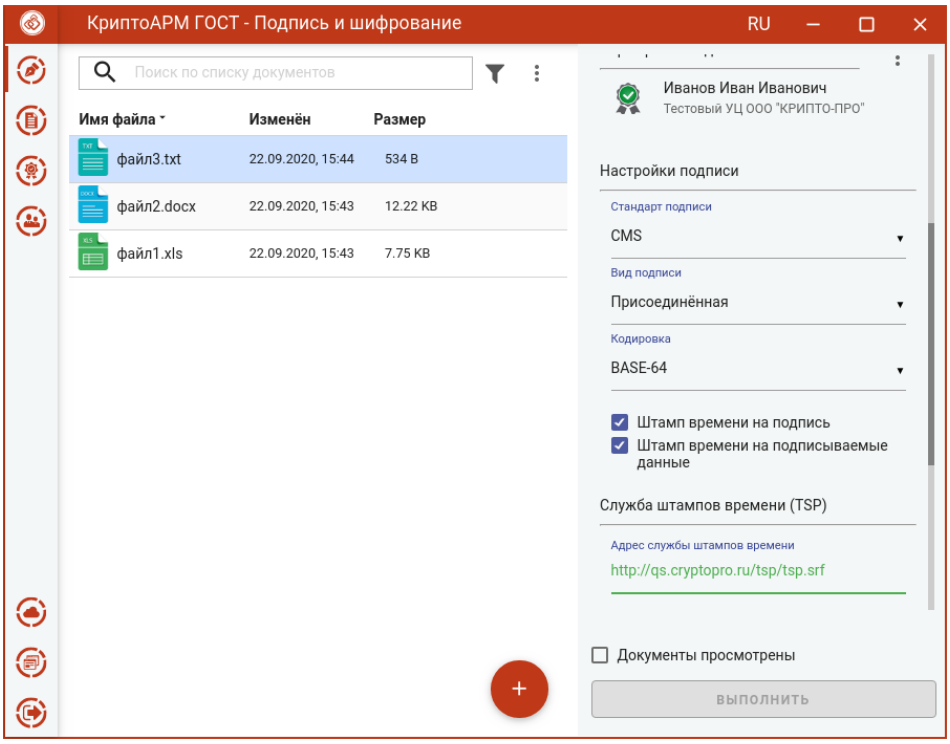
5.3 Создание подписи со штампом времени (TSP)

Служба штампов времени используется для простановки штампов времени на документы. Данные, защищенные электронной подписью Службы, содержат надежную информацию о времени существования электронного документа. Штампы времени используются для привязки факта существования каких-либо данных ко времени.

Создание подписи со штампом времени возможно только при установленном модуле КриптоПро TSP Client и лицензии на него.

Для создания подписи со штампом времени нужно выбрать подписываемые файлы, сертификат подписи и установить дополнительные параметры:

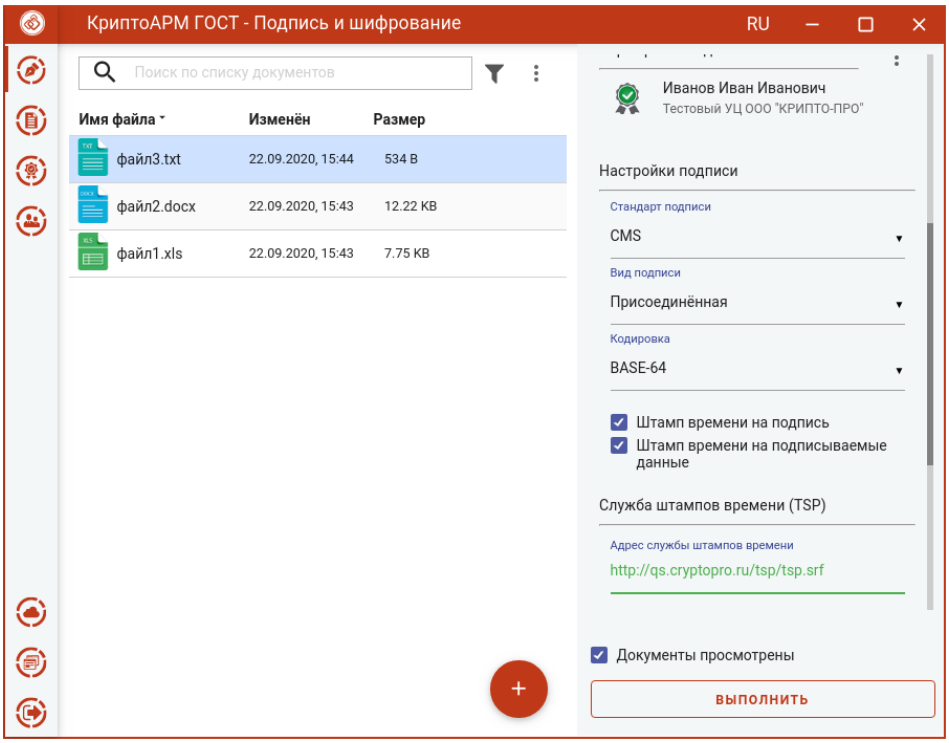
- установить флаг **Штамп времени на подпись**, если требуется поставить штамп на подпись;
- установить флаг **Штамп времени на подписываемые данные**, если требуется поставить штамп на данные;



Установка флага для добавления штампа времени в подпись

- **Адрес службы штампов времени** - можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: <протокол>://<сервер>[:порт][/путь]. В качестве протокола может быть указан "http" и "https".
- **Использовать настройки прокси-сервера** – если при подключении к службе TSP используется прокси-сервер, то установка флага активирует его настройки: **Адрес прокси-сервера, Порт, Логин, Пароль,** которые можно узнать у системного администратора.

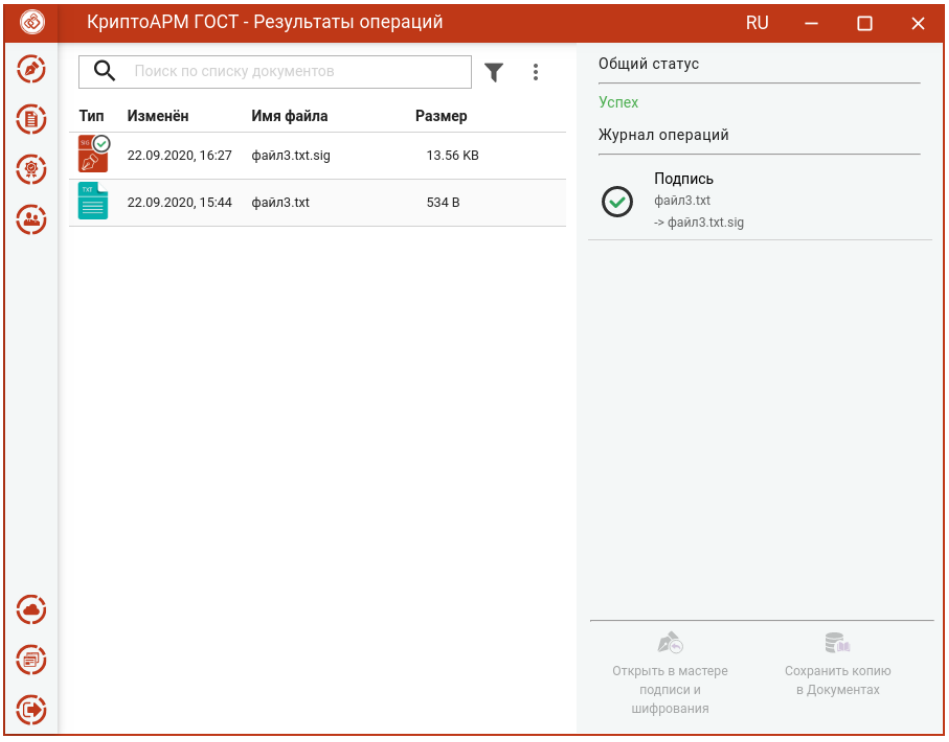
После заполнения параметров подписи и установки флага, что **Документы просмотрены** перед их подписанием, становится доступна кнопка **Выполнить.**



Подпись документов со штампом времени

Нажатие на кнопку **Выполнить** запускает процесс подписи.

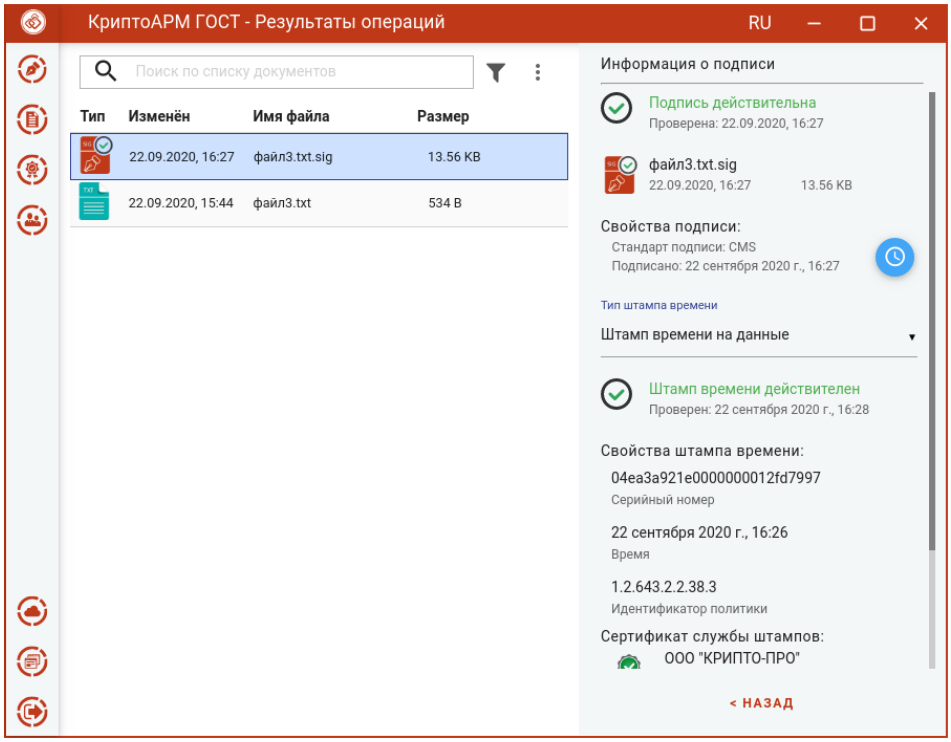
Исходные документы (оригиналы) и результаты операции подписи отображаются в отдельном мастере **Результаты операций.**



Результаты операции подписи

После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов.

При просмотре свойств подписи отображается информация о штампе времени.



Информация о штампе времени при просмотре подписи

5.4 Создание усовершенствованной подписи

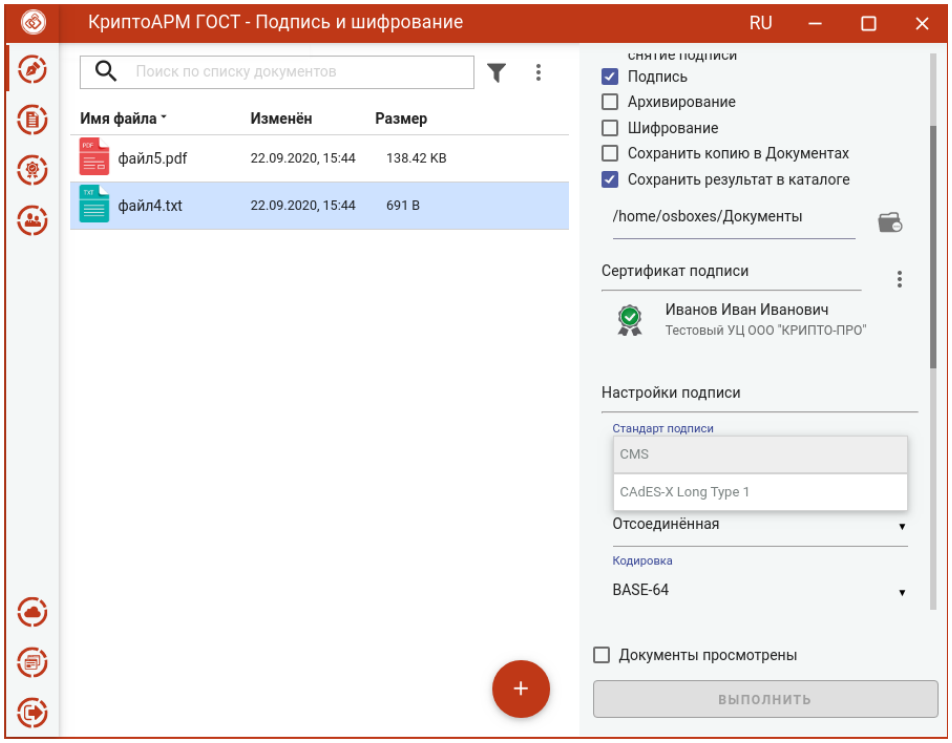
Усовершенствованная квалифицированная электронная подпись поможет доказать юридическую значимость документа в спорных ситуациях. Например, когда помимо авторства и целостности документа (которые дает обычная КЭП) необходимо подтвердить, что сертификат был действителен в момент подписания документа.

Формат усовершенствованной подписи предусматривает включение в электронную подпись информации о времени создания подписи (TSP) и о статусе сертификата электронной подписи (OCSP) в момент подписания (действителен или отозван).

Создание усовершенствованной подписи возможно только при установленных модулях TSP Client и OCSP Client и лицензий на них.

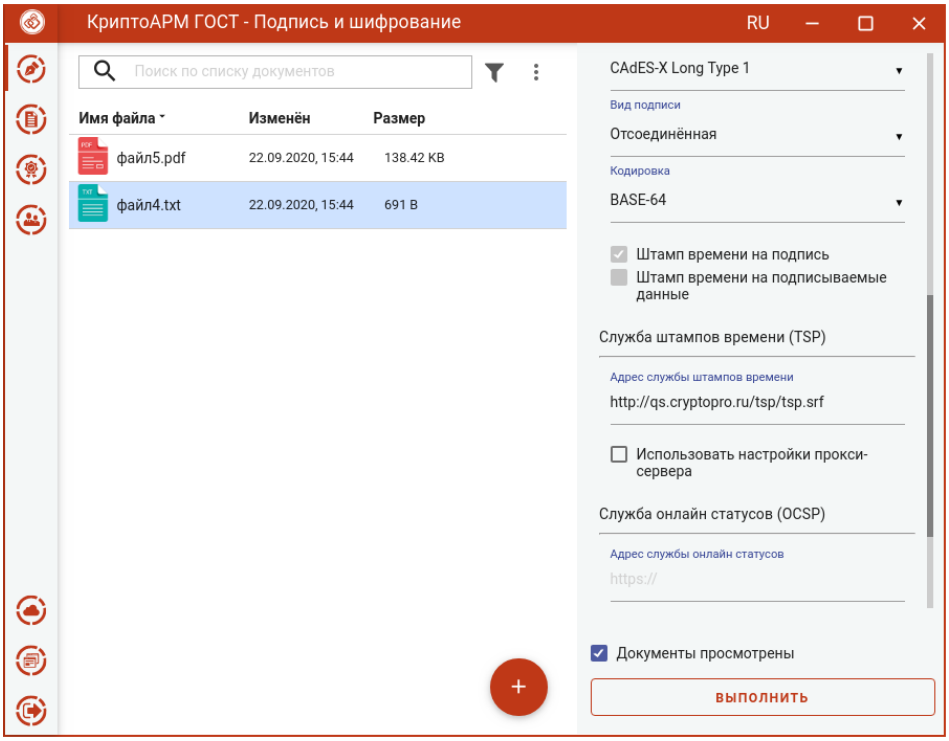
Для создания усовершенствованной подписи нужно выбрать подписываемые файлы, установить опцию **Подпись**, задать сертификат подписи и установить дополнительные параметры:

- Выбрать стандарт подписи **CAdES-X Type 1**;



Стандарт подписи CAdES-X Type 1

- Заполнить параметры раздела **Служба штампов времени (TSP)**: **Адрес службы штампов времени, Использовать настройки прокси-сервера** (если при подключении к службе TSP используется прокси-сервер)



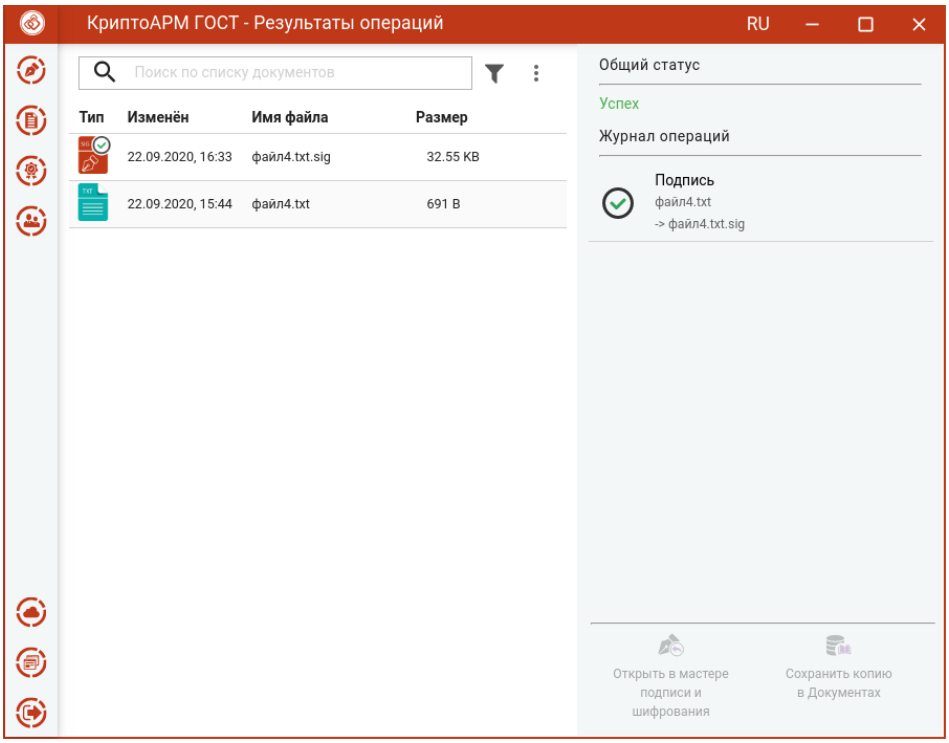
Параметры службы штампов времени

- Заполнить параметры раздела **Службы online статусов (OCSP)**: **Адрес службы online статусов.** Это необязательный параметр, задается, если в сертификате данное поле не заполнено.

После заполнения параметров и установки флага, что **Документы просмотрены** перед их подписанием, становится доступна кнопка **Выполнить.**

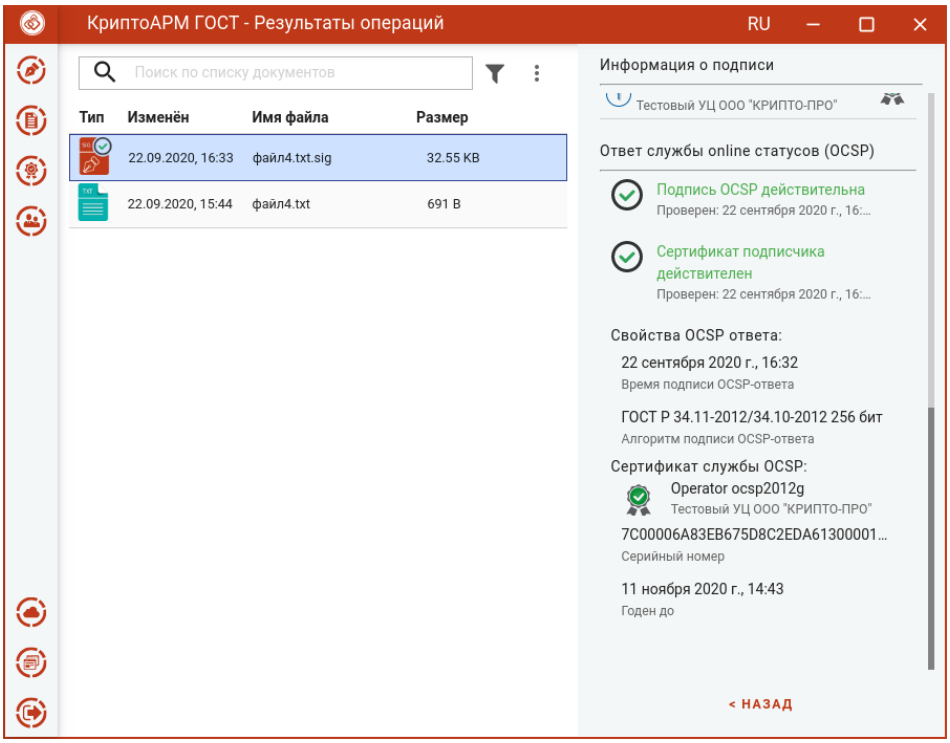
Нажатие на кнопку **Выполнить** запускает процесс подписи.

Исходные документы (оригиналы) и результаты операции подписи отображаются в отдельном мастере **Результаты операций**.



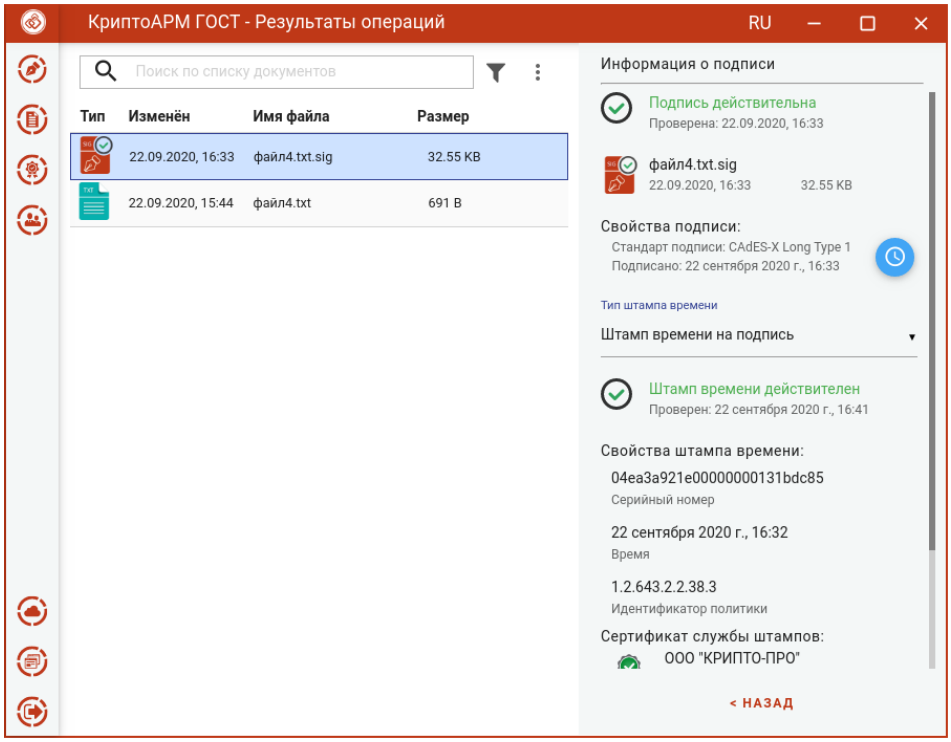
Результаты операций подписи

При просмотре свойств подписи отображается информация о OCSP ответе.



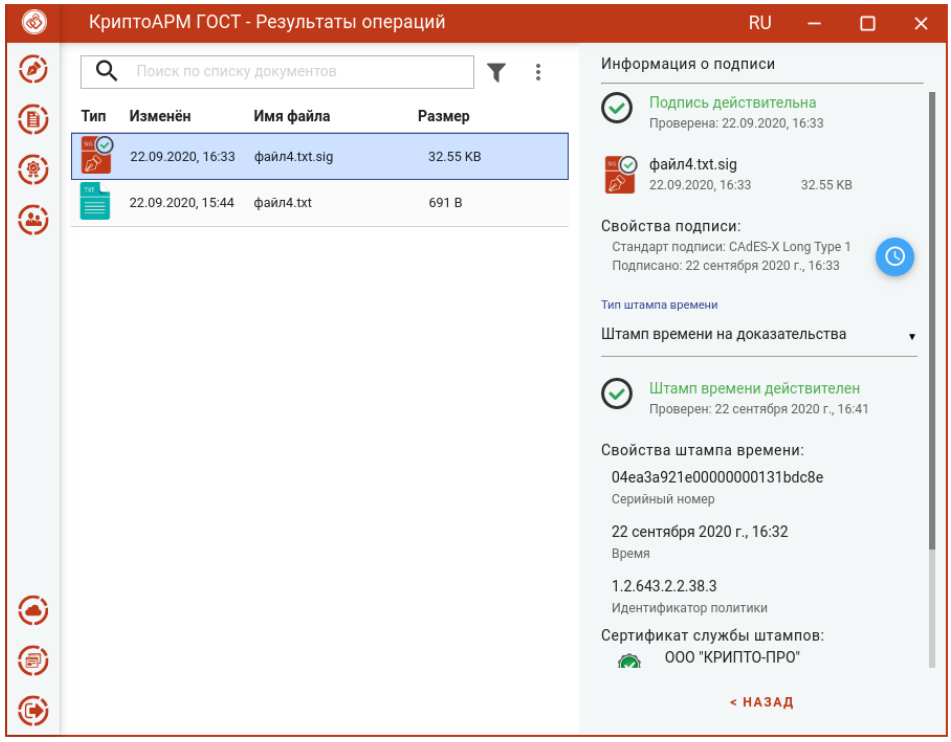
Информация об OCSP ответе при просмотре подписи

Информация о штампе времени на подпись.



Информация об штампе времени на подпись

Информация о доказательствах подлинности.

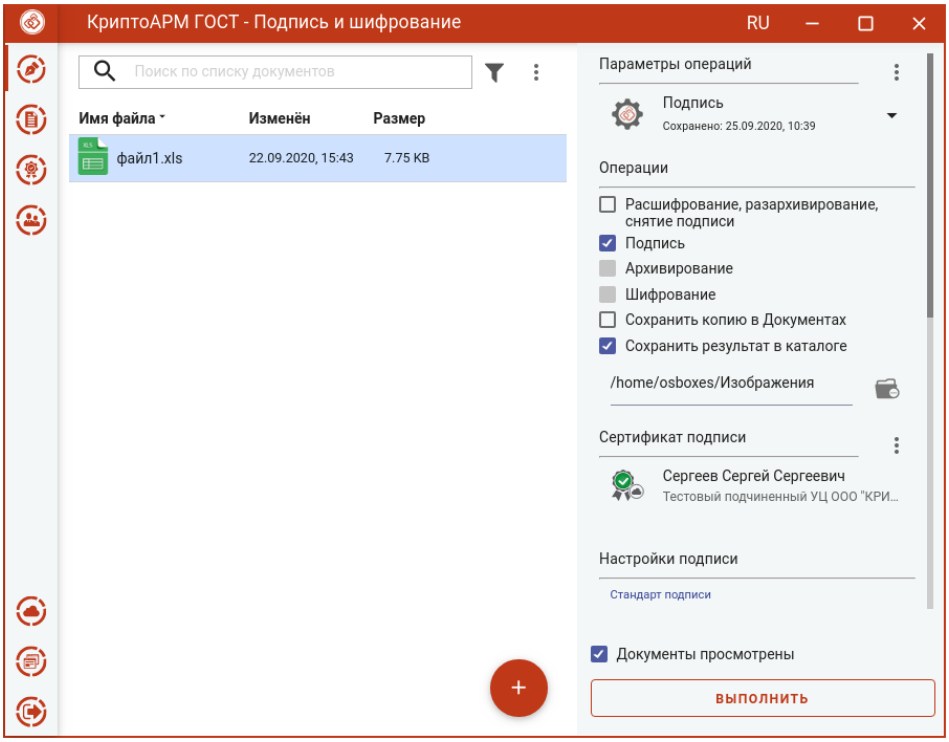


Информация о доказательствах подлинности

5.5 Подпись сертификатом DSS

Подпись сертификатом DSS ничем не отличается от подписи обычным сертификатом, за исключением некоторых шагов.

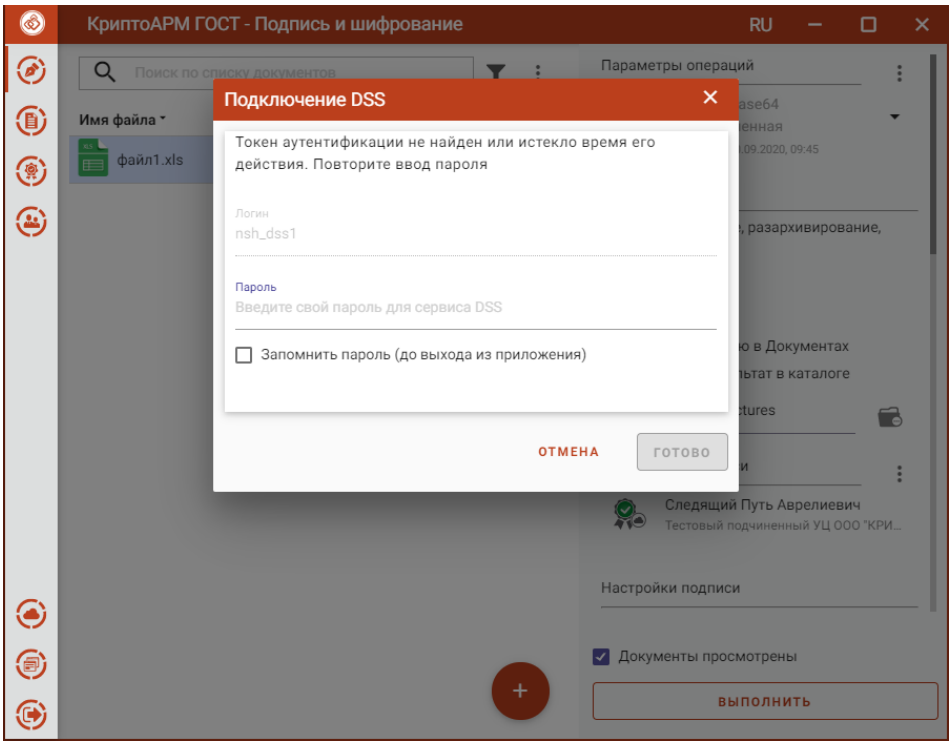
Нужно выбрать файлы, выбрать сертификат подписи DSS и установить флаг, что **Документы просмотрены** перед подписанием.



Выбор файлов и сертификата для подписи DSS

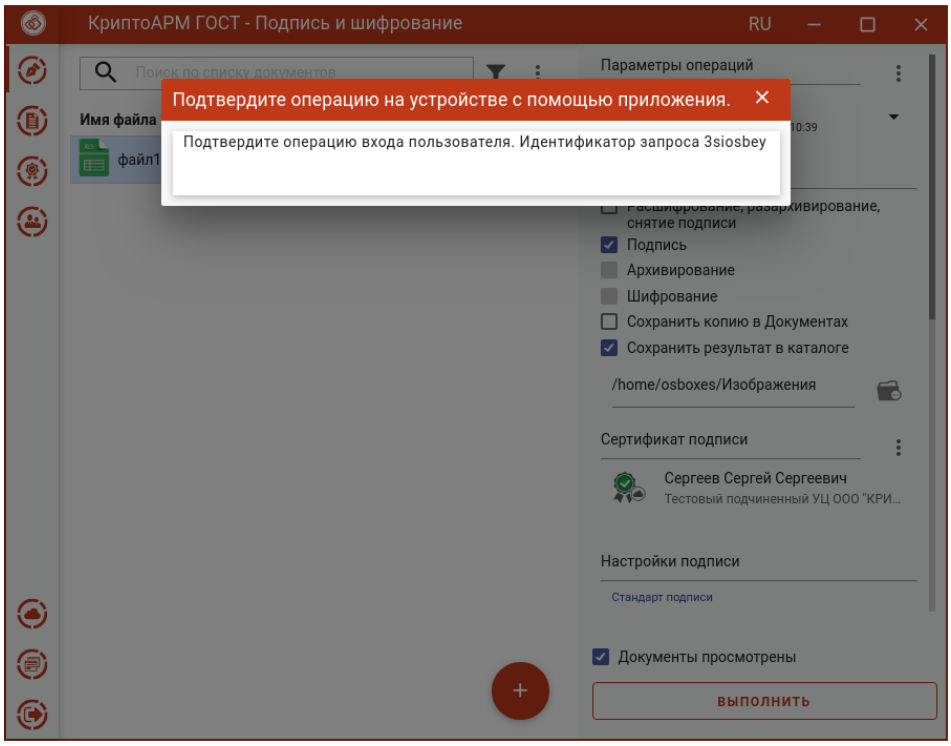
При нажатии на кнопку **Выполнить** открывается:

- окно для ввода пароля для аутентификации на сервисе DSS, если для аутентификации задан пароль и время действия токена аутентификации истекло. Если токен аутентификации не истек, то данный шаг пропускается.



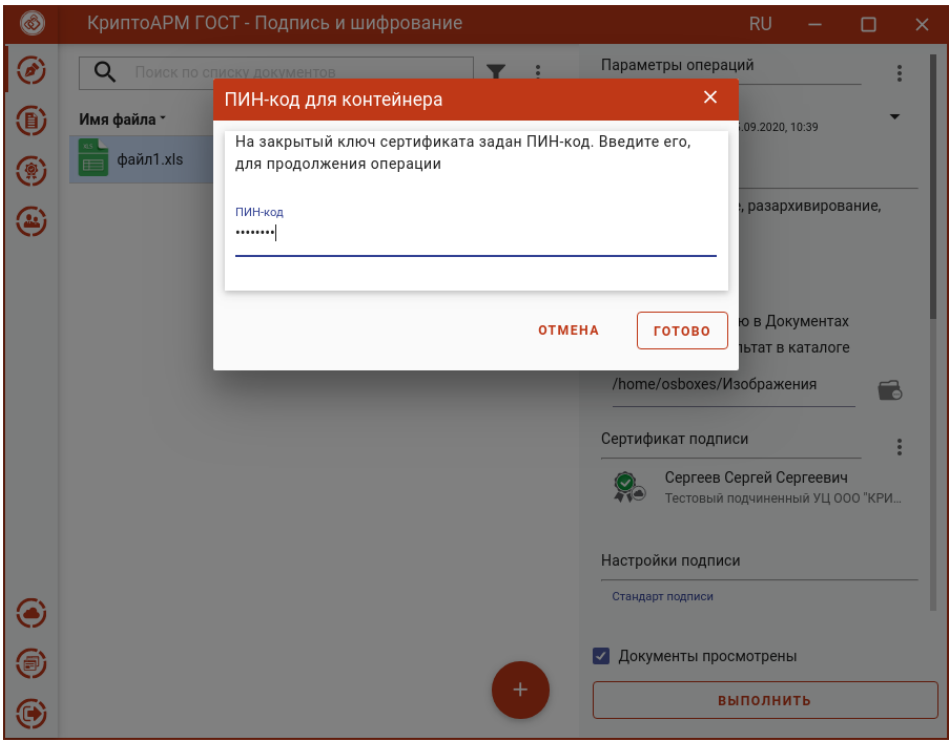
Ввод пароля аутентификации на сервисе DSS

- окно для подтверждения аутентификации на сервисе DSS, если для аутентификации задан вход по сим карте или по мобильному приложению, и время действия токена аутентификации истекло. Если токен аутентификации не истек, то данный шаг пропускается.



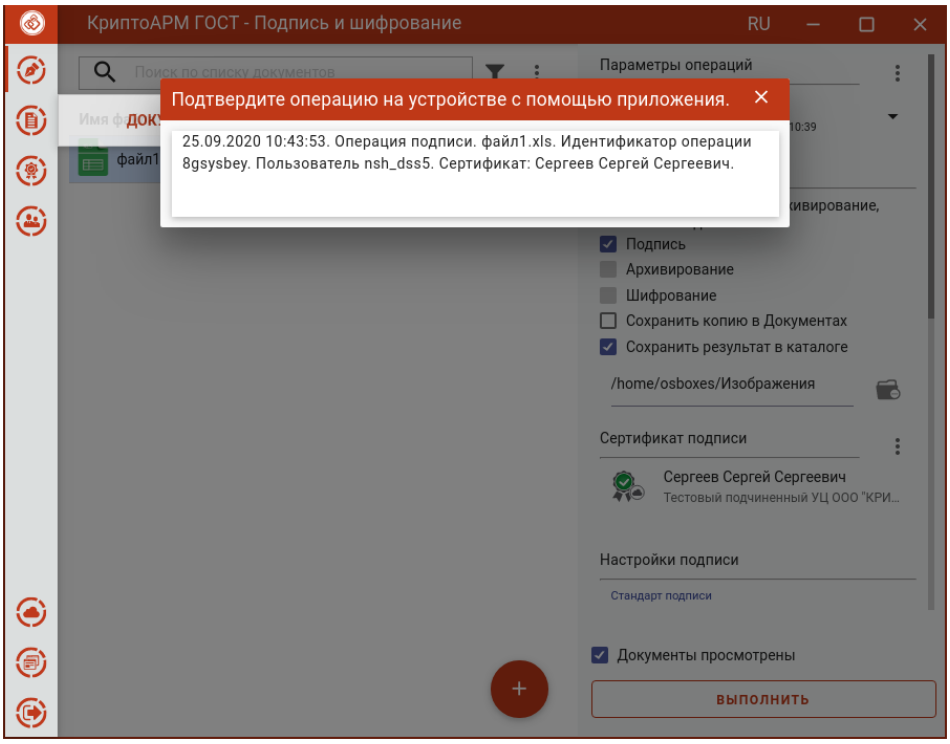
Окно подтверждения аутентификации на сервисе DSS

Далее открывается окно для ввода пароля к ключевому контейнеру. Если пароль не задан, то данный шаг пропускается.



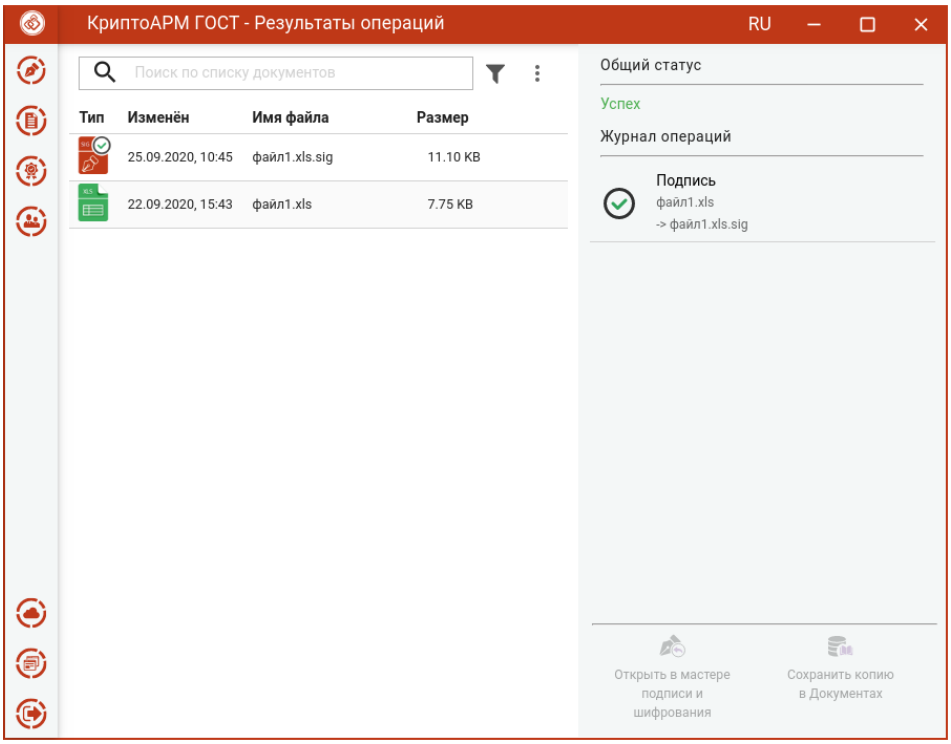
Ввод пароля к ключевому контейнеру

Если у пользователя в личном кабинете DSS в настройках аутентификации стоит подтверждение операции подписи сим карте или с помощью мобильного приложения, то на следующем шаге появляется сообщение, что операцию нужно подтвердить.



Окно ожидания подтверждения операции подписи

После подтверждения операции на устройстве происходит подпись файла.



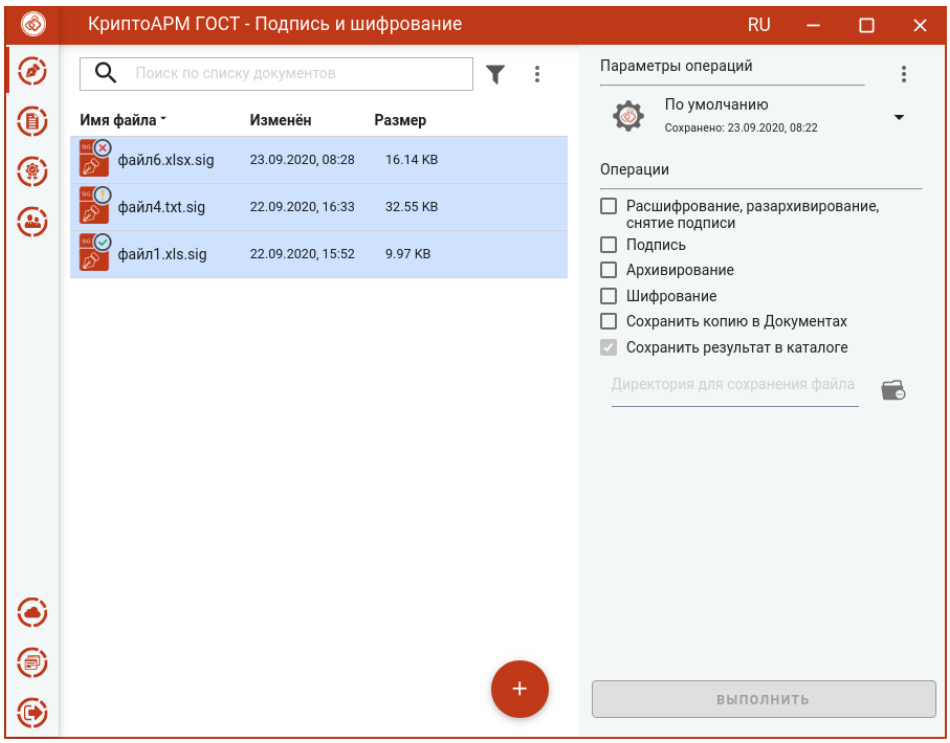
Подписанный файл

Для DSS подписи наличие лицензии на программный продукт КриптоПро CSP необязательно.

5.6 Проверка электронной подписи

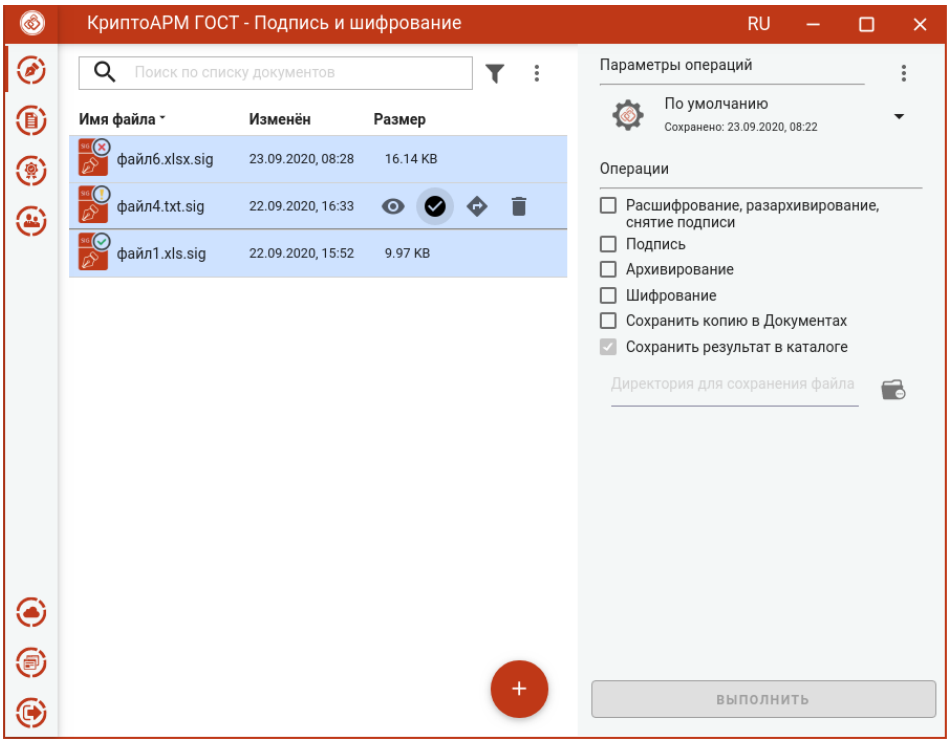
Для проверки подписи достаточно выбрать файлы расширением **.sig**, которые содержат электронную подпись. Никаких дополнительных настроек при проверке подписи производить не нужно.

Результат проверки подписей отображается в виде общего сообщения и цветового индикатора на иконке для каждого файла: зеленый - подпись действительна; красный - подпись недействительна; оранжевый – не удалось проверить подпись.



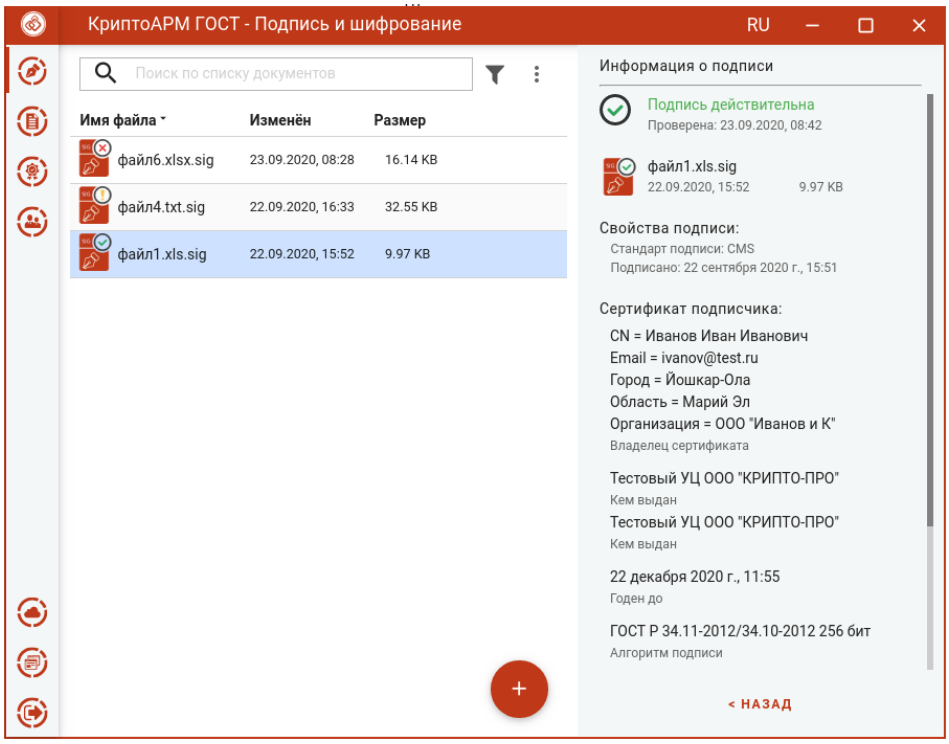
Результат проверки подписи файлов

Если при проверке отделенной подписи, исходный файл не будет найден автоматически, то индикатор проверки будет оранжевого цвета. Для выбора исходного файла надо нажать иконку проверки подписи в меню файла. Откроется окно для его выбора.



Иконка вызова проверки подписи файла

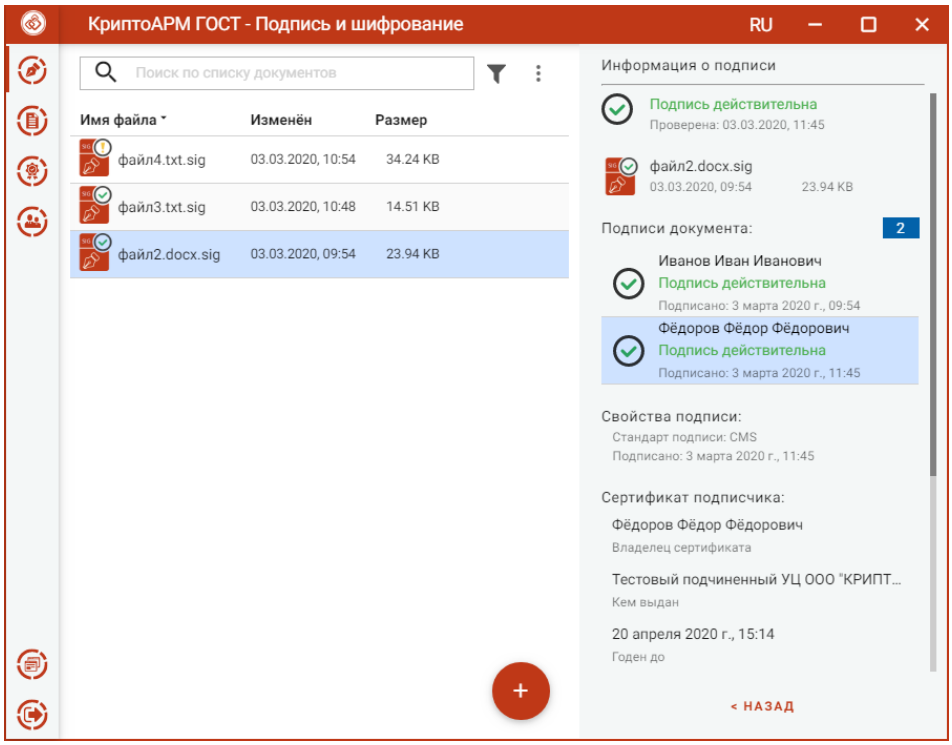
При выделении одного подписанного файла в правой области отображается информация о подписи.



Отображение информации о подписи

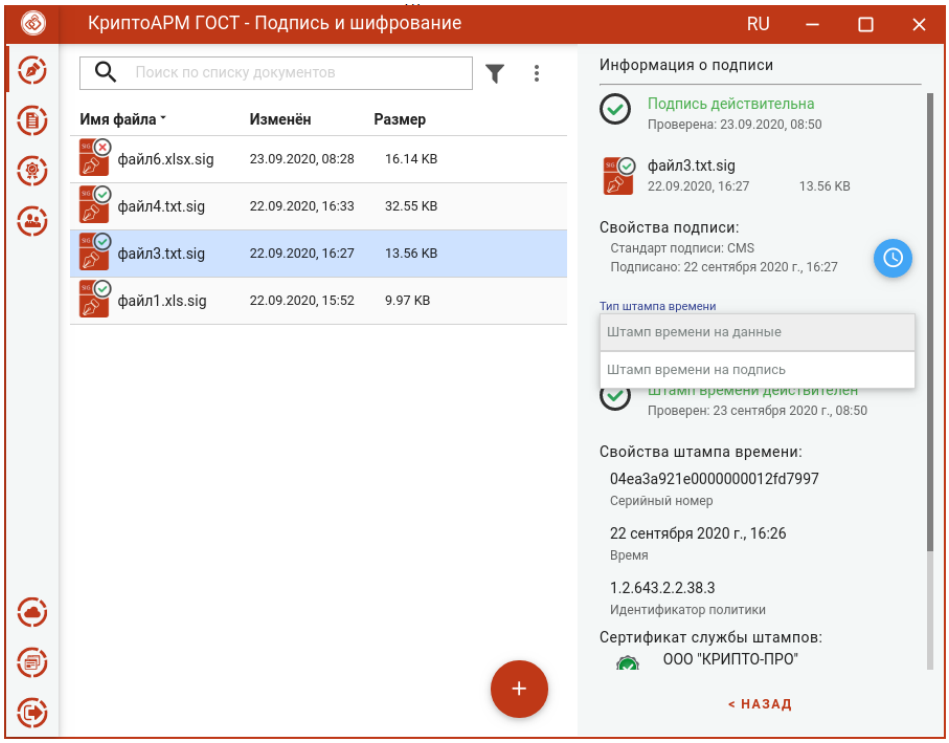
По кнопке **Назад** информация о подписи закрывается и происходит возврат к операциям.

Если документ подписан несколькими подписями (имеет соподписи), то для просмотра информации нужно выбрать подпись из списка.



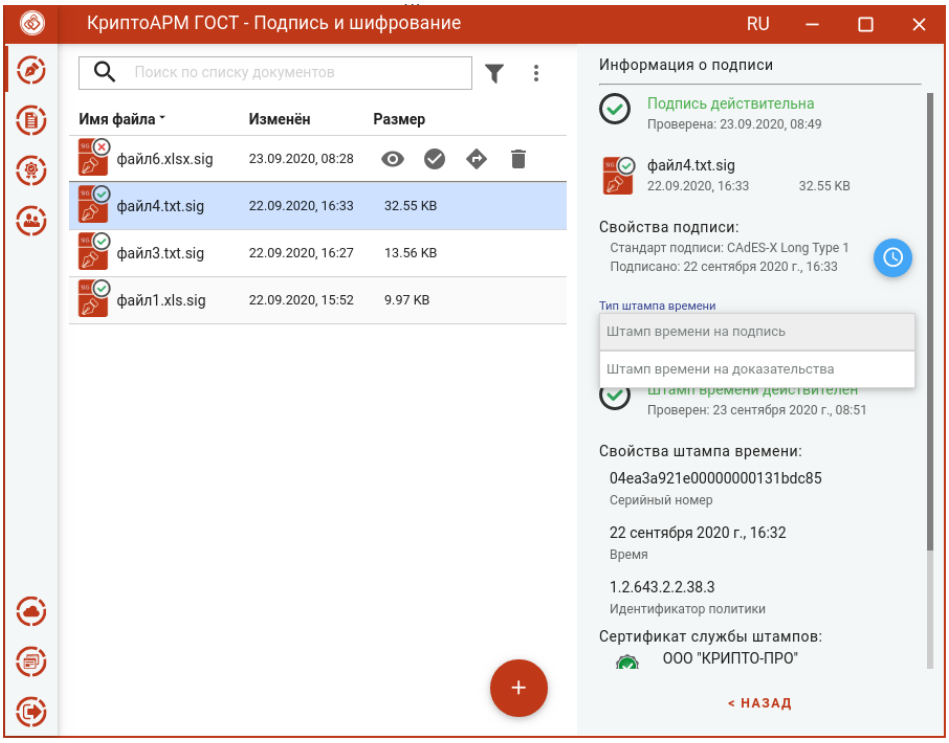
Выбор подписи для просмотра информации

Если документ подписан подписью со штампом времени, то для просмотра параметров штампа нужно нажатием на иконку развернуть информацию и выбрать в выпадающем списке тип штампа времени.



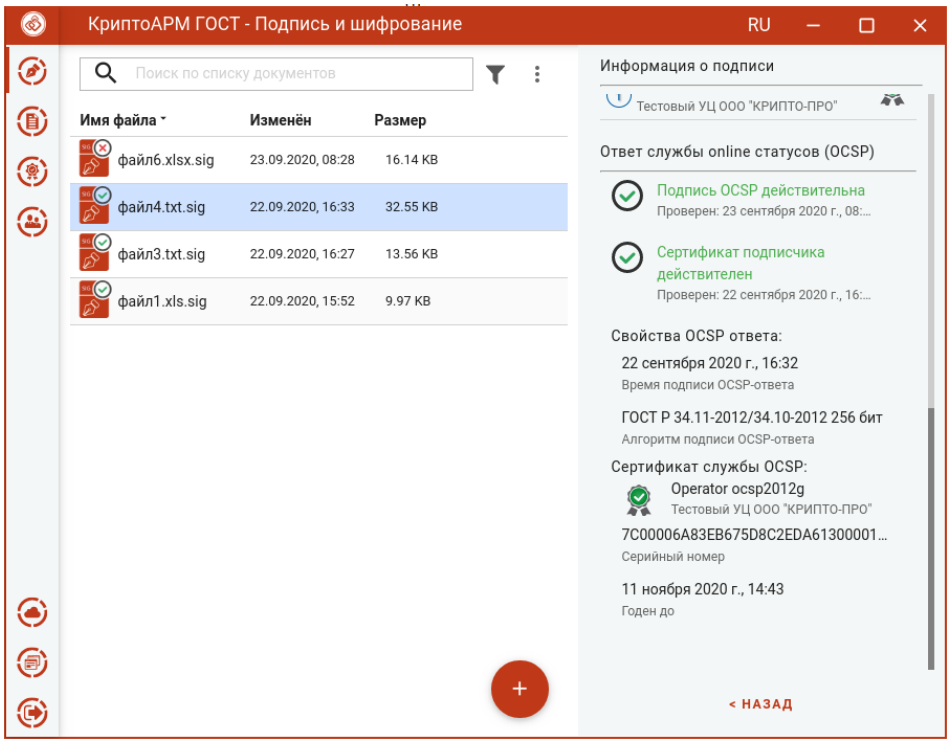
Отображение информации о подписи со штампом времени

Если документ подписан усовершенствованной подписью, то для просмотра сведений о штампах времени в усовершенствованной подписи, нужно нажатием на иконку развернуть информацию и выбрать в выпадающем списке тип штампа времени.



Отображение информации о штампах времени усовершенствованной подписи

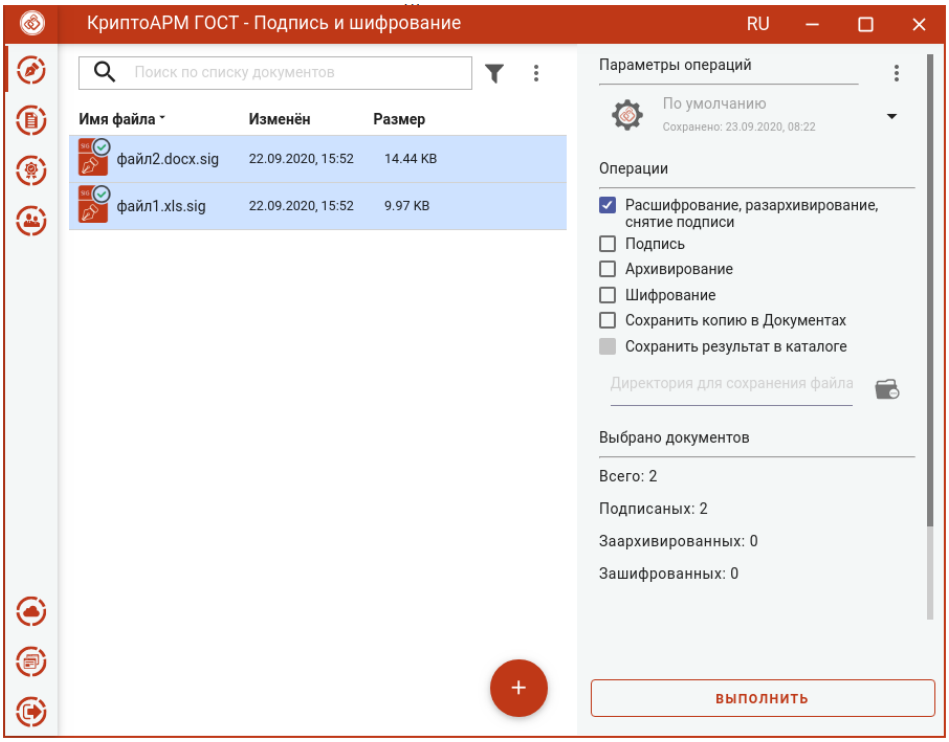
Информация о OCSP ответе усовершенствованной подписи представлена на рисунке.



Отображение информации о OCSP ответе усовершенствованной подписи

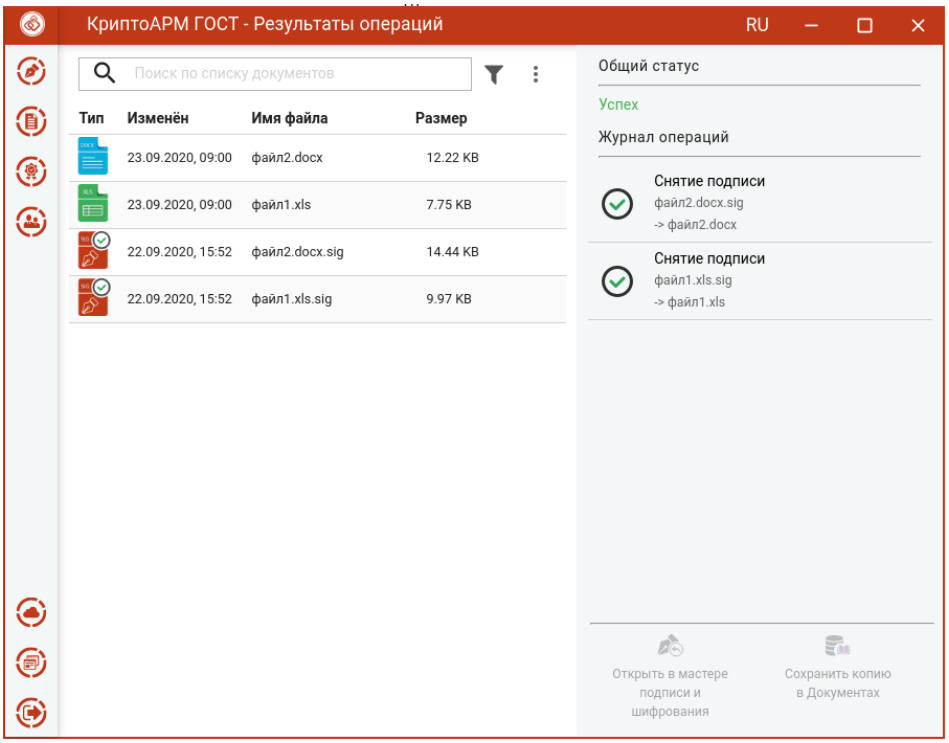
5.7 Снятие электронной подписи

Для снятия подписи достаточно выбрать файлы с расширением **.sig**, которые содержат электронную подпись, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить**. Дополнительные параметры при снятии подписи выбирать не нужно.



Выделенные файлы для снятия подписи

Подписанные и полученные файлы отображаются в отдельном мастере **Результаты операций**.



Результат снятия подписи с файлов

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

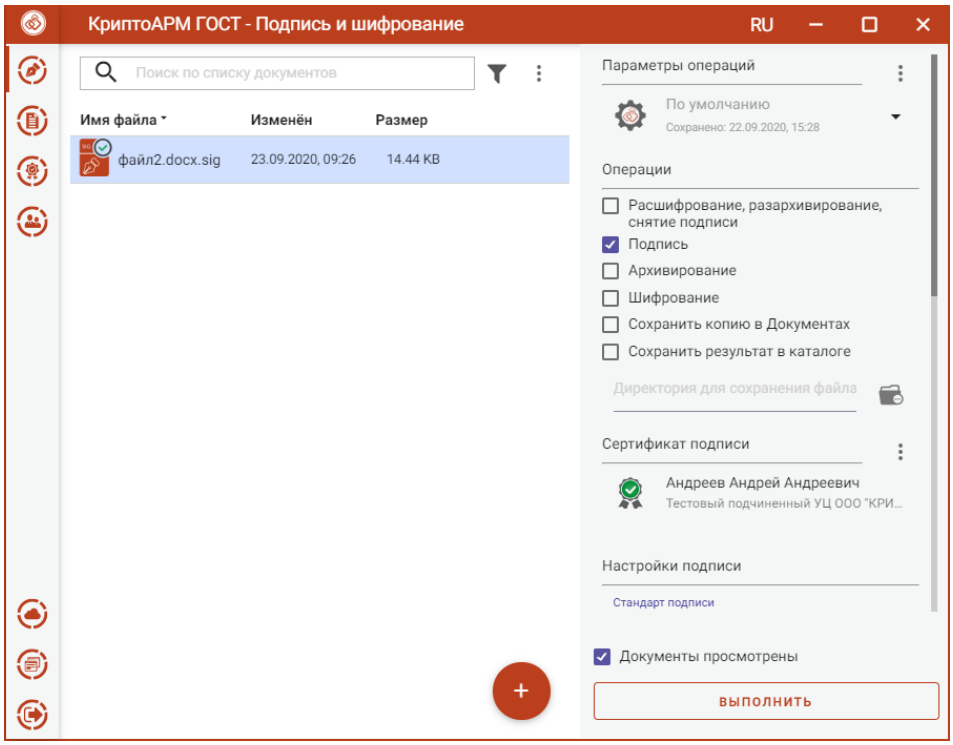
Внимание! Документы, полученные в результате обратных операций (расшифрование, разархивирование, снятие подписи), сохраняются во временную папку, расположенную в папке пользователя в каталоге ./Trusted/CryptoARM GOST/TEMP, и остаются там до выполнения следующей операции. Далее временная папка очищается.

После выполнения операции файлы из мастера **Подписи и шифрования** удаляются. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

Для отделенной подписи при выполнении операции снятия подписи возникает сообщение об ошибке.

5.8 Добавление подписи

Приложение КриптоАРМ ГОСТ позволяет добавлять электронные подписи к уже подписанному файлу. Для этого нужно выбрать файл, содержащий электронную подпись (с расширением **.sig**), установить опцию **Подпись**, задать сертификат подписи, и установить флаг, что **Документы просмотрены**.



Добавление подписи к уже подписанному файлу

Для всех добавленных подписей настройки, такие как кодировка и вид, используются по умолчанию, как для первой подписи.

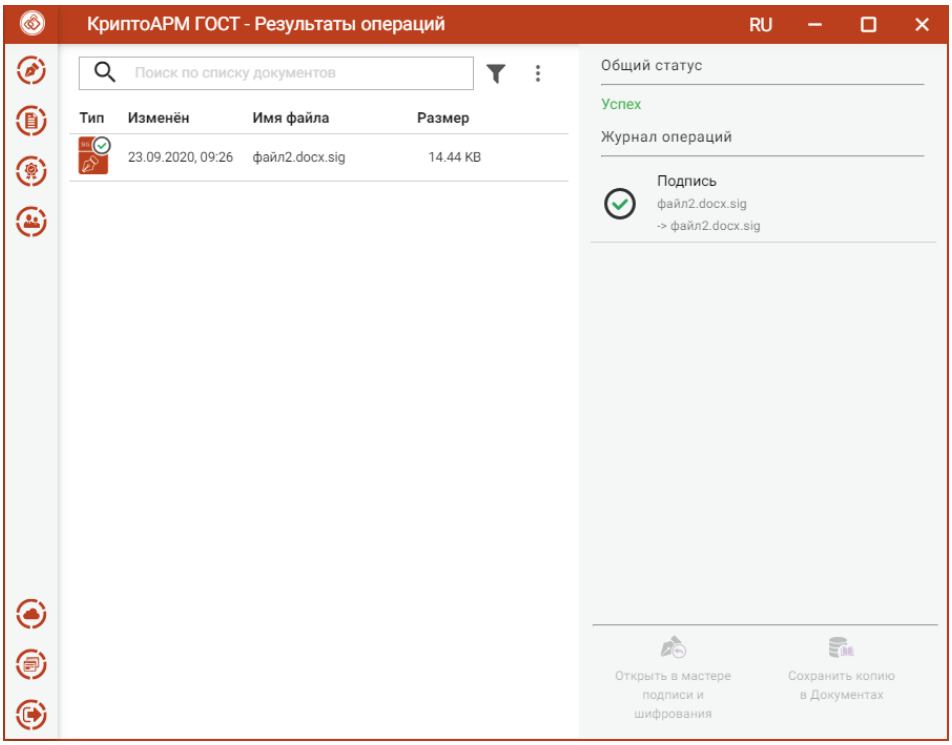
Тип подписи и использование штампов времени можно настроить.

Можно задать каталог для сохранения подписанного документа, выбрав в операциях опцию **Сохранить результат в каталоге.** Если флаг не установлен, то файл сохраняется папку с исходным файлом.

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Выбранные параметры подписи можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте Управление параметрами операции.

Нажатие на кнопку **Выполнить** запускает процесс подписи. Результаты операции соподписи отображаются в отдельном мастере **Результаты операций**.



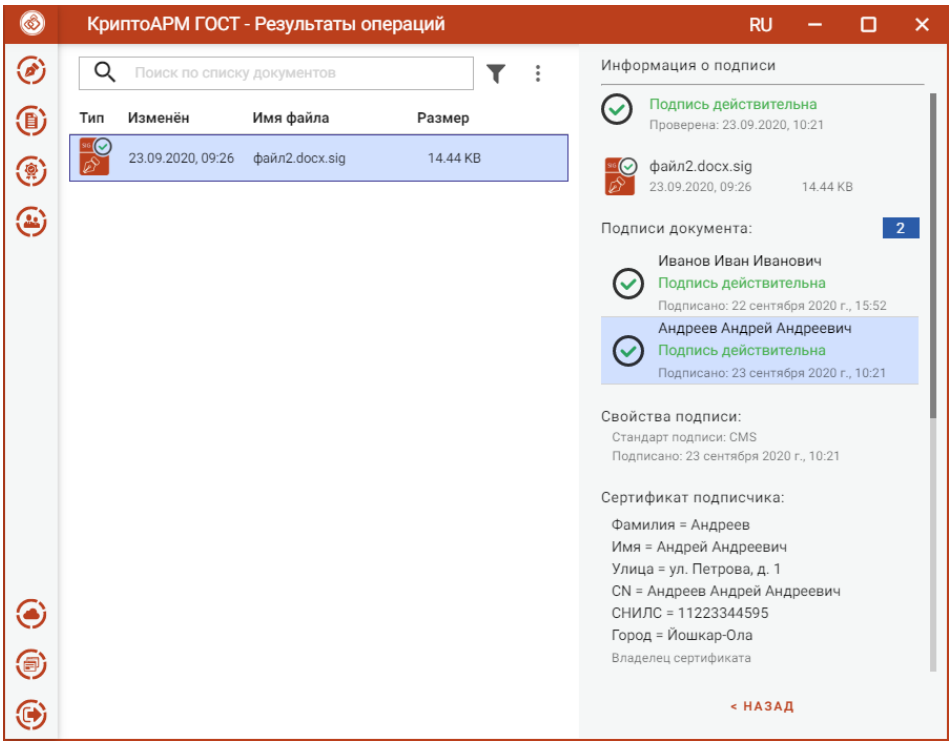
Результаты операции добавления подписи

Подписанный файл сохраняется в заданном каталоге, если в операциях был выбран каталог для сохранения результатов. Или исходный файл заменяется, если в операциях не был установлен флаг **Сохранить результат в каталоге**. Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученного после операции файла сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Для подписанного документа доступны операции:

- **Просмотр** - открывается оригинал документа через приложение, которое ассоциировано с его расширением;
- **Проверить подпись** – принудительно запускает процесс проверки подписи;
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл.

При выделении подписного файла открывается информация, содержащая сведения о всех подписях. Чтобы посмотреть информацию о конкретной подписи, нужно выбрать ее из списка.



Выбор подписи при просмотре информации

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

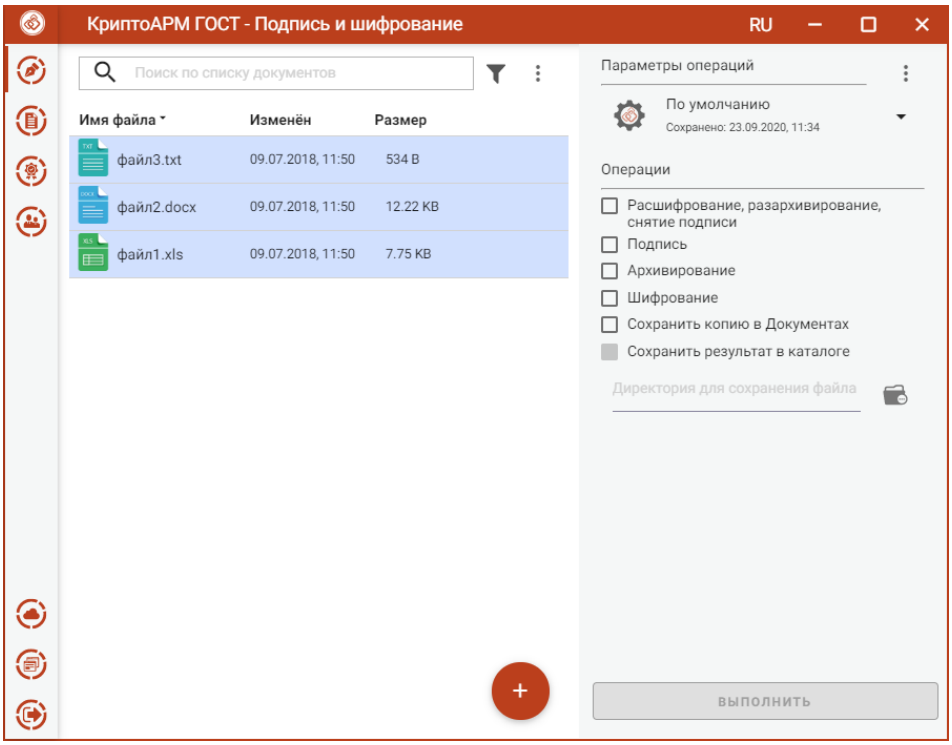
5.9 Шифрование файлов

Для шифрования файлов нужно выбрать файлы, установить опцию **Шифрование**, задать сертификаты получателей и параметры шифрования.

5.9.1 Выбор файлов для шифрования

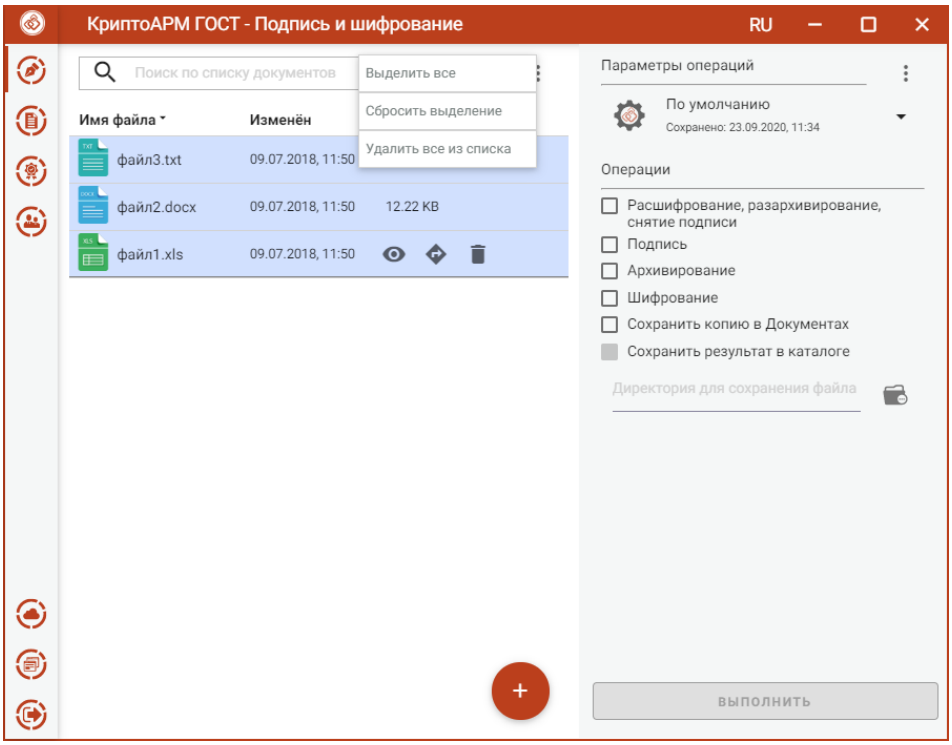
В приложении доступно шифрования одного или группы выбранных файлов. Файлы для шифрования можно добавить двумя способами: через кнопку **Добавить (+)** или перетащив их мышкой в область формирования списка файлов.

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список.



Список файлов для шифрования

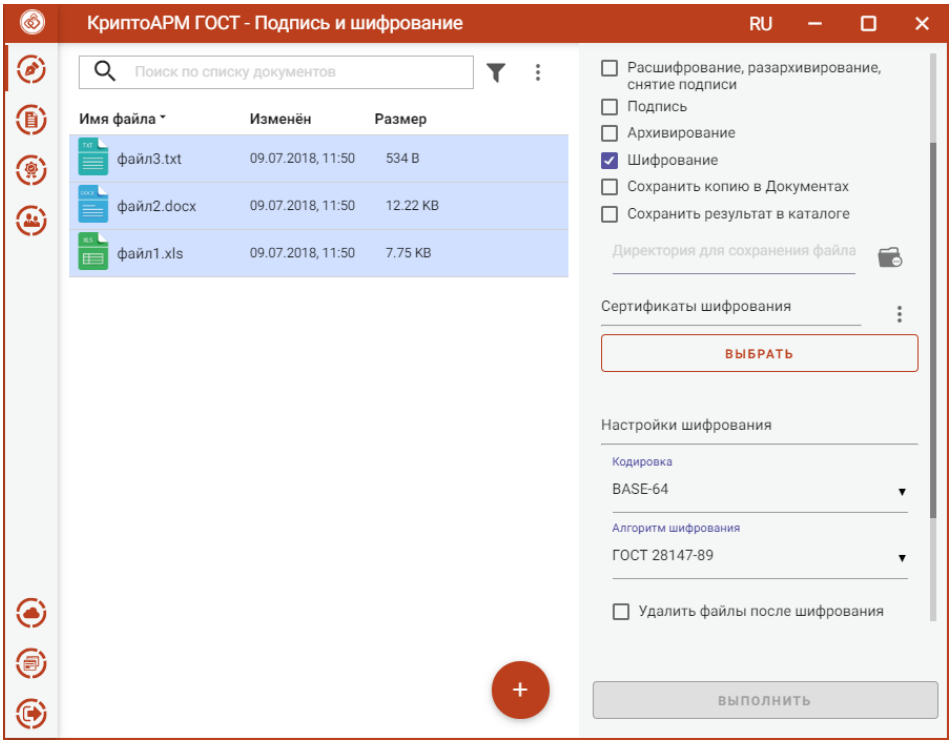
Для данного списка доступны поиск, фильтрация, управление файлами через контекстное меню или кнопками для каждого файла.



Контекстное меню управления списком файлов

5.9.2 Настройка параметров шифрования

Для доступа к настройке параметров шифрования в разделе **Операции** необходимо выбрать опцию **Шифрование**.

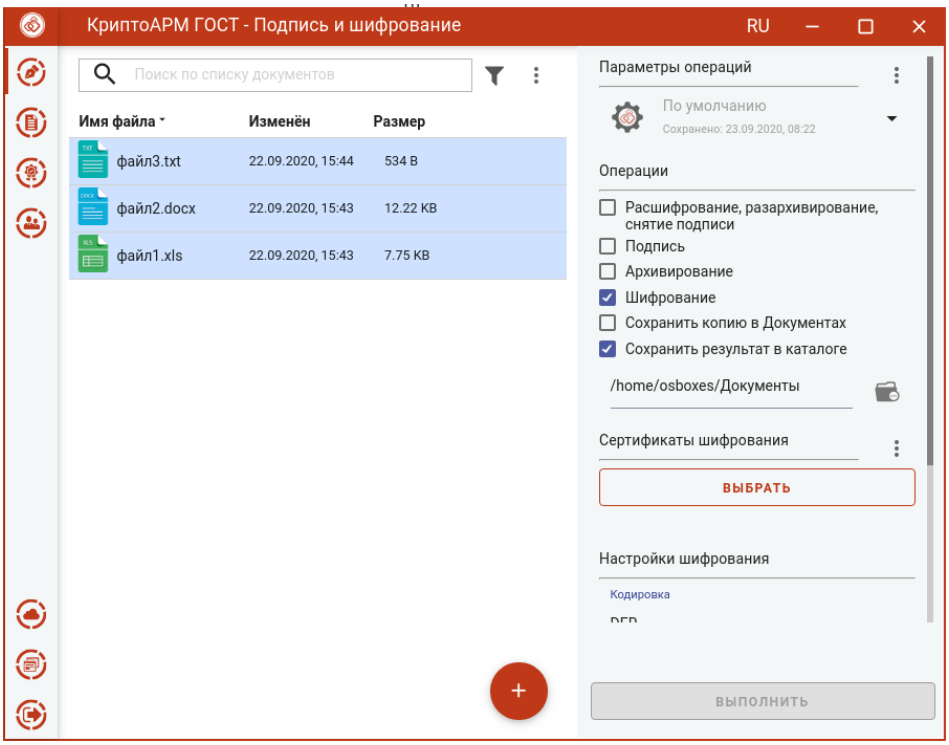


Выбор параметров шифрования

В параметрах можно настроить:

- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнечик». Данный параметр доступен для выбора только начиная с версии КриптоПро CSP 5.0.11635.
- **Удалить файлы после шифрования** - исходные файлы, в случае успешного завершения операции, удаляются из файловой системы.

Можно задать каталог для сохранения зашифрованных документов, выбрав в операциях опцию **Сохранить результат в каталоге.** При установке флага становится доступно поле выбора каталога.



Выбор каталога для сохранения зашифрованного файла

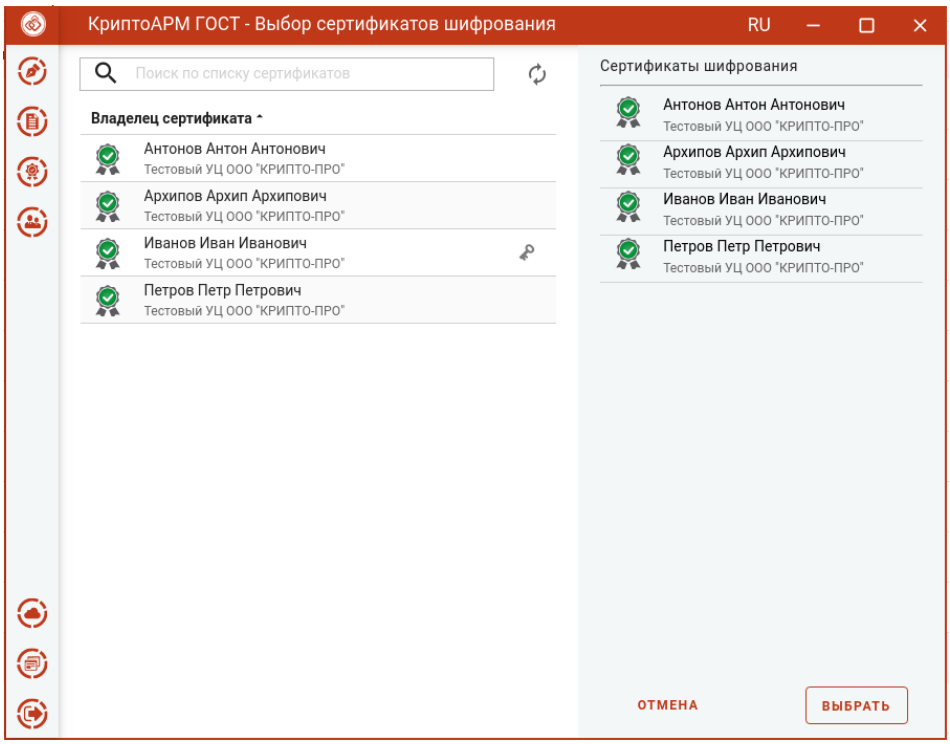
Если флаг не установлен, то файлы сохраняются рядом с исходным файлом.

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Выбранные параметры шифрования можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте **Управление параметрами операции.**

5.9.3 Выбор сертификатов шифрования

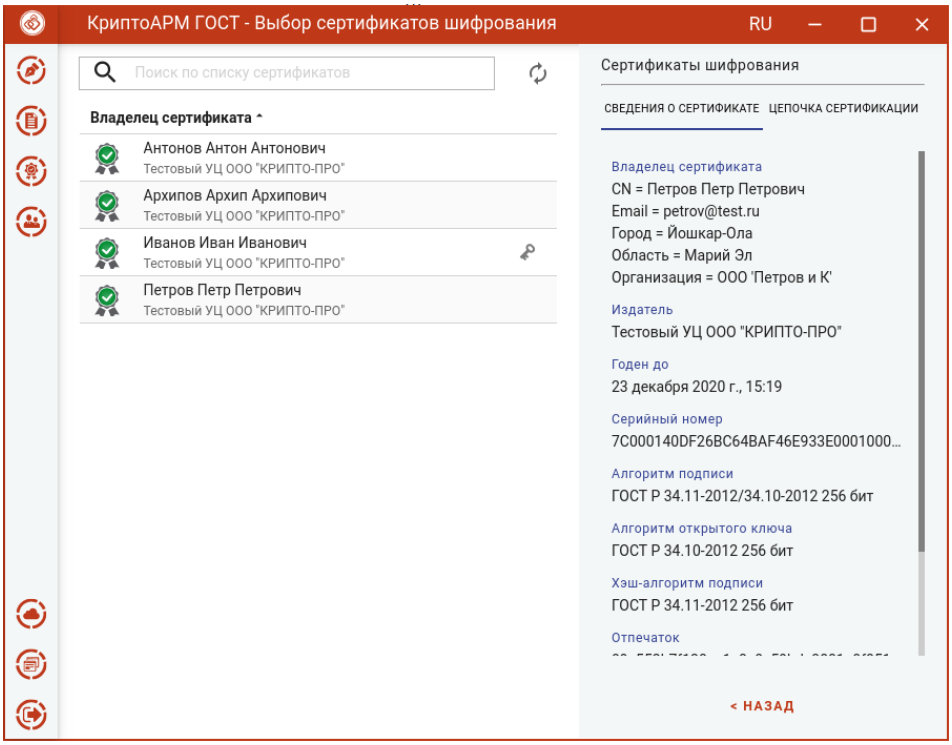
Для того, чтобы выполнить шифрование необходимо выбрать сертификаты получателей. Эта операция производится нажатием кнопки **Выбрать** сертификаты шифрования. В появившемся диалоговом окне отображаются сертификаты категории **Личные** и категории **Сертификаты других пользователей**.



Выбор сертификатов шифрования

В списке допускается выбор нескольких сертификатов, так как число получателей может быть различным.

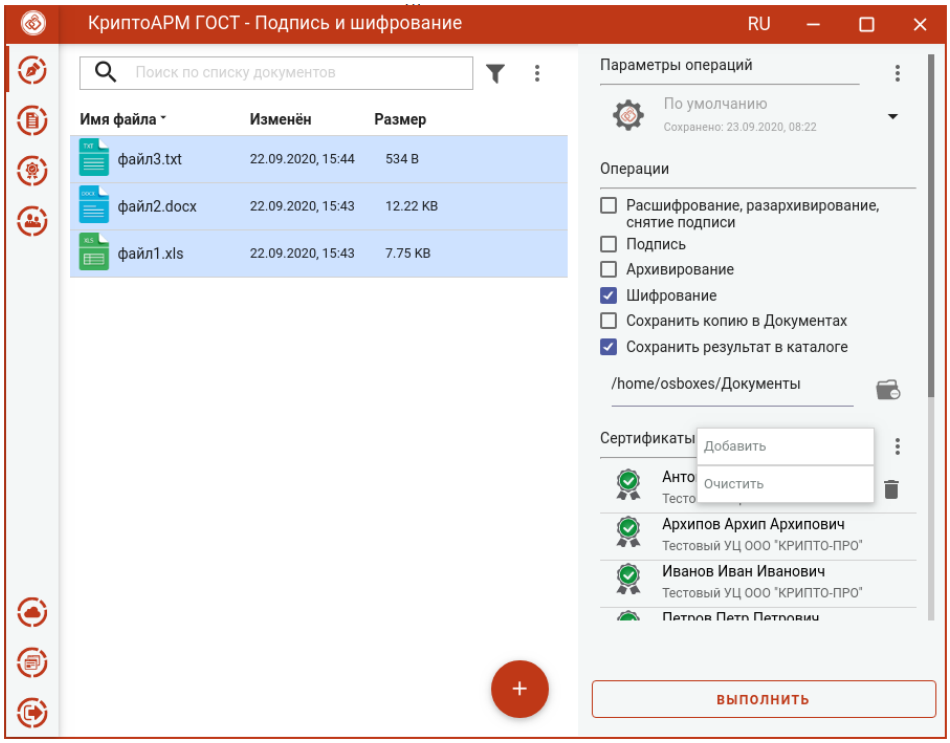
Выбранные сертификаты получателей перемещаются в правый список. Сертификаты в списке можно удалять, по ним можно посмотреть детальную информацию, нажав на интересующий сертификат в правой области.



Информация о сертификате шифрования

Если список сертификатов получателей заполнен, то его можно зафиксировать нажатием на кнопку **Выбрать**.

Изменить список сертификатов шифрования можно с помощью контекстного меню. Удалить сертификаты из сформированного списка можно кнопкой **Удалить**.

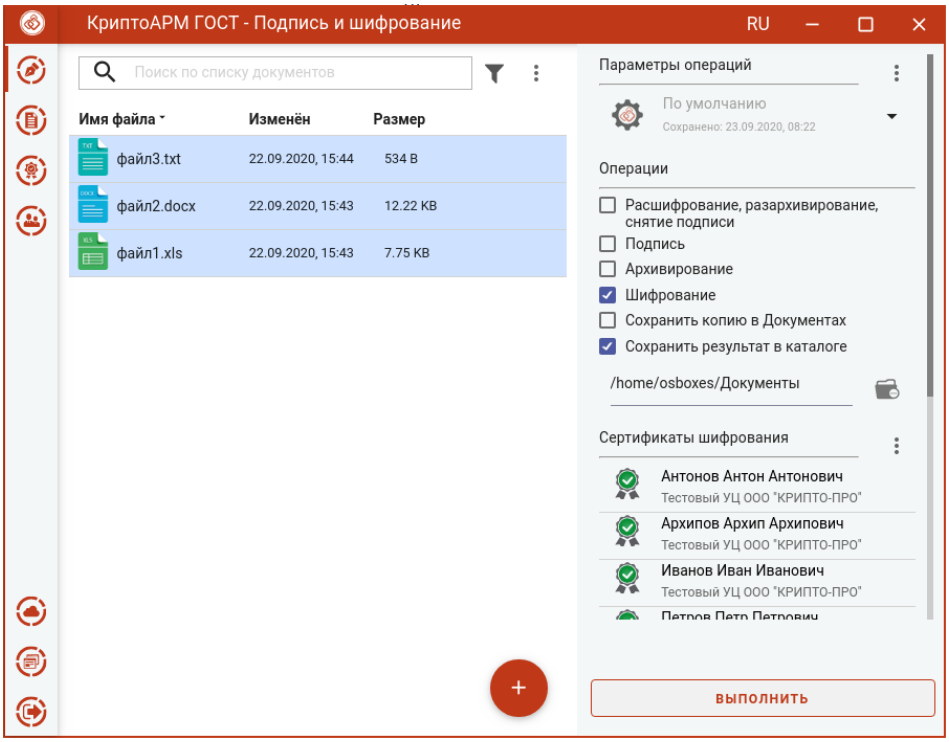


Изменение списка сертификатов шифрования

Если список личных сертификатов и сертификатов других пользователей пуст, то можно их создать или импортировать в разделе Сертификаты.

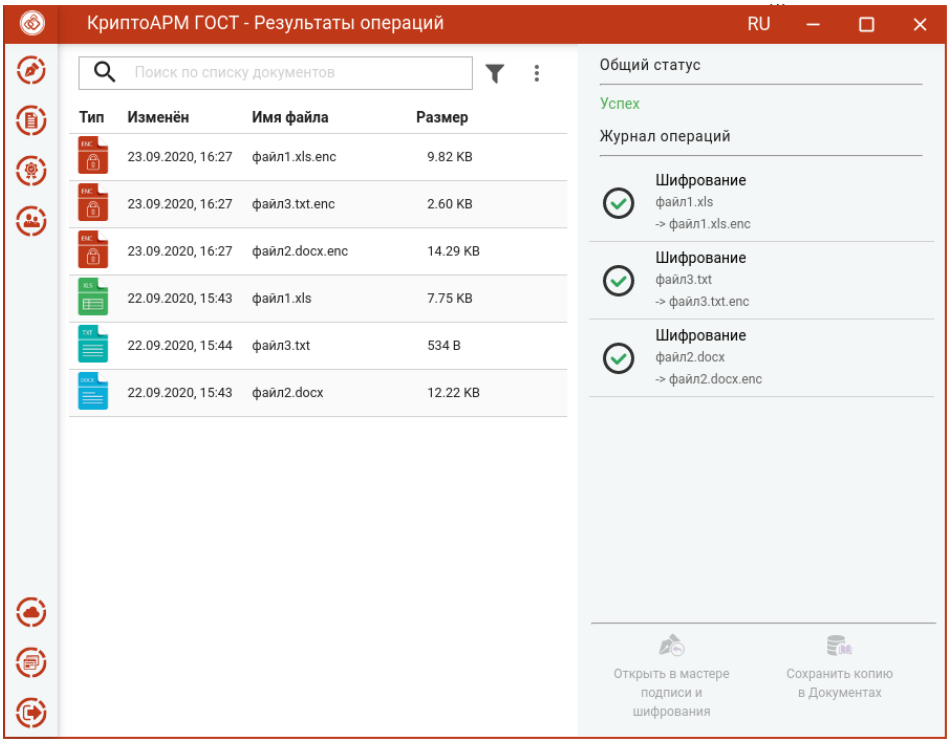
5.9.4 Шифрование файлов

При условии выбора файлов, установки опции **Шифрование**, задания сертификатов получателей становится доступной кнопка **Выполнить**. Шифровать можно любые файлы, кроме зашифрованных.



Шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс шифрования. Исходные и зашифрованные файлы отображаются в отдельном мастере **Результаты операций**.



Результаты операции шифрования

Если в параметрах шифрования была выбрана опция **Удалить файлы после шифрования**, то в **Результатах операций** будут только полученные зашифрованные файлы.

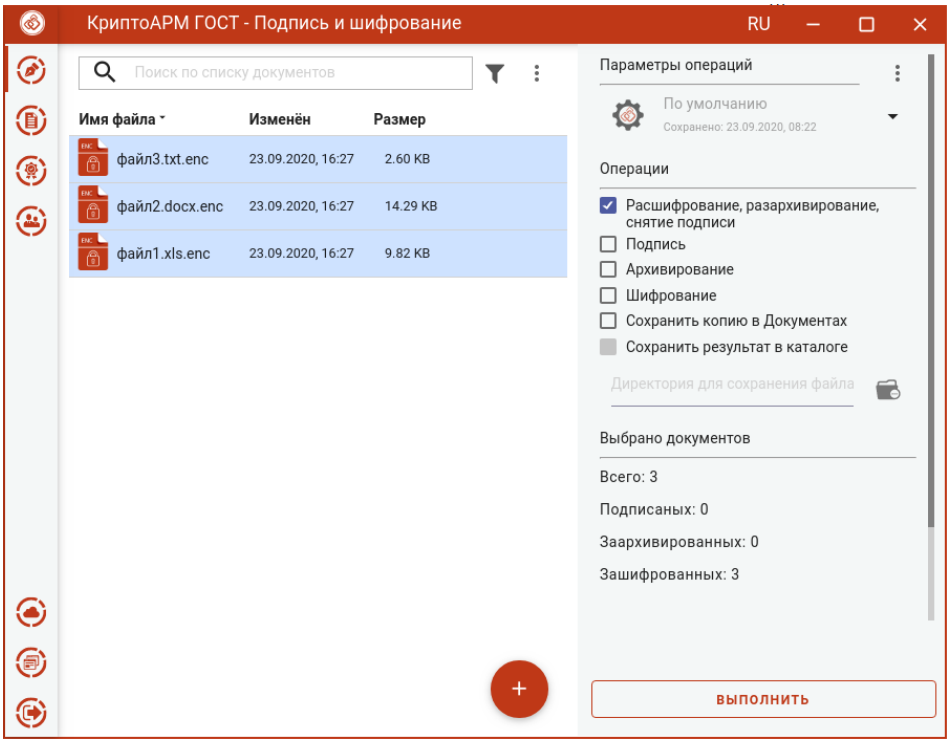
Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в**

Документах служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

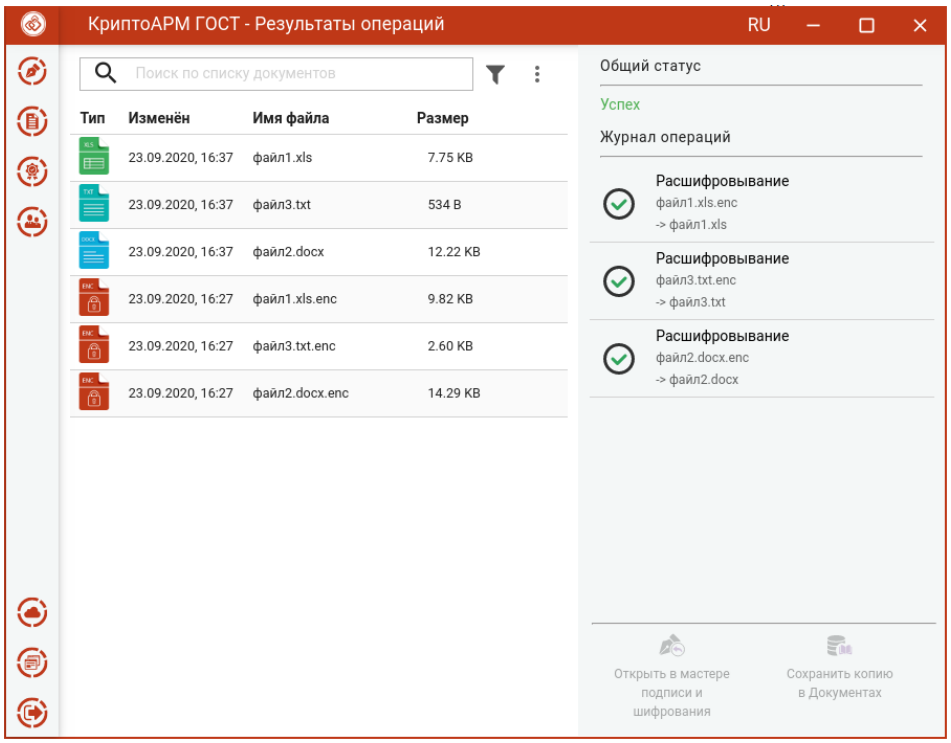
5.10 Расшифрование файлов

Для расшифрования достаточно выбрать зашифрованные файлы с расширением **.enc**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить**. Настройка дополнительных параметров для операции расшифрования не требуется.



Мастер расшифрования файлов

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций.**

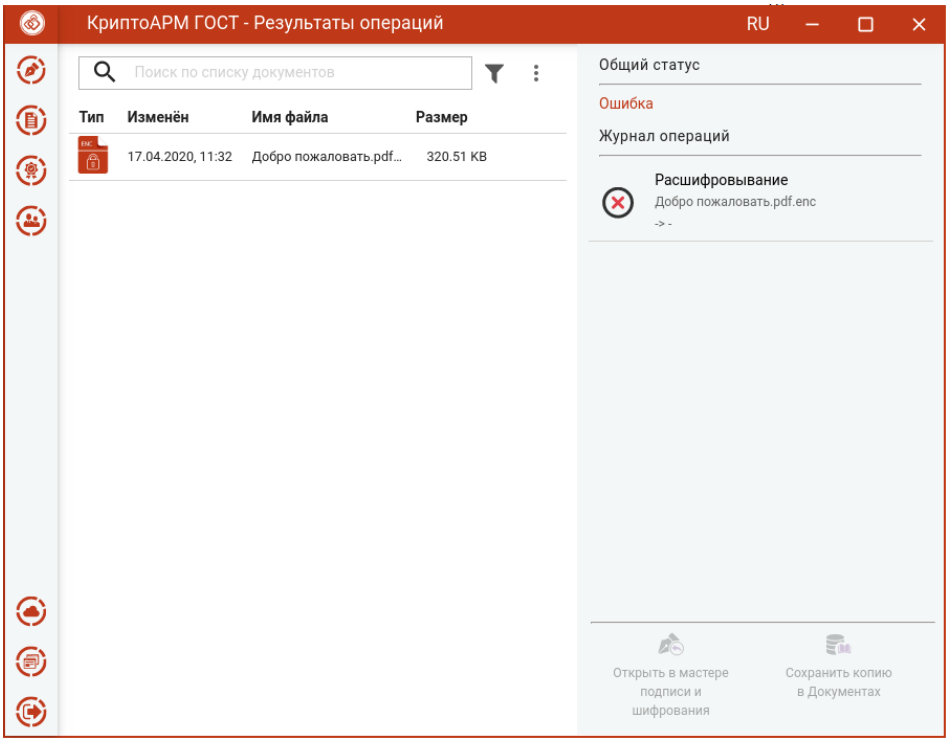


Результат операции расшифрования

Внимание! Документы, полученные в результате обратных операций (расшифрование, разархивирование, снятие подписи), сохраняются во временную папку, расположенную в папке пользователя в каталоге ./Trusted/CryptoARM GOST/TEMP, и остаются там до выполнения следующей операции. Далее временная папка очищается.

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученных после операции файлов в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Если в хранилище сертификатов не окажется сертификата с закрытым ключом, который был выбран в качестве сертификата получателя при шифровании, расшифрование не будет выполнено. В мастере **Результаты операций** будут только зашифрованные файлы.



Ошибка при расшифровании файлов

5.11 Прямые групповые операции (подпись, архивирование, шифрование)

В приложении доступно выполнение следующих групповых операций:

- **Подпись и архивирование** – документ сначала подписывается, затем архивируется;
- **Подпись и шифрование** – документ сначала подписывается, затем шифруется.
- **Архивирование и шифрование** – документ сначала архивируется, затем шифруется.
- **Подпись, архивирование и шифрование** – документ сначала подписывается, затем архивируется, потом шифруется.

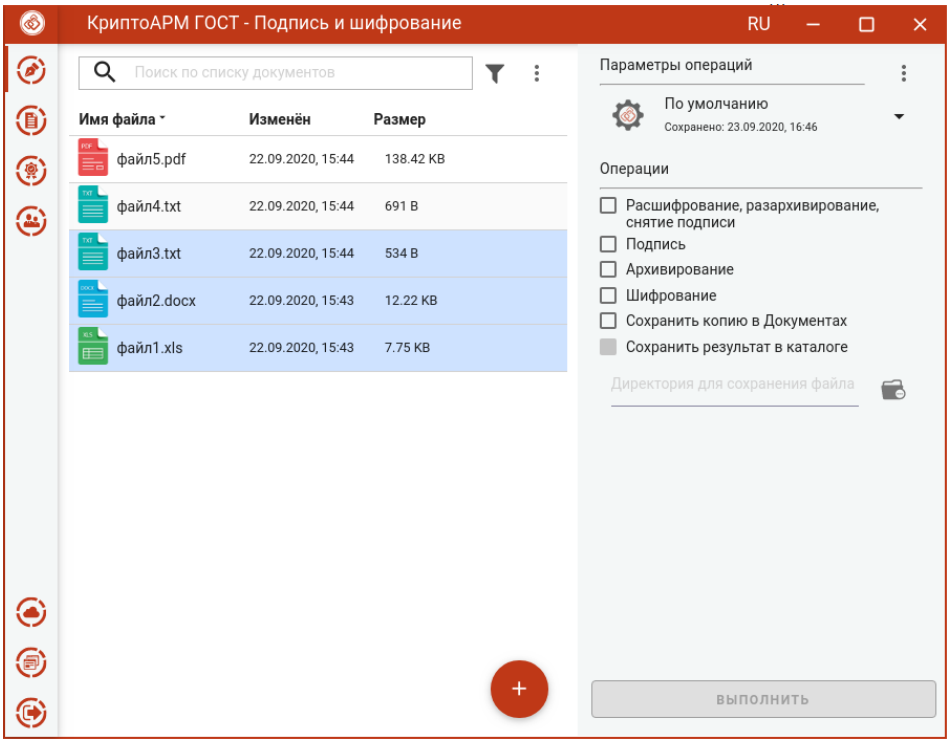
5.11.1 Подпись и архивирование

Для подписи и архивирования файлов нужно в мастере **Подпись и шифрование** выбрать файлы, выбрать опции **Подпись** и **Архивирование** в разделе операций, задать сертификат подписи и параметры подписи.

5.11.1.1 Выбор файлов

В приложении доступно выполнение операций для одного или группы файлов. Файлы можно добавить двумя способами: через кнопку **Добавить (+)** или перетащив мышкой в область формирования списка файлов.

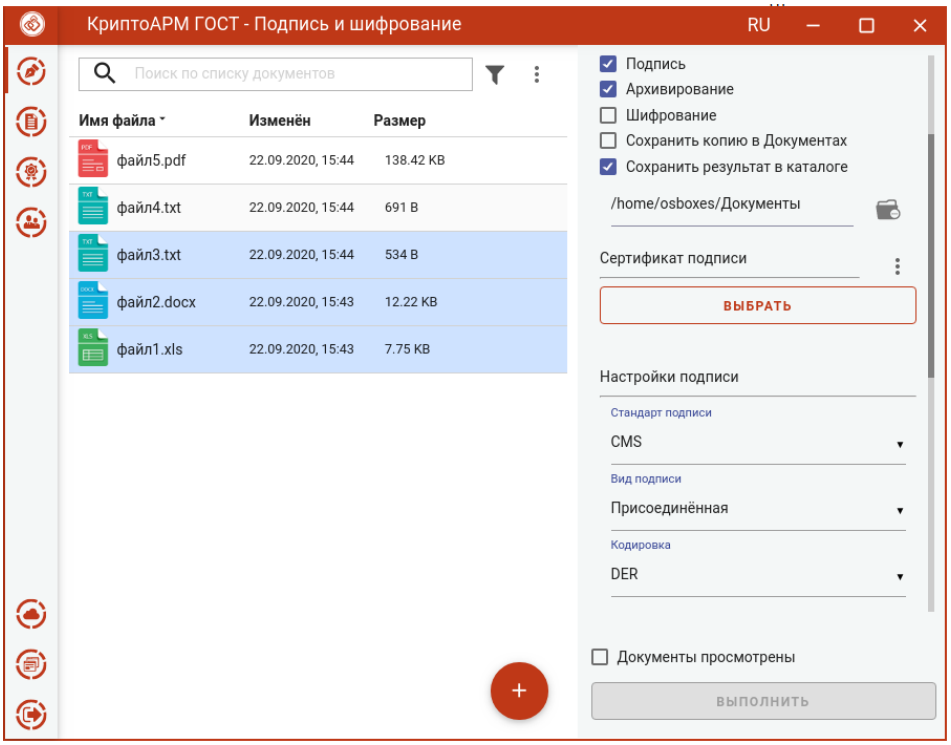
Выбранные файлы заносятся в левую область и представляют собой одноуровневый список.



Список файлов для операции

5.11.1.2 Установка параметров подписи и архивирования

Для операций подписи и архивирования файлов в разделе **Операции** необходимо выбрать опции **Подпись** и **Архивирование,** становятся доступны настройки параметров подписи.



Настройка параметров подписи

В параметрах можно настроить:

- **Сертификат подписи**.
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее в пункте Создание усовершенствованной подписи). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client и КриптоПро OCSP Client.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.

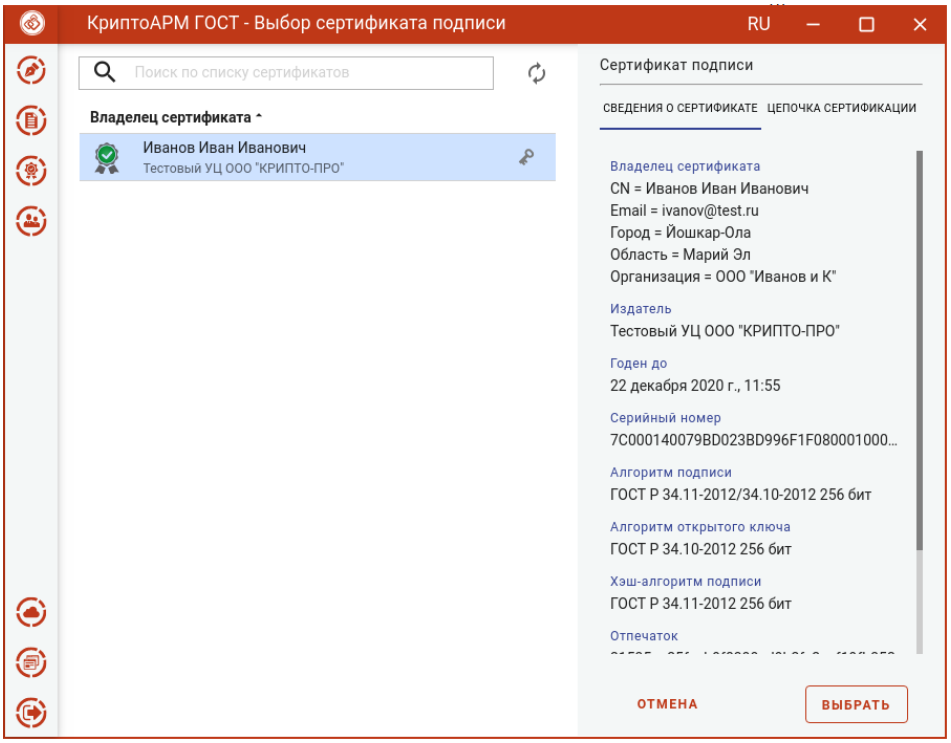
Можно задать каталог для сохранения полученных документов, выбрав в операциях опцию **Сохранить результат в каталоге.** При установке флага становится доступно поле выбора каталога. Если флаг не установлен, то файл сохраняется рядом с исходным.

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Выбранные параметры можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте Управление параметрами операции**.**

5.11.1.3 Выбор сертификата подписи

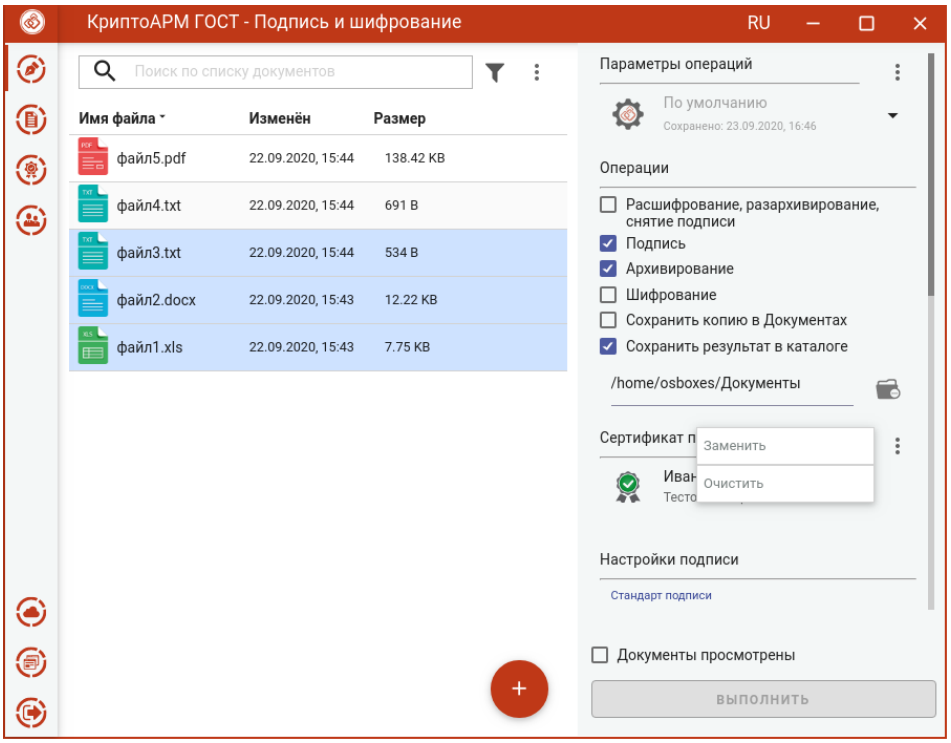
Для того, чтобы выполнить подпись необходимо выбрать сертификат, к которому привязан закрытый ключ. Эта операция производится нажатием кнопки **Выбрать** сертификат подписи. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи.



Выбор сертификата подписи

Выбор сертификата подписи осуществляется его выделением и нажатием на кнопку **Выбрать**.

Сертификат подписи можно изменить с помощью контекстного меню.

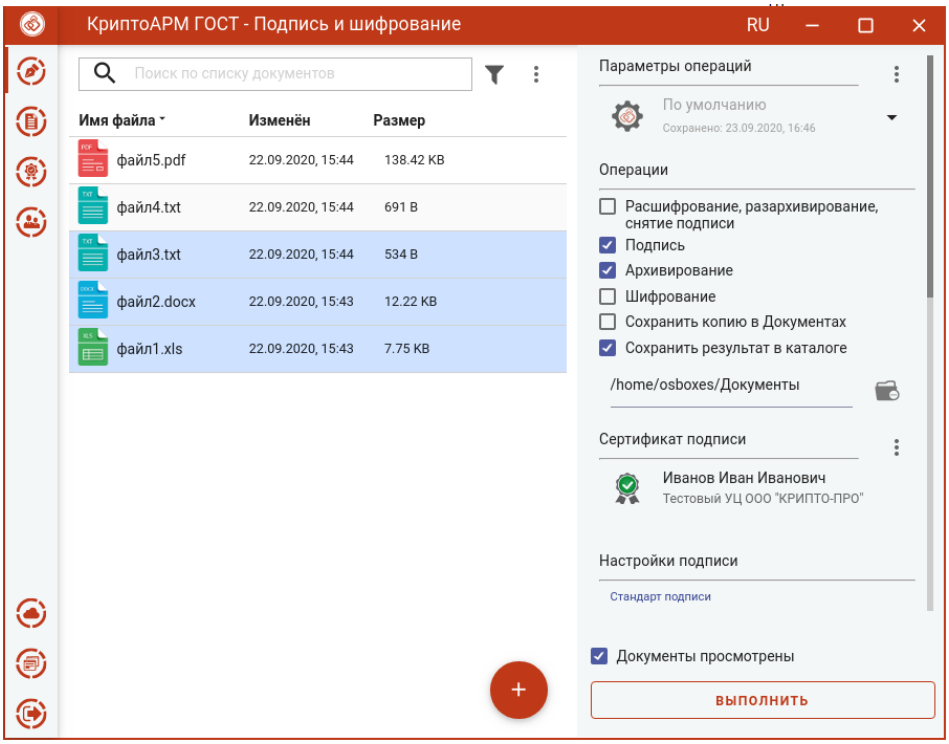


Изменение сертификата подписи

Если в хранилище личных сертификатов нет сертификата с закрытым ключом, то можно его создать или импортировать в разделе Сертификаты.

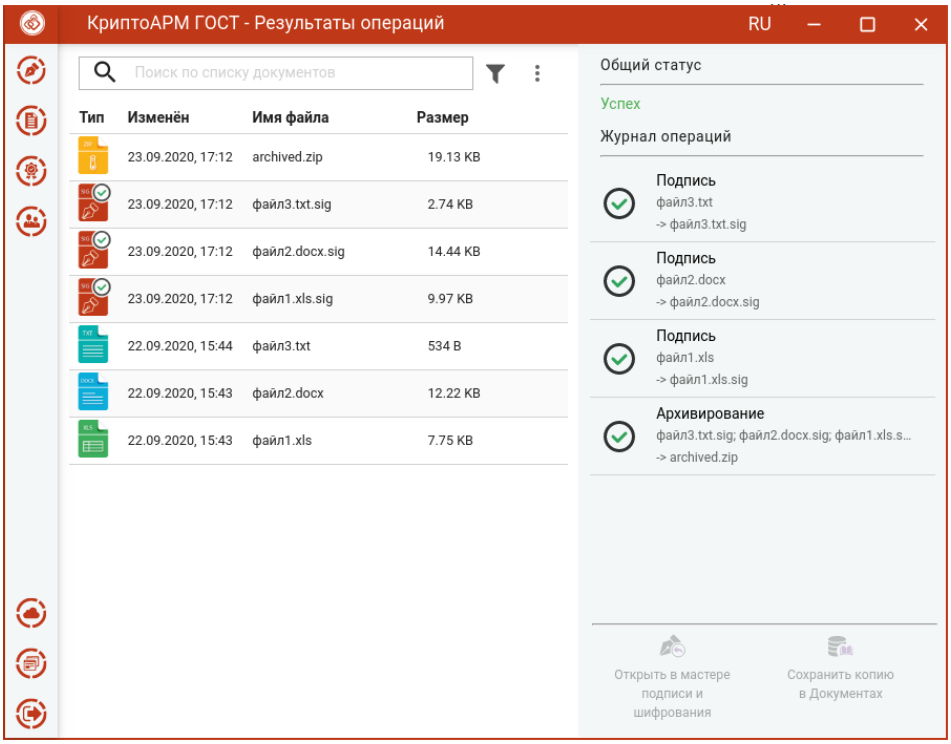
5.11.1.4 Подпись и архивирование файлов

При условии выбора сертификата подписи, файлов и установленного флага, что **Документы просмотрены**, в мастере становится доступной кнопка **Выполнить**. Подписать и заархивировать можно любые файлы, кроме зашифрованных.



Подпись и архивирование файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи, а затем подписанные файлы архивируются. Исходные документы (оригиналы), подписанные файлы (промежуточные) и результаты операции архивирования отображаются в отдельном мастере **Результаты операций**.



Результаты операций

Если архивируется несколько файлов, то архиву автоматически задается имя **archived.zip**. Если архивируется один файл, то к имени файла добавляется расширение .sig.zip.

Архив сохраняется в каталоге, если в операциях был выбран каталог для сохранения результатов, или в домашней папке пользователя, если в операциях не был установлен флаг **Сохранить результат в каталоге**.

Подписанные файлы сохраняются во временную папку TEMP, расположенную в домашней папке пользователя в каталоге ./Trusted/CryptoARM GOST/, и остаются до выполнения следующей операции.

Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученного после операции файла сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Для подписанных файлов подпись проверяется автоматически.

После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

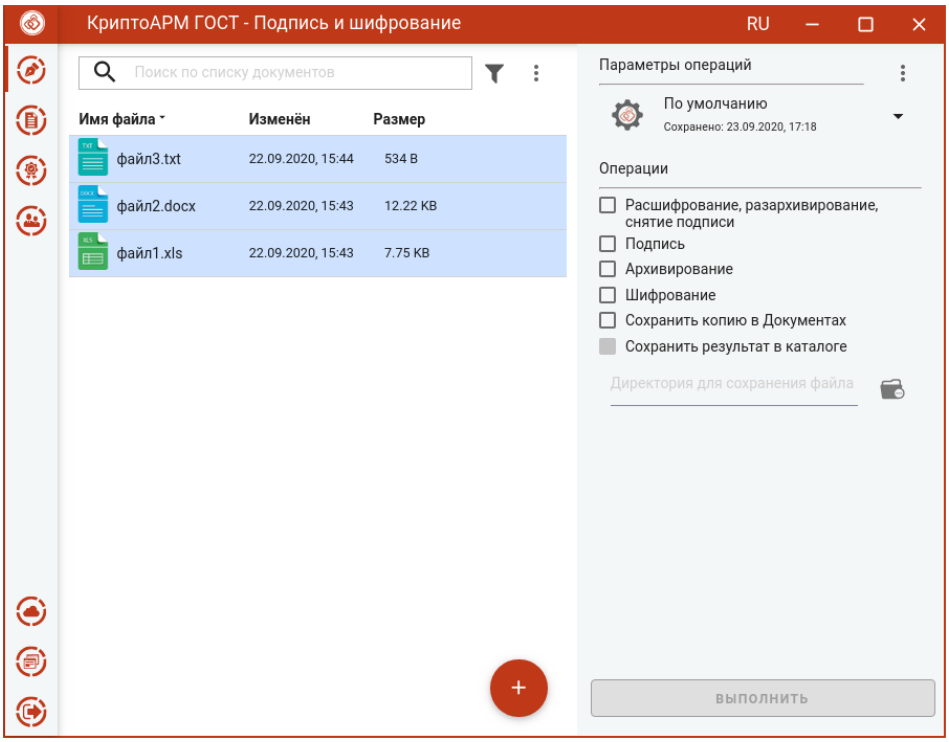
5.11.2 Подпись и шифрование

Для подписи и шифрования файлов нужно в мастере **Подпись и шифрование** выбрать файлы, выбрать опции **Подпись** и **Шифрование** в разделе операций, задать сертификат подписи, сертификаты получателей, параметры подписи и шифрования.

5.11.2.1 Выбор файлов

В приложении доступно выполнение операций для одного или группы файлов. Файлы можно добавить двумя способами: через кнопку **Добавить (+)** или перетащив мышкой в область формирования списка файлов.

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список.

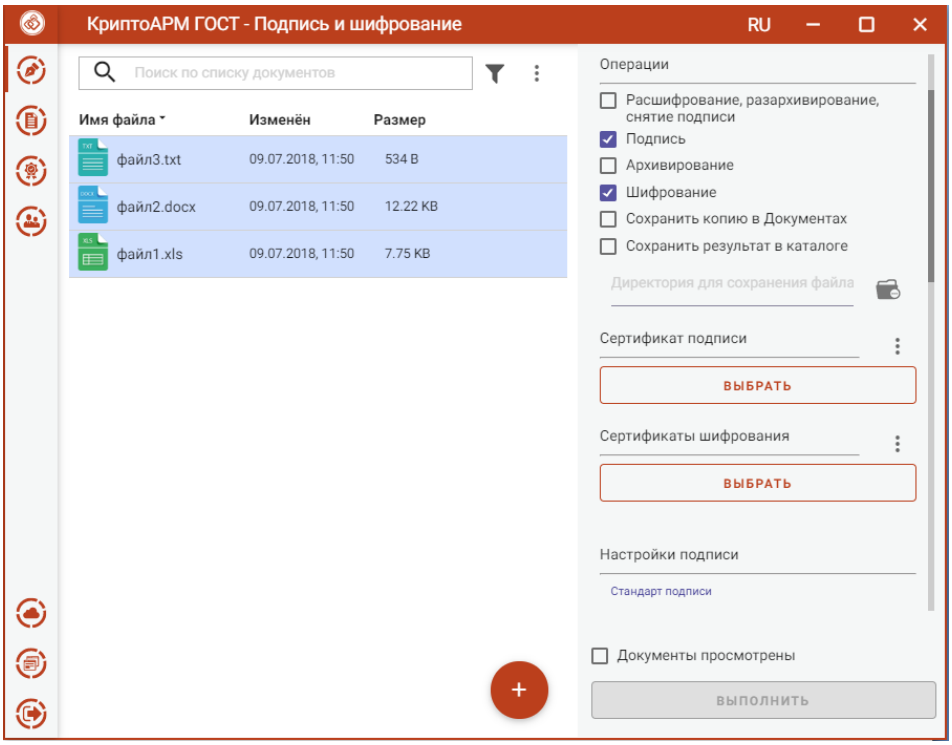


Список файлов для операции

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла.

5.11.2.2 Установка параметров подписи и шифрования

Для операций подписи и шифрования файлов в разделе **Операции** необходимо выбрать опции **Подпись** и **Шифрование.** Становятся доступны настройки параметров подписи и шифрования.



Настройка параметров подписи и шифрования

В параметрах подписи можно настроить:

- **Сертификат подписи** - сертификат, к которому привязан закрытый ключ. Выбор сертификата производится нажатием кнопки **Выбрать**. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи.
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее в пункте Создание усовершенствованной подписи). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client и КриптоПро OCSP Client.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.

В параметрах шифрования можно настроить:

- **Сертификаты шифрования** - сертификаты получателей. Выбор производится нажатием кнопки **Выбрать** сертификаты шифрования. В появившемся диалоговом окне отображаются сертификаты категории **Личные** и категории **Сертификаты других**

пользователей (Контакты). В списке допускается выбор нескольких сертификатов, так как число получателей может быть различным.

- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнечик». Данный параметр доступен для выбора только начиная с версии КриптоПро CSP 5.0.11635.
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции.

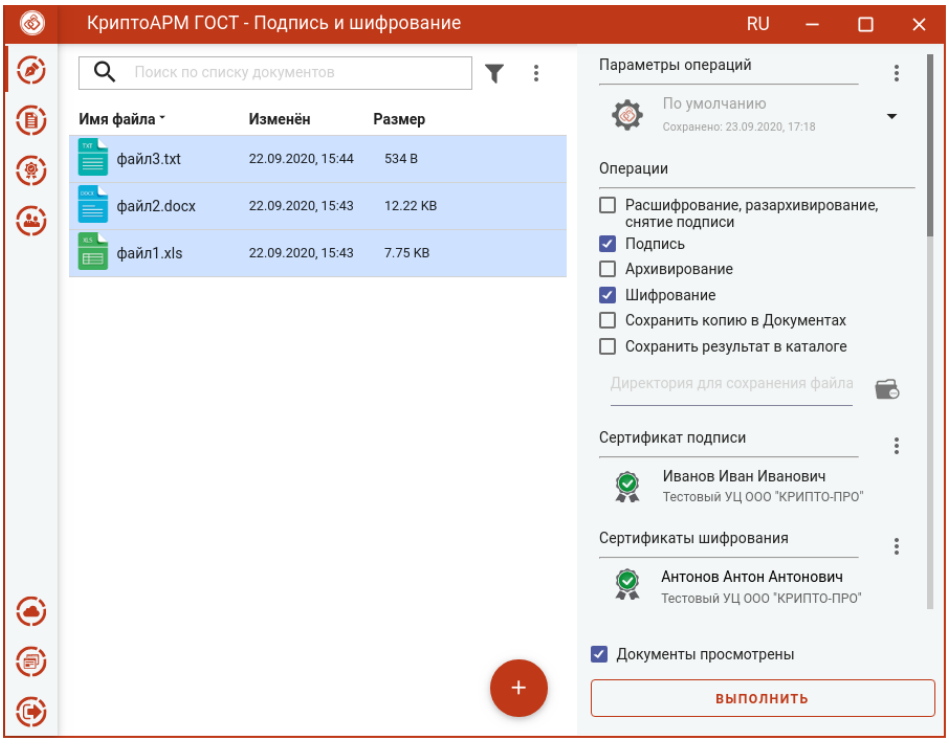
Можно задать каталог для сохранения полученных документов, выбрав в операциях опцию **Сохранить результат в каталоге. П**ри установке флага становится доступно поле выбора каталога. Если флаг не установлен, то файл сохраняется рядом с исходным.

Опция **Сохранить копию в Документах** служит для сохранения копии полученных после операции файлов в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Выбранные параметры можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте Управление параметрами операции**.**

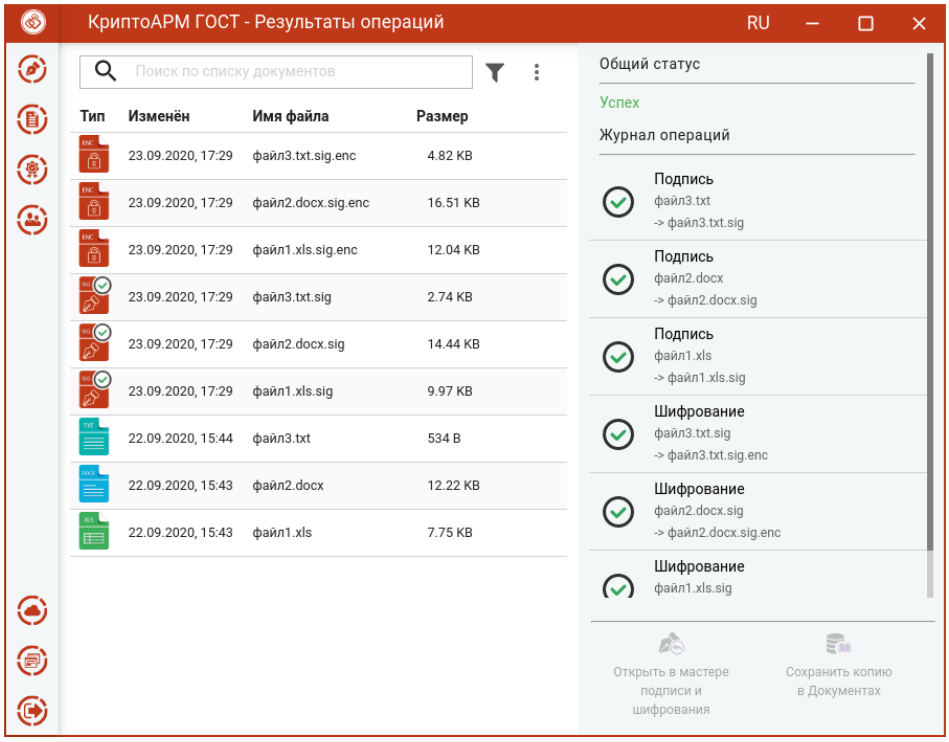
5.11.2.3 Подпись и шифрование файлов

При условии выбора сертификата подписчика, сертификатов получателей, файлов для выполнения операции и установленного флага, что документы просмотрены, в мастере становится доступной кнопка **Выполнить**. Подписать и зашифровать можно любые файлы, кроме зашифрованных.



Подпись и шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи, а затем подписанные файлы шифруются. Исходные документы (оригиналы), подписанные файлы (промежуточные) и результаты операции шифрования отображаются в отдельном мастере **Результаты операций**.



Результаты операций

Зашифрованные файлы сохраняются в каталоге, если в операциях был выбран каталог для сохранения результатов, или рядом с исходными файлами. Подписанные файлы сохраняются во временную папку TEMP, расположенную в домашней папке пользователя в каталоге ./Trusted/CryptoARM GOST/, и остаются до выполнения следующей операции.

Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученных после операции файлов сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Если при выборе параметров подписи был указан вид подписи **Отсоединенная**, то перед шифрованием исходные файлы и подписанные архивируются, а затем шифруются. В итоге операции подписи и шифрования получится зашифрованный архив archived.zip.enc, который сохраняется в папку пользователя, если не задан каталог для сохранения результатов.

Если в параметрах шифрования была выбрана опция **Удалить после шифрования**, то в **Результатах операций** будут только полученные зашифрованные файлы.

Для подписанных файлов подпись проверяется автоматически.

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученных после операции файлов в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

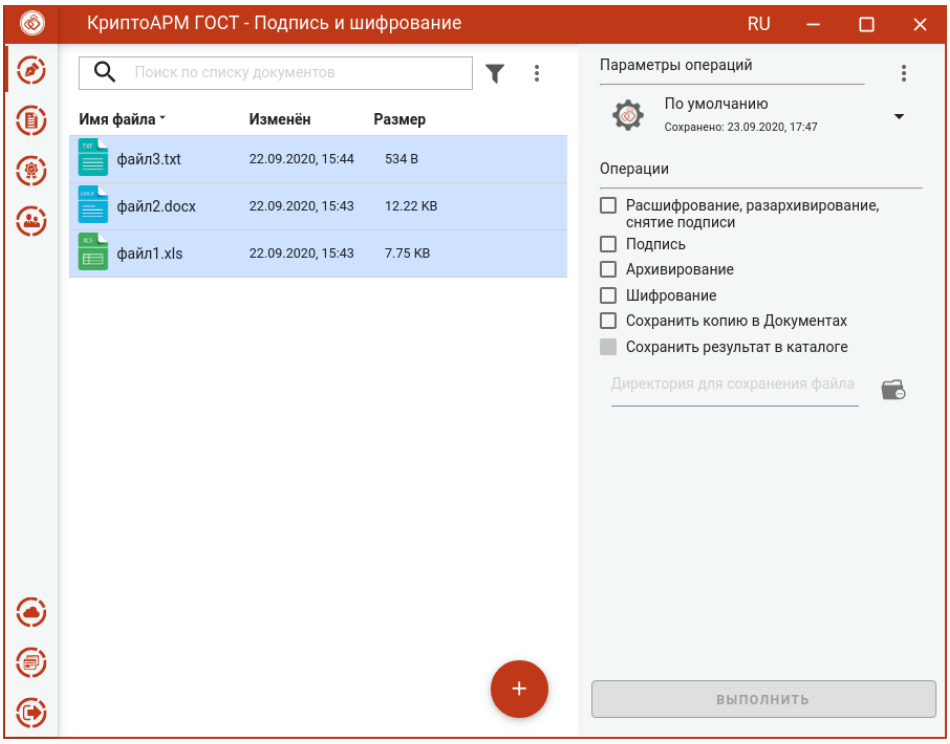
5.11.3 Архивирование и шифрование

Для архивирования и шифрования файлов нужно в мастере **Подписи и шифрования** выбрать файлы, выбрать в разделе операций опции **Архивирование** и **Шифрование**, задать сертификаты получателей, параметры шифрования.

5.11.3.1 Выбор файлов

В приложении доступно выполнение операций для одного или группы файлов. Файлы можно добавить двумя способами: через кнопку **Добавить (+)** или перетащив мышкой в область формирования списка файлов для операции.

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список.

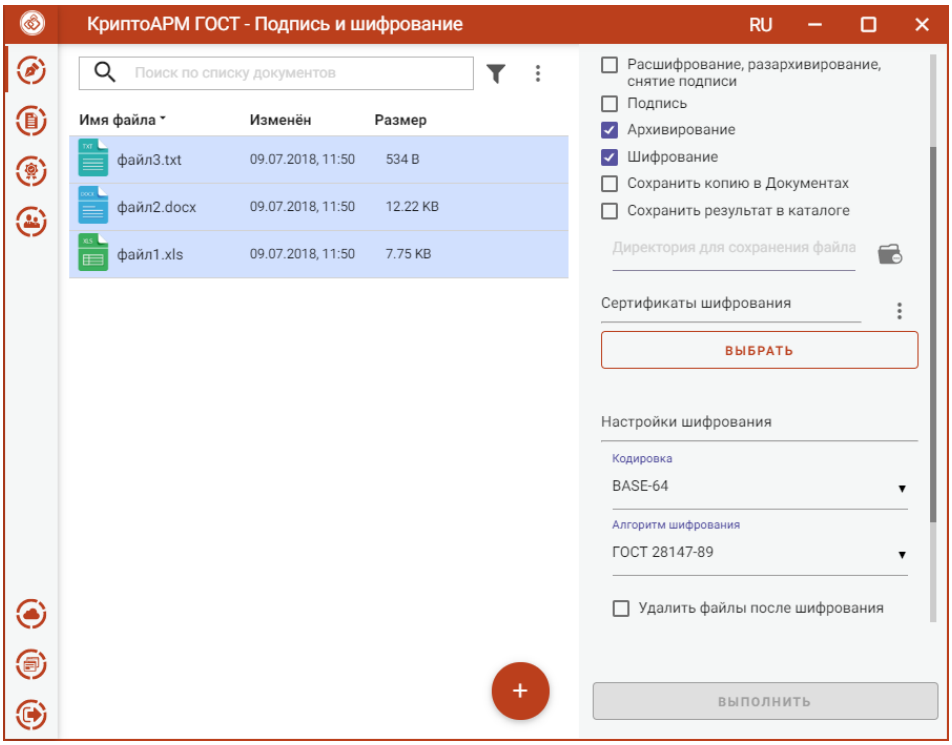


Список файлов для операции

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла.

5.11.3.2 Установка параметров архивирования и шифрования

В разделе **Операции** необходимо выбрать опции **Архивирование** и **Шифрование,** становятся доступны настройки параметров шифрования.



Настройка параметров архивирования и шифрования

В параметрах шифрования можно настроить:

- **Сертификаты шифрования** - сертификаты получателей. Выбор производится нажатием кнопки **Выбрать** сертификаты шифрования. В появившемся диалоговом окне отображаются сертификаты категории **Личные** и категории **Сертификаты других пользователей (Контакты)**. В списке сертификатов допускается выбор нескольких сертификатов, так как число получателей может быть различным.
- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнечик». Данный параметр доступен для выбора только начиная с версии КриптоПро CSP 5.0.11635.
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции.

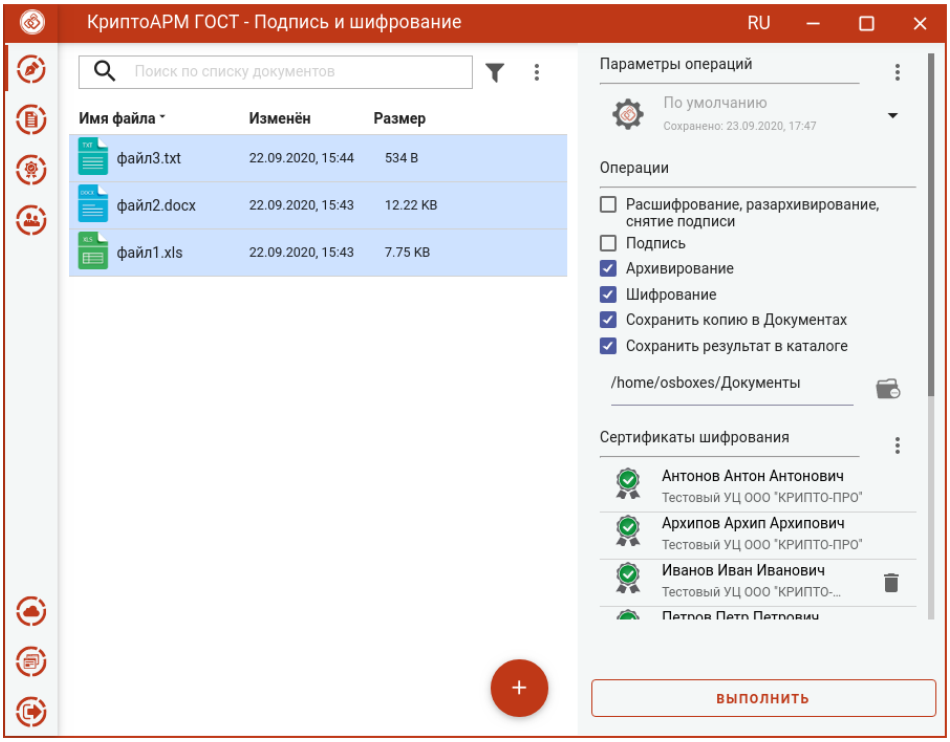
Можно задать каталог для сохранения полученных документов, выбрав в операциях опцию **Сохранить результат в каталоге.** При установке флага становится доступно поле выбора каталога. Если флаг не установлен, то файлы сохраняются рядом с исходным.

Опция **Сохранить копию в Документах** служит для сохранения копии полученных после операции файлов в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Выбранные параметры можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте Управление параметрами операции**.**

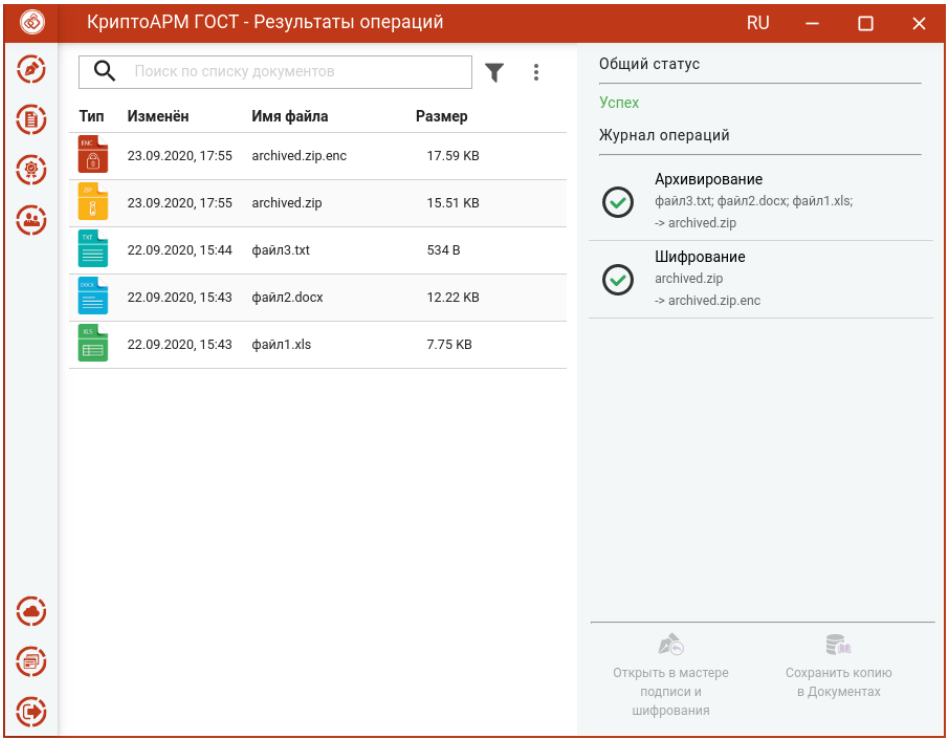
5.11.3.3 Архивирование и шифрование файлов

При условии выбора сертификатов получателей, файлов, в мастере становится доступной кнопка **Выполнить**. Заархивировать и зашифровать можно любые файлы, кроме зашифрованных.



Архивирование и шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс архивирования, а затем архив шифруется. Исходные документы (оригиналы), архив (промежуточный) и результаты операции шифрования отображаются в отдельном мастере **Результаты операций.**



Результаты операций

Если архивируется несколько файлов, то архиву автоматически задается имя **archived.zip**. Если архивируется один файл, то к имени файла добавляется расширение zip.enc.

Полученный файл сохраняется в каталоге, если в операциях был выбран каталог для сохранения результатов, или в папке пользователя. Архив сохраняется во временную папку TEMP, расположенную в домашней папке пользователя в каталоге ./Trusted/CryptoARM GOST/, и остается до выполнения следующей операции.

Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученного после операции файла сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Если в параметрах шифрования была выбрана опция **Удалить файлы после шифрования**, то в **Результатах операций** будет только полученный зашифрованный файл.

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

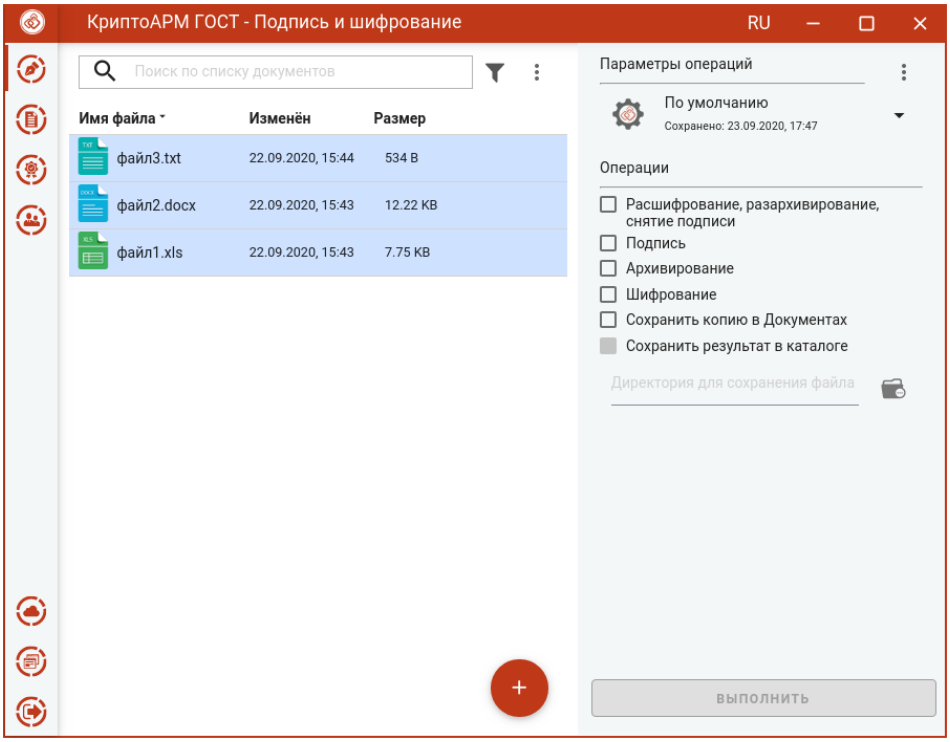
5.11.4 Подпись, архивирование и шифрование

Для подписи, архивирования и шифрования файлов нужно в мастере **Подписи и шифрования** выбрать файлы, выбрать в разделе операций опции **Подпись, Архивирование** и **Шифрование**, задать сертификат подписи, сертификаты получателей, параметры подписи и шифрования.

5.11.4.1 Выбор файлов

В приложении доступно выполнение операций для одного или группы файлов. Файлы можно добавить двумя способами: через кнопку **Добавить (+)** или перетащив мышкой в область формирования списка файлов для операции.

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список.

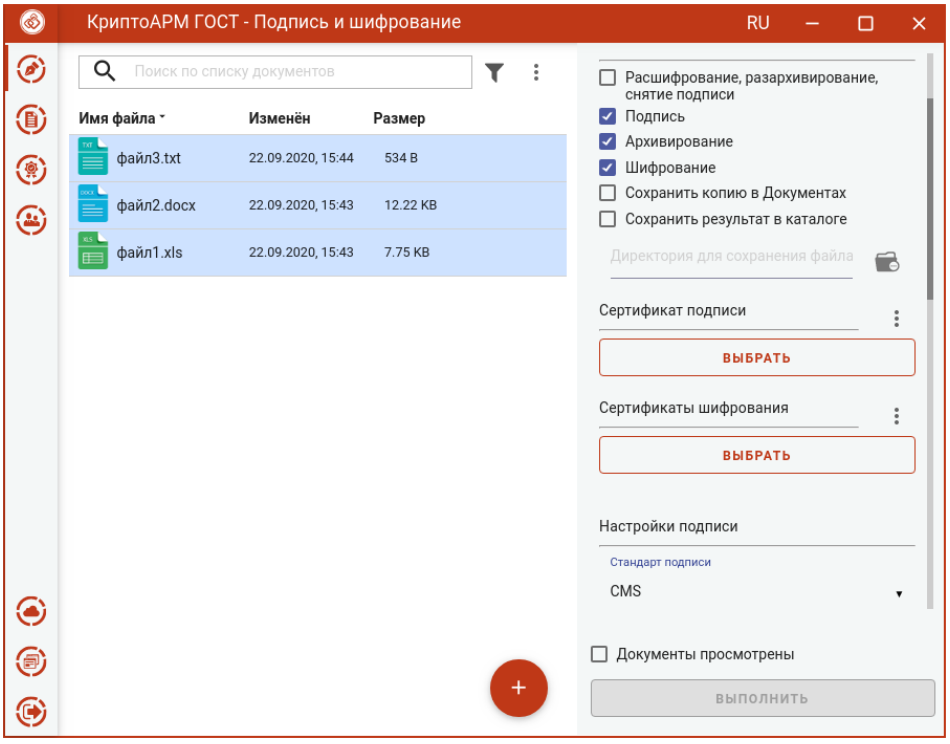


Список файлов для операций

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла.

5.11.4.2 Установка параметров подписи и шифрования

В разделе **Операции** необходимо выбрать опции **Подпись, Архивирование** и **Шифрование,** становятся доступны настройки параметров подписи и шифрования.



Настройка параметров подписи и шифрования

В параметрах подписи можно настроить:

- **Сертификат подписи** - сертификат, к которому привязан закрытый ключ. Выбор сертификата производится нажатием кнопки **Выбрать**. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи.
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее в пункте Создание усовершенствованной подписи). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client и КриптоПро OCSP Client.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно в пункте Создание подписи со штампом времени). Данная опция доступна только при установленном модуле КриптоПро TSP Client.

В параметрах шифрования можно настроить:

- **Сертификаты шифрования** - сертификаты получателей. Выбор производится нажатием кнопки **Выбрать**. В появившемся диалоговом окне отображаются сертификаты категории **Личные** и категории **Сертификаты других пользователей (Контакты)**. В списке сертификатов допускается выбор нескольких сертификатов, так как число получателей может быть различным.
- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнечик». Данный параметр доступен для выбора только начиная с версии КриптоПро CSP 5.0.11635.
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции.

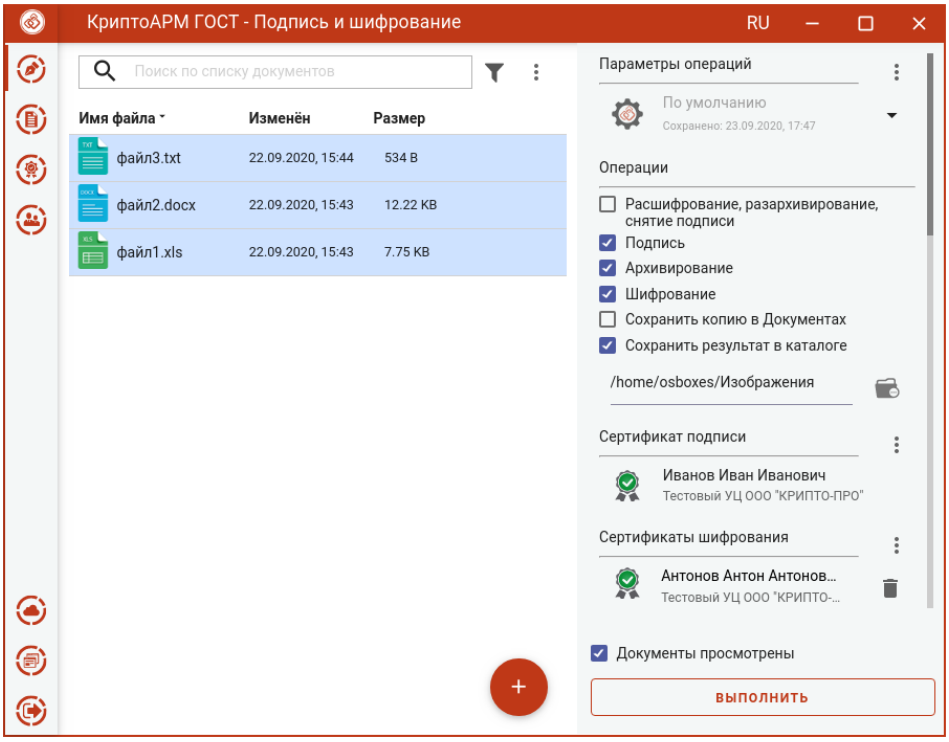
Можно задать каталог для сохранения полученных документов, выбрав в операциях опцию **Сохранить результат в каталоге.** При установке флага становится доступно поле выбора каталога. Если флаг не установлен, то файл сохраняется в папку пользователя.

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Выбранные параметры можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте Управление параметрами операции**.**

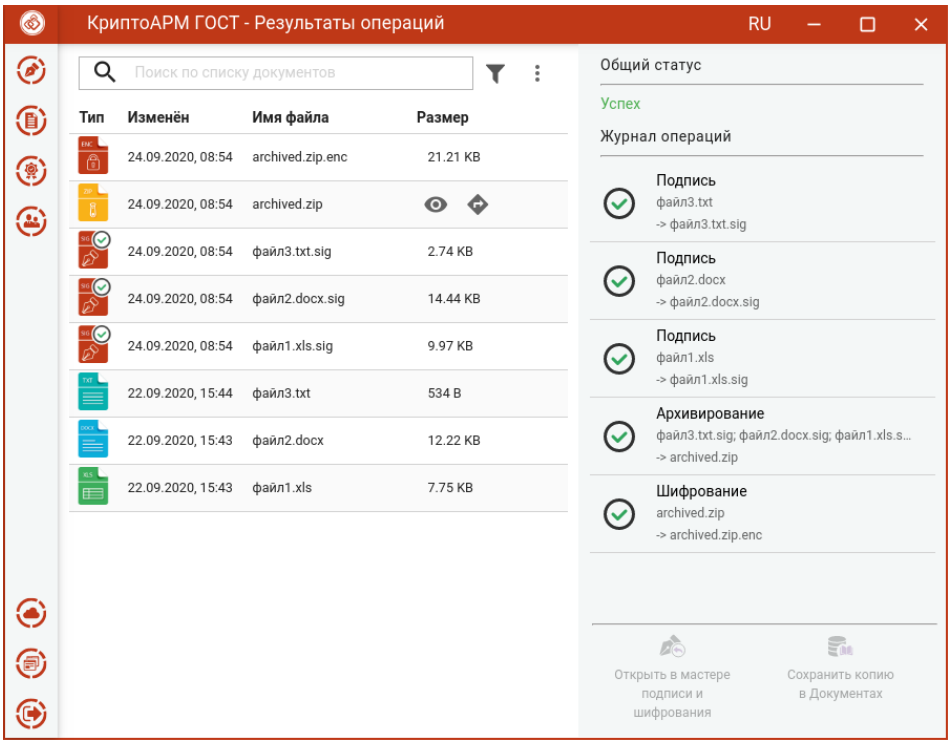
5.11.4.3 Подпись, архивирование и шифрование файлов

При условии выбора сертификатов, файлов, установленного флага, что **Документы просмотрены**, в мастере становится доступной кнопка **Выполнить**.



Подпись, архивирование и шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи, потом архивирования, а затем архив шифруется. Исходные документы (оригиналы), подписанные файлы, архив (промежуточные) и результат операции шифрования отображаются в отдельном мастере **Результаты операций.**



Результаты операций

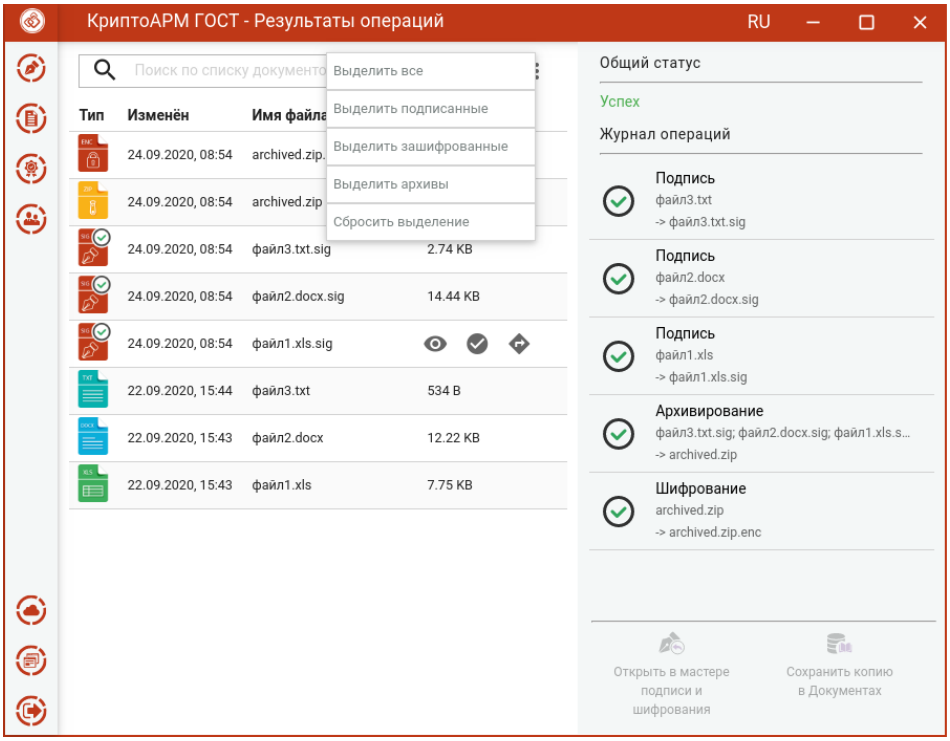
Если подписывается и архивируется несколько файлов, то архиву автоматически задается имя **archived.zip**. Если подписывается и архивируется один файл, то к имени файла добавляется расширение .sig.zip.enc.

Полученный файл сохраняется в каталоге, если в операциях был выбран каталог для сохранения результатов, или в папке пользователя. Подписанные файлы и архив сохраняется во временную папку TEMP, расположенную в домашней папке пользователя в каталоге ./Trusted/CryptoARM GOST/, и остается до выполнения следующей операции.

Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученного после операции файла сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Если в параметрах шифрования была выбрана опция **Удалить файлы после шифрования**, то в **Результатах операций** будет только полученный зашифрованный файл, исходные и промежуточные будут удалены.

Для списка документов доступны поиск, фильтрация, выделение по типу операции. Для каждого файла доступны просмотр, переход в папку, а для подписанных файлов – проверка подписи.



Операции с документами в результатах операций

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

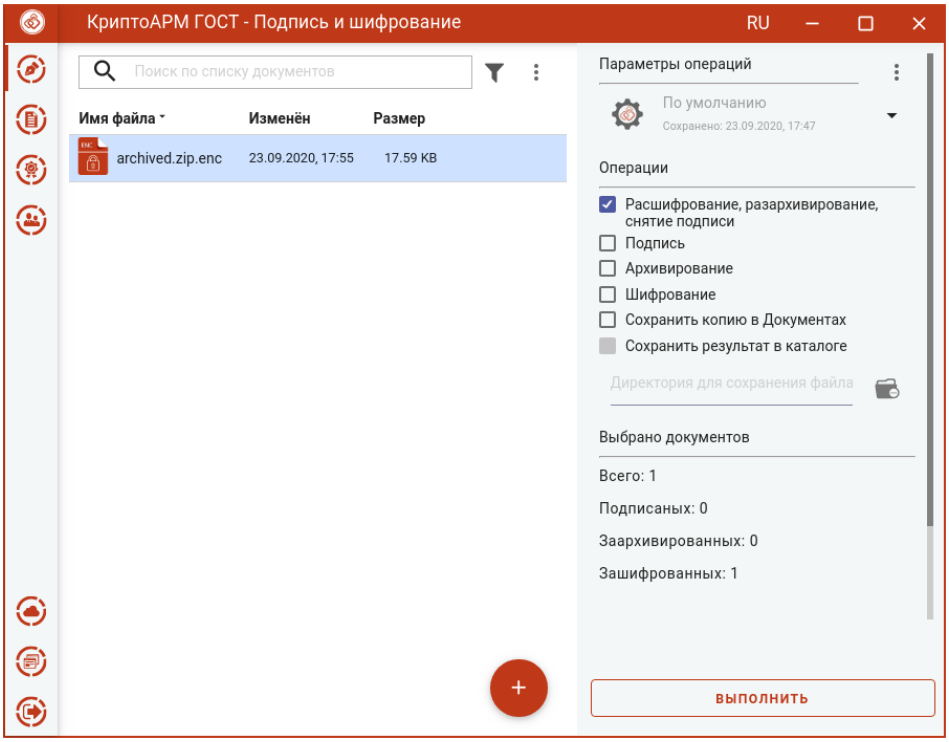
После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

5.12 Обратные групповые операции (расшифрование, разархивирование, снятие подписи)

В приложении доступно выполнение обратных групповых операций (расшифрование, разархивирование и снятие подписи) за одну итерацию. Требуется только выбрать файлы, включить опцию **Расшифрование, разархивирование, снятие подписи** и нажать кнопку **Выполнить**.

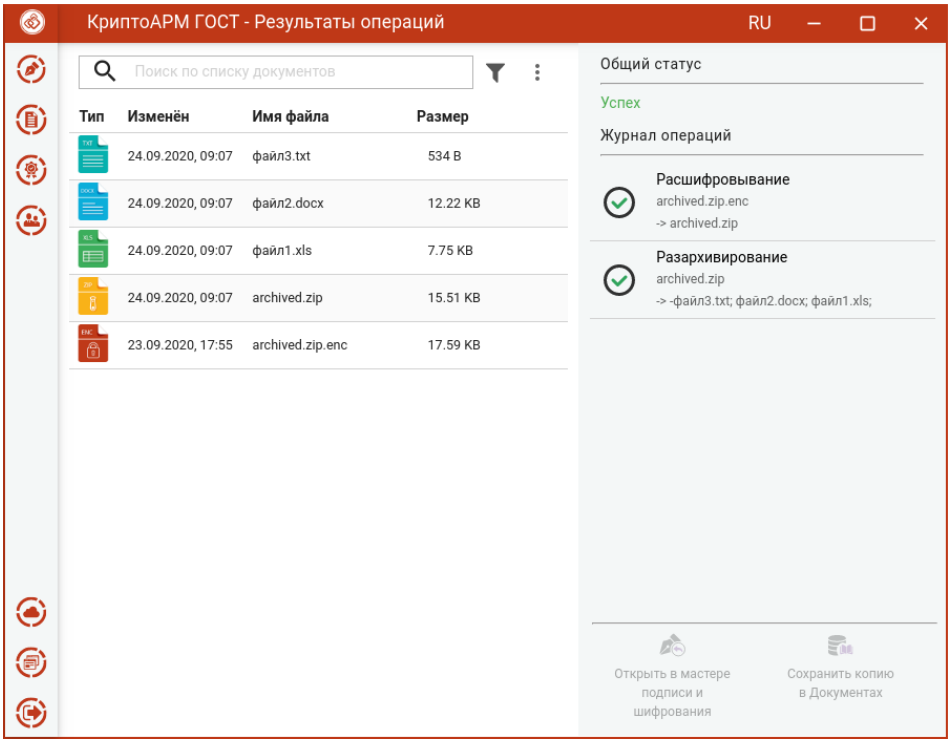
5.12.1 Расшифрование и разархивирование файлов

Для расшифрования и разархивирования достаточно выбрать зашифрованные архивы (файлы с расширением .**zip.enc)**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить**. Настройка дополнительных параметров для операции не требуется.



Расшифрование и разархивирование файлов

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций**.



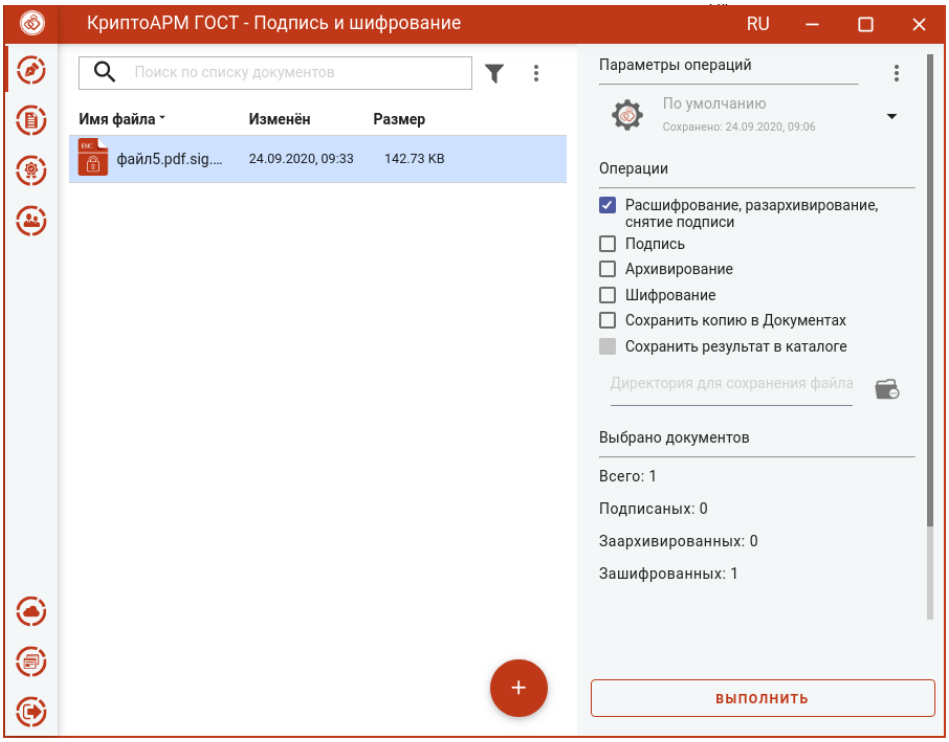
Результаты расшифрования и разархивирования файлов

Внимание! Документы, полученные в результате обратных операций (расшифрование, разархивирование, снятие подписи), сохраняются во временную папку, расположенную в папке пользователя в каталоге ./Trusted/CryptoARM GOST/TEMP, и остаются там до выполнения следующей операции. Далее временная папка очищается.

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученных после операции файлов в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Документы из данного каталога доступны в пункте меню **Документы**.

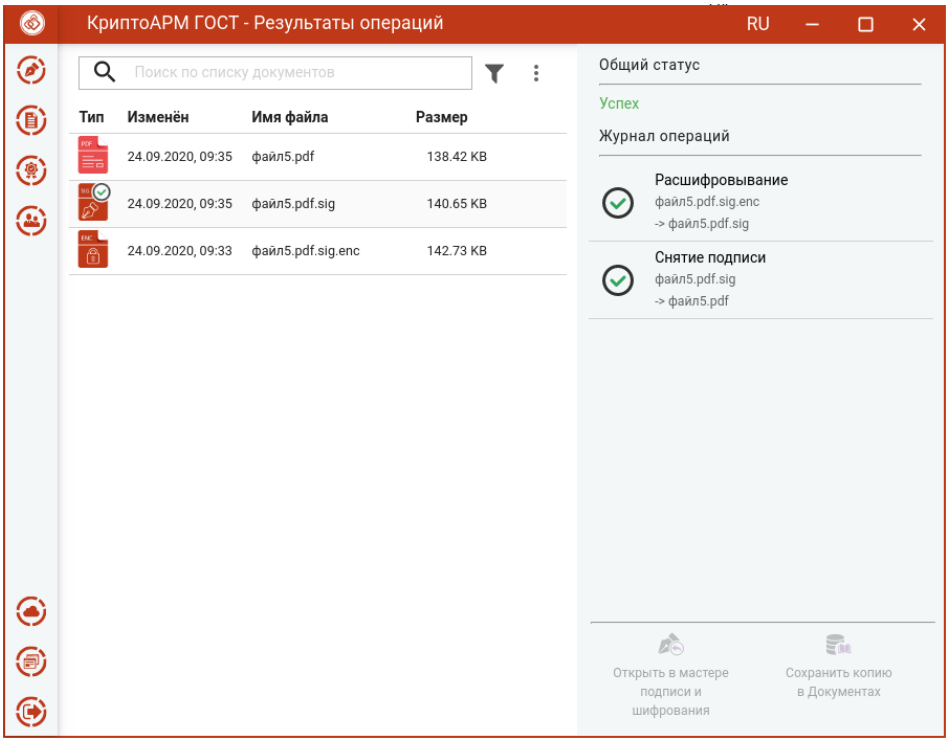
5.12.2 Расшифрование и снятие подписи с файлов

Для расшифрования и снятия подписи достаточно выбрать подписанный и зашифрованный файл (расширением **.sig.enc)**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить**. Настройка дополнительных параметров для операции не требуется.



Расшифрование и снятие подписи

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций**.



Результаты расшифрования и снятия подписи

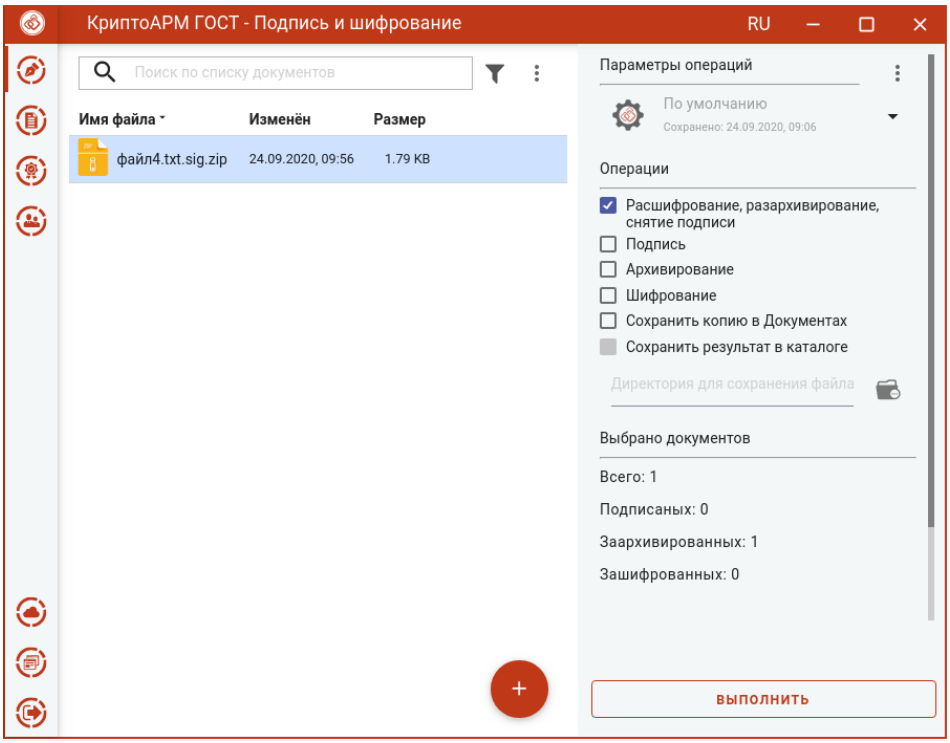
Внимание! Документы, полученные в результате обратных операций (расшифрование, разархивирование, снятие подписи), сохраняются во временную папку, расположенную в папке пользователя в каталоге ./Trusted/CryptoARM GOST/TEMP, и остаются там до выполнения следующей операции. Далее временная папка очищается.

Документы из результатов операций можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах (Ошибка! Источник ссылки не н айден.).** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

5.12.3 Разархивирование и снятие подписи

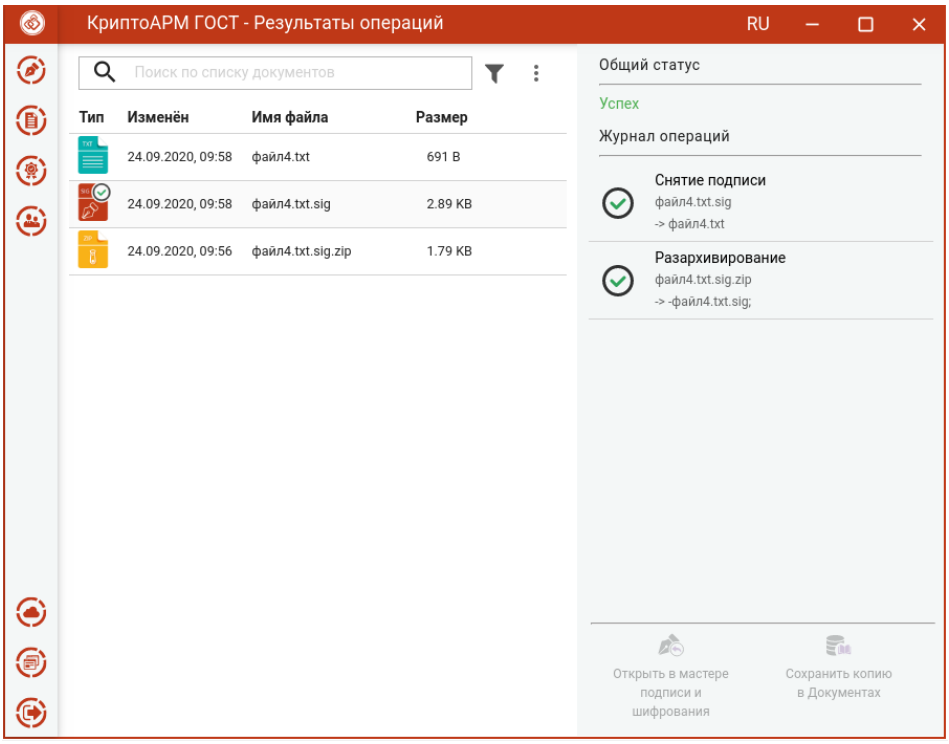
Для разархивирования и снятия подписи достаточно выбрать подписанный и заархивированный файл (с расширением **.sig.zip)**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить**. Если несколько подписанных файлов были упакованы в архив, то выбирается архивный файл с расширением **.zip**.

Настройка дополнительных параметров для операции не требуется.



Разархивирование и снятие подписи

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций**.



Результаты разархивирования и снятия подписи

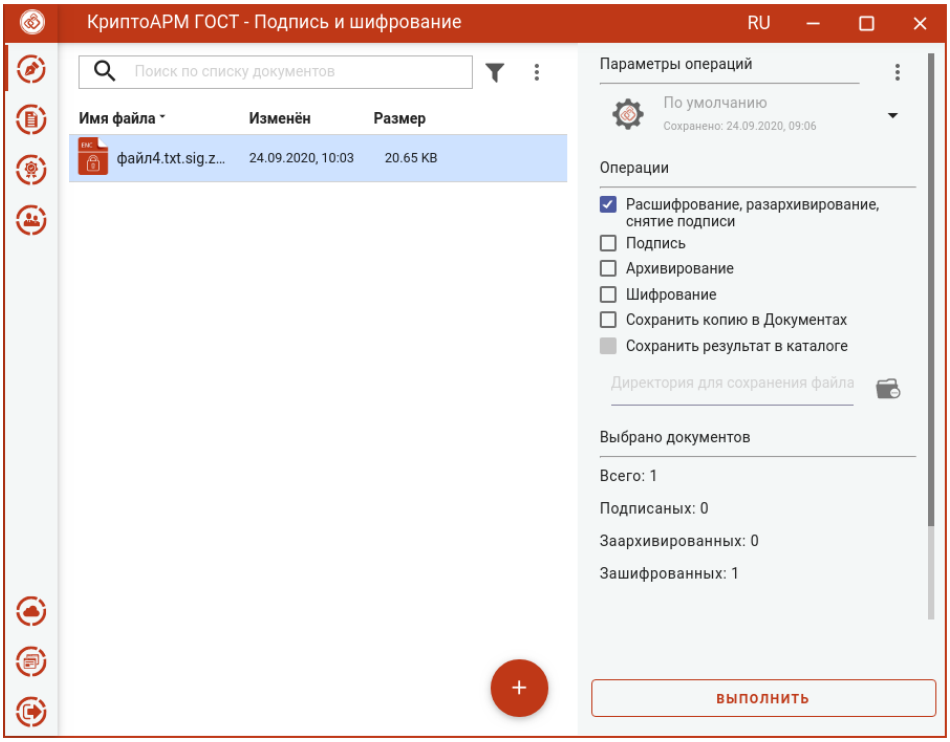
Внимание! Документы, полученные в результате обратных операций (расшифрование, разархивирование, снятие подписи), сохраняются во временную папку, расположенную в папке пользователя в каталоге ./Trusted/CryptoARM GOST/TEMP, и остаются там до выполнения следующей операции. Далее временная папка очищается.

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

5.12.4 Расшифрование, разархивирование и снятие подписи

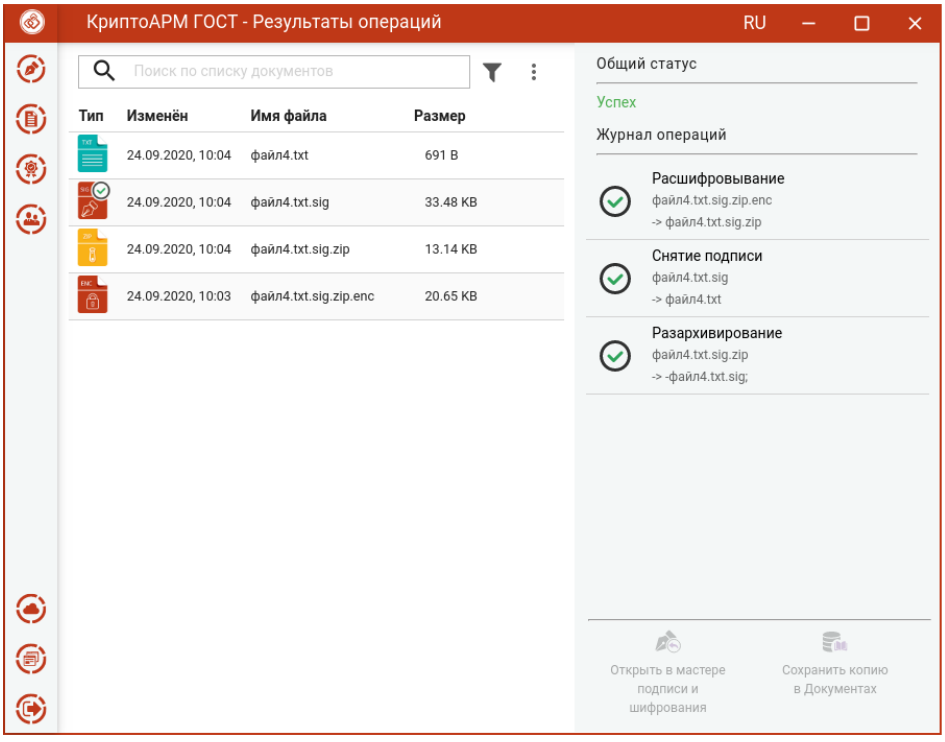
Для расшифрования, разархивирования и снятия подписи достаточно выбрать зашифрованный архив, содержащий подписанные файлы (с расширением **.sig.zip.enc)**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить**. Если несколько подписанных файлов были упакованы в архив и зашифрованы, то выбирается зашифрованный архив с расширением **.zip.enc**.

Настройка дополнительных параметров для операции не требуется.



Расшифрование, разархивирование и снятие подписи

Исходный зашифрованный и полученные файлы отображаются в отдельном мастере **Результаты операций**.



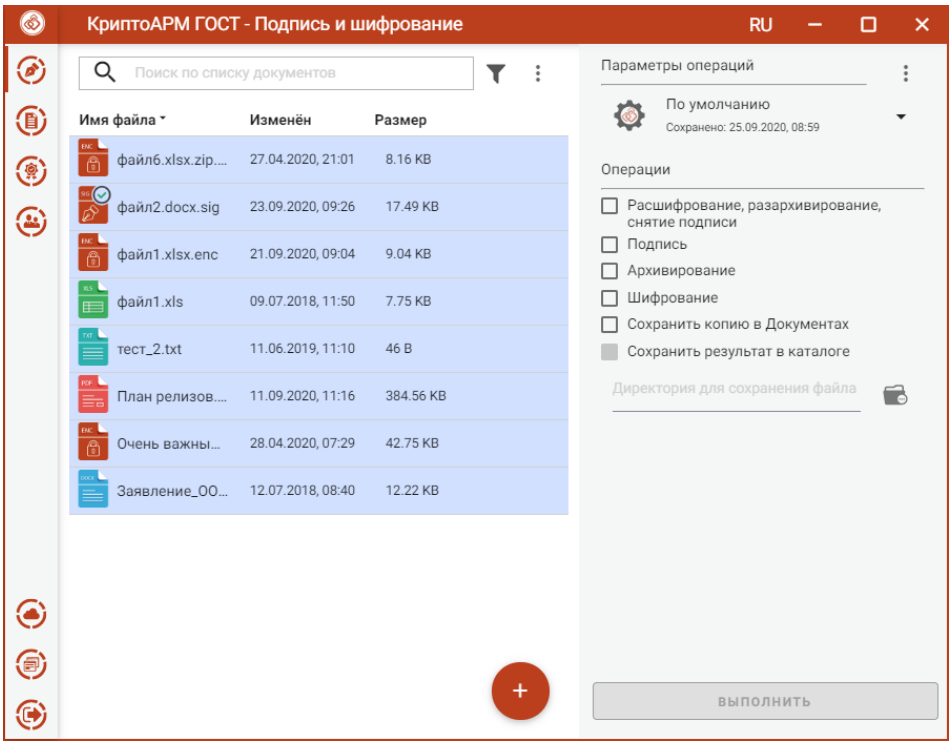
Результаты расшифрования, разархивирования и снятия подписи

Внимание! Документы, полученные в результате обратных операций (расшифрование, разархивирование, снятие подписи), сохраняются во временную папку, расположенную в папке пользователя в каталоге ./Trusted/CryptoARM GOST/TEMP, и остаются там до выполнения следующей операции. Далее временная папка очищается.

Документы из **Результатов операций** можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах.** Операция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Документы из данного каталога доступны в пункте меню **Документы**.

5.13 Управление списком файлов для выполнения операций

Список файлов для выполнения операций представляет собой одноуровневый список.



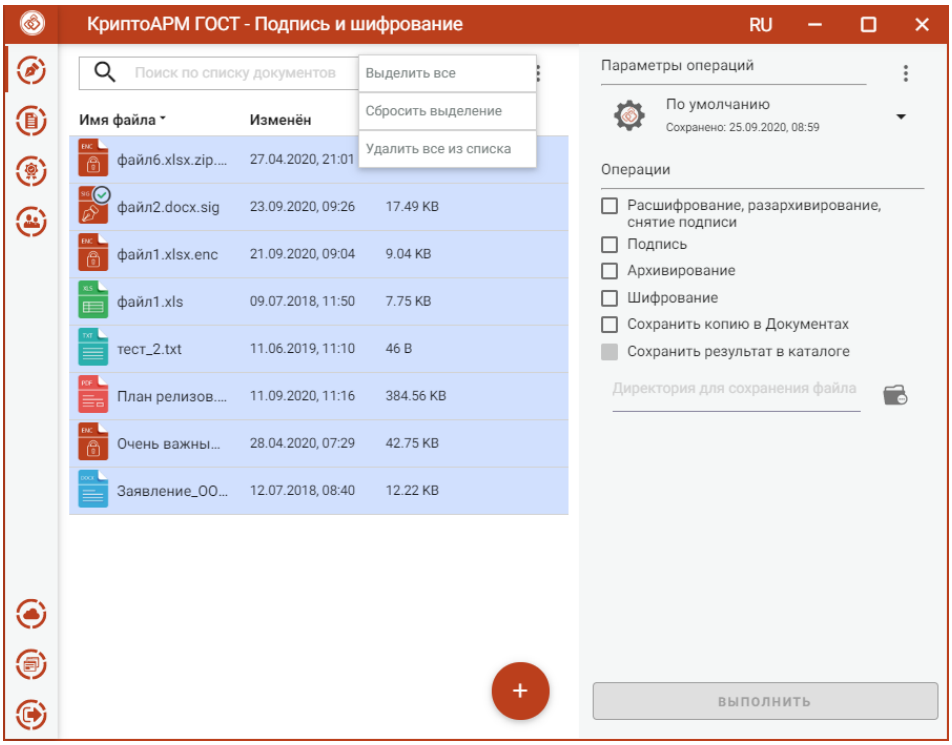
Список файлов

Файлы в список можно добавить двумя способами: через кнопку **Добавить(+)** или перетащив файлы мышкой в область формирования списка.

По умолчанию файлы в списке сортируются по дате создания - от новых к старым. Отсортировать файлы можно по любому столбцу, нажав на название столбца.

Для списка доступно контекстное меню, состоящее из пунктов:

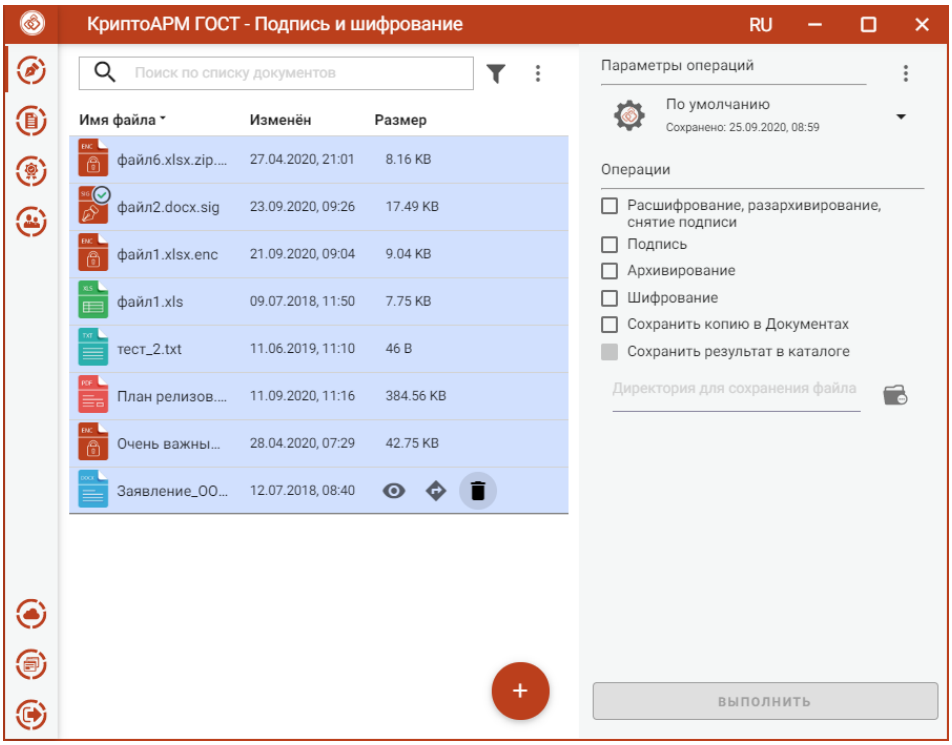
- **Выделить все** - выделяются все добавленные в список файлы;
- **Сбросить выделение** - отменяется выделение всех выбранных в списке файлов;
- **Удалить все из списка** - список очищается. При очистке списке файлы из файловой системы не удаляются.



Контекстное меню списка файлов

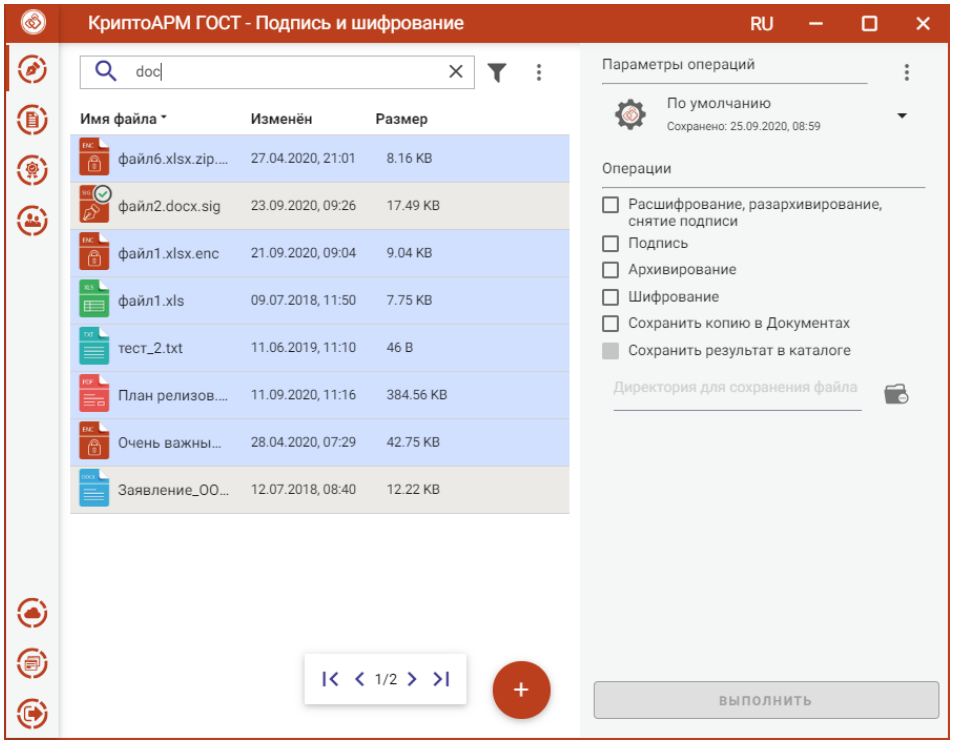
Для каждого файла доступны кнопки операции, всплывающие при наведении на файл курсором мыши:

- **Просмотр** - выполняется открытие файла через приложение, которое ассоциировано с его расширением;
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл.
- **Проверить подпись** – доступна только для подписанных файлов. Принудительно запускает процесс проверки подписи.
- **Удалить** - файл удаляется из текущего списка. При выполнении этой операции файл остается в файловой системе.



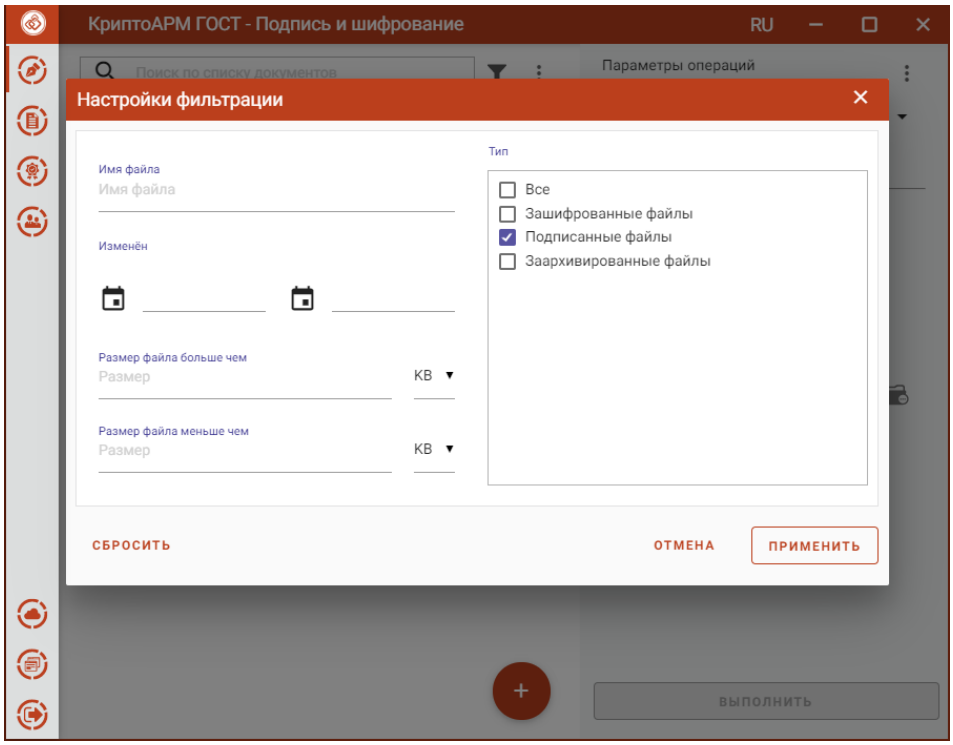
Кнопки операций файла

В приложении реализован поиск файлов по символьному совпадению.



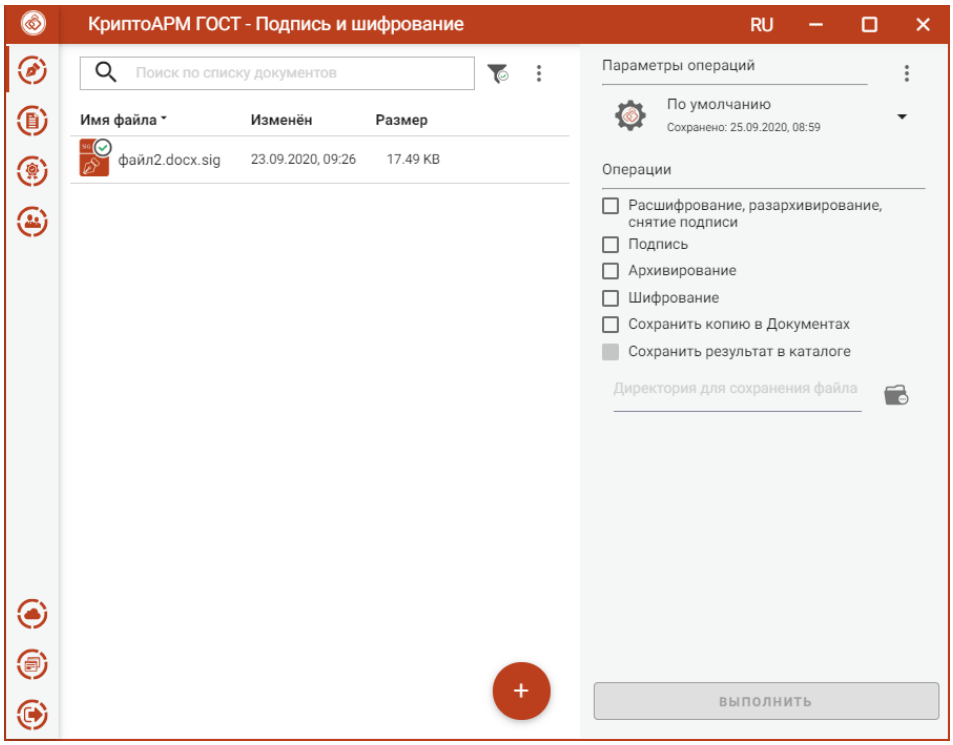
Поиск файлов

Список файлов можно отфильтровать, задав настройки фильтрации.



Настройки фильтра файлов

Применение фильтрации выполняется по нажатию кнопки **Применить**. В зависимости от выставленных критериев, в списке файлов остаются только те записи, которые удовлетворяют (суммарно) этим критериям.



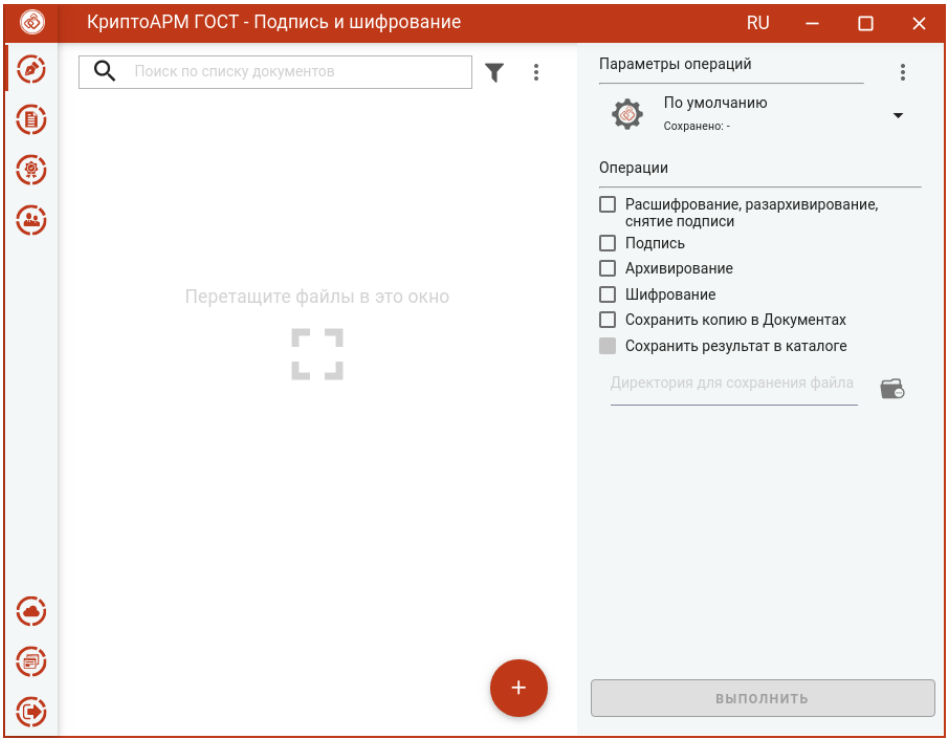
Результат применения фильтрации файлов

Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации.

5.14 Управление параметрами операции

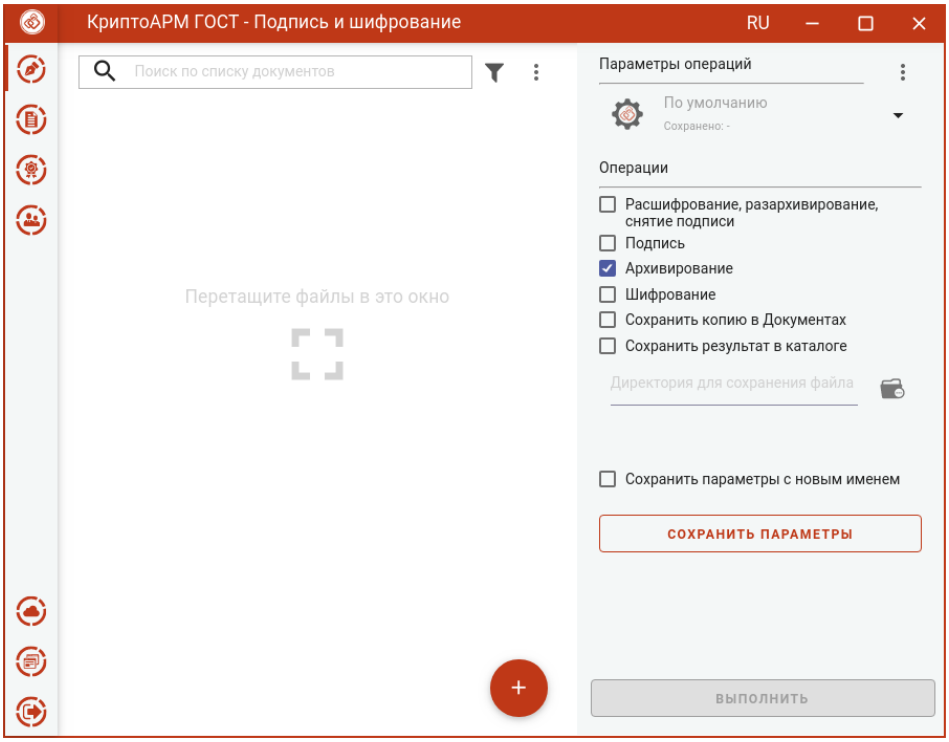
В мастере **Подписи и шифрования** выбранные операции и их параметры можно сохранить и использовать при последующих запусках приложения, не устанавливая каждый раз.

При первом запуске приложения создаются параметры **По умолчанию** с пустыми опциями операций и параметров операций.



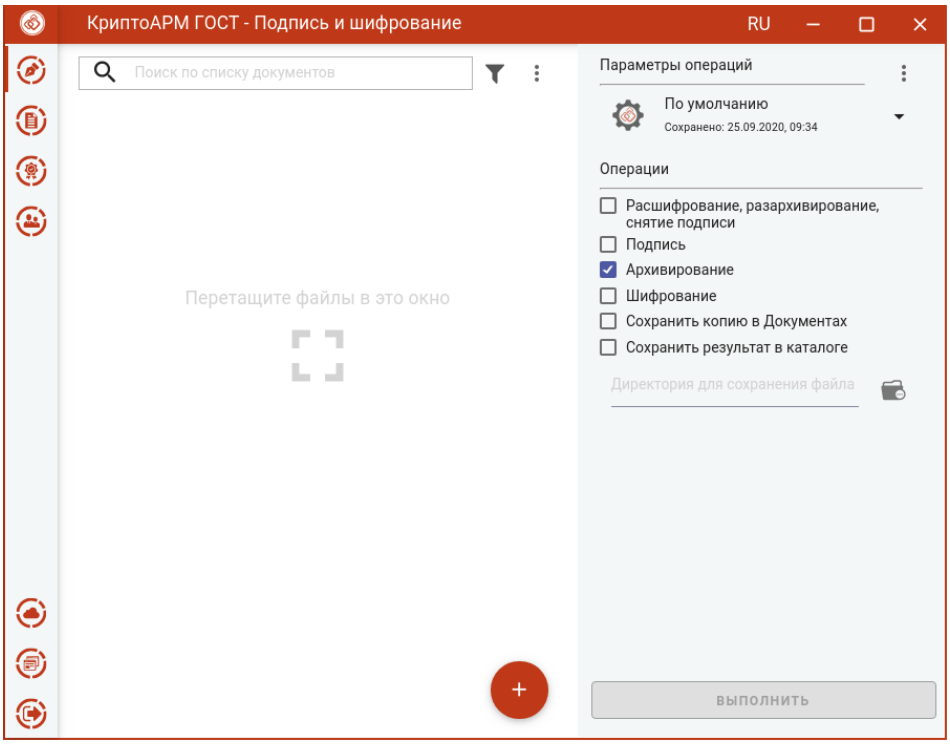
Параметры операций по умолчанию

При любом изменении опции операций или параметров операции становится доступна кнопка сохранения изменений **Сохранить параметры**.



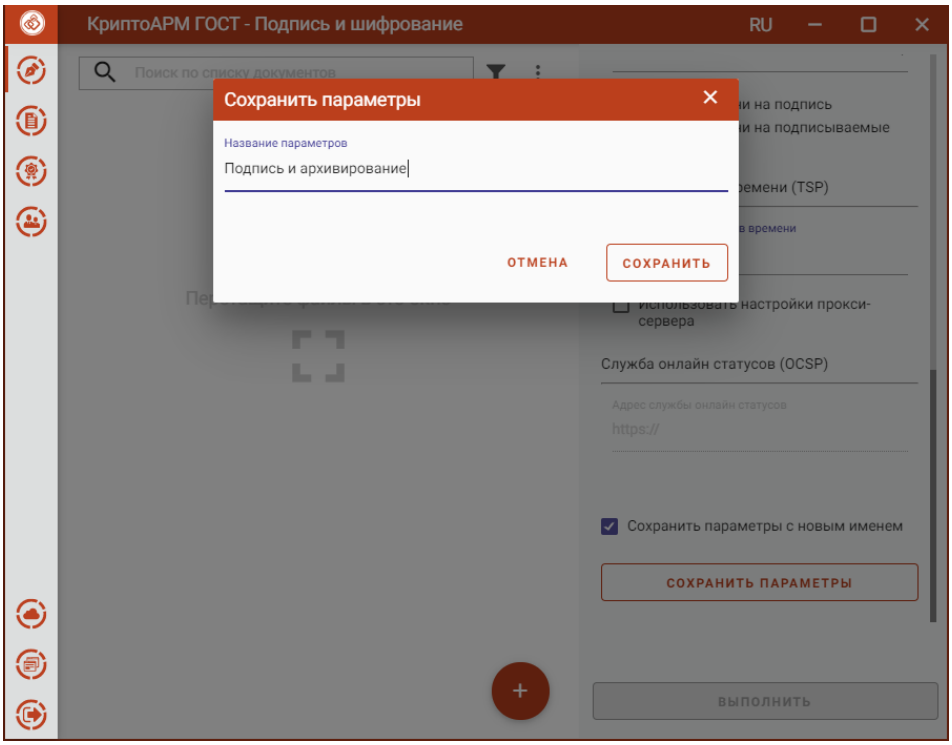
Кнопка сохранения изменений параметров операций

При нажатии на кнопку происходит сохранение выбранных параметров в текущие параметры операций. Кнопка **Сохранить параметры** скрывается до изменений.



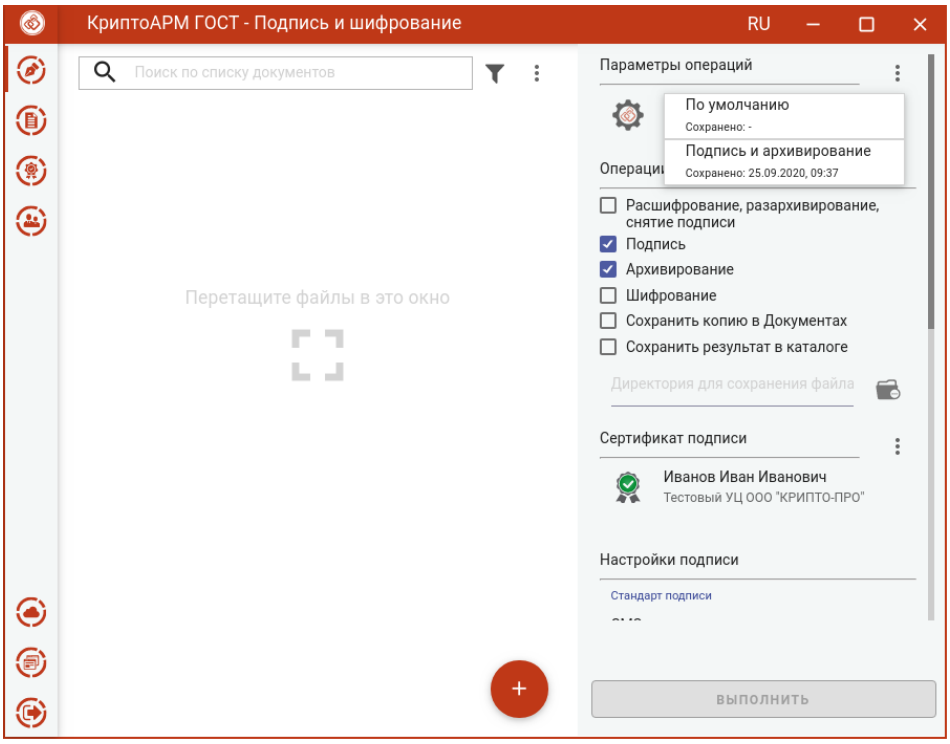
Сохранение изменений в текущие параметры операций

Если выбрать опцию **Сохранить параметры с новым именем** и нажать кнопку **Сохранить параметры**, то открывается окно ввода названия параметров операций.



Задание названия параметров операций

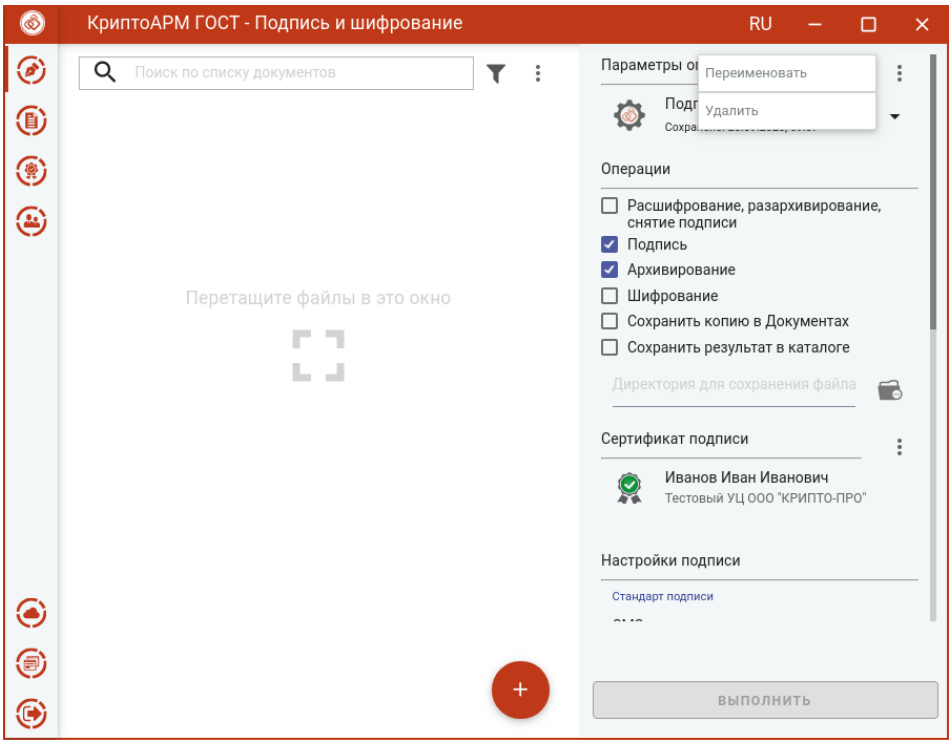
По кнопке **Сохранить** происходит сохранение выбранных параметров с заданным именем. Выбрать параметры операций можно в выпадающем списке из ранее сохраненных параметров.



Выбор параметров операций

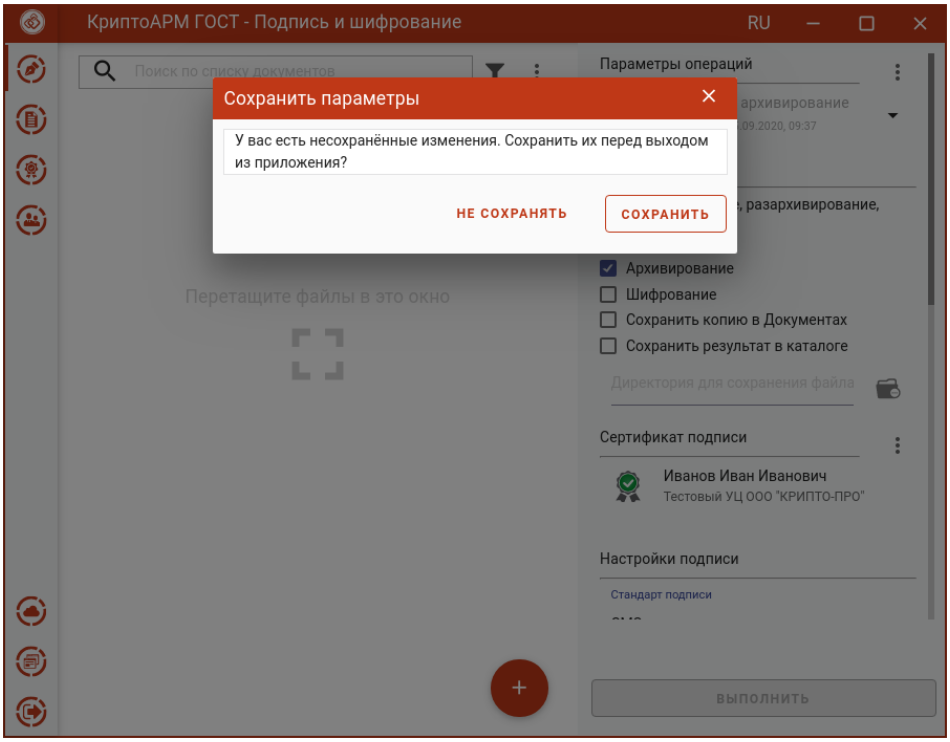
Можно настроить несколько параметров операций и выбирать нужные из списка.

Параметры операций можно переименовать или удалить через контекстное меню.



Контекстное меню параметров операций

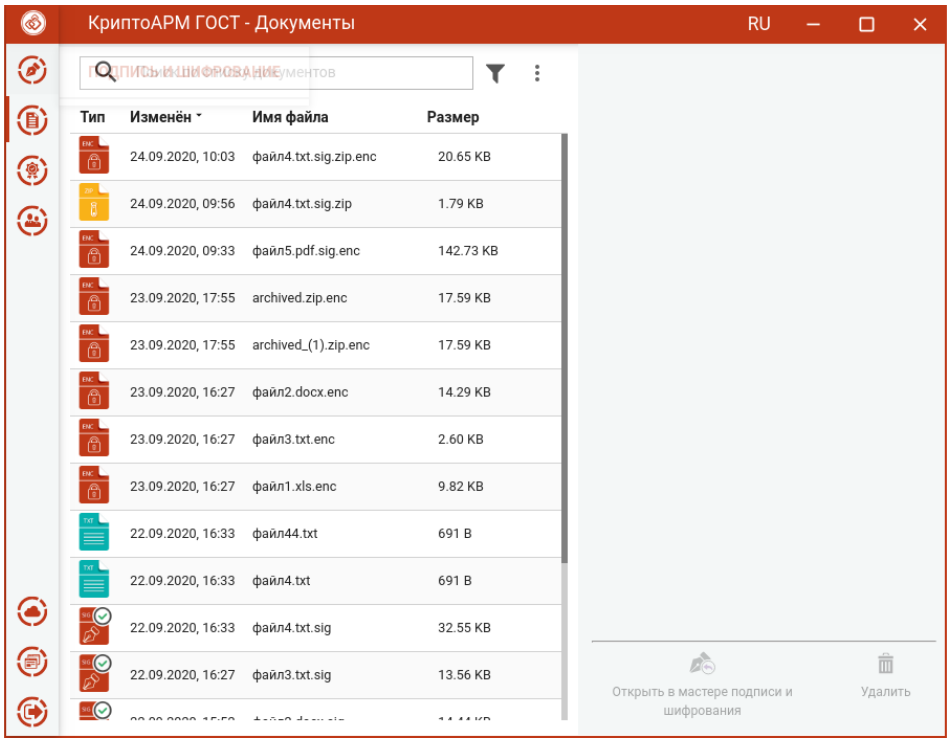
Если в **Параметрах операций** были сделаны изменения и не сохранены, то выбор других параметров выпадающего списка заблокирован. При закрытии приложения появляется окно с предложением сохранить сделанные изменения, сбросить изменения или закрыть без сохранения.



Предложение сохранить изменения в параметрах

5.15 Документы

Для сохранения копии результатов выполнения операций подписи, снятия подписи, архивирования, шифрования и расшифрования используется каталог **Документы**. Файлы данного каталога располагаются в каталоге пользователя в папке \.Trusted\CryptoARM GOST\Documents\. Просмотреть документы в каталоге можно, выбрав пункт меню **Документы**.

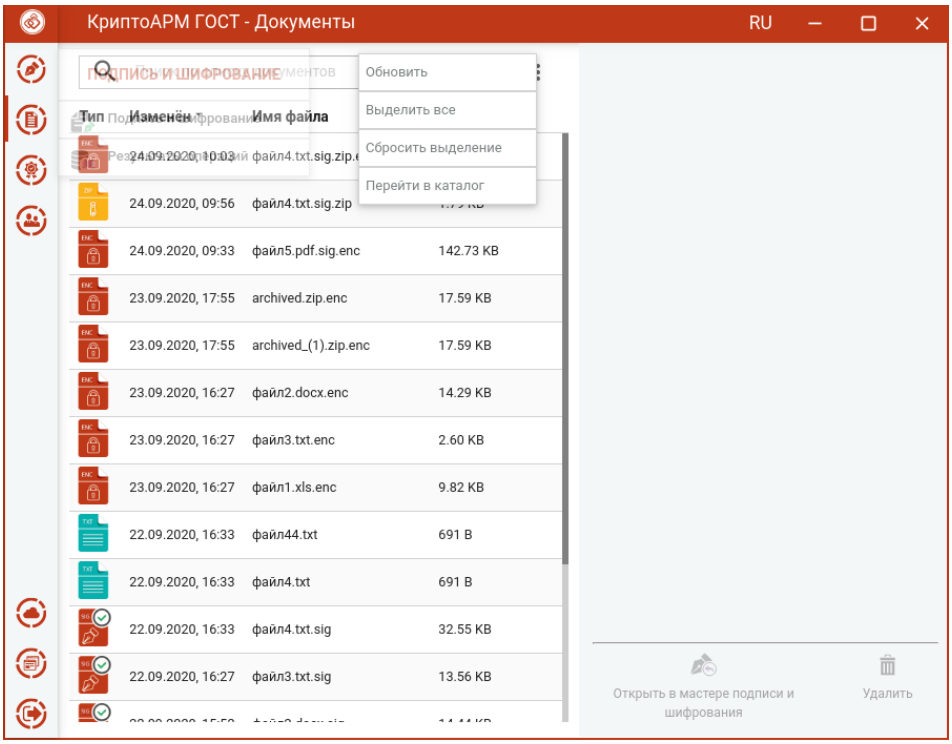


Список документов

По умолчанию файлы в списке сортируются по дате создания - от новых к старым. Отсортировать файлы можно по любому столбцу, нажав на название столбца.

Для списка доступно контекстное меню, состоящее из пунктов:

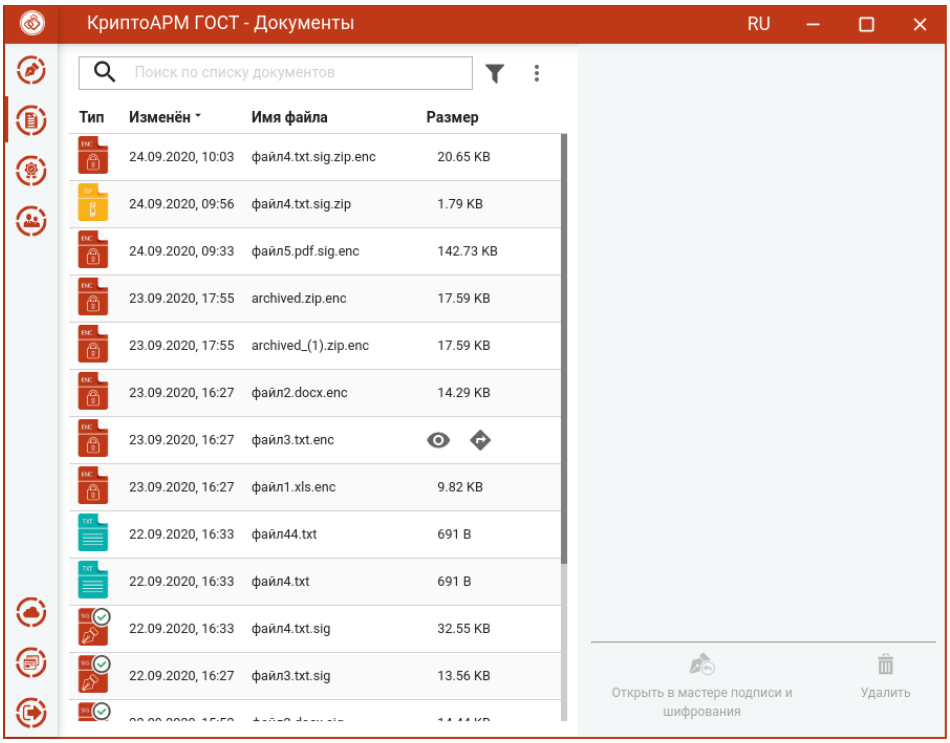
- **Обновить** – для обновления списка;
- **Выделить все** - выделяются все файлы в списке;
- **Сбросить выделение** – для сброса выделения документов в списке;
- **Перейти в каталог** - выполняется открытие каталога документов.



Контекстное меню списка Документов

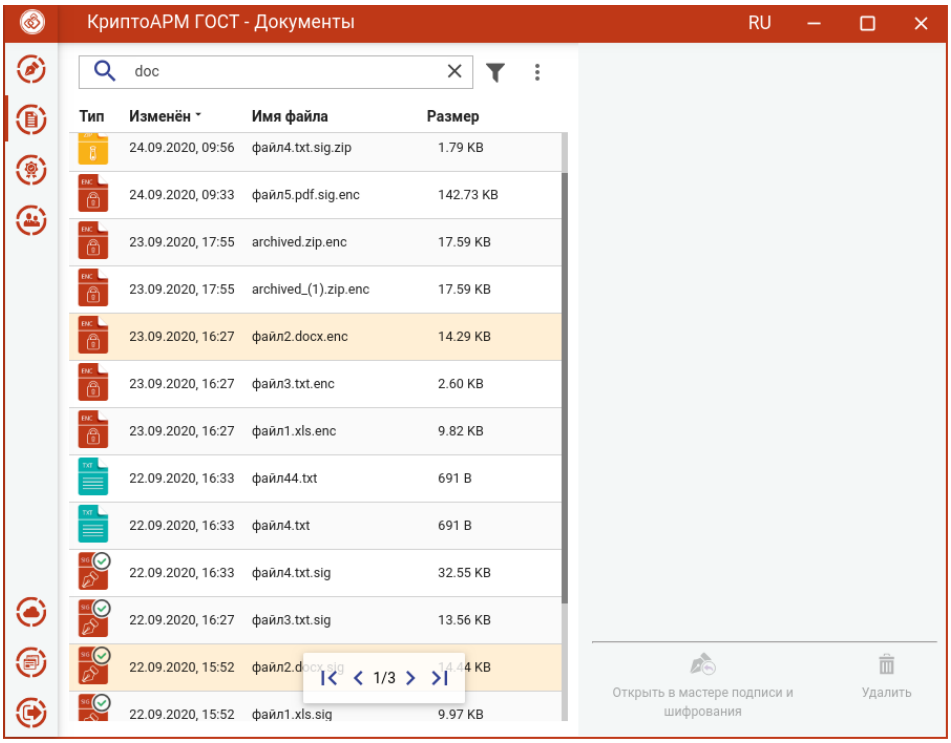
Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши:

- **Просмотр** - выполняется открытие файла через приложение, которое ассоциировано с его расширением;
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл.



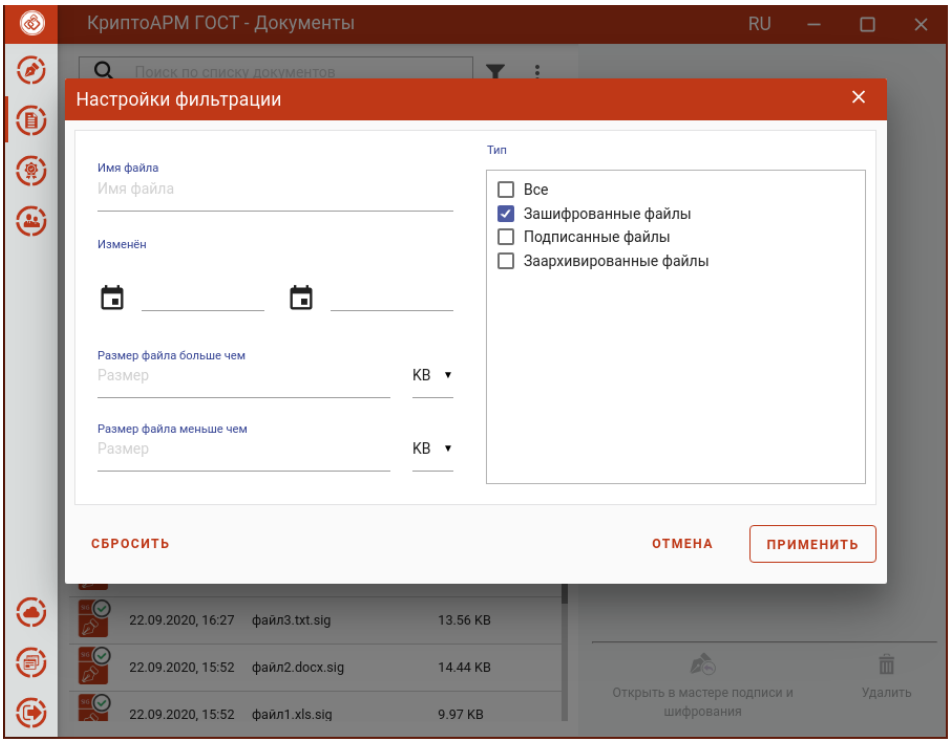
Кнопки операций документа

В приложении реализован поиск документов по символьному совпадению.



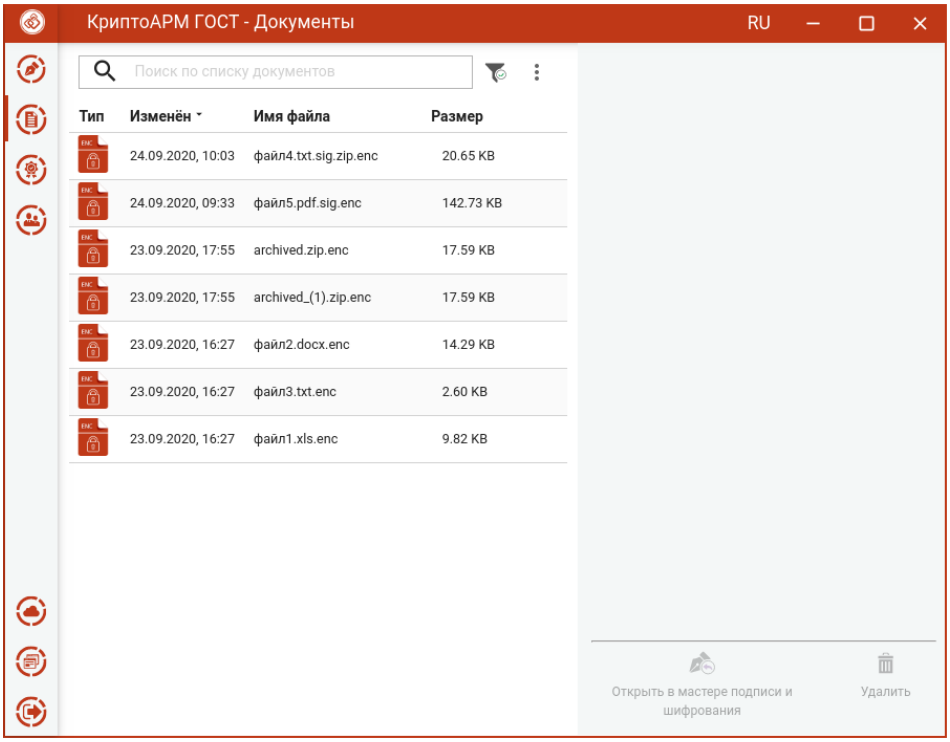
Поиск документов

Список документов можно отфильтровать, задав настройки фильтрации.



Настройки критериев фильтра документов

Применение фильтрации выполняется по нажатию кнопки **Применить**. В зависимости от выставленных критериев фильтра в списке документов остаются только те записи, которые удовлетворяют (суммарно) этим критериям.

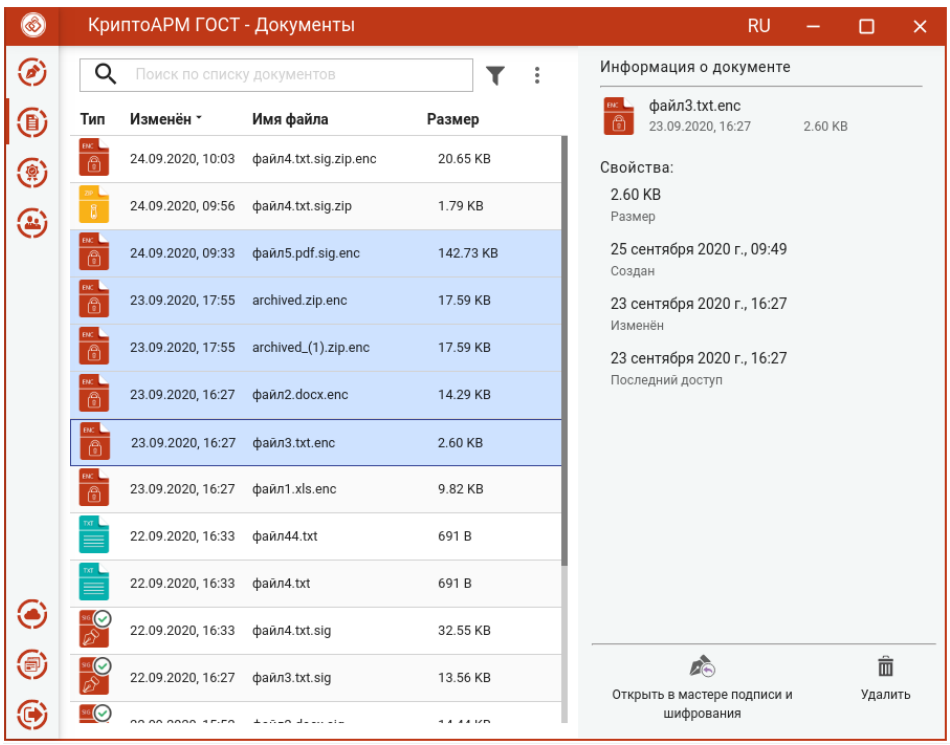


Результат применения фильтрации документов

Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации.

Для списка файлов в разделе **Документы** доступны операции:

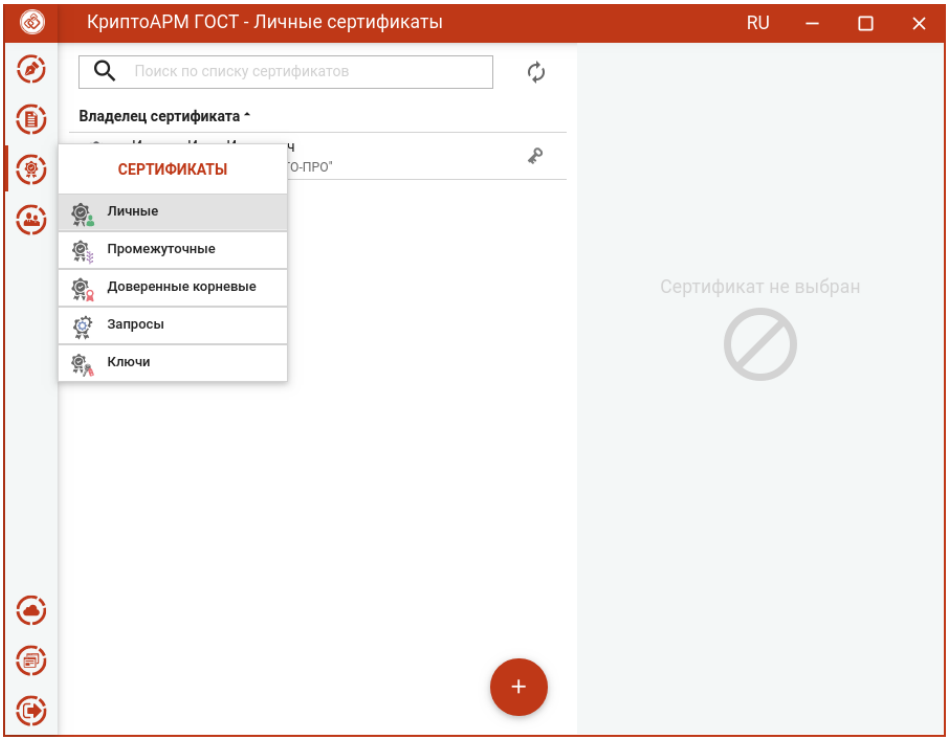
- **Открыть в мастере подписи и шифрования** – выбранные документы открываются в мастере **Подписи и шифрования** для выполнения других операций
- **Удалить** – происходит физическое удаление файлов из каталога в папке пользователя \.Trusted\CryptoARM GOST\Documents\.



Доступные операции для документов

5.16 Сертификаты

Для управления сертификатами в приложении добавлен отдельный пункт меню **Сертификаты**. При выборе данного пункта открывается раздел со список личных сертификатов и подменю с категориям сертификатов.

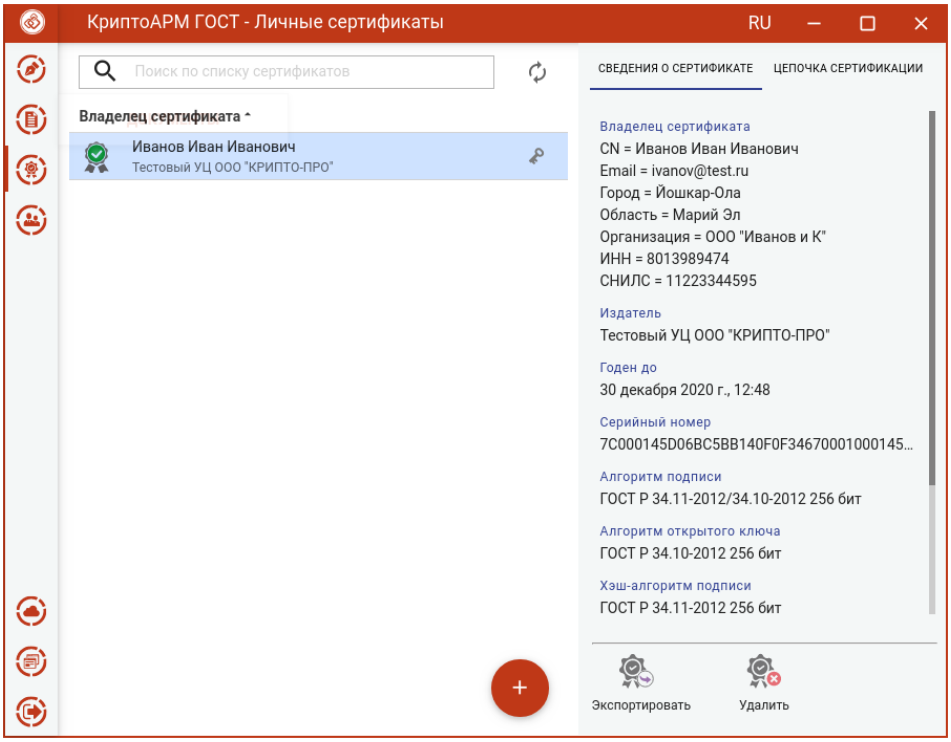


Список личных сертификатов с подменю

Подменю содержит пункты:

- **Личные** – для управления сертификатами, у которых есть привязка к закрытому ключу;
- **Промежуточные** - для управления промежуточными сертификатами;
- **Корневые доверенные** - для управления доверенными корневыми сертификатами;
- **Запросы** – для управлениями запросами на сертификат;
- **Списки отзыва** – для управления списками отзыва сертификатов;
- **Ключи** – для отображения ключевых контейнеров.

В левой области представления отображается список сертификатов выбранного раздела, в правой области отображается информация о выделенном сертификате.



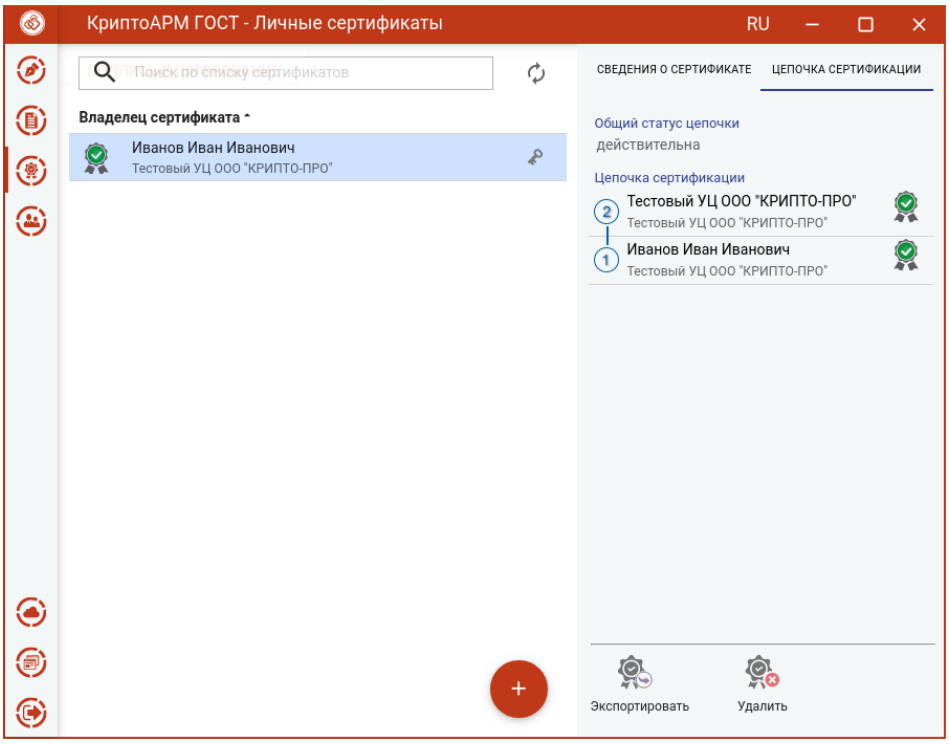
Отображение сведений о выбранном сертификате

При отображении сертификатов, они проверяются на корректность (математическая корректность и построение цепочки доверия).

Если к сертификату привязан закрытый ключ, то отображается знак ключа. Облачные сертификаты выделены знаком облака.

Возможно появление одного из двух статусов проверки сертификата: корректный и некорректный.

На вкладке **Цепочка сертификации** отображается общий статус цепочки и «дерево» сертификатов.



Представление цепочки сертификатов

5.16.1 Импорт сертификата из файла

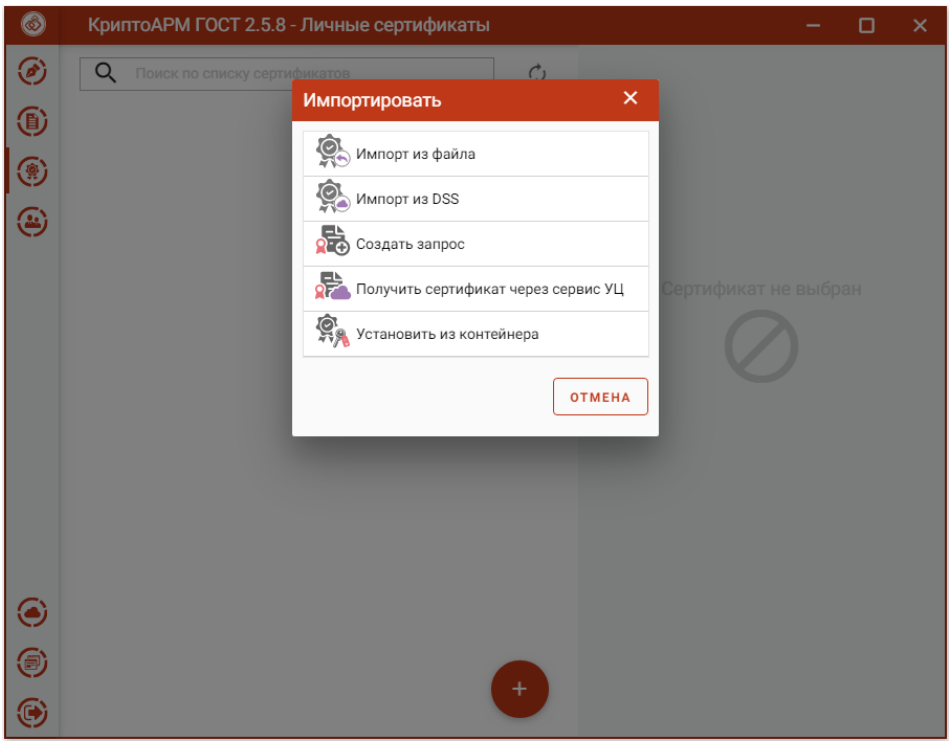
В приложении допускается импорт двух типов сертификатов:

- **с привязкой к закрытому ключу** – pfx контейнер, содержащий сертификат и закрытый ключ. Или сертификат, который будет привязан к имеющемуся закрытому ключу в хранилище. Такие сертификаты устанавливаются в **Личное хранилище сертификатов** и их можно использовать для подписи и расшифрования .
- **без привязки к закрытому ключу** – обычный сертификат, который устанавливается в хранилище промежуточных или корневых сертификатов для построения цепочки. Или в хранилище сертификатов других пользователей (**Контакты**) для шифрования в адрес этого сертификата.

5.16.1.1 Импорт личного сертификата с привязкой к закрытому ключу

Импорт сертификата выполняется кнопкой **Добавить (+)** в соответствующем разделе.

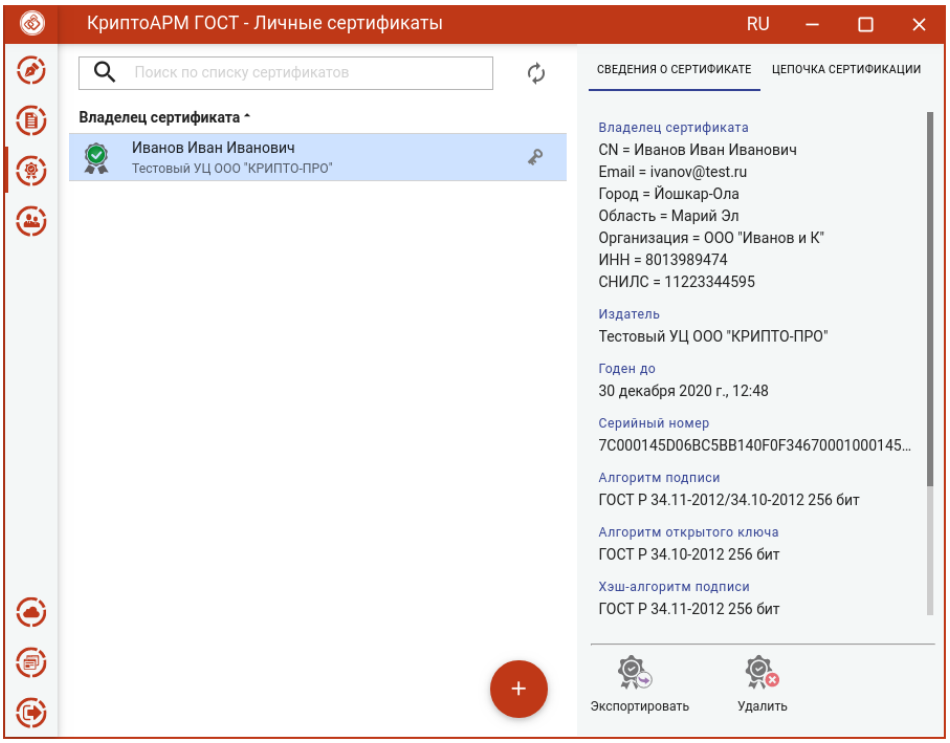
В открывшемся окне нужно выбрать операцию **Импорт из файла**.



Меню выбора способа добавления сертификатов

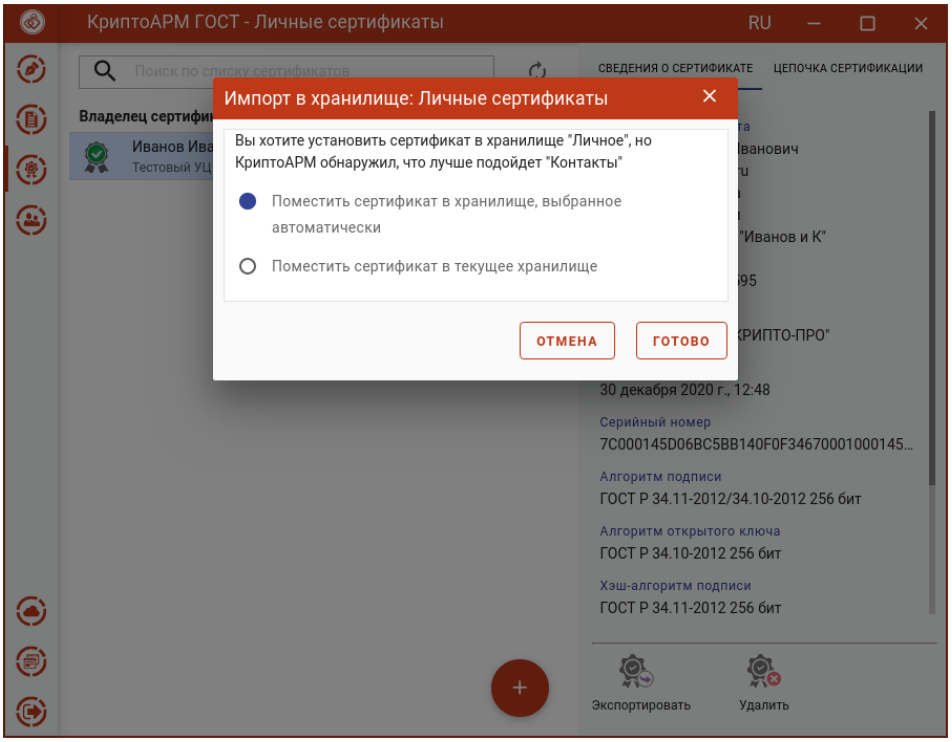
В открывшемся файловом менеджере нужно выбрать файл сертификата. Это может быть файл формата pfx, содержащий ключевую пару (закрытый ключ и сертификат), или обычный сертификат, у которого есть закрытый ключ в хранилище.

При успешном выполнении операции импорта сертификат автоматически помещается в личные сертификаты.



Отображение импортированного личного сертификата

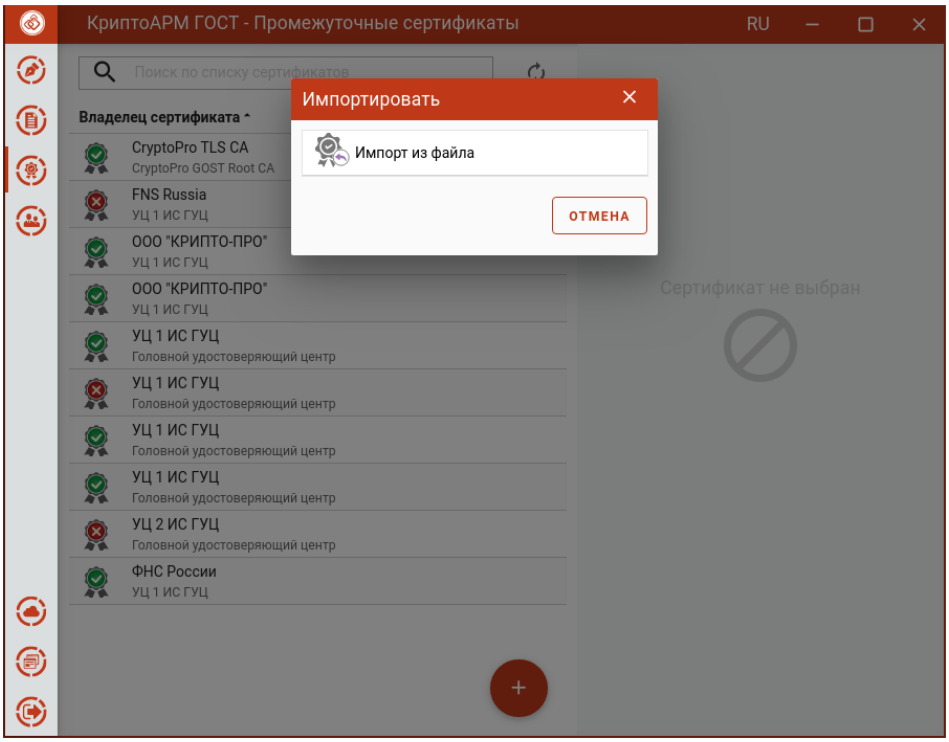
Если при импорте не будет найден закрытый ключ, соответствующий сертификату, то возникнет сообщение с предложением установить данный сертификат в подходящее хранилище, или принудительно - в выбранное. Если сертификат без закрытого ключа будет установлен в личное хранилище, то данным сертификатом нельзя будет подписывать и расшифровывать файлы.



Выбор хранилища для установки сертификата

5.16.1.2 Импорт сертификата без привязки к закрытому ключу

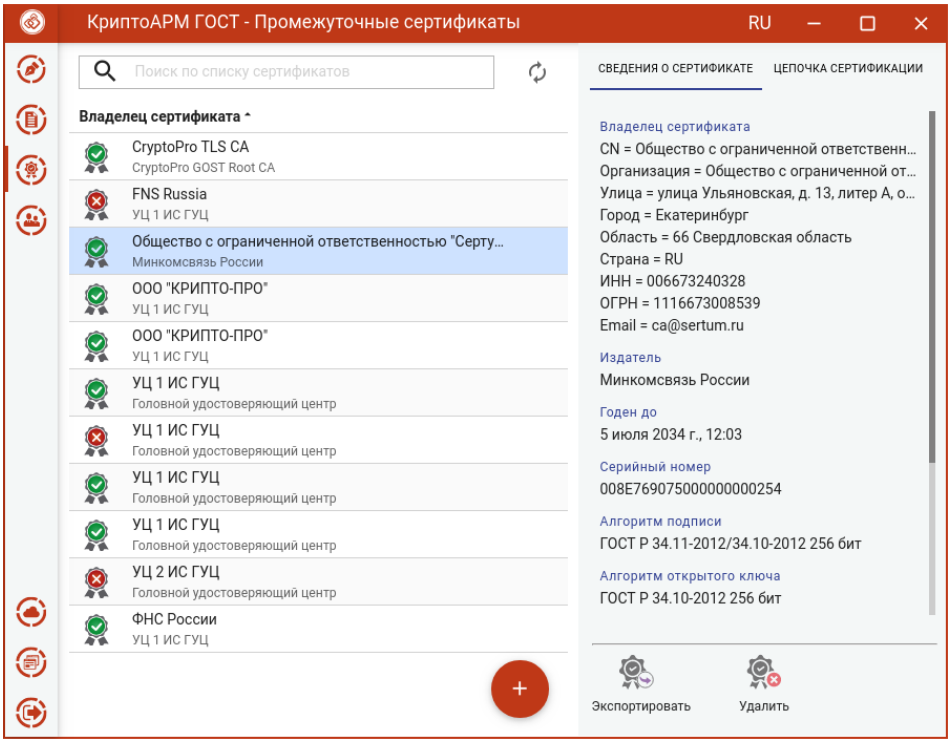
Импорт сертификата в хранилище выполняется кнопкой добавления сертификата (**+**) и выбора опции **Импорт из файла**.



Импорт сертификата из файла

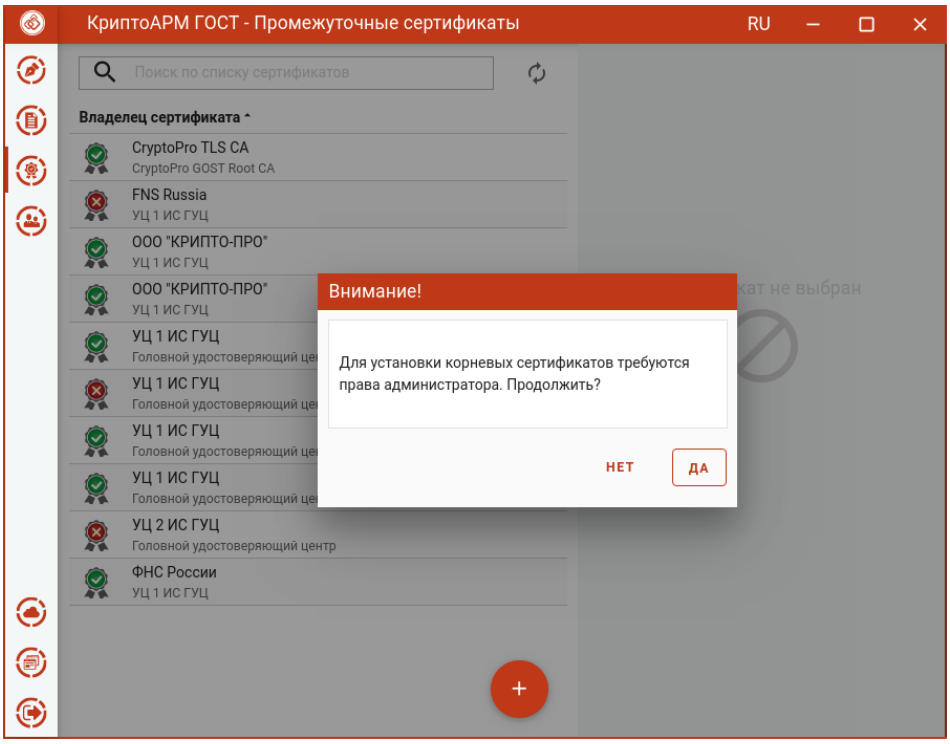
В открывшемся файловом менеджере нужно выбрать файл сертификата.

При успешном выполнении операции импорта, сертификат автоматически помещается в выбранное хранилище.



Отображение импортированного сертификата

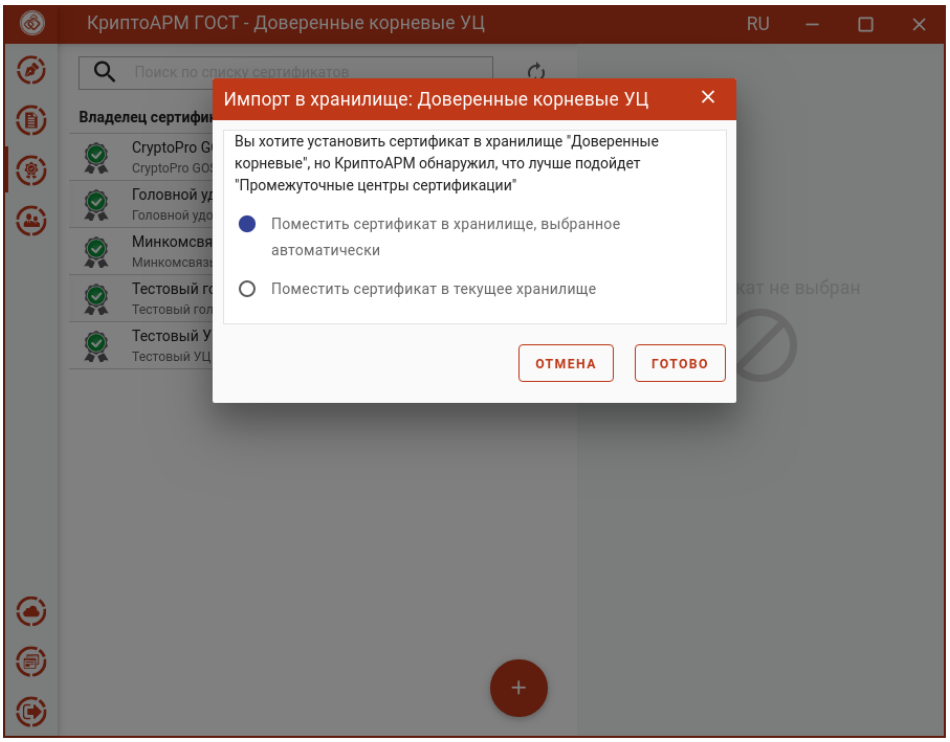
При импорте промежуточных и корневых сертификатов нужны права администратора.



Запрос на разрешение действий от администратора

При нажатии на **Да** будет запрошен пароль администратора. Если выбрано **Нет**, сертификат не импортируется.

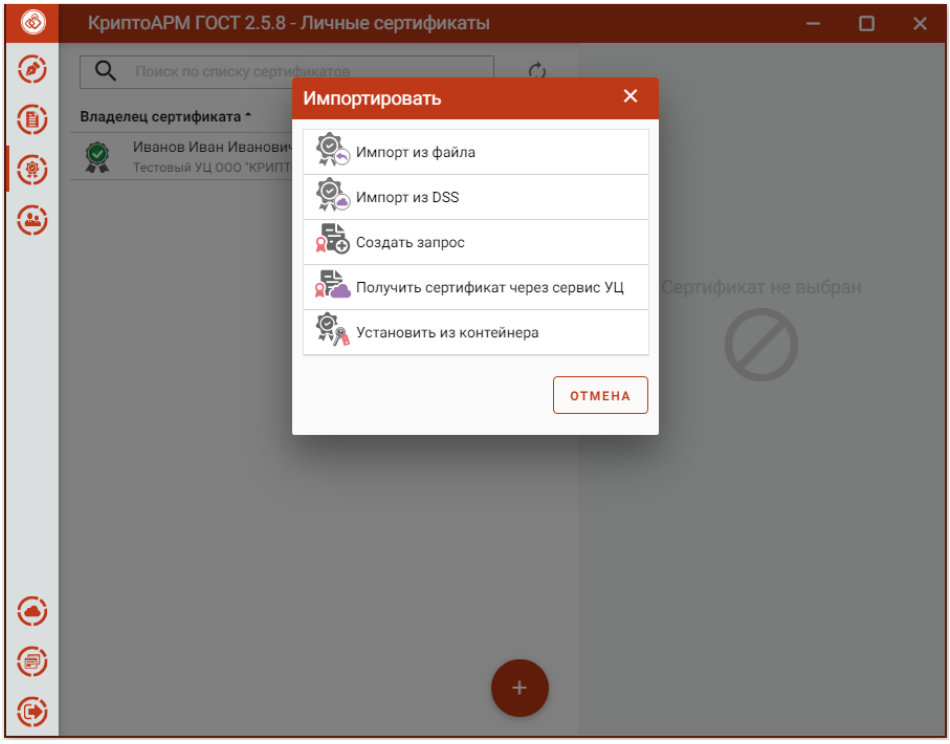
Если при импорте приложение определило, что для данного сертификата лучше подойдет другое хранилище, то возникнет сообщение с предложением установить сертификат в подходящее хранилище или принудительно - в выбранное.



Выбор хранилища для установки сертификата

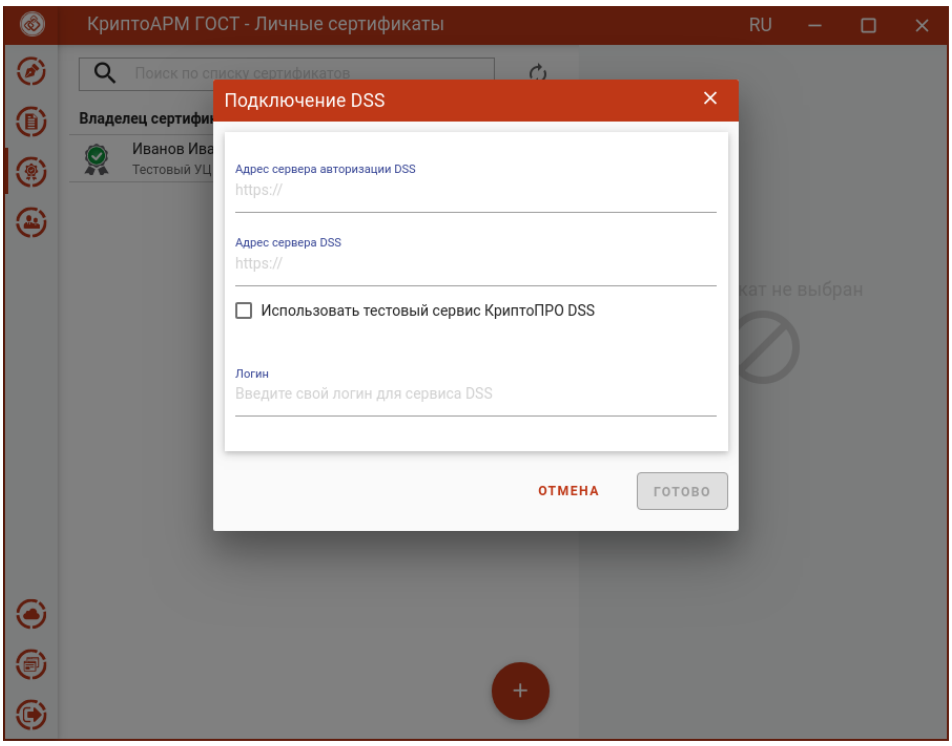
5.16.2 Импорт сертификата из DSS

Для выполнения импорта сертификата из DSS в хранилище можно воспользоваться кнопкой **Добавить (+)**. В открывшемся окне нужно выбрать операцию **Импорт из DSS**. Данная опция при импорте доступна только для категории личных сертификатов.



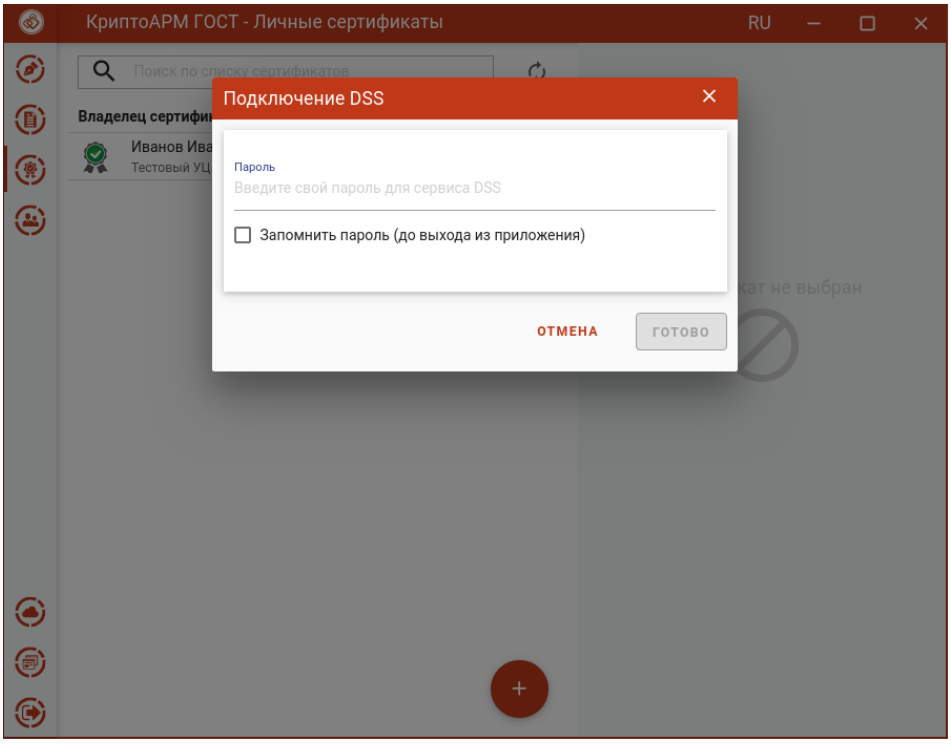
Выбор способы импорта сертификата из DSS

Открывается окно для ввода адресов серверов авторизации и логина для DSS.



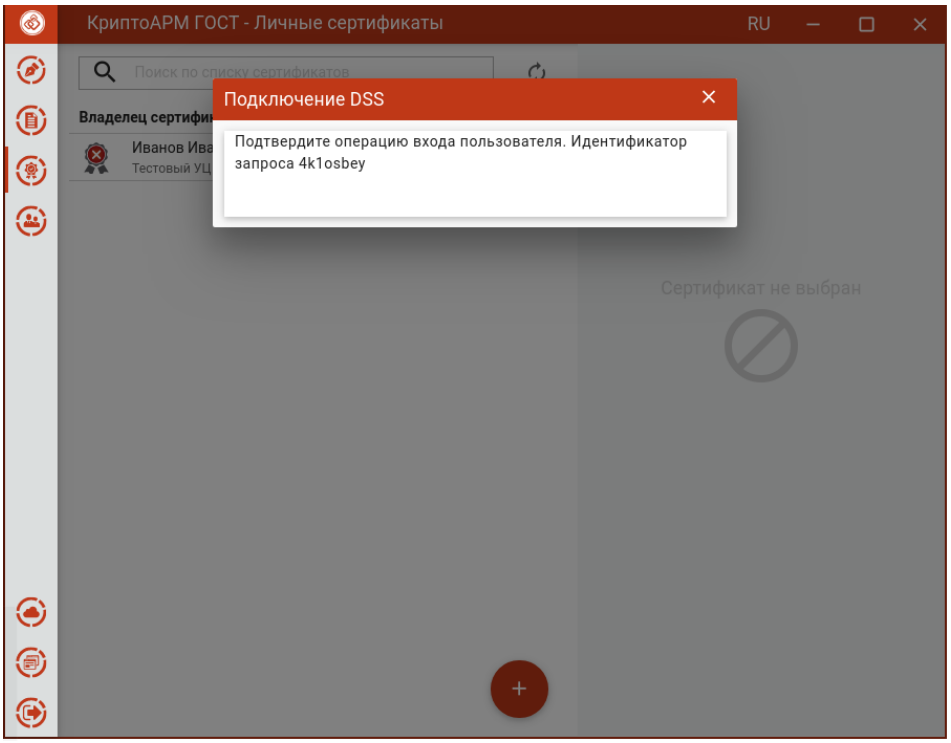
Настройка адресов серверов DSS

Если у пользователя в личном кабинете DSS в настройках стоит подтверждение по паролю, то на следующем шаге нужно ввести пароль для подключения к сервису DSS. Если пароль не задан, то данный шаг пропускается.



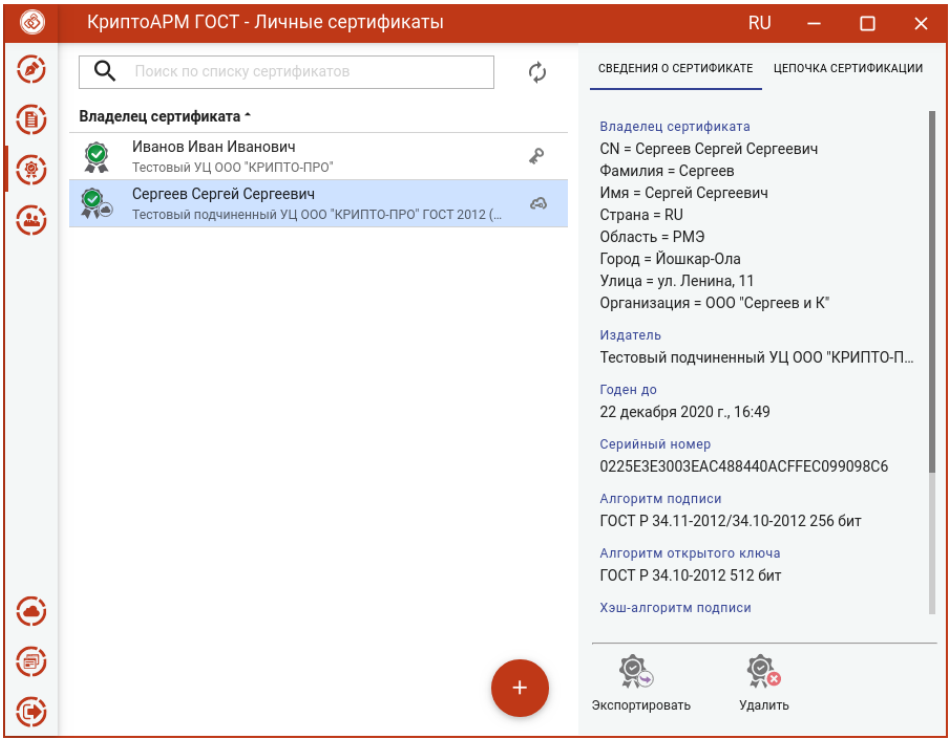
Ввод пароля для подключения к сервису DSS

Если у пользователя в личном кабинете DSS в настройках стоит подтверждение аутентификации по сим катре или с помощью мобильного приложения, то при нажатии на кнопку **Готово** появляется сообщение, что операцию нужно подтвердить. Если нет, то данный шаг пропускается.



Окно запроса подтверждения входа

При успешной аутентификации на следующем шаге сертификаты DSS автоматически помещаются в хранилище **Личных сертификатов**.

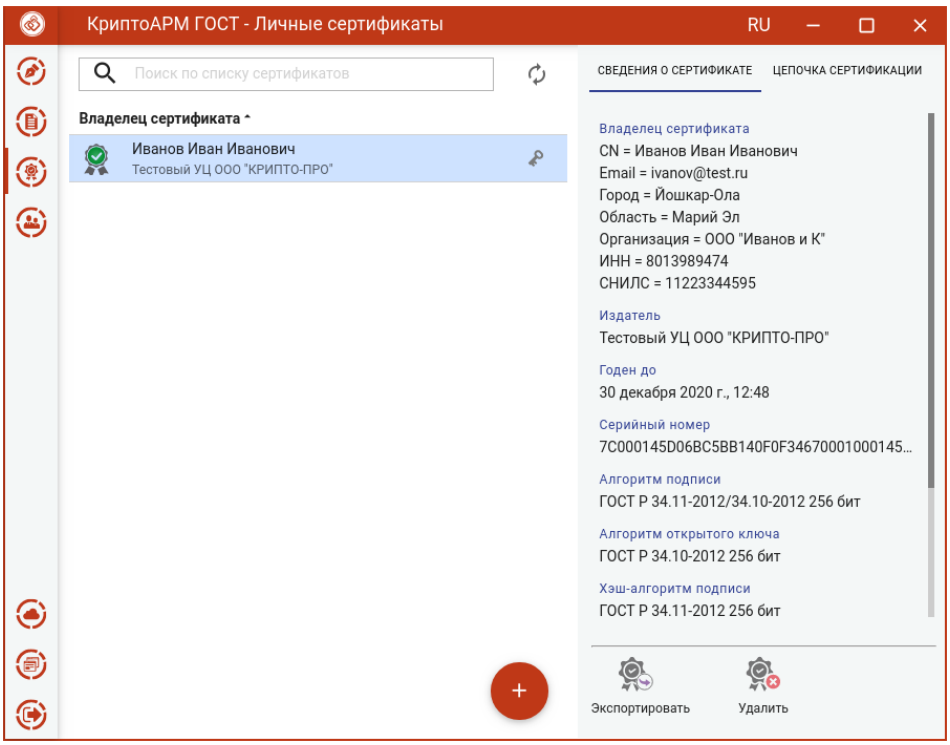


Отображение импортированного DSS сертификата

Сертификаты DSS отличаются от сертификатов, хранящихся локально, индикатором «облако».

5.16.3 Экспорт сертификата в файл

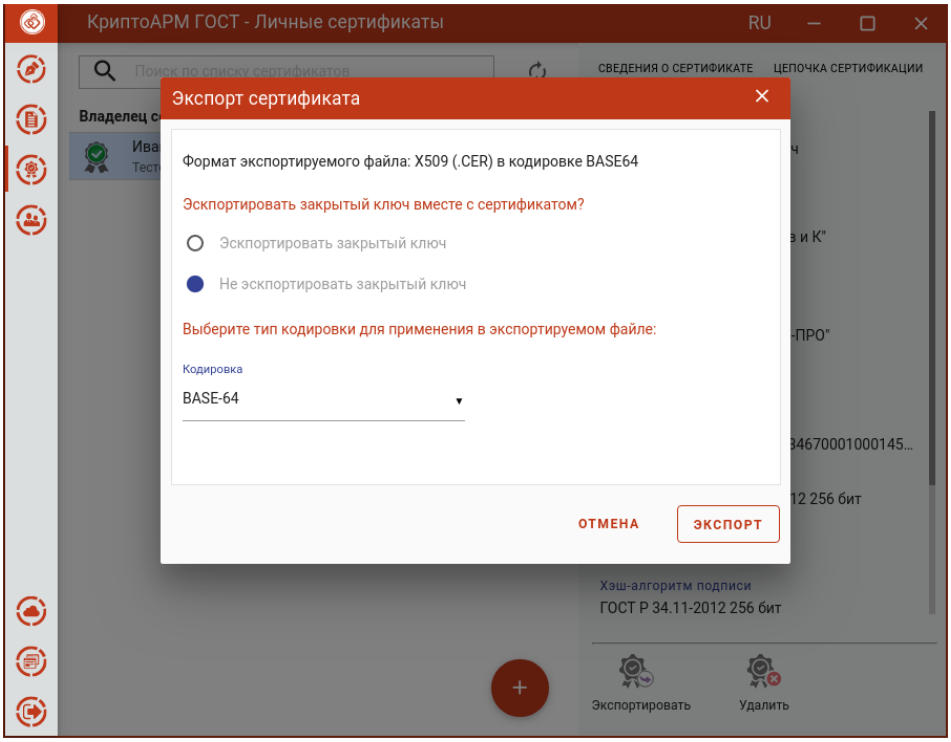
Для экспорта сертификата в файл нужно выделить сертификат и нажать кнопку **Экспортировать**.



Экспорт сертификата

Если у сертификата экспортируемый закрытый ключ, то такой сертификат можно экспортировать вместе с ним.

При экспорте сертификата с не экспортируемым закрытым ключом появляется окно, в котором можно выбрать только кодировку файла.

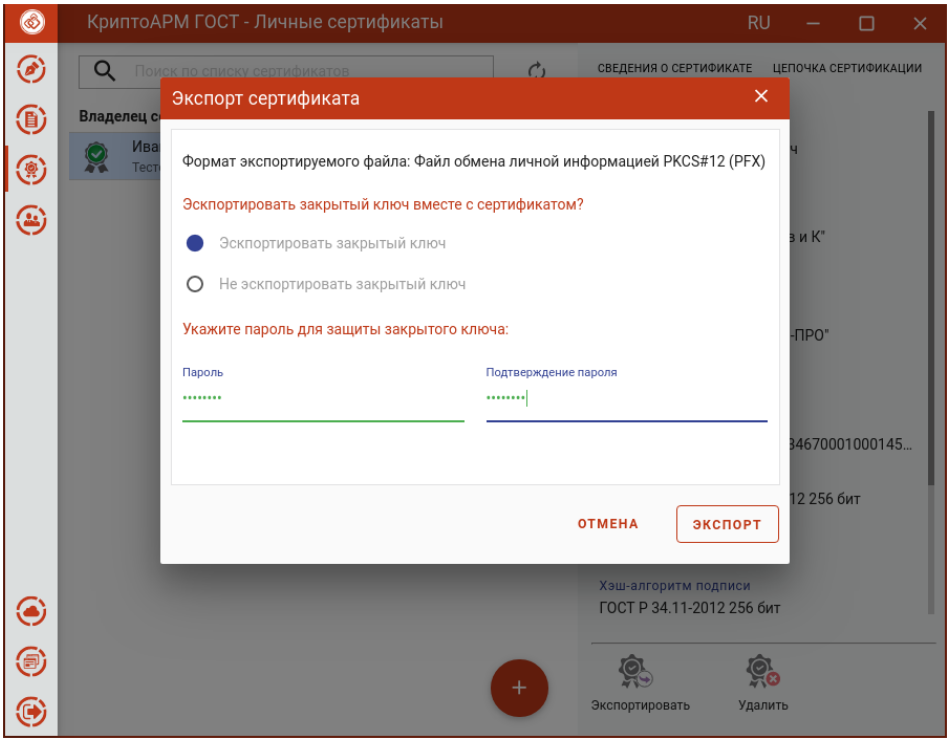


Выбор кодировки файла сертификата

После нажатия кнопки **Экспорт** в появившемся окне указать путь и имя файла, куда будет сохранен сертификат (по умолчанию, файл export.cer).

При экспорте сертификата с экспортируемым закрытым ключом в появившемся диалоговом окне можно выбрать способ экспорта сертификата:

- экспортировать только сертификат без закрытого ключа. В таком случае нужно только выбрать кодировку файла сертификата.
- экспортировать сертификат вместе с закрытым ключом. В таком случае надо указать пароль для защиты закрытого ключа.



Экспорт сертификата вместе с закрытым ключом

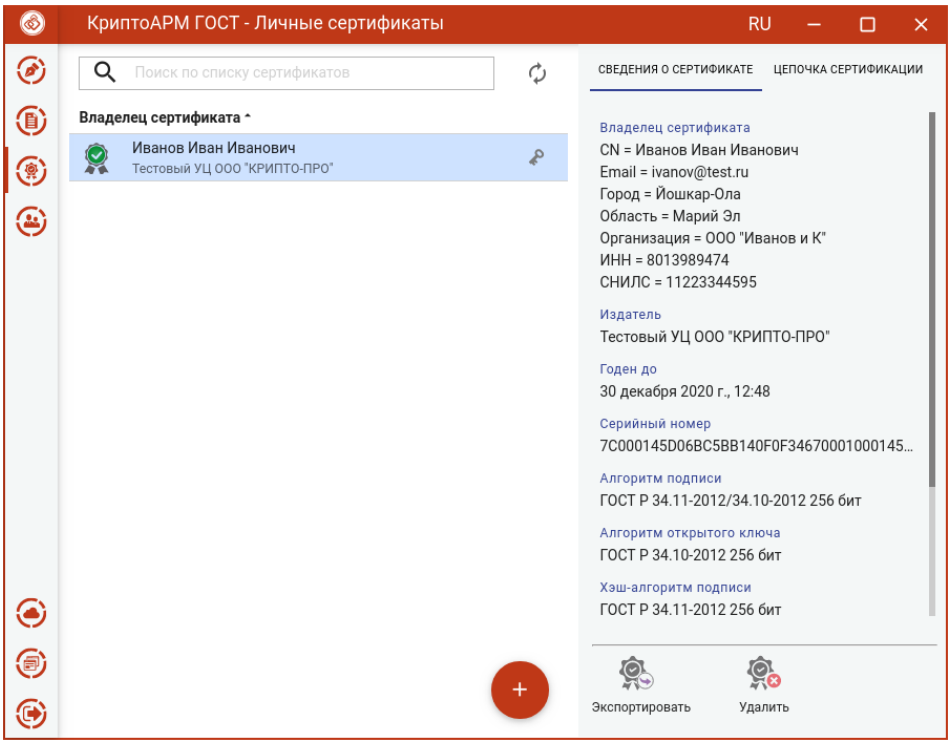
После нажатия кнопки **Экспорт** в появившемся окне указать путь и имя файла, куда будет сохранен сертификат (по умолчанию, файл export.pfx).

По окончании операции возникнет сообщение об успешном экспорте сертификата.

Примечание: если контейнер экспортируемого сертификата защищен паролем, то при экспорте сертификата вместе с закрытым ключом необходимо будет вводить пароль к нему.

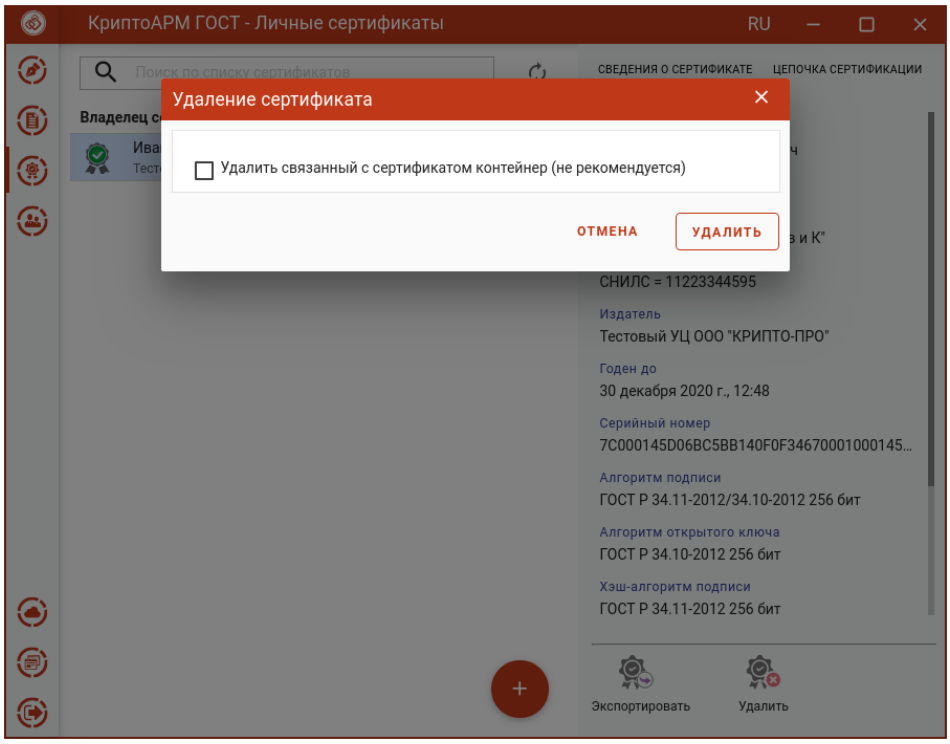
5.16.4 Удаление сертификата

Для удаления сертификата нужно выделить сертификат и нажать **Удалить**.



Просмотр сертификата

Открывается окно подтверждения удаления.



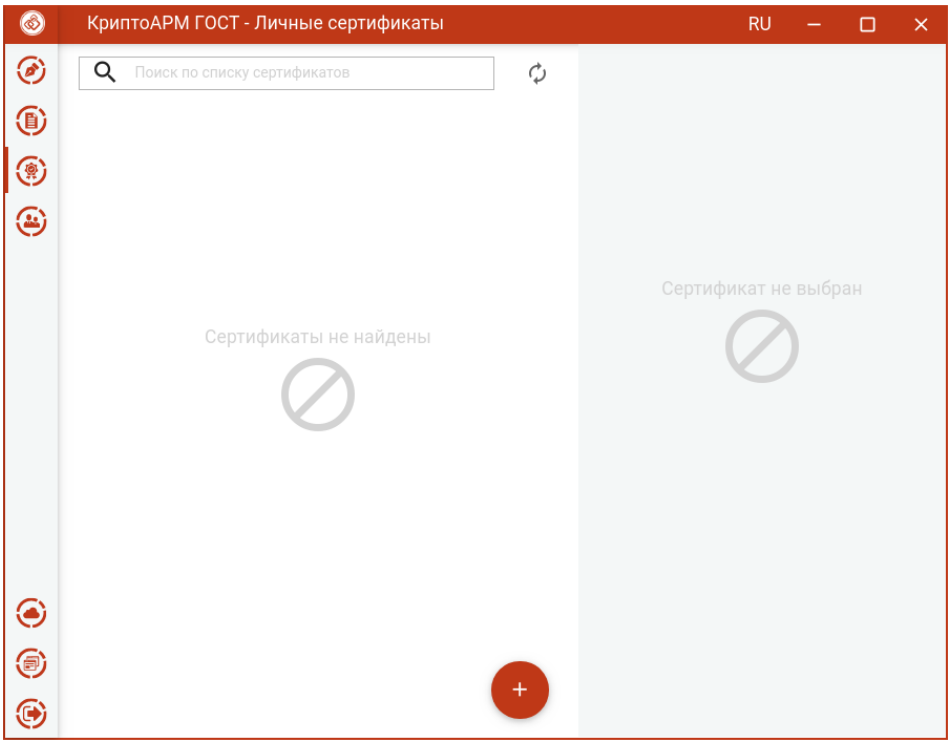
Подтверждение удаления сертификата

Если у сертификата есть привязка к закрытому ключу, то при удалении сертификата возможно удаление закрытого ключа. Для этого надо поставить флаг **Удалить связанный с сертификатом контейнер**.

Примечание. Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.

Нажать **Удалить** для подтверждения удаления.

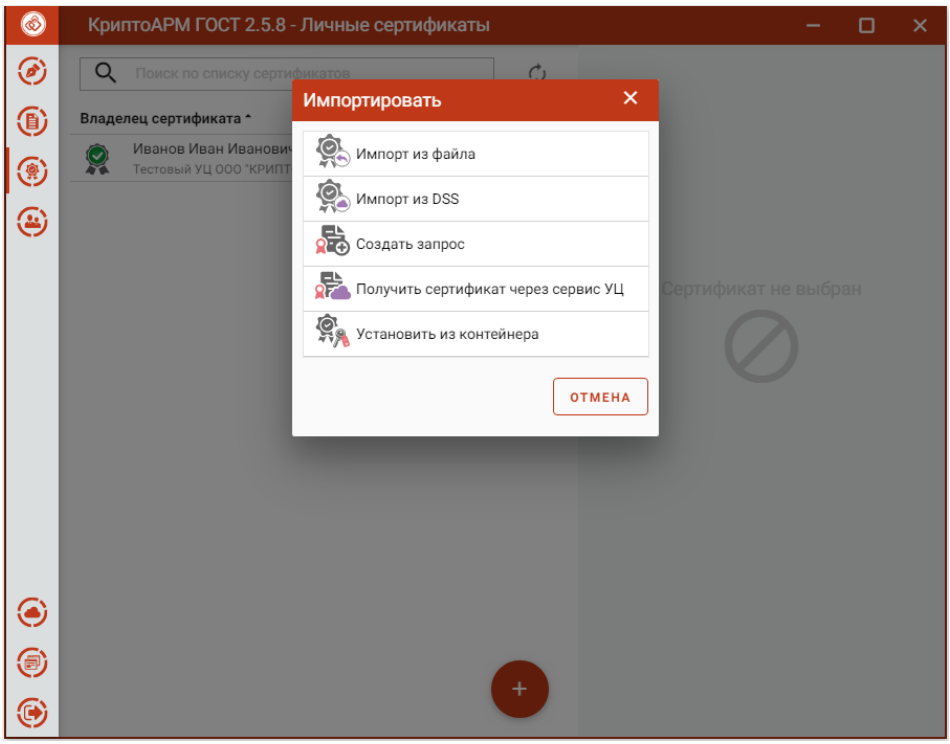
При успешном выполнении операции сертификат удаляется из списка.



Удаление сертификата

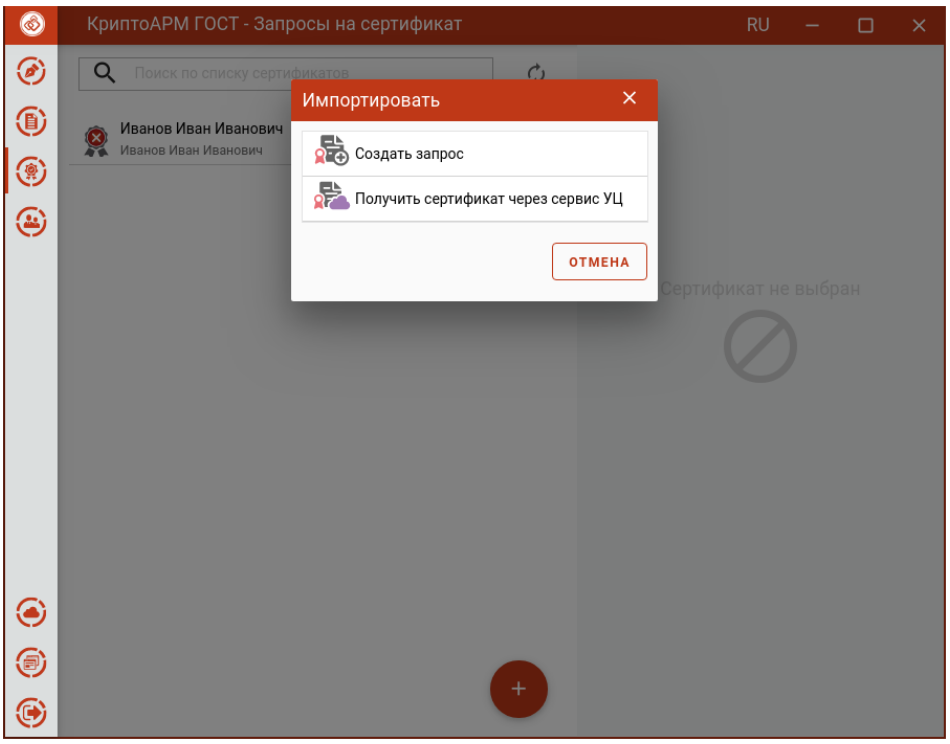
5.16.5 Создание запроса на сертификат

Для создания запроса на сертификат в окне добавления сертификата следует выбрать операцию **Создать запрос**. Создать запрос можно со списка **Личных сертификатов**.



Создание запроса на сертификат в списке личных сертификатов

Или со списка запросов

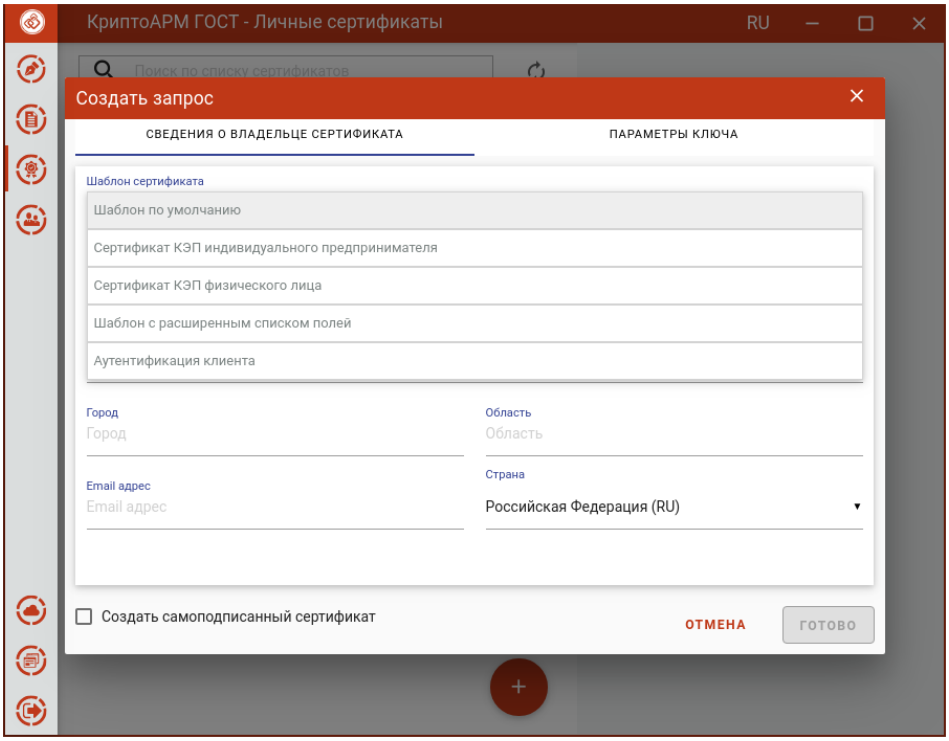


Создание запроса на сертификат в списке запросов

Сбор необходимых данных для генерации запроса распределены на две вкладки: **Сведения о владельце сертификата** и **Параметры ключа**.

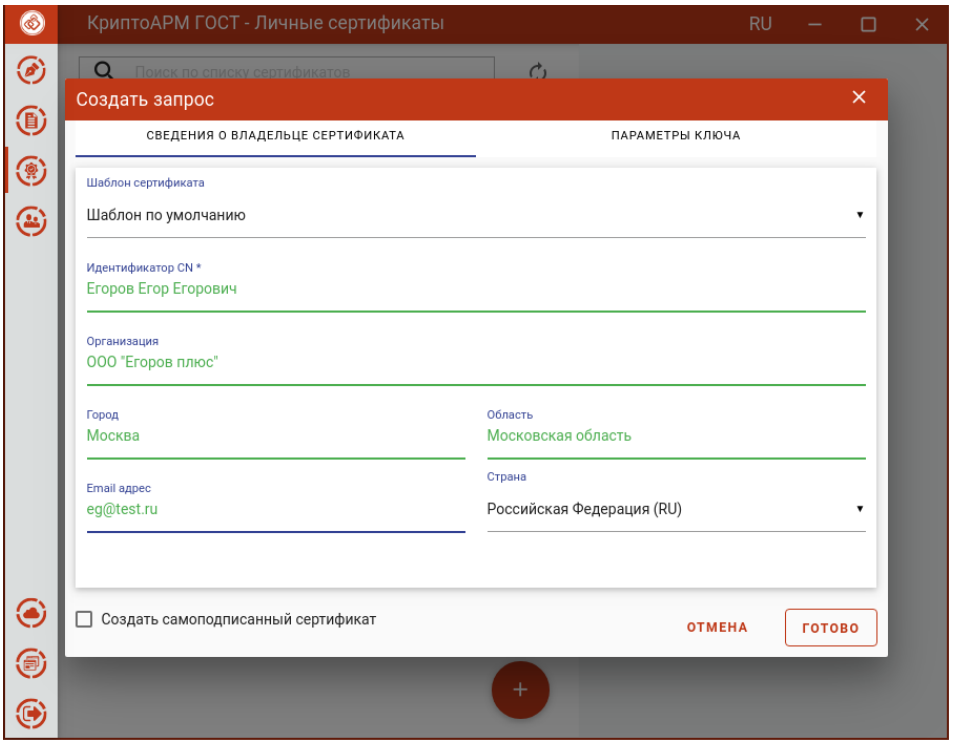
В **Сведениях о владельце сертификата** указывается:

- Шаблон сертификата;



Выбор шаблона сертификата

- Основная информация, в которой, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце сертификата.

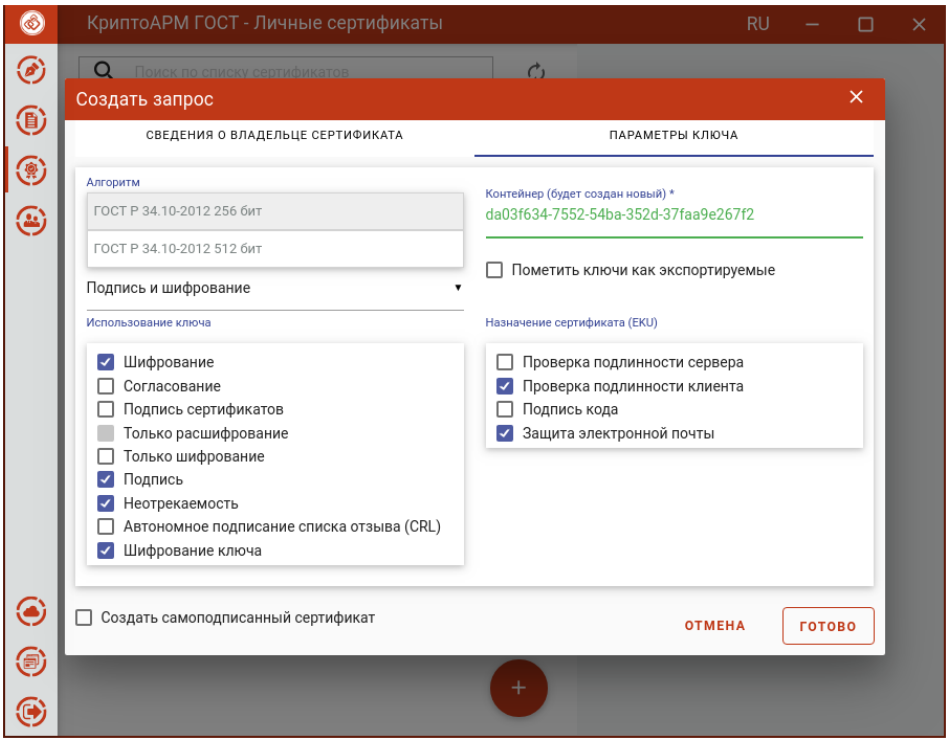


Информация о владельце сертификата

- Флаг **Создать самоподписанный сертификат** служит для создания сертификата и его автоматической установки в личное хранилище пользователя. Запросы на самоподписанные сертификаты не создаются.

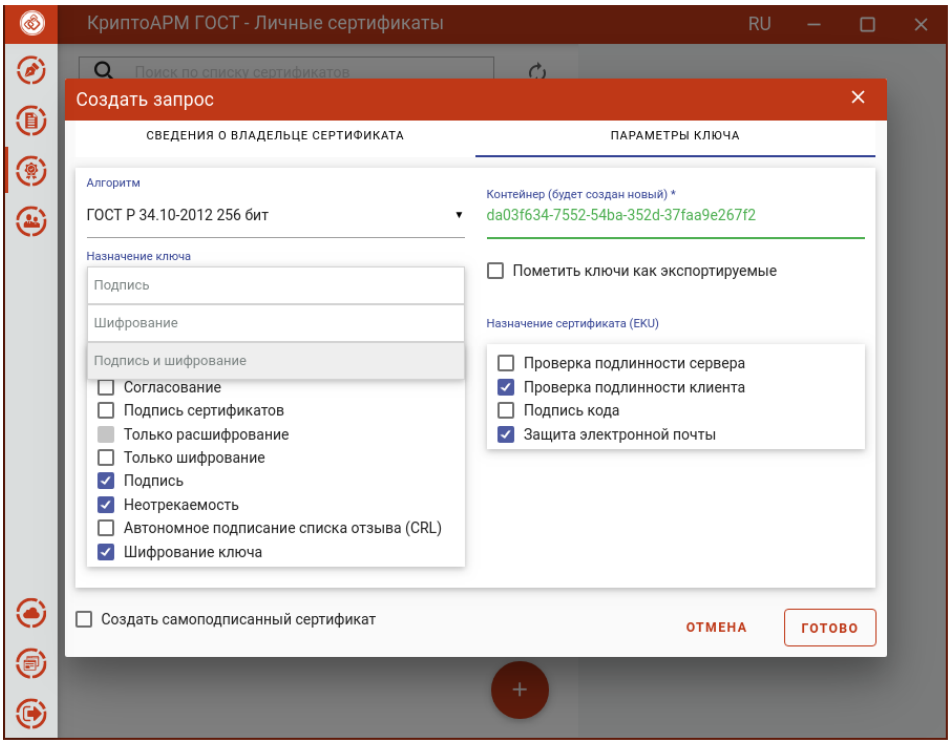
В **Параметрах ключа** указывается:

- Алгоритм ключа;



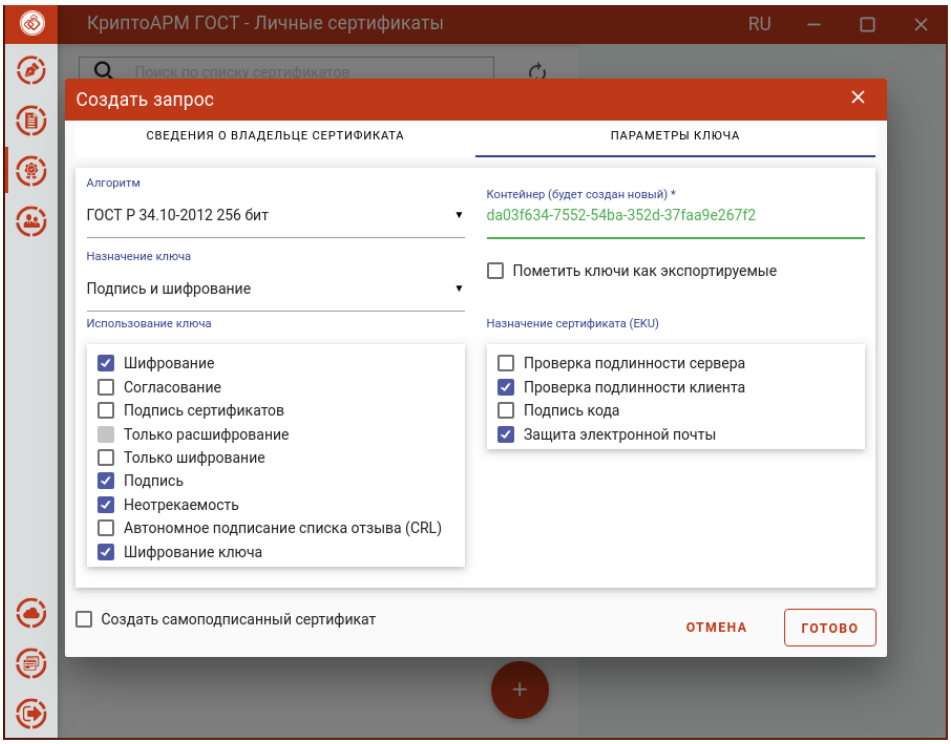
Выбор алгоритма ключа

- Назначение ключа;



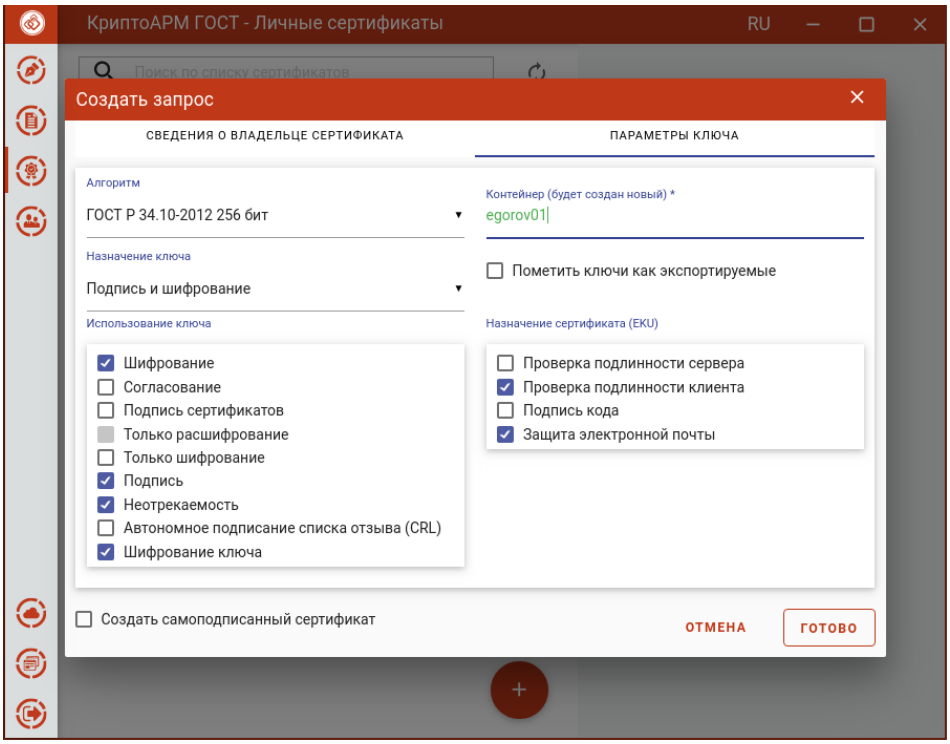
Выбор назначения ключа

- Использование ключа;



Выбор использования ключа

- Контейнер - будет создан на основе нового ключевого набора. Можно задать свое имя ключевого набора или оставить созданное автоматически.

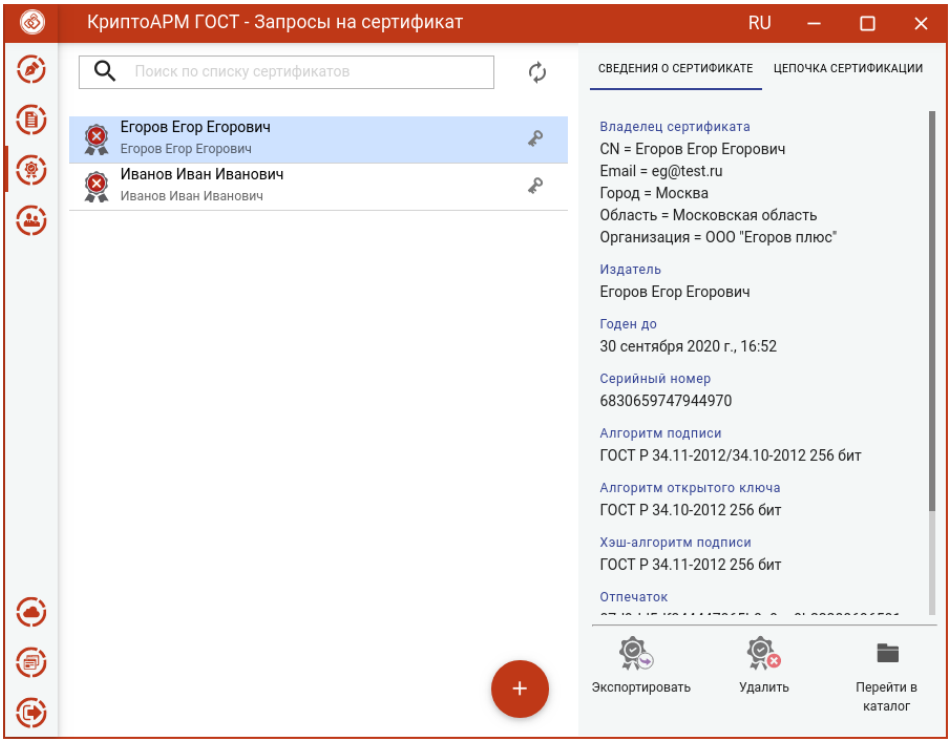


Задание названия ключевого контейнера

- Пометить ключи как экспортируемые. Если отметить этот флаг, то можно проводить экспорт сертификата вместе с закрытым ключом.
- Назначение сертификата (EKU).

На основе указанных данных по кнопке **Готово** будет сформирован запрос на сертификат. Для сертификата выберите ключевой носитель для хранения контейнера (Реестр, диск, токен). На запрос системы установите пароль на данный контейнер и подтвердите его. После завершения операции возникнет окно с информацией о ее результатах

Запрос сохраняется в файл <CN сертификата>_<алгоритм >_<дата генерации>.req в папке пользователя в каталоге \.Trusted\CryptoARM GOST\CSR и отображается в подпункте **Запросы** раздела **Сертификаты**.



Форма просмотра запроса на сертификат

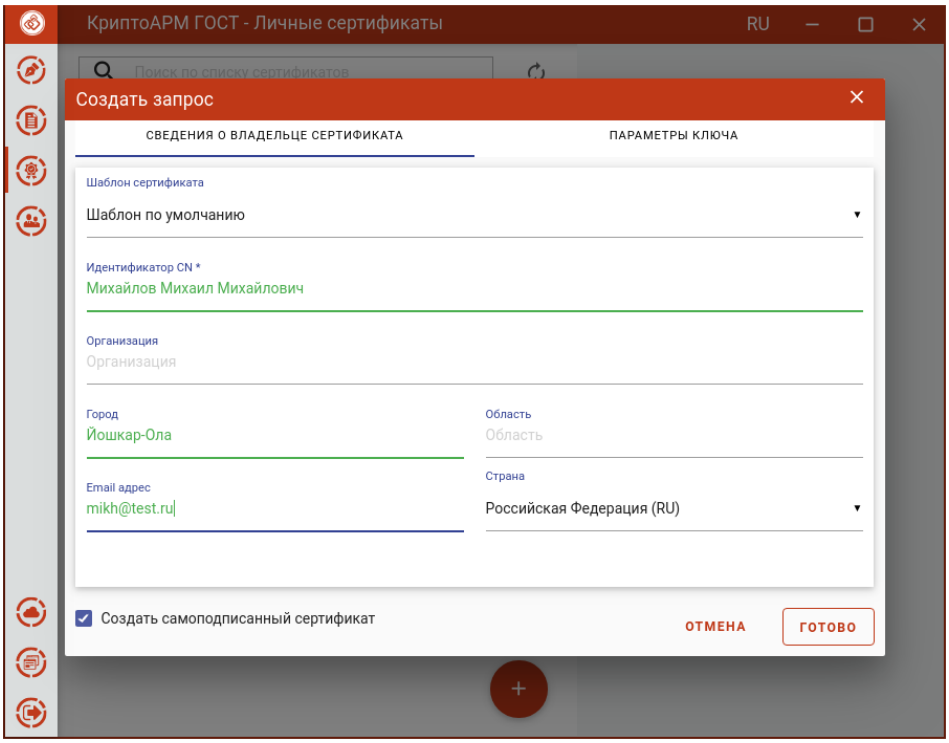
Для запроса доступны следующие операции:

- **Экспортировать** – для сохранения сертификата в файл;
- **Удалить** – для удаления запроса из списка, при этом файл запроса не удаляется из папки;
- **Перейти в каталог** – для открытия каталога в файловом менеджере, где располагается файл запроса.

Созданный файл запроса на сертификат следует направить на рассмотрение в Удостоверяющий центр (УЦ). Полученный из УЦ сертификат следует импортировать для работы в приложении.

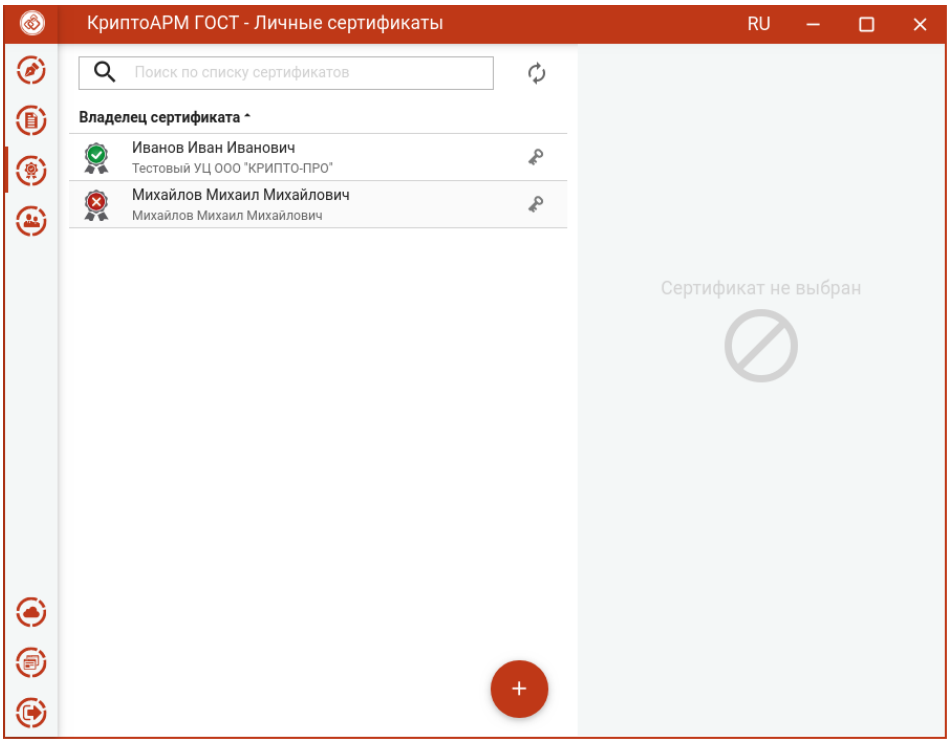
5.16.6 Создание самоподписанного сертификата

Для создания самоподписанного сертификата на форме **Создать запрос** следует поставить флаг **Создание самоподписанного сертификата**. Создание запроса описано в разделе Создание запроса на сертификат.



Создание самоподписанного сертификата

На основе указанных данных по кнопке **Готово** будет сформирован самоподписанный сертификат. Для сертификата выберите ключевой носитель для хранения контейнера (Реестр, диск, токен). На запрос системы установите пароль на данный контейнер и подтвердите его. После завершения операции возникнет окно с информацией о ее результатах. Сертификат будет в списке **Личных сертификатов.**



Список личных сертификатов

Чтобы самоподписанный сертификат был действительным, нужно импортировать его в хранилище **Доверенных корневых**. Для этого сначала необходимо сертификат экспортировать в файл, а потом импортировать.

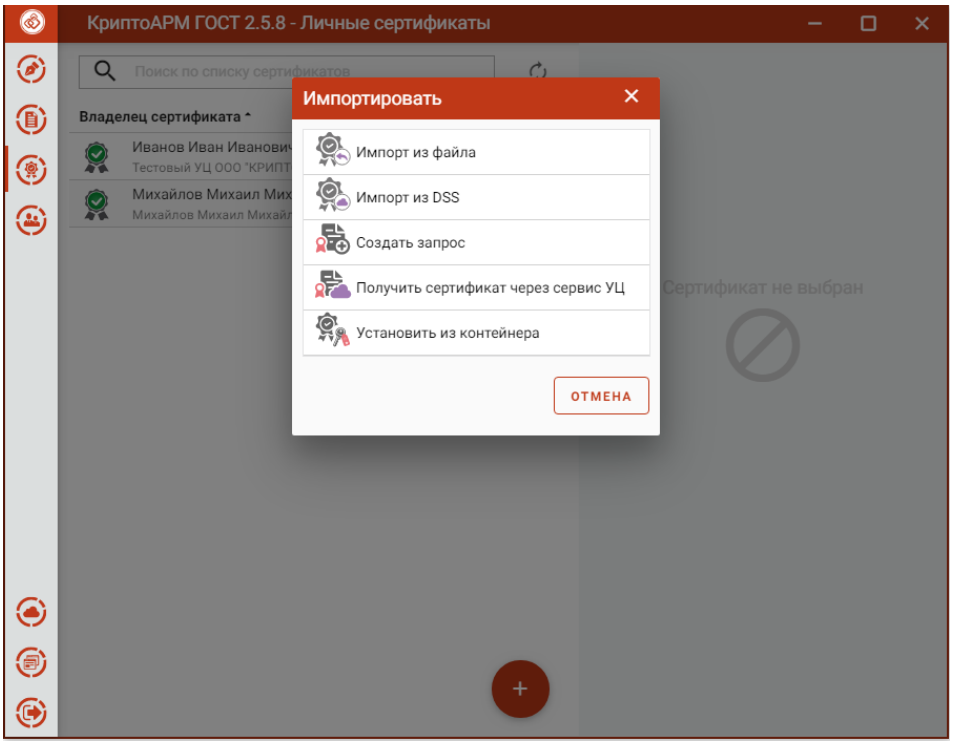
При генерации самоподписанного сертификата запрос на сертификат не создается.

5.16.7 Получить сертификат через сервис УЦ

Для создания запроса и выпуска сертификата нужно добавить сервис подключения к КриптоПро УЦ 2.0. А потом, используя это подключение, создать запрос на сертификат.

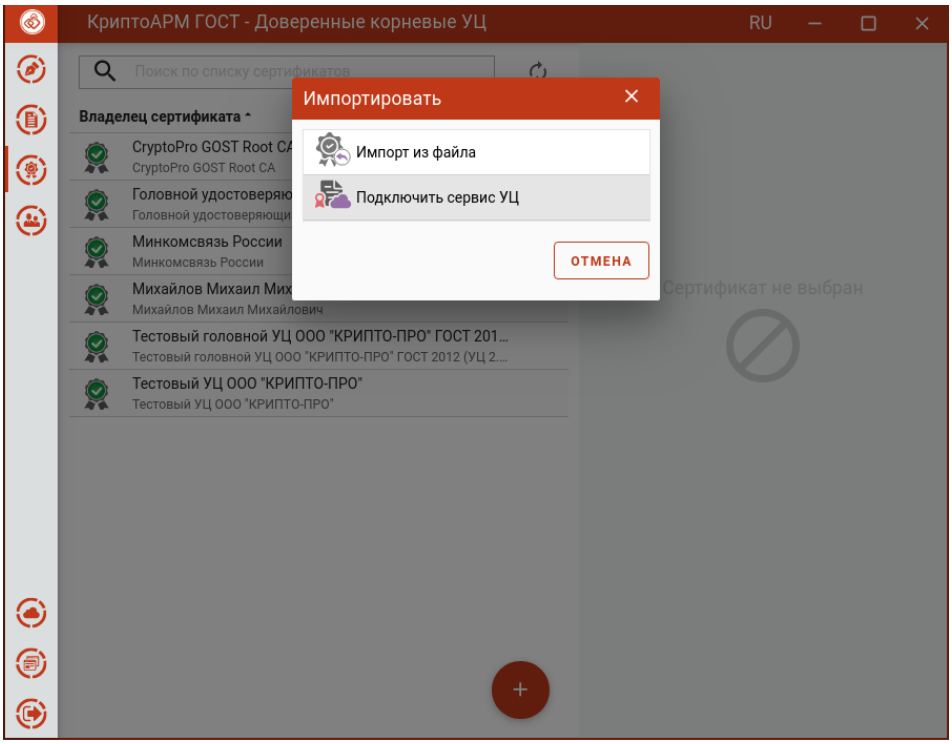
5.16.7.1 Добавление нового сервиса

Создать подключение можно, выбрав опцию **Получить сертификат через сервис УЦ,** в списке **Личных сертификатов** или в списке **Запросов** при добавлении сертификата.



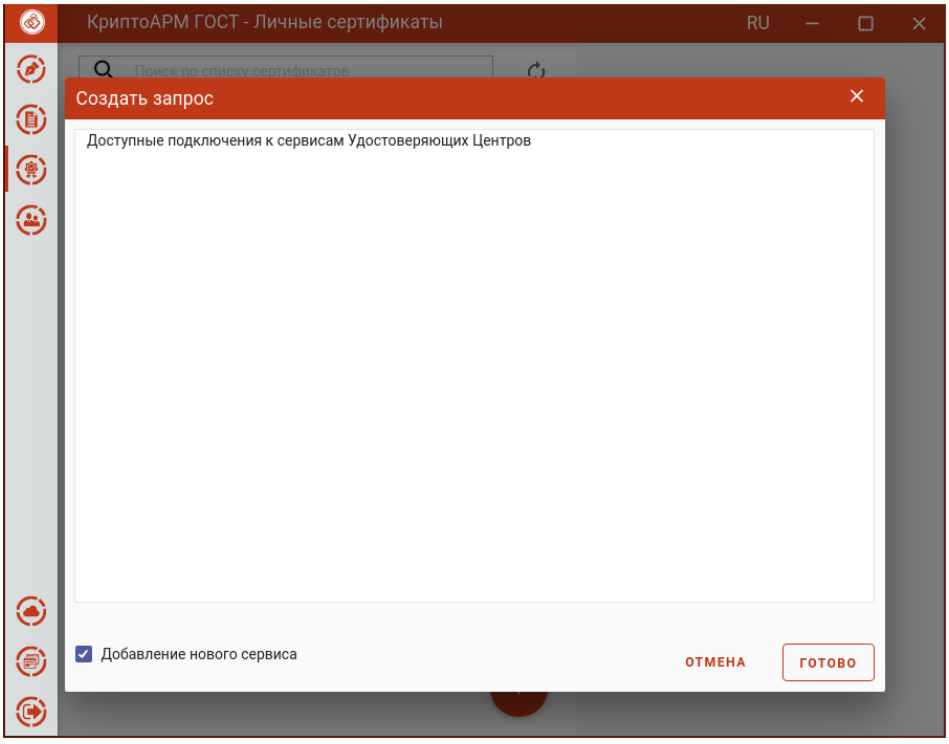
Добавление подключения в списке Личных сертификатов.

Создать подключение можно, выбрав опцию **Подключить сервис УЦ,** при добавлении сертификата в списке **Доверенных корневых сертификатов**.



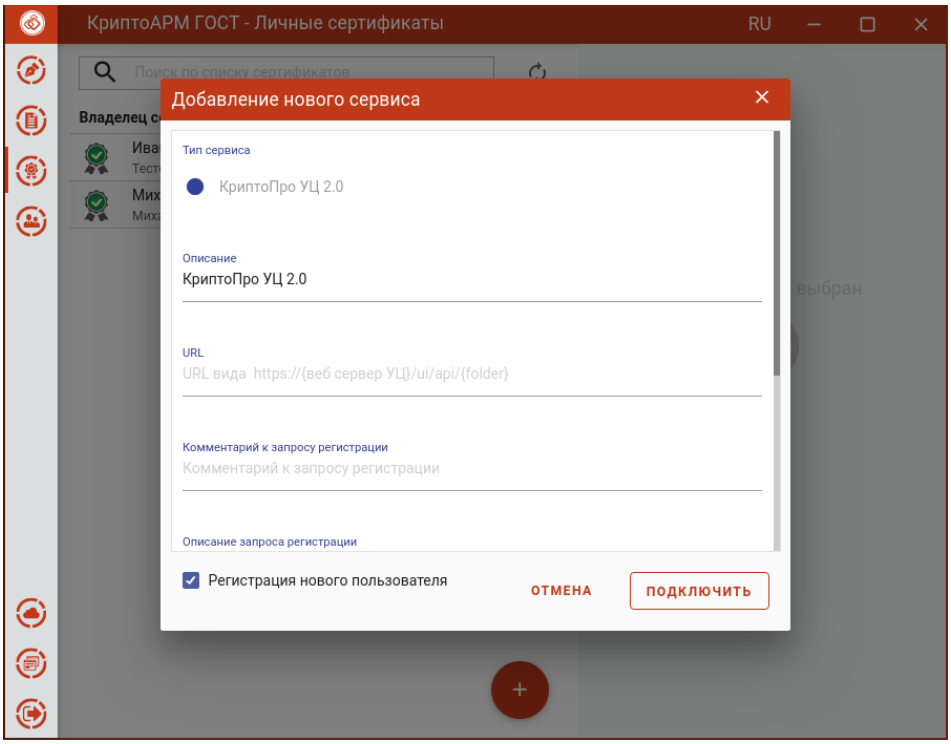
Добавление подключения в списке Корневых сертификатов

В открывшемся окне установить флаг **Добавление нового сервиса** и нажать кнопку **Готово**.



Добавление нового сервиса

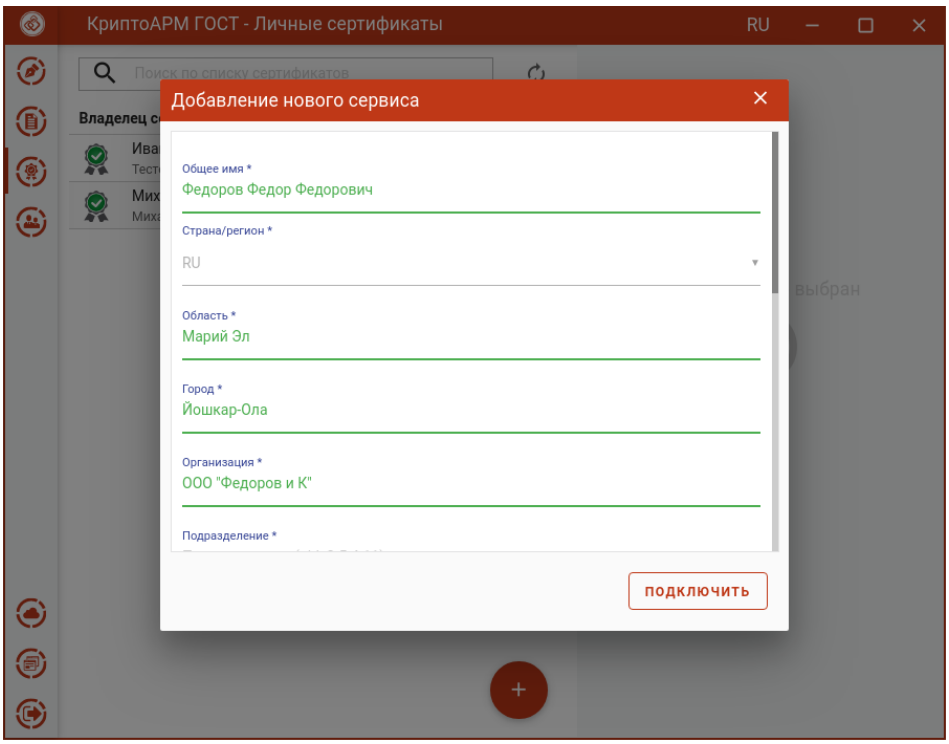
Открывается форма ввода полей для регистрации сервиса.



Форма ввода полей для создания сервиса

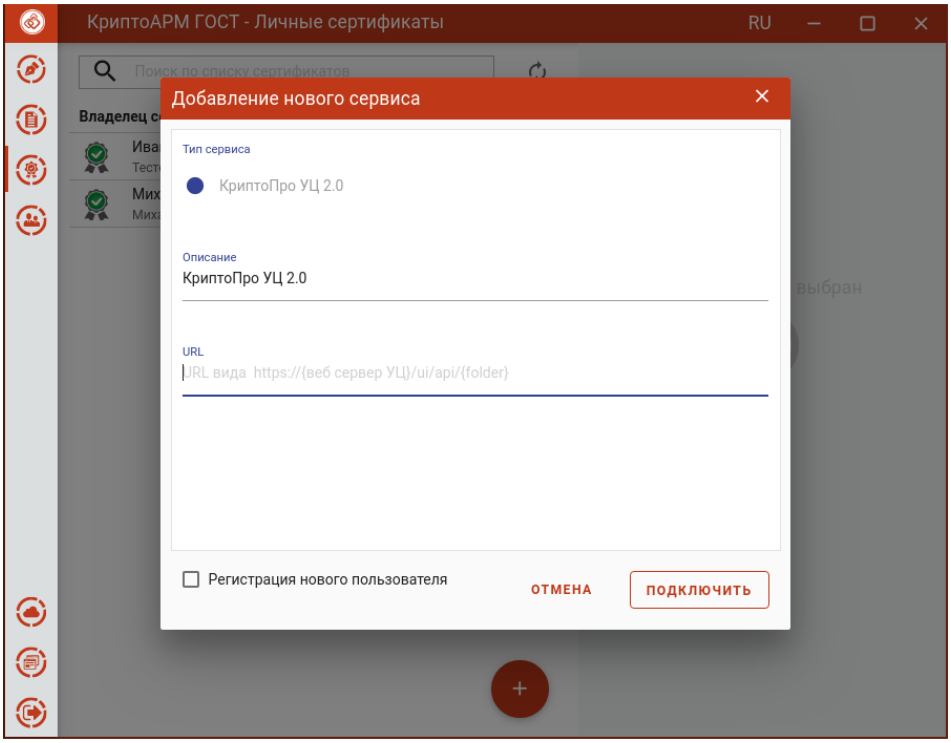
Если пользователь ранее не был не зарегистрирован в УЦ, то для добавления подключения нужно установить галку в поле **Регистрация нового пользователя** и нажать кнопку **Подключить**.

На следующем шаге нужно ввести данные для регистрации и нажать **Подключить**.



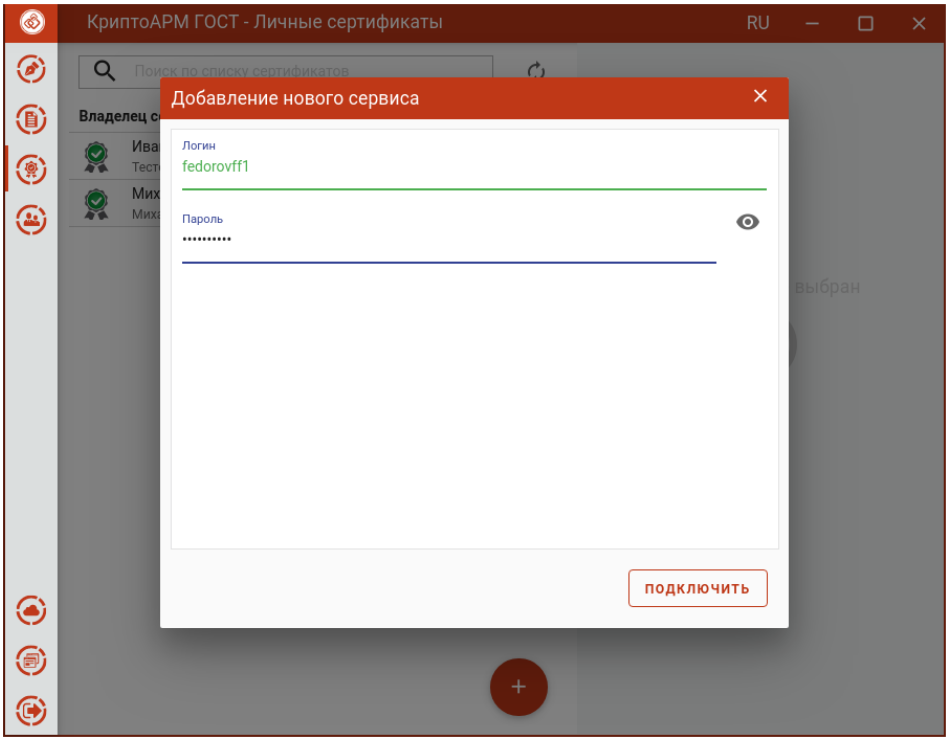
Форма регистрации нового пользователя для подключения к УЦ

Если пользователь уже был зарегистрирован в УЦ, и у него есть логин и пароль для авторизации на сервисе, то для добавления подключения нужно снять галку в поле **Регистрация нового пользователя** и нажать кнопку **Подключить**.



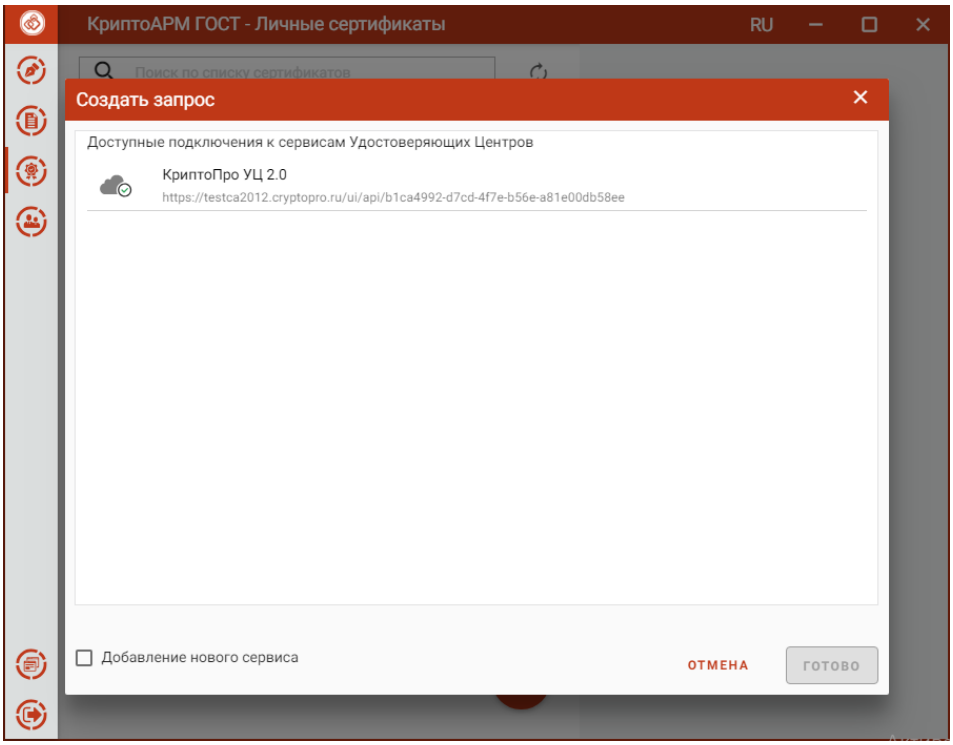
Форма подключения к УЦ без регистрации пользователя

На следующем шаге нужно ввести данные для авторизации и нажать **Подключить**.



Авторизация на сервисе УЦс помощью логина и пароля

После успешной регистрации или авторизации созданное подключение УЦ появляется в списке сервисов, когда выбирается опция **Получение сертификата через сервис УЦ**.



Список подключенных сервисов

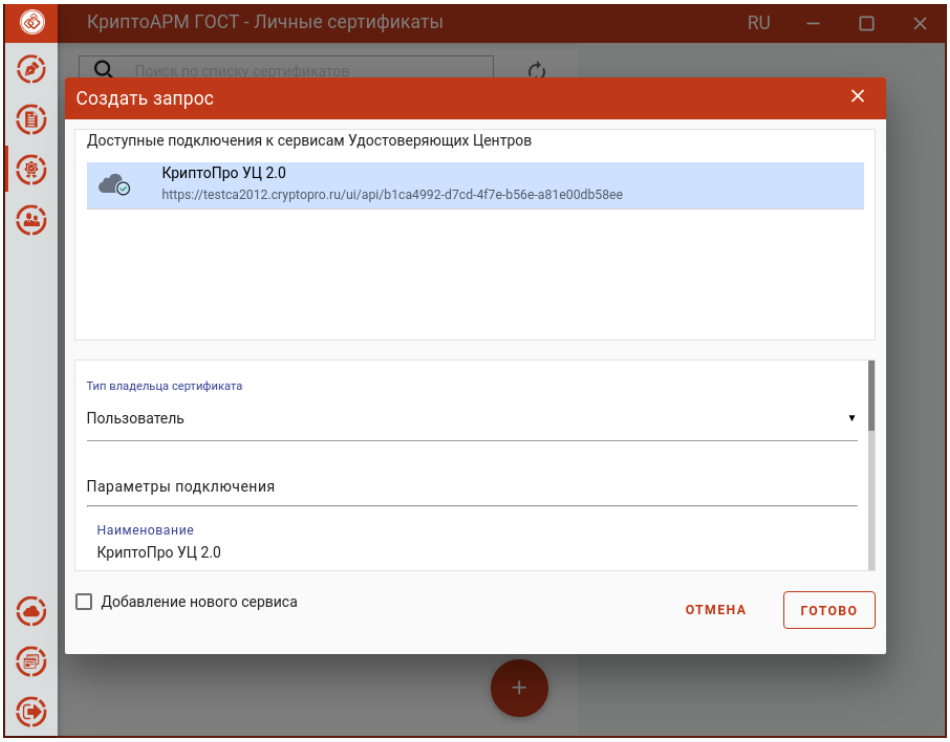
На основе созданного подключения можно создать запрос на сертификат.

Если подключение в списке с иконкой  , то соединение с сервисом по указанному пользователем адресу успешно создано.

Если подключение в списке с иконкой  , то соединение с сервисом по указанному пользователем адресу успешно создано, но, или нет аутентификации на сервисе, или запрос по регистрации на сервисе еще не подтвержден. Пользователю следует подождать подтверждения регистрации.

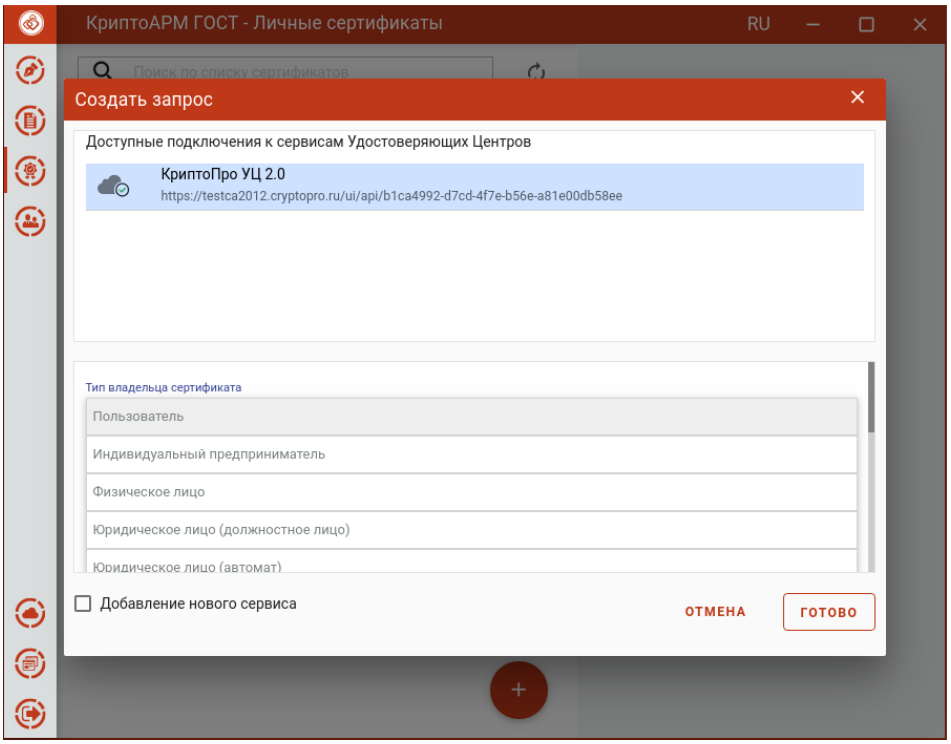
5.16.7.2 Создание запроса на сертификат

Для создания запроса на сертификат нужно выбрав опцию **Получить сертификат через сервис УЦ** при добавлении сертификата в списке **Личных сертификатов** или в списке **Запросов**. В открывшемся окне выбрать подключение.



Выбор подключения к сервису УЦ

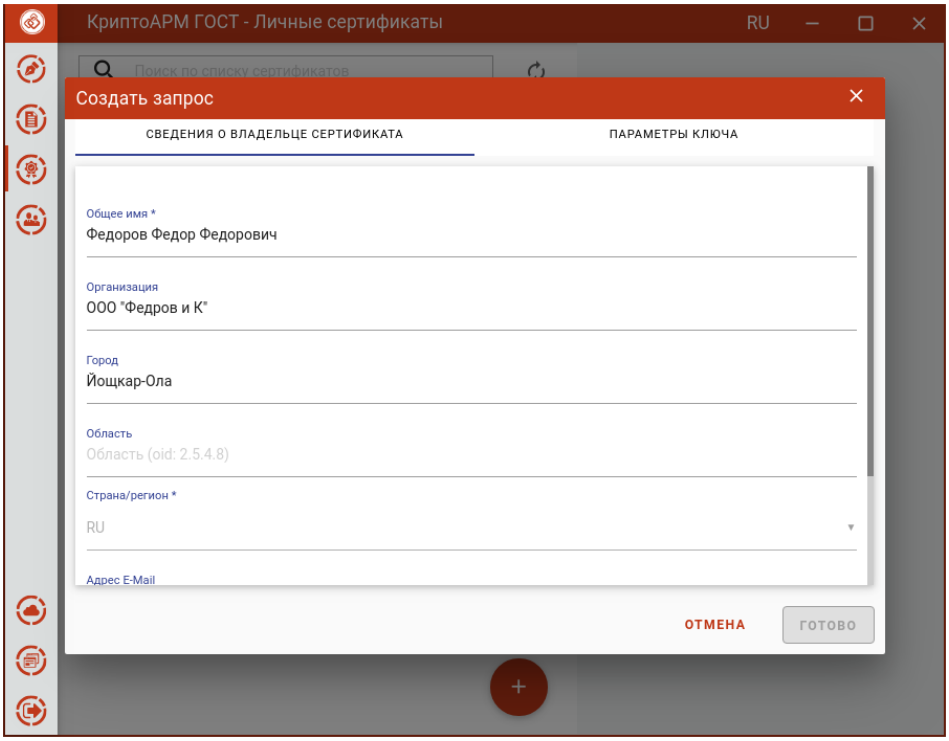
Выбрать тип владельца сертификата



Выбор типа владельца сертификата

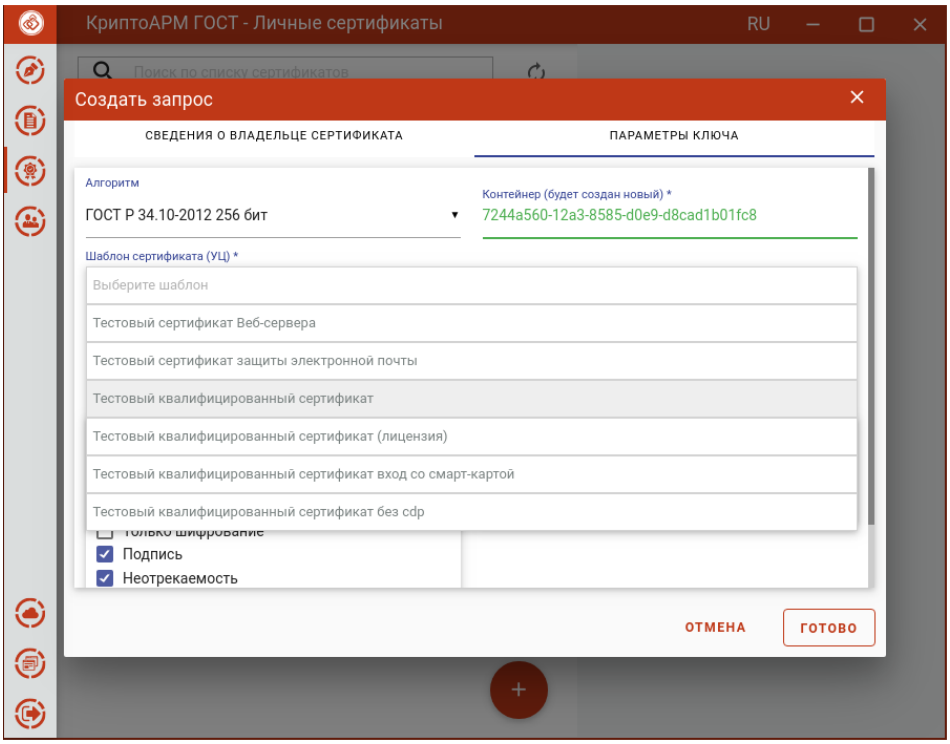
По нажатию на кнопку **Готово** открывается форма для заполнения полей запроса на сертификат, соответствующих выбранному шаблону. Поля, заполненные при регистрации пользователя на сервисе УЦ, подставляются в соответствующие поля на форме запроса.

Следует заполнить необходимые поля в запросе на вкладках **Сведения о владельце сертификата.**



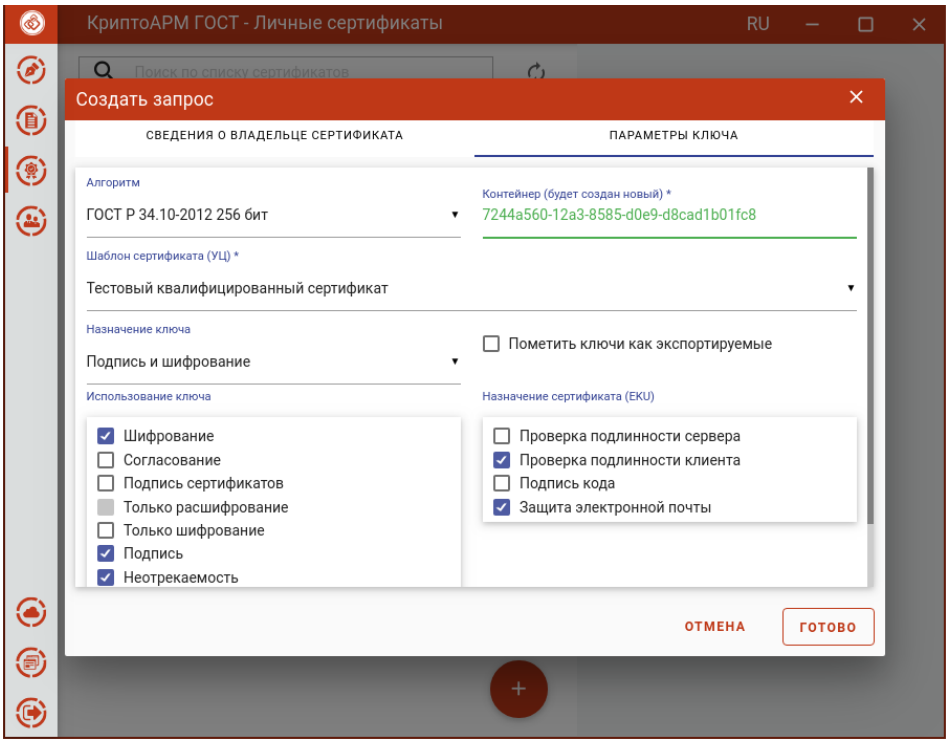
Форма создания запроса на сертификат

И **Параметры ключа,** выбрав **Шаблон сертификата (УЦ)**.



Выбор шаблона сертификата (УЦ)

После заполнения всех обязательных полей становится доступна кнопка **Готово.**



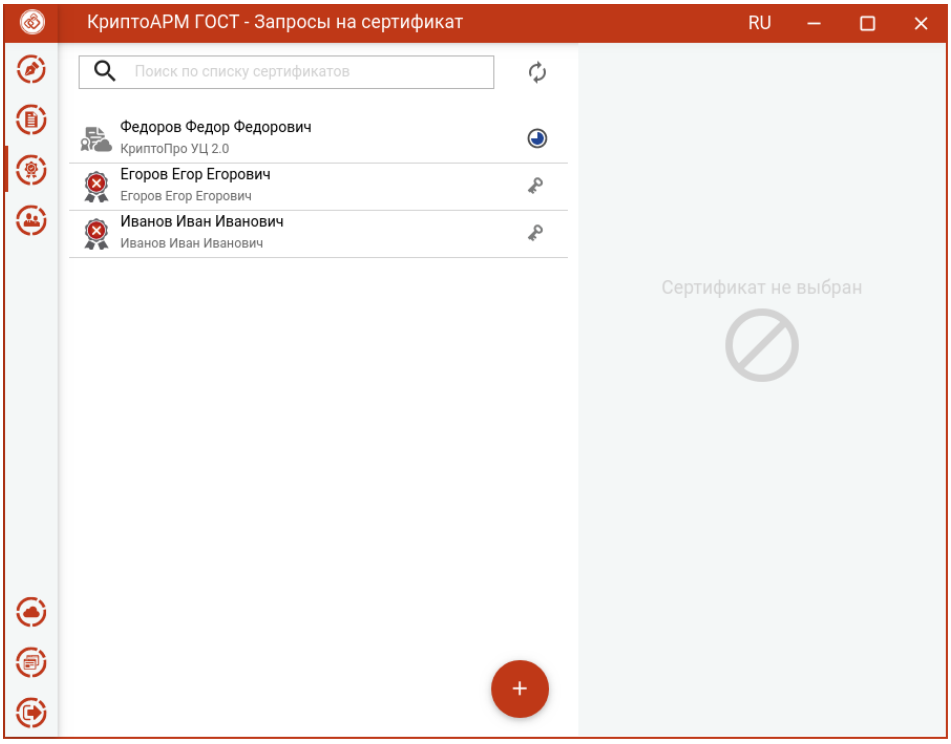
Параметры ключа на форме созданя запроса

Для сертификата нужно выбрать ключевой носитель для хранения контейнера (Реестр, диск, токен). На запрос системы - установить пароль на данный контейнер и подтвердить его. После завершения операции возникнет окно с информацией о ее результатах.

Запрос сохраняется в раздел **Запросы** на вкладке управления сертификатами.

5.16.7.3 Управление запросами на сертификат, созданными через сервис УЦ.

Запрос, созданный через подключенный сервис УЦ, сохраняется в раздел **Запросы**.

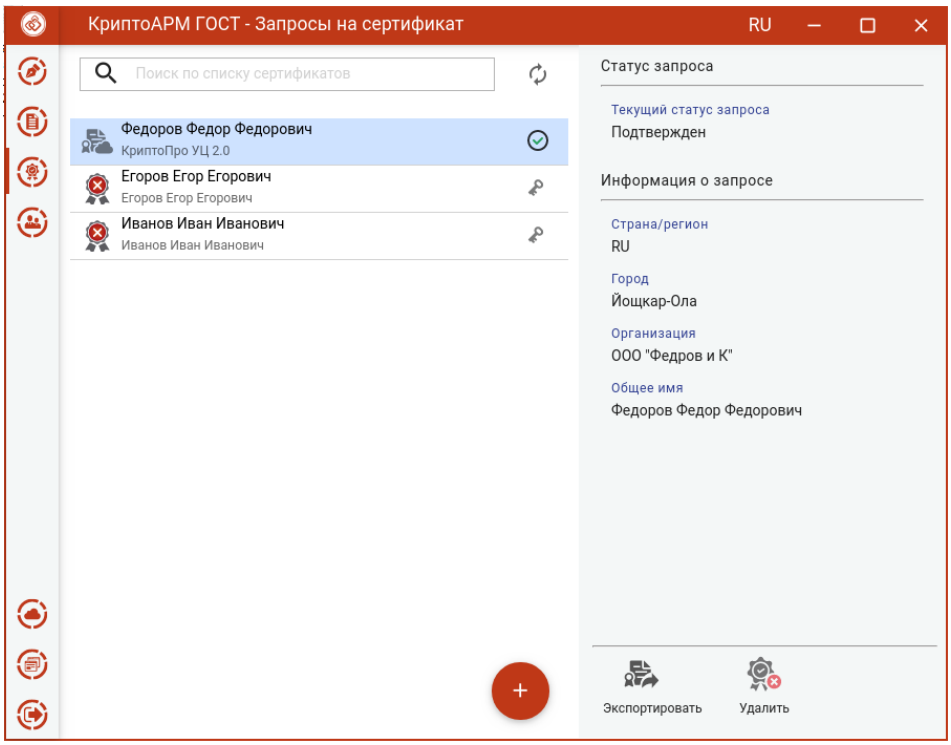


Список запросов

Для отображения статуса запроса применяются следующие обозначения:

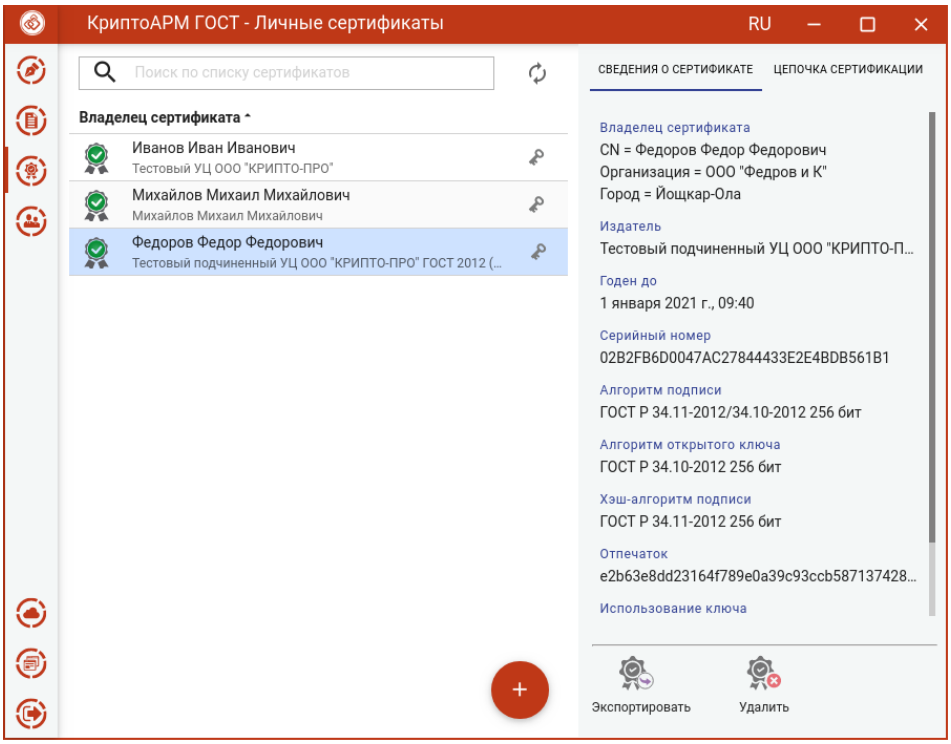
	Для данного запроса сертификат выпущен и установлен в хранилище КриптоПро.
	Запрос отклонен Удостоверяющим Центром.
	Запрос находится в обработке Удостоверяющим центром.
	Проблемы с соединением, не позволяющие актуализировать статус запроса.

Когда запрос будет обработан Удостоверяющим Центром и выпущен сертификат, при выделении запроса в списке, его статус измениться на .



Статус запроса, когда сертификат выпущен и установлен в хранилище

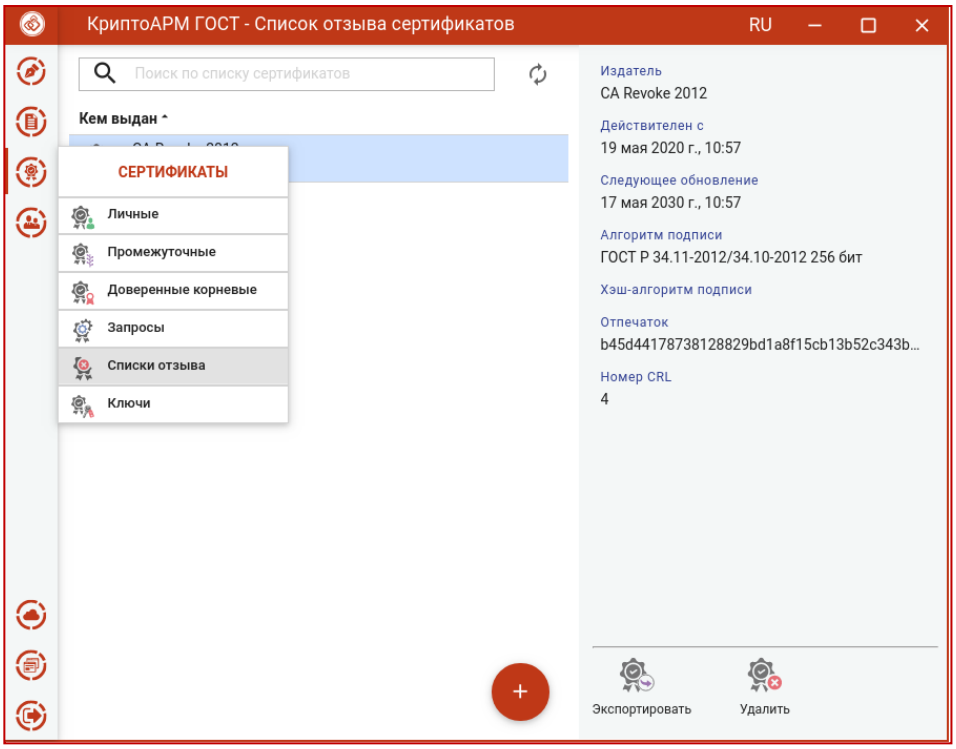
Сертификат установится в **Личное хранилище**.



Список личных сертификатов

5.16.8 Списки отзыва сертификатов (CRL)

Для работы со списками отзыва сертификатов в пункт меню добавлен подпункт **Списки отзыва**.

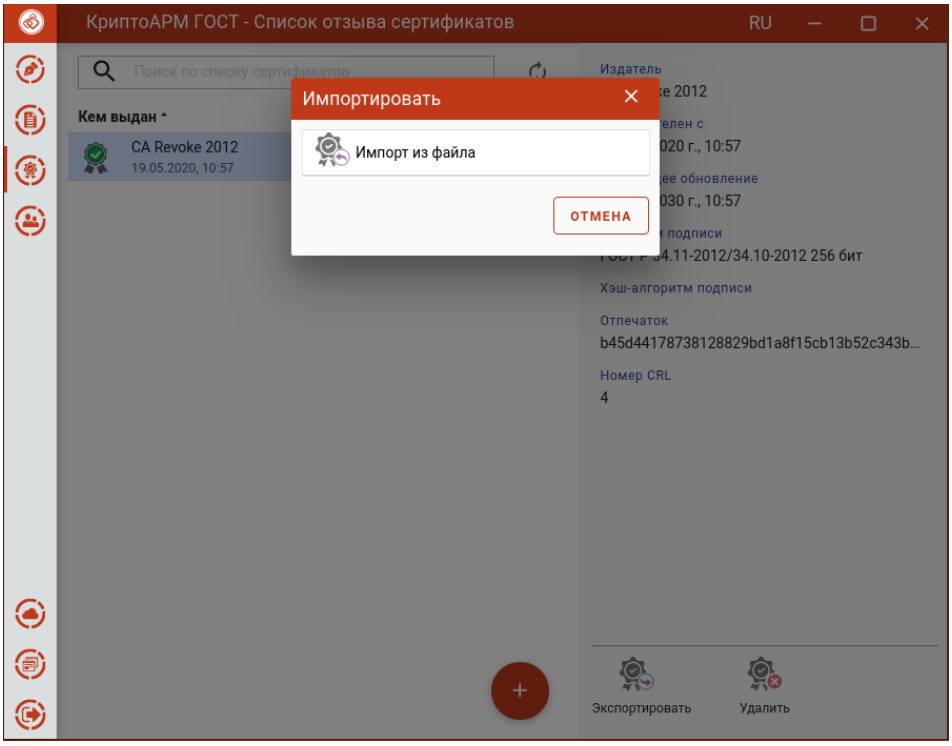


Выбор пунтк меню для управления списком отзыва

Списки отзыва можно импортировать, экспортировать и удалять.

5.16.8.1 Импорт COC

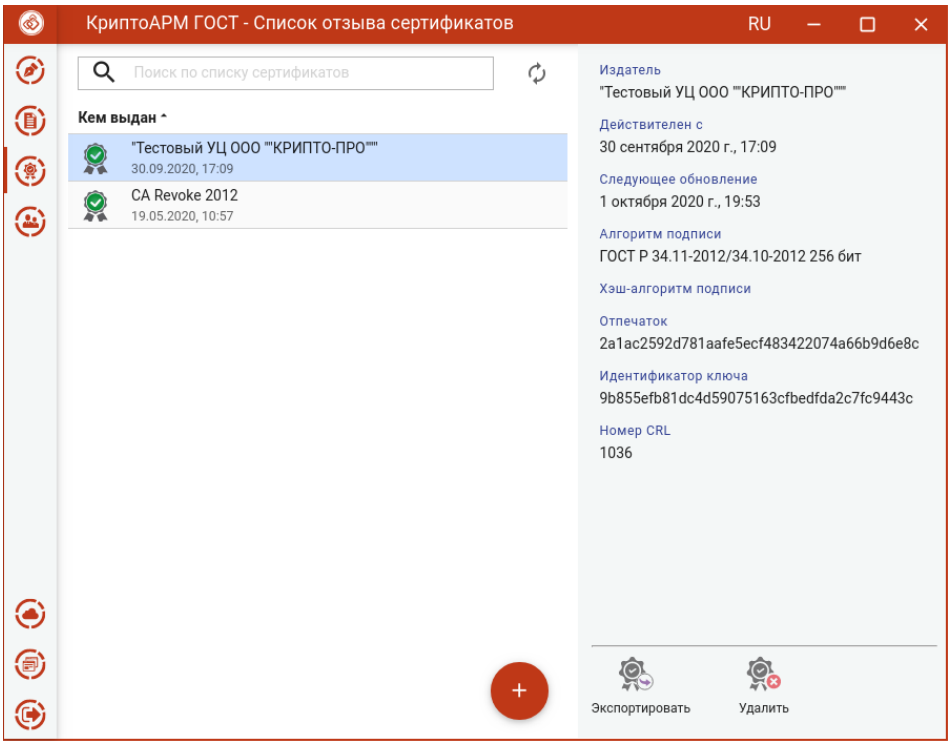
Для импорта списка отзыва надо нажать кнопку **Добавить (+)** и выбрать опцию **Импорт из файла** на любом списке сертификатов или COC.



Импорт списка отзыва сертификатов

В открывшемся файловом менеджере выбрать файл списка отзыва. Может быть запрошен пароль администратора.

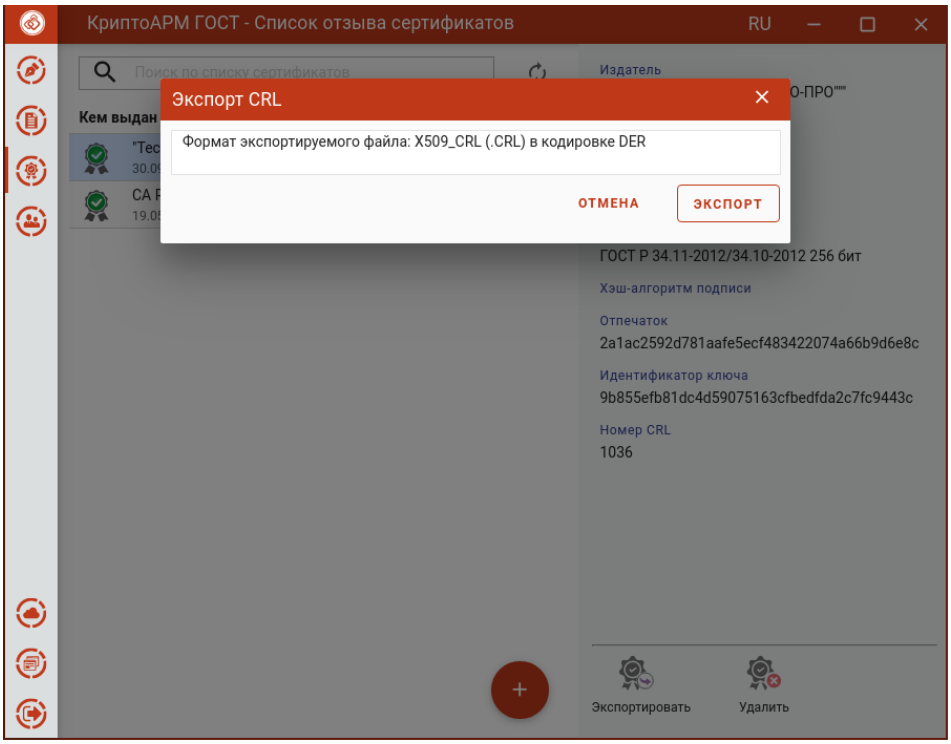
При успешном импорте COC отображается в разделе **Список отзыва сертификатов**.



Просмотр информации о списке отзыва

5.16.8.2 Экспорт COC.

Для экспорта в мастере **Список отзыва** нужно выбрать COC и нажать кнопку **Экспортировать**. Открывается форма подтверждения экспорта.



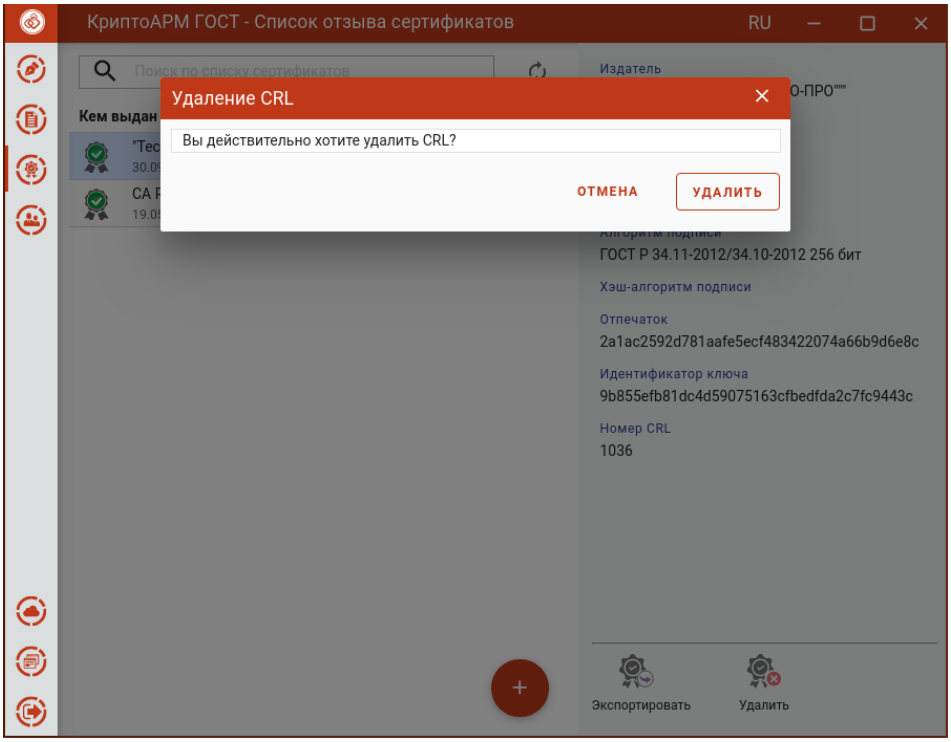
Выбор кодировки экспортируемого COC

При нажатии на **Экспорт** следует выбрать директорию для сохранения и задать имя файла COC.

При успешном сохранении COC в файл, появляется сообщение об этом.

5.16.8.3 Удаление COC.

Для удаления в мастере **Список отзыва** нужно выбрать COC и нажать кнопку **Удалить.** Подтвердить удаление в соответствующем окне.



Подтверждение удаления COC

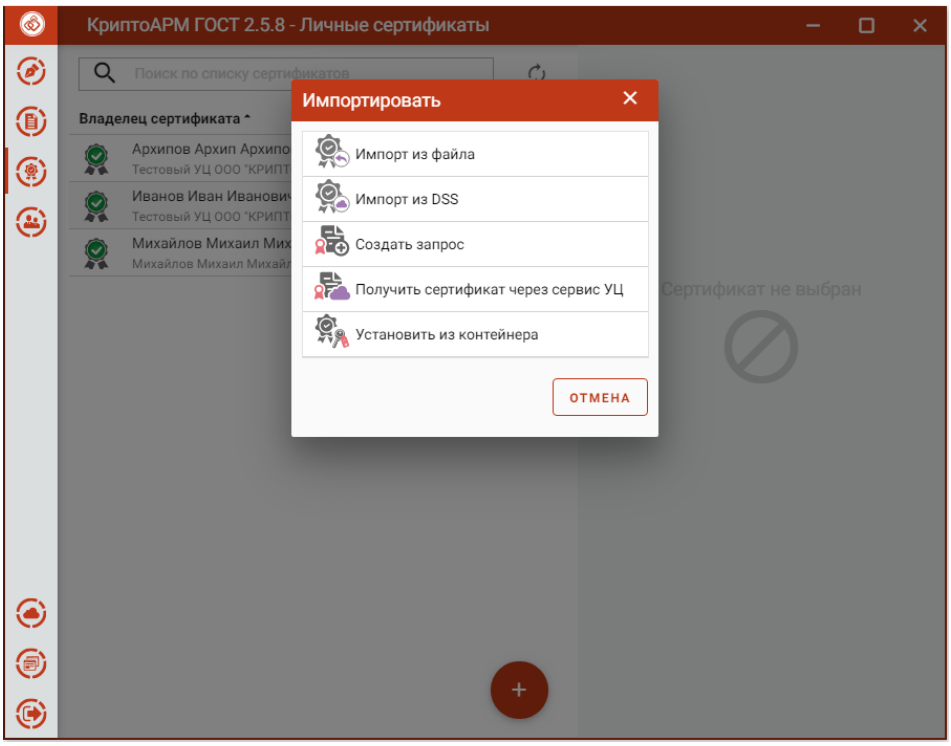
После успешного удаления появится сообщение об этом, COC исчезнет из списка.

5.16.9 Ключи

Данный раздел предназначен для управления контейнерами закрытых ключей на подключенных носителях или в реестре.

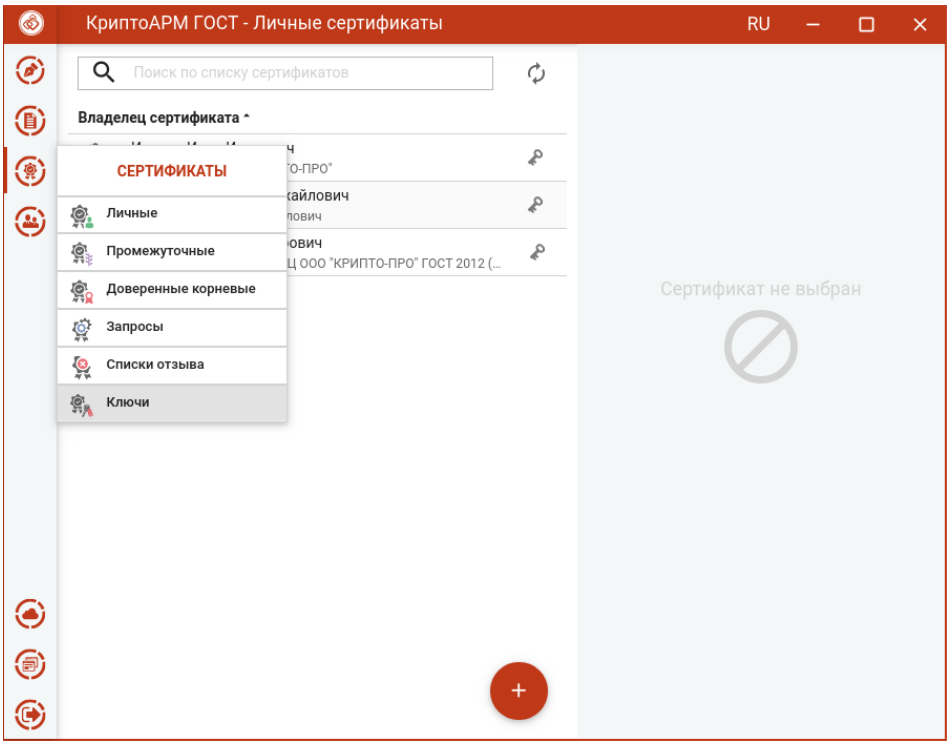
Установку сертификата из ключевого контейнера можно двумя способами.

В списке **Личных сертификатов** нажать **Добавить (+)** и выбрать операцию **Установить из контейнера.**



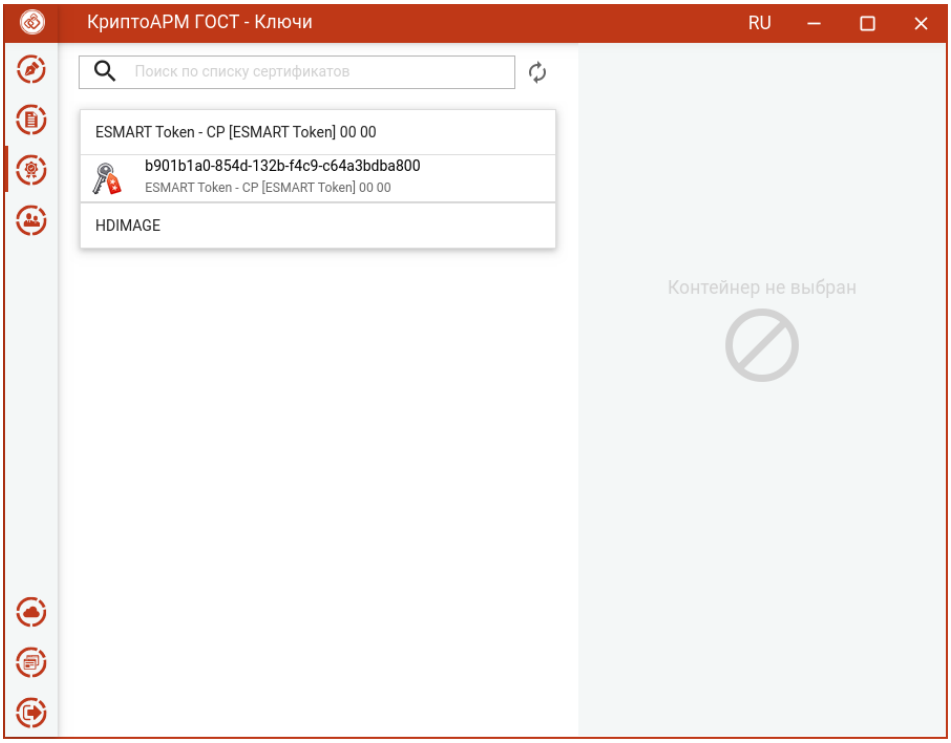
Установка из контейнера на списке Личных сертификатов

Или выбрать в меню **Сертификаты** подпункт **Ключи**.



Пункт меню Ключи

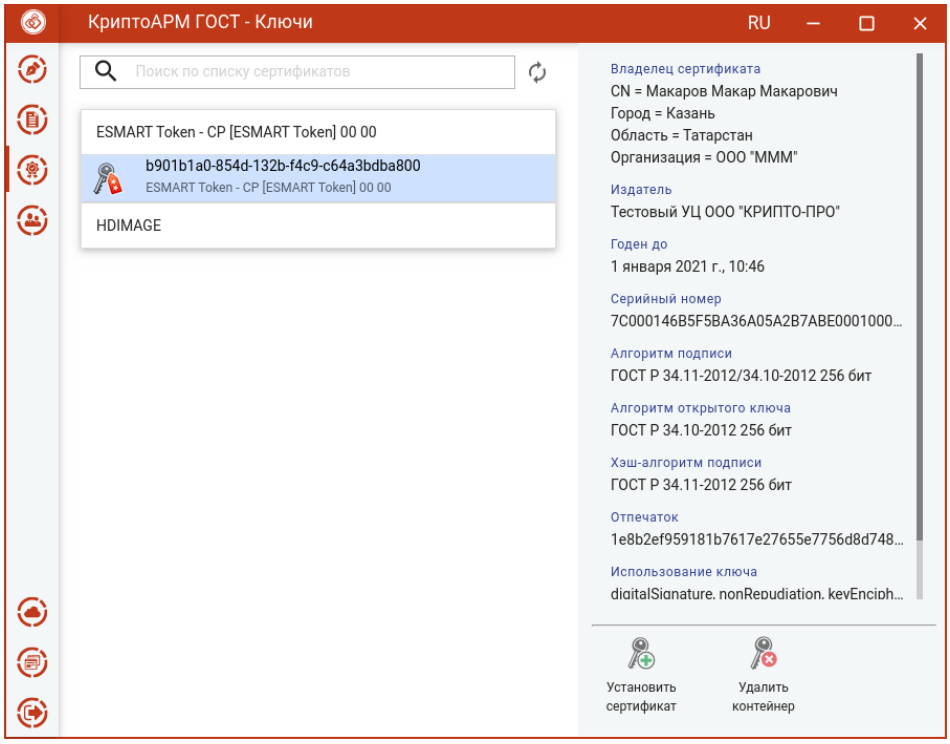
В левой области представления отображаются все подключенные хранилища контейнеров закрытых ключей. В правой области отображается информация о сертификате в выделенном контейнере.



Хранилища контейнеров закрытых ключей

В каждом из хранилищ отображаются контейнеры закрытых ключей. В случае отсутствия контейнеров в хранилище, оно может быть скрыто как пустое.

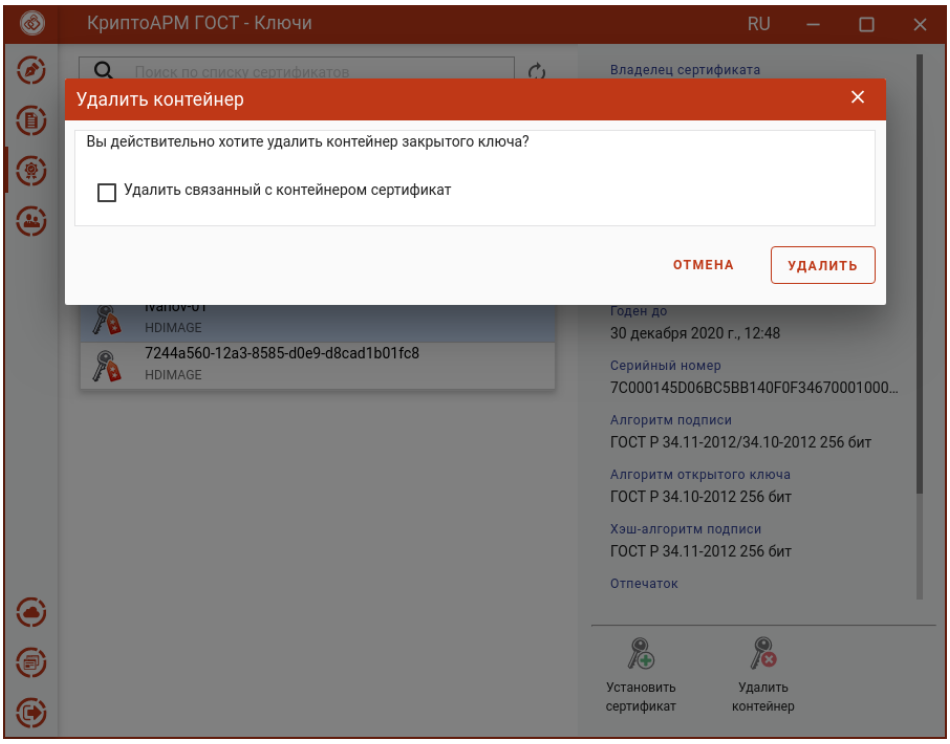
После выбора контейнера отображается информация о находящемся в нем сертификате.



Информация о сертификате в контейнере

По кнопке **Установить сертификат** происходит установка сертификата в **Личное хранилище** сертификатов. Данный сертификат становится доступен для выполнения операций подписи, шифрования и расшифрования.

Для удаления контейнера нужно нажать кнопку **Удалить контейнер** и подтвердить операцию.



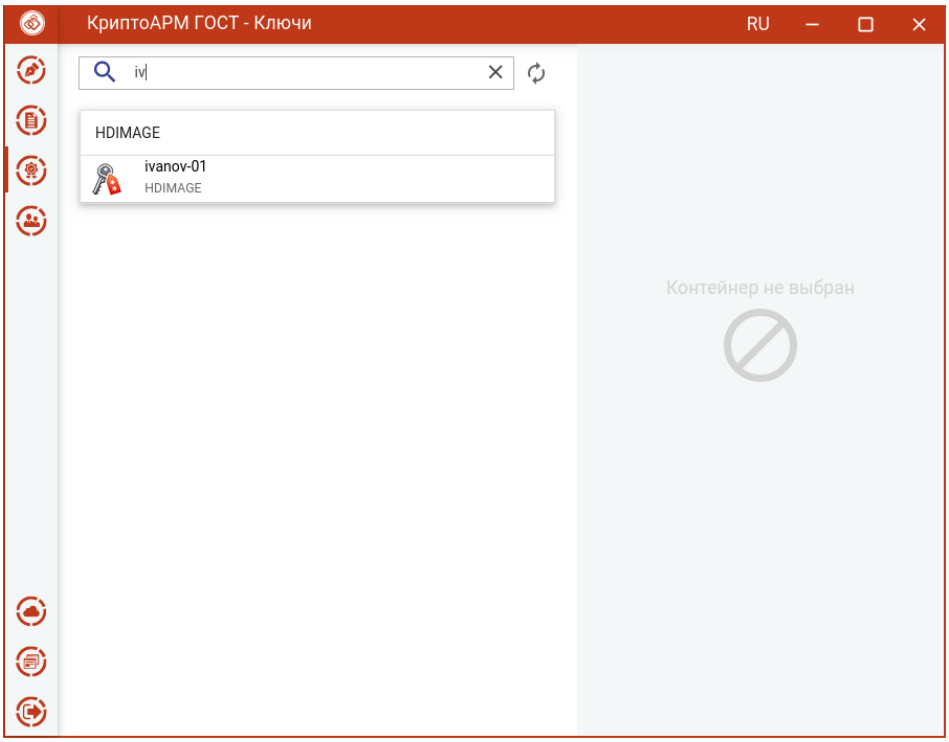
Подтверждение удаления контейнера

Если установить флаг **Удалить связанный с контейнером сертификат**, то вместе с контейнером сертификат удалится из хранилища **Личных сертификатов**.

Если флаг не установлен, сертификат останется в хранилище **Личных сертификатов** без привязки к ключевому контейнеру. Таким сертификатом нельзя выполнять операции подписи и расшифрования.

Примечание. Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.

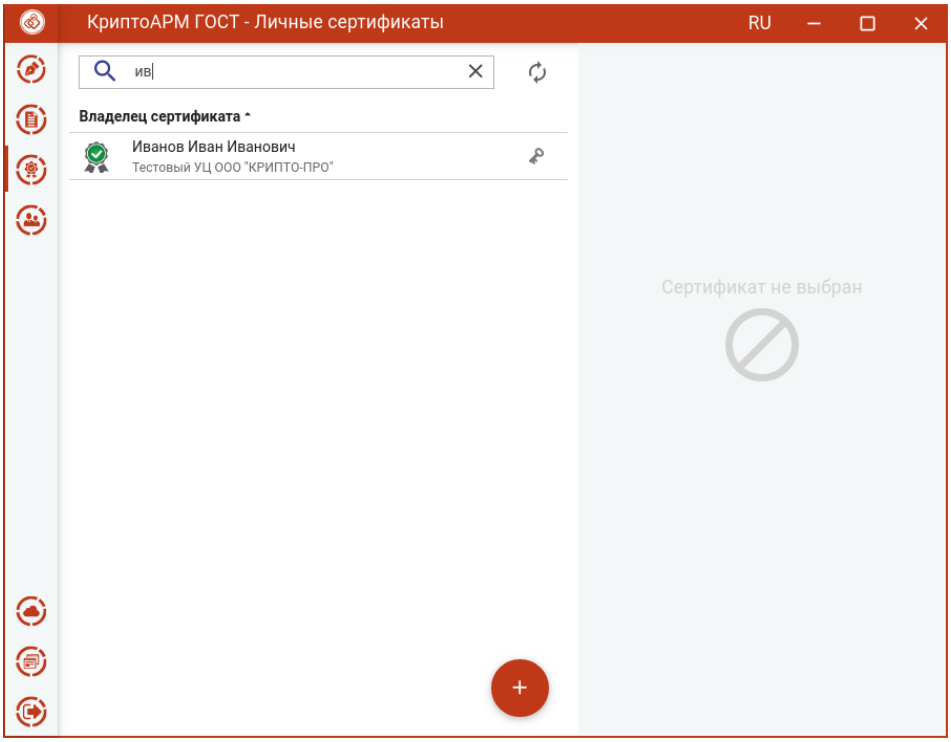
В приложении реализован поиск контейнеров по символьному совпадению в названии контейнера.



Поиск контейнера

5.16.10 Поиск сертификата

В элементах интерфейса, где процесс выполнения операции учитывает выбор сертификата из списка, реализована функция поиска сертификатов. Нужно в строке поиска ввести ключевую фразу.



Поиск сертификата

Поиск сертификатов реализован на основе совпадения ключевой фразы с любым текстовым свойством сертификата. В результате вместо полного списка в окне остаются только сертификаты, удовлетворяющие критерию поиска.

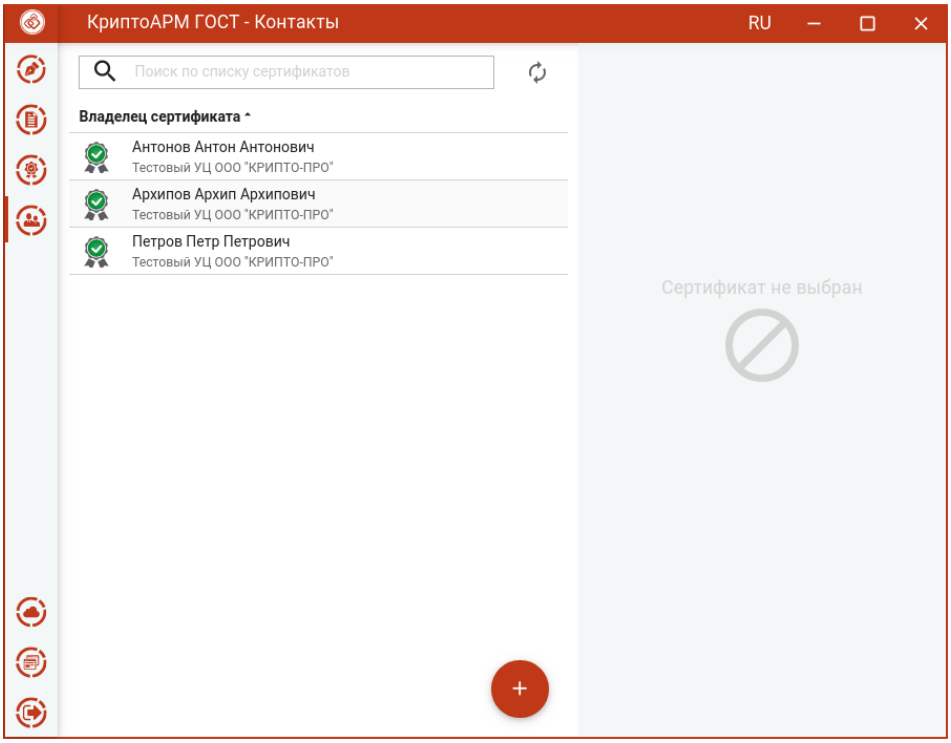
Чтобы отменить фильтр поиска требуется удалить ключевую фразу или нажать на кнопку **Отмена (x)**.

Примечание. В случае неправильно указанного критерия поиска список сертификатов может оказаться пустым, о чем будет свидетельствовать надпись - Сертификаты отсутствуют.

5.17 Контакты

В разделе **Контакты** представлены сертификаты других пользователей, в адрес которых происходит шифрование документов.

Переход в список контактов происходит при выборе пункта меню **Контакты**.

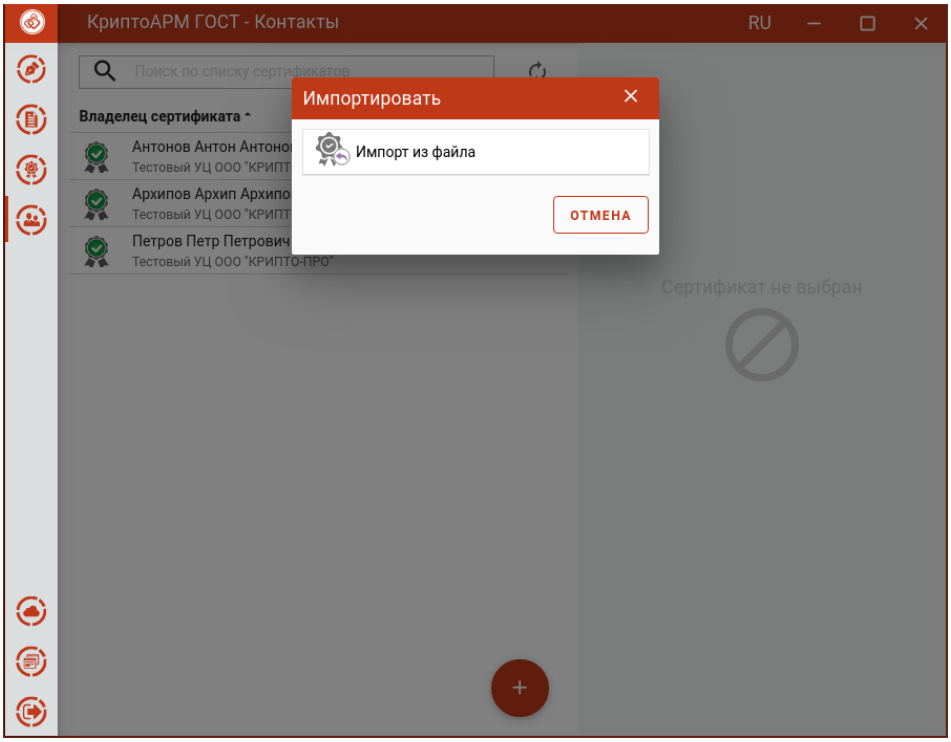


Список контактов

Контакты можно импортировать, экспортировать и удалять. Так же в списке контактов работает поиск.

5.17.1 Импорт контакта

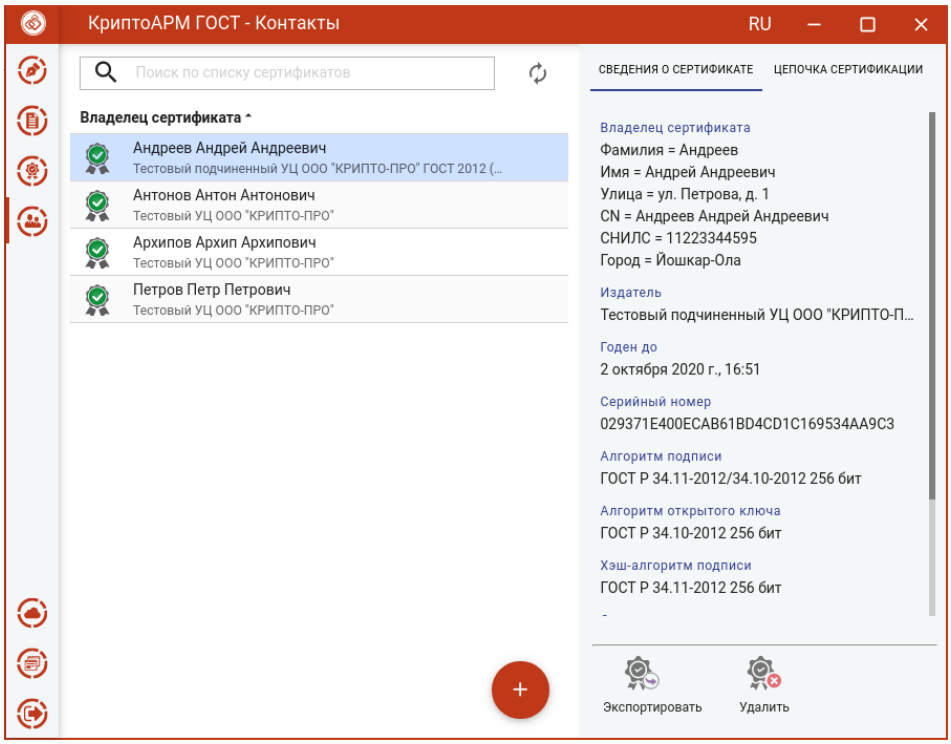
Для импорта контакта нужно в списке нажать кнопку **Добавит (+)** и выбрать опцию **Импорт из файла**.



Импорт контакта

В открывшемся файловом менеджере нужно выбрать файл сертификата.

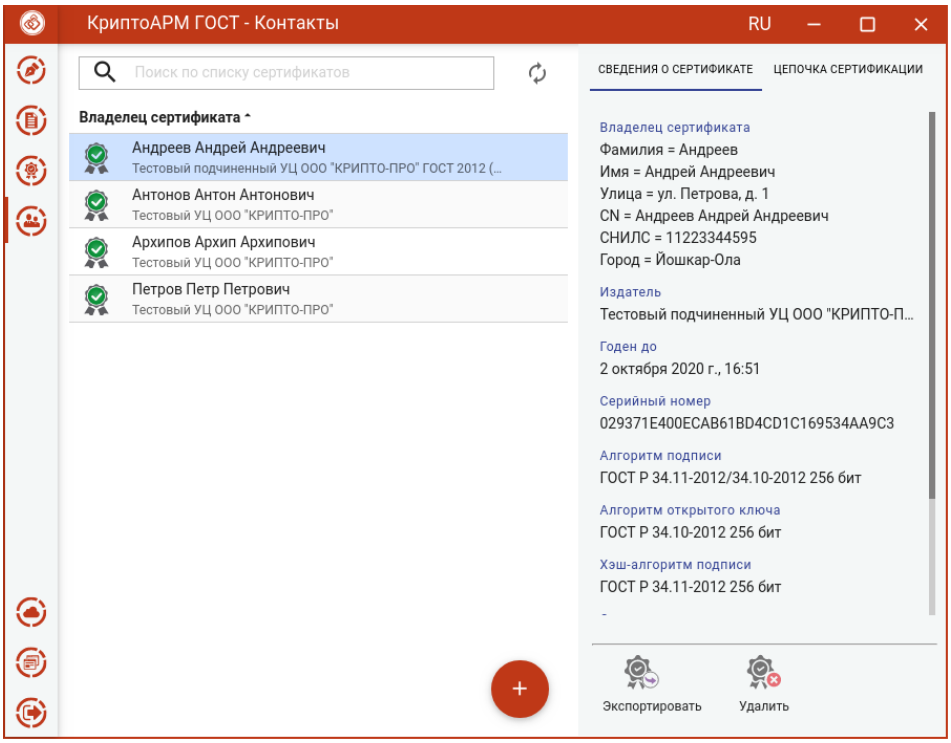
При успешном выполнении операции импорта, контакт появляется в списке, а сертификат автоматически помещается в хранилище сертификатов других пользователей.



Отображение импортированного контакта

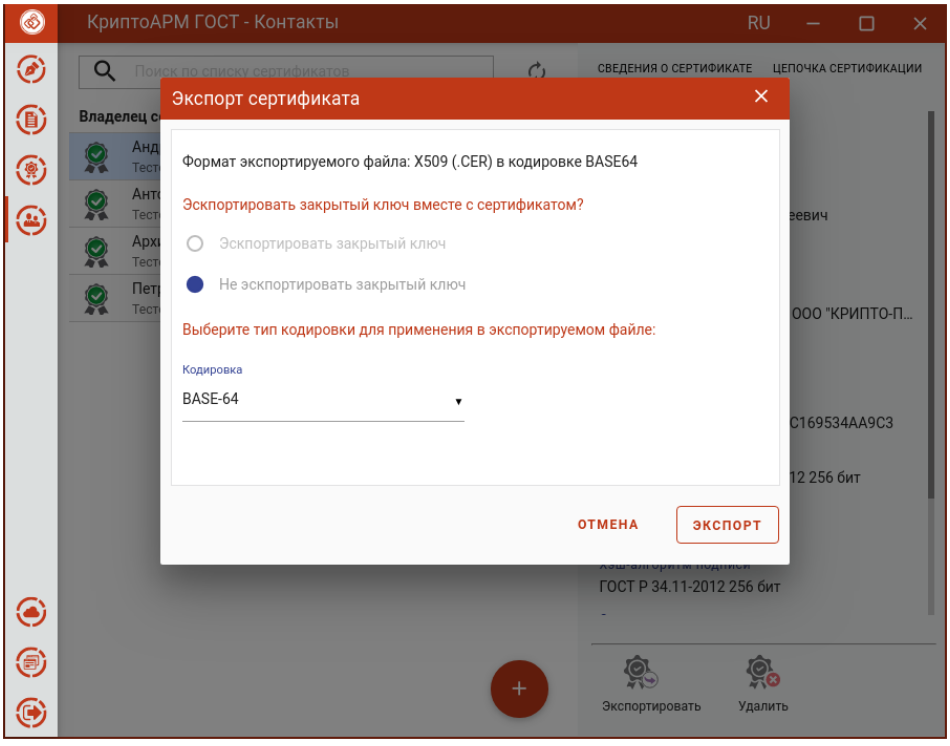
5.17.2 Экспорт контакта в файл

Для экспорта контакта в файл нужно выделить его в списке и нажать кнопку **Экспортировать**.



Экспорт контатка

При экспорте появляется окно, в котором можно выбрать только кодировку файла сертификата.



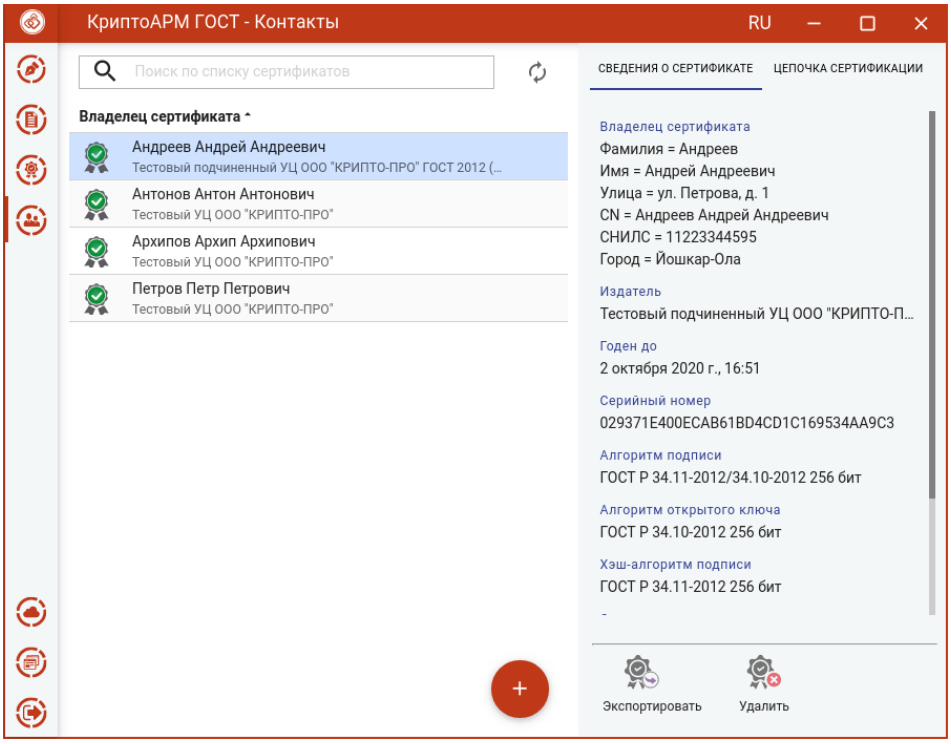
Выбор кодировки файла сертификата

После нажатия кнопки **Экспорт**, в открывшемся файловом менеджере указать путь и имя файла, куда будет сохранен сертификат (по умолчанию, файл export.cer).

По окончании операции возникнет сообщение об успешном экспорте сертификата.

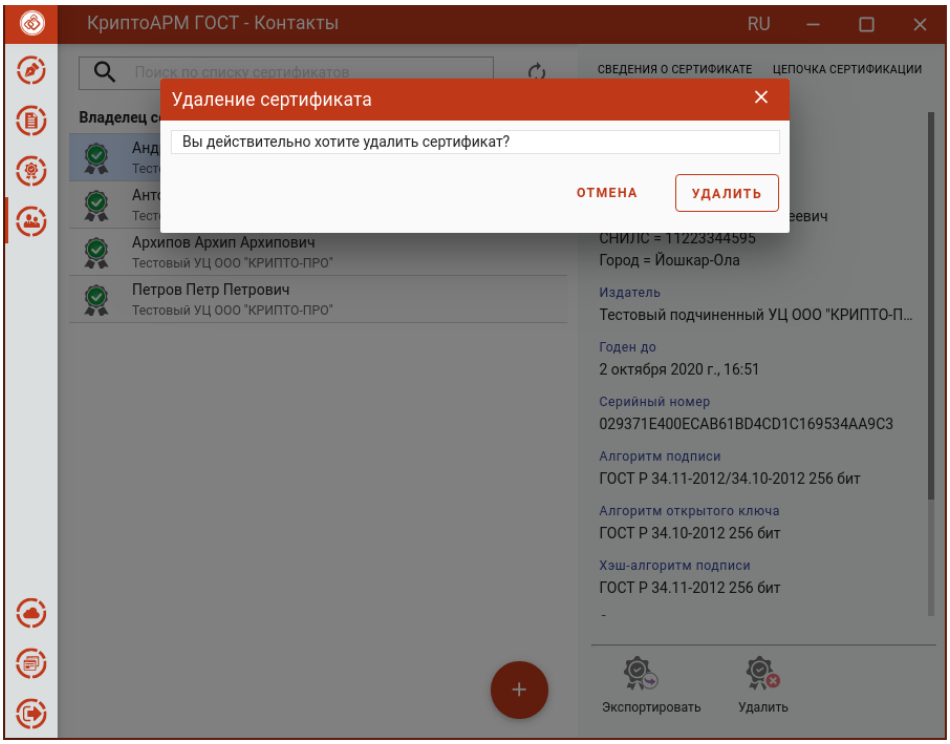
5.17.3 Удаление контакта

Для удаления контакта нужно выбрать операцию **Удалить** на форме просмотра.



Удаление контакта

В появившемся диалоговом окне нажать **Удалить** для подтверждения удаления.

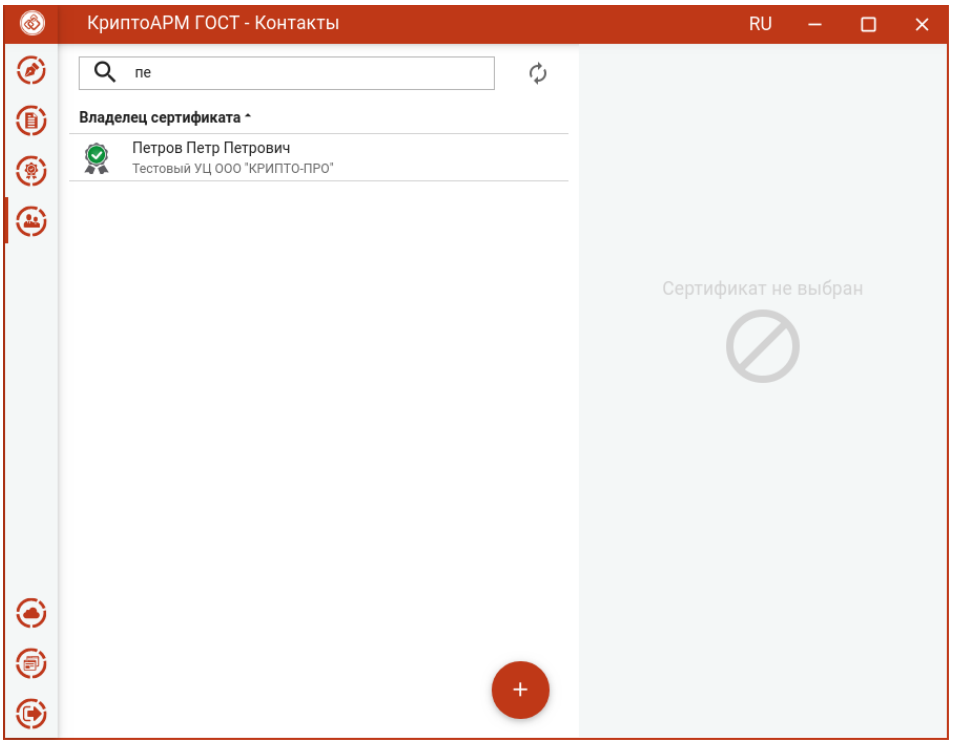


Подтверждение удаления контакта

При успешном удалении появляется сообщение об этом. Сертификат удаляется из списка **Контактов**.

5.17.4 Поиск контакта

Для списка **Контактов** реализован поиск по ключевой фразе. Для этого надо в строке поиска ввести критерий поиска.



Поиск контакта

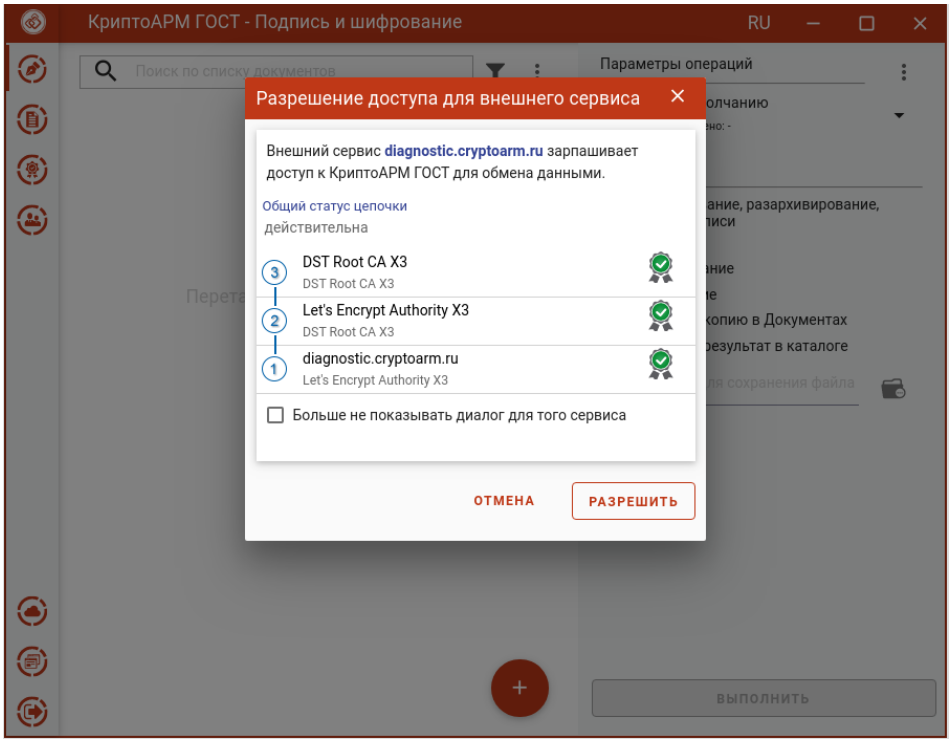
Поиск реализован на основе совпадения ключевой фразы с любым текстовым свойством сертификата. В результате вместо полного списка в окне остаются только контакты, удовлетворяющие критерию поиска.

Чтобы отменить фильтр поиска требуется удалить ключевую фразу или нажать на кнопку **Отмена (x)**.

Примечание. В случае неправильно указанного критерия поиска список контактов может оказаться пусты, о чем будет свидетельствовать надпись - Сертификаты отсутствуют.

5.18 Система доверия к внешним сайтам

Приложение КриптоАРМ ГОСТ может открываться по зарегистрированной ссылке из браузера для выполнения запросов сайта. Для того, чтобы ограничить доступ нежелательных сайтов к приложению, при открытии КриптоАРМ ГОСТ с внешних ресурсов отображается окно с разрешением.



Разрешение на открытие КриптоАРМ ГОСТ с внешнего сервиса

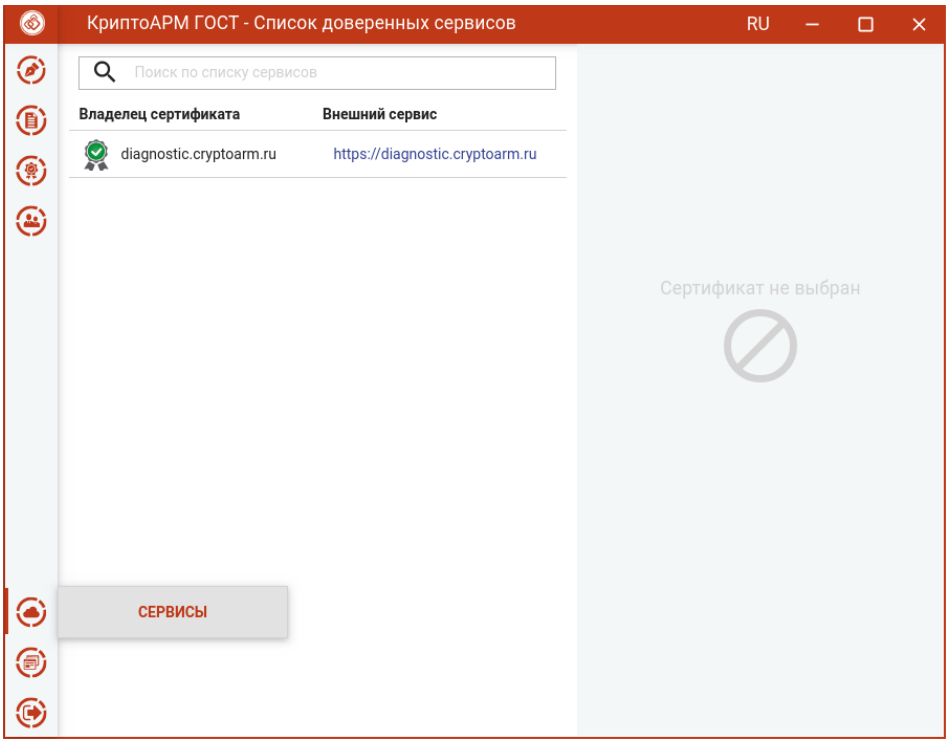
По нажатию кнопки **Разрешить** приложение готово для выполнения запросов сервиса.

При отмене или закрытии окна разрешения обмен данными между внешним сервисом и приложением не выполняется.

При установке флага **Больше не показывать диалог для этого сервиса** и нажатию кнопки **Разрешить** доменное имя сервиса и сертификат сохраняются в список доверенных сайтов. При последующем обращении к КриптоАРМ ГОСТ с этого сайта окно разрешения доступа открываться не будет.

Если сертификаты в цепочке недействительные или цепочка не построилась, то ответственность за разрешение возлагается на пользователя. Для построения действительной цепочки надо установить корневой и промежуточные сертификаты сервиса в соответствующие хранилища.

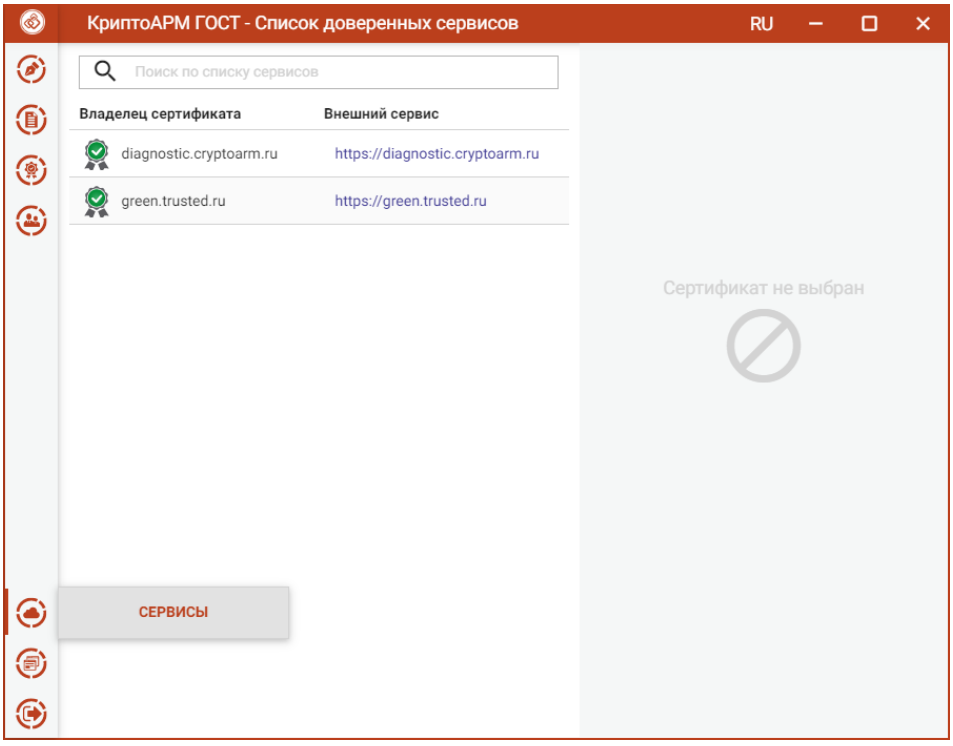
Список доверенных сайтов доступен через пункт меню **Сервисы**.



Переход в список доверенных сайтов

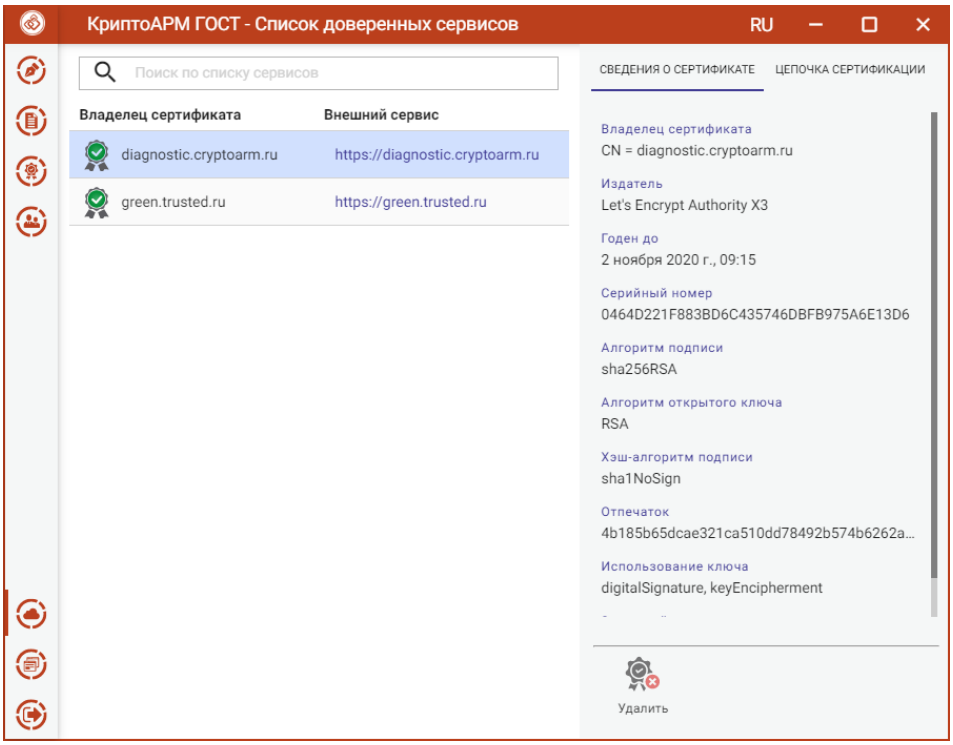
5.18.1 Список доверенных сервисов

Если, при вызове КриптоАРМ ГОСТ по зарегистрированной ссылке из браузера, разрешение для данного сайта было запомнено, то доменное имя сервиса и сертификат сохраняются в список доверенных сайтов. Список доступен из меню **Сервисы**.



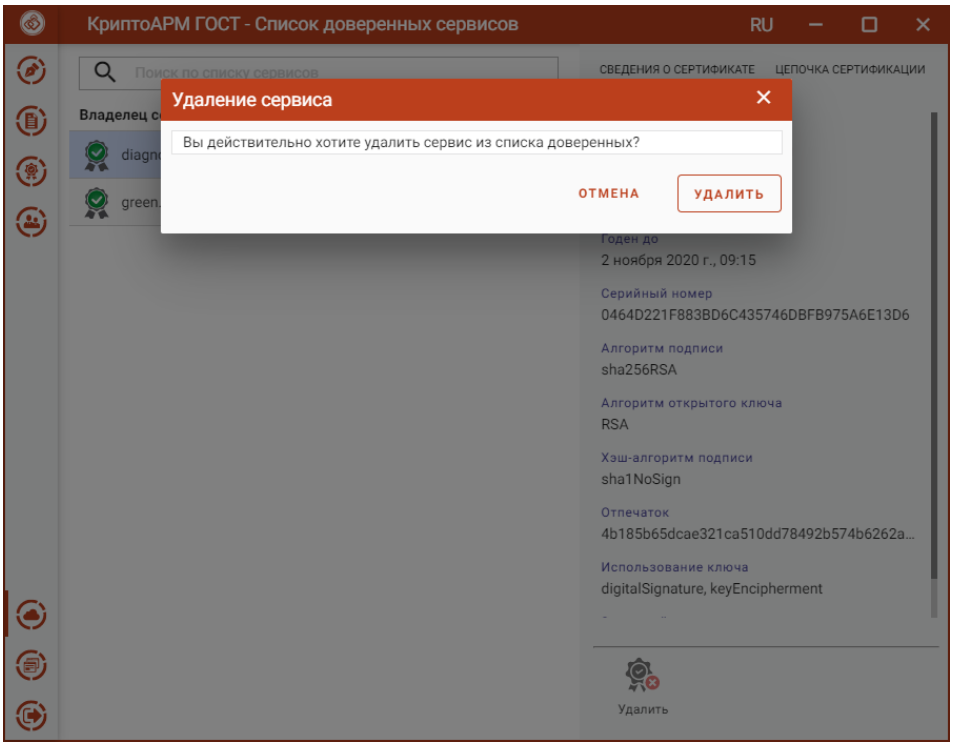
Сервисы

При выделении в списке сервиса отображается информация о его сертификате.



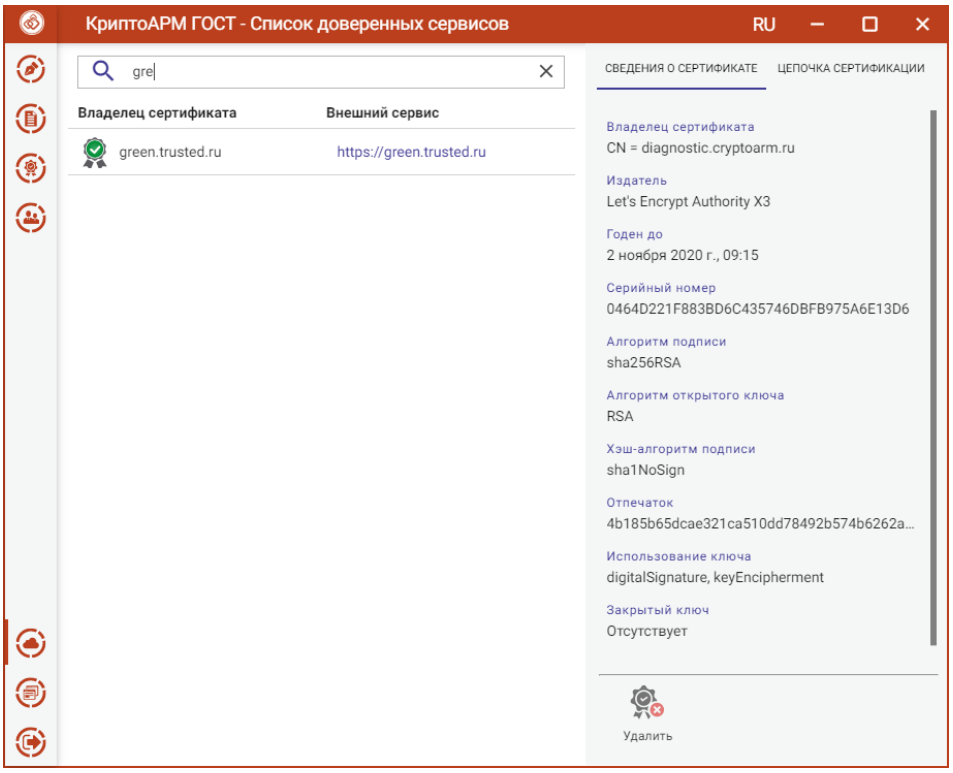
Информация о сервисе

Сервис можно **Удалить**, нажав кнопку на форме просмотра. Открывается окно подтверждения удаления.



Подтверждение удаления сервиса

Для списка сервисов есть поиск по символьному совпадению. В списке отображаются только элементы, удовлетворяющие критериям поиска.

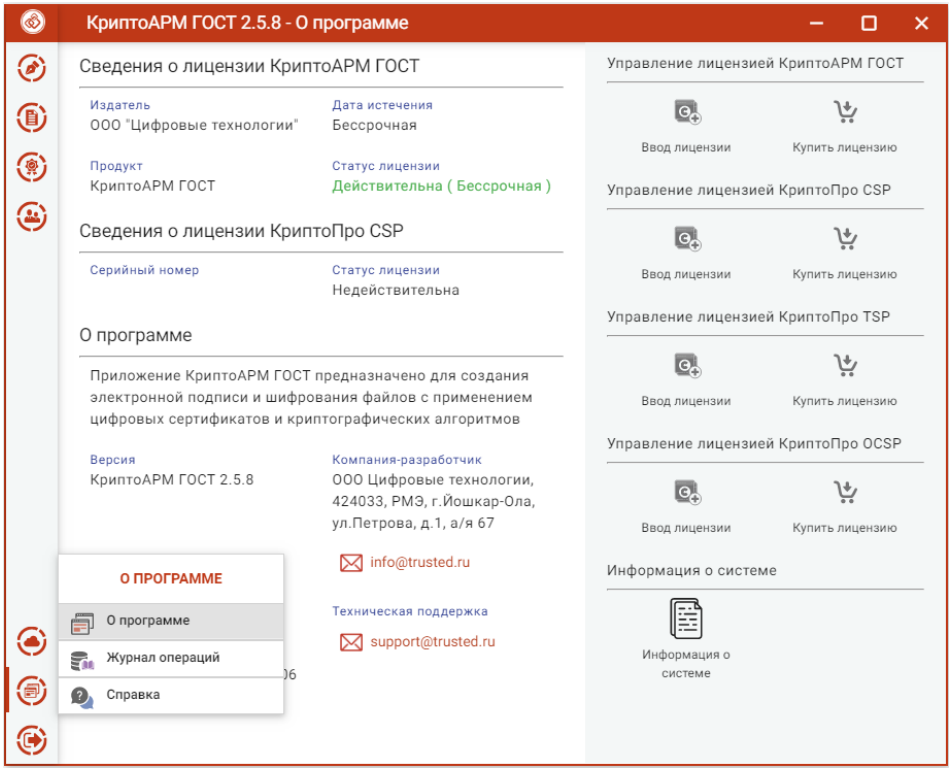


Поиск сервисов

5.19 О программе

Пункт меню **О программе** содержит подпункты:

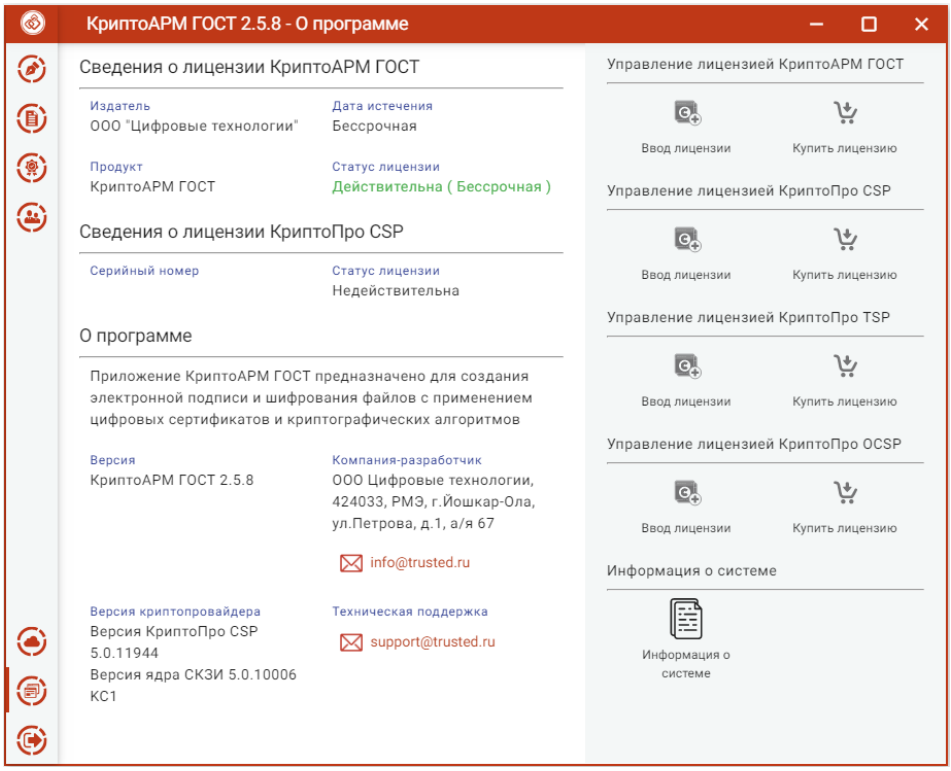
- **О программе** – для отображения краткой информации о приложении и лицензиях;
- **Журнал операций** – для отображения выполняемых операций в приложении;
- **Справка** – для открытия полного руководства пользователя приложения.



Меню О программе

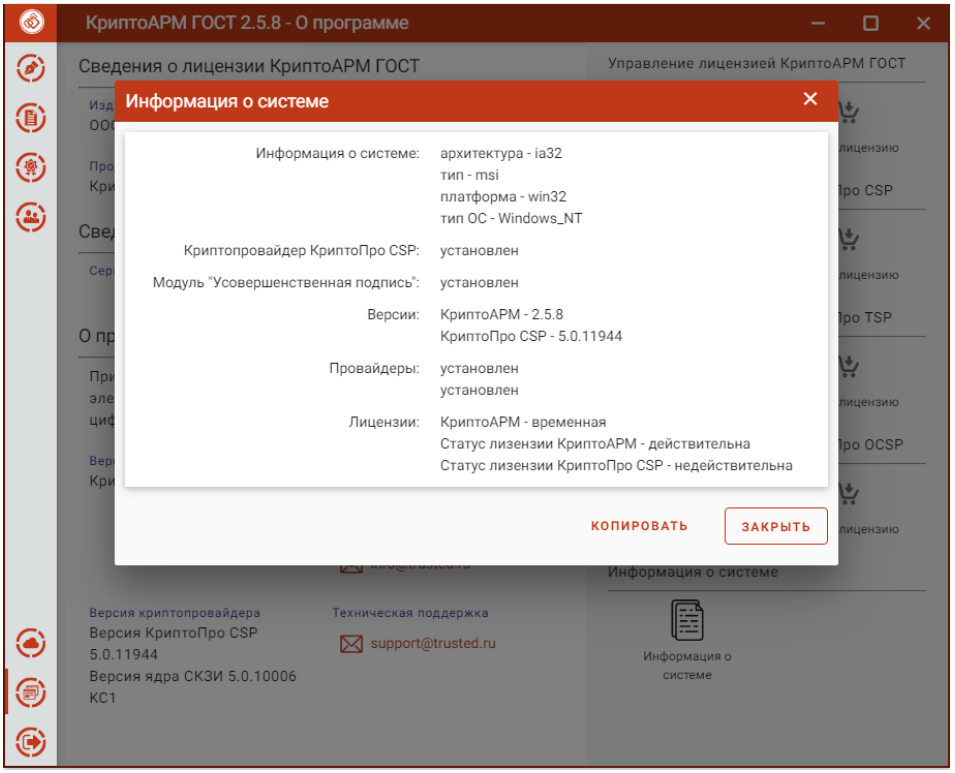
5.19.1 О программе

Краткие сведения о программе, лицензиях на КриптоАРМ ГОСТ и КриптоПро CSP, контактные данные компании - разработчика, а так же адрес электронной почты для получения дополнительной технической поддержки, можно узнать, выбрав подпункт **О программе**.



Информация о программе

Информация о системе необходима при обращении в техническую поддержку.

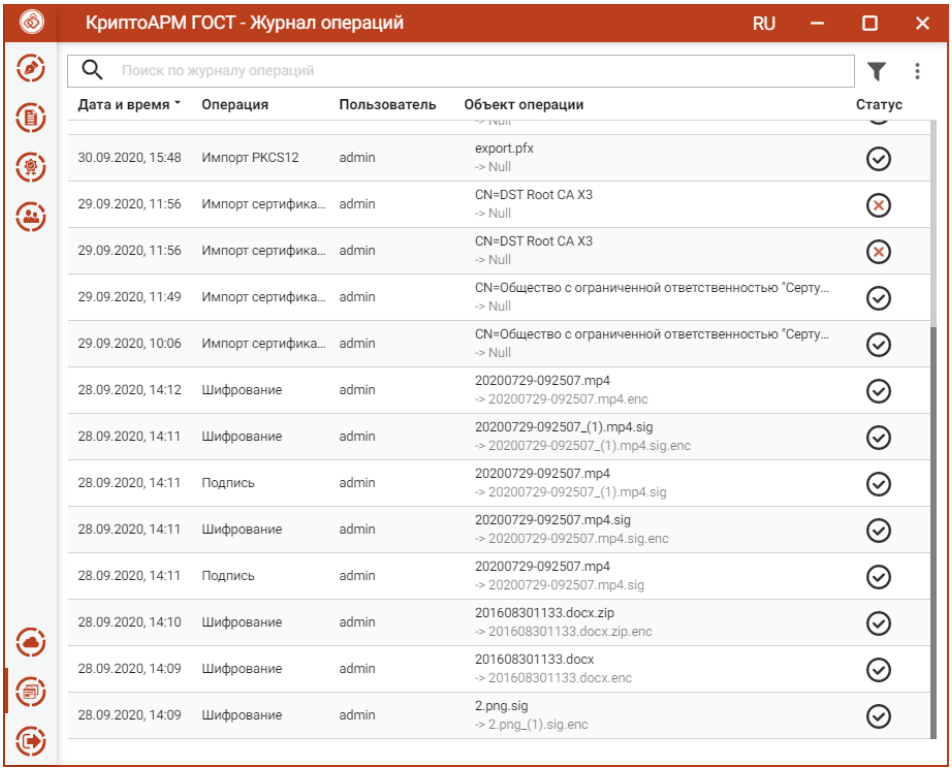


Информация о системе

Для этого нужно скопировать информацию в буфер обмена кнопкой **Копировать** и вставить в текс обращения в техническую поддержку с описанием вопроса или проблемы.

5.19.2 Журнал операций

Журнал операций предназначен для отображения операций, выполняемых пользователем.



Журнал операций

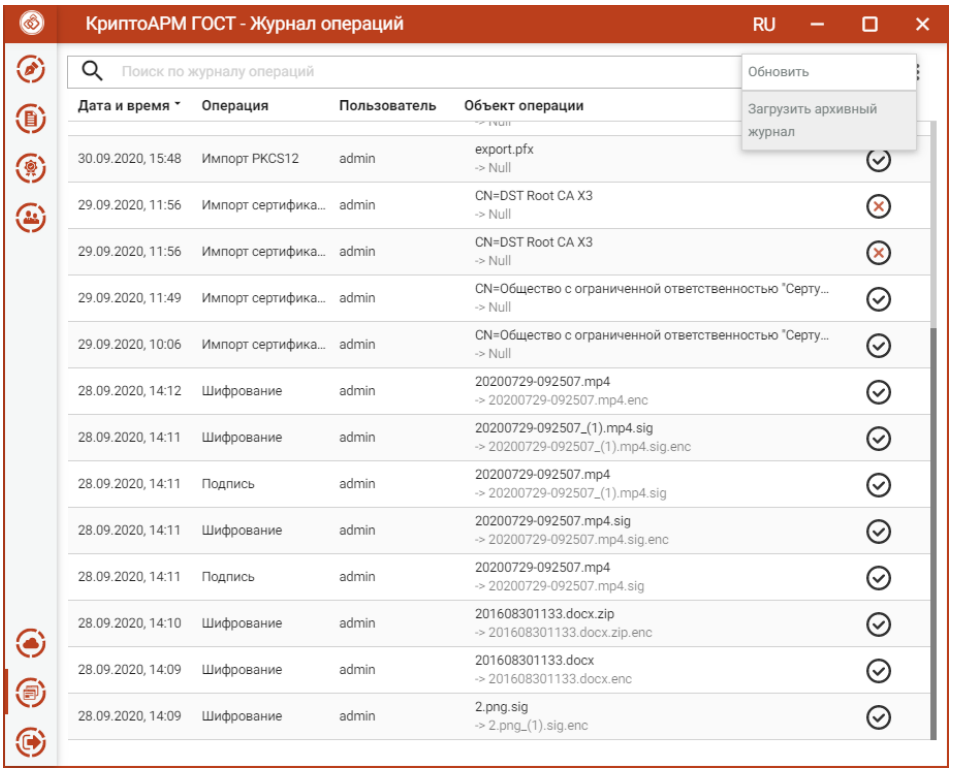
В журнале отображаются следующие типы операций:

- подпись;
- снятие подписи;
- шифрование;
- расшифрование;
- генерация сертификата;
- генерация запроса на сертификат;
- импорт сертификата;
- импорт сертификата в формате pkcs#12;
- удаление сертификата;
- удаление контейнера.

Текущая версия **Журнала операций** записывается в файл cryptoarm_gost_operations[порядковый номер журнала].log, который находится в папке пользователя в катаалоге .Trusted.

По мере накопления записей выполняется автоматический переход к новому файлу журнала со следующим порядковым номером.

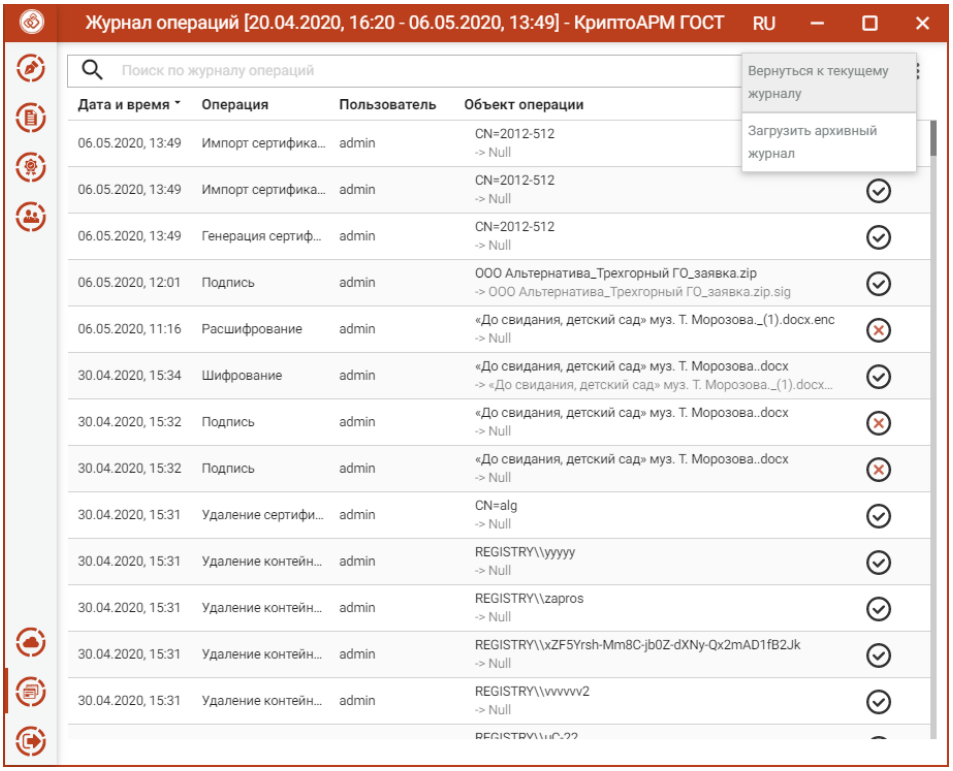
При работе с журналом операций предусмотрен режим загрузки ранее сохраненного архива для просмотра, поиска и фильтрации записей. Для этого используется пункт **Загрузить архивный журнал** контекстного меню журнала.



Контекстное меню журнала операций

По кнопке **Обновить** контекстного меню происходит обновление записей в **Журнале операций**.

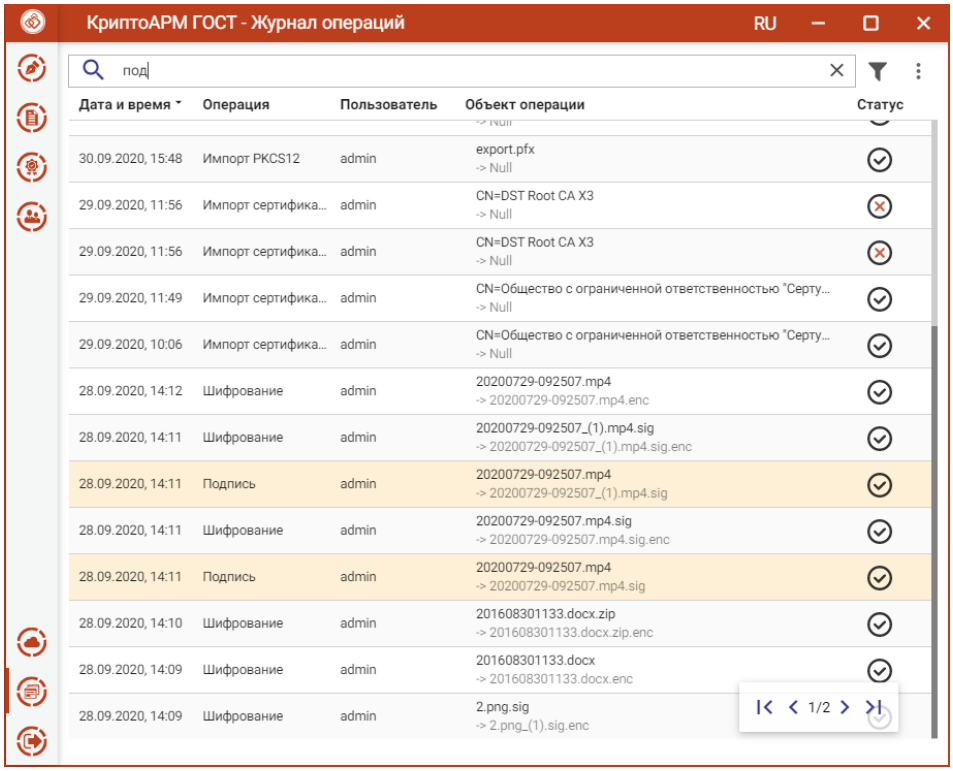
Для возврата к текущему журналу операций используется пункт контекстного меню **Вернуться к текущему журналу.**



Контекстное меню архивного журанала операций

5.19.2.1 Поиск записей в журнале операций

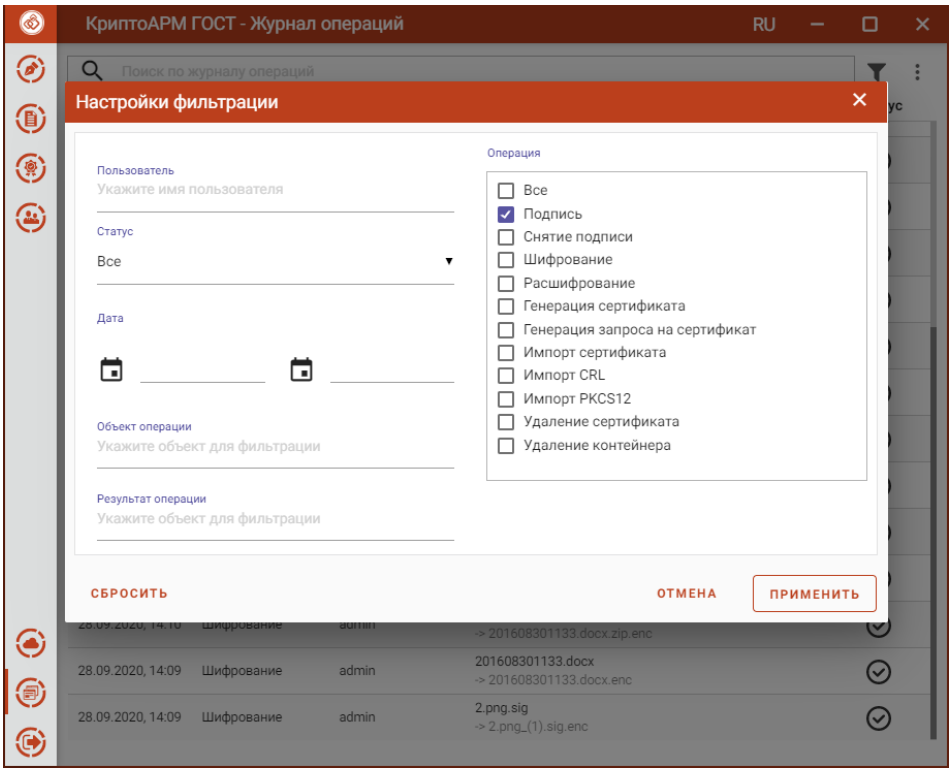
В приложении реализован поиск записей **Журнала операций** по символьному совпадению.



Поиск записей в журнале операций

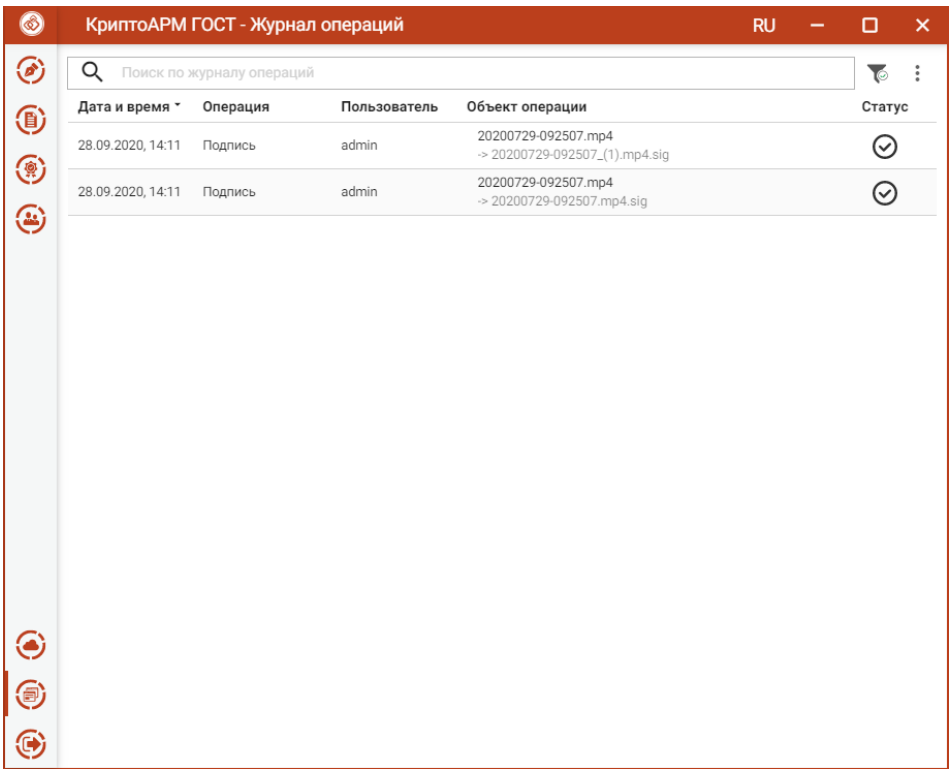
5.19.2.2 Фильтрация журнала операций

Для открытия окна настроек критериев фильтра на панели управления имеется кнопка, при нажатии на которую открывается окно настроек фильтрации.



Настройки критериев фильтра журнала операций

Применение фильтрации выполняется по нажатию кнопки **Применить**. В зависимости от выставленных критериев фильтра, в журнале остаются только те записи, которые удовлетворяют (суммарно) этим критериям.



Результат применения фильтрации журнала операций

Для сброса заданных критериев служит кнопка **Сбросить** в окне настроек фильтрации.

5.19.3 Справка

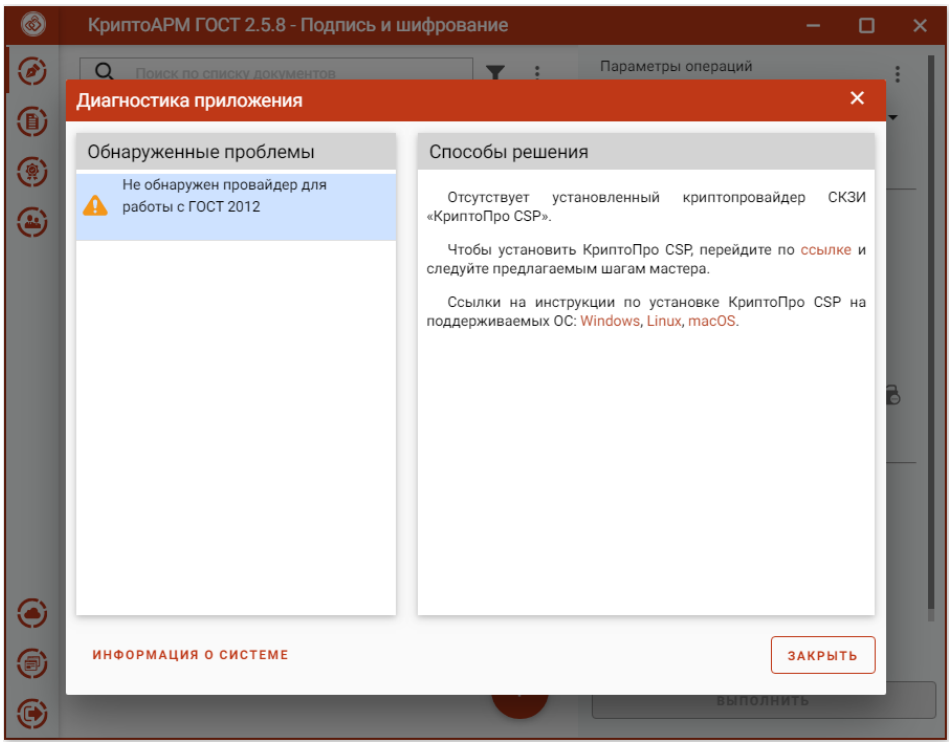
При выборе пункта меню **Справка** открывается руководство пользователя приложения КриптоАРМ ГОСТ.

6 Диагностика неполадок при запуске приложения

При обнаружении проблем, затрудняющих дальнейшую работу приложения КриптоАРМ ГОСТ, запускается мастер диагностики приложения. В мастере подробно описываются возникшие неполадки и способы их решения.

6.1 Отсутствует СКЗИ КриптоПро CSP

Приложение КриптоАРМ ГОСТ не работает без установленного в системе СКЗИ КриптоПро CSP. В таком случае при запуске приложения будет предупреждающее сообщение.



Сообщение об отсутствии СКЗИ КриптоПро CSP

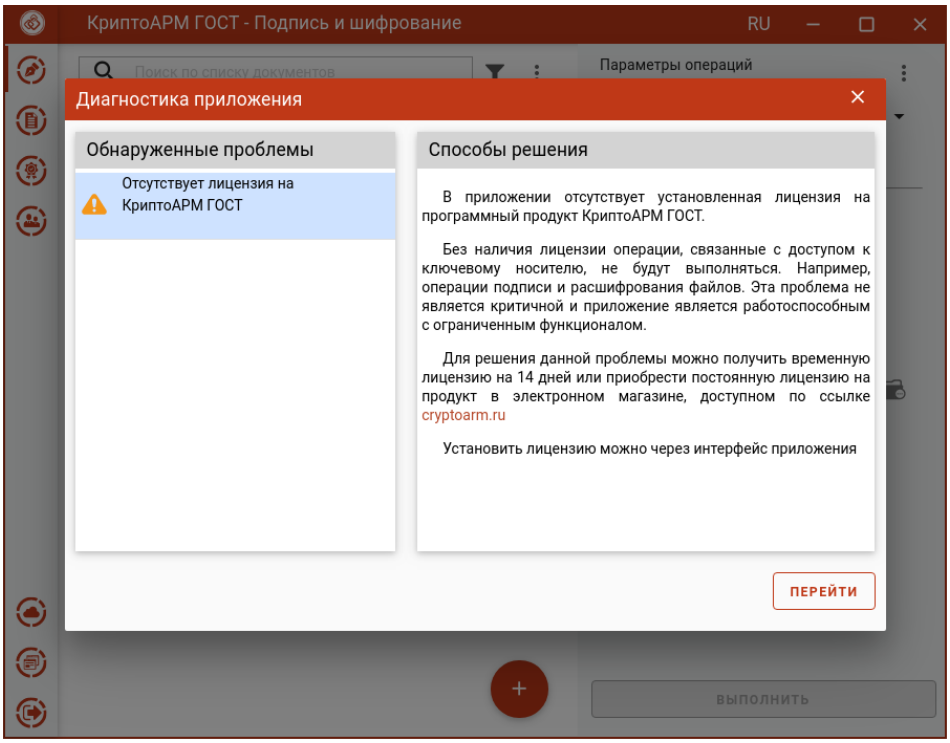
Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Инструкция по установке СКЗИ КриптоПро CSP описана в п.Установка криптопровайдера КриптоПро CSP.

Информация о системе служит для копирования в буфер обмена и последующей вставки в текст обращения в техническую поддержку.

6.2 Отсутствует лицензия на КриптоАРМ ГОСТ

Без установленной лицензии на программный продукт КриптоАРМ ГОСТ при запуске приложения возникает предупреждающее сообщение.



Сообщение об отсутствии лицензии на КриптоАРМ ГОСТ

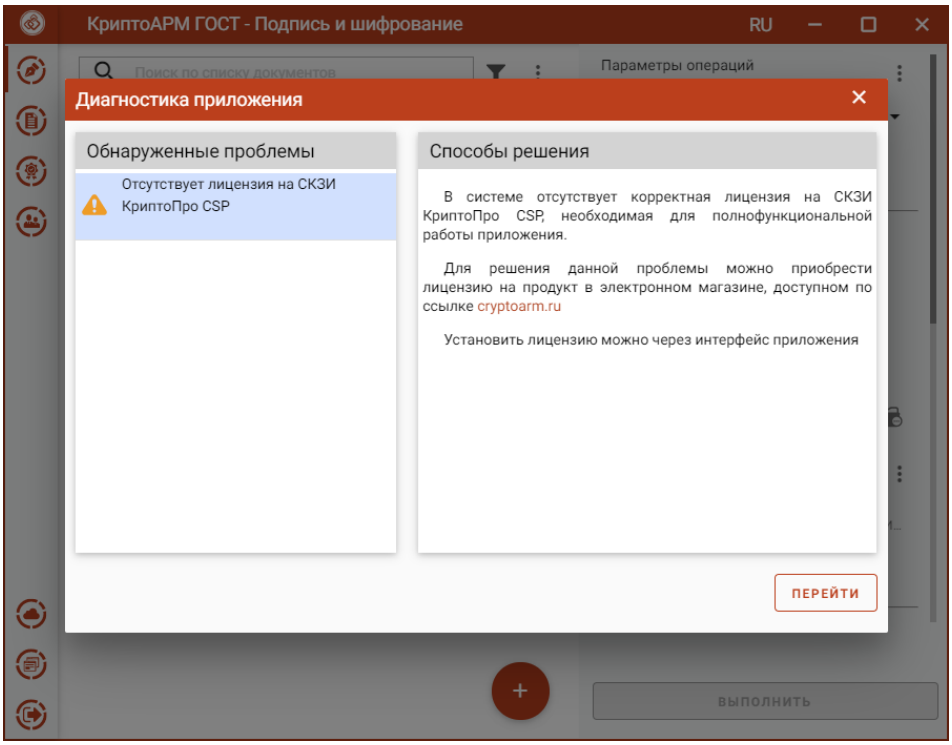
По кнопке **Перейти** происходит переход на вкладку **О программе**, где можно установить лицензию.

При закрытии мастера диагностики приложение остается работоспособным, но с ограниченным функционалом. Без лицензии не будут выполняться операции, связанные с доступом к закрытому ключу (например, подпись и расшифрование).

Инструкция по установке лицензии в приложении КриптоАРМ ГОСТ описана в п. Установка лицензии на программный продукт данного руководства.

6.3 Отсутствует лицензия на КриптоПро CSP

Без установленной лицензии на программный продукт КриптоПро CSP при запуске приложения возникает предупреждающее сообщение.



Сообщение об отсутствии лицензии на КриптоПро CSP

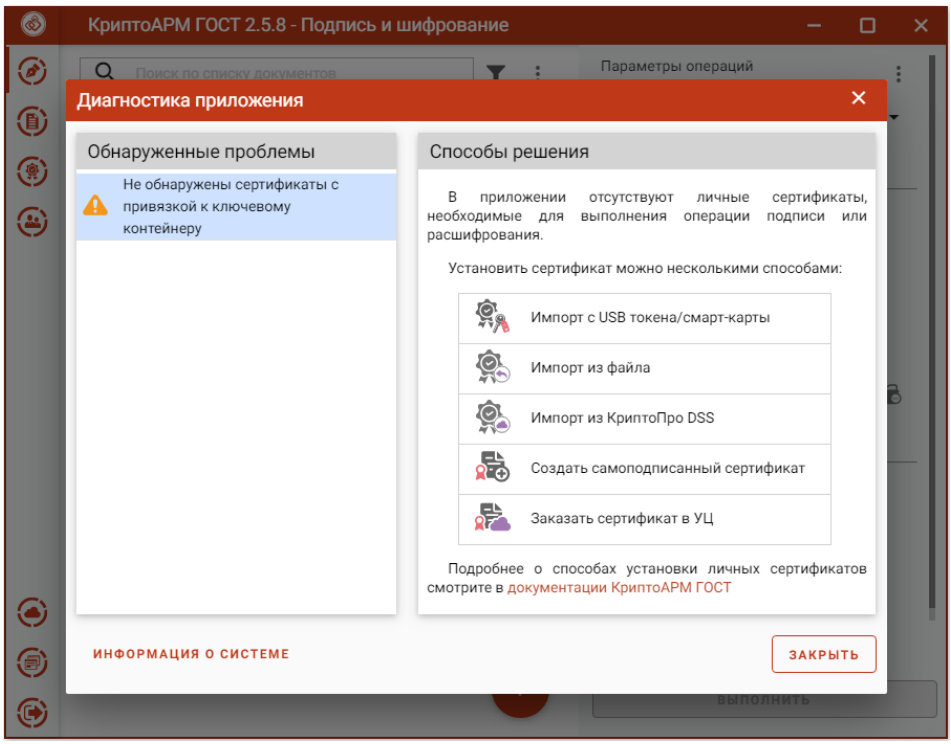
По кнопке **Перейти** происходит переход на вкладку **О программе**, где можно установить лицензию.

При закрытии мастера диагностики приложение остается работоспособным, но с ограниченным функционалом. Без лицензии не будут выполняться операции, связанные с доступом к закрытому ключу (например, подпись и расшифрование).

Инструкция по установке лицензии в приложении КриптоПро CSP описана в п. Установка лицензии на программный продукт.

6.4 Не обнаружены сертификаты с привязкой к ключевому контейнеру

При отсутствии в личном хранилище сертификатов, с привязкой к закрытому ключу, при запуске приложения возникает предупреждающее сообщение и способы решения.



Сообщение об отсутствии сертификатов с привязкой к закрытому ключу

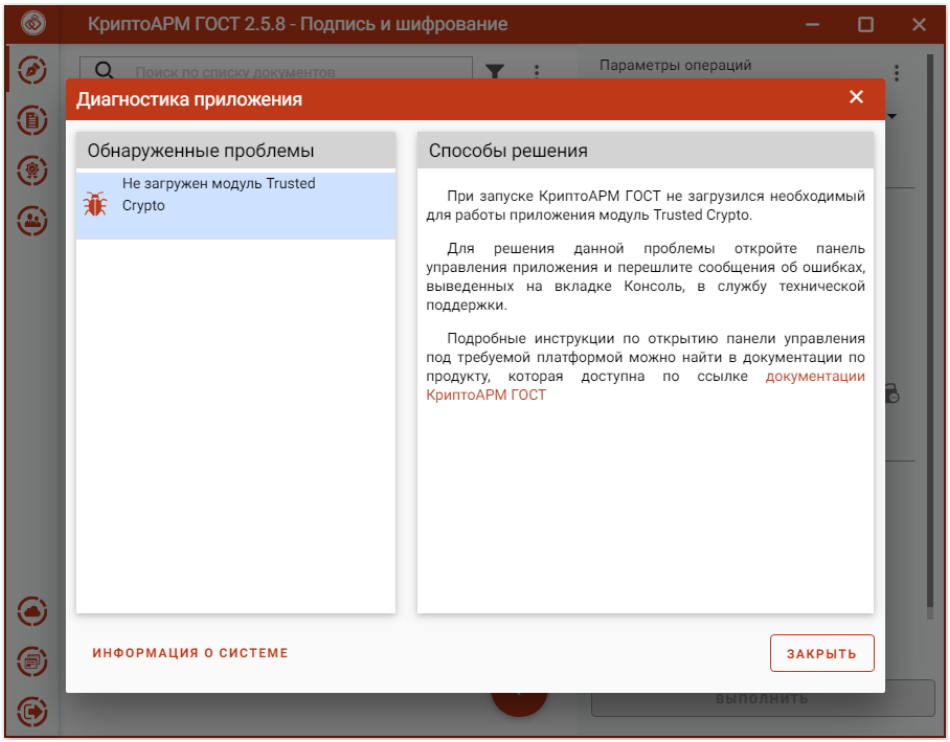
Добавить личный сертификат можно несколькими способами:

- импортировать с USB токена/смарт-карты - при выборе открывается вкладка **Ключи**, где нужно выбрать контейнер и установить сертификат (подробнее Установка сертификата из ключевого контейнера);
- импортировать из файла – открывается файловый менеджер для выбора файла сертификата (подробнее Импорт личного сертификата с привязкой к закрытому ключу);
- импортировать из КриптоПро DSS – открывается окно ввода адресов серверов DSS и логина пользователя (подробнее Импорт сертификата из DSS);
- создать самоподписанный сертификат – открывается форма создания запроса на сертификат (подробнее Создание самоподписанного сертификата);
- заказать сертификат в УЦ – происходит переход на сайт подбора электронной подписи.

Информация о системе служит для копирования в буфер обмена и последующей вставки в текст обращения в техническую поддержку.

6.5 Не загружен модуль Trusted Crypto

Приложение КриптоАРМ ГОСТ не работает без модуля Trusted Crypto. В таком случае при запуске приложения будет предупреждающее сообщение.



Сообщение об ошибке в модуле Trusted Crypto

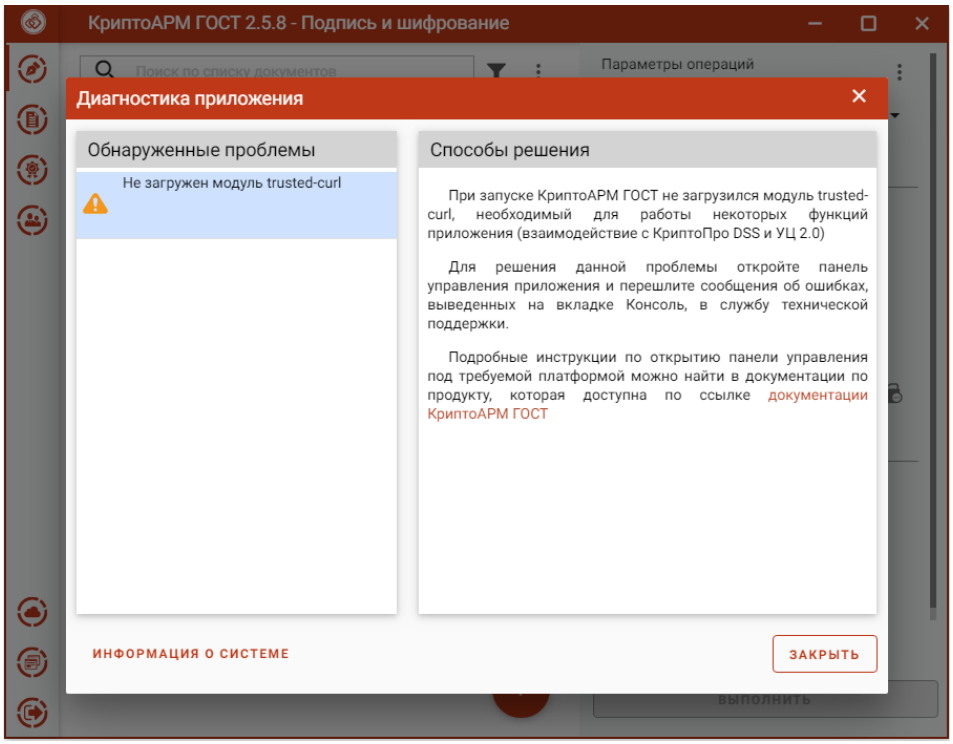
Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Для решения данной проблемы необходимо запустить приложение в консольном режиме, скопировать информацию об ошибке и связаться со специалистами технической поддержки продукта КриптоАРМ ГОСТ. Так же в текс обращения следует включить сведения о системе, скопировав ее нажатием на **Информацию о системе**.

Инструкция по включению консольного режима описана в пункте Включение режима логирования и консоль управления данного руководства.

6.6 Не загружен модуль Trusted Curl

Приложение КриптоАРМ ГОСТ без модуля Trusted Crypto остается работоспособным. Без данного модуля невозможно использовать сертификаты DSS и получать сертификаты через КриптоПро УЦ 2.0.



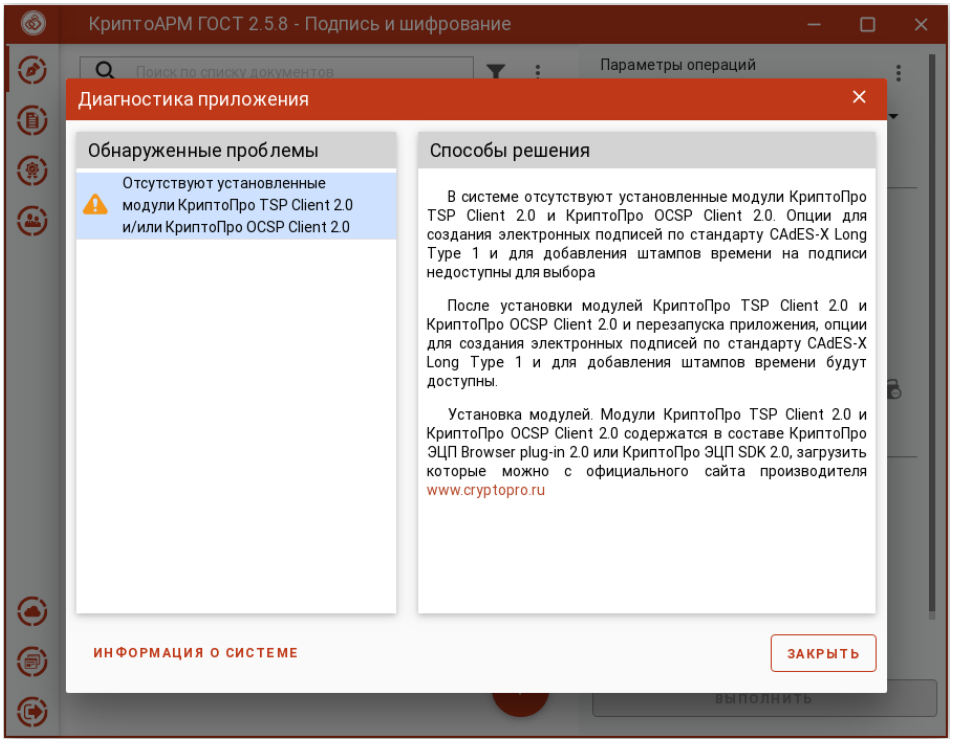
Сообщение об ошибке в модуле Trusted Curl

Для решения данной проблемы необходимо запустить приложение в консольном режиме, скопировать информацию об ошибке и связаться со специалистами технической поддержки продукта КриптоАРМ ГОСТ. Так же в текс обращения следует включить сведения о системе, скопировав ее нажатием на **Информацию о системе**.

Инструкция по включению консольного режима описана в пункте Включение режима логирования и консоль управления данного руководства.

6.7 Отсутствуют установленные модули КриптоПро TSP Client 2.0/OCSP Client 2.0

При отсутствии модулей КриптоПро TSP Client 2.0 или КриптоПро OCSP Client 2.1 возникает информационное сообщение.



Сообщение об отсутствии установленных модулей TSP/OCSP

Приложение остается работоспособным, но без возможности создавать усовершенствованную подпись или подпись со штампом времени.

Как установить данные модули, описано в пункте установки КриптоПро CSP.

Информация о системе служит для копирования в буфер обмена и последующей вставки в текст обращения в техническую поддержку.

7 Включение режима логирования и консоль управления

Приложение КриптоАРМ ГОСТ построено на основе браузера, в котором исполняются скрипты, написанные на языке JavaScript и отображается интерфейс приложения. Ошибки, которые возникают при работе интерфейсной части приложения, связанные с проблемами подключения модулей и других компонент можно отследить в консоли управления, которую предоставляет браузер.

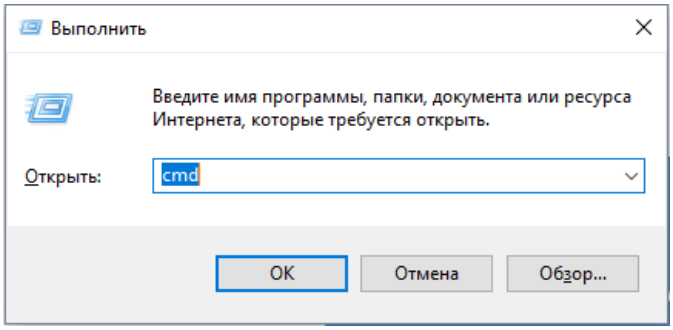
Открыть браузерную консоль приложения КриптоАРМ ГОСТ можно, запустив приложение из командной строки и указав параметр **devtools**. Данная команда открывает окно с инструментарием для веб-разработки, где одной из вкладок будет представление консоли.

Для более глубокого анализа причин возникновения ошибок используется включение режима логирования, то есть сохранение служебной информации о выполненных операциях в текстовый файл. Данный режим включается указанием параметра **logcrypto** при запуске приложения из командной строки.

Особенности включения этих режимов при работе с приложением на различных платформах представлены в следующих подраздела.

7.1 Отслеживание ошибок на платформе MS Windows

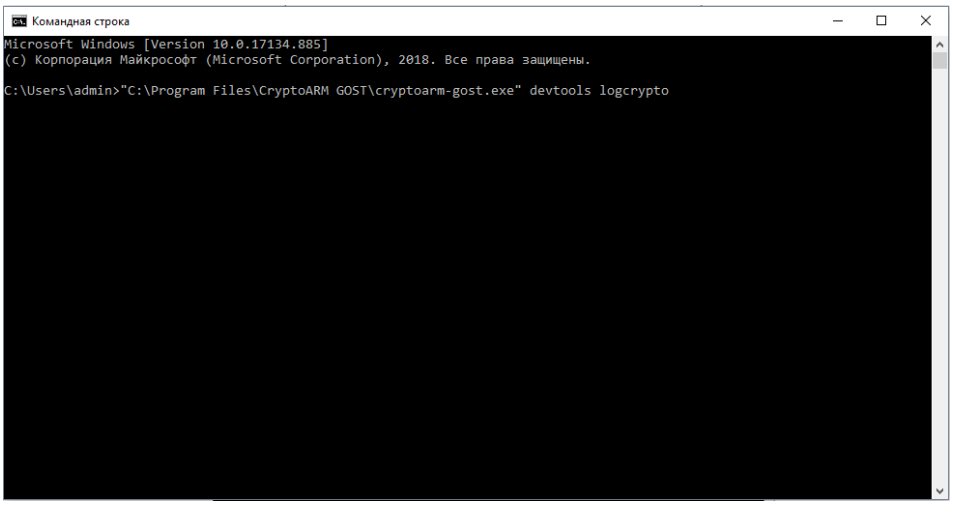
Для запуска командной строки нажать Win+R. Ввести команду cmd и ОК



Диалог для запуска приложений

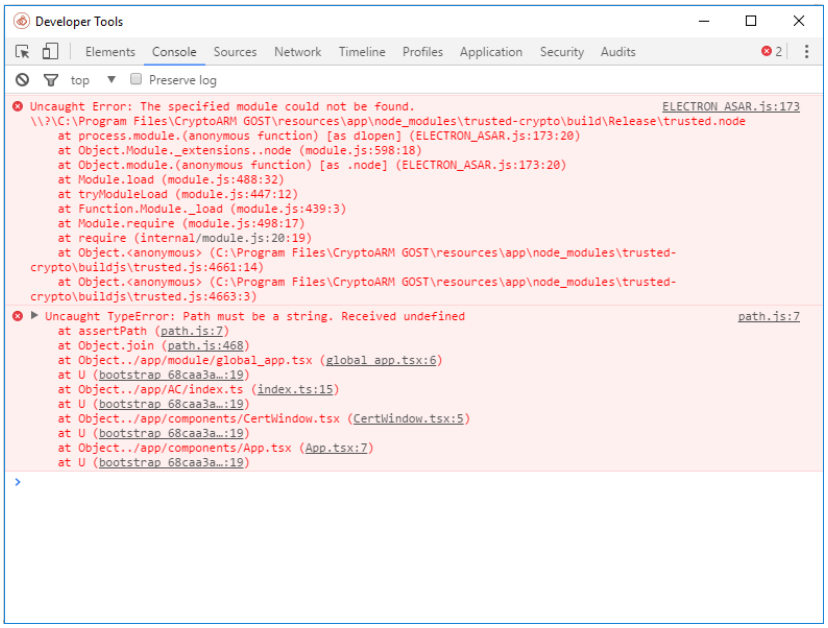
В открывшемся окне ввести команду запуска приложения КриптоАРМ ГОСТ:

"C:\Program Files\CryptoARM GOST\cryptoarm-gost.exe" devtools logcrypto



Диалог командной строки

В результате выполнения этой команды откроется приложение КриптоАРМ ГОСТ с дополнительной панелью управления и сохранением информации об операциях в журнал логирования.



Окно с вкладкой консоли управления

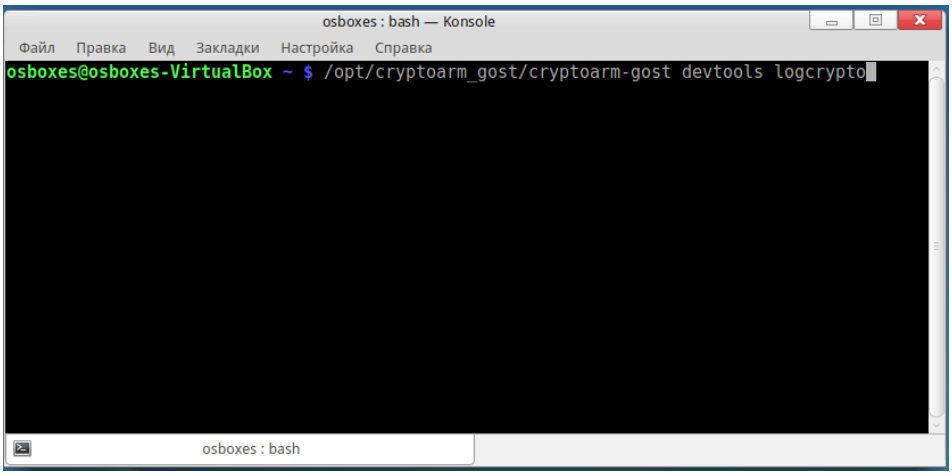
При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

Журнал логирования представляет собой текстовый файл cryptoarm_gost.log, который располагается в каталоге пользователя в папке .Trusted.

7.2 Отслеживание ошибок на платформе Linux

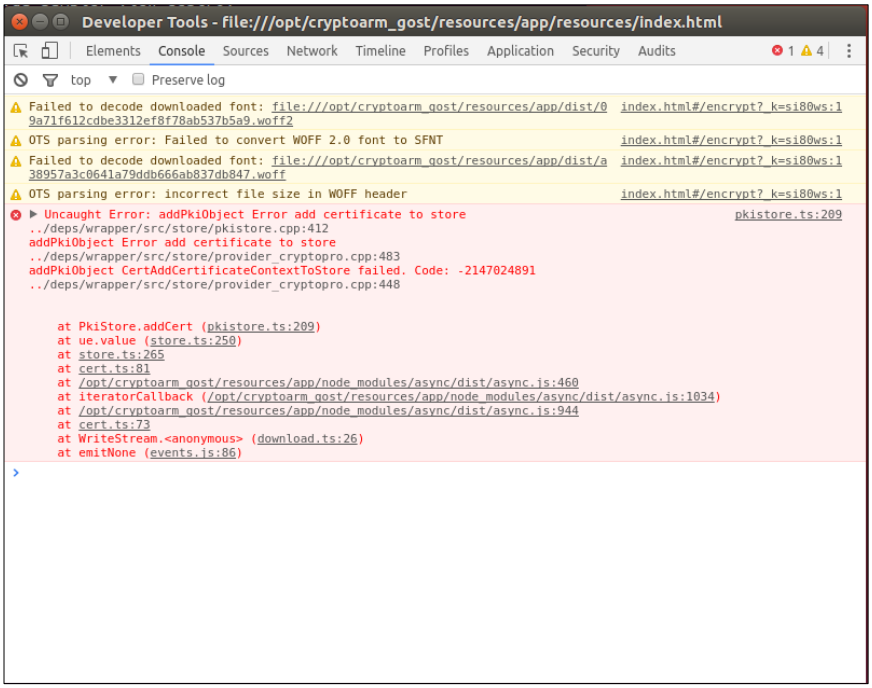
Для получения доступа к дополнительной панели управления приложением и включением режима логирования, в терминале ОС Linux нужно ввести команду:

/opt/cryptoarm_gost/cryptoarm-gost devtools logcrypto



Окно терминала

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне на вкладке Console отобразится текст ошибки.



Окно с вкладкой консоли управления

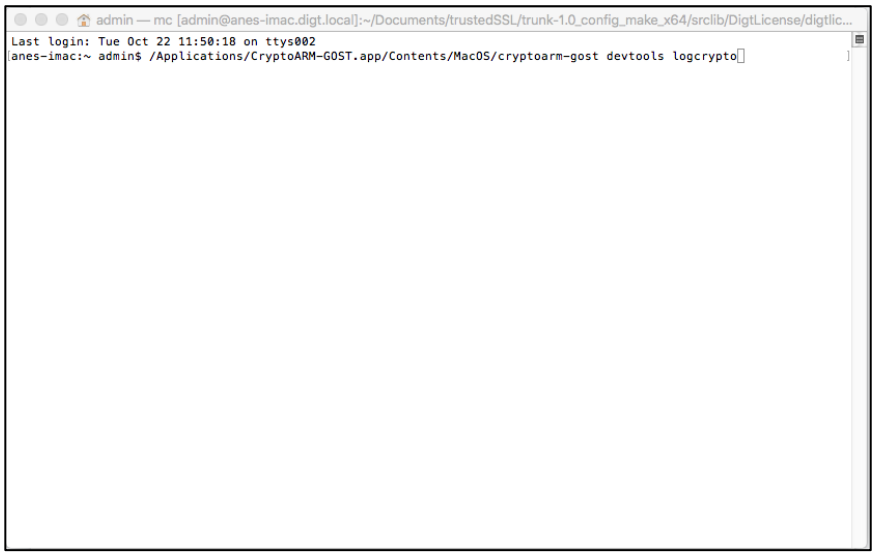
При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

Журнал логирования представляет собой текстовый файл cryptoarm_gost.log, который располагается в каталоге пользователя в папке .Trusted.

7.3 Отслеживание ошибок на платформе OS X

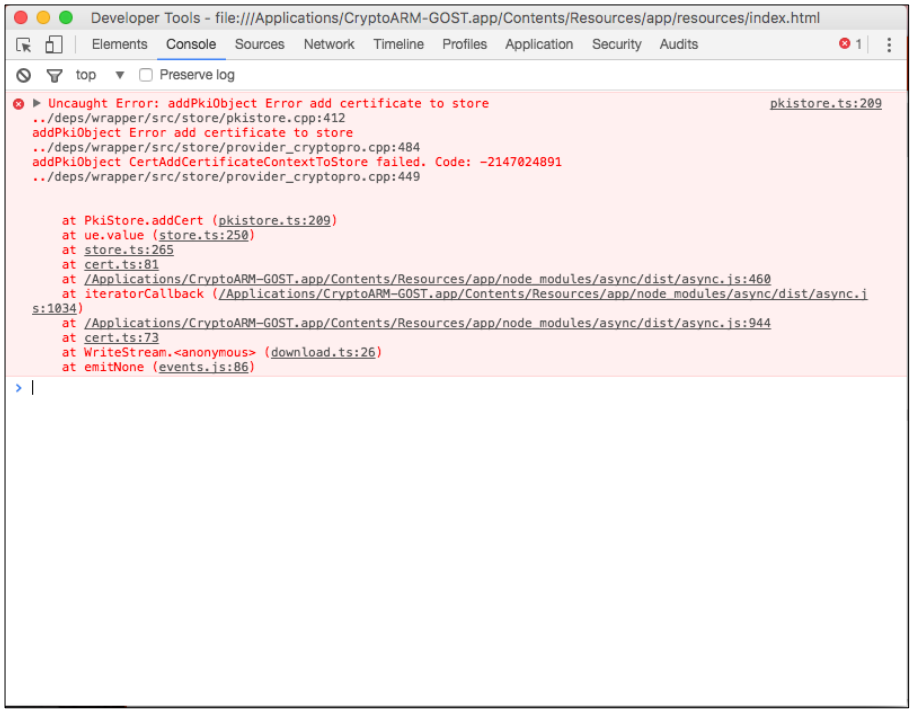
Для получения доступа к дополнительной панели управления приложением и включением режима логирования, в терминале ОС OS X ввести команду:

/Applications/CryptoARM-GOST.app/Contents/MacOS/cryptoarm-gost devtools logcrypto



Окно терминала

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне на вкладке Console отобразится текст ошибки.



Окно с вкладкой консоли управления

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

Журнал логирования представляет собой текстовый файл cryptoarm_gost.log, который располагается в каталоге пользователя в папке .Trusted.

8 Управление сертификатами и ключами с помощью командной строки

8.1 Перенос контейнера закрытого ключа под требуемую операционную систему

Для примера рассмотрим наиболее часто встречающуюся задачу переноса контейнера закрытого ключа из операционной системы Windows под Linux или OS X. Если в операционной системе Windows сертификат и закрытый ключ могут находится в локальном хранилище Crypto API, то для работы под операционными системами Linux или OS X его нужно импортировать в специальное системное хранилище. Важно, у закрытого ключа должен быть установлен флаг «Экспортируемый».

Перенос выполняется в два шага – экспорт контейнера и сертификата, импорт контейнера и установка сертификата в личное хранилище:

В операционной системе Windows скопировать контейнер закрытого ключа можно следующим образом. Откройте приложение КриптоПро CSP и перейдите на вкладку **Сервис**. На вкладке выберите команду **Скопировать контейнер закрытого ключа**. Введите пароль для ключевого контейнера и задайте имя ключевого контейнера (например, test). Сохраните контейнер на диск или флешку. После этого откройте диалог Сертификаты (должна запуститься консоль MMC), перейдите в раздел **Личное, Реестр, Сертификаты** и экспортируйте сертификат без закрытого ключа с помощью мастера. Сохраните его в файл (например, test.cer).

Для импорта импортировать сертификата под операционными системами Linux (OS X) выполните следующие действия. Скопируйте контейнер закрытого ключа (директорию /test/ в формате 8.3) и файл сертификата (test.cer) из корня дискеты или флешки в директорию /var/opt/cprocsp/keys/имя_пользователя. При этом необходимо проследить чтобы: владельцем файлов был пользователь, в директории с именем которого расположен контейнер (от его имени будет осуществляться работа с ключами); на директорию с ключами были выставлены права, разрешающие владельцу всё, остальным ничего; на файлы были выставлены права, разрешающие владельцу по крайней мере чтение и запись, остальным ничего.

- Проверить, отображается ли контейнер можно командой

  /opt/cprocsp/bin/<arch>/csptest -keyset -enum_cont -fqcn -verifycontext

- Привязать сертификат к закрытому ключу можно командой

  /opt/cprocsp/bin/<arch>/certmgr -inst -store uMy -file /var/opt/cprocsp/keys/<сертификат>.cer -cont '\\.\HDIMAGE\test' –pin ***

- Выполнить проверку привязки сертификата к закрытому ключу можно через команду

  /opt/cprocsp/bin/<arch>/certmgr -list -store uMy

  в результате выполнения предыдущей команды должно быть выведено сообщение **PrivateKey Link: Yes. Container: HDIMAGE\\test.000\.**

В приведенных выше командах под **<arch>** подразумеваться один из следующих идентификаторов платформы: **ia32** - для 32-разрядных систем Linux; **amd64** - для 64-разрядных систем Linux; **не указывается** - для OS X.

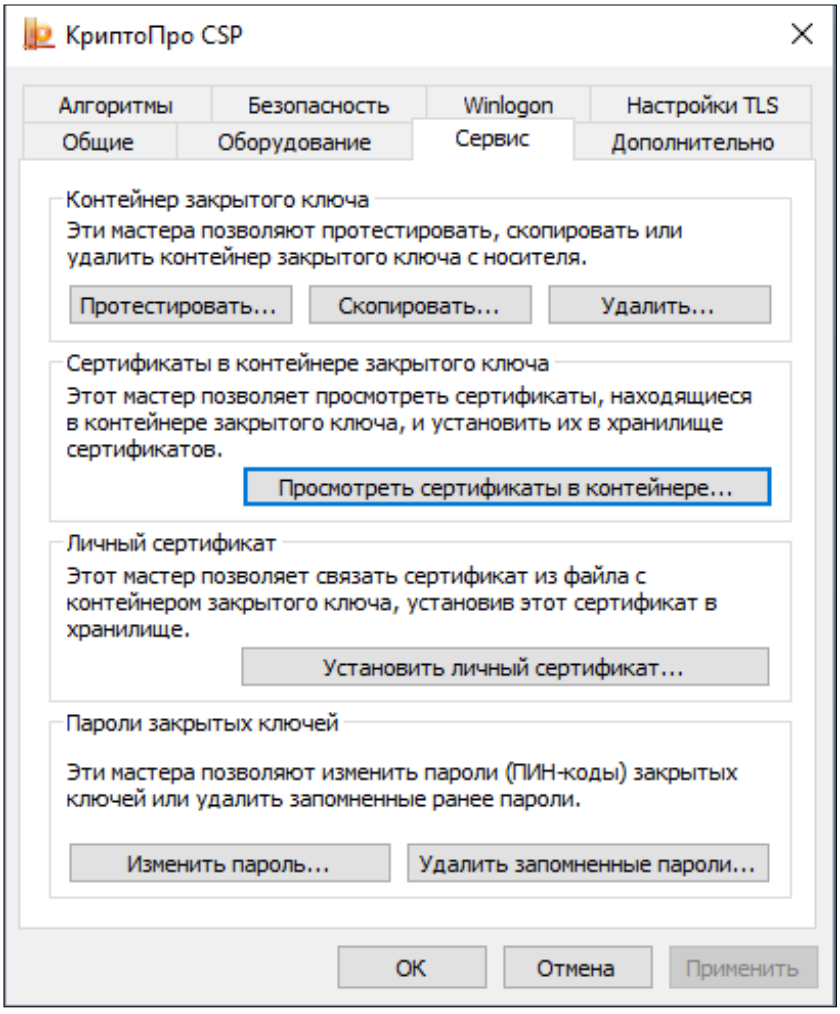
8.2 Установка сертификата с токена с сохранением привязки к закрытому ключу

Если сертификат и закрытый ключ находятся на токене, то для работы с таким сертификатом его надо установить в локальное хранилище.

Это можно сделать через программный интерфейс приложения КриптоАРМ ГОСТ или с помощью команд программы КриптоПРО CSP. Установка сертификата с токена через КриптоАРМ ГОСТ описана в разделе Ключи.

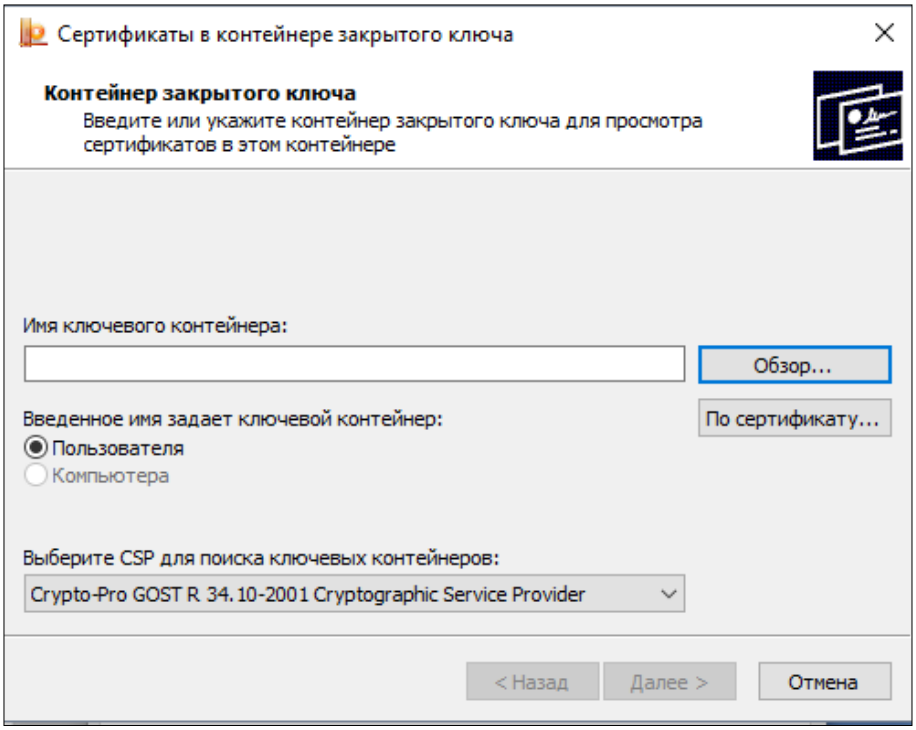
Установка с помощью программы КриптоПРО CSP отличается в операционных системах Windows, Linux и OS X.

Установка на операционной системе Windows выполняется следующим образом. Нужно подключить токен (например, Рутокен) и открыть программу КритоПро CSP. В появившемся диалоге перейти на вкладку **Сервис**.

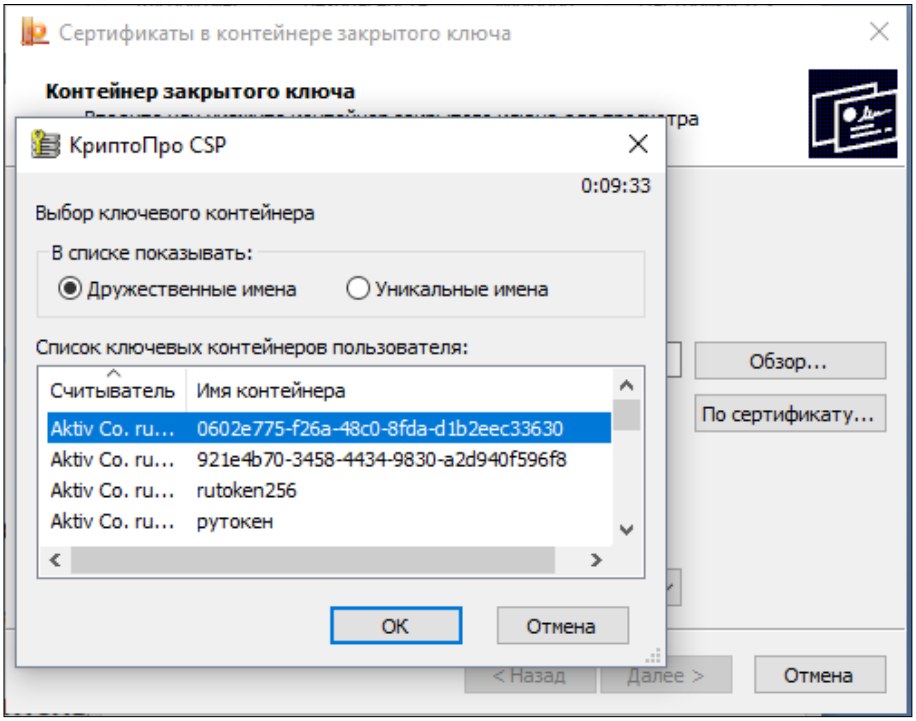


Диалог настроек криптопровайдера. Вкладка Сервис

После нажатия на кнопку **Просмотреть сертификаты в контейнере** должен открыться диалог поиска контейнера, в котором требуется нажать кнопку **Обзор**.

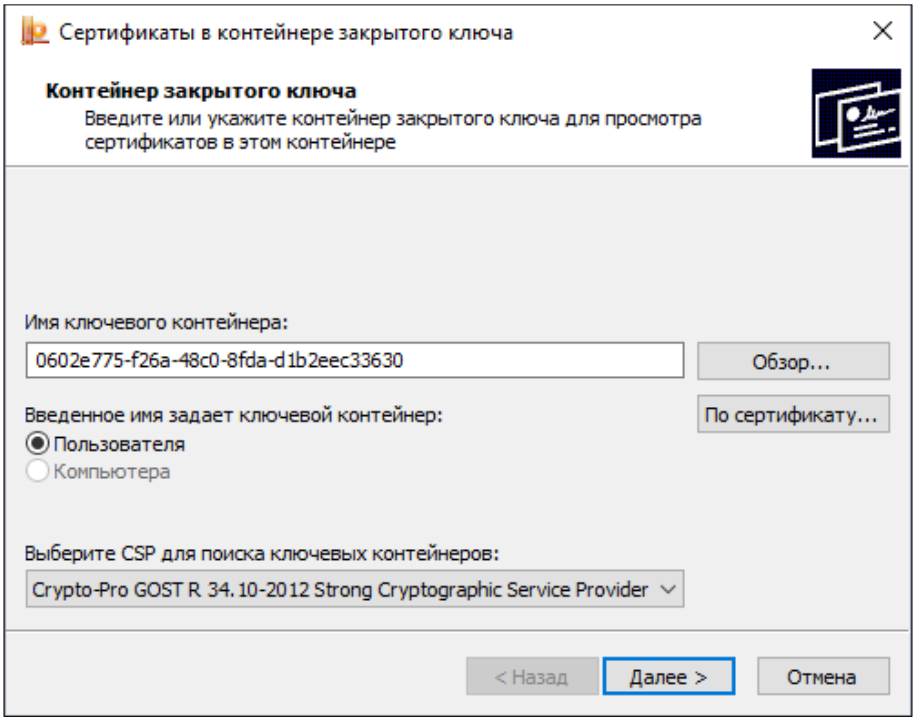


Диалог поиска ключевого контейнера



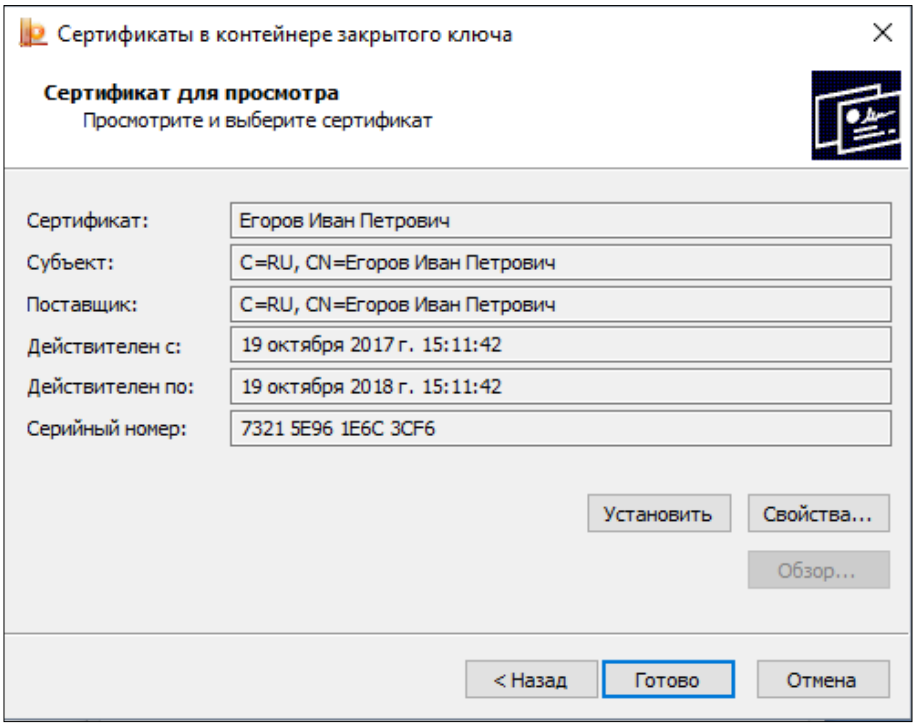
Выбор ключевого контейнера

Затем нужно выбрать нужный контейнер и нажать на кнопку **Далее**.



Просмотр содержимого контейнера

В контейнере содержится сертификат, сведения о котором будут отображены на последнем шаге мастера. Этот сертификат можно установить в систему, нажав на кнопку **Установить**.



Сведения о сертификате внутри контейнера

После успешной установки сертификата можно открыть приложение КриптоАРМ ГОСТ и перейти на вкладку **Сертификаты**. Установленный сертификат должен отображаться в списке **Личные сертификаты**.

1. Для установки сертификата под операционной системой Linux нужно подключить токен (например, Рутокен) и открыть Терминал (Terminal). Далее следует ввести команду:

/opt/cprocsp/bin/<arch>/list_pcsc

В результате получаем имя устройства, например,

Aktiv Rutoken ECP 00 00
Total: SYS: 0.010 sec USR: 0.000 sec UTC: 0.430 sec
ErrorCode: 0x00000000]

В команде под **<arch>** подразумеваться один из следующих идентификаторов платформы:

ia32 - для 32-разрядных систем;
amd64 - для 64-разрядных систем.

Далее нужно ввести команду:

sudo /opt/cprocsp/sbin/<arch>/cpconfig -hardware reader -add "имя_устройства", где в кавычках указывается имя устройства.

Например, sudo /opt/cprocsp/sbin/amd64/cpconfig -hardware reader -add "Aktiv Rutoken ECP"

Затем потребуется ввести пароль администратора (пользователя root), после чего должно появиться сообщение вида

Adding new reader:
Nick name: Aktiv Rutoken ECP
Succeeded, code:0x0

Для просмотра контейнеров на токене можно ввести команду

/opt/cprocsp/bin/<arch>/csptest -keys -verifyc -enu –fq -u

В результате получаем имя устройства и имя контейнера и после символа | - имя устройства и уникальное имя:

\\.\Aktiv Rutoken ECP\имя_контейнера | \\.\Aktiv Rutoken ECP\уникальное_имя

Затем требуется ввести для копирования сертификата с токена

/opt/cprocsp/bin/<arch>/certmgr -inst -cont '\\.\Aktiv Rutoken ECP\уникальное_имя'

В кавычках должно быть указано имя Вашего устройства и уникальное имя контейнера (справа от символа |). В терминале должна вывестись информация об установленном Вами сертификате.

После завершения установки можно открыть программу КриптоАРМ ГОСТ и перейти на вкладку **Сертификаты**. Установленный сертификат должен отображаться в списке Личные сертификаты. Если сертификат отображается как действительный (зеленый индикатор), то с ним можно работать. Если сертификат отображается как недействительный (красный индикатор), то надо устанавливать корневой и промежуточные сертификаты. Для получения корневых и промежуточных сертификатов лучше обратиться в удостоверяющий центр.

Для установки сертификата по операционной системой OS X требуется подключить токен (например, Рутокен) и открыть Терминал (Terminal). В терминале следует ввести команду:

/opt/cprocsp/bin/csptest -card -enum

В результате получаем имя устройства, например,

Aktiv Rutoken ECP 00 00
Total: SYS: 0.010 sec USR: 0.000 sec UTC: 0.430 sec
ErrorCode: 0x00000000]

Затем требуется ввести команду

sudo /opt/cprocsp/sbin/cpconfig -hardware reader -add "имя_устройства", где в кавычках указывается имя устройства.

Например**, sudo /opt/cprocsp/sbin/cpconfig -hardware reader -add "Aktiv Rutoken ECP"**

Далее требуется ввести пароль администратора (пользователя root). В результате должно быть выведено сообщение вида:

Adding new reader:
Nick name: Aktiv Rutoken ECP
Succeeded, code:0x0

Для просмотра контейнеров на токене ввести команду:

/opt/cprocsp/bin/csptest -keys -verifyc -enu –fq -u

В итоге получаем имя устройства и имя контейнера и после символа | - имя устройства и уникальное имя:

\\.\Aktiv Rutoken ECP\имя_контейнера | \\.\Aktiv Rutoken ECP\уникальное_имя

Ввести или вставить команду для копирования сертификата с токена

/opt/cprocsp/bin/certmgr -inst -cont '\\.\Aktiv Rutoken ECP\уникальное_имя'

В кавычках должно быть имя Вашего устройства и уникальное имя контейнера (справа от символа |). В терминале должна вывестись информация об установленном Вами сертификате.

После установки требуется открыть программу КриптоАРМ ГОСТ, перейти на вкладку **Сертификаты**. Установленный сертификат должен отображаться в списке **Личные сертификаты**. Если сертификат отображается как действительный (зеленый индикатор), то с ним можно работать. Если сертификат отображается как недействительный (красный индикатор), то надо устанавливать корневой и промежуточные сертификаты. Для получения корневых и промежуточных сертификатов лучше обратиться в удостоверяющий центр.

8.3 Установка доверенных коневых, промежуточных сертификатов и списка отзыва сертификата

Для работы с сертификатами нужно установить сертификат удостоверяющего центра (обычно файл с расширением .cer или .p7b), при необходимости, цепочку сертификатов (обычно файл с расширением .cer или .p7b), а также список отозванных сертификатов (обычно файл с расширением .crl). Чаще всего расширение .cer соответствует сертификату, а .p7b - контейнеру, в котором может содержаться один или больше сертификатов (например, их цепочка).

Для получения корневых и промежуточных сертификатов нужно обратиться в удостоверяющий центр.

Установить сертификаты можно через программный интерфейс приложения КриптоАРМ ГОСТ или с помощью команд программы КриптоПРО CSP. Установка сертификата с через КриптоАРМ ГОСТ описана в пункте **«**Сертификаты**»** в разделе «Импорт сертификата».

Установка корневого, промежуточных и списка отозванных сертификатов с помощью программы КриптоПРО CSP для Linux и OS X осуществляется командами:

- Установка корневого сертификата удостоверяющего центра

  /opt/cprocsp/bin/<arch>/certmgr -inst -cert -file <название файла корневого сертификата>.cer -store uRoot

- Установка цепочки промежуточных сертификатов

  /opt/cprocsp/bin/<arch>/certmgr -inst -cert -file <название файла промежуточных сертификатов>.p7b -store CA

- Установка списка отозванных сертификатов

  /opt/cprocsp/bin/<arch>/certmgr -inst -crl -file <название файла списка отозванных сертификатов>.crl

В приведенных выше командах под <arch> подразумеваться один из следующих идентификаторов платформы:

ia32 - для 32-разрядных систем Linux;
amd64 - для 64-разрядных систем Linux;
для OS X разрядность не указывается.

9 Часто встречающиеся проблемы

9.1 Сертификат недействительный (иконка красная)

Нужно установить в хранилище сертификатов корневой сертификат. Если статус сертификата не изменился, то нужно импортировать все промежуточные сертификаты. Установка сертификата сертификата описана в пункте Импорт сертификата из файла.

Если после установки корневого и промежуточных сертификатов статус сертификата не изменился, то нужно импортировать еще список отзыва. См. Списки отзыва сертификатов (COC).

9.2 Подпись недействительная

Нужно установить корневой и/или промежуточные сертификаты для сертификата подписи (Импорт сертификата из файла). Может понадобиться установка списка отзыва (Списки отзыва сертификатов (COC).

9.3 При переустановке пакета приложения на новую версию для ОС Linux возникает конфликт

Нужно в команду установки пакета добавить флаг **--force**.

9.4 Не загружен модуль trusted-crypto. ОС Windows

Установить “Распространяемый пакет Visual C++ для Visual Studio 2015” (https://www.microsoft.com/ru-RU/download/details.aspx?id=48145)

9.5 Не запускается приложение на Ubuntu 18.04, или другой deb системе (Astra Linux)

Надо установить библиотеку libgconf-2.s:o.4

sudo apt-get install libgconf-2-4

9.6 Не запускается КриптоАРМ ГОСТ на Windows.

Возможно, одновременно стоит КрипПро CSP и Лисси. Нужно оставить только КрипПро CSP.

9.7 Не запускается КриптоАРМ ГОСТ на Windows.

Возможно, версия КрипПро CSP ниже 4.

9.8 Не устанавливается лицензия на Windows

Тогда надо установить лицензию "вручную".

Нужно поместить Вашу лицензию в файл license.lic. Для этого создать простой текстовый файл, записать туда лицензию и потом переименовать, чтобы расширение файла было lic.

Поместить файл в каталог:

C:\Users\<имя пользователя>\AppData\Local\Trusted\CryptoARM GOST

Папка AppData - скрытая, поэтому надо настроить отображение скрытых папок.

Если каталогов \Trusted\CryptoARM GOST нет, то создать их.

9.9 Если раньше работало и перестало

Лицензии действительные, ошибка типа при попытке доступа к разделам **Подписать**, **Зашифровать, Сертификаты, Контейнеры** программа зависает на статусе **Пожалуйста, подождите…**

Возможно установили (потом удалили или нет) другой криптопровайдер (например, VipNet) - будет конфликт. Нужно удалить другой криптопровайдер, потом удалить файл настроек. Для этого нужно закрыть программу (**Выход** в меню или в трее), перейти в каталог пользователя в папку .Trusted\CryptoARM GOST\ и удалить файл settings.json.

9.10 КриптоАРМ ГОСТ 2.0, если на unix системах не работает с КриптоПро 4

Признак - нет никаких сертификатов на вкладке **Сертификаты**

Чтобы заработало, надо доустановить пакет КриптоПро cprocsp-rsa.

Затем в конфиге (/etc/opt/cprocsp/config.ini) от администратора добавить блоки:

- **Для Linux:**

  (этот после блока [Defaults\Provider\"Crypto-Pro RSA CSP"])

  [Defaults\Provider\"Crypto-Pro Enhanced RSA and AES CSP"]

  "Image Path" = "/opt/cprocsp/lib/amd64/librsaenh.so"

  "Function Table Name" = "CPRSA_GetFunctionTable"

  Type = 24

  (Этот после блока [Defaults\"Provider Types"\"Type 001"])

  [Defaults\"Provider Types"\"Type 024"]

  Name = "Crypto-Pro Enhanced RSA and AES CSP"

  TypeName = "RSA Full and AES"

- **Для MacOS:**

  (этот после блока [Defaults\Provider\"Crypto-Pro RSA CSP"])

  [Defaults\Provider\"Crypto-Pro RSA CSP and AES CSP"]

  "Image Path" = "/opt/cprocsp/lib/librsaenh.dylib"

"Function Table Name" = "CPRSA_GetFunctionTable"

type = 24

(Этот после блока [Defaults\"Provider Types"\"Type 001"])

[Defaults\"Provider Types"\"Type 024"]

Name = "Crypto-Pro RSA CSP and AES CSP"

TypeName = "RSA Full (Signature and Key Exchange)"

Для редактирования конфигурационного файла можно запросить скрипт в технической поддержке.

9.11 Не создается запрос на сертификат на линукс при КриптоПро CSP 4

Нужно на форме запроса на сертификат перед названием ключевого контейнера писать \\.\HDIMAGE\

Например, имя может быть таким \\.\HDIMAGE\9f5e1bed-a31e-bc4d-a66c-7a95f943dcc7

9.12 Не импортируются корневые, промежуточные сертификаты, СОС на линукс.

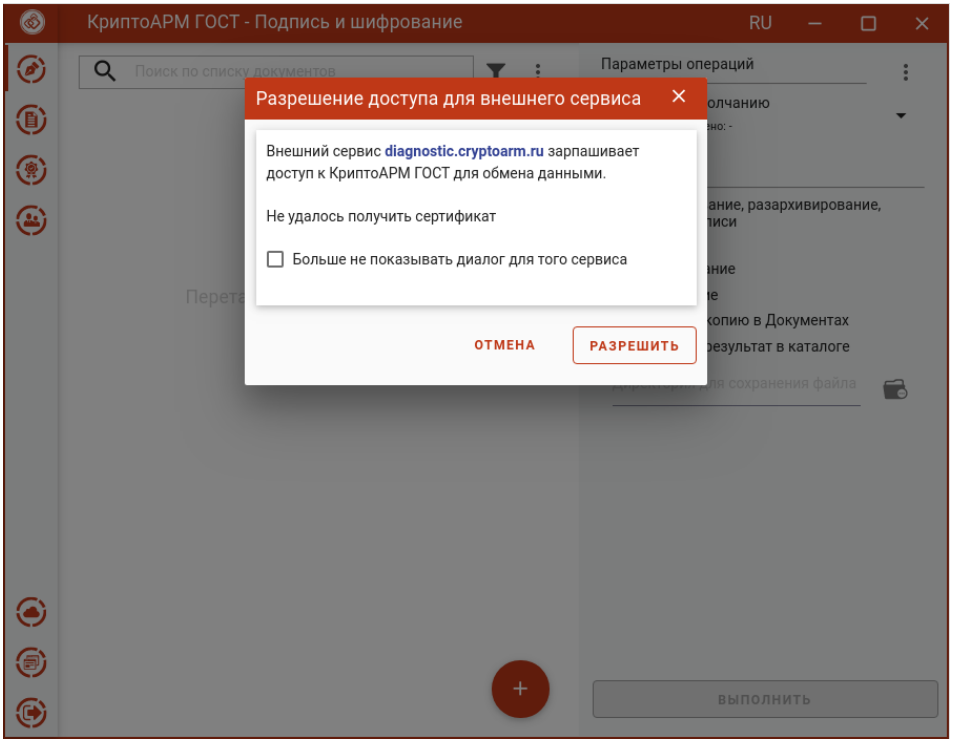
1. **Если пользователь не в группе sudo.**
   Надо его добавить в группу sudo или установить сертификаты через команды КриптоПро.

2. **Особенность для пользователей ОС на платформе Альт** 64bit- Альт Рабочая Станция 8/9, Альт Рабочая Станция К 8/9, . Альт 8/9 СП, Альт Образование 8/9.

Нужно установить сертификаты через команды КриптоПро.

Описание импорта сертификатов в разделе Установка доверенных коневых, промежуточных сертификатов и списка отзыва сертификата.

9.13 Если при открытии КриптоАРМ ГОСТ по ссылке с внешнего сервиса не удалось получить сертификат сервиса



Ошибка при получении сертификата сервиса

Необходимо импортировать корневой сертификат сайта (сервиса), с которого происходит открытие КриптоАРМ ГОСТ в хранилище **Доверенных корневых сертификатов**.