КриптоАРМ ГОСТ

Руководство пользователя

ОГЛАВЛЕНИЕ

Общие сведения о программном продукте 5
Функциональность версии 2.1 5
Поддерживаемые криптопровайдеры 6
Лицензия на программный продукт 6
Доля использования OpenSource проектов 6
Системные требования 7
Поддерживаемые операционные системы 8
1. Установка программного продукта 9
1.1. Установка на платформу Microsoft Windows 9
1.2. Установка на платформу Linux 11
1.3. Установка на платформу OS X 12
2. Удаление программного продукта 17
2.1. Удаление приложения на платформе MS Windows 17
2.2. Удаление приложения на платформе Linux 17
2.3. Удаление приложения на платформе OS X 18
3. Установка лицензии на программный продукт 19
3.1. Установка лицензии через пользовательский интерфейс 19
3.1.1. Установка постоянной лицензии 19
3.2. Установка лицензии через командную строку 21
4. Установка криптопровайдера КриптоПро CSP 22
4.1. Установка криптопровайдера на платформу MS Windows 22
4.2. Установка криптопровайдера на платформу Linux 22
4.3. Установка криптопровайдера на платформу OS X 23
4.4. Установка лицензии на программный продукт КриптоПРО CSP 23
4.4.1. Установка лицензии через пользовательский интерфейс. 24
4.4.2. Установка лицензии через командную строку 26
5. Графический пользовательский интерфейс приложения 27
5.1. Начало работы с приложением 27
5.2. Создание электронной подписи 28
5.3. Подпись сертификатом DSS 33
5.4. Проверка электронной подписи 35
5.5. Снятие электронной подписи 36
5.6. Добавление подписи 38
5.7. Шифрование файлов 39
5.8. Расшифрование файлов 44

5.9. Управление списком файлов для выполнения операций....45
5.10. Документы....49
5.11. Сертификаты....53
5.11.1. Импорт сертификата из файла....55
5.11.2. Импорт сертификата из DSS....56
5.11.3. Экспорт сертификата в файл....58
5.11.4. Удаление сертификата....61
5.11.5. Создание запроса на сертификат....62
5.11.6. Создание самоподписанного сертификата....67
5.11.7. Списки отзыва сертификатов (COC)....68
5.11.8. Поиск сертификата....71
5.12. Установка сертификата из ключевого контейнера....71
5.13. Настройки....74
5.14. Журнал операций....80
5.15. О программе....84
5.16. Справка....84
5.17. Отправка запросов на сертификат и установка сертификатов на основе КриптоПро УЦ 2.0 ...84
6. Диагностика неполадок при запуске приложения....93
6.1. Отсутствует СКЗИ КриптоПро CSP....93
6.2. Отсутствует лицензия на КриптоАРМ ГОСТ....94
6.3. Отсутствует лицензия на КриптоПро CSP....95
6.4. Не обнаружены сертификаты с привязкой к ключевому контейнеру....96
6.5. Не загружен модуль Trusted Crypto....97
7. Включение режима логирования и консоль управления....97
7.1. Отслеживание ошибок на платформе MS Windows....98
7.2. Отслеживание ошибок на платформе Linux....99
7.3. Отслеживание ошибок на платформе OS X....100
8. Управление сертификатами и ключами с помощью командной строки....102
8.1. Перенос контейнера закрытого ключа под требуемую операционную систему....102
8.2. Установка сертификата с токена с сохранением привязки к закрытому ключу....104
8.3. Установка доверенных коневых, промежуточных сертификатов и списка отзыва сертификата 109
9. Часто встречающиеся проблемы....110
9.1. Не загружен модуль trusted-crypto. ОС Windows....110
9.2. Не запускается приложение на Ubuntu 18.04, или другой deb системе (Astra Linux)....110
9.3. Не запускается КриптоАРМ ГОСТ на Windows....110
9.4. Не запускается КриптоАРМ ГОСТ на Windows....110

9.5. Не устанавливается лицензия на Windows....110
9.6. Если раньше работало и перестало. 110
9.7. КриптоАРМ ГОСТ 2.0, если на unix системах не работает с КриптоПро 4....111
9.8. Не создается запрос на сертификат на линукс при КриптоПро CSP 4....111
Команда разработки и сопровождения продукта....112
Контактная информация....113

Общие сведения о программном продукте

КриптоАРМ ГОСТ - это универсальное приложение с графическим пользовательским интерфейсом для выполнения операций по созданию и проверке электронной подписи файлов, шифрования и расшифрования, управления сертификатами, размещенных в хранилищах криптопровайдеров[1].

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.

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

Функциональность версии 2.1

Приложение текущей версии рассчитано на выполнение операций:

Электронная подпись	– электронная подпись произвольных файлов на поддерживаемых платформах; – добавление электронной подписи к уже существующим (функция создания соподписи); – создание как присоединенной, так и отделенной электронной подписи; – поддержка стандарта электронной подписи ГОСТ Р 34.10-2012.
Шифрование	– шифрование и расшифрование файлов на поддерживаемых платформах; – удаление исходного файла после шифрования; – шифрование данных 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.) 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.

[1] Криптопровайдер (Cryptography Service Provider, CSP) — это независимый модуль, позволяющий осуществлять криптографические операции в операционных системах MS Windows, Linux, OSX, управление которым происходит с помощью функций CryptoAPI. В качестве примера, устанавливаемого криптопровайдера служит криптопровайдер КриптоПро CSP.

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

Поддерживаемые криптопровайдеры

Для корректной работы с ГОСТ алгоритмами требуется установка криптопровайдера КриптоПро CSP. В приложении осуществляется поддержка КриптоПро CSP версии 4.0 и выше.

Лицензия на программный продукт

При первой установке приложения активируется временная лицензия сроком на 2 недели. После истечения ознакомительного периода для полнофункциональной работы приложения требуется приобретение и установка лицензии. Без установки лицензии на операции: установления TLS соединения, доступа к закрытому ключу при операциях подписи и расшифрования будут наложены ограничения.

Для приобретения лицензии на программный продукт КриптоАРМ ГОСТ можно обратиться в компанию разработчика приложения. Контактные данные компании представлены в разделе Контактная информация.

Доля использования OpenSource проектов

При разработке программного продукта были использованы OpenSource проекты:

- Electron - MIT License
- archiver - MIT License
- async - MIT License
- history - MIT License
- immutable - MIT License
- request - Apache License 2.0
- reselect - MIT License
- socket.io - MIT License
- sudo-prompt - MIT License
- winston - MIT License
- react - MIT License

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;
- 2Gb 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);
- 2Gb 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.
- 2Gb оперативной памяти;
- 150 Mb дискового пространства для установки и работы приложения;
- требование к видеоадаптеру не критично. Должно поддерживаться минимальное разрешение 800x600.

Поддерживаемые операционные системы

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

- Microsoft Windows 10 64bit/32bit.
- Ubuntu 16.04 64bit и выше.
- CentOS 7 64bit.
- Rosa Fresh 64bit
- Rosa Enterprise Desktop (RED) X3 64bit.
- 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
- Mac OS X 10.12, 10.13.

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 2 недели.

1. Установка программного продукта

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. В зависимости от выбранной разрядности запустите на исполнение файл:

CryptoARM_GOST_vx.x.x_x64.exe (где x.x.x – номер версии) для 64-разрядной ОС;

CryptoARM_GOST _vx.x.x_x86.exe (где x.x.x – номер версии) для 32-разрядной ОС).

Откроется мастер установки приложения КриптоАРМ ГОСТ, начальный шаг которого представлен на рис.1.1.1.

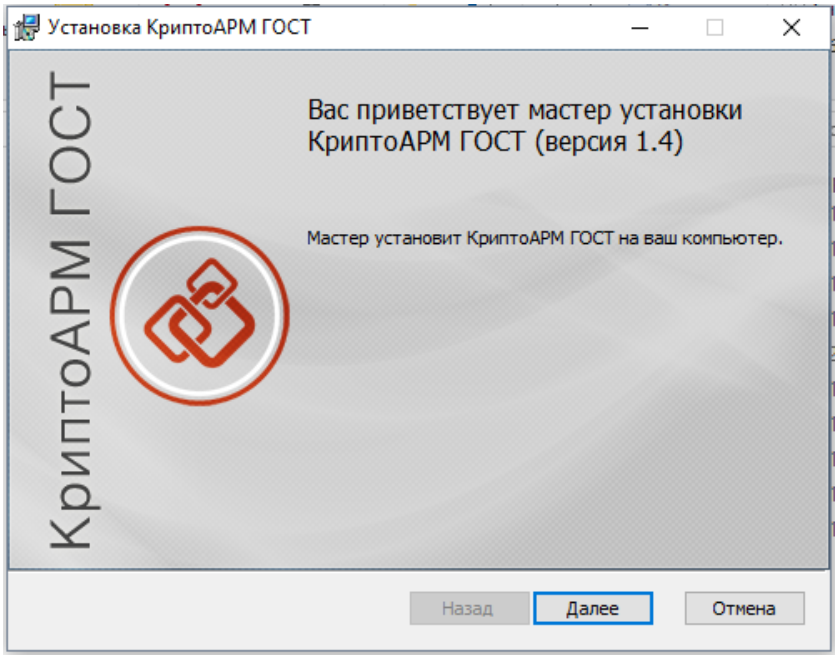


Рис.1.1.1. Начальный шаг мастера установки приложения

На следующем шаге мастера предлагается ознакомиться с условиями лицензионного соглашения (рис.1.1.2), и в случае согласия принять условия и перейти к следующему шагу мастера, нажав кнопку **Далее**.

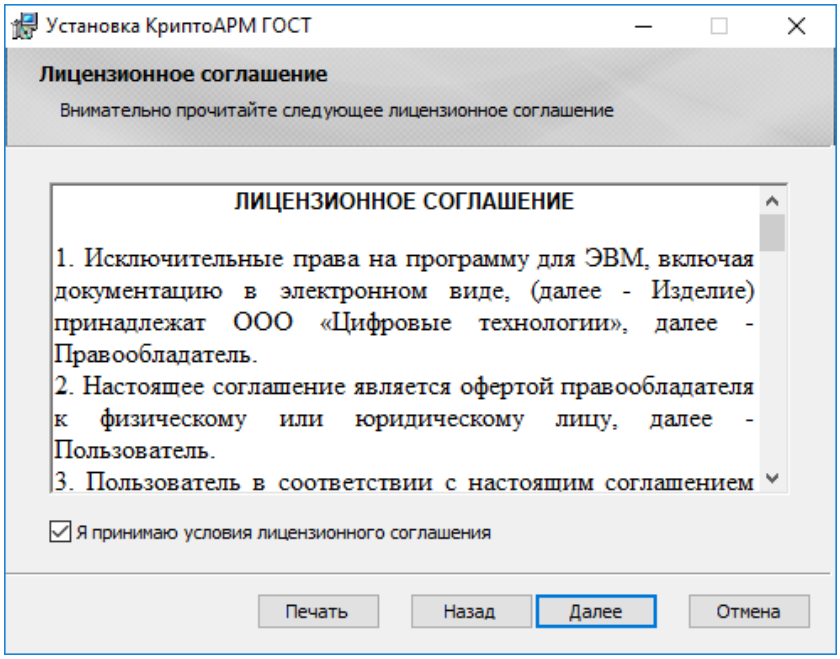


Рис.1.1.2. Условия лицензионного соглашения

На следующем шаге мастера выберете каталог для установки КриптоАРМ ГОСТ (по умолчанию приложение устанавливается в каталог C:\Program Files\CryptoARM GOST\) и нажать **Далее** (рис.1.1.3). На шаге выборочной установки для текущей версии продукта не предлагается никаких дополнительных компонент.

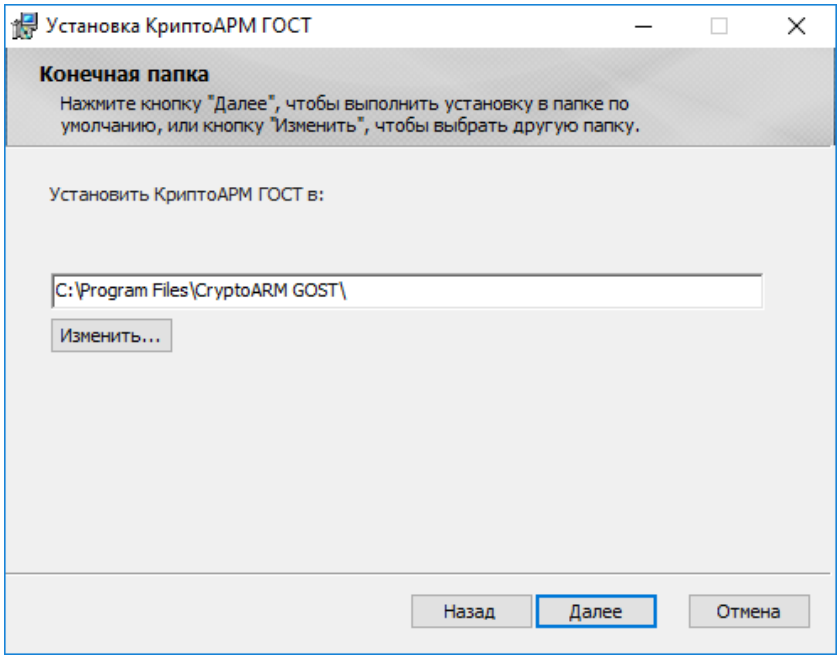


Рис.1.1.3. Выбор каталога установки приложения

На заключительном шаге мастера нажмите кнопку **Установить** (рис.1.1.4). Установка выполняется с правами администратора.

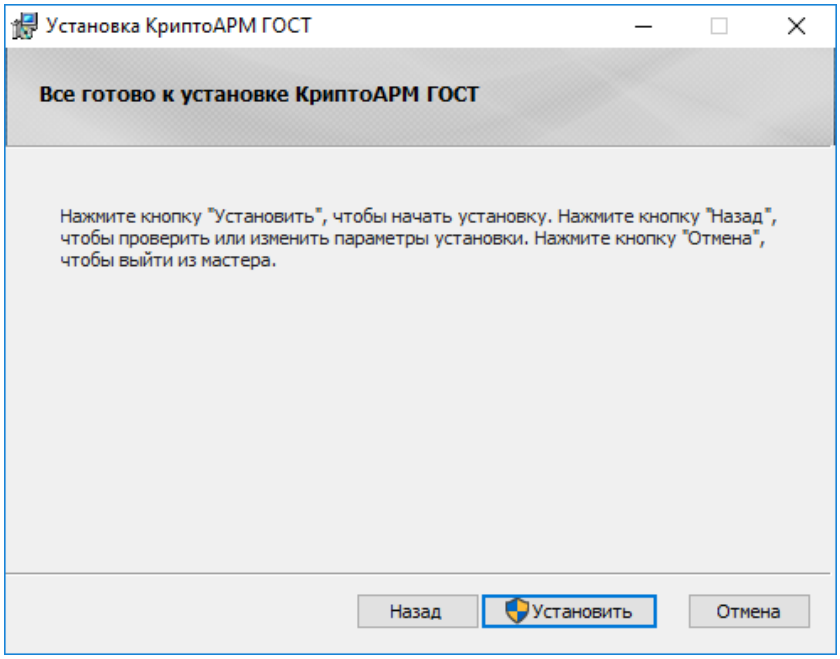


Рис.1.1.4. Выбор каталога установки приложения

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.

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 приложения КриптоАРМ ГОСТ 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_x32.rpm (где x.x.x – номер версии) для 32-разрядных ОС, основанных на RPM.

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

- Второй способ установки приложения выполняется с помощью командной строки. Для этого нужно запустить терминал и ввести команду:

  sudo dpkg - i CryptoARM_GOST_vx.x.x_xYY.deb (YY - разрядность ОС) - для ОС, основанных на Debian (Debian/Ubuntu);

sudo rpm - i CryptoARM_GOST_vx.x.x_xYY.rpm (YY - разрядность ОС) - 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.

1.3. 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).

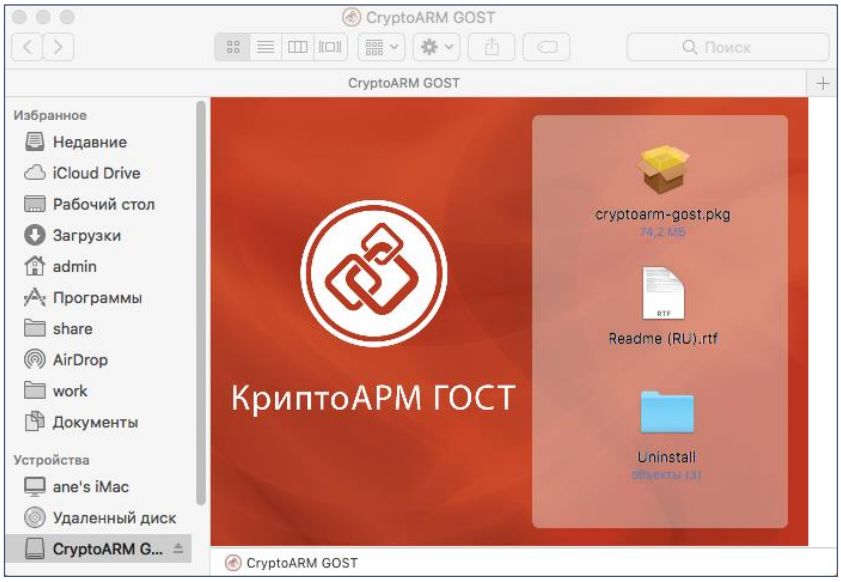


Рис.1.3.1. Состав образа диска

Для установки программы КриптоАРМ ГОСТ запустите на исполнение файл **CryptoARM_GOST_vx.x.x_x64.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**.

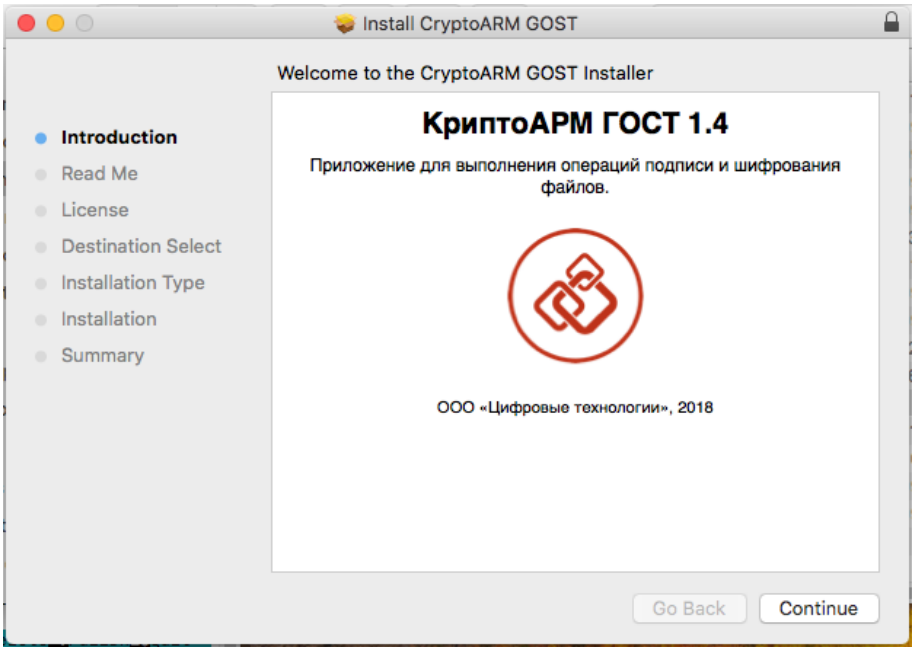


Рис.1.3.2. Начальный шаг мастера установки пакета приложения

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

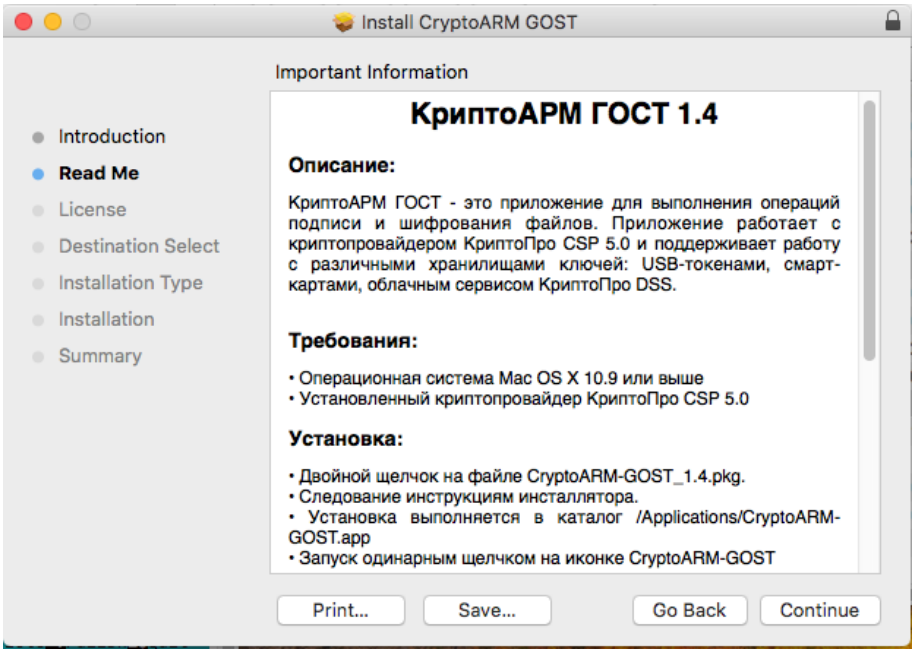


Рис.1.3.3. Просмотр информации о программном продукте

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

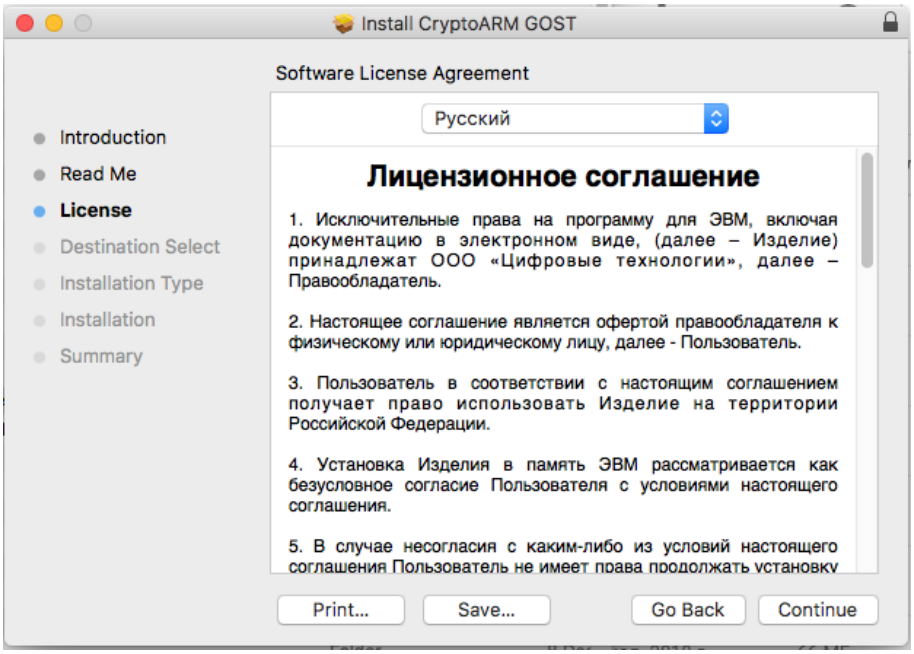


Рис.1.3.4. Просмотр информации о лицензии

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

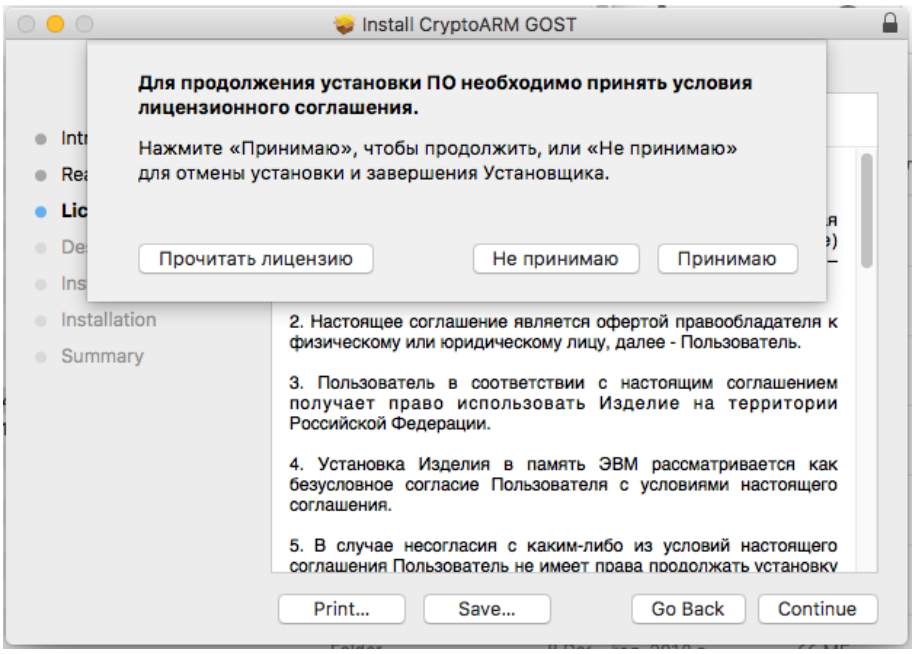


Рис.1.3.5. Соглашение с условиями лицензии

Выберете диск, на который будет установлено приложение (рис.1.3.6) и нажмите **Продолжить**.

Рис.1.3.6. Информация о размещении приложения на жестком диске

На следующем шаге мастера нажмите кнопку **Установить** (рис.1.3.7).

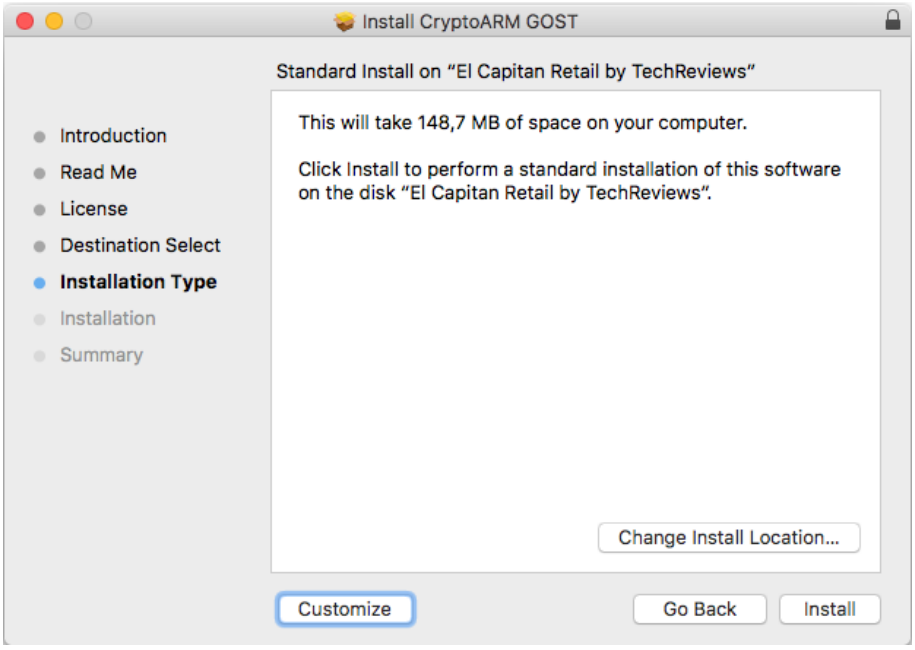


Рис.1.3.7. Подтверждение установки на физический носитель

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

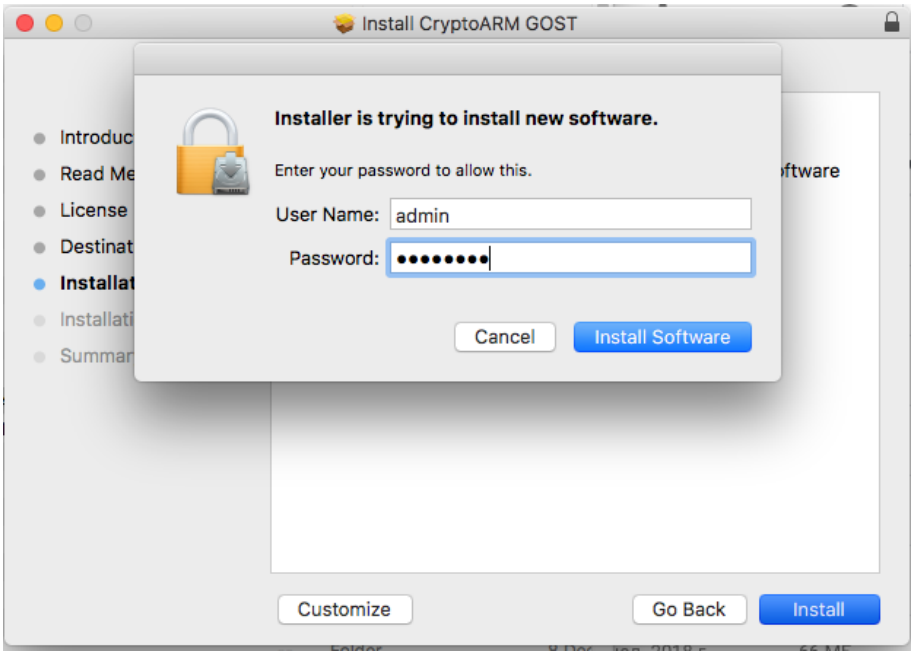


Рис.1.3.8. Информация о размещении приложения на жестком диске

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.

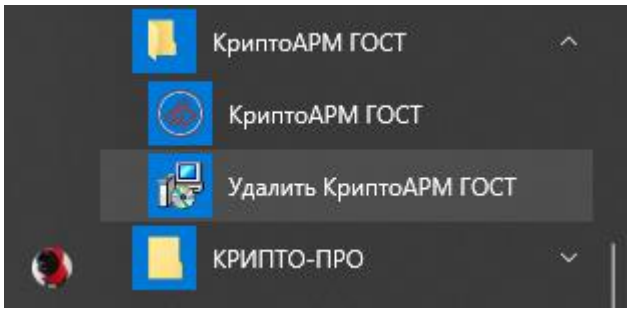
После завершения установки можно отмонтировать диск стандартными средствами ОС.

2. Удаление программного продукта

2.1. Удаление приложения на платформе MS Windows

Удалить приложение КриптоАРМ ГОСТ можно следующим образом:

- 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**.
- 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) (см. рисунок ниже) 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.

2.2. 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.

- 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.
- 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.

2.3. 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 (рис. 2.3.1). Для удаления приложения из каталога Application запускается **скрипт unistall_cryptoarm_gost**. Для полного удаления приложения (настроек, кэша, лицензий) используется скрипт **full_uninstall_cryptoarm_gost**. Затем ну жно ввести пароль администратора.

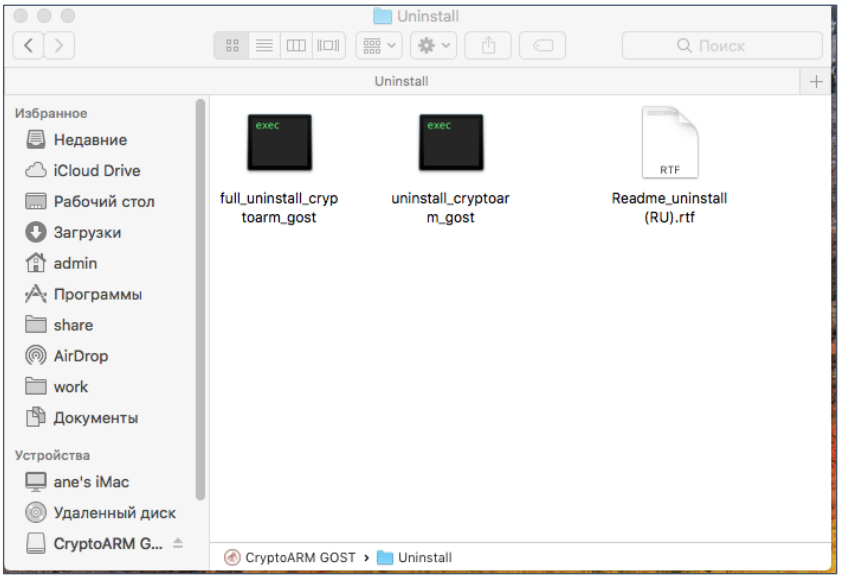


Рис.2.3.1. Каталог скриптов удаления приложения

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.

3. Установка лицензии на программный продукт

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 с помощью консольных команд, выполняющих копирование файла лицензии в заданный каталог.

3.1. Установка лицензии через пользовательский интерфейс

3.1.1. Установка постоянной лицензии

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **О программе** через главное меню приложения. На открывшейся странице, которая представлена на рис.3.1.1 нажать на кнопку **Ввод лицензии** в разделе управления лицензией КриптоАРМ ГОСТ. В результате должно появиться всплывающее окно ввода лицензии, предполагающее выполнение действия одним из двух способов (рис. 3.1.2): выполнение ввода копированием содержимого файла лицензии в текстовое поле и выполнение ввода указанием файла лицензии.

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

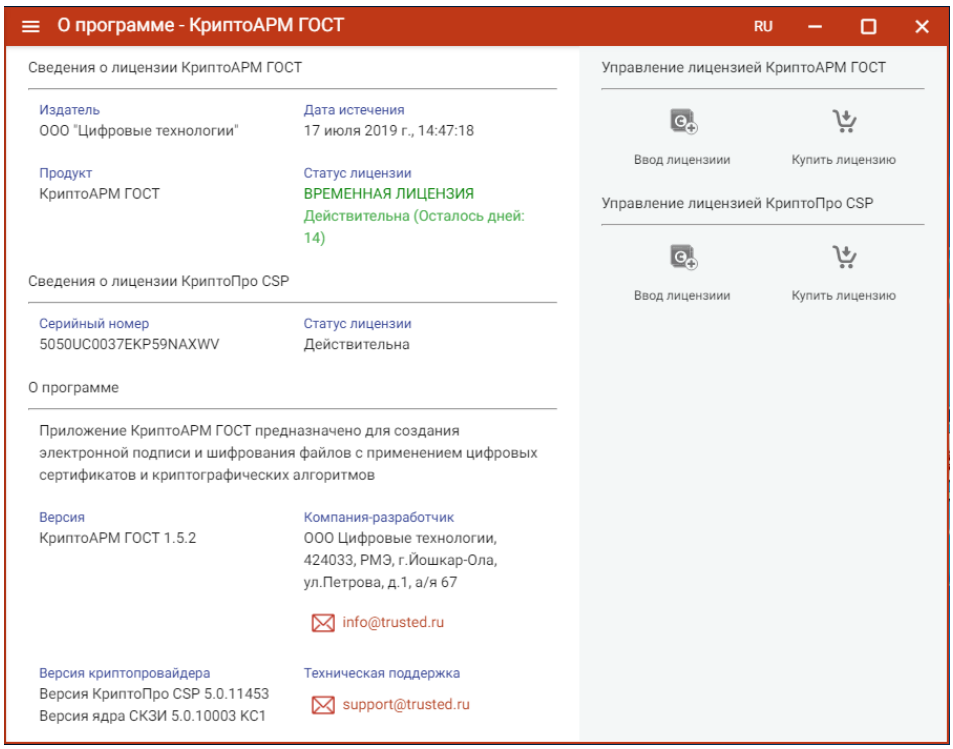


Рис.3.1.1. Страница ввода лицензионного ключа на программный продукт

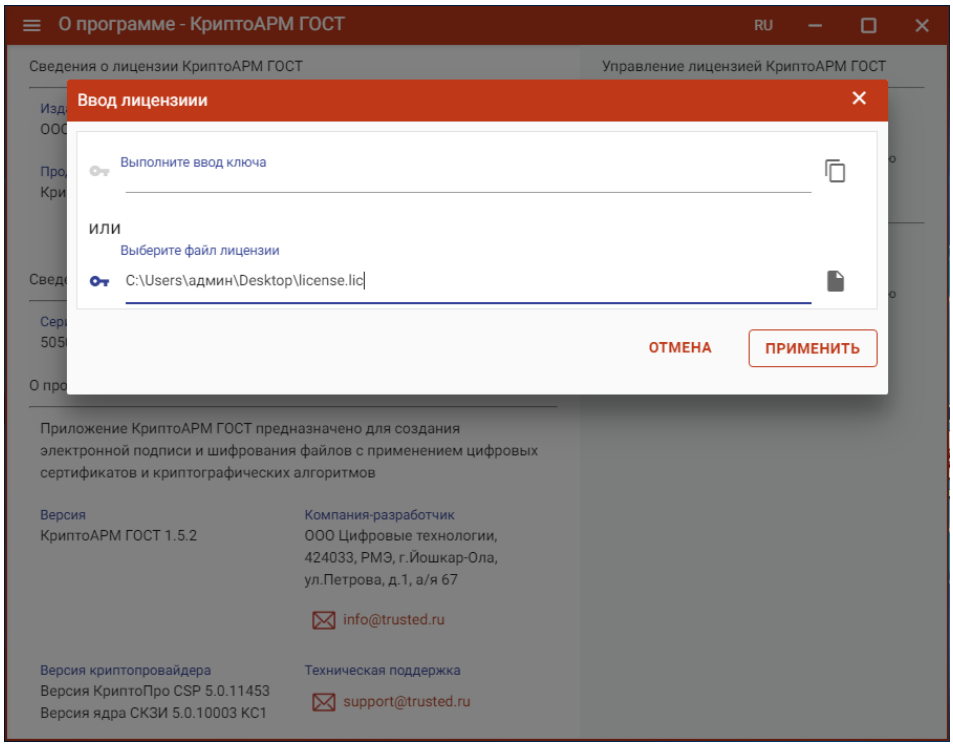


Рис.3.1.2. Диалоговое окно с выбором варианта ввода лицензионного ключа

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

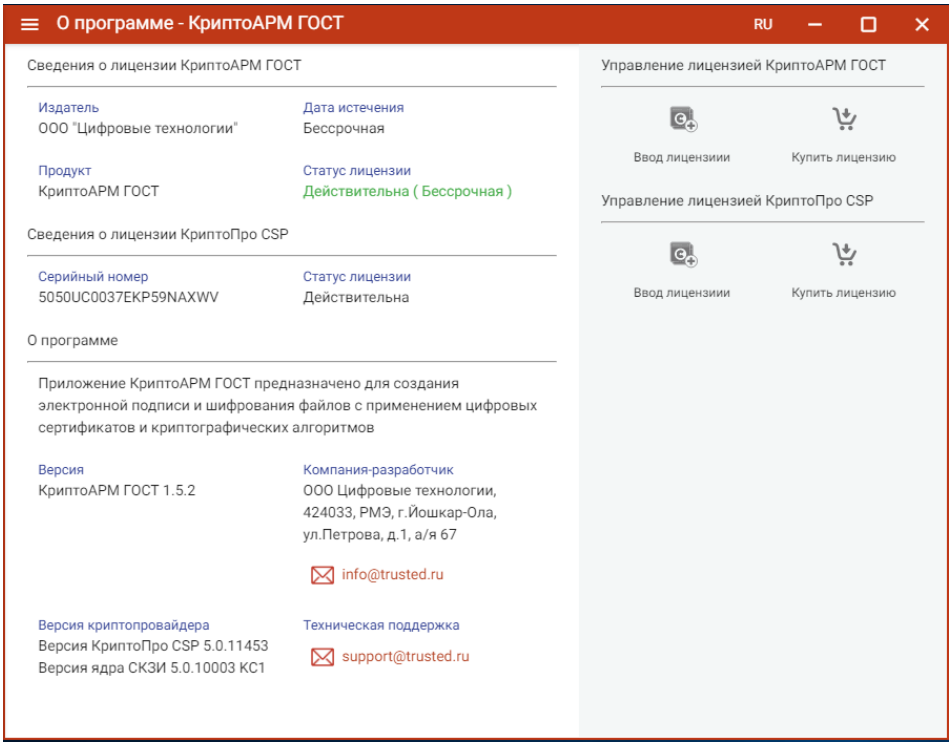


Рис. 3.1.3 Сведения о лицензии

3.2. Установка лицензии через командную строку

Для целей развертывания приложения на множестве рабочих мест использование диалога ввода лицензии не подходит. Наилучшим вариантом здесь является установка лицензии с помощью копирование файла лицензии license.lic в каталог установки:

- Под платформой Windows – каталог

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

- Под платформой Linux – каталог ./etc/opt/Trusted/CryptoARM GOST/.

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. Установка криптопровайдера КриптоПро CSP

Для выполнения операций с использованием российских криптографических алгоритмов на рабочее место нужно установить СКЗИ «КриптоПро CSP».

4.1. Установка криптопровайдера на платформу MS Windows

Для установки КриптоПро CSP 5.0 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. 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.

Пакеты зависят друг от друга, поэтому должны устанавливаться по порядку с учётом этих зависимостей.

Для установки пакета используется команда:

rpm -i <файл_пакета>
Например, **rpm -i ./lsb-cprocsp-base-5.0.10874-5.noarch.rpm**

На ОС, основанных на Debian (Debian/Ubuntu), для установки пакетов используется команда:

alien -kci <файл_пакета>
Например, **alien -kci ./lsb-cprocsp-base-5.0.10874-5.noarch.deb**

На ОС, основанных на Debian (Debian/Ubuntu), для установки 32-битных пакетов на 64битную ОС используется команда:

dpkg-architecture -ai386 -c alien -kci <файл_пакета>

Порядок установки пакетов приведен ниже. Возможно, потребуется предварительно установить пакеты **lsb-base**, **alien**, **lsb-core** из стандартного репозитория ОС:

sudo apt-get install lsb-base alien lsb-core
sudo alien -kci lsb-cprocsp-base-<...>.noarch.deb
sudo alien -kci lsb-cprocsp-rdr-64-<...>.deb
sudo alien -kci lsb-cprocsp-capilite-<...>.deb
sudo alien -kci lsb-cprocsp-kc1-<...>.deb

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

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 alien -kci cprocsp-rdr-gui-<>.deb

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 alien -kci cprocsp-rdr-pcsc-<...>.deb

Для ключевого носителя Рутокен:

sudo alien -kci cprocsp-rdr-rutoken-<...>.deb
sudo alien -kci ifd-rutokens_1.0.4_1.x86_64.deb

Для ключевого носителя JaCarta:

sudo alien -kci cprocsp-rdr-jacarta -<...>.deb

Для работы с сертификатами, находящимися в «облаке», в систему надо установить следующие пакеты:

sudo alien -kci cprocsp-cptools-gtk- -<...>.deb
sudo alien -kci cprocsp-rdr-cloud-<...>.deb
sudo alien -kci cprocsp-rdr-cloud-gtk-<...>.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.

4.3. 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 .

4.4. 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.

4.4.1. Установка лицензии через пользовательский интерфейс.

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **О программе** через главное меню приложения. На открывшейся странице, которая представлена на рис.4.4.1 нажать на кнопку **Ввод лицензии** в разделе управления лицензией КриптоПРО CSP. В результате должно появиться всплывающее окно ввода лицензии копированием содержимого файла лицензии в текстовое поле (рис. 4.4.2).

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

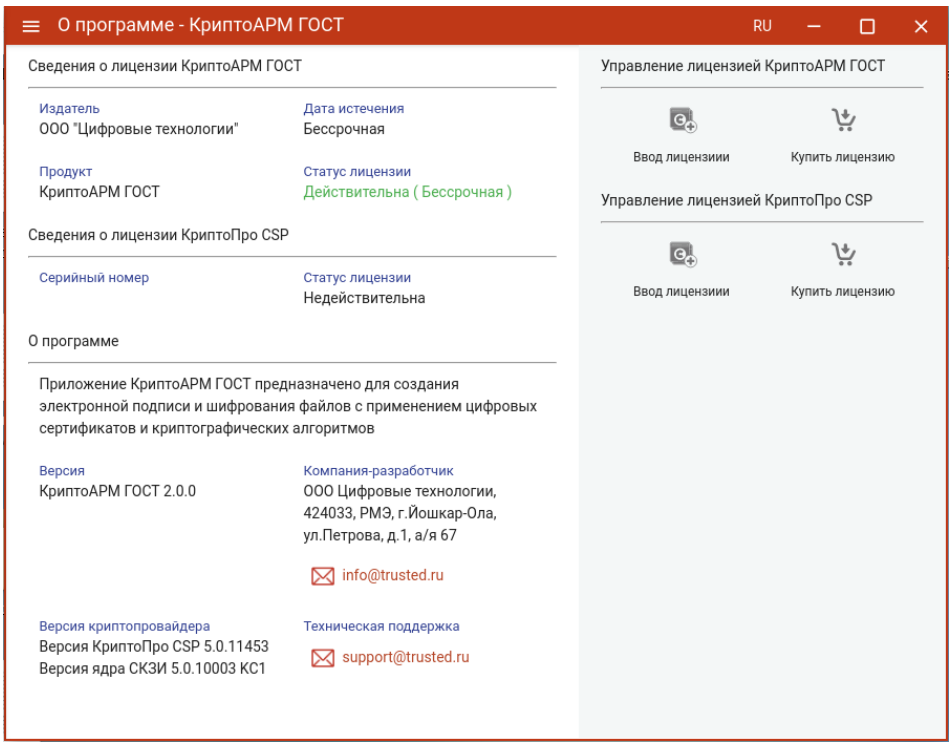


Рис.4.4.1. Страница ввода лицензионного ключа на КриптоПРО CSP

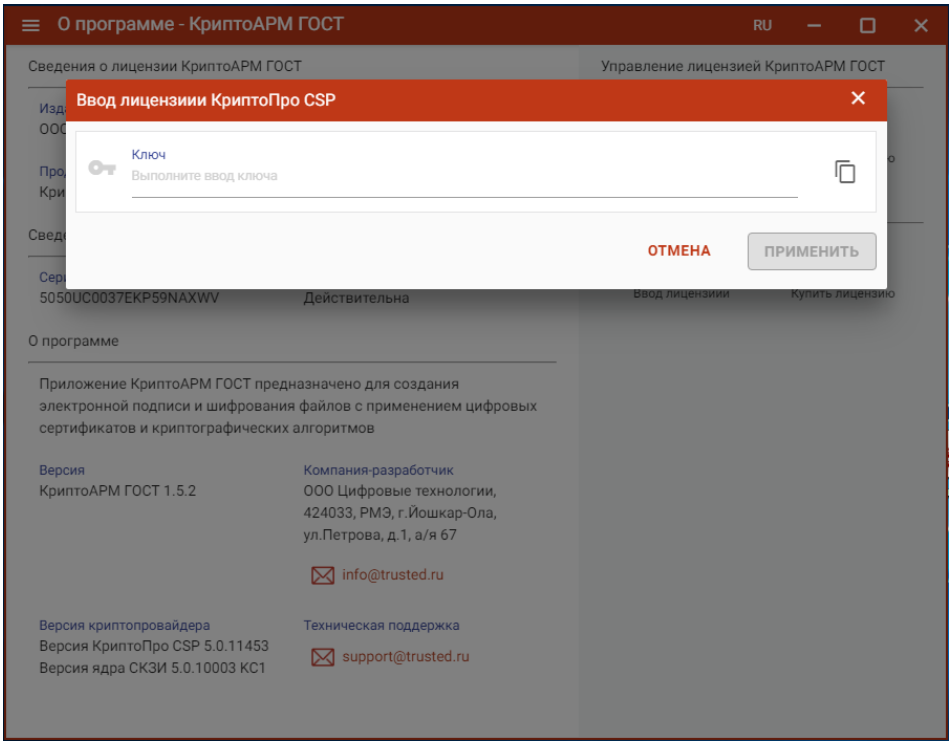


Рис. 4.4.2. Диалоговое окно ввода лицензионного ключа

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

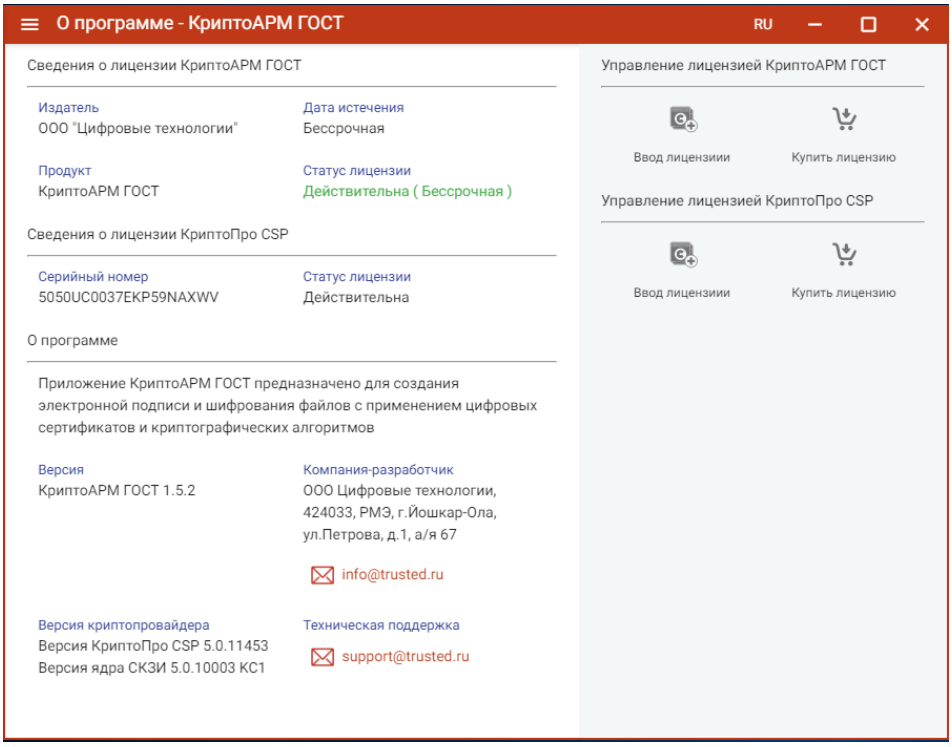


Рис. 4.4.3 Сведения о лицензии

4.4.2. Установка лицензии через командную строку

Установка лицензии на КриптоПРО CSP осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo.

Просмотр информации о лицензии осуществляется командой:

 # cpconfig -license -view

Ввод лицензии производится командой (серийный номер следует вводить с соблюдением регистра символов):

 # cpconfig -license -set <серийный_номер>

5. Графический пользовательский интерфейс приложения

5.1. Начало работы с приложением

Работа с приложением КриптоАРМ ГОСТ начинается со страницы **Подпись и шифрование** (рис.5.1.1). Левая часть окна предназначена для управления списком файлов; в правой части располагается панель выбора настроек, сертификатов подписи и шифрования и кнопки операций.

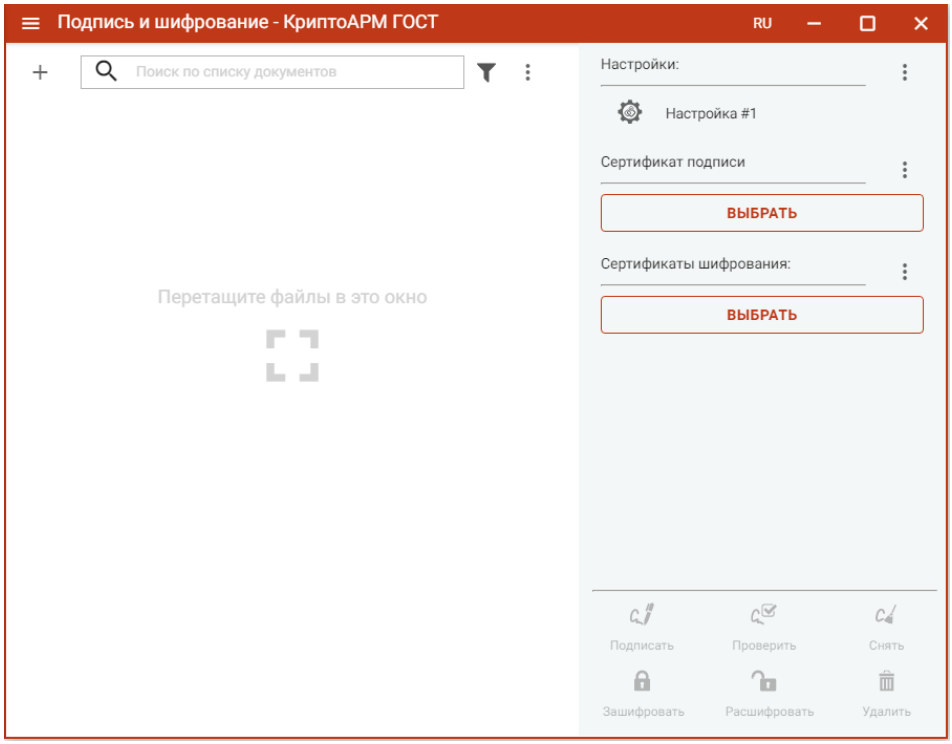


Рис.5.1.1. Стартовое окно приложения

В верхней левой части окна расположена кнопка вызова главного меню приложения  , через которое можно выполнить переход ко всем представлениям (рис.5.1.2).

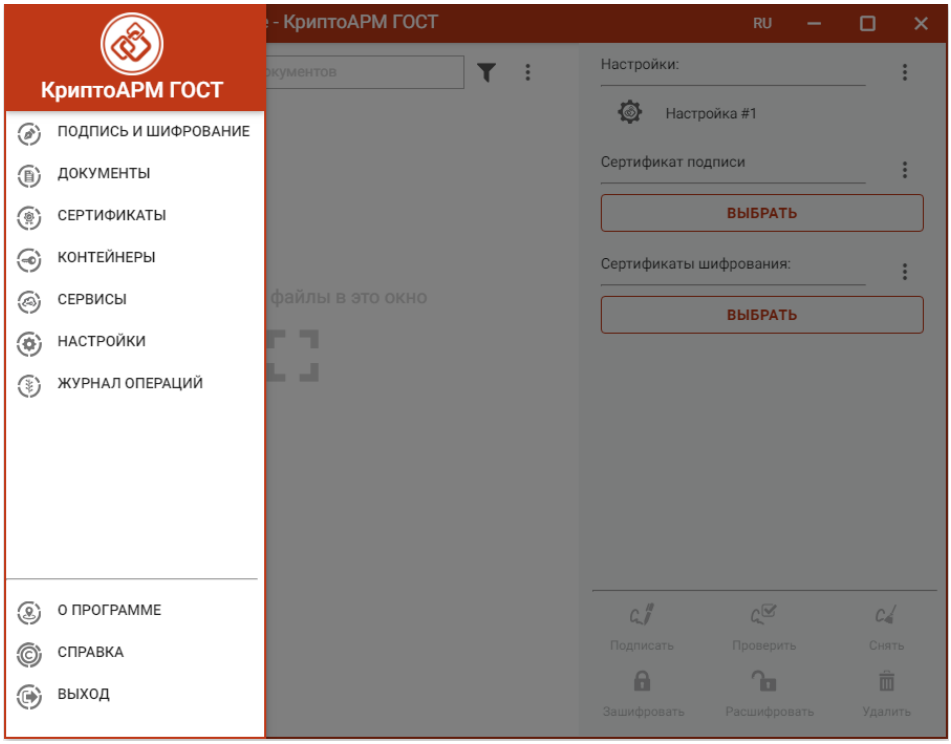


Рис.5.1.2. Основное меню приложения

При первом запуске приложения в домашней папке пользователя создается подкаталог с наименованием **.Trusted**. Данный подкаталог 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

Для подписи файлов нужно выбрать подписываемые файлы, сертификат подписи и задать настройки подписи. Подписать файлы можно на странице **Подпись и шифрование** или **Документы**.

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

Выбранные файлы заносятся в плевую область и представляют собой одноуровневый список (рис. 5.2.1).

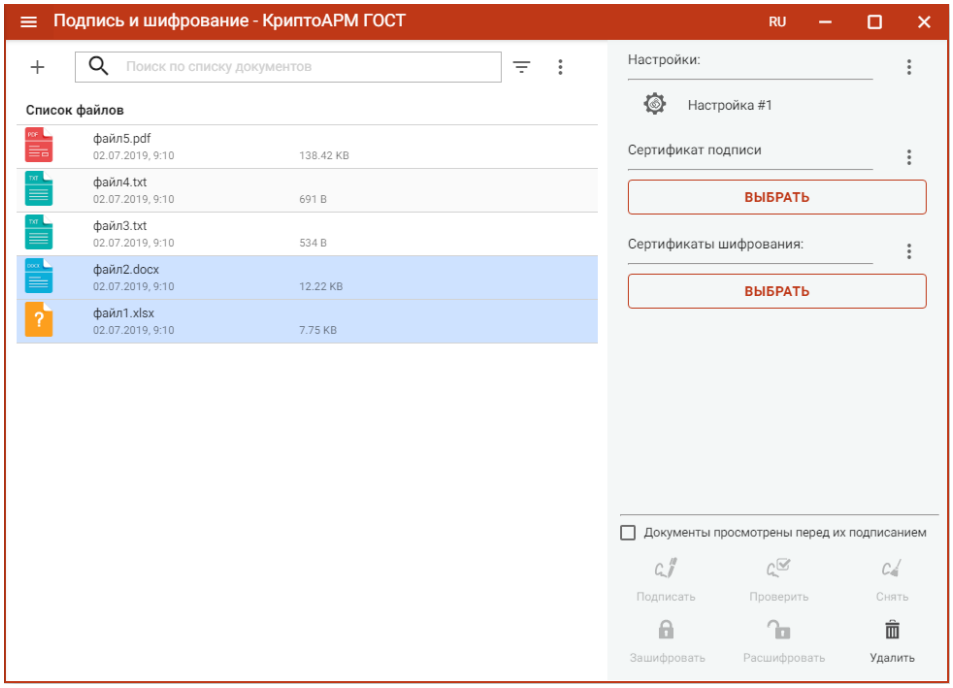


Рис.5.2.1. Список подписываемых файлов

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (рис. 5.2.2).

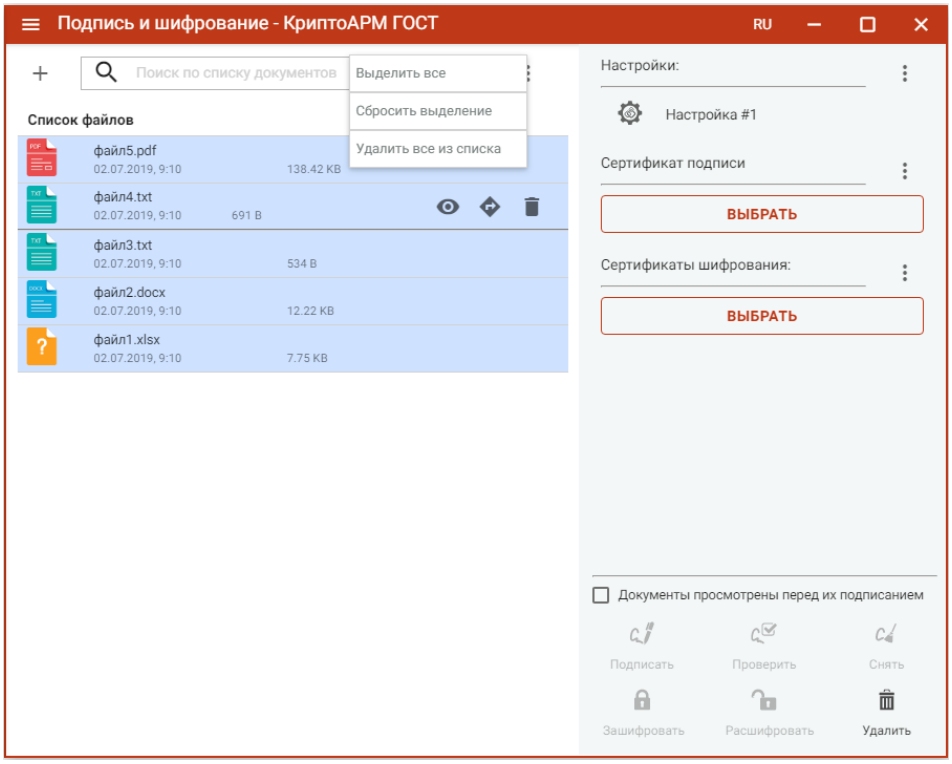


Рис. 5.2.2. Контекстное меню управления списком файлов

Настройки подписи. При первом запуске приложения создается настройка по умолчанию «Настройка #1», в которой задается кодировка подписи base64, вид подписи – присоединенная, в подпись будет добавлено время подписи.

Для изменения настроек подписи можно изменить текущую настройку, выбрав в контекстном меню **Изменить** (рис. 5.2.3), или добавить новую настройку, выбрав пункт меню **Настройки**.

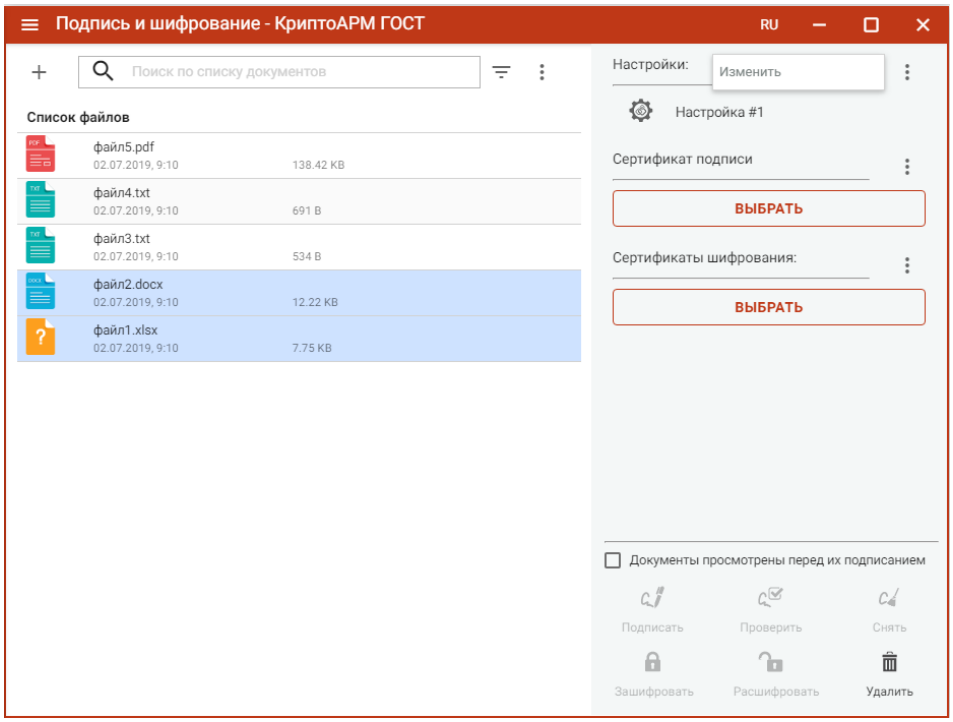


Рис. 5.2.3. Контекстное меню настроек

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 (рис.5.2.4).

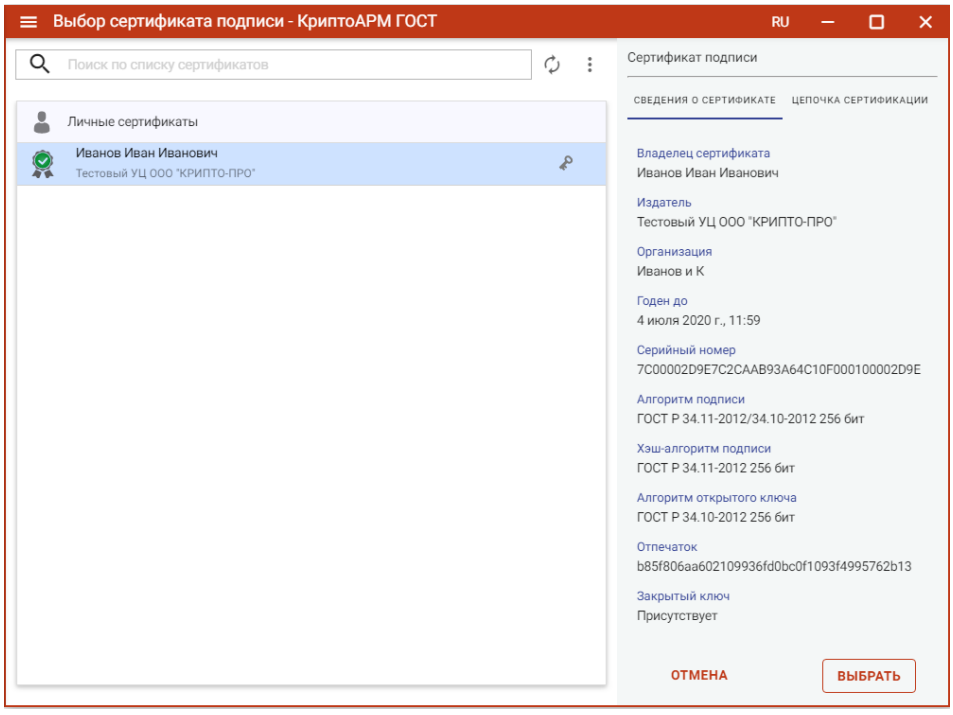


Рис. 5.2.4. Выбор сертификата подписи

Выбор сертификата подписи осуществляется его выделением и нажатием на кнопку **Выбрать**. При этом выбранный сертификат становится сертификатом подписи по умолчанию в выбранной настройке. При следующем запуске приложения данный сертификат будет уже выбран в качестве сертификат подписи.

Сертификат подписи можно изменить с помощью контекстного меню (рис. 5.2.5).

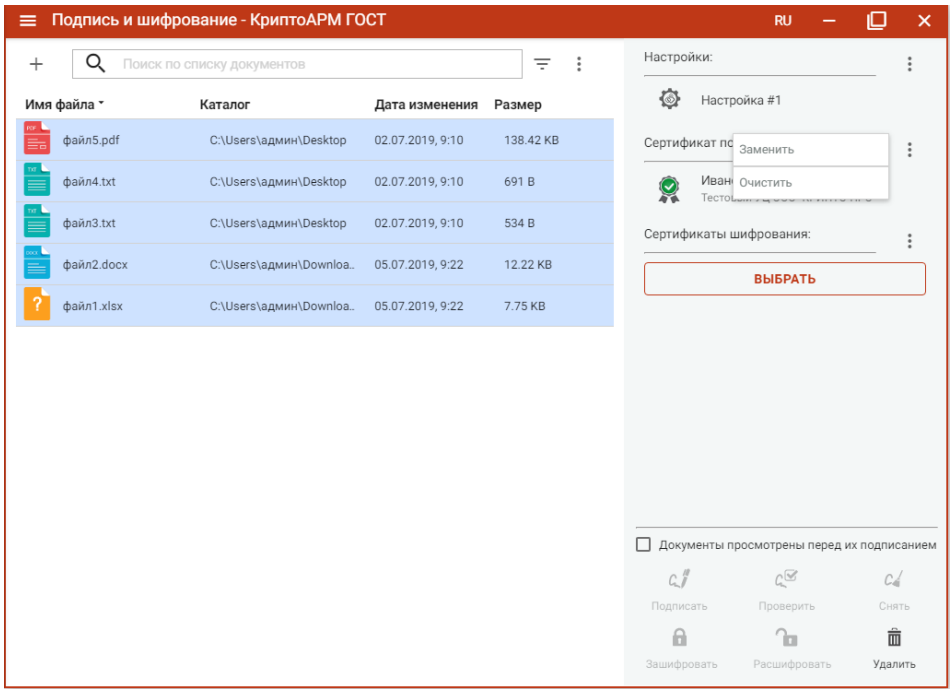


Рис. 5.2.5. Изменение сертификата подписи

Если в хранилище личных сертификатов нет сертификата с закрытым ключом, то можно создать или импортировать сертификат, воспользовавшись контекстным меню списка сертификатов (рис. 5.2.6).

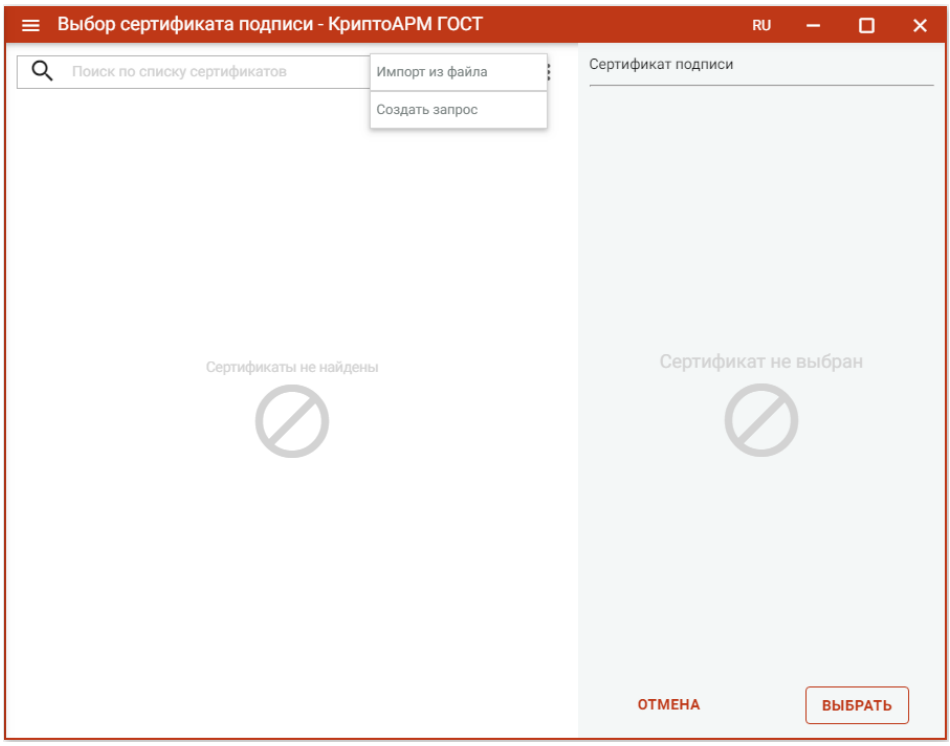


Рис. 5.2.6. Добавление сертификата подписи

Подпись файлов. При условии выбора сертификата подписчика, файлов для подписи и установленного флага, что документы просмотрены перед подписанием, в мастере становится доступной кнопка **Подписать** (рис.5.2.7).

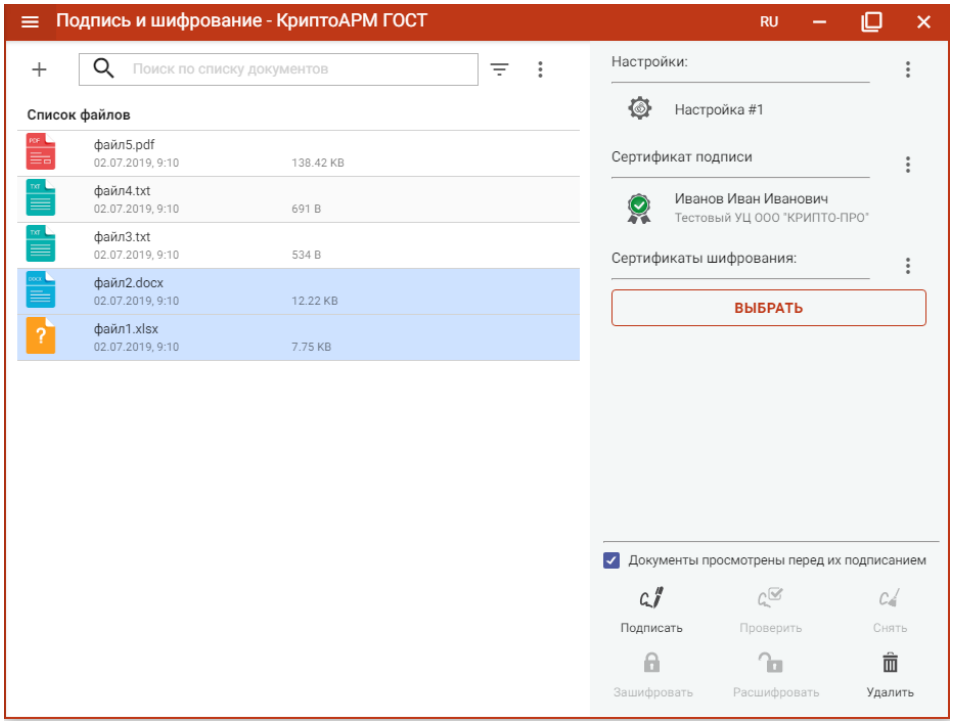


Рис.5.2.7. Подпись файлов

Нажатие на кнопку **Подписать** запускает процесс подписи. Выбранные файлы подписываются по очереди. Для подписанных файлов меняется иконка, наименование, дата создания. Сразу происходит проверка подписи, результат которой отображается в виде индикатора на иконке подписанного файла.

Если в настройках стоит флаг «Сохранить в разделе Документы», то подписанные файлы они сохраняются в каталог /Trusted/CryptoARM GOST/Documents в папке пользователя, и доступны в пункте меню **Документы**.

Для подписанных файлов становятся доступны кнопки **Проверить** и **Снять** (рис. 5.2.8).

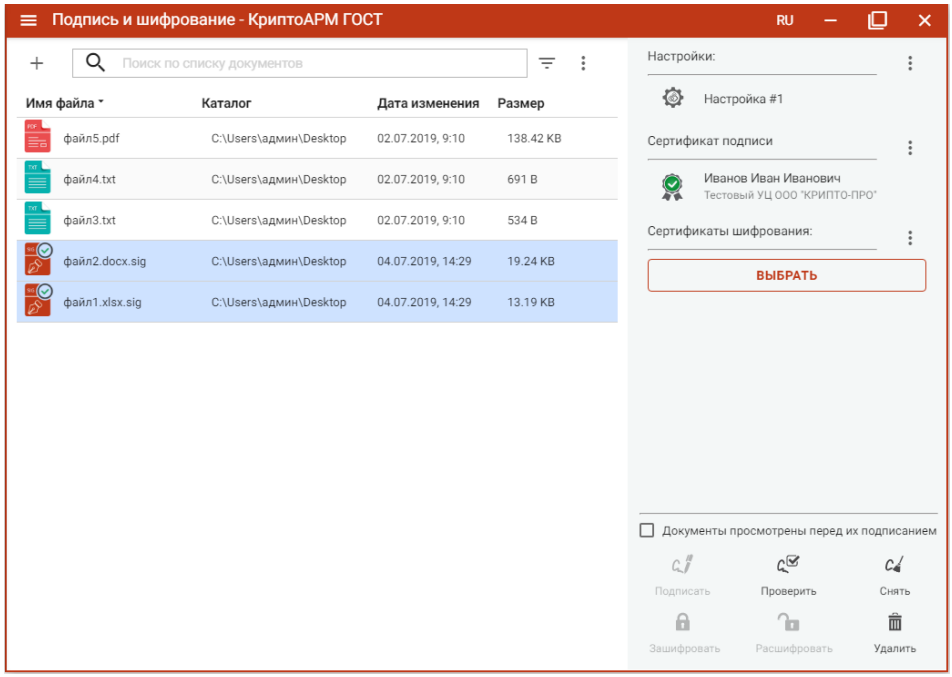


Рис.5.2.8. Подписанные файлы

5.3. Подпись сертификатом DSS

Подпись сертификатом DSS ничем не отличается от подписи обычным сертификатом, за исключением некоторых шагов. Также нужно выбрать файлы для подписи, выбрать сертификат DSS подписчика и установить флаг, что документы просмотрены перед подписанием (рис. 5.3.1).

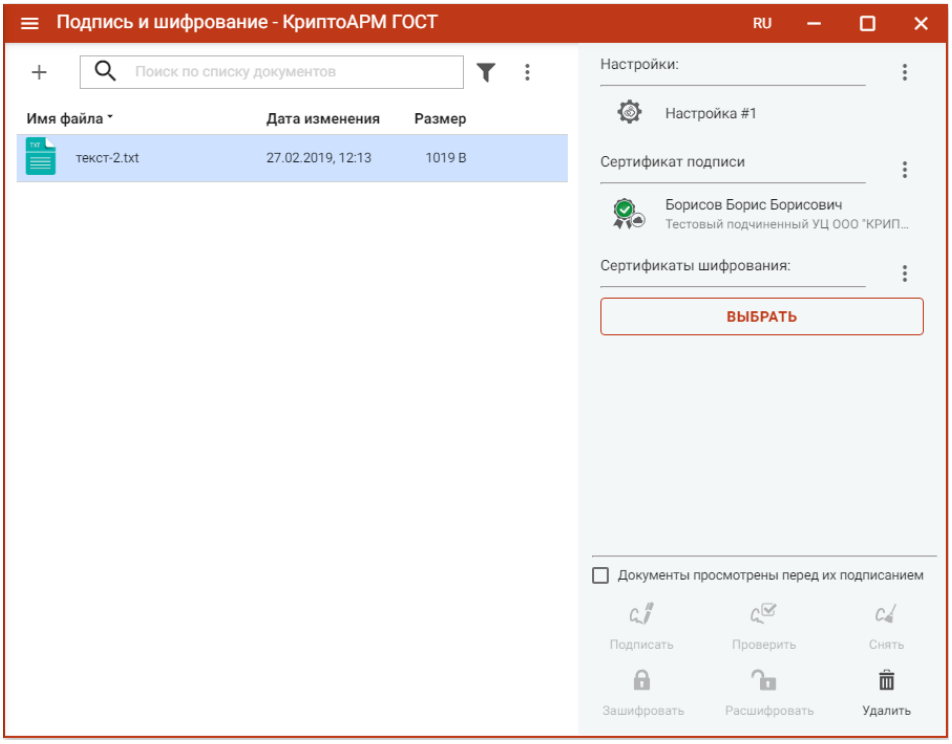


Рис. 5.3.1. Выбор файлов и сертификата для подписи DSS

При нажатии на кнопку **Подписать** открывается окно для ввода пароля к ключевому контейнеру (рис. 5.3.2). Если пароль не задан, то данный шаг пропускается.

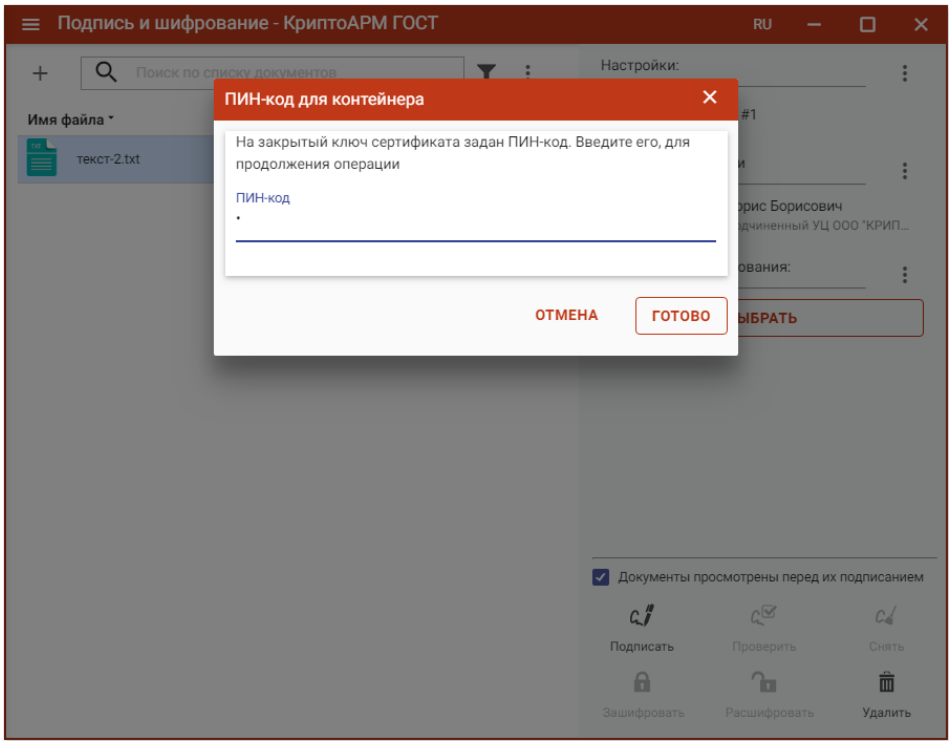


Рис. 5.3.2. Ввод пароля к ключевому контейнеру

Если у пользователя в личном кабинете DSS в настройках аутентификации стоит подтверждение операции подписи по SMS, по электронной почте или с помощью мобильного приложения, то на следующем шаге появляется сообщение, что операцию нужно подтвердить (рис. 5.3.3).

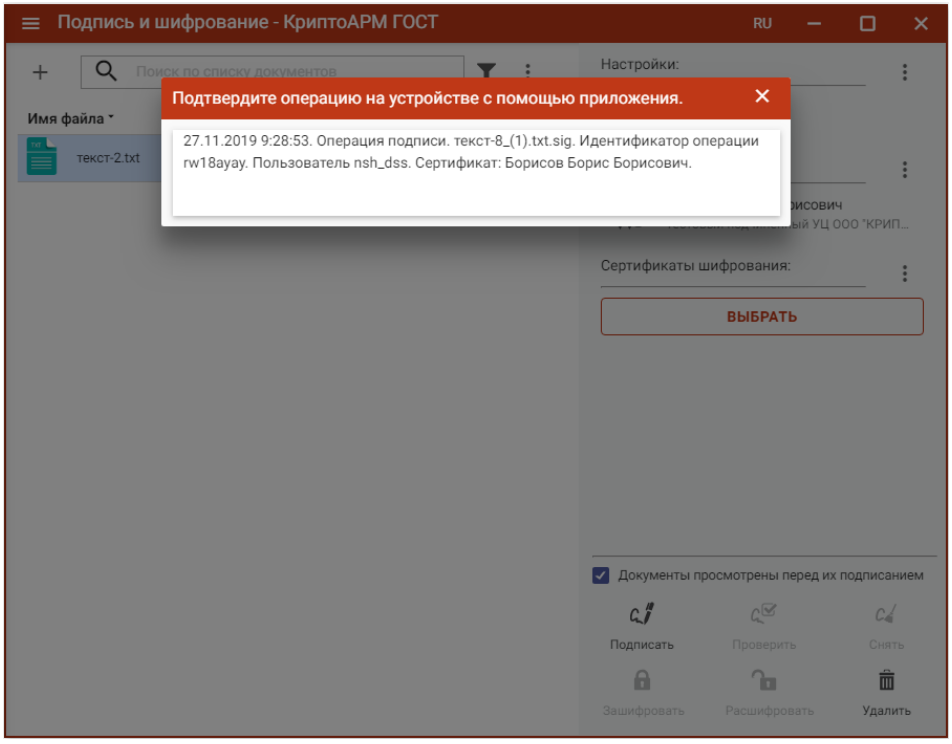


Рис. 5.3.3. Окно ожидания подтверждения операции подписи

После подтверждения операции на устройстве происходит подпись файла.

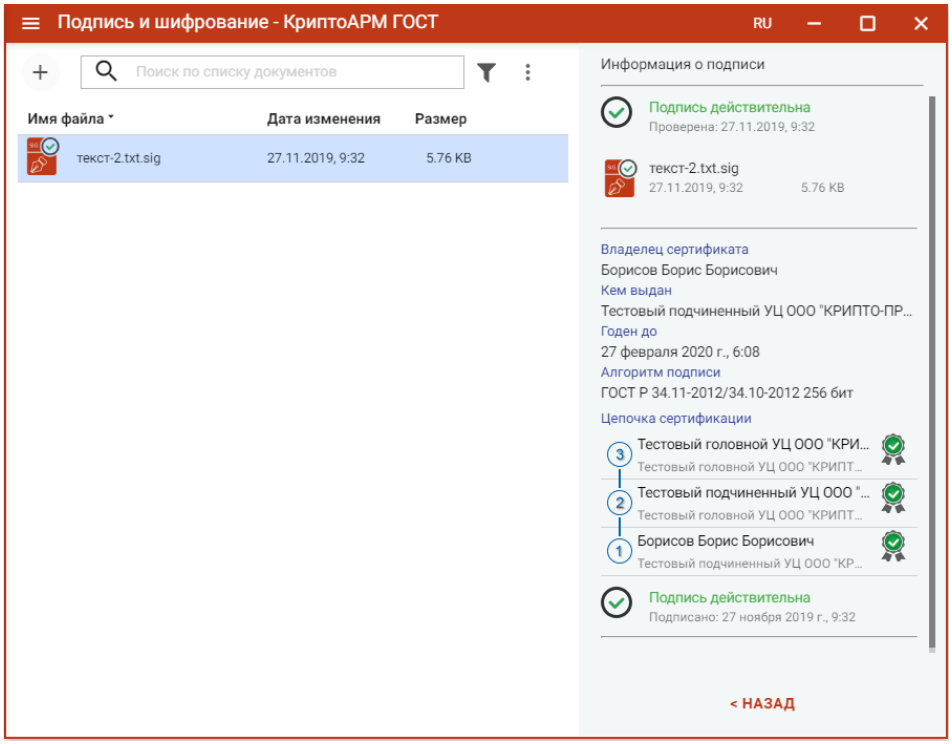


Рис. 5.3.4. Подписанный файл

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

5.4. Проверка электронной подписи

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

Если при проверке, отделенной от подписываемого файла подписи, исходный файл не будет найден автоматически, будет предложен его выбор.

Результат проверки подписей отображается в виде общего сообщения и цветового индикатора на иконке для каждого файла (рис. 5.4.1): зеленый - подпись действительна; красный - подпись недействительна.

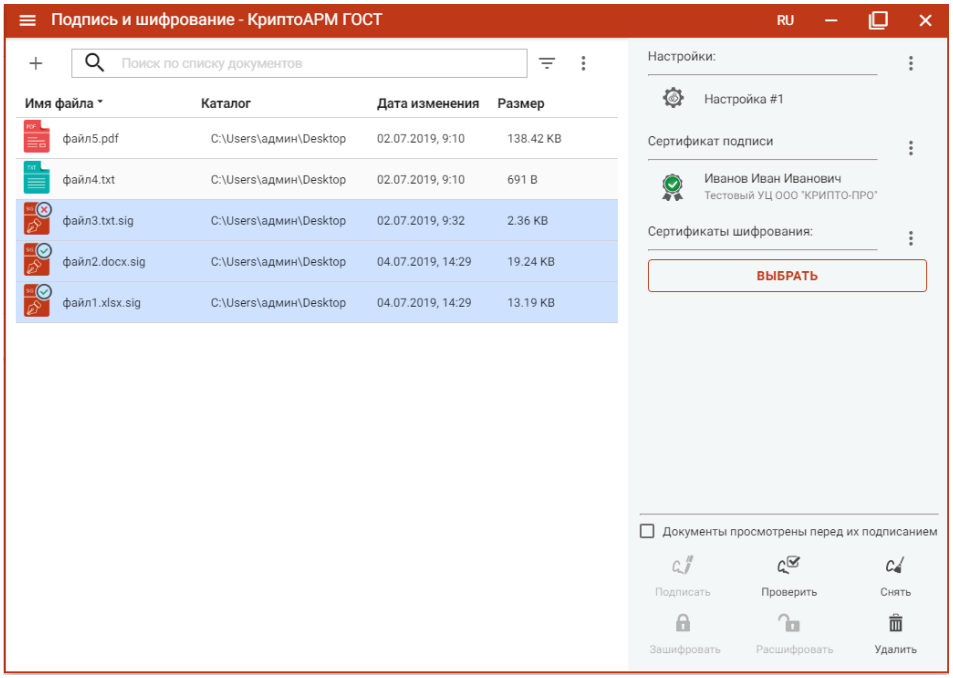


Рис. 5.4.1. Результат проверки подписи файлов

При выделении одного подписанного файла в правой области отображается информация о подписи (рис. 5.4.2).

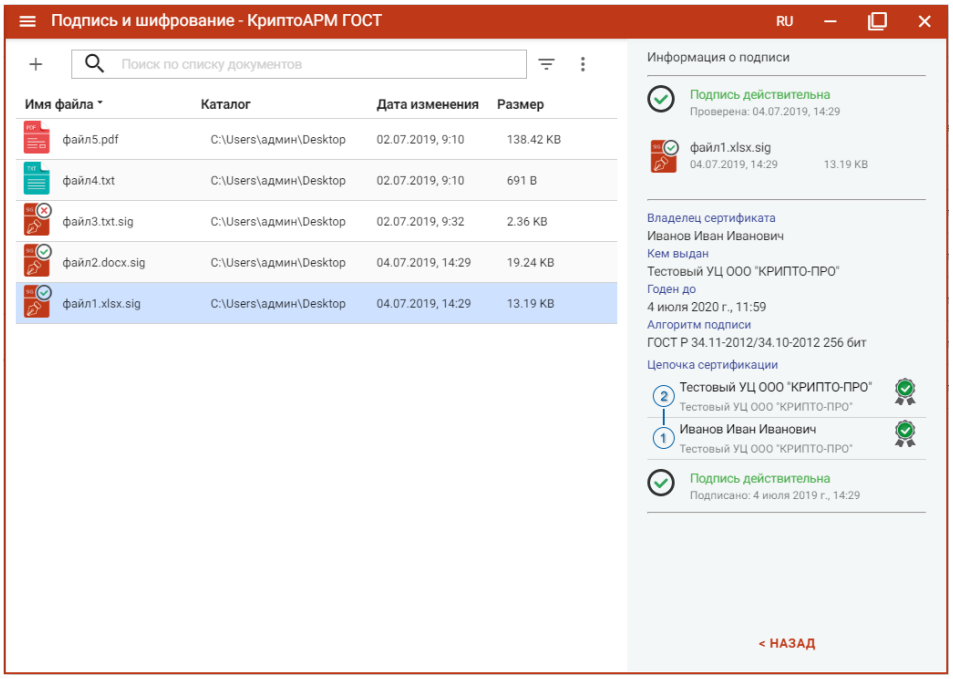


Рис. 5.4.2. Отображение информации о подписи

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

5.5. Снятие электронной подписи

Для снятия подписи достаточно выбрать подписанные файлы - файлы с расширением **.sig**, которые содержат электронную подпись и нажать на кнопку **Снять** (рис. 5.5.1).

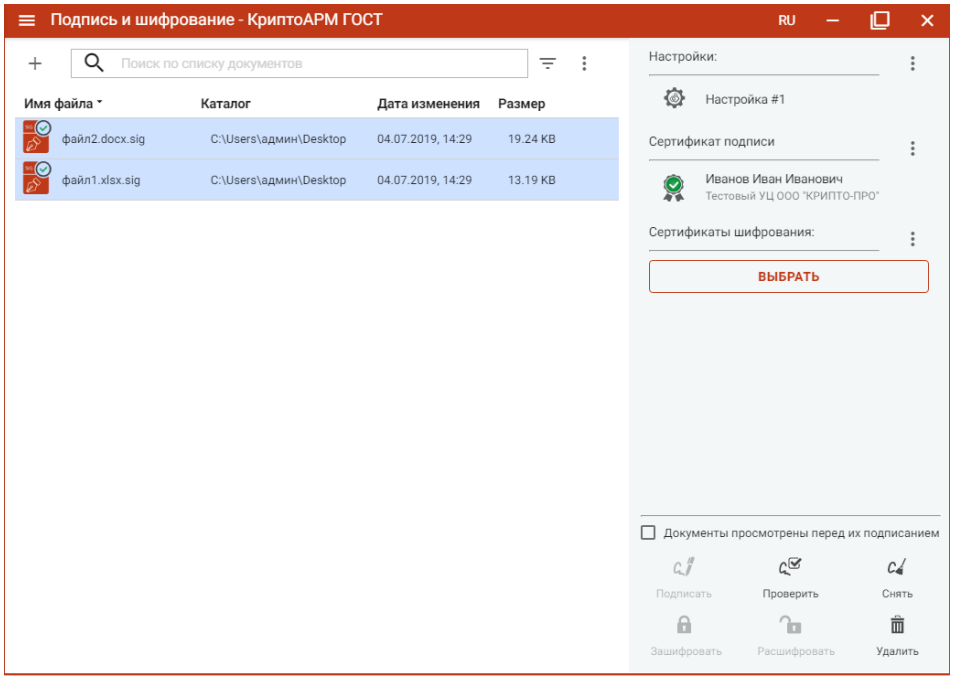


Рис. 5.5.1. Выделенные файлы для снятия подписи

При снятии подписи у файлов меняется иконка, наименование, дата создания. Если в настройках подписи установлен флаг «Сохранить в разделе Документы», то файлы сохраняются в каталог с документами в папке пользователя /.Truste/CryptoARM GOST/Documents/ (рис. 5.5.2).

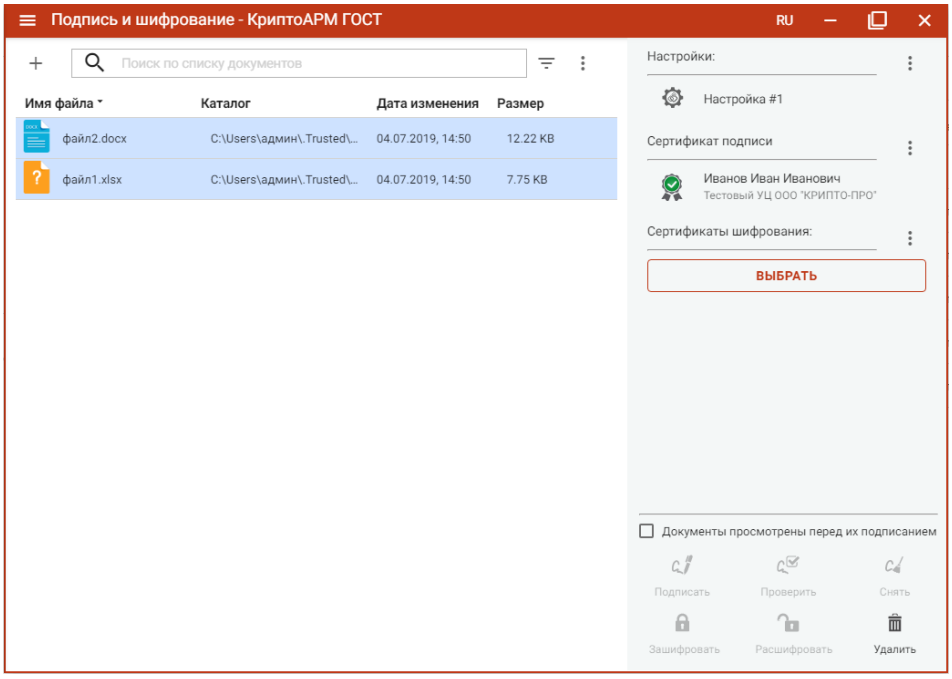


Рис. 5.5.2. Результат снятия подписи с файлов

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

5.6. Добавление подписи

Приложение КриптоАРМ ГОСТ позволяет добавлять электронные подписи к уже подписанному файлу. Добавление подписи осуществляется по нажатию на кнопку **Подписать**, при условии, что выбран сертификат подписи, файлы, содержащие электронную подпись (файлы с расширением **.sig)** и установлен флаг, что документы просмотрены перед подписанием (рис. 5.6.1).

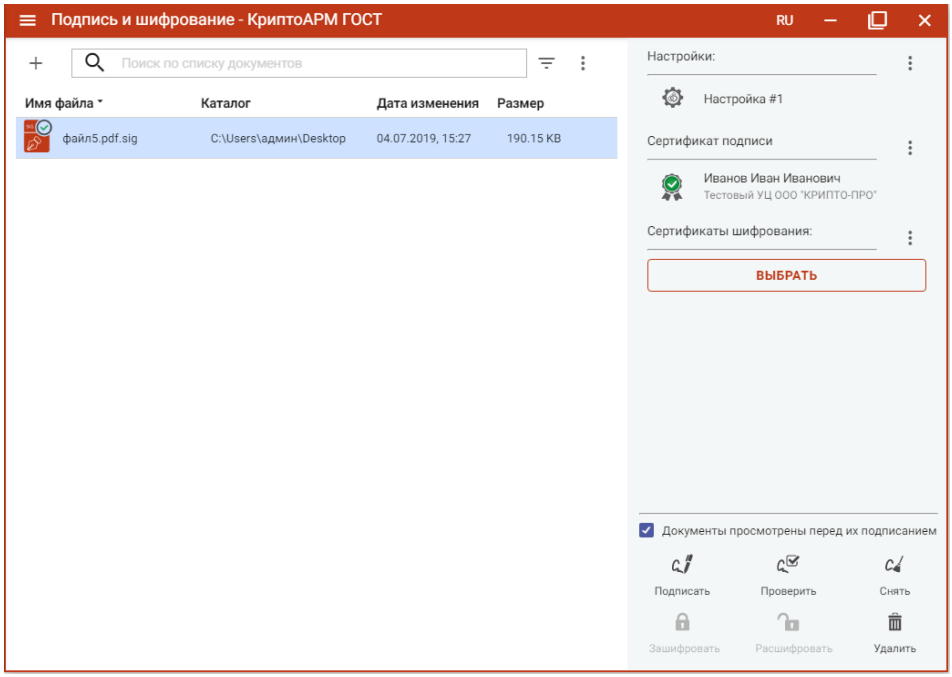


Рис. 5.6.1. Добавление подписи к уже подписанным файлам

Для всех добавленных подписей настройки подписи используются по умолчанию, как для первой подписи. В информации о подписи содержатся сведения о всех подписях (рис. 5.6.2).

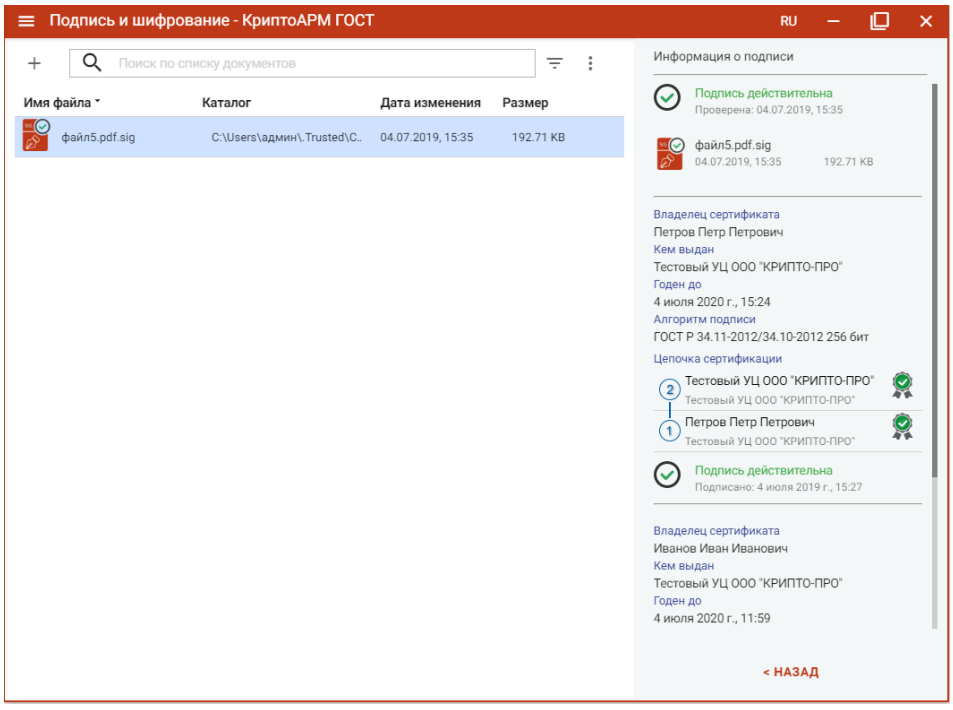


Рис. 5.6.2. Отображение информации о нескольких подписях файла

5.7. Шифрование файлов

Для шифрования файлов нужно выбрать файлы, сертификаты получателей и задать настройки шифрования. Зашифровать файлы на странице **Подпись и шифрование** или **Документы**.

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

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (рис. 5.7.1).

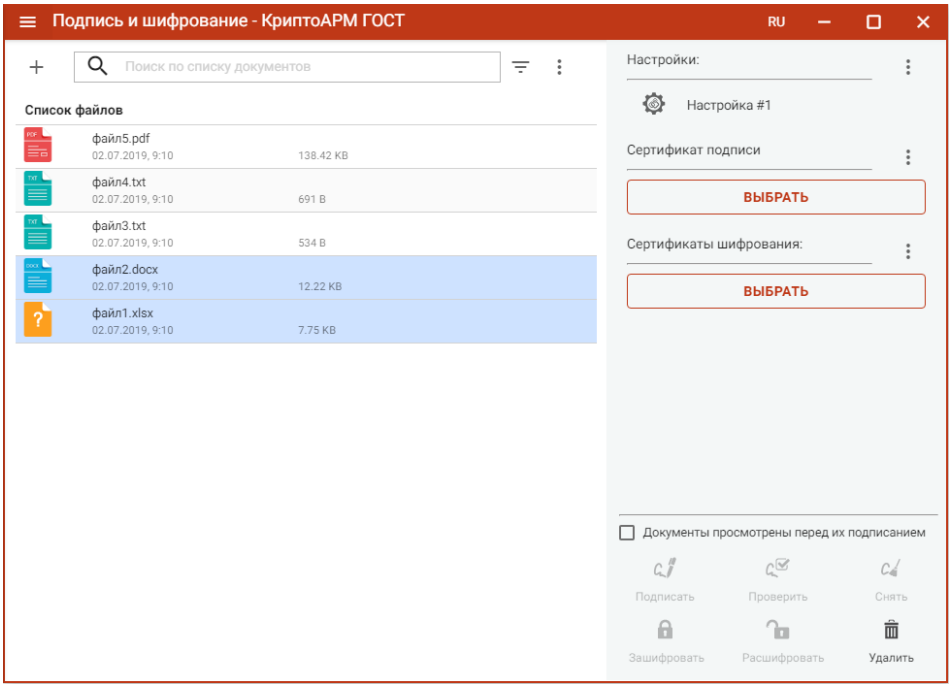


Рис. 5.7.1. Список файлов для шифрования

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (рис. 5.7.2).

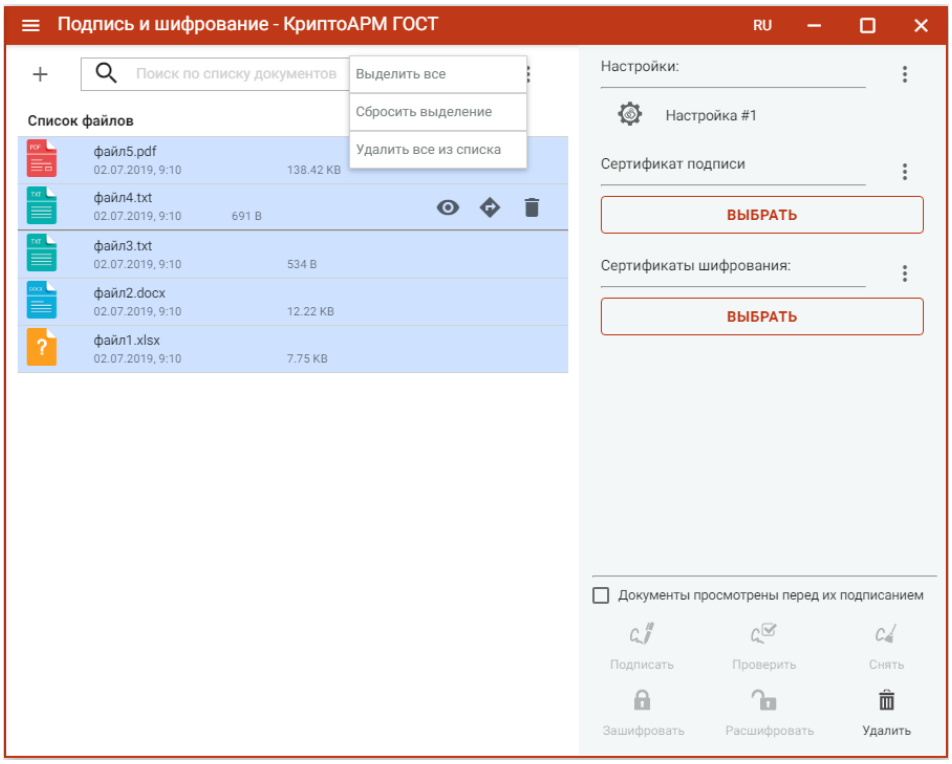


Рис. 5.7.2. Контекстное меню управления списком файлов

НАСТРОЙКИ ШИФРОВАНИЯ. При первом запуске приложения создается настройка по умолчанию «Настройка #1», в которой задается кодировка зашифрованного файла base64., без дополнительных настроек шифрования

Для изменения настроек шифрования можно изменить текущую настройку, выбрав в контекстном меню **Изменить** (рис. 5.7.3), или добавить новую настройку, выбрав пункт меню **Настройки**.

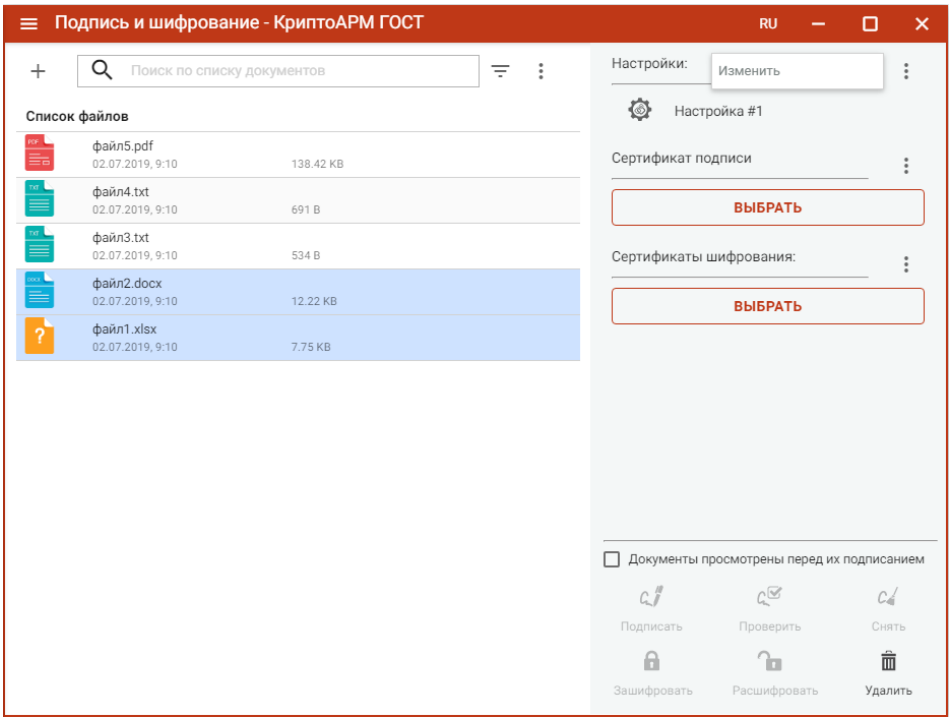


Рис. 5.7.3. Контекстное меню настроек

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** (рис.5.7.4).

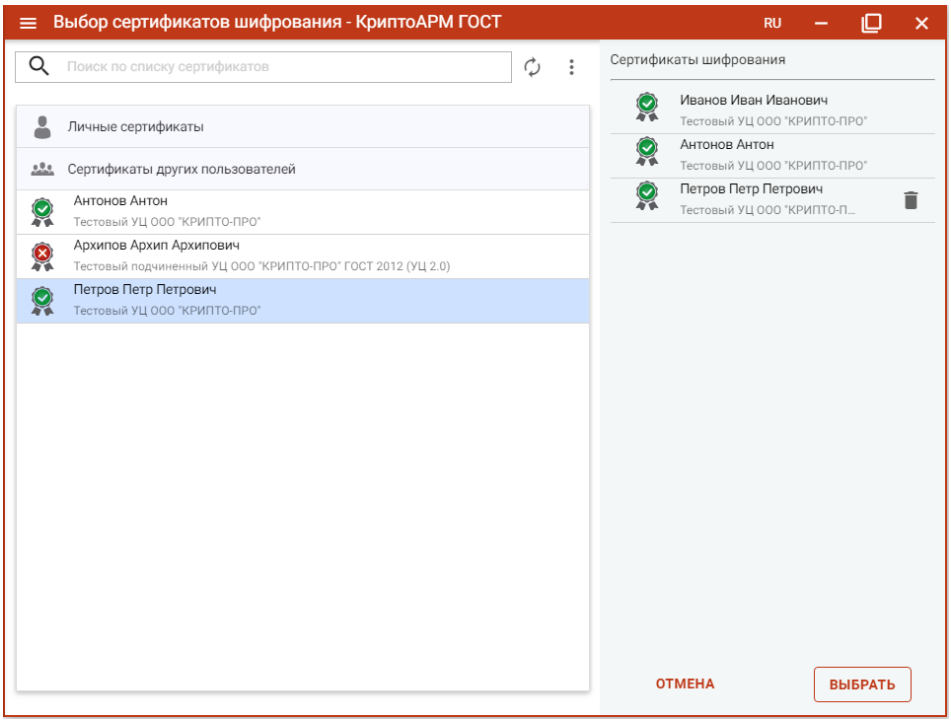


Рис. 5.7.4. Выбор сертификатов шифрования

В списке сертификатов 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 (рис. 5.7.5).

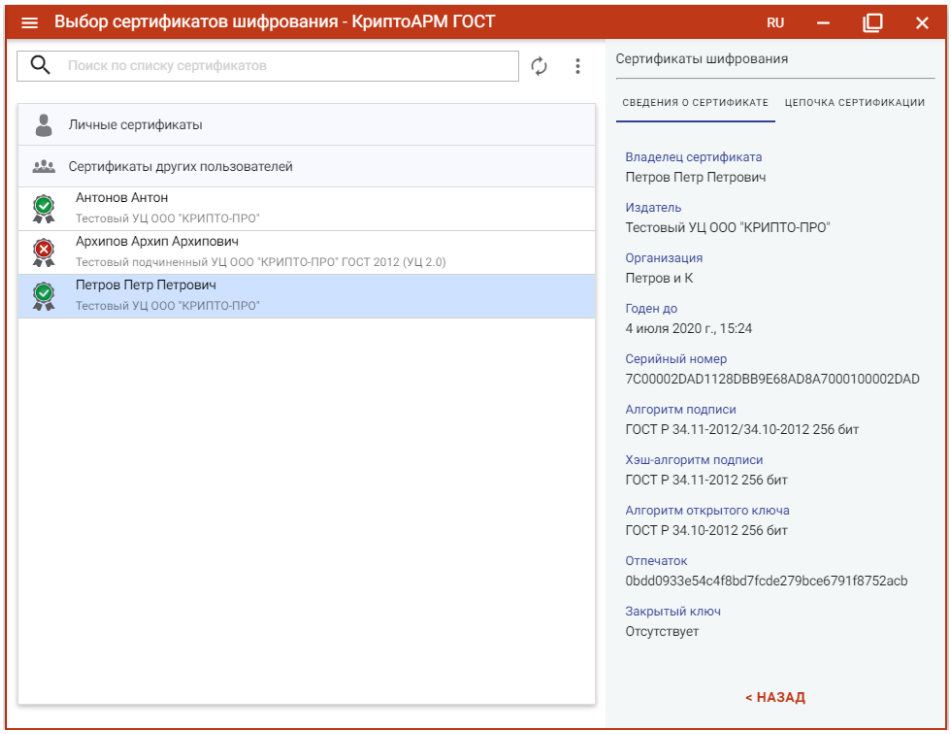


Рис. 5.7.5. Информация о сертификате шифрования

Если список сертификатов получателей заполнен, то его можно зафиксировать нажатием на кнопку **Выбрать**. При этом выбранные сертификаты становятся сертификатами шифрования по умолчанию в выбранной настройке. При следующем запуске приложения данные сертификаты уже будут выбраны в качестве сертификатов получателей.

Изменить список сертификатов шифрования можно с помощью контекстного меню (рис. 5.7.6). Удалить сертификаты из сформированного списка можно кнопкой **Удалить**.

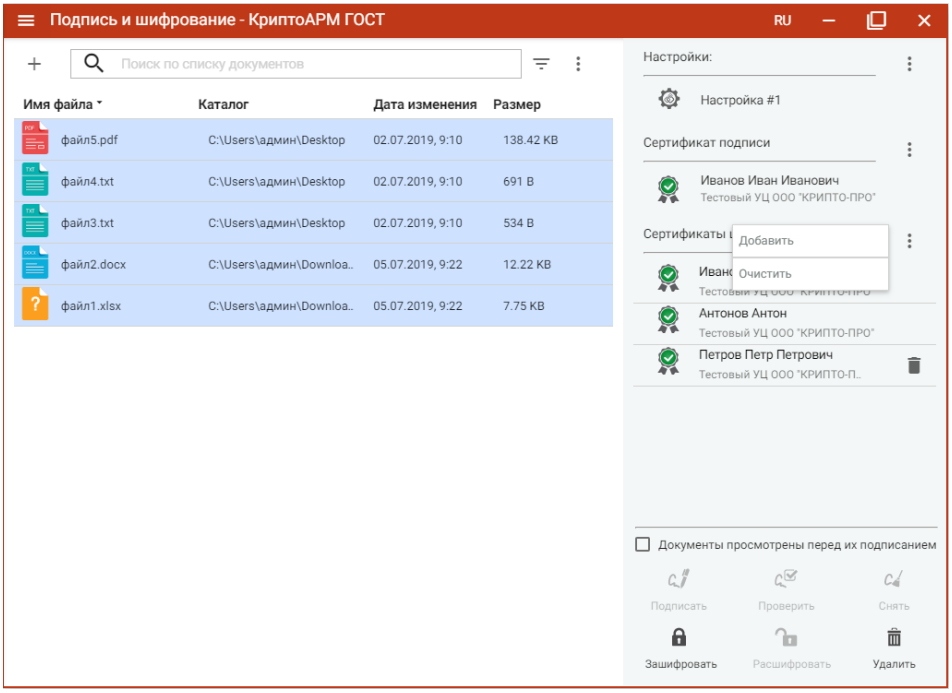


Рис. 5.7.6. Изменение списка сертификатов шифрования

Если список личных сертификатов и сертификатов других пользователей пуст, то можно создать или импортировать сертификат, воспользовавшись контекстным меню списка сертификатов (рис. 5.7.7).

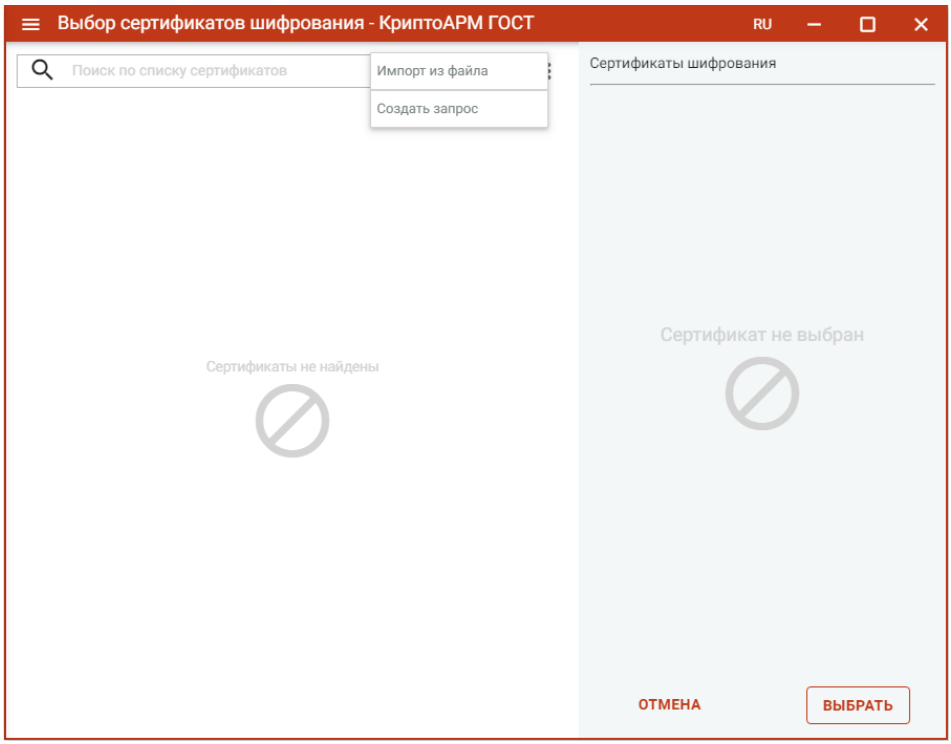


Рис. 5.7.7. Добавление сертификатов шифрования

ШИФРОВНИЕ ФАЙЛОВ. При условии выбора сертификатов получателей и файлов в мастере становится доступной кнопка **Зашифровать** (рис.5.7.8).

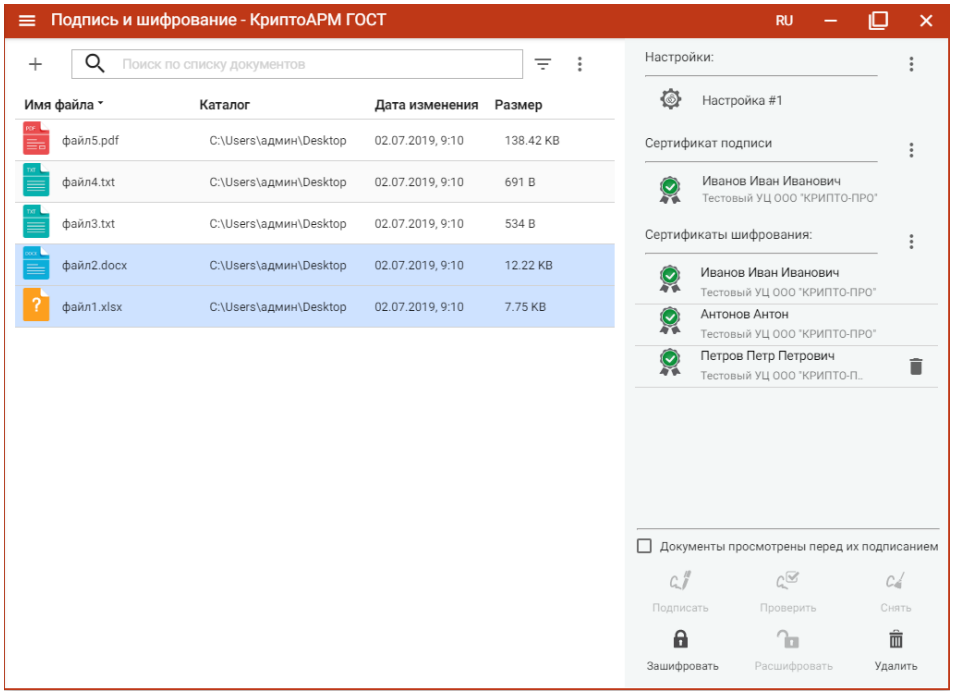


Рис. 5.7.8. Шифрование файлов

Нажатие на кнопку **Зашифровать** запускает процесс шифрования. Выбранные файлы шифруются по очереди. Для зашифрованных файлов меняется иконка, наименование, дата создания.

Если в настройках стоит флаг «Сохранить в разделе Документы», то файлы сохраняются в каталог /Trusted/CryptoARM GOST/Documents в папке пользователя, и доступны в пункте меню **Документы**.

Для зашифрованных файлов становится доступна кнопка **Расшифровать** (рис. 5.7.9).

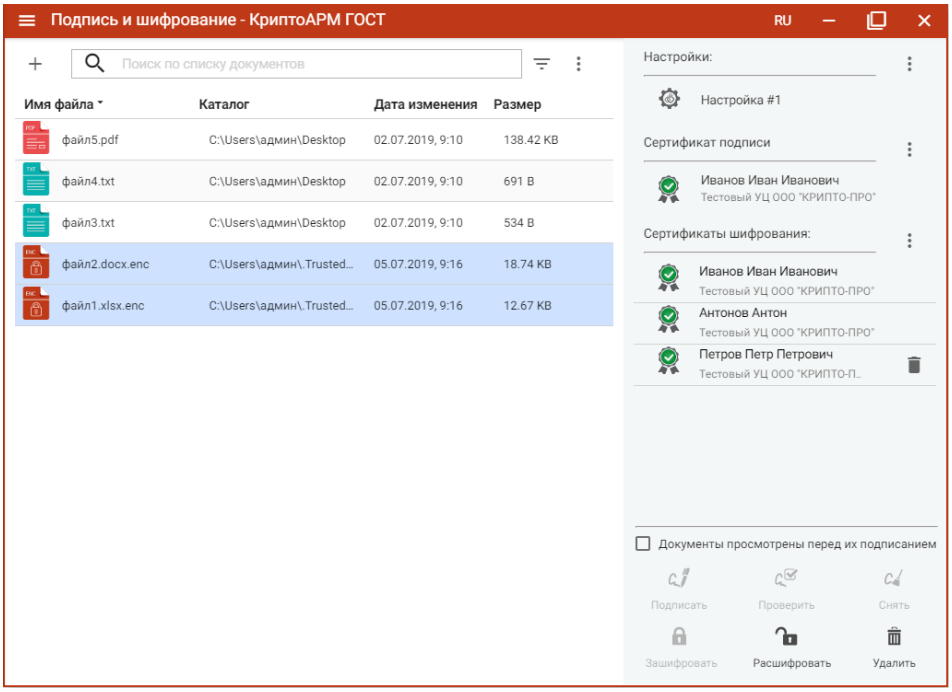


Рис. 5.7.9. Зашифрованные файлы

5.8. Расшифрование файлов

Для расшифрования достаточно выбрать файлы - файлы с расширением **.enc**, и нажать на кнопку **Расшифровать**. Если в хранилище сертификатов не окажется сертификата с закрытым ключом, который был выбран в качестве сертификата получателя при шифровании, расшифрование не будет выполнено.

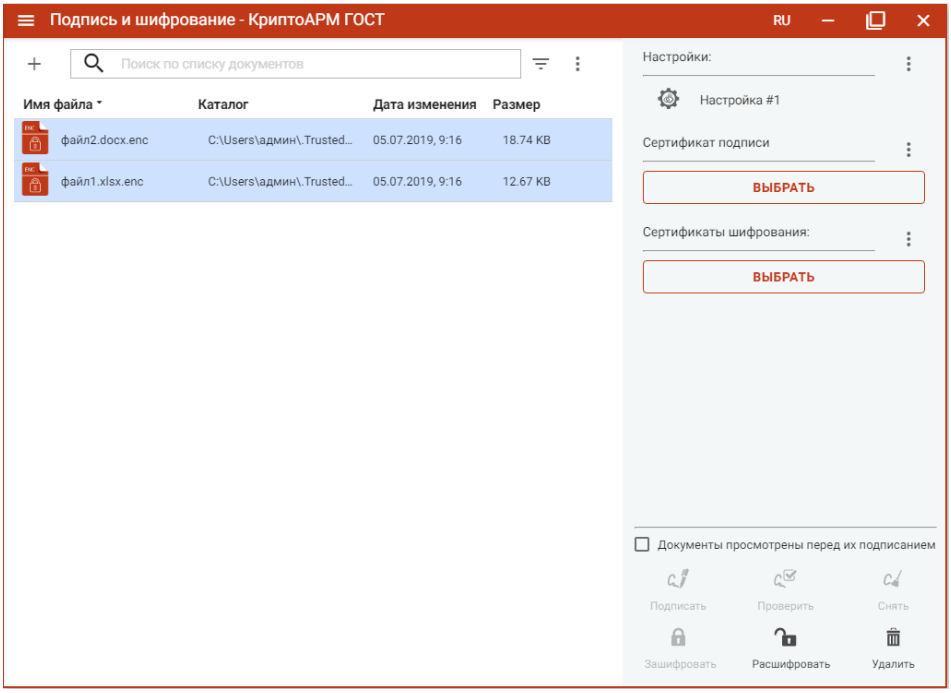


Рис. 5.8.1. Мастер расшифрования файлов

При расшифровании у файлов меняется иконка, наименование, дата создания (рис. 5.8.2). Если в настройках стоит флаг «Сохранить в разделе Документы», то файлы сохраняются в

каталог /Trusted/CryptoARM GOST/Documents в папке пользователя, и доступны в пункте меню **Документы**.

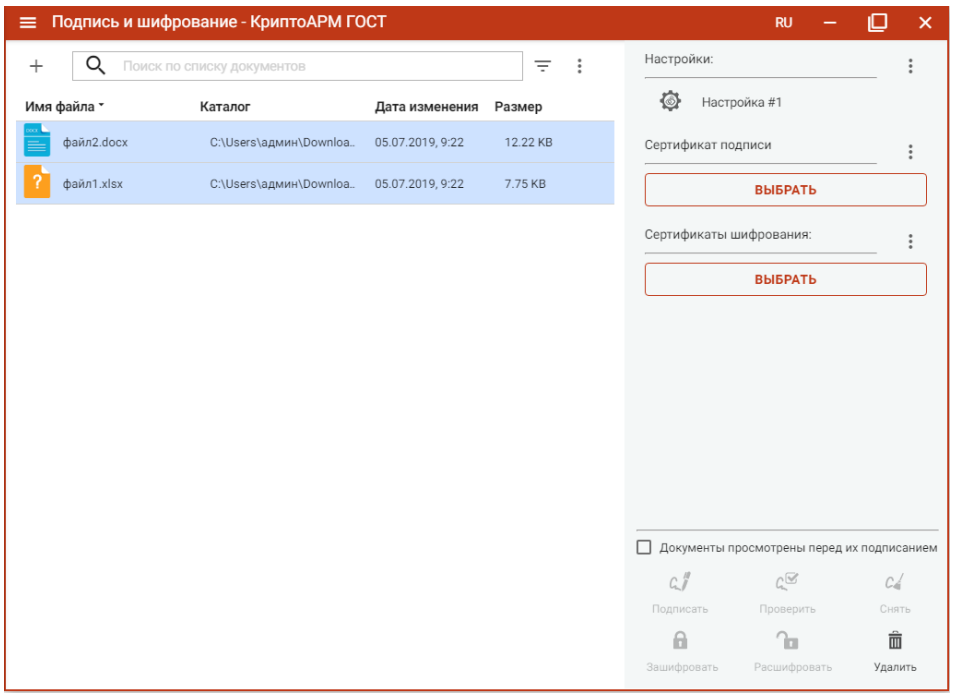


Рис. 5.8.2. Результат операции расшифрования

5.9. Управление списком файлов для выполнения операций

Список файлов для выполнения операций представляет собой одноуровневый список (рис. 5.9.1).

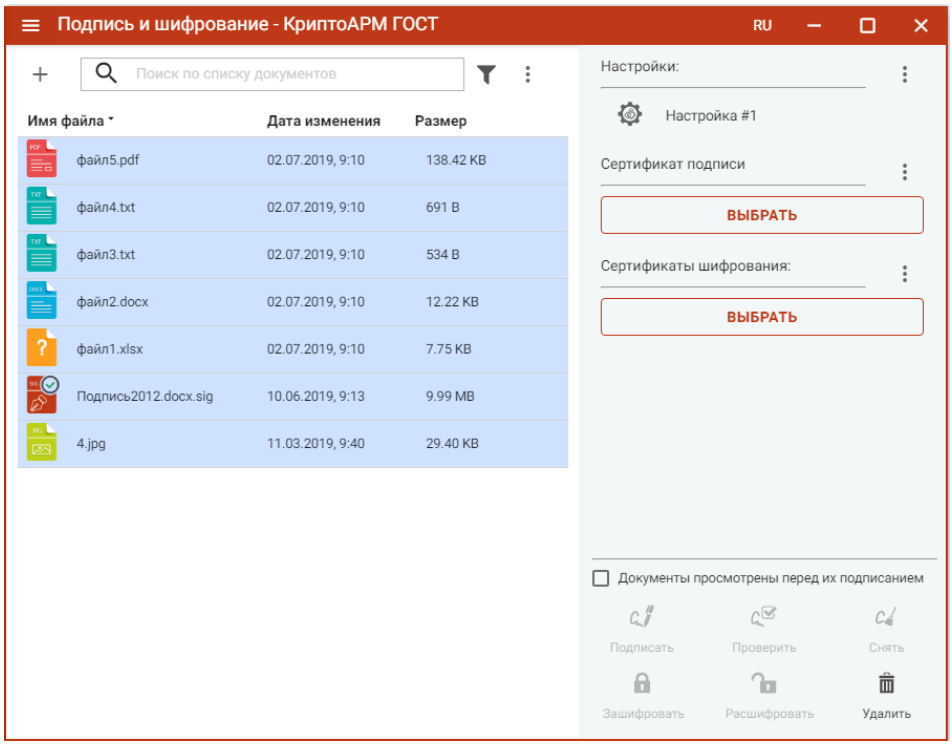


Рис. 5.9.1. Список файлов

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

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 (рис. 5.9.2), 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.

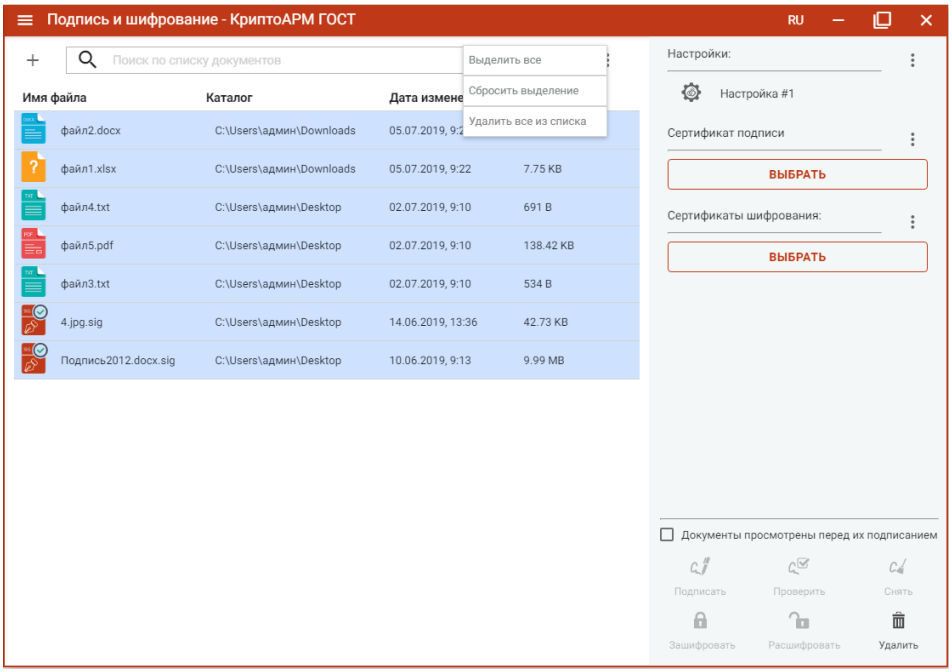


Рис. 5.9.2. Контекстное меню списком файлов

Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши (рис. 5.9.3):

- **Просмотр** - выполняется открытие файла через приложение, которое ассоциировано с его расширением;
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл;
- **Удалить**- файл удаляется из текущего списка. При выполнении этой операции файл остается в файловой системе в неизменном виде.

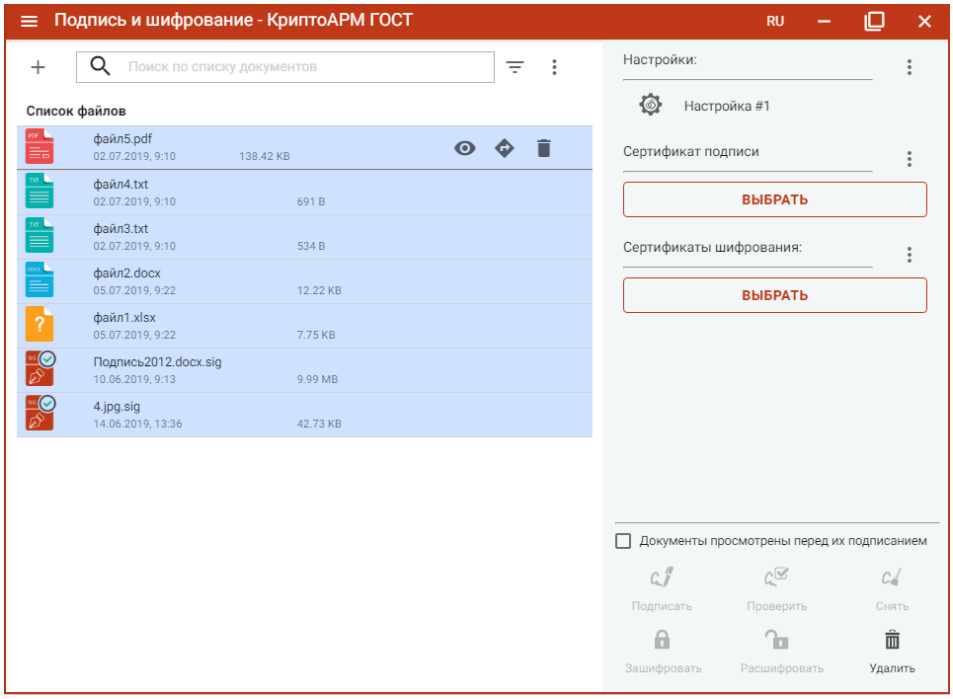


Рис. 5.9.3. Кнопки операций файла

Можно удалить все выделенные файлы в списке с помощью кнопки **Удалить** в разделе операций в правой области окна. Файлы не удаляются из файловой системы.

В приложении реализован поиск файлов по символьному совпадению (рис. 5.9.4)

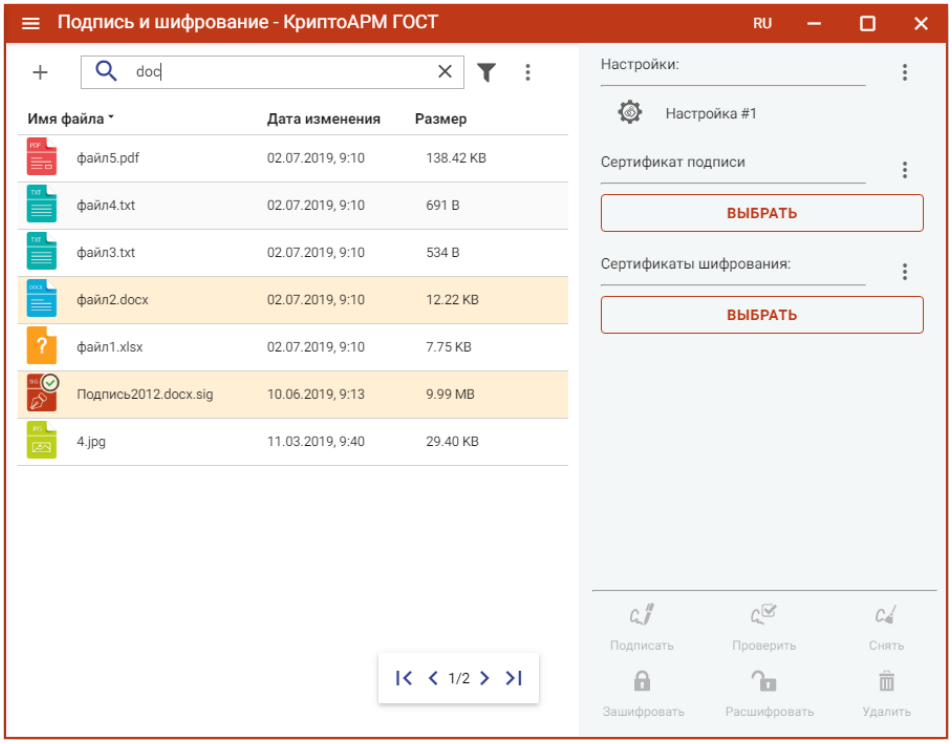


Рис. 5.9.4. Поиск файлов

Список файлов можно отфильтровать, задав настройки фильтрации (рис. 5.9.5).

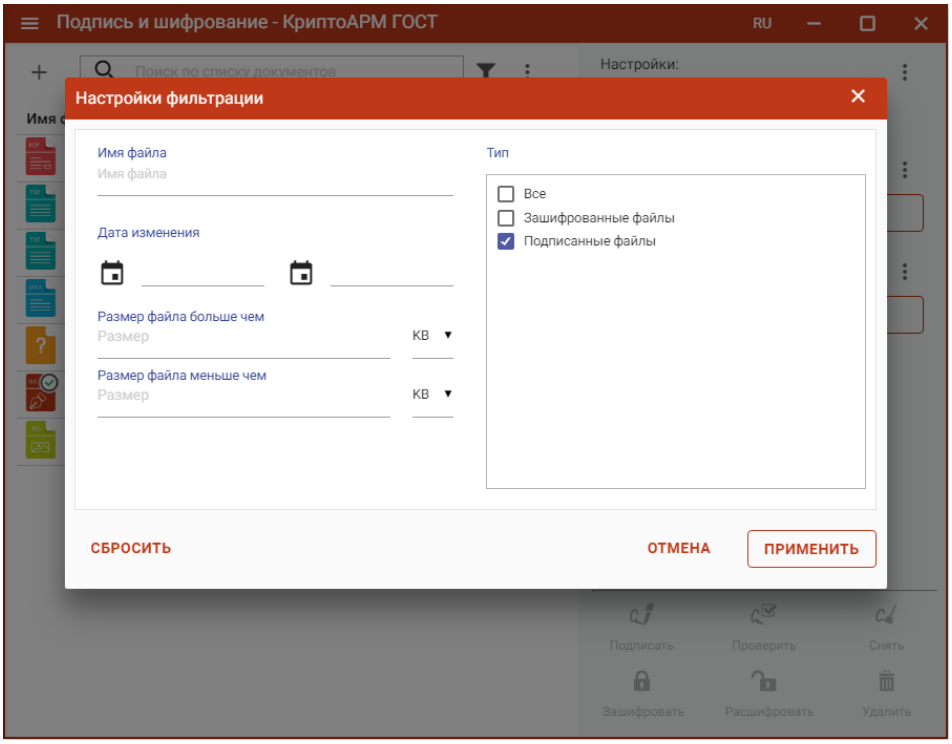


Рис. 5.9.5. Настройки критериев фильтра файлов

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

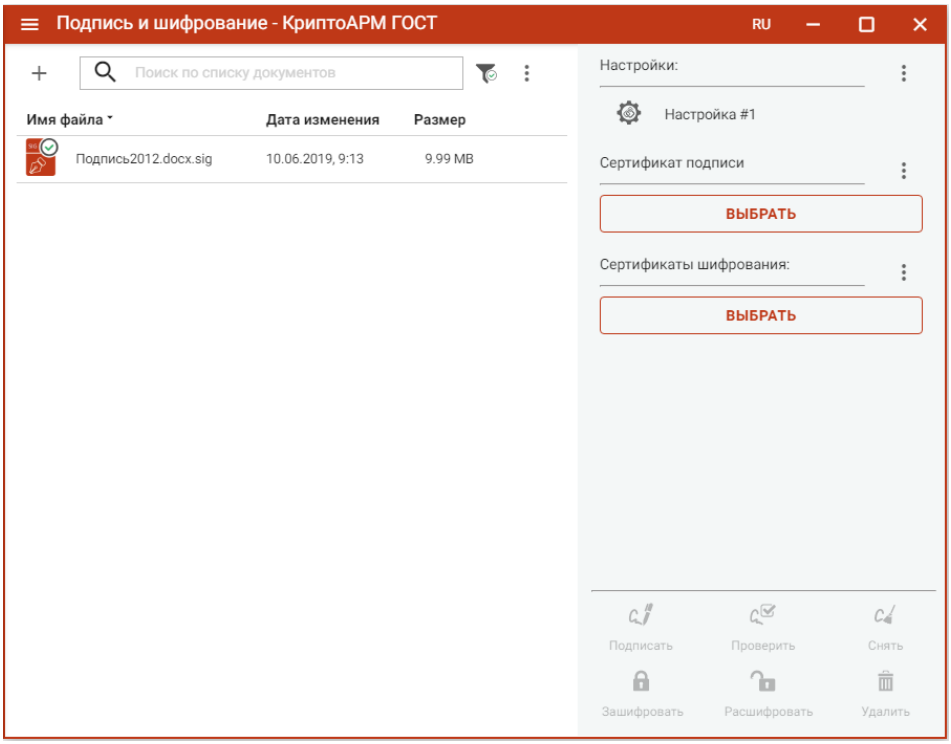


Рис. 5.9.6. Результат применения фильтрации файлов

Для сброса заданных критериев фильтрации служит кнопка «Сбросить» в окне настроек фильтрации (рис. 5.9.5).

5.10. Документы

Для сохранения результатов выполнения операций подписи, снятия подписи, шифрования и расшифрования используется каталог Документы. Каталог с документами располагается в каталоге пользователя в папке \.Trusted\CryptoARM GOST\Documents\. Просмотреть документы в каталоге можно, выбрав пункт меню **Документы** (рис. 5.10.1).

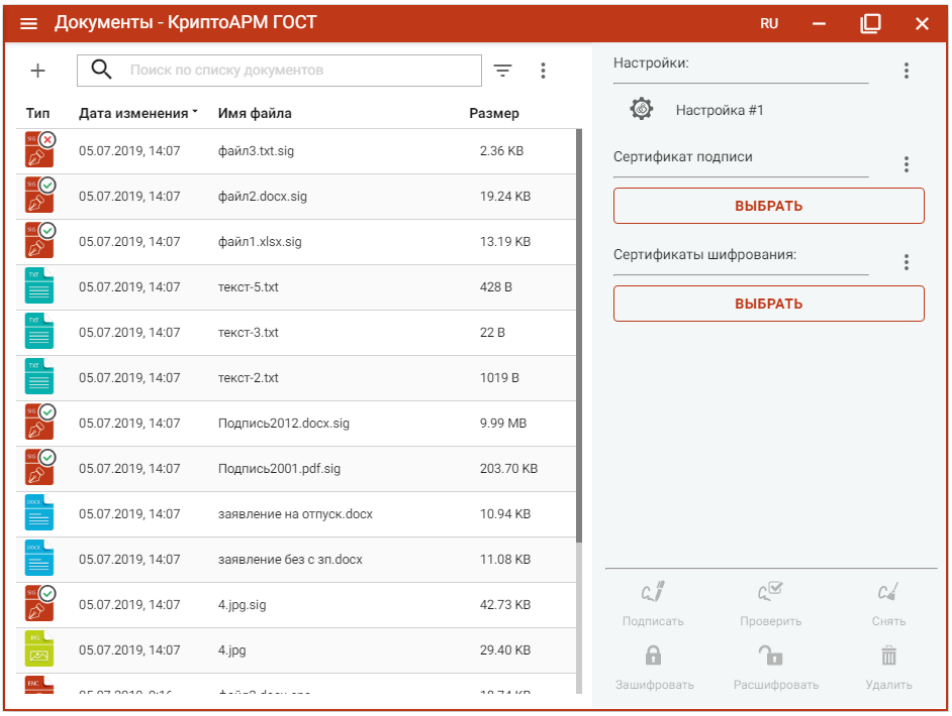


Рис. 5.10.1 Список документов

Формирование списка документов происходит двумя способами:

- файлы добавляются через кнопку Добавить файлы («+») (или перетаскиванием мышкой), при этом файлы физически копируются в папку \.Trusted\CryptoARM GOST\Documents\ в каталоге пользователя;
- в результате выполнения операций подписи, снятия подписи, шифрования и расшифрования, если в настройке стоит флаг «Сохранить в разделе Документы».

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 (рис. 5.10.2), состоящее из пунктов:

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

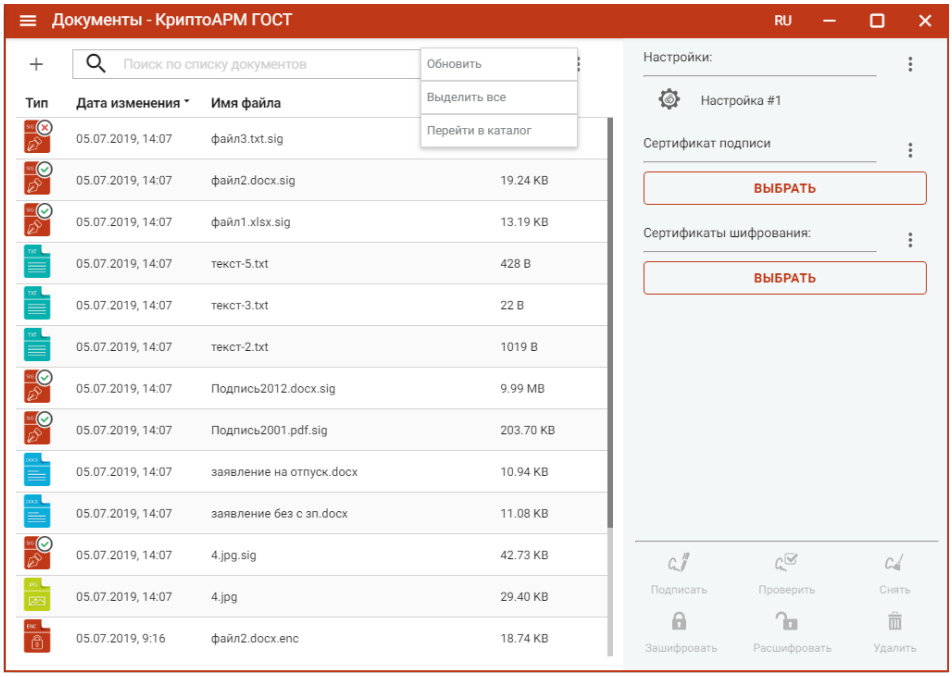


Рис. 5.10.2. Контекстное меню списка Документов

Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши (рис. 5.10.3):

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

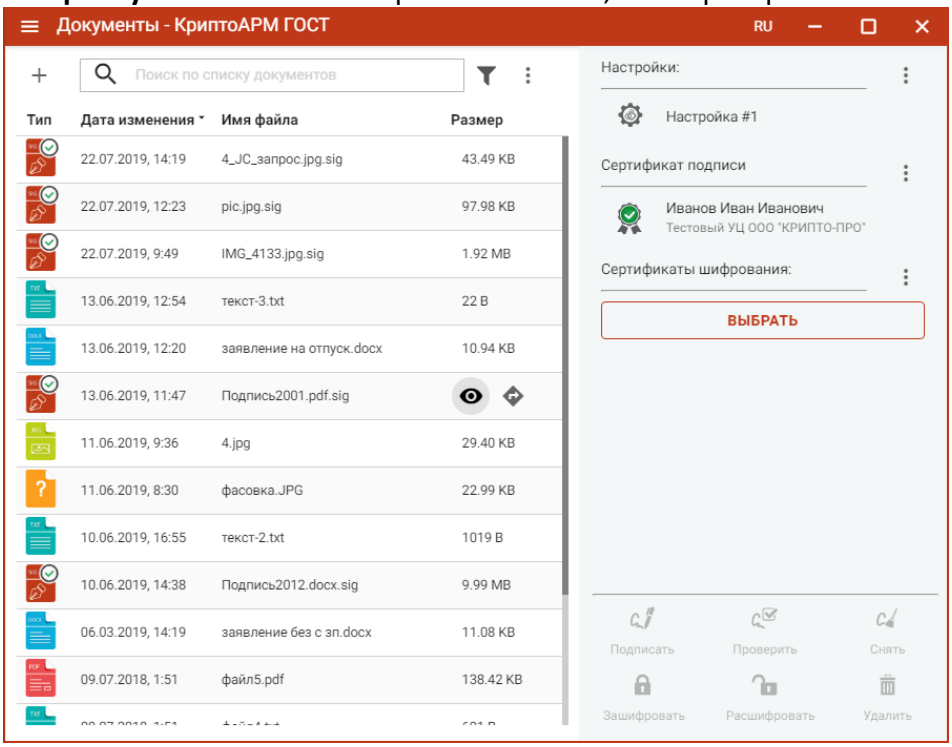


Рис. 5.10.3. Кнопки операций документа

Можно удалить все выделенные документы в списке с помощью кнопки **Удалить** в разделе операций в правой области окна. Документы удаляются из файловой системы.

В приложении реализован поиск документов по символьному совпадению (рис. 5.10.4)

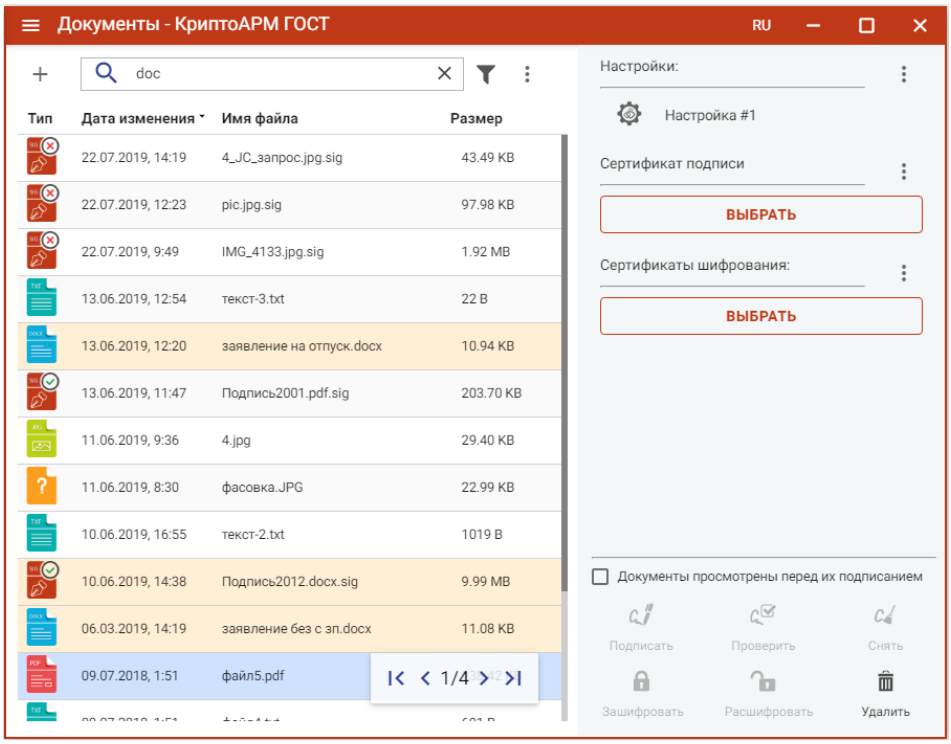


Рис. 5.10.4. Поиск документов

Список документов можно отфильтровать, задав настройки фильтрации (рис. 5.10.5).

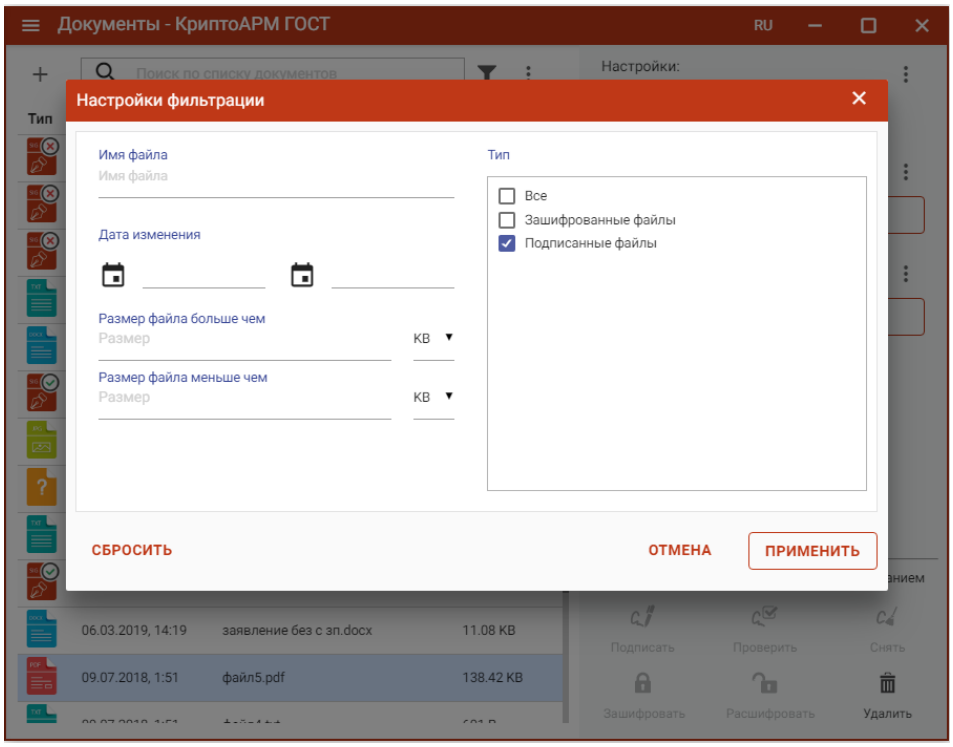


Рис.5.10.5. Настройки критериев фильтра документов

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.

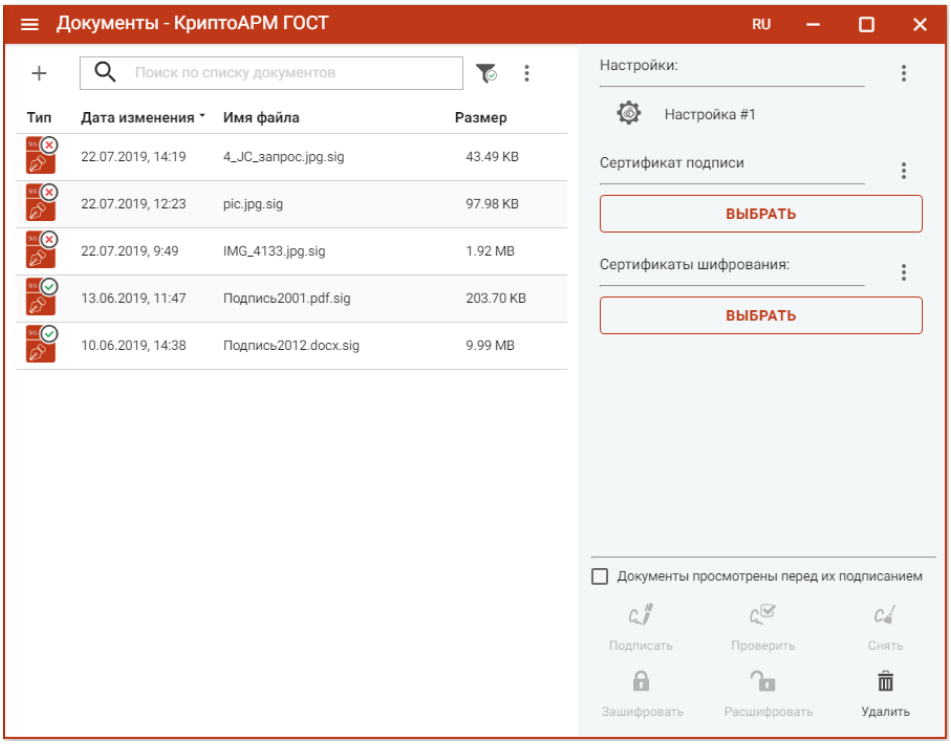


Рис. 5.10.6. Результат применения фильтрации документов

Для сброса заданных критериев фильтрации служит кнопка «Сбросить» в окне настроек фильтрации (рис. 5.10.5).

В зависимости от типа выделенных документов в списке и от выбранных сертификатов подписи и шифрования становятся доступны кнопки для выполнения операций с данными документами (рис. 5.10.7):

- **Подписать**;
- **Проверить подпись;**
- **Снять подпись**;
- **Зашифровать**;
- **Расшифровать.**

Выполнение операций аналогично операциям на вкладке **Подпись и шифрование**.

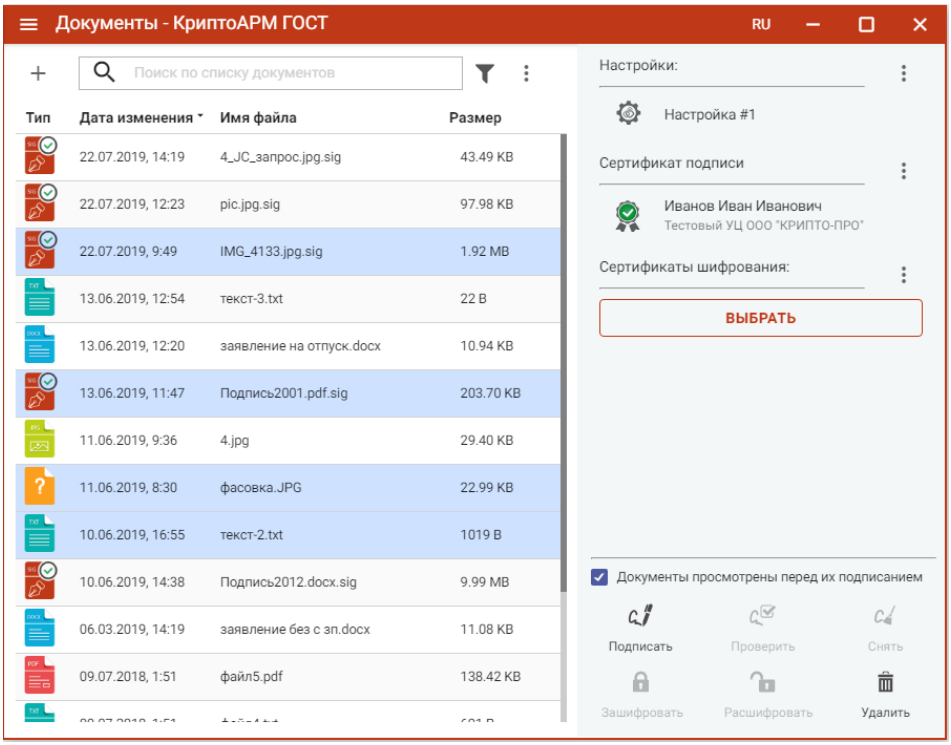


Рис. 5.10.7 Доступные операции для документов

5.11. Сертификаты

Для управления сертификатами в приложении добавлена отдельная вкладка списка сертификатов. В левой области представления отображаются разделы, соответствующие категориям сертификатов (рис. 5.11.1). В правой области отображается информация о выделенном сертификате.

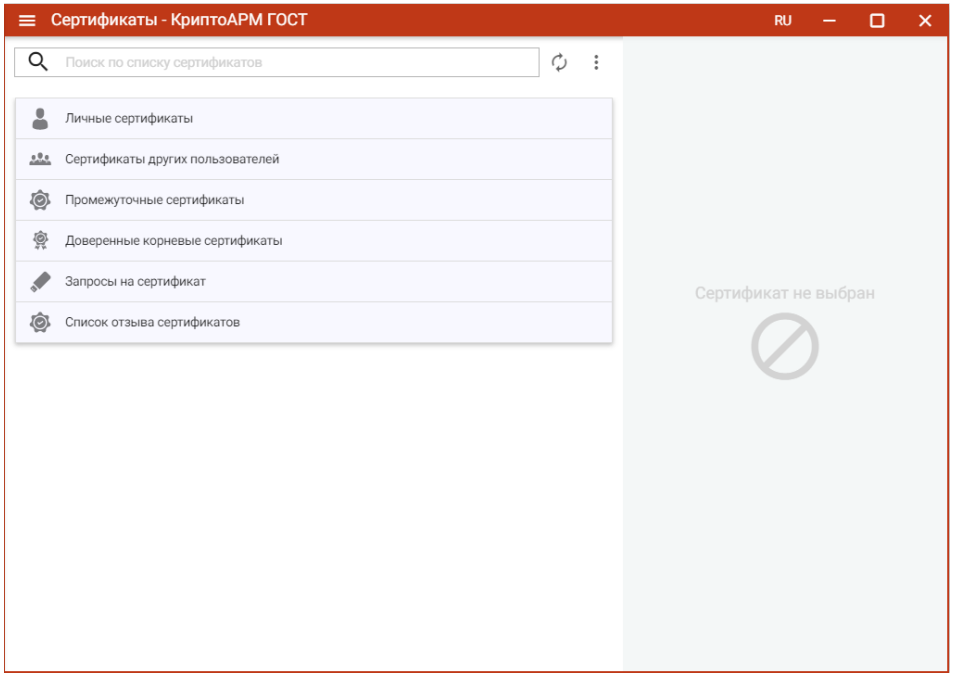


Рис. 5.11.1. Категории сертификатов

В каждой из категорий списка сертификатов отображаются сертификаты со всех подключённых хранилищ криптопровайдеров. В случае отсутствия сертификатов по отдельным категориям, категории могут быть скрыты как пустые. При отображении списка сертификатов, они проверяются на корректность (математическая корректность и построение цепочки доверия). Если к сертификату привязан закрытый ключ, то отображается знак ключа. Возможно появление одного из двух статусов проверки сертификата: сертификат корректный, сертификат не корректный.

После выбора сертификата в списке отображается информация о нем (рис. 5.11.2).

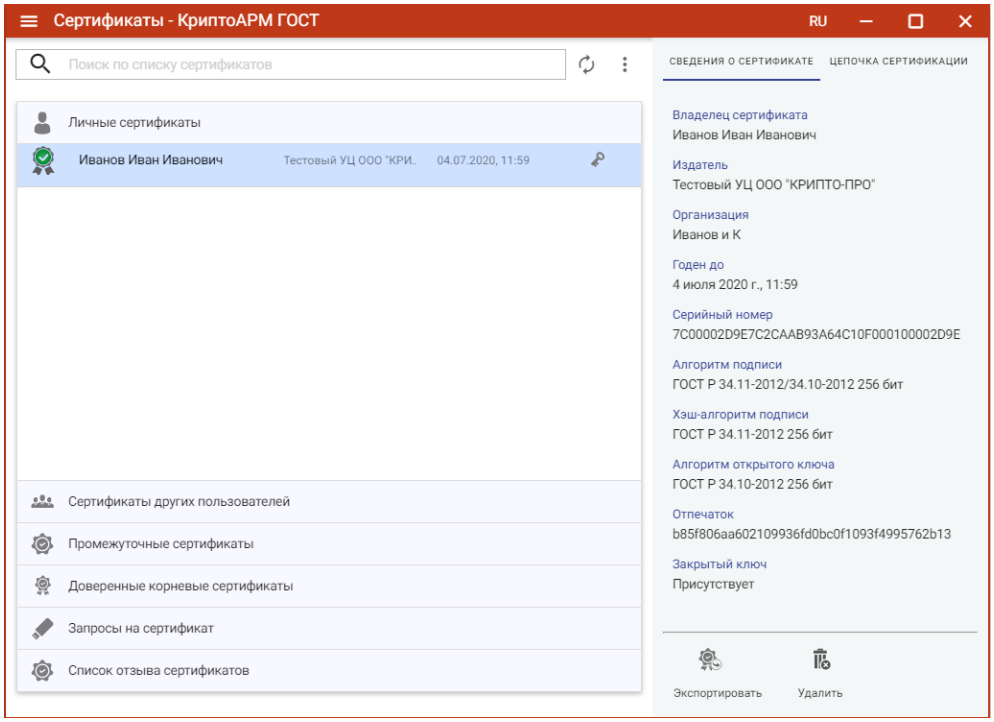


Рис. 5.11.2. Отображение сведений о выбранном сертификате

На вкладке **Цепочка сертификации** отображается общий статус построения цепочки доверия и приводится «дерево» сертификации (рис. 5.11.3).

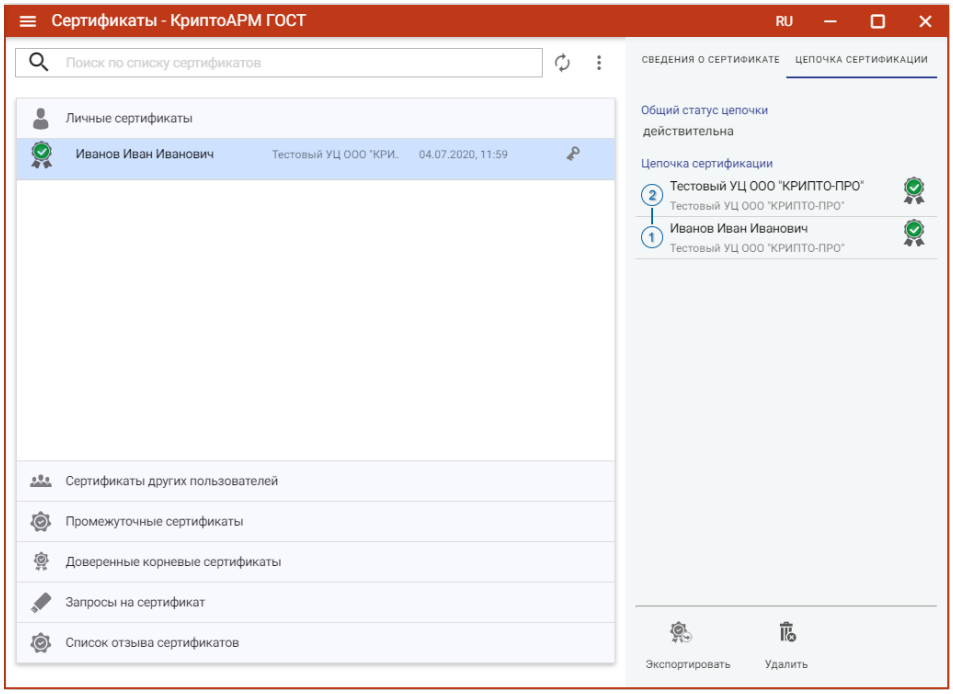


Рис. 5.11.3. Представление цепочки сертификации (цепочки доверия)

5.11.1. Импорт сертификата из файла

Для выполнения импорта нового сертификата в хранилище можно воспользоваться контекстным меню - выбрать операцию **Импорт из файла** (рис. 5.11.4). В появившемся диалоговом окне нужно выбрать файл сертификата (поддерживаются кодировки BASE64 и DER).

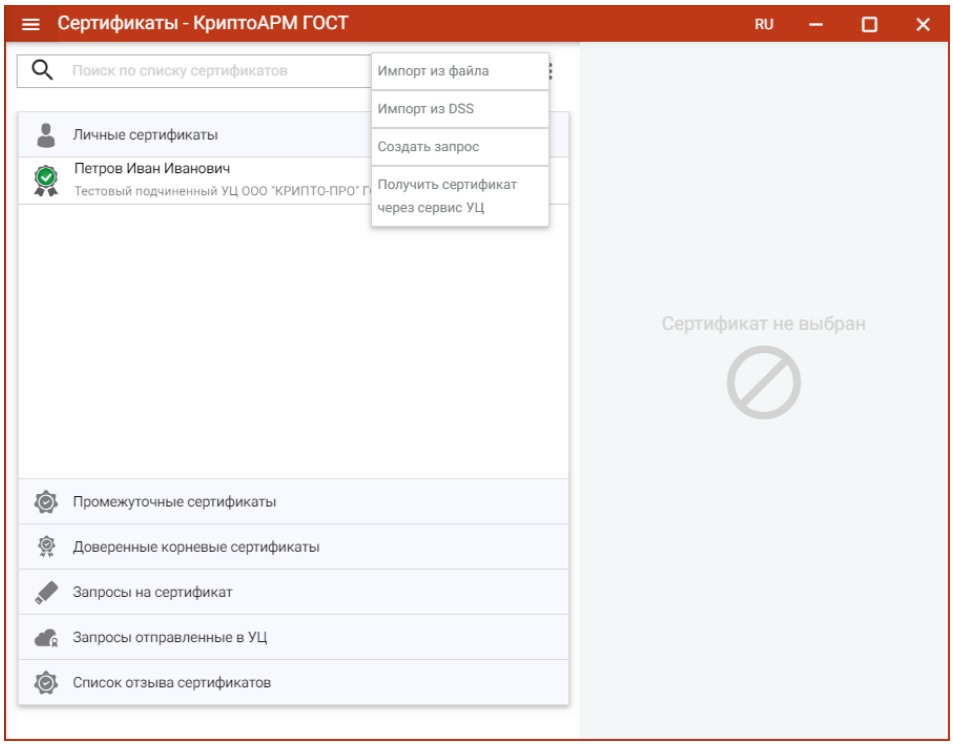


Рис.5.11.4. Контекстное меню списка сертификатов

Сертификат при импорте автоматически помещается в соответствующую категорию (рис. 5.11.5):

- **Личные сертификаты** – сертификаты, используемые пользователем и связанные с закрытыми ключами;
- **Сертификаты других пользователей** – сертификаты пользователей для обмена шифрованными или подписанными данными;
- **Промежуточные сертификаты** - сертификаты промежуточных центров сертификации;
- **Доверенные корневые сертификаты** - автоматически подписанные сертификаты от центра сертификации, которые неявным образом являются доверенными. Здесь хранятся сертификаты, изданные сторонними удостоверяющими центрами, Microsoft.

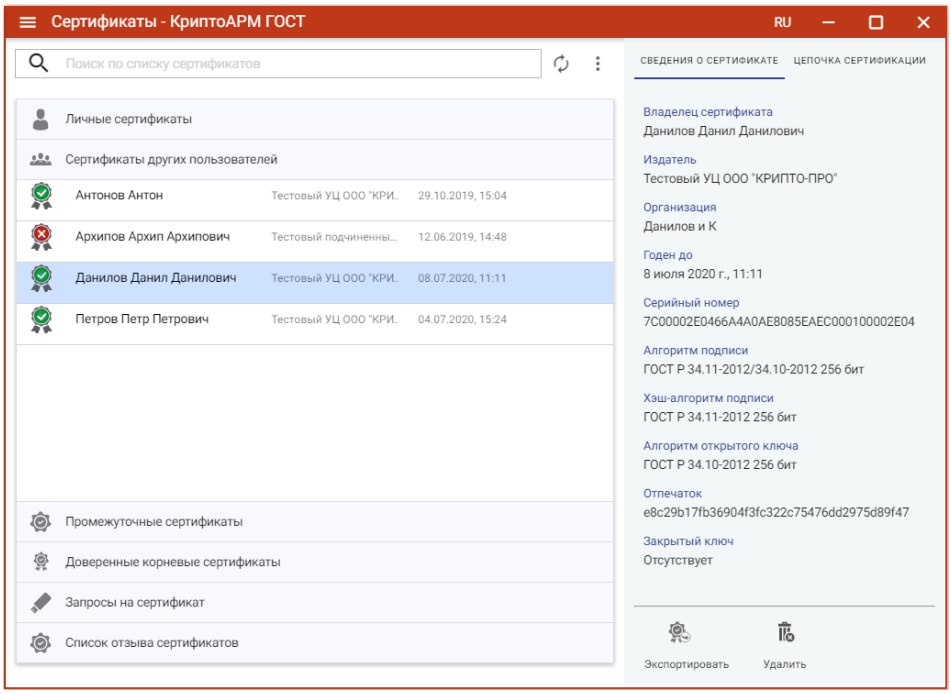


Рис. 5.11.5. Отображение импортированного сертификата

5.11.2. Импорт сертификата из DSS

Для выполнения импорта сертификата из DSS в хранилище можно воспользоваться контекстным меню - выбрать операцию **Импорт из DSS** (рис. 5.11.4).

Открывается окно для ввода адресов серверов авторизации и DSS, логина и пароля для аутентификации (рис. 5.11.6).

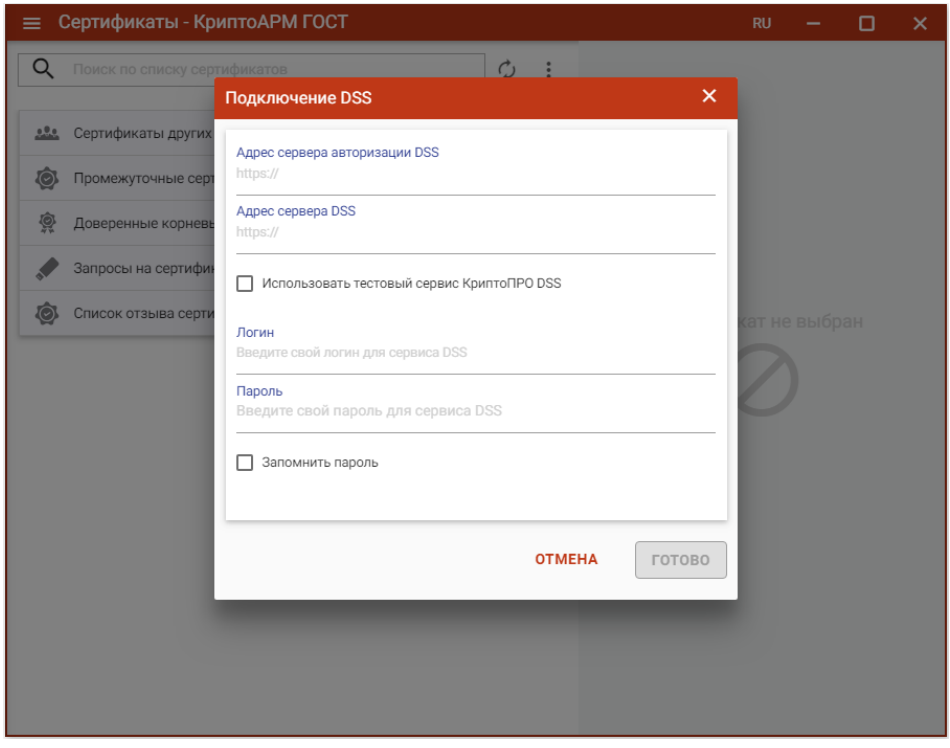


Рис. 5.11.6. Настройка адресов серверов DSS

Если у пользователя в личном кабинете DSS в настройках стоит подтверждение аутентификации по SMS, по электронной почте или с помощью мобильного приложения, то при нажатии на кнопку **Готово** появляется сообщение, что операцию нужно подтвердить (рис. 5.11.6.1). Если нет, то данный шаг пропускается.

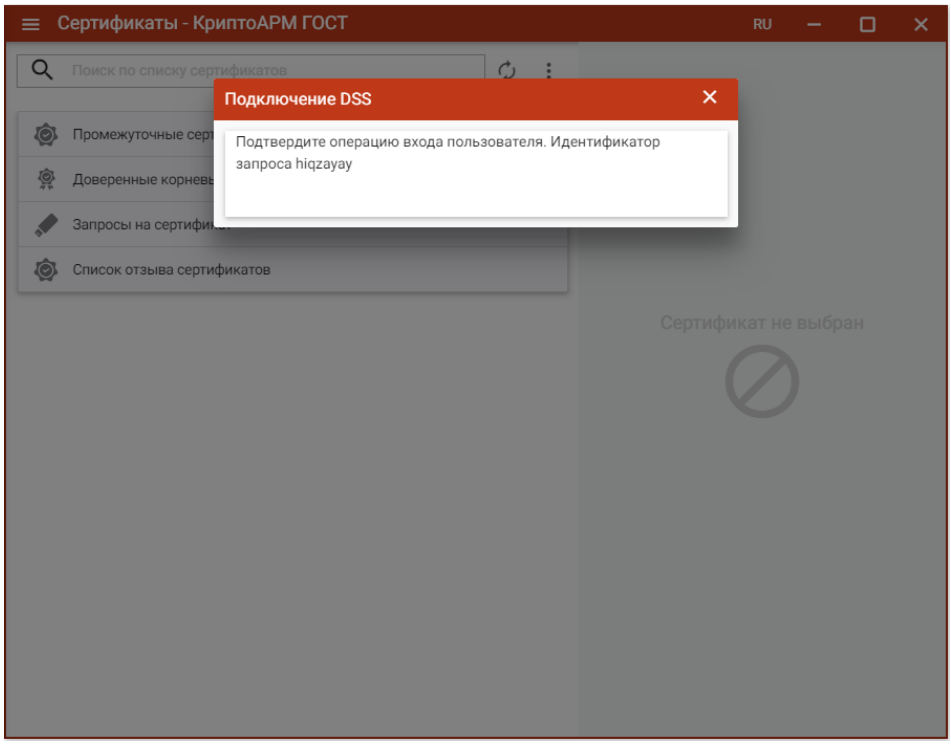


Рис. 5.11.6.1. Окно запроса подтверждения входа

При успешной аутентификации на следующем шаге сертификаты DSS автоматически помещаются в хранилище личных сертификатов (рис. 5.11.7).

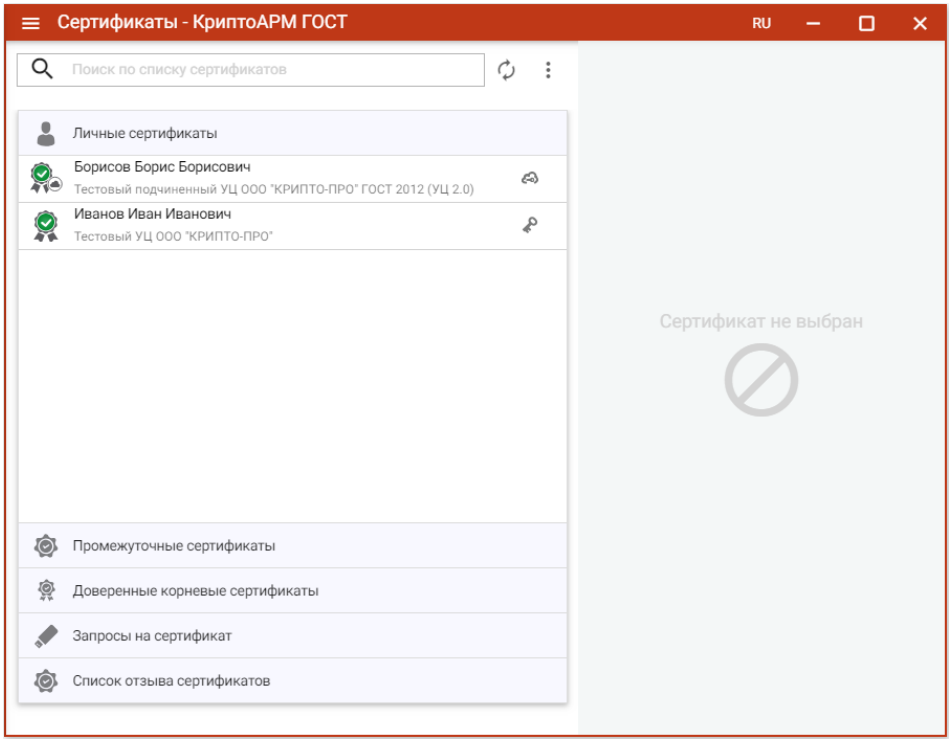


Рис. 5.11.7. Отображение импортированного DSS сертификата

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

5.11.3. Экспорт сертификата в файл

Для экспорта сертификата в файл нужно выделить сертификат и нажать кнопку операции **Экспортировать** (рис. 5.11.8). Если у сертификата экспортируемый закрытый ключ, то такой сертификат можно экспортировать вместе с закрытым ключом.

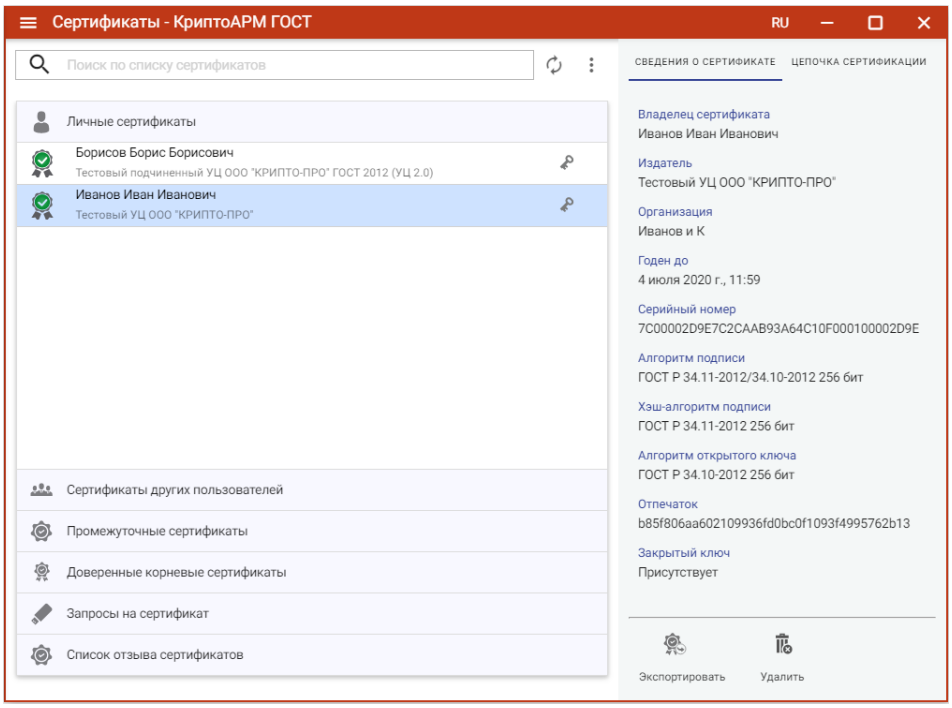


Рис. 5.11.8. Экспорт сертификата

При экспорте сертификата с не экспортируемым закрытым ключом появляется окно, в котором можно выбрать только кодировку файла сертификата (рис. 5.11.9).

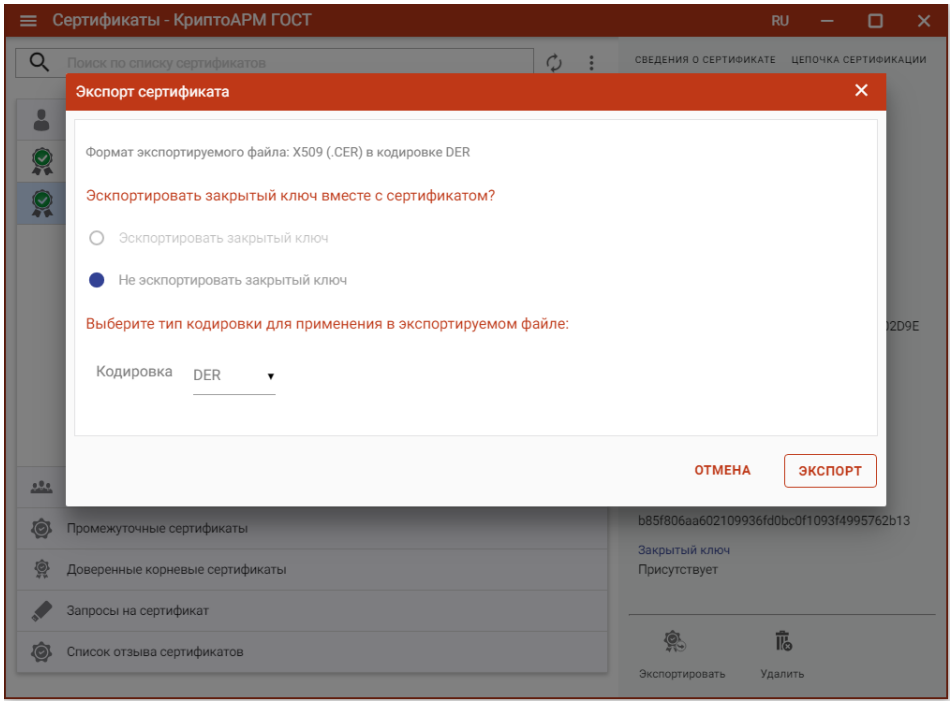


Рис. 5.11.9. Выбор кодировки файла сертификата

После нажатия кнопки **Экспорт**, в появившемся диалогом 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 (рис. 5.11.9).
- Экспортировать сертификат вместе с закрытым ключом. В таком случае надо указать пароль для защиты закрытого ключа (рис. 5.11.10).

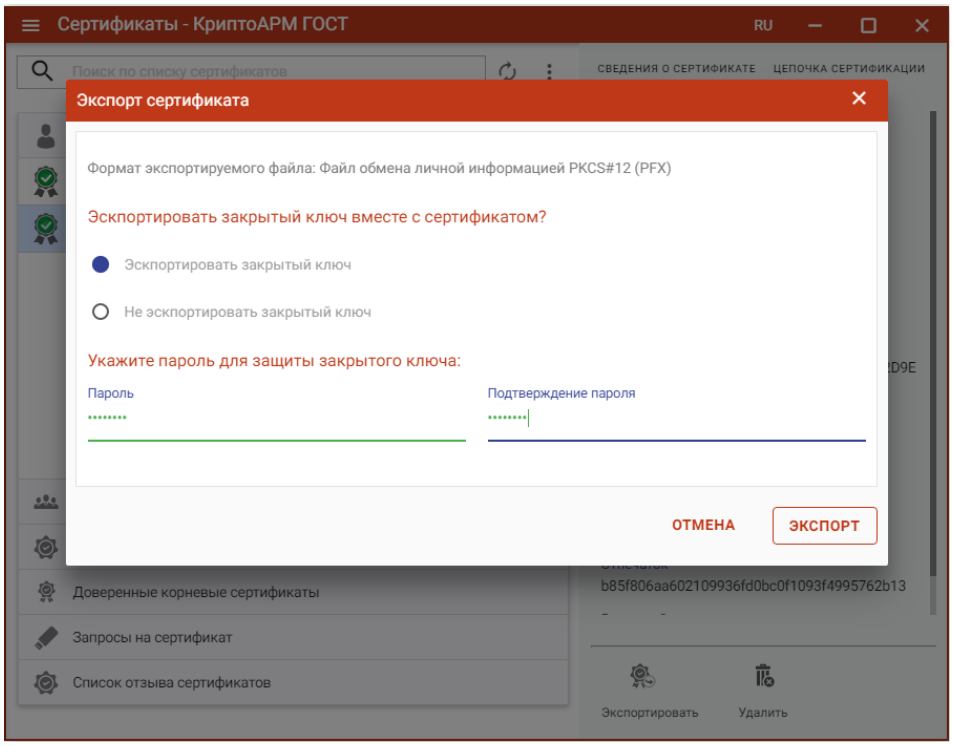


Рис. 5.11.10. Экспорт сертификата вместе с закрытым ключом

После нажатия кнопки **Экспорт**, в появившемся диалогом 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 ключевому контейнеру.

5.11.4. Удаление сертификата

Для удаления сертификата нужно выбрать операцию **Удалить** (рис. 5.11.11).

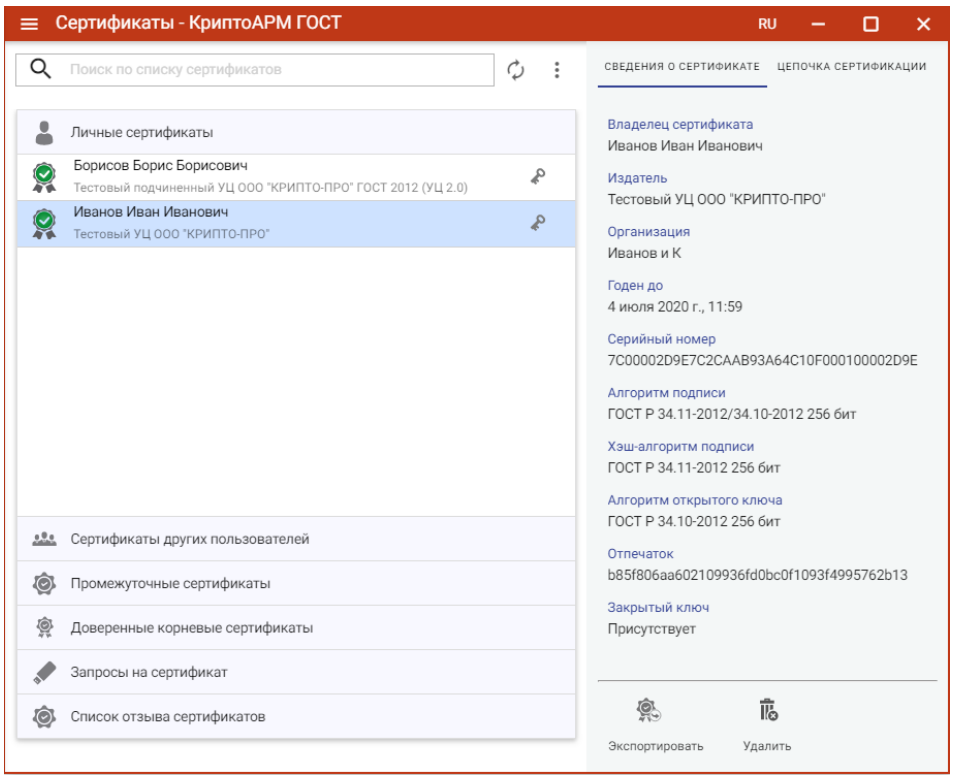


Рис. 5.11.11. Удаление сертификата

В появившемся диалоговом окне нажать **Удалить** для подтверждения удаления (рис. 5.11.12)

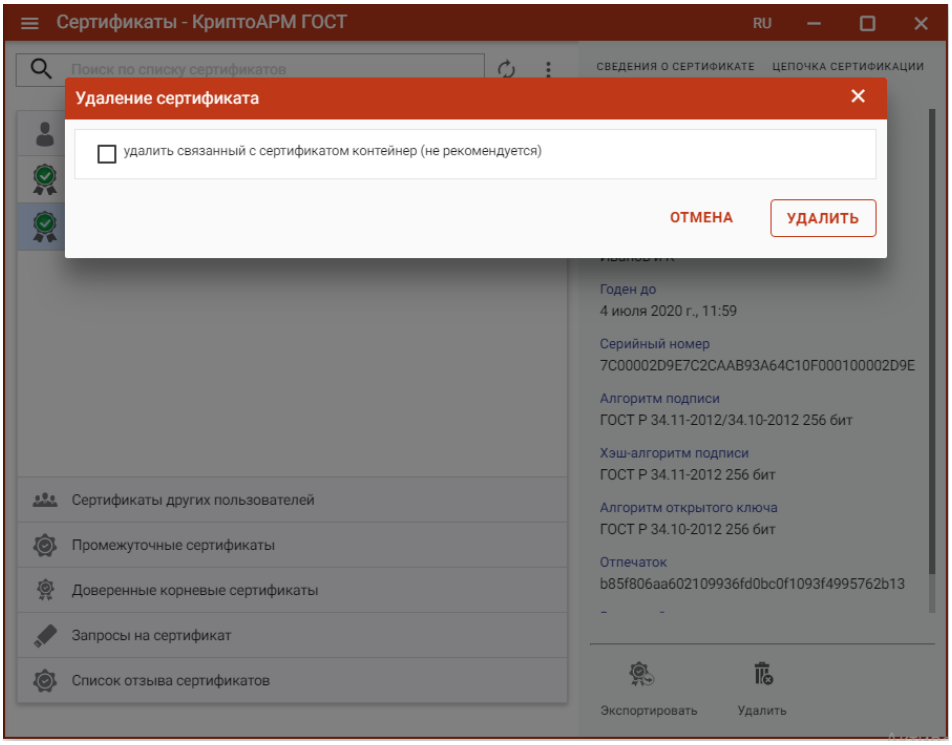


Рис. 5.15.12 Подтверждение удаления сертификата

Если у сертификата есть привязка к закрытому ключу, то при удалении сертификата возможно удаление закрытого ключа. Для удаления сертификат вместе с закрытым ключом в диалоговом окне надо поставить «галочку» **Удалить связанный с сертификатом контейнер** и нажать кнопку **Удалить**.

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

5.11.5. Создание запроса на сертификат

Для создания запроса на сертификат в контекстном меню списка сертификатов следует выбрать операцию **Создать запрос** (рис. 5.11.13).

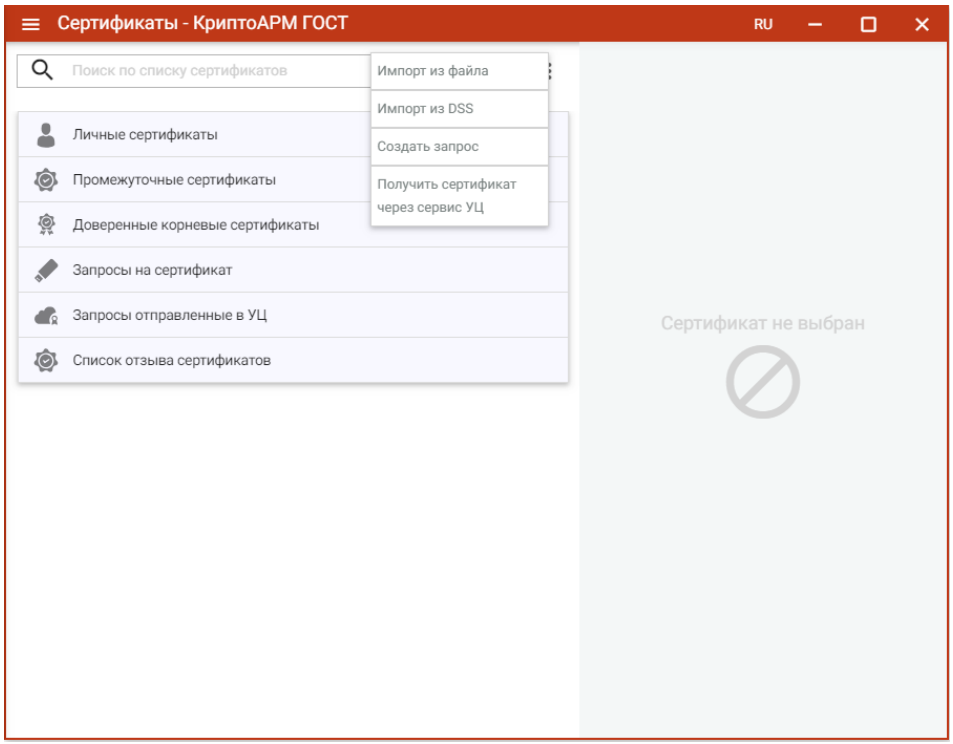


Рис. 5.11.13. Создание запроса на сертификат

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

В параметрах субъекта указывается:

- Шаблон сертификата (рис. 5.11.14);

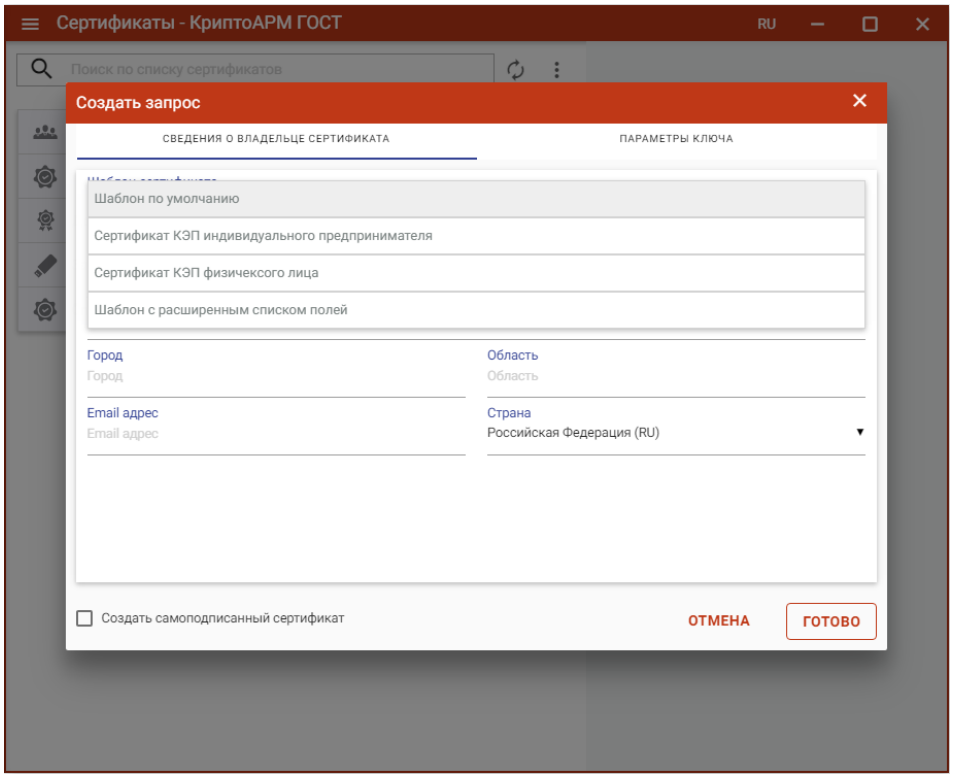


Рис. 5.11.14. Выбор шаблона сертификата

– Основная информация, в которой, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце сертификата (рис. 5.11.15).

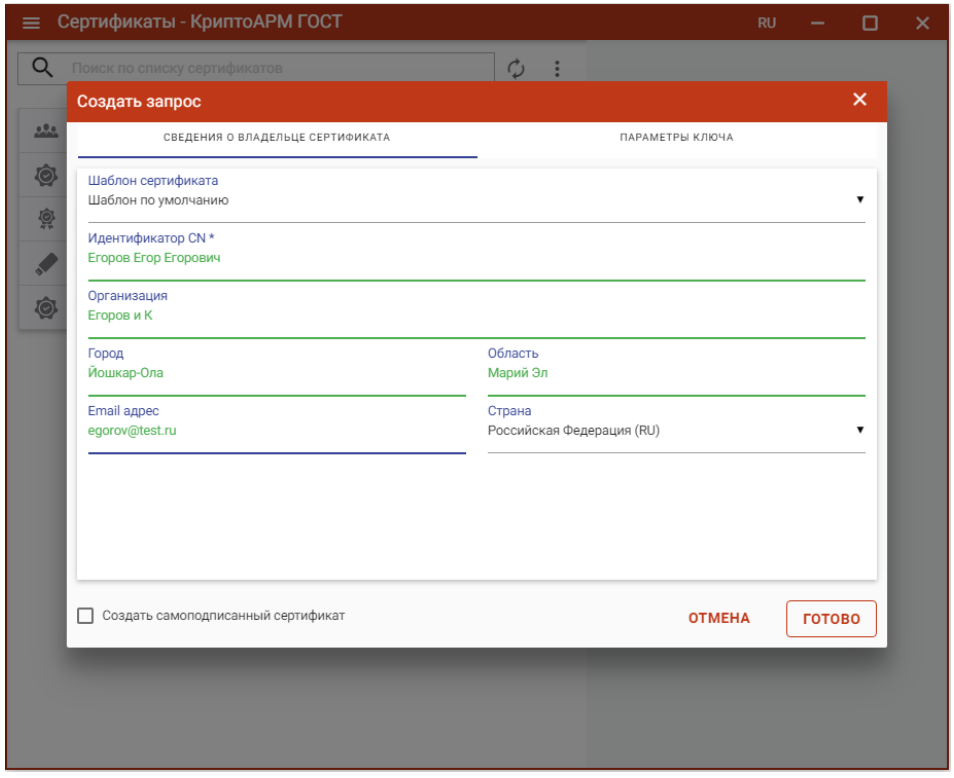


Рис. 5.11.15. Информация о владельце сертификата

– При установке флага **Создать самоподписанный сертификат** происходит создание сертификата и его автоматическая установка в личное хранилище пользователя. Запросы на самоподписанные сертификаты не создаются.

В параметрах ключа указывается:

– Алгоритм ключа (рис. 5.11.16);

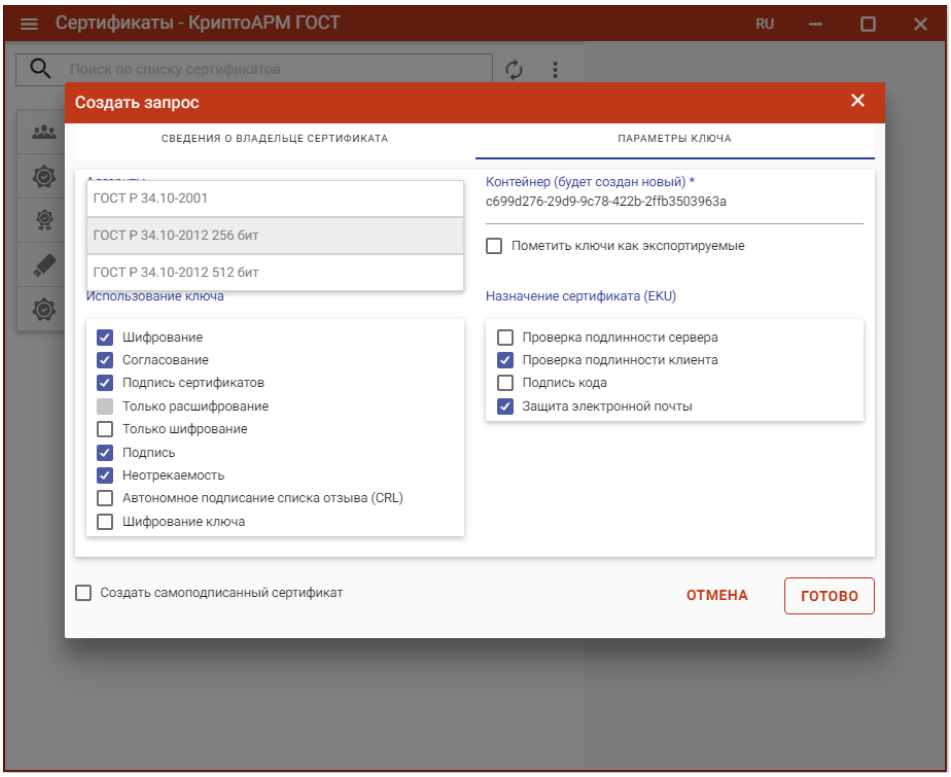


Рис. 5.11.16. Выбор алгоритма ключа

– Назначение ключа (рис. 5.11.17);

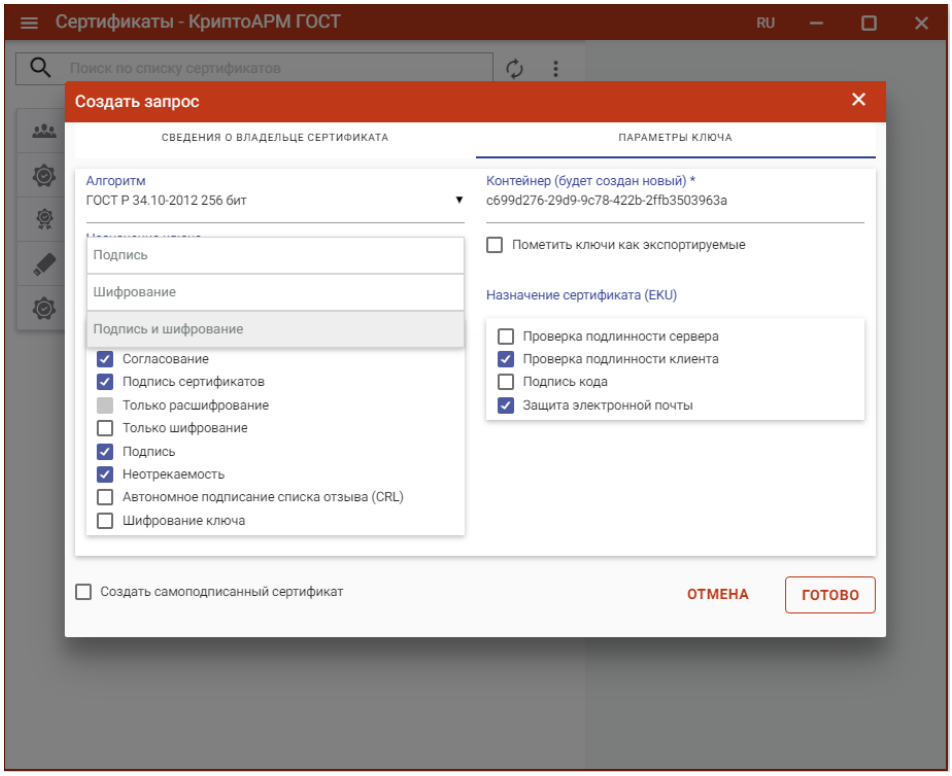


Рис. 5.11.17. Выбор назначения ключа

– Использование ключа (рис. 5.11.18);

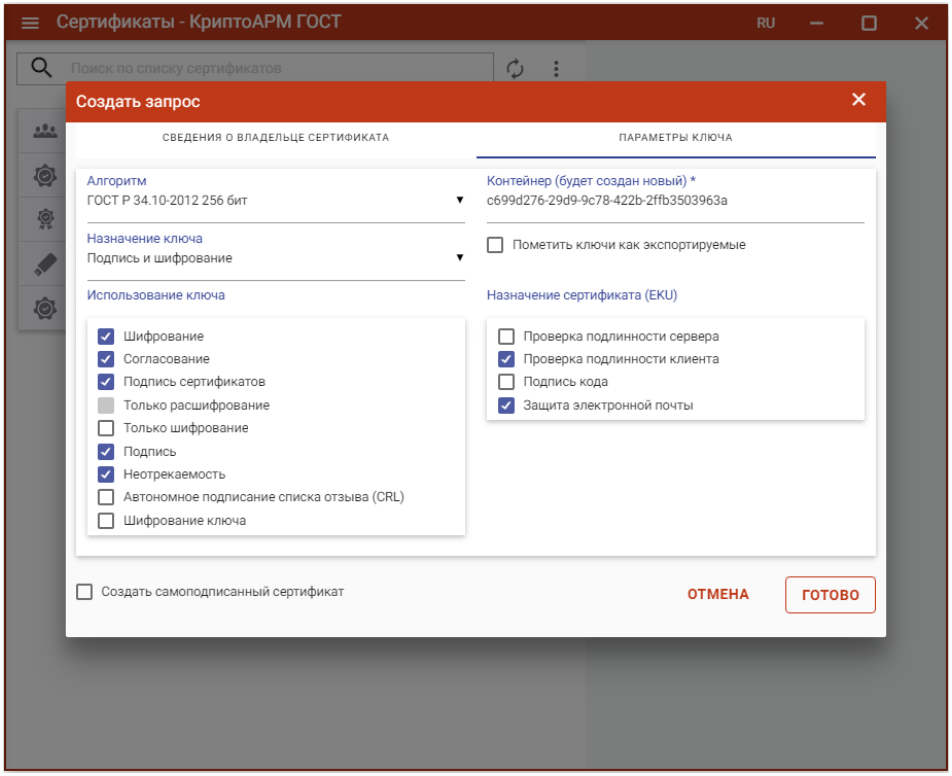


Рис. 5.11.18. Выбор использования ключа

– Контейнер - сертификат будет создан на основе нового ключевого набора. Можно задать свое имя ключевого набора или оставить созданное автоматически.
– 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 на вкладке **Запросы на сертификат** (рис. 5.11.19).

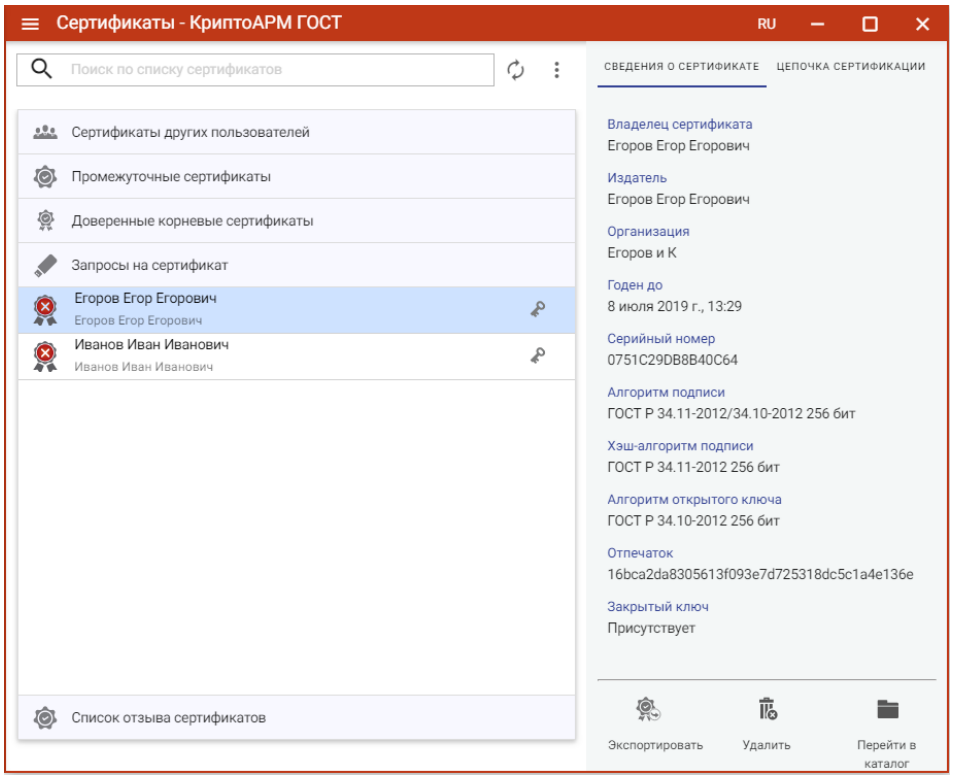


Рис. 5.11.19. Форма просмотра запроса на сертификат

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 с данным сертификатом в приложении.

5.11.6. Создание самоподписанного сертификата

Для создания самоподписанного сертификата на форме **Создать запрос** следует поставить флаг **Создание самоподписанного сертификата** (рис. 5.11.20).

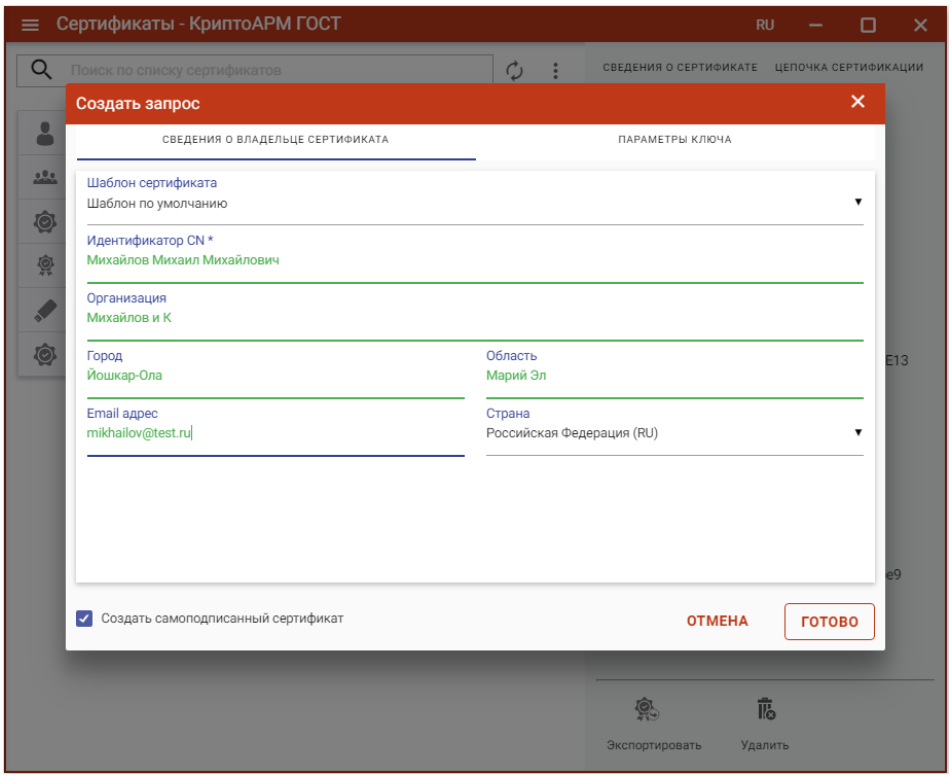


Рис. 5.11.20. Создание самоподписанного сертификата

На основе указанных данных по кнопке **Готово** будет сформирован самоподписанный сертифкат. 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 (рис. 5.11.21)

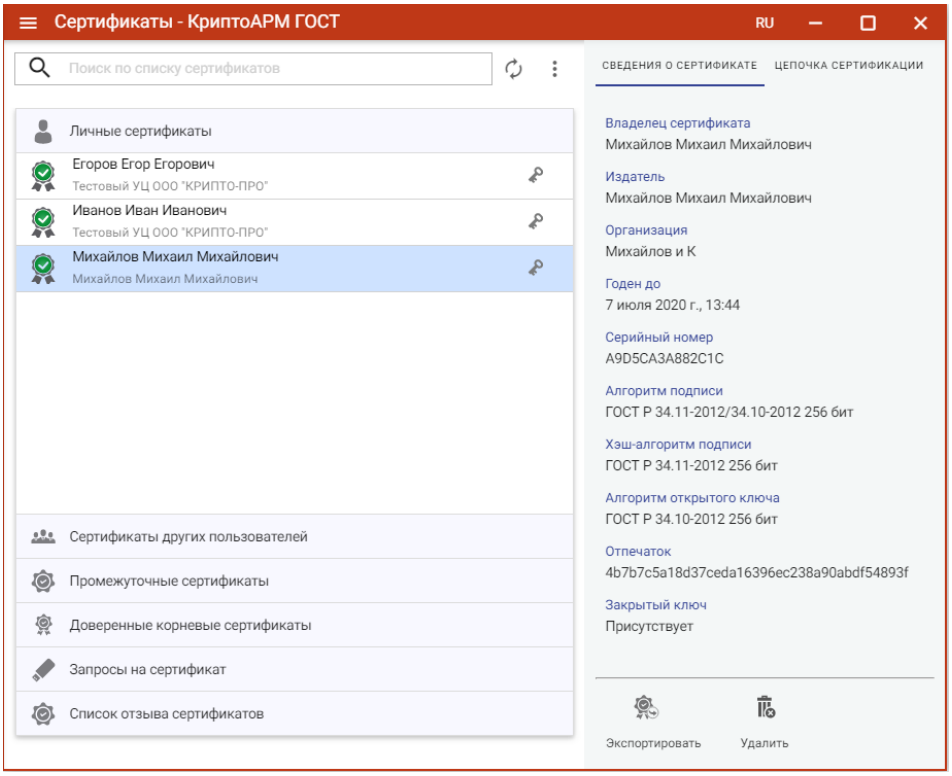


Рис. 5.11.21. Список Личных сертификатов

При генерации самоподписанного сертификата запрос на сертификат не создается.

5.11.7. Списки отзыва сертификатов (CRL)

Для работы со списками отзыва сертификатов в мастере управления сертификатами добавлен раздел **Списки отзыва сертификатов** (рис. 5.11.22).

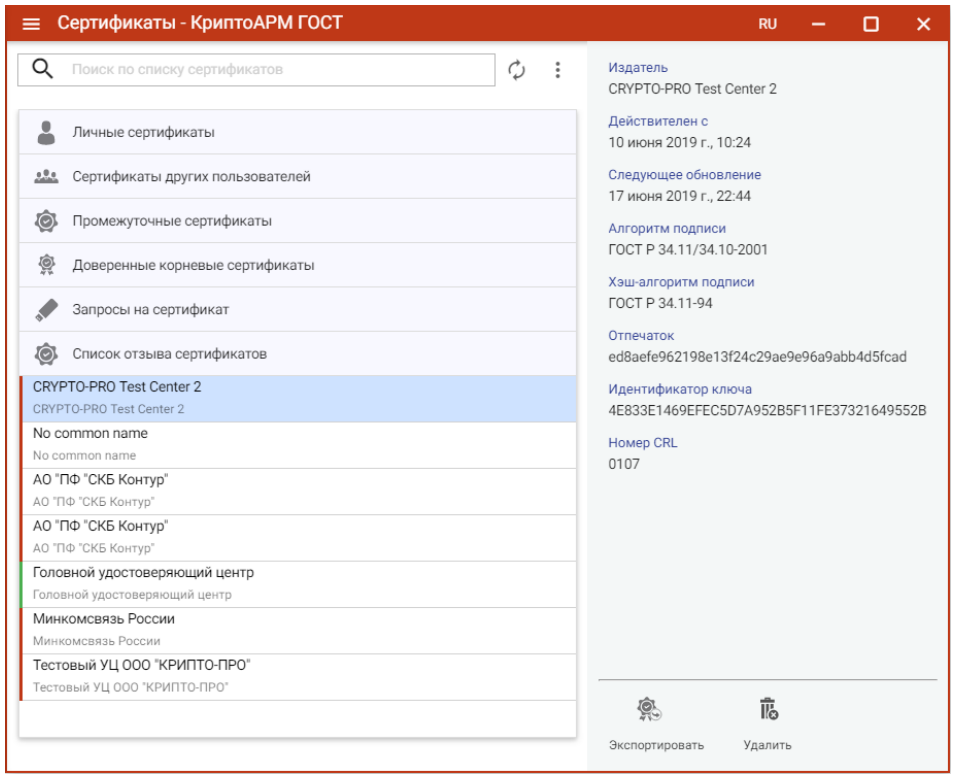


Рис. 5.11.22. Списки отзыва сертификатов

Если раздел не отображается в списке, значит в хранилище нет импортированных списков отзыва сертификатов.

Для импорта списка отзыва надо выбрать в контекстном меню Импорт из файла и выбрать файл списка отзыва (рис. 5.11.23)

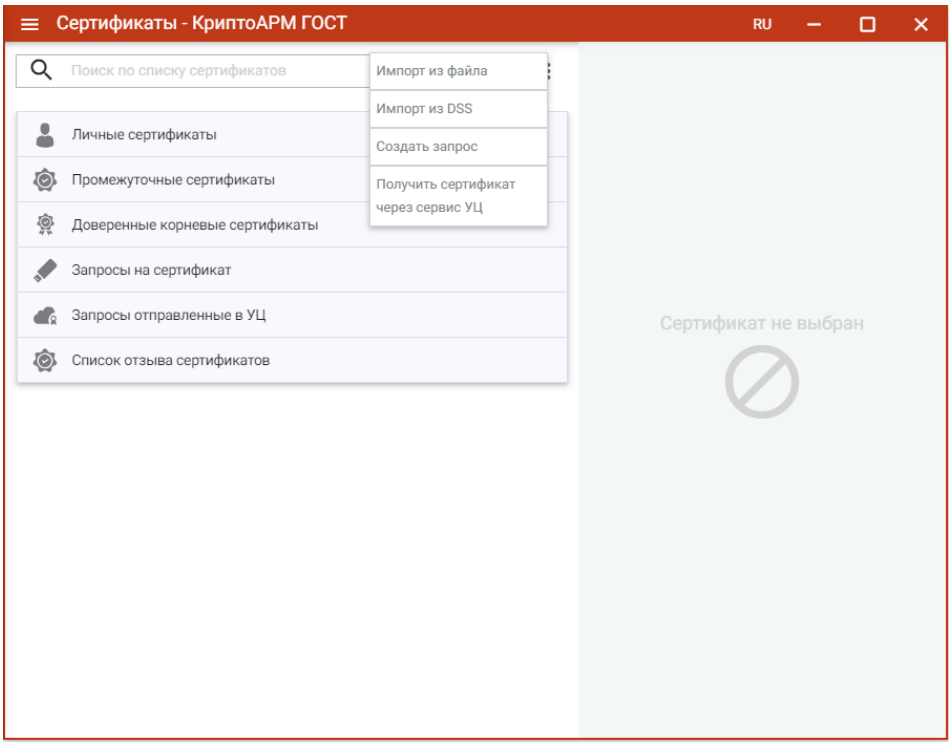


Рис. 5.11.23. Импорт списка отзыва сертификатов

Импортированный список отображается в разделе **Список отзыва сертификатов** (рис. 8.10.23).

Выбранный COC можно экспортировать или удалить, выбрав соответствующую операцию на форме просмотра COC (рис. 8.10.22).

Экспорт COC. При выборе Экспортировать открывается форма выбора кодировки файла (рис. 5.11.24). При нажатии на **Экспорт** следует выбрать директорию для сохранения и задать имя файла COC.

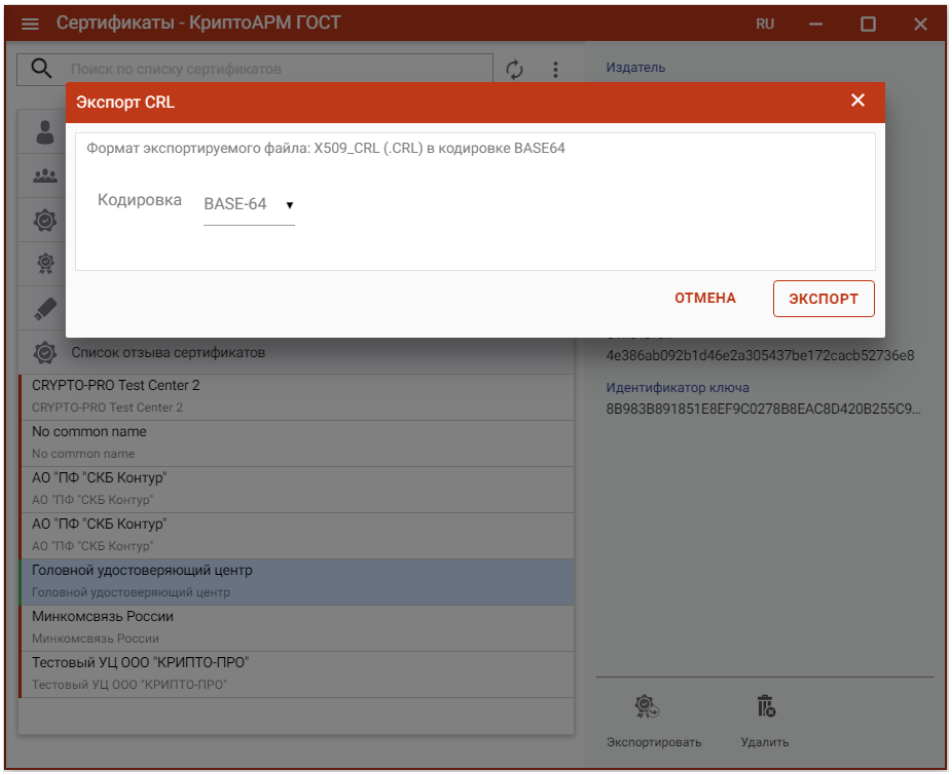


Рис. 5.11.24. Выбор кодировки экспортируемого СОС

Удаление СОС. Для удаления СОС надо нажать кнопку **Удалить** и подтвердить удаление в соответствующем окне (рис. 5.11.25).

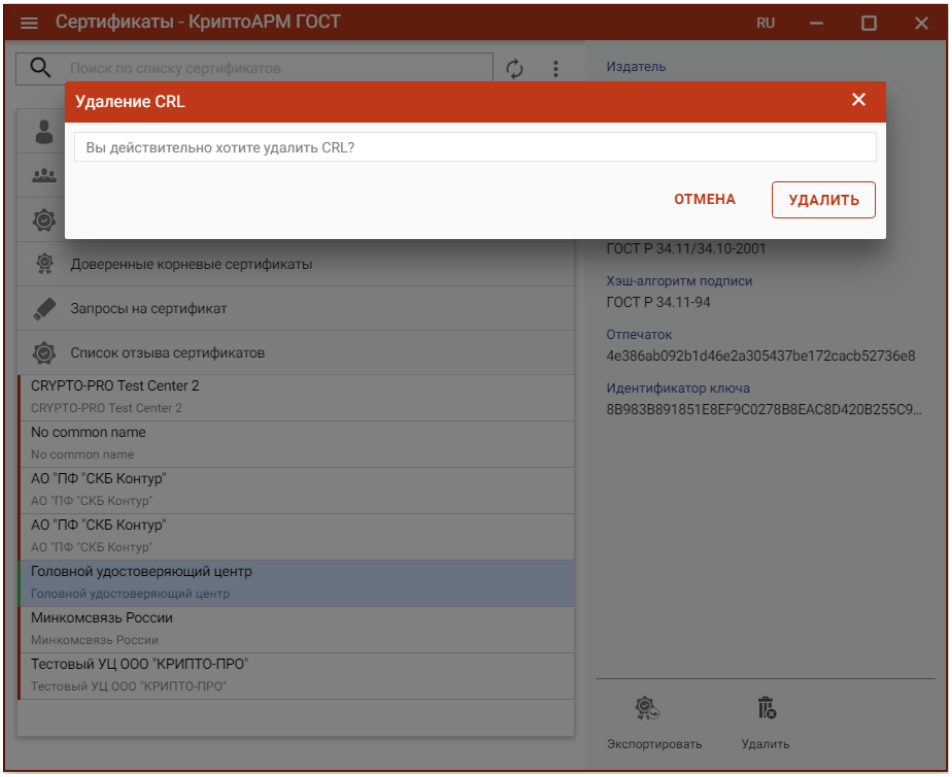


Рис. 5.11.25. Подтверждение удаления СОС

5.11.8. Поиск сертификата

В элементах пользовательского интерфейса, где процесс выполнения операции учитывает выбор сертификата из списка, реализована функция поиска сертификатов (рис. 5.11.26). Для включения режима поиска нужно нажать на кнопку **Поиск** и в строке поиска ввести ключевую фразу.

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.

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

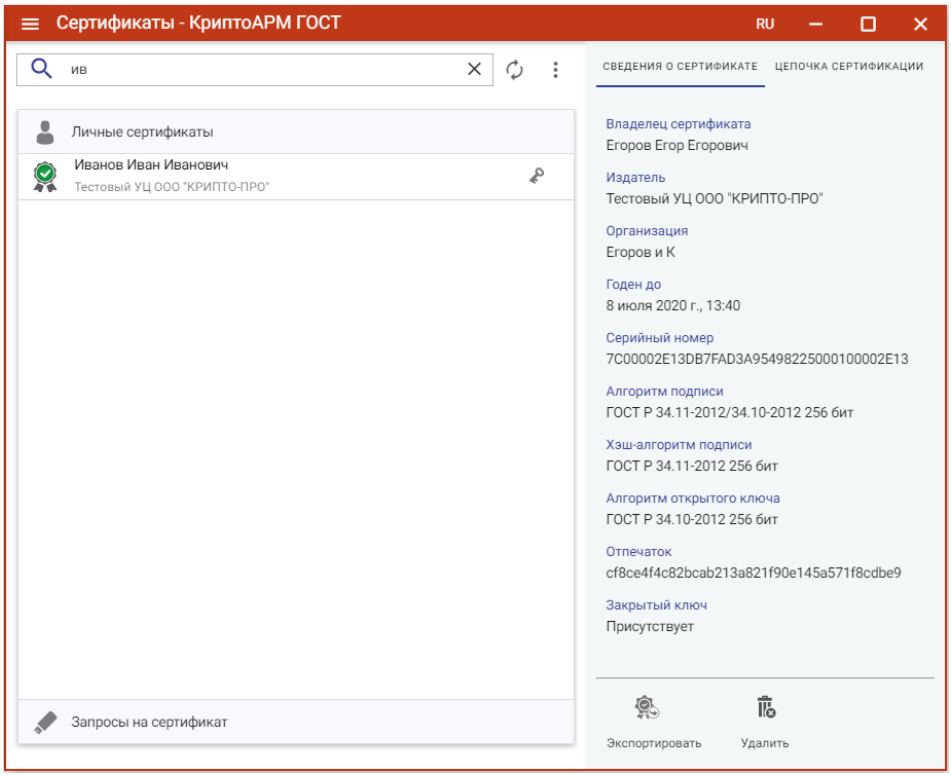


Рис. 5.11.26. Поиск сертификата

5.12. Установка сертификата из ключевого контейнера

Для установки сертификата из ключевого контейнера в приложении добавлено отдельное представление **Контейнеры**. В левой области представления отображаются все подключенные хранилища контейнеров закрытых ключей. В правой области отображается информация о сертификате в выделенном контейнере (рис. 5.12.1).

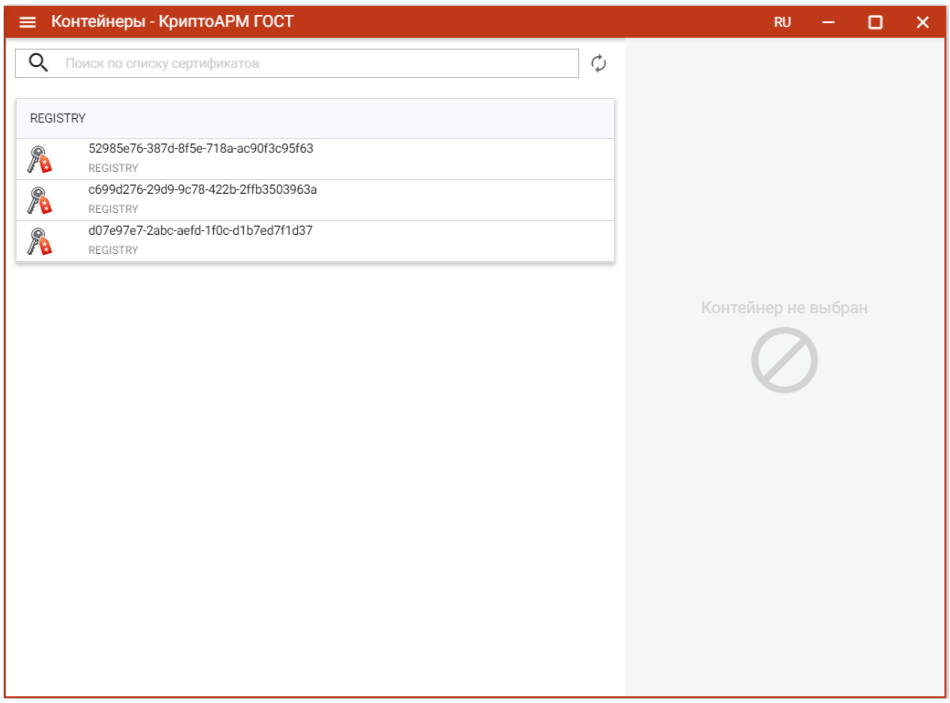


Рис. 5.12.1. Хранилища контейнеров закрытых ключей

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 (рис. 5.12.2).

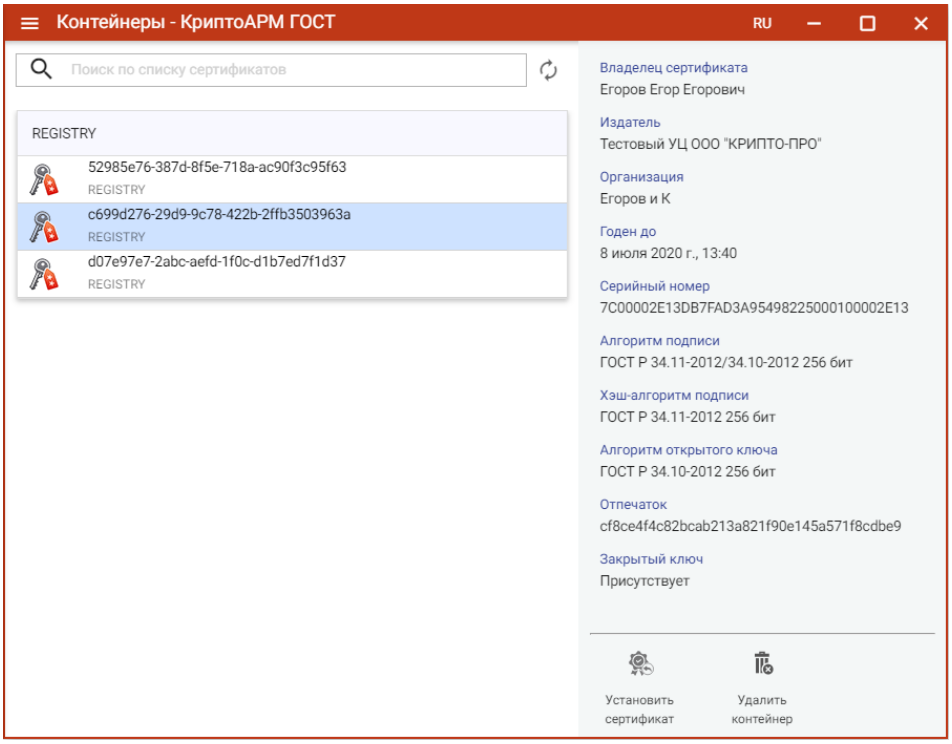


Рис. 5.12.2. Информация о сертификате в контейнере

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 (рис. 5.12.3). 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.

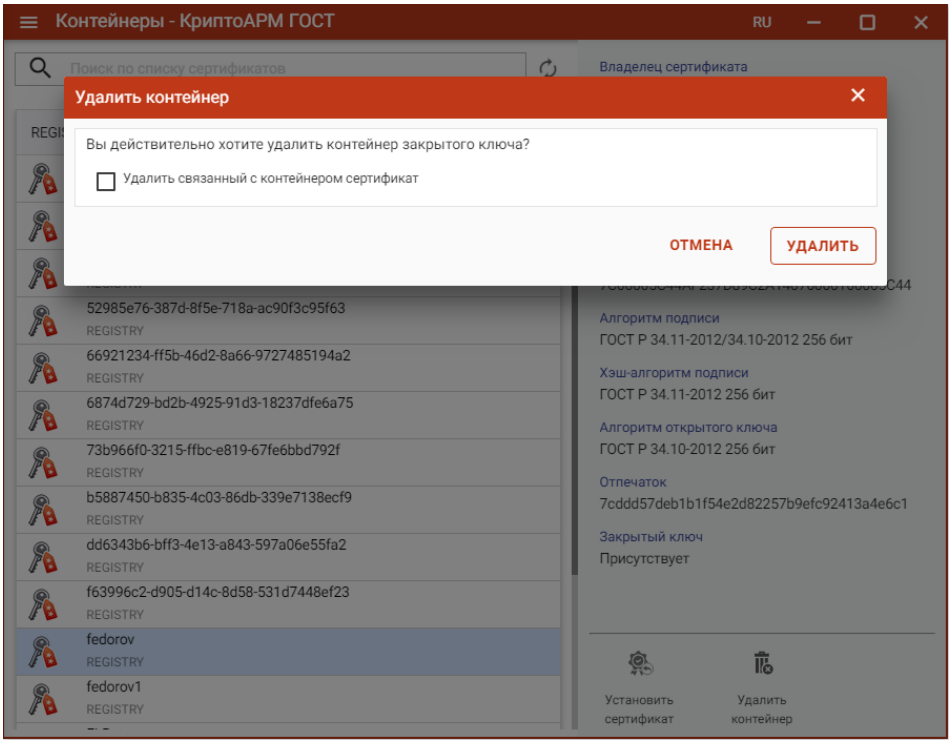


Рис. 5.12.3. Удаление контейнера

В приложении реализован поиск контейнеров по символьному совпадению в названии контейнера (рис. 5.12.4).

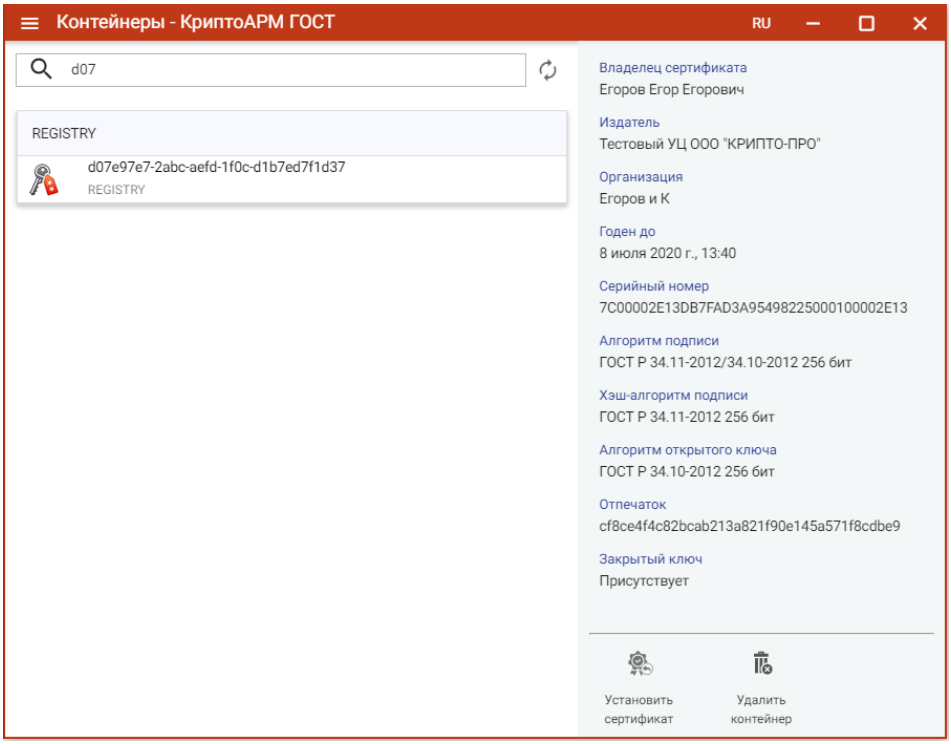


Рис. 5.12.4. Поиск контейнера

5.13. Настройки

Для задания параметров операций подписи и шифрования в приложении добавлен раздел **Настройки**. В настройках задается кодировка файла, формат подписи (присоединенная или отсоединенная), каталог сохранения результирующих документов. Кроме того в настройке хранятся сертификаты, которые заданы в качестве сертификатов подписи и получателей шифрованных сообщений.

При установке приложения создается настройка по умолчанию (рис. 5.13.1)

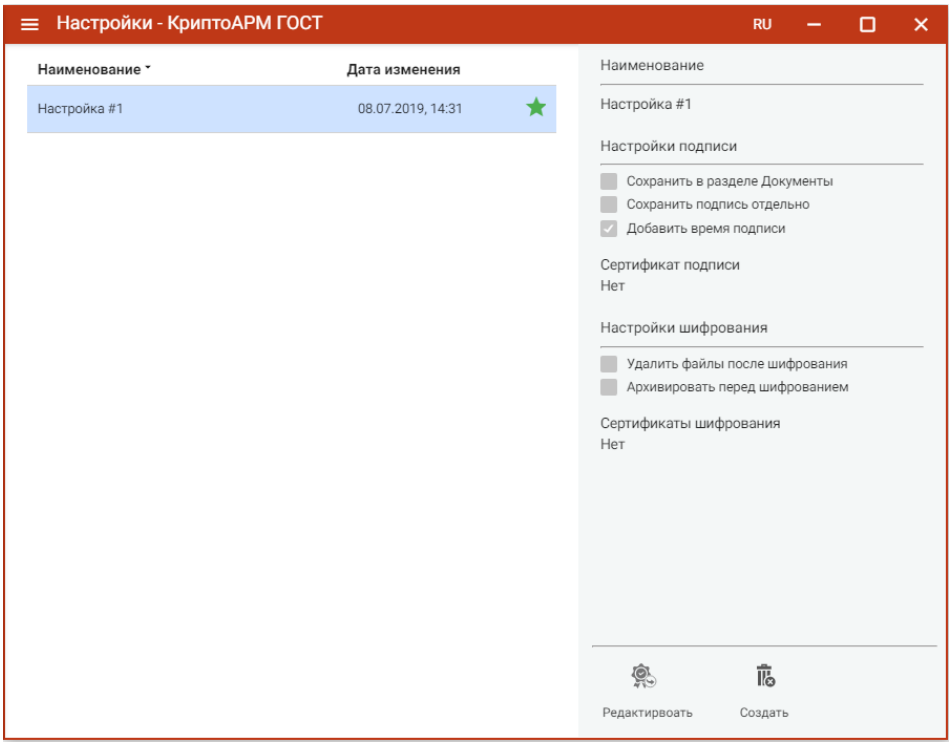


Рис. 5.13.1. Настройки

Настройки можно редактировать, создавать, удалять, импортировать и экспортировать.

Создание настройки. При нажатии на кнопку **Создать** открывается форма создания настройки (рис. 5.13.2).

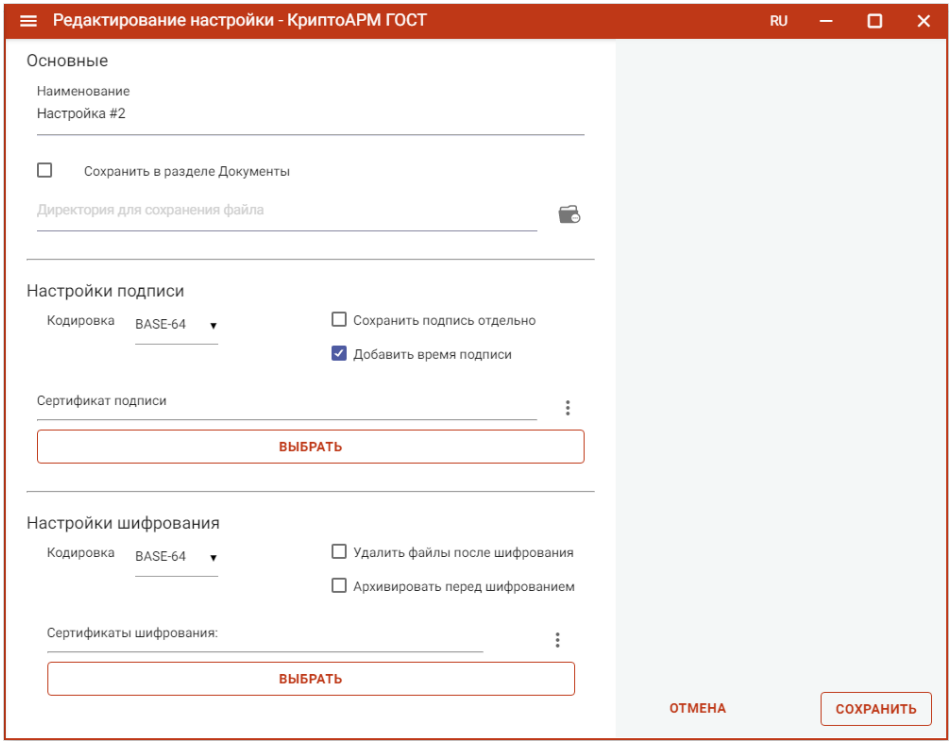


Рис. 5.13.2. Создание настройки

В поле **Наименование** задается название настройки.

Если установлен флаг **Сохранить в разделе Документы**, то все результирующие файлы операций подписи, снятия подписи, добавления подписи, шифрования и расшифрования будут

сохранятся в каталоге ./Trusted/CryptoARM GOST/Documents/, расположенной в папке пользователя.

Директорию для сохранения файла можно задать любую (на которую у пользователя есть право редактирования), тогда все результирующие файлы операций подписи, снятия подписи, добавления подписи, шифрования и расшифрования будут сохранятся в заданную директорию.

Если флаг **Сохранить в разделе Документы** не установлен и не задана **директория для сохранения файла**, тогда все результирующие файлы операций подписи, снятия подписи, добавления подписи, шифрования и расшифрования сохраняются в тот же каталог, где расположен исходный файл.

В **Настройках подписи** задаются следующие параметры:

- **Кодировка** - сохранение подписанного файла в одной из двух кодировок BASE64 или DER;
- **Сохранить подпись отдельно** - при установленном флаге подпись сохраняется отдельно от исходного файла;
- **Добавить время подписи** - при установленном флаге в подпись сохраняется время (системное) подписи;
- **Сертификат подписи** – выбранный сертификат будет использован для подписи документов. Выбранный сертификат можно изменить, выбрав в контекстном меню сертификата **Изменить**. Или **Очистить** данное поле, а затем выбрать сертификат из списка (рис. 5.13.3). В качестве сертификата подписи может использоваться только сертификат из категории Личные сертификаты, имеющий закрытый ключ.

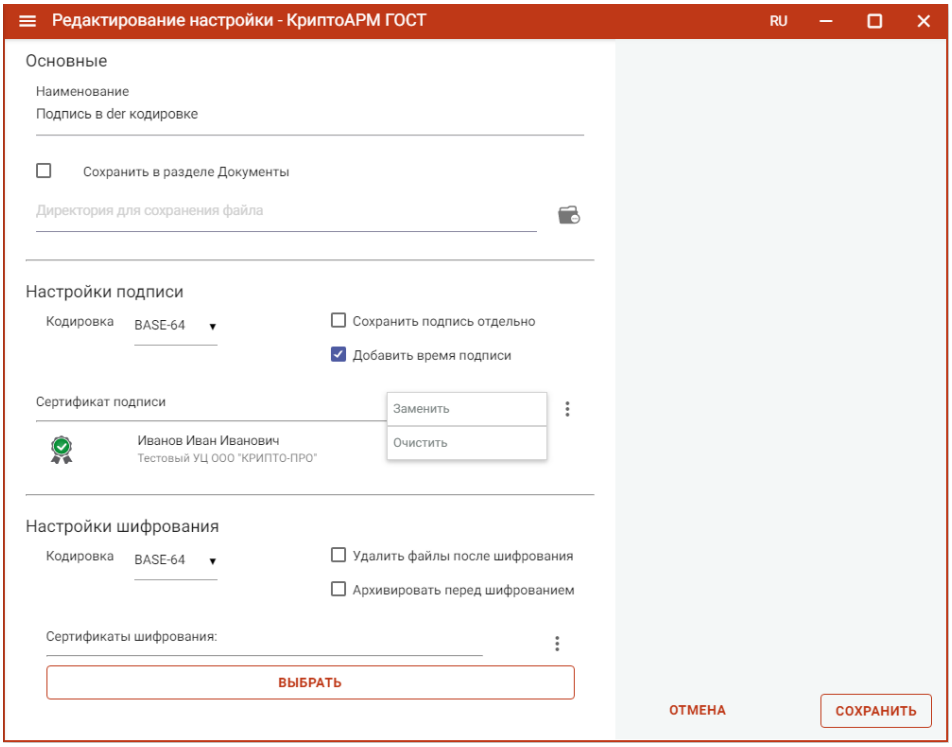


Рис. 5.13.3. Редактирование поля сертификата подписи

В **Настройках шифрования** задаются следующие параметры:

- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER;

- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции;
- **Архивировать перед шифрованием** - файлы архивируются (ZIP) перед выполнением операции шифрования. Шифруется созданный ZIP-архив;
- **Сертификаты шифрования** – выбранные сертификаты будут использоваться для шифрования документов. Сертификаты можно изменить, выбрав в контекстном меню **Изменить**. Или **Очистить** данный список, а затем выбрать сертификаты. Так же можно удалить отдельный сертификат (рис. 5.13.4). В список сертификатов шифрования можно добавить только сертификаты категорий Личные и Сертификаты других пользователей.

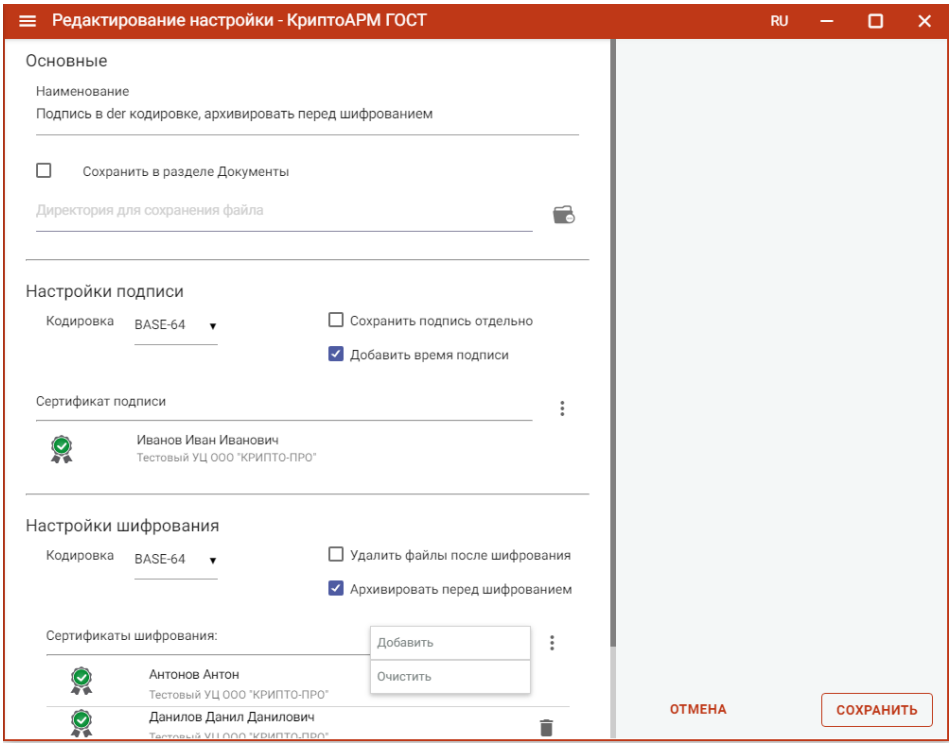


Рис. 5.13.4. Редактирование списка сертификатов шифрования

По нажатию на кнопку **Сохранить** происходит создание настройки с заданными параметрами (рис. 5.13.5).

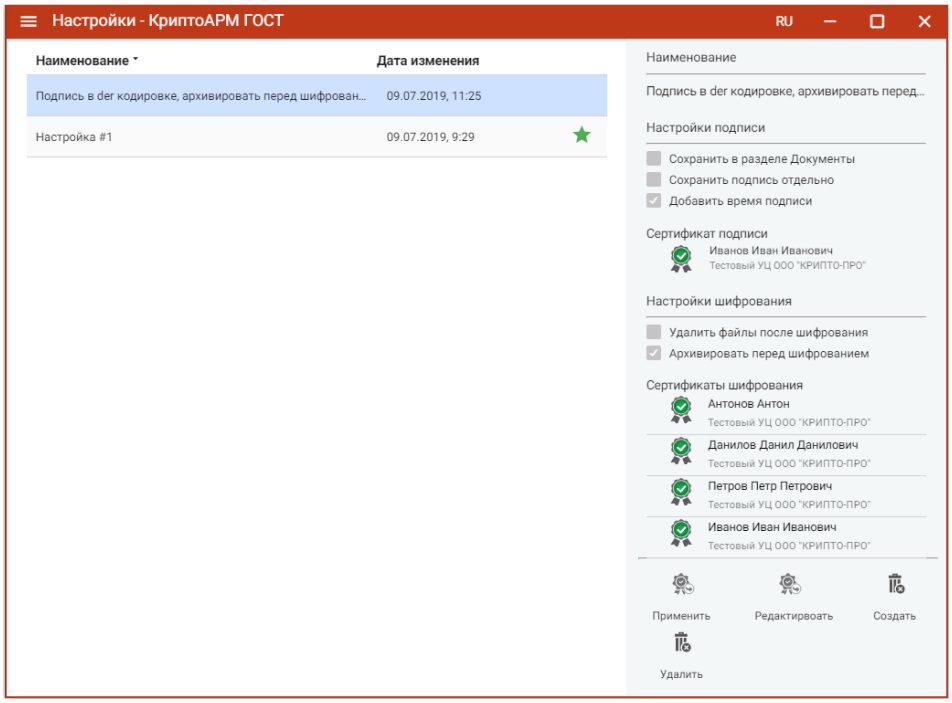


Рис. 5.13.5. Сохранение созданной настройки

Установка настройки по умолчанию. Для того, чтобы при подписи и шифрования параметры операций выбирались из заданной настройки, нужно установить эту настройку настройкой по умолчанию. Для этого надо выделить настройку в списке настроек и нажать кнопку **Применить.** (рис. 5.13.6).

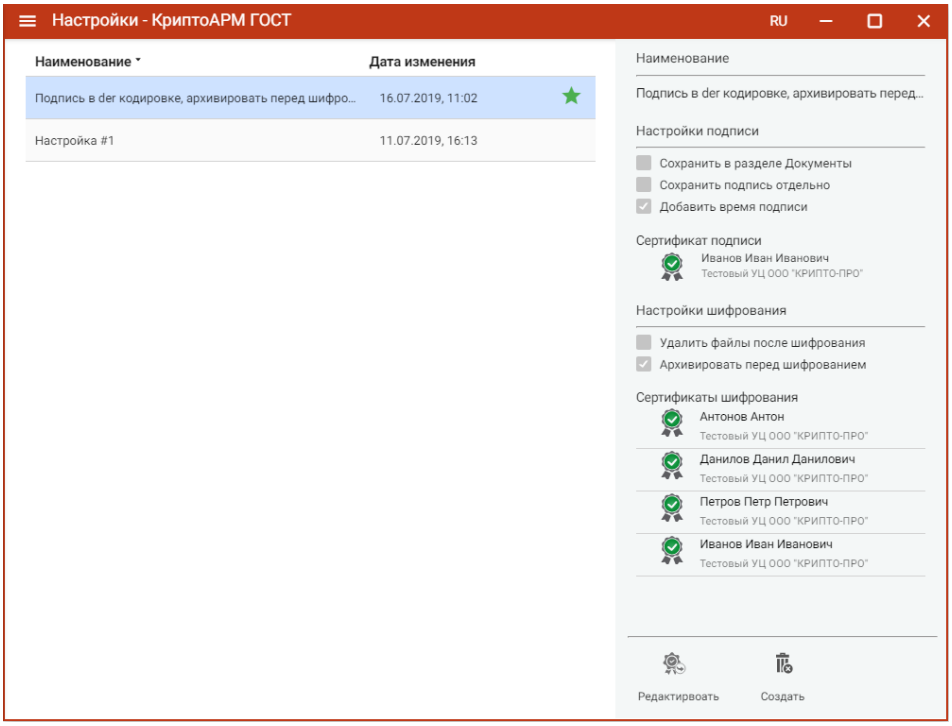


Рис. 5.13.6. Установка настройки по умолчанию

Редактирование настройки. При нажатии на кнопку **Редактировать** открывается форма редактирования настройки (рис. 5.13.7).

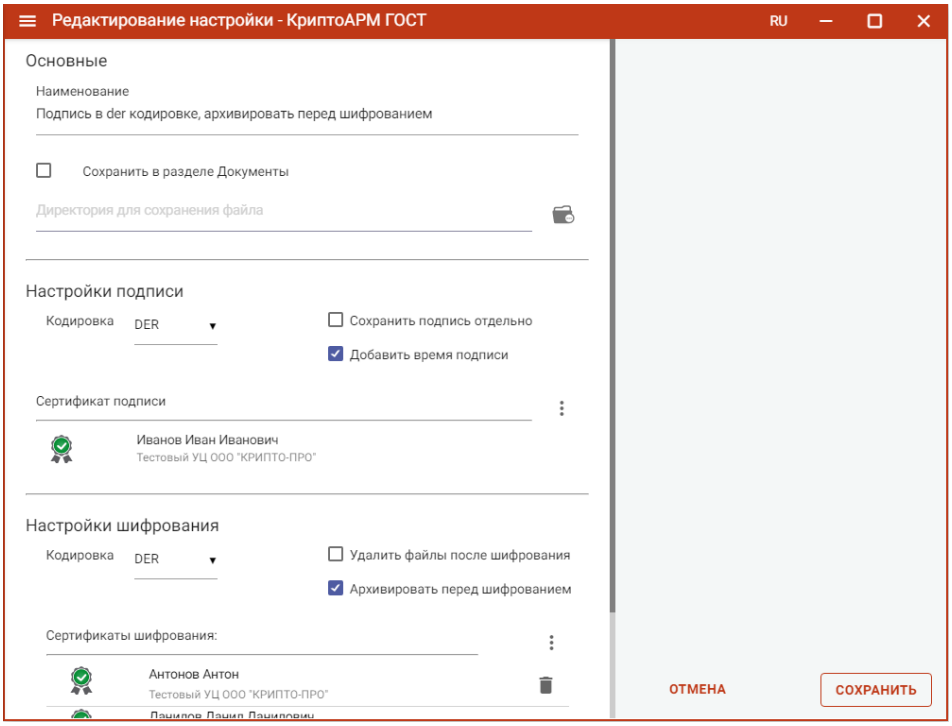


Рис. 5.13.7. Редактирование настройки

По кнопке **Сохранить** сделанные в настройке изменения сохраняются. По кнопке **Отмена** происходит возврат к параметрам настройки до редактирования.

Удаление настройки. По нажатию на кнопку **Удалить** происходит удаление настройки (рис. 5.13.8).

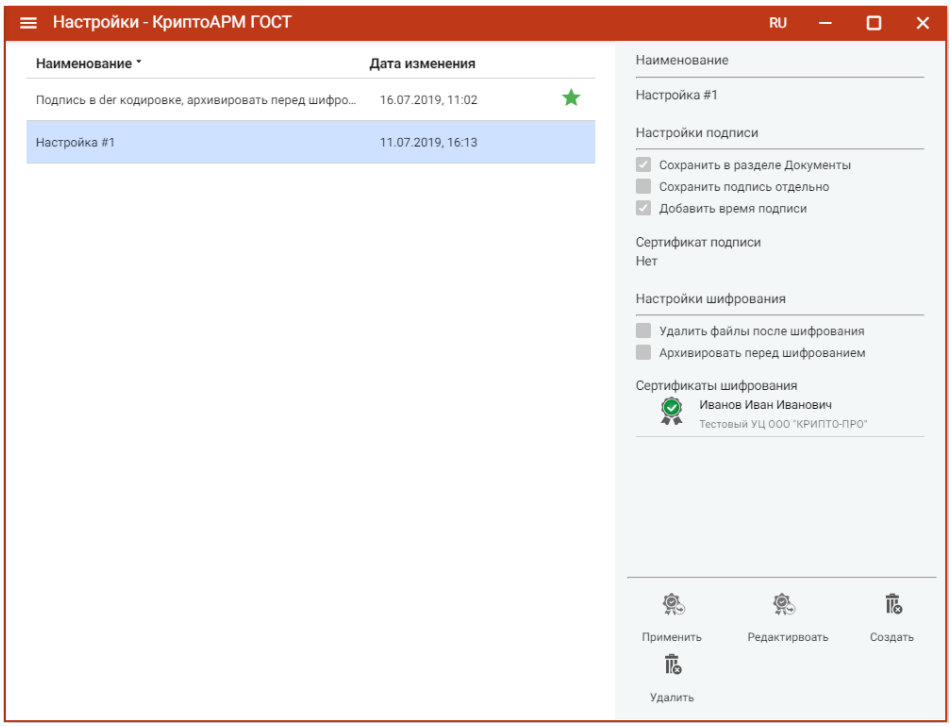


Рис. 5.13.8. Удаление настройки

Операция удаления недоступна для настройки по умолчанию.

5.14. Журнал операций

Журнал операций предназначен для отображения операций, выполняемых пользователем (рис. 5.14.1).

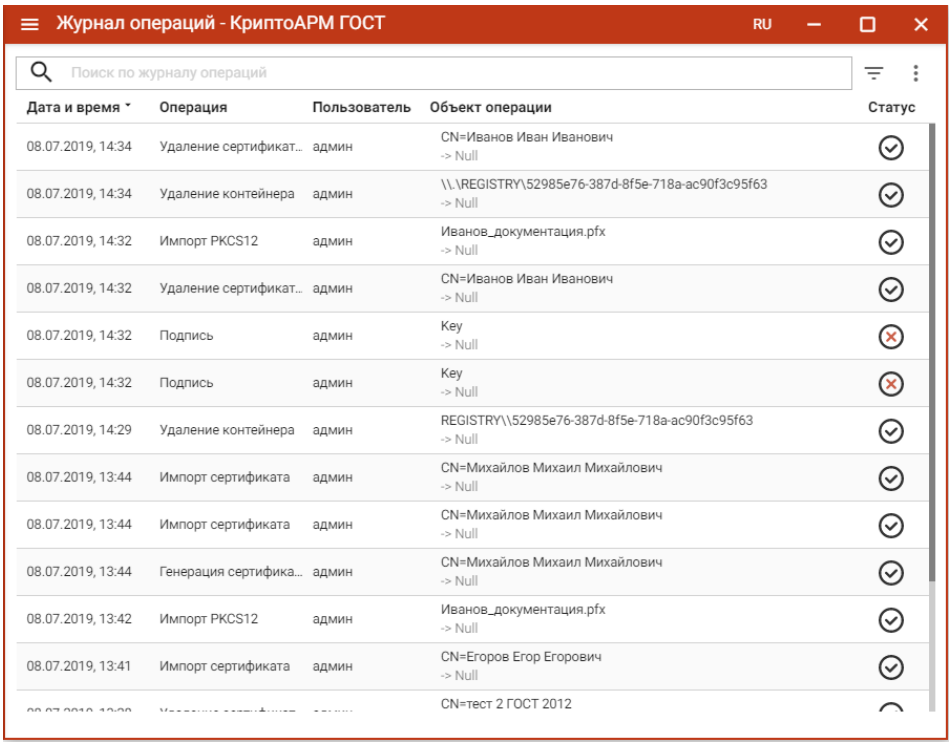


Рис. 5.14.1 Журнал операций

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 директории \.Trusted\CryptoARM_Gost\ под Windows и \.Trusted\CryptoARM_Gost\ под OSX и Linux.

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

При работе с журналом операций предусмотрен режим загрузки ранее сохраненной в архив его части для просмотра, поиска и фильтрации записей. Для этого используется пункт **Загрузить архивный журнал** контекстного меню журнала (рис.5.14.2)

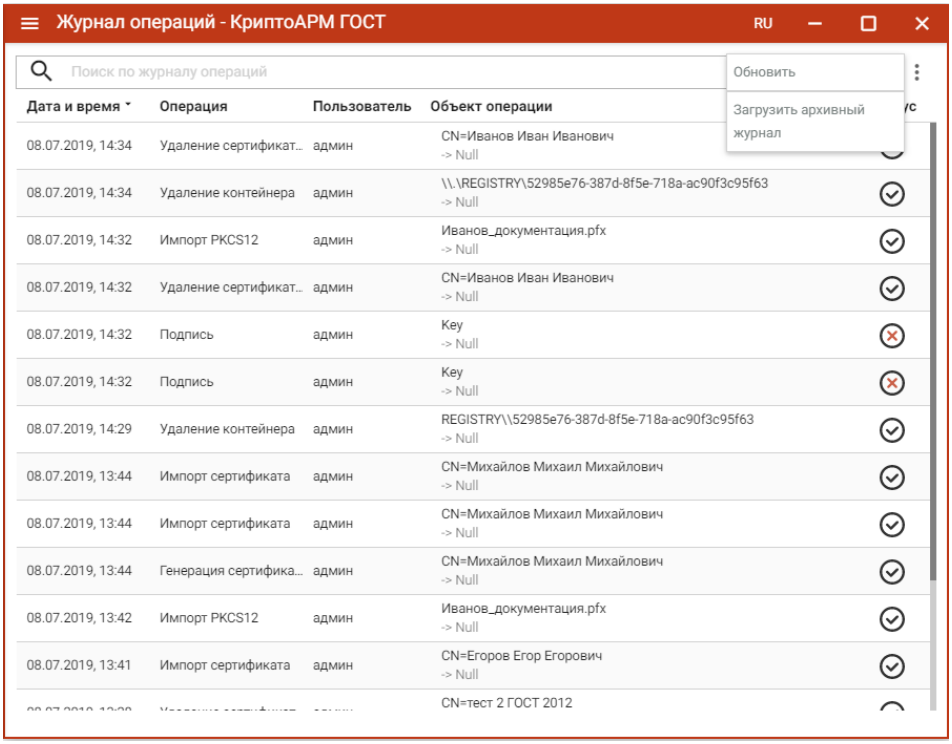


Рис. 5.14.2 Контекстное меню журнала операций

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

Для возврата к текущему журналу операций используется пункт контекстного меню архивного журнала **Вернуться к текущему журналу** (рис. 5.14.3)

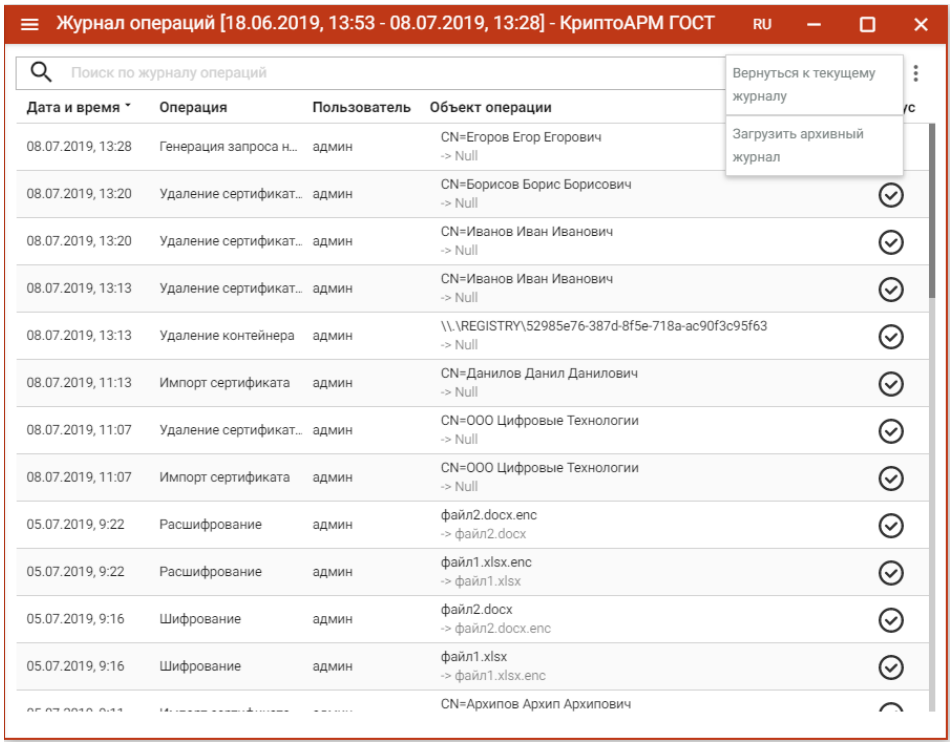


Рис. 5.14.3. Контекстное меню архивного журанала операций

ПОИСК ЗАПИСЕЙ В ЖУРНАЛЕ ОПЕРАЦИЙ. В приложении реализован поиск записей журнала операций по символьному совпадению (рис. 5.14.4)

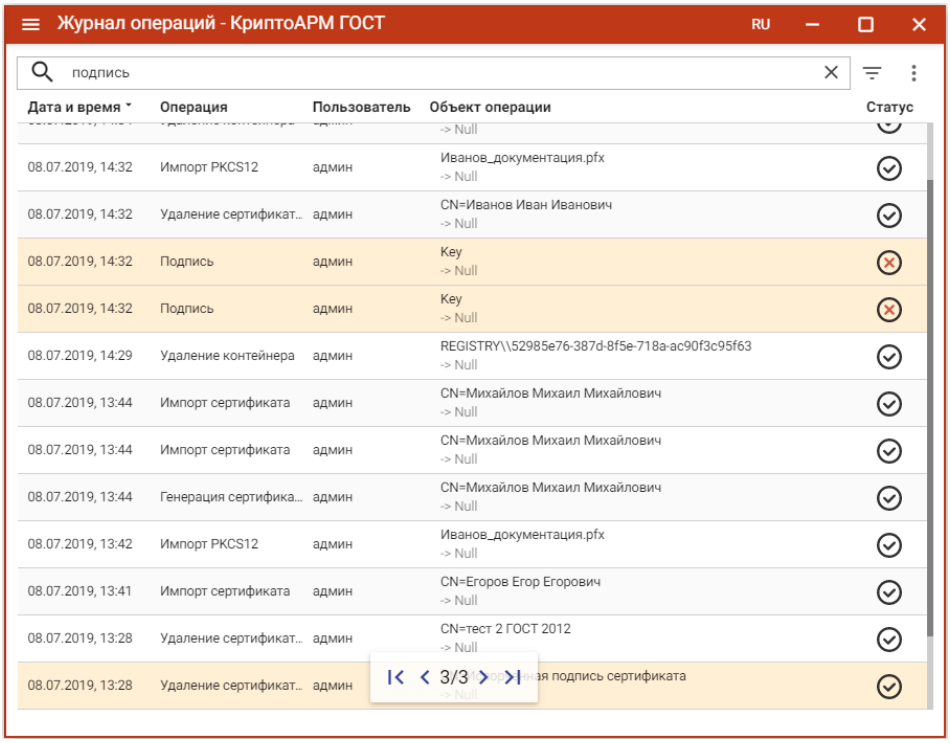


Рис. 5.14.4. Поиск записей в журнале операций

ФИЛЬТРАЦИЯ ЖУРНАЛА ОПЕРАЦИЙ. Для открытия окна настроек критериев фильтра на панели управления имеется кнопка, при нажатии на которую открывается окно настроек фильтрации (рис. 5.14.5).

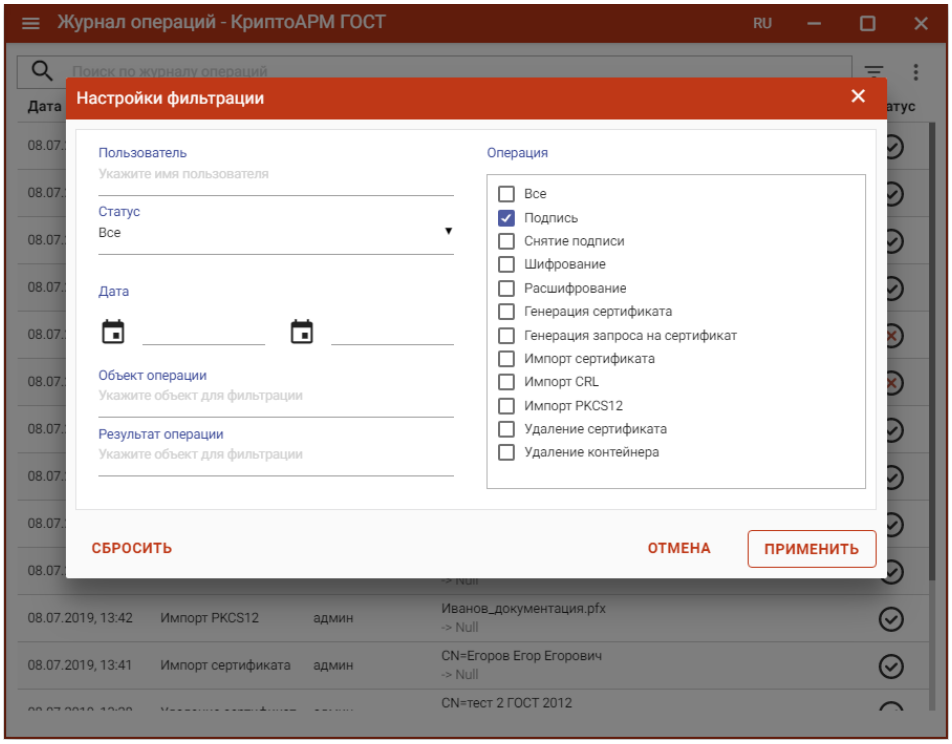


Рис. 5.14.5. Настройки критериев фильтра журнала операций

Применение фильтрации выполняется по нажатию кнопки **Применить**. В зависимости от выставленных критериев фильтра в журнале остаются только те записи, которые удовлетворяют (суммарно) этим критериям (рис. 8.13.6).

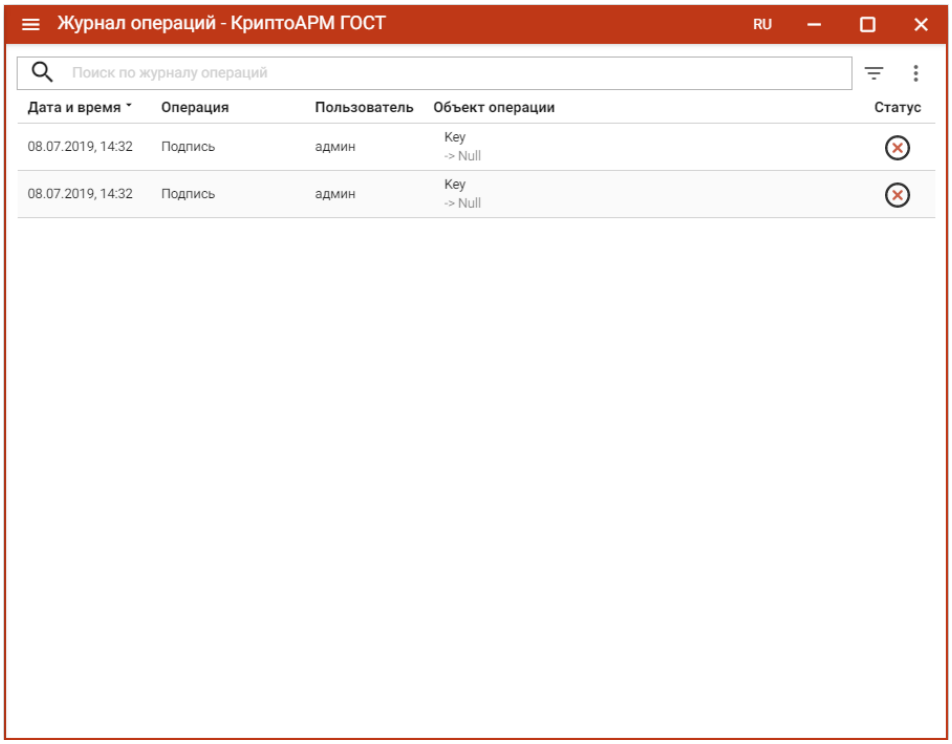


Рис. 5.14.6. Результат применения фильтрации журнала операций

Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации (рис. 5.14.5).

5.15. О программе

Краткие сведения о программе, сведения о лицензиях на КриптоАРМ ГОСТ и КриптоПро CSP, а так же адрес электронной почты для получения дополнительной технической поддержки можно узнать, выбрав в основном меню пункт **О программе** (рис. 5.15.1).

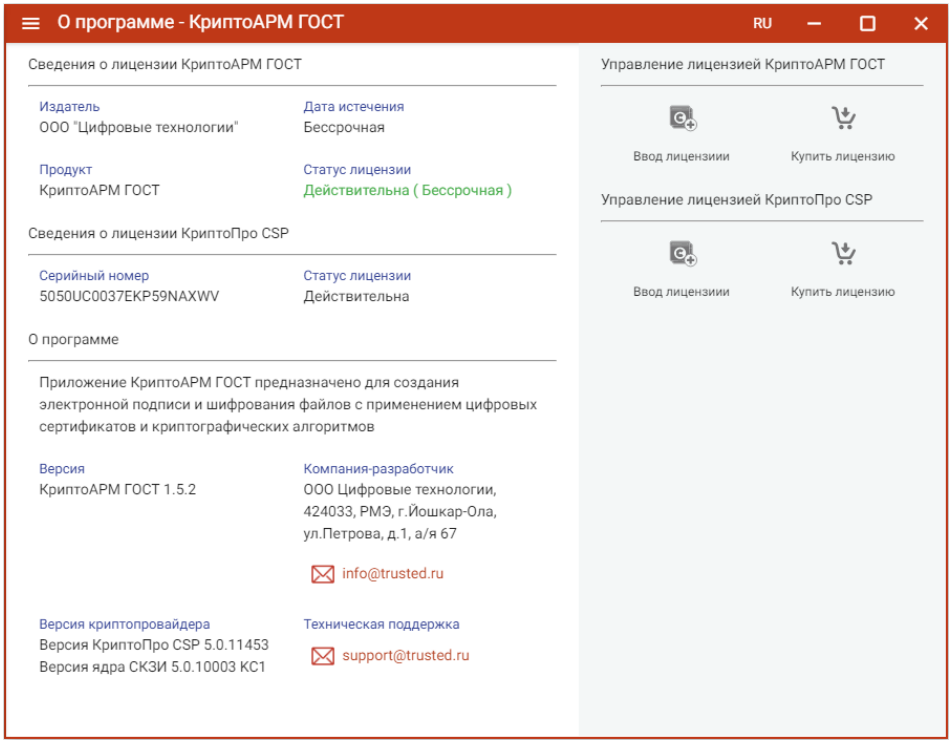


Рис. 5.15.1. Информация о программе

5.16. Справка

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

5.17. Отправка запросов на сертификат и установка сертификатов на основе КриптоПро УЦ 2.0

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

Создать подключение можно, выбрав пункт основного меню **Сервисы**. Открывается форма со списком зарегистрированных сервисов. Левая часть окна предназначена для управления списком сервисов; правая - для отображения информации и управления выбранным сервисом (рис. 5.17.1).

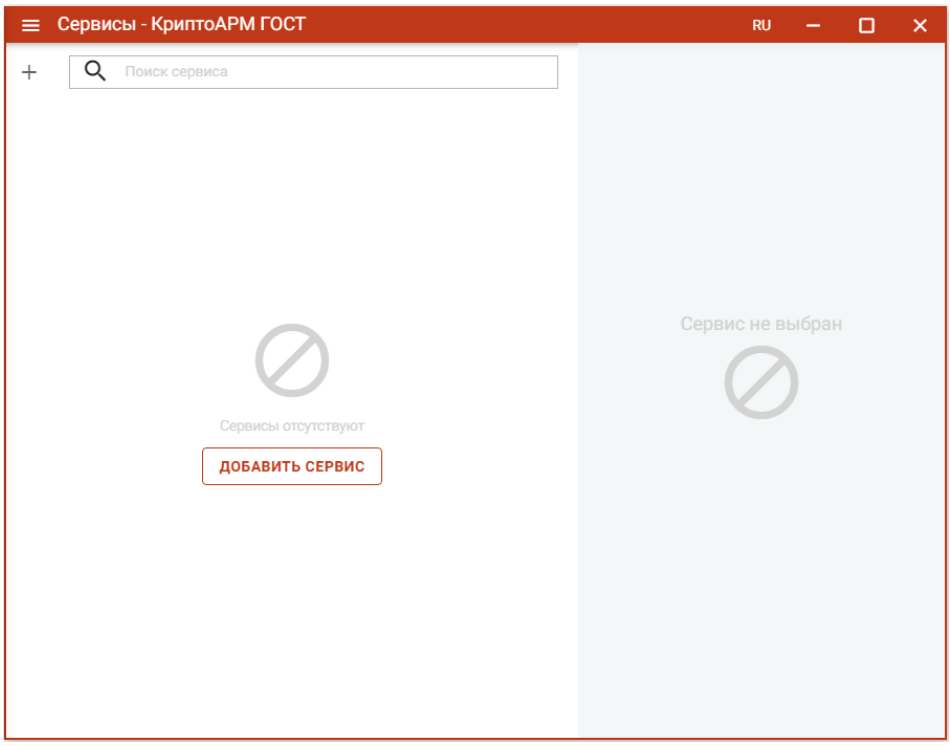


Рис. 5.17.1. Пустой список сервисов

ДОБАВЛЕНИЕ НОВОГО СЕРВИСА. Добавить подключение к сервису можно двумя способами: через кнопку **Добавить сервис** на пустом списке или через кнопку + рядом со строкой поиска. При нажатии на кнопку добавления сервиса открывается окно ввода параметров подключения (рис. 5.17.2).

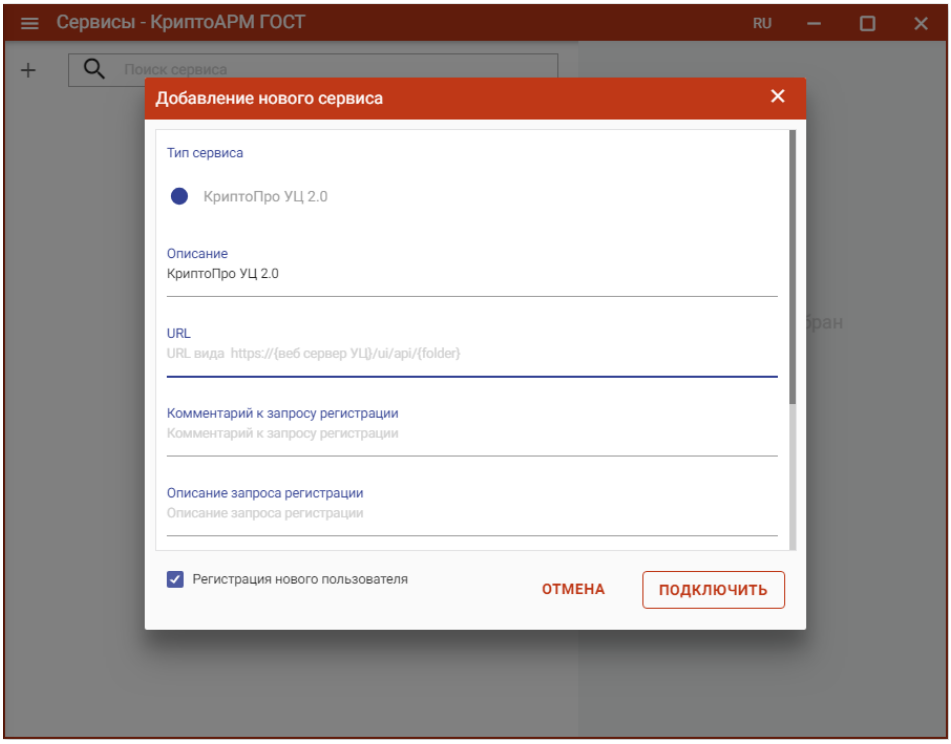


Рис. 5.17.2.

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** (рис. 5.17.3).

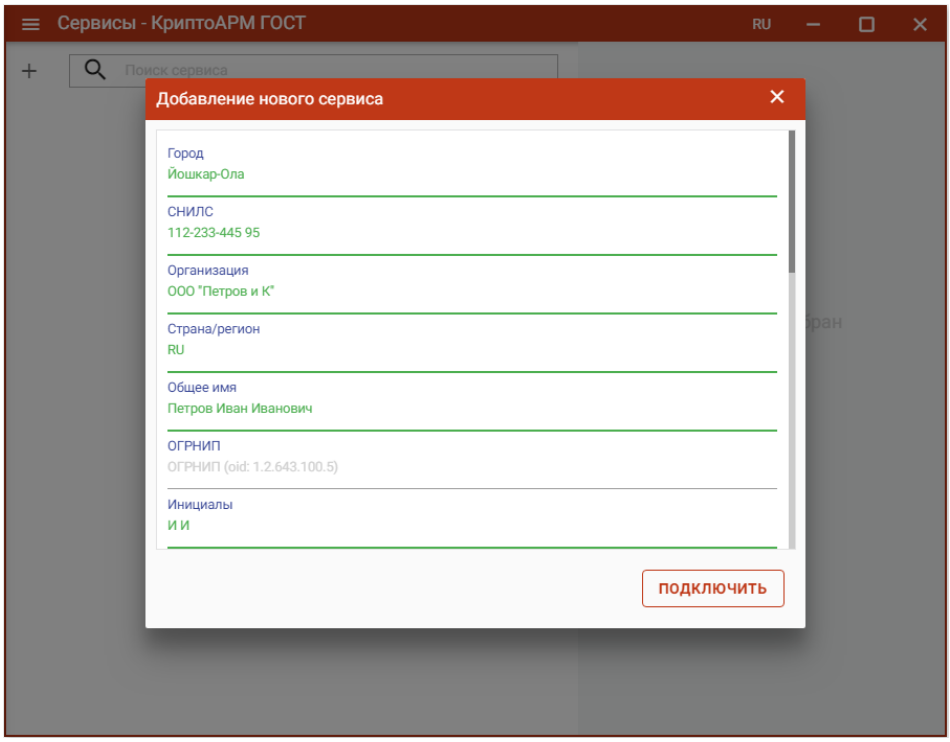


Рис. 5.17.3. Форма регистрации нового пользователя для подключения к УЦ

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**. На следующем шаге нужно ввести данные для авторизации и нажать **Подключить** (рис. 5.17.4).

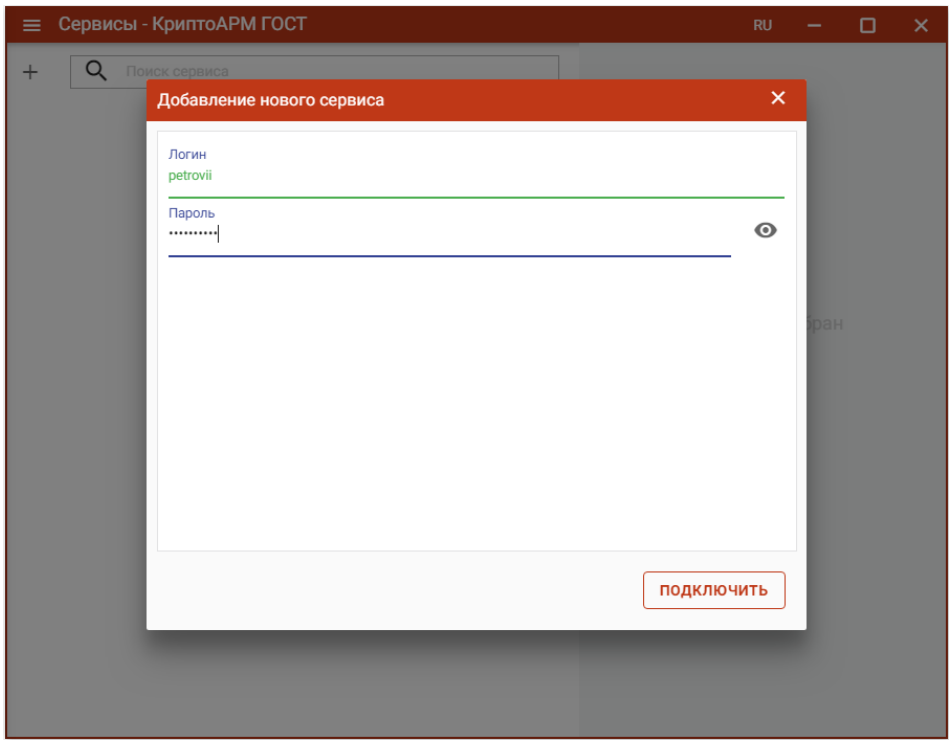


Рис. 5.17.4. Авторизация на сервисе УЦс помощью логина и пароля

После успешной регистрации или авторизации созданное подключение с сервисом по указанному пользователем адресу появляется в списке сервисов (рис. 5.17.5).

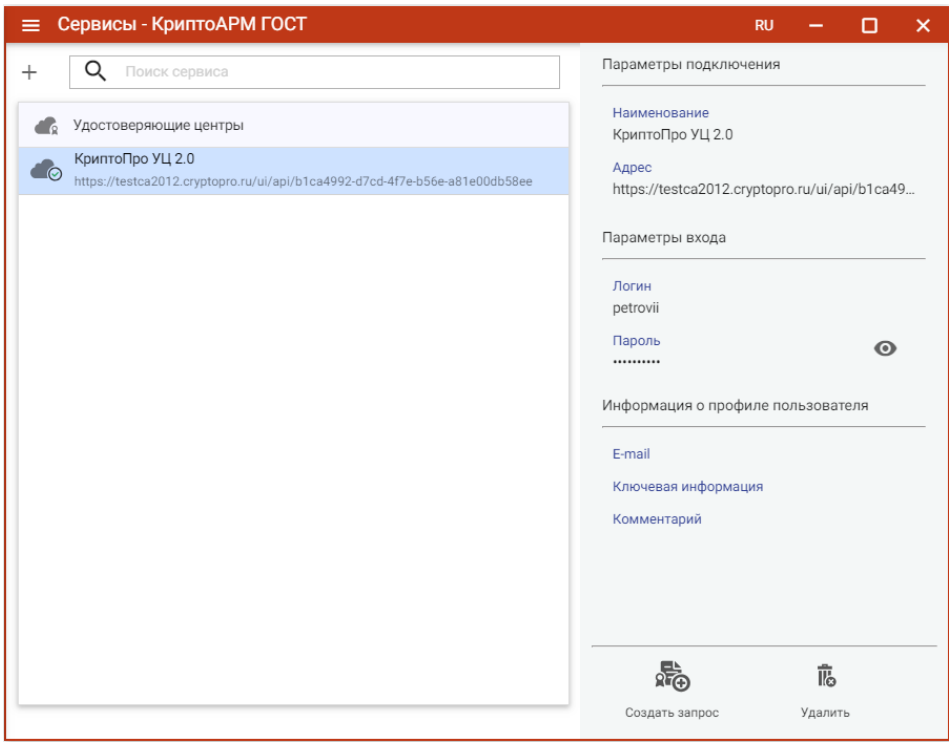


Рис. 5.17.5. Список подключенных сервисов

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, но или нет аутентификации на сервисе, или запрос по регистрации на сервисе еще не подтвержден. Пользователю следует подождать подтверждения регистрации.

Запрос на сертификат можно создать с формы просмотра подключения к сервисам УЦ или через пункт контекстного меню списка сертификатов (пункт основного меню Сертификаты).

СОЗДАНИЕ ЗАПРОСА НА СЕРТИФИКАТ С ФОРМЫ ПРОСМОТРА ПОДКЛЮЧЕНИЯ. При нажатии на кнопку **Создать запрос** открывается окно выбора шаблона сертификата (рис. 5.17.6).

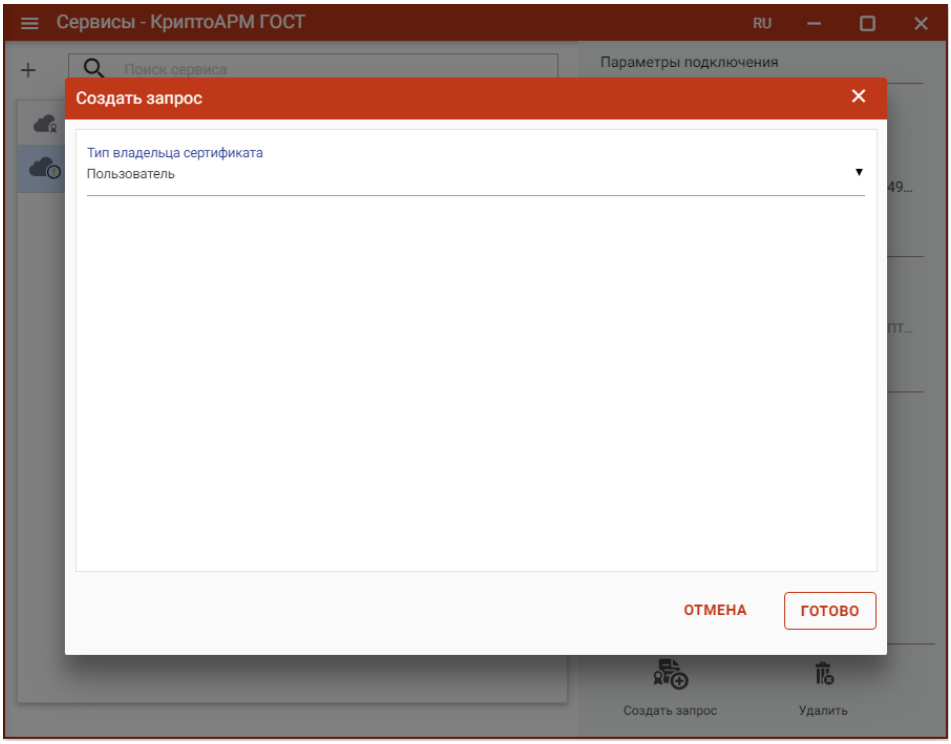


Рис. 5.17.6. Выбор шаблона запроса на сертификат

По нажатию на кнопку **Готово** открывается форма для заполнения полей запроса на сертификат, соответствующих выбранному шаблону. Причем поля, заполненные при регистрации пользователя на сервисе УЦ, подставляются в соответствующие поля на форме запроса (рис. 5.17.7).

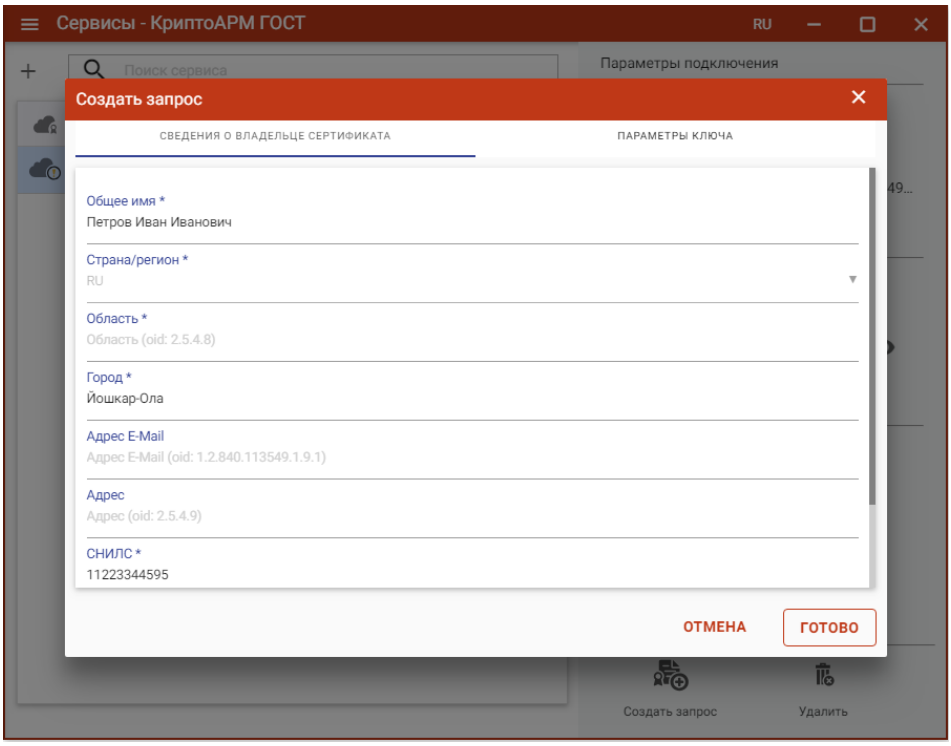


Рис. 5.17.7. Форма создания запроса на сертификат

Следует заполнить необходимые поля в запросе на вкладках **Сведения о владельце сертификата** и **Параметры ключ**а и нажать кнопку **Готово**. 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, отправленные в УЦ** на вкладке управления сертификатами.

СОЗДАНИЕ ЗАПРОСА НА СЕРТИФИКАТ ИЗ КОНТЕКСТНОГО МЕНЮ СПИСКА СЕРТИФИКАТОВ. Для создания запроса на сертификат в контекстном меню списка сертификатов нужно выбрать пункт меню **Получить сертификат через сервис УЦ** (рис. 5.17.8).

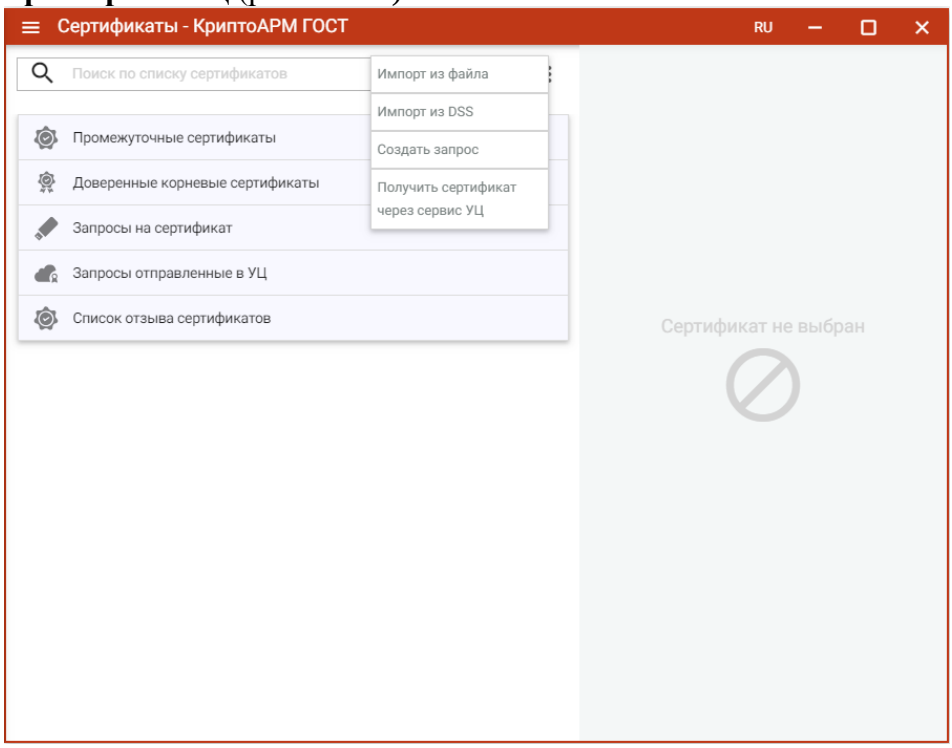


Рис. 5.17.8. Контекстное меню списка сертификатов

На первом шаге нужно выбрать подключение к сервису УЦ и шаблон (рис. 5.17.9)

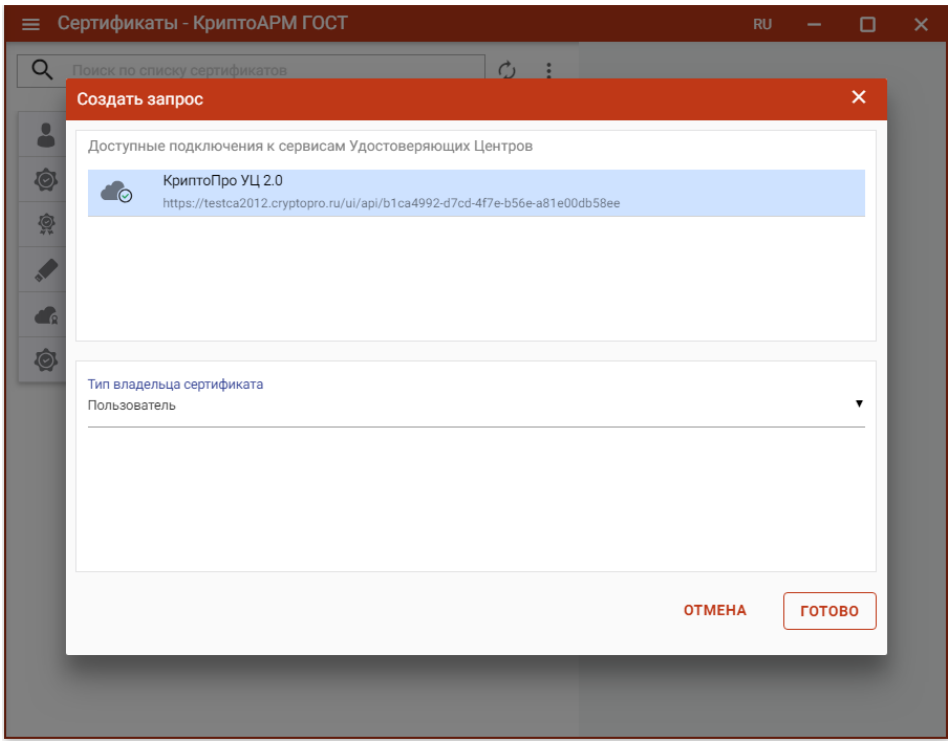


Рис. 5.17.9. Выбор сервиса и шаблона запроса на сертификат

По нажатию на кнопку **Готово** открывается форма для заполнения полей запроса на сертификат, соответствующих выбранному шаблону. Причем поля, заполненные при регистрации пользователя на сервисе УЦ, подставляются в соответствующие поля на форме запроса (рис. 5.17.10).

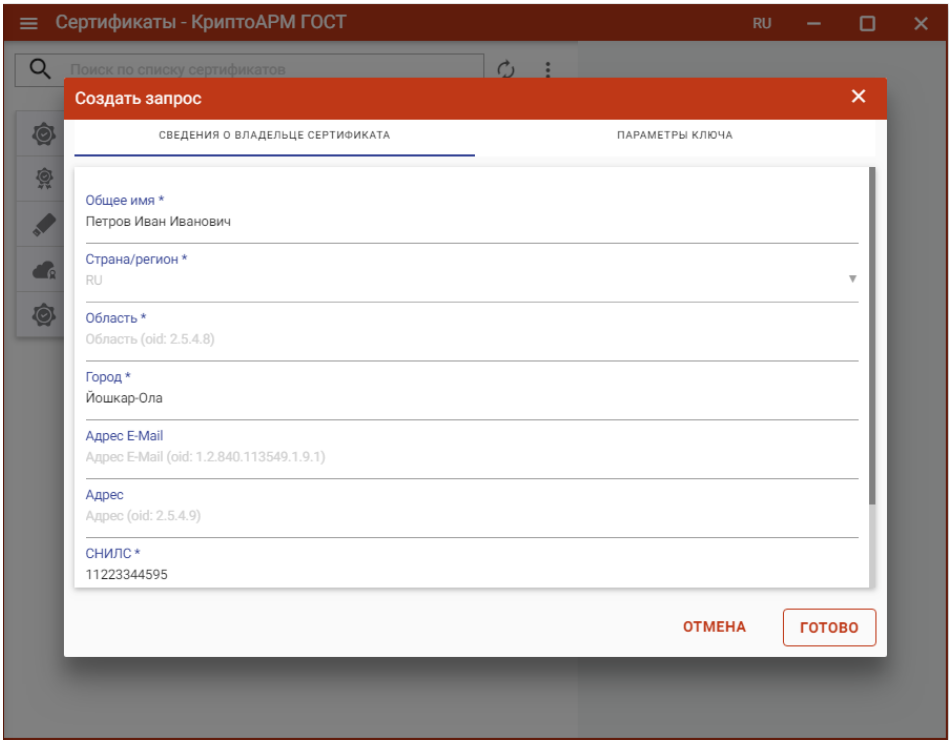


Рис. 5.17.10. Выбор сервиса и шаблона запроса на сертификат

Следует заполнить необходимые поля в запросе на вкладках **Сведения о владельце сертификата** и **Параметры ключа** и нажать кнопку **Готово**. 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, отправленные в УЦ** на вкладке управления сертификатами.

Управление запросами на сертификат, созданными через сервис УЦ. Запрос, созданный через подключенный сервис УЦ, сохраняется в раздел **Запросы, отправленные в УЦ** на вкладке управления сертификатами (рис. 5.17.11).

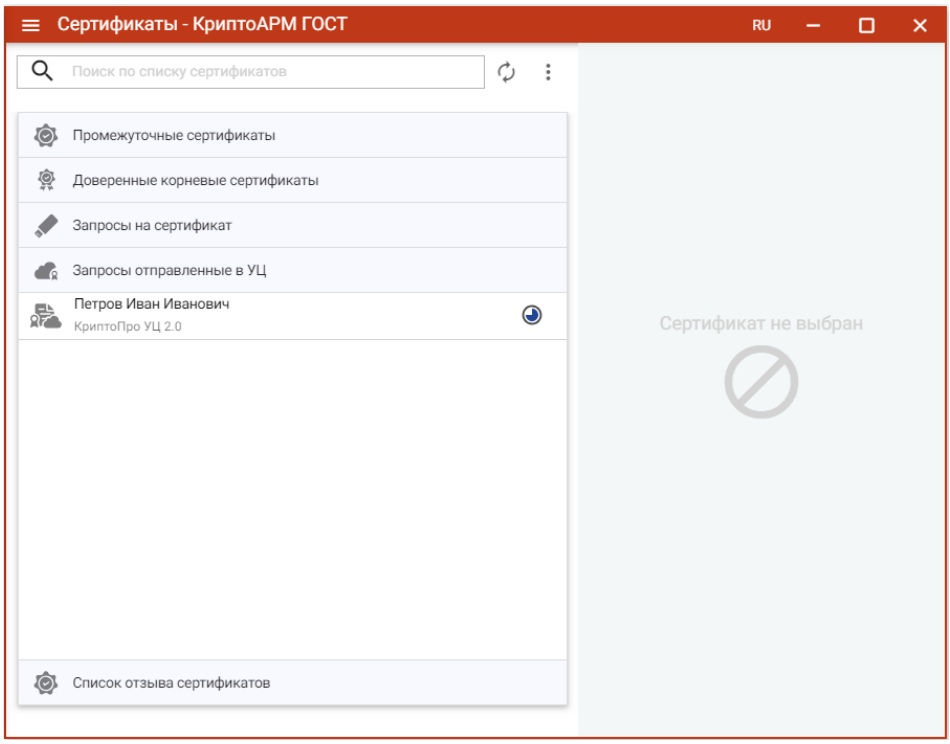


Рис. 5.17.11. Список запросов, отправленных в УЦ

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, статус запроса измениться на  (рис. 5.17.12), а сертификат установиться в Личное хранилище (рис. 5.17.13).

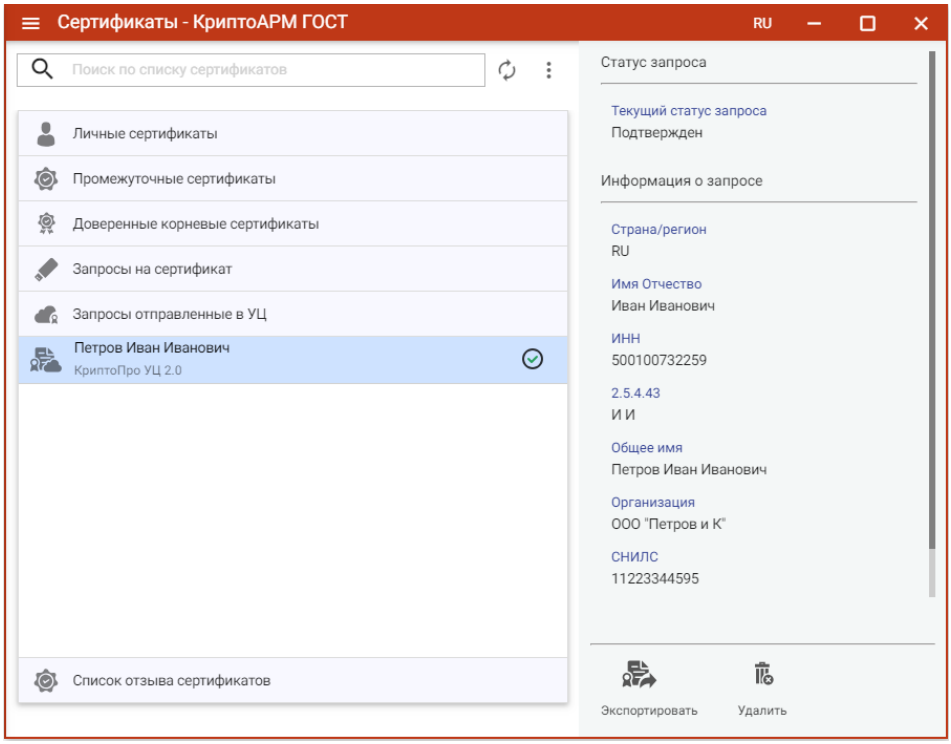


Рис. 5.17.12. Статус запроса, когда сертификат выпущен и установлен в хранилище

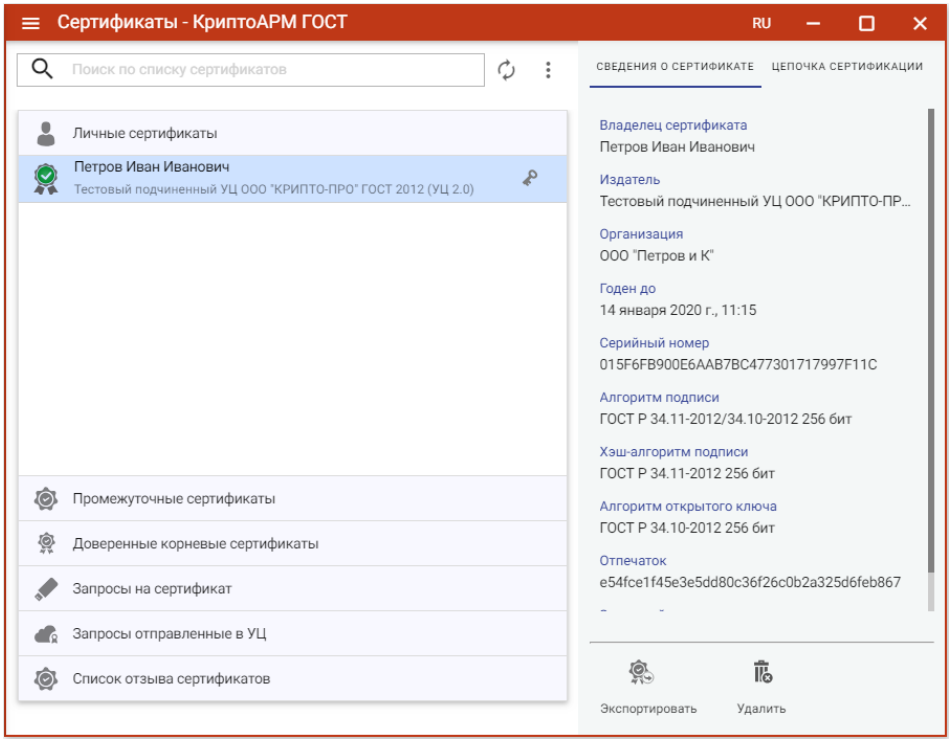


Рис. 5.17.13. Список личных сертификатов

Запрос на сертификат, полученный через сервис УЦ можно экспортировать в файл и удалить.

Удаление подключения к сервису УЦ. Для удаления подключения на форме просмотра сервиса нужно нажать кнопку **Удалить**. Появляется окно с подтверждением удаления (рис. 5.17.14).

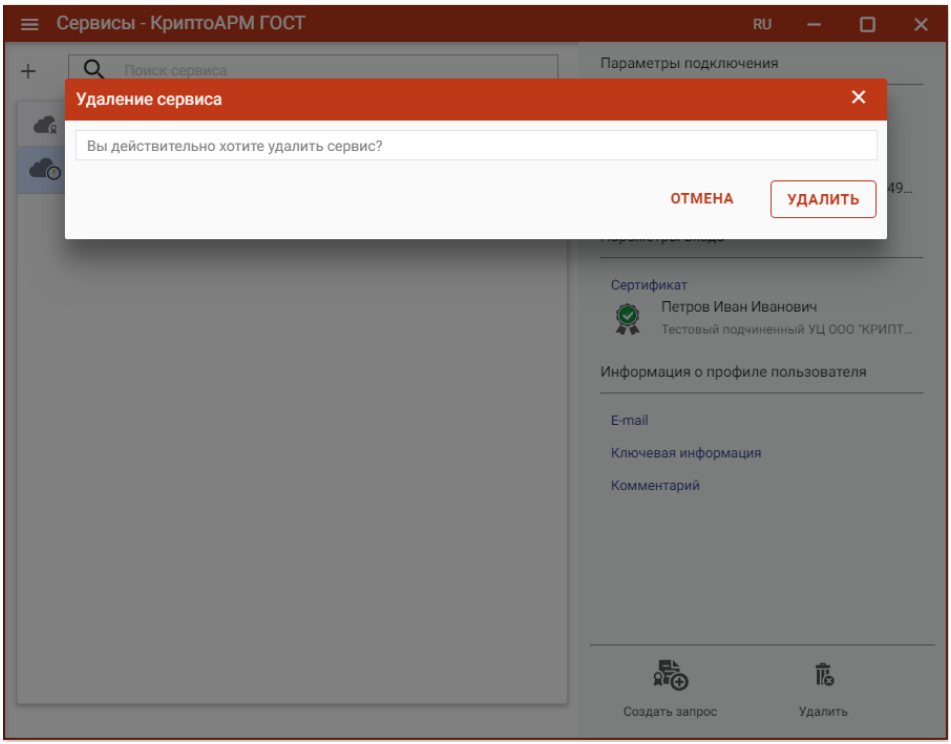


Рис. 5.17.14. Подтверждение удаления сервиса

После подтверждения удаления сервис из списка удаляется. При этом запрос на сертификат, созданный через сервис УЦ, и полученный сертификат не удаляются.

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 (рис. 6.1.1)

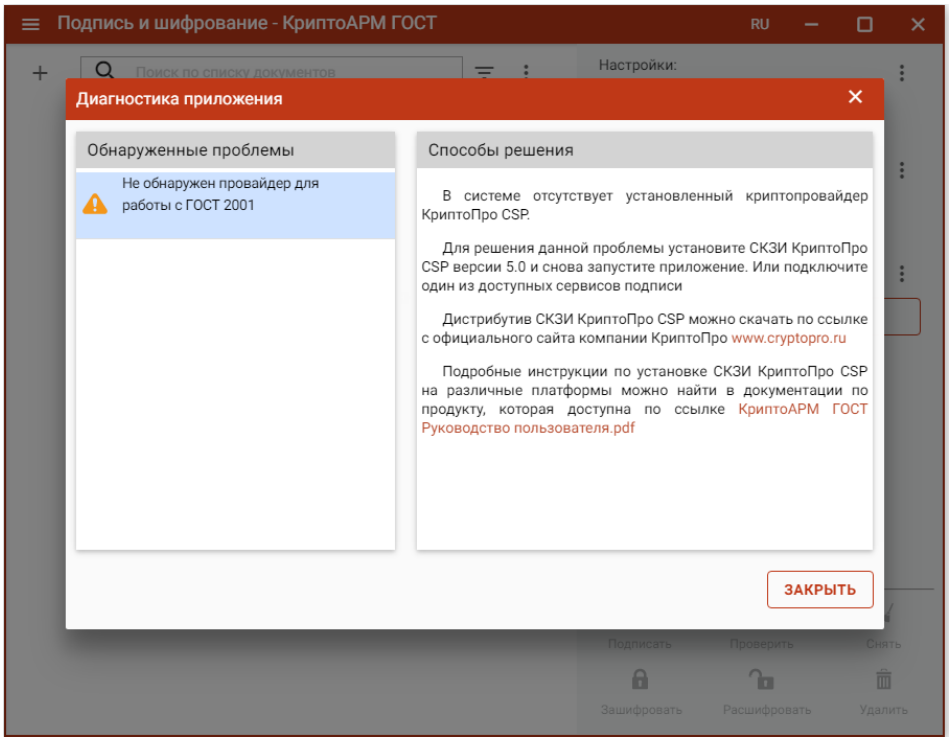


Рис. 6.1.1 Сообщение об отсутствии СКЗИ КриптоПро CSP

Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Инструкция по установке СКЗИ КриптоПро CSP описана в п. 4 «Установка криптопровайдера КриптоПро CSP».

6.2. Отсутствует лицензия на КриптоАРМ ГОСТ

Без установленной лицензии на программный продукт КриптоАРМ ГОСТ при запуске приложения возникает предупреждающее сообщение (рис. 6.2.1).

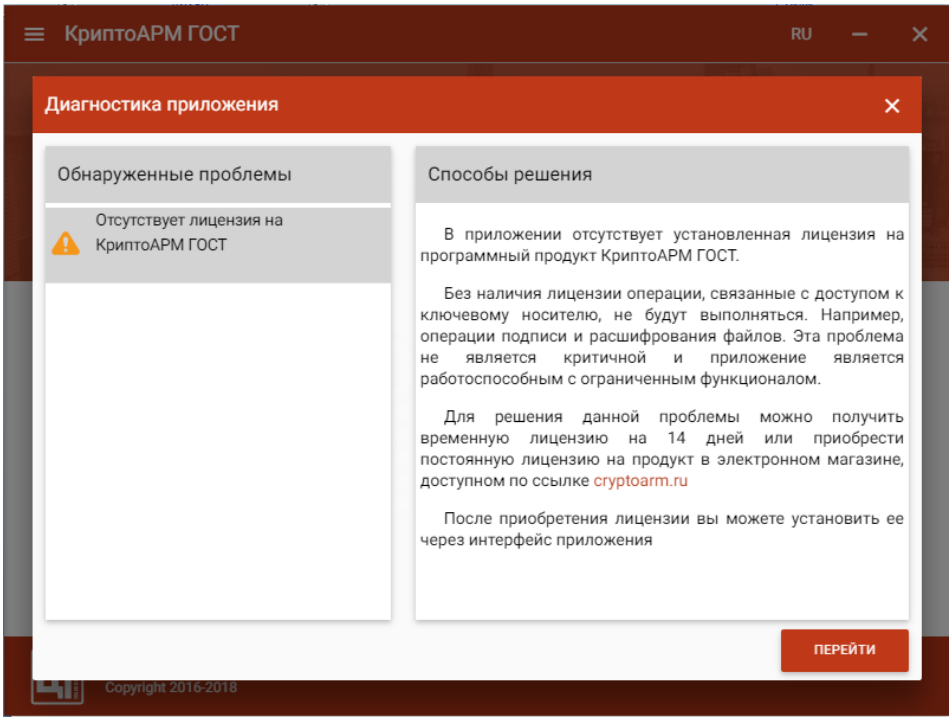


Рис. 6.2.1 Сообщение об отсутствии лицензии на КриптоАРМ ГОСТ

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. 3 «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 (рис. 6.3.1).

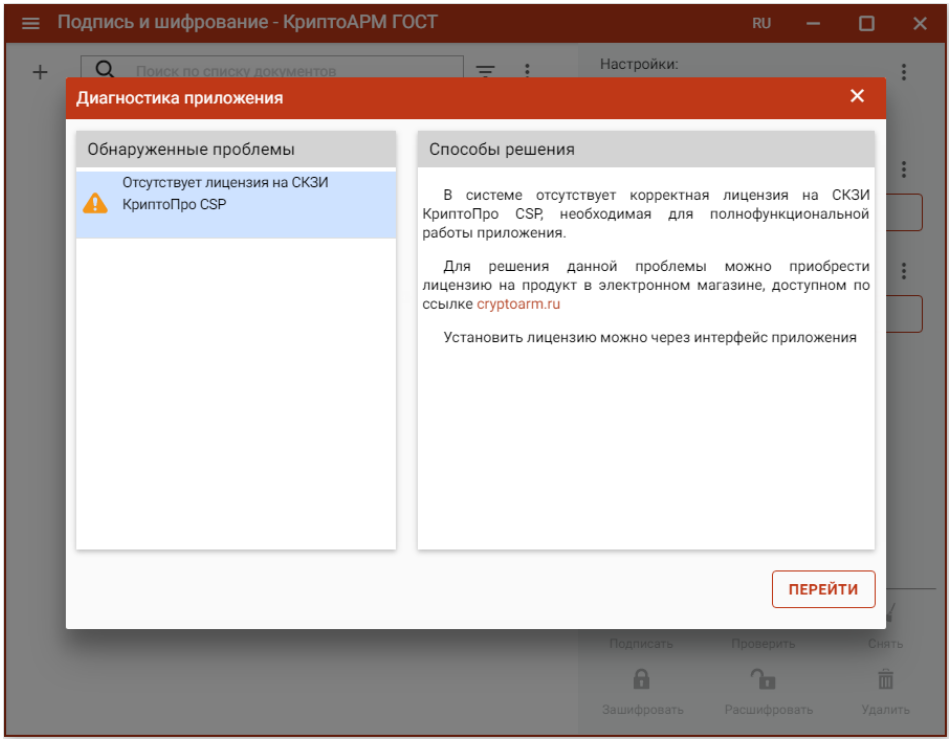


Рис. 6.3.1 Сообщение об отсутствии лицензии на КриптоПро CSP

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. 4.4 «Установка лицензии на программный продукт» данного руководства.

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 (рис. 6.4.1)

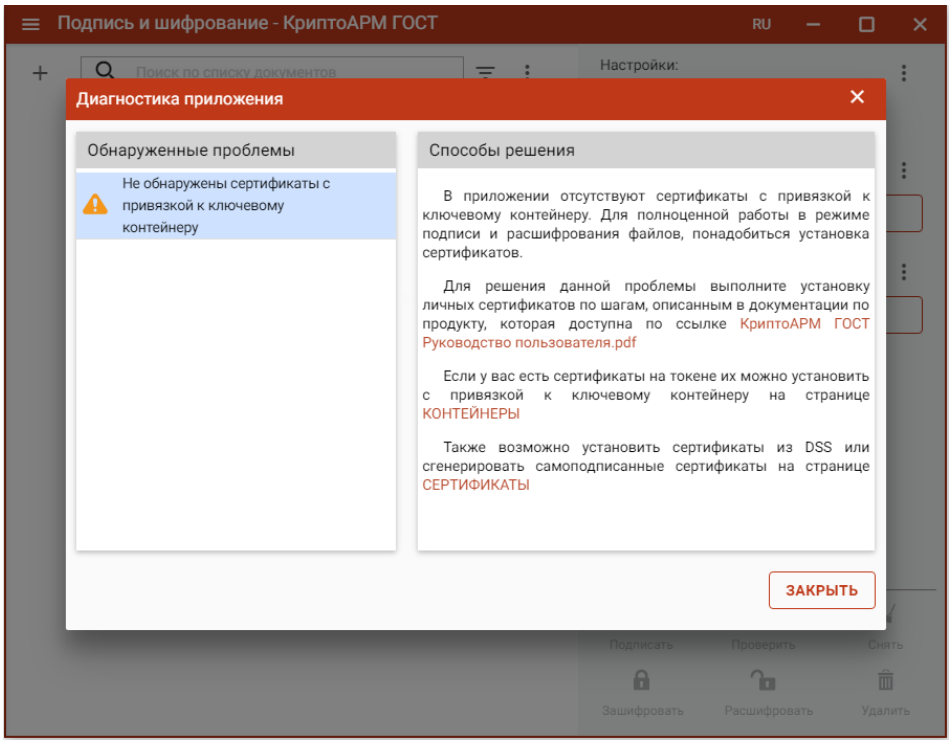


Рис. 6.4.1 Сообщение об отсутствии сертификатов с привязкой к закрытому ключу

Добавить личный сертификат можно несколькими способами:

- установить со стороннего носителя;
- установить из DSS (только для КриптоПРО CSP 5);
- сгенерировать запрос на сертификат и установить полученный сертификат;
- сгенерировать самоподписанный сертификат.

Установить личный сертификат со стороннего носителя можно одним из следующих способов:

1) Используя вкладку **Контейнеры**, если сертификат и закрытый ключ находятся на ключевом носителе (Рутокен, JaCarta). Для перехода на вкладку нужно вставить в компьютер ключевой носитель и нажать кнопку **Перейти**. Инструкция по установке сертификата из контейнера описана в п. 8.11 «Установка сертификата из ключевого контейнера».
2) Используя инструкцию в п. «Перенос контейнера закрытого ключа под требуемую операционную систему», если сертификат и контейнер расположены в другой операционной системе
3) Используя инструкцию из п. «Установка сертификата с токена с сохранением привязки к закрытому ключу», если сертификат и закрытый ключ находятся на ключевом носителе (Рутокен, JaCarta), но по каким-то причинам не удалось установить сертификат на вкладке **Контейнеры.**

Установить сертификат из DSS можно, перейдя по ссылке на страницу **Сертификаты**, выбрав пункт контекстного меню «Импорт из DSS».

Сгенерировать запрос на сертификат или создать самоподписанный сертификат можно, перейдя по ссылке в окне диагностики приложения на вкладку **Сертификаты.** Подробнее описано в пункте «Сертификаты» в разделе «Создание запроса на сертификат» и «Создание самоподписанного сертификата»

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 (рис. 6.5.1)

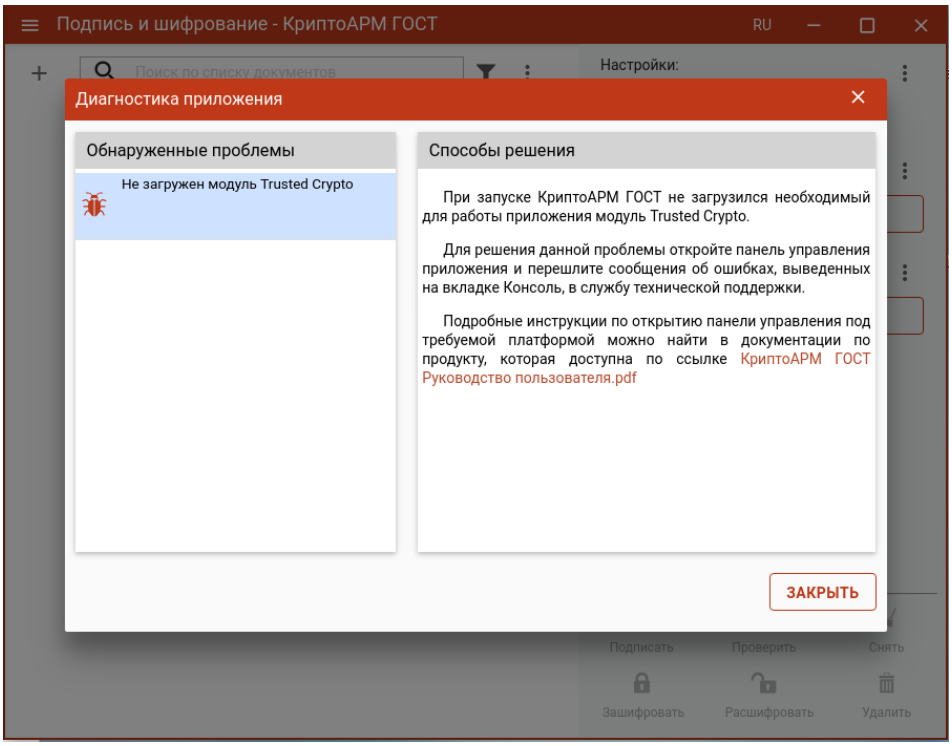


Рис. 6.5.1 Сообщение об ошибке в модуле Trusted Crypto

Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

Для Windows 7 для решения данной проблемы нужно установить “Распространяемый пакет Visual C++ для Visual Studio 2015” (https://www.microsoft.com/ru-RU/download/details.aspx?id=48145)

Для решения данной проблемы на других ОС необходимо запустить приложение в консольном режиме, скопировать информацию об ошибке и связаться со специалистами технической поддержки продукта КриптоАРМ ГОСТ. Инструкция по включению консольного режима описана в п. 9 «Включение режима логирования и консоль управления» данного руководства.

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

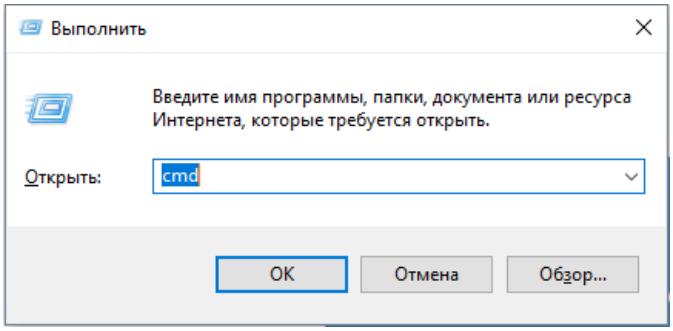


Рис. 7.1.1. Диалог для запуска приложений

В открывшемся окне ввести команду запуска приложения КриптоАРМ ГОСТ (рис. 7.1.2):

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

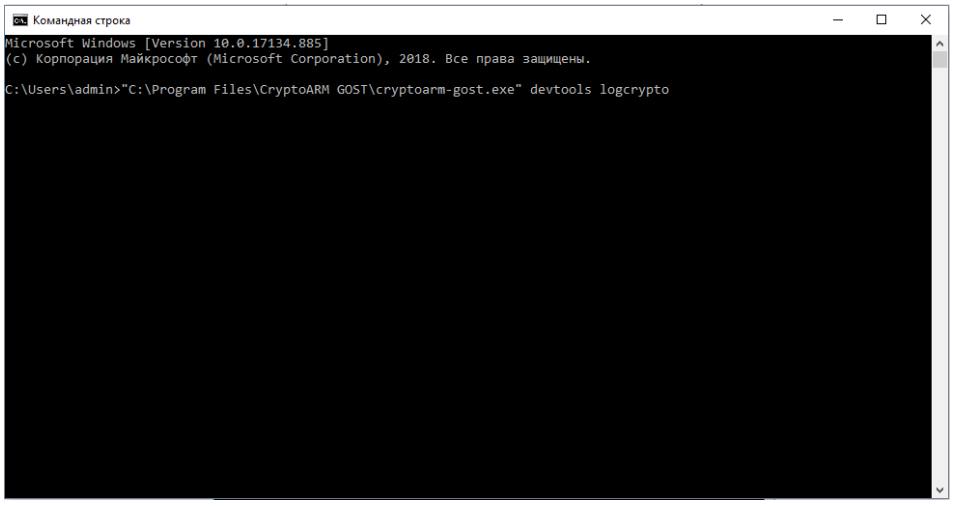


Рис. 7.1.2. Диалог командной строки

В результате выполнения этой команды откроется приложение КриптоАРМ ГОСТ с дополнительной панелью управления, которая представлена на рис. 7.1.3 и сохранением информации об операциях в журнал логирования.

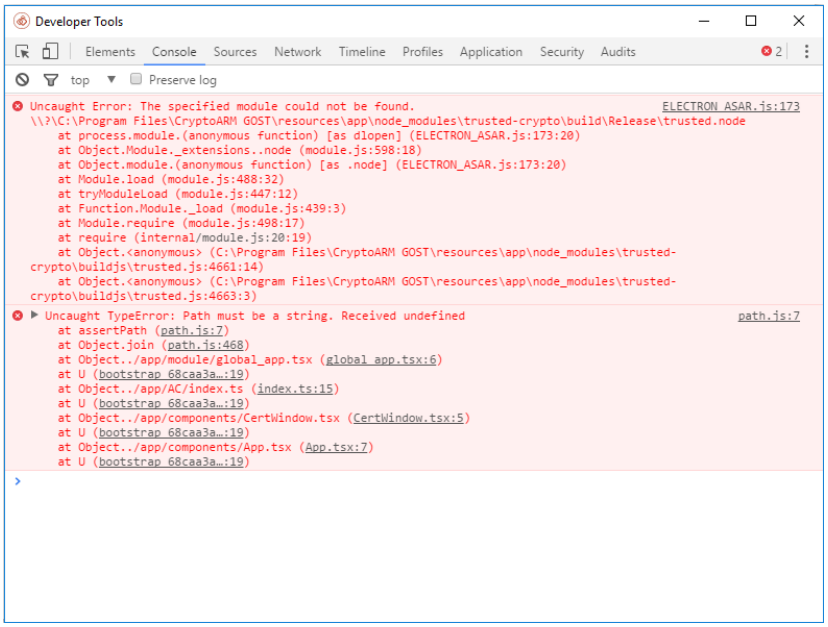


Рис. 7.1.3. Окно с вкладкой консоли управления

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 (рис. 7.2.1):

/opt/cryptoarm_gost/cryptoarm-gost devtools logcrypto

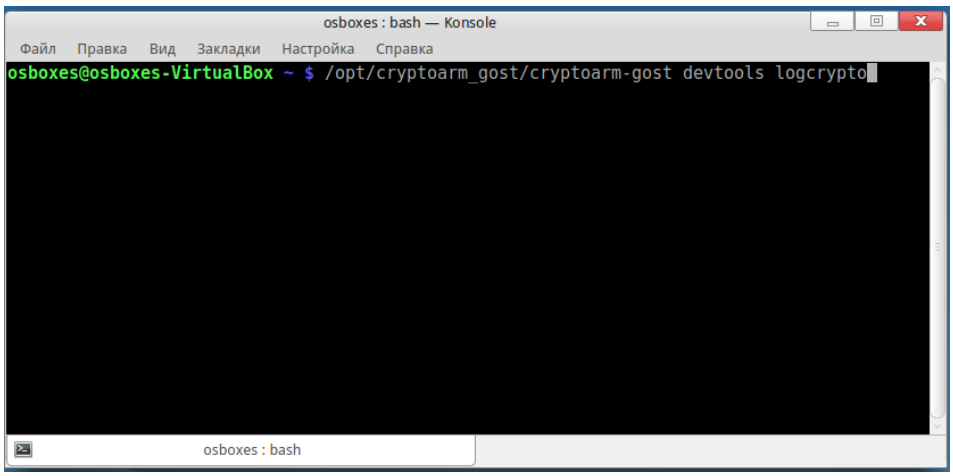


Рис. 7.2.1. Окно терминала

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне на вкладке Console отобразится текст ошибки (рис. 7.2.2).

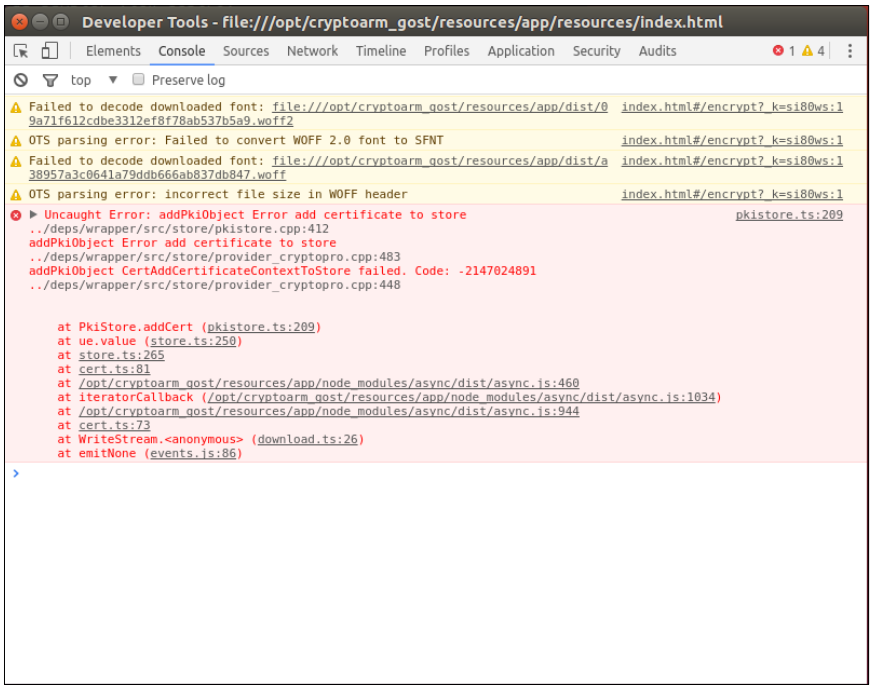


Рис. 7.2.2. Окно с вкладкой консоли управления

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 (рис. 7.3.1):

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

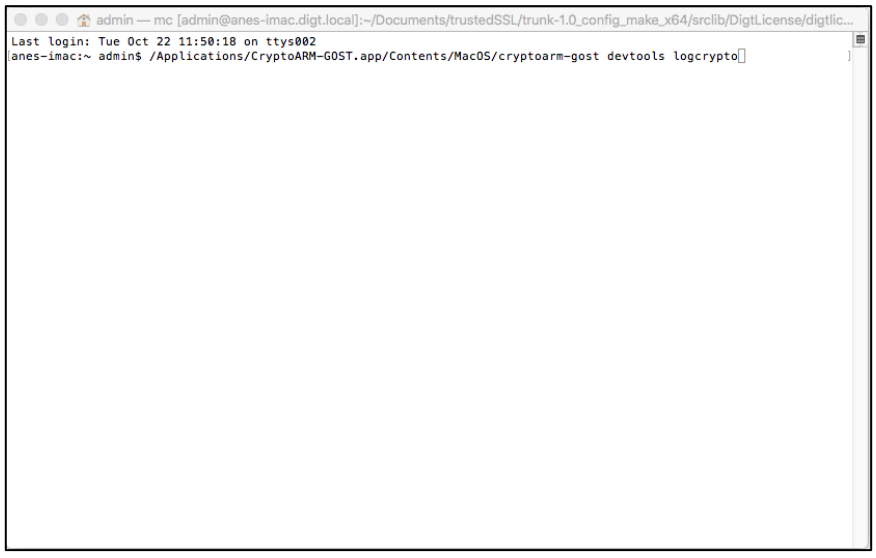


Рис. 7.3.1. Окно терминала

При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне на вкладке Console отобразится текст ошибки (рис. 7.3.2).

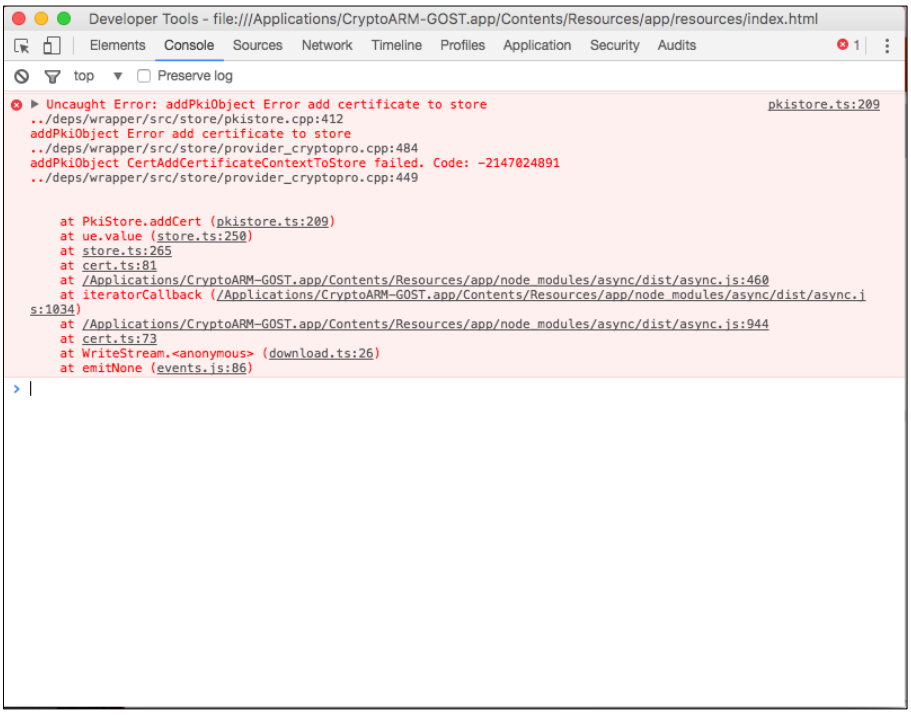


Рис. 7.3.2. Окно с вкладкой консоли управления

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, чтобы 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 **«Установка сертификата из ключевого контейнера».**

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**, как показано на рис.8.2.1.

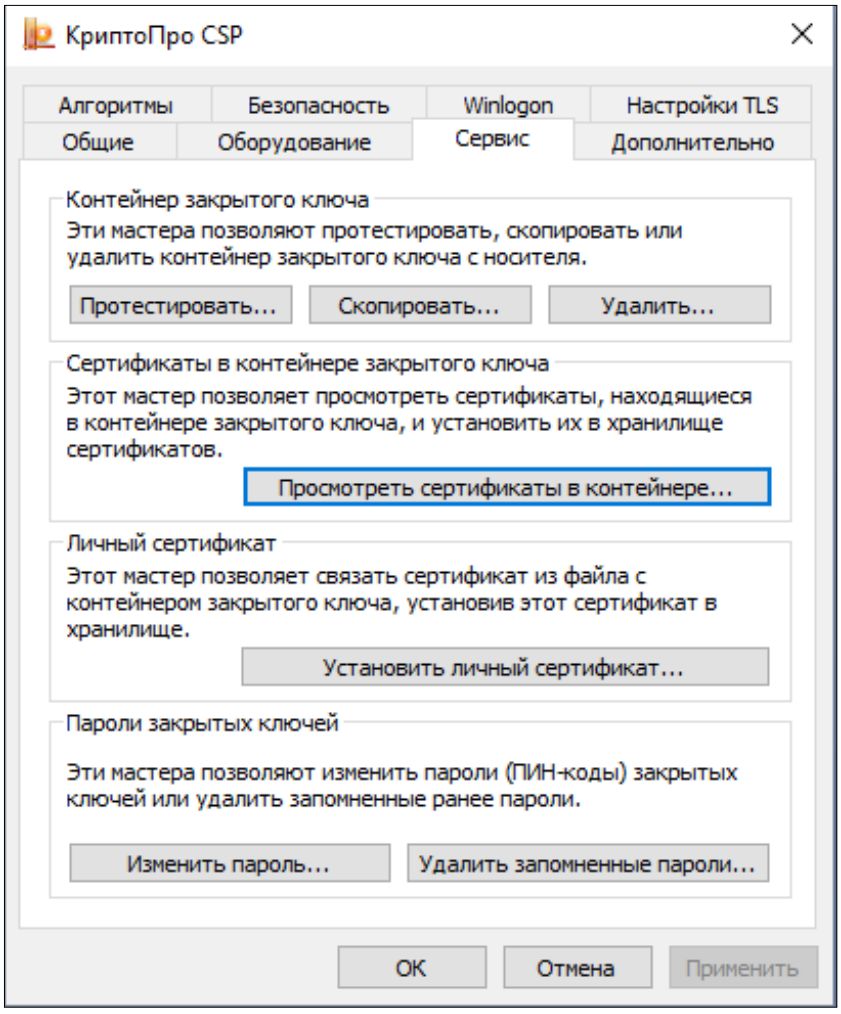


Рис.8.2.1. Диалог настроек криптопровайдера. Вкладка Сервис

После нажатия на кнопку **Просмотреть сертификаты в контейнере** должен открыться диалог поиска контейнера (рис. 8.2.2) в котором требуется нажать кнопку **Обзор**.

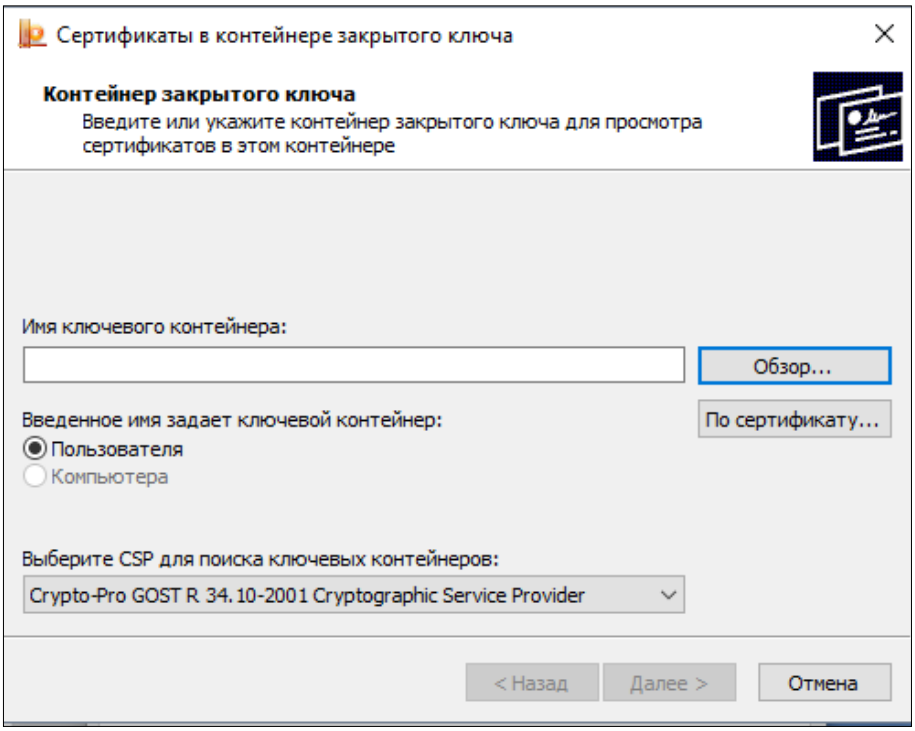


Рис.8.2.2. Диалог поиска ключевого контейнера

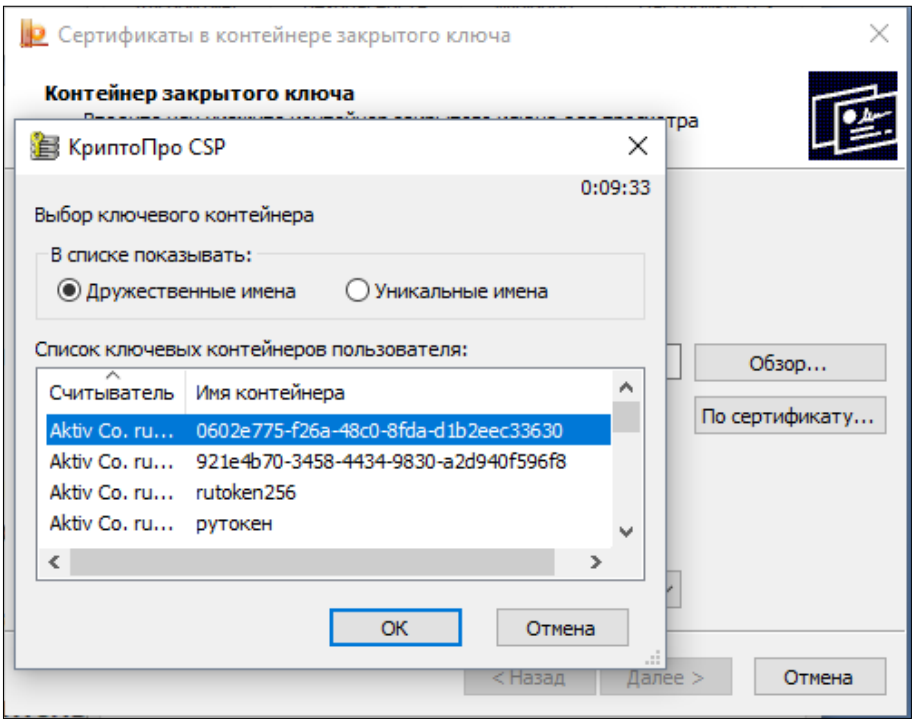


Рис.8.2.3. Выбор ключевого контейнера

Затем нужно выбрать нужный контейнер и нажать на кнопку **Далее** (см. рис. 8.2.4).

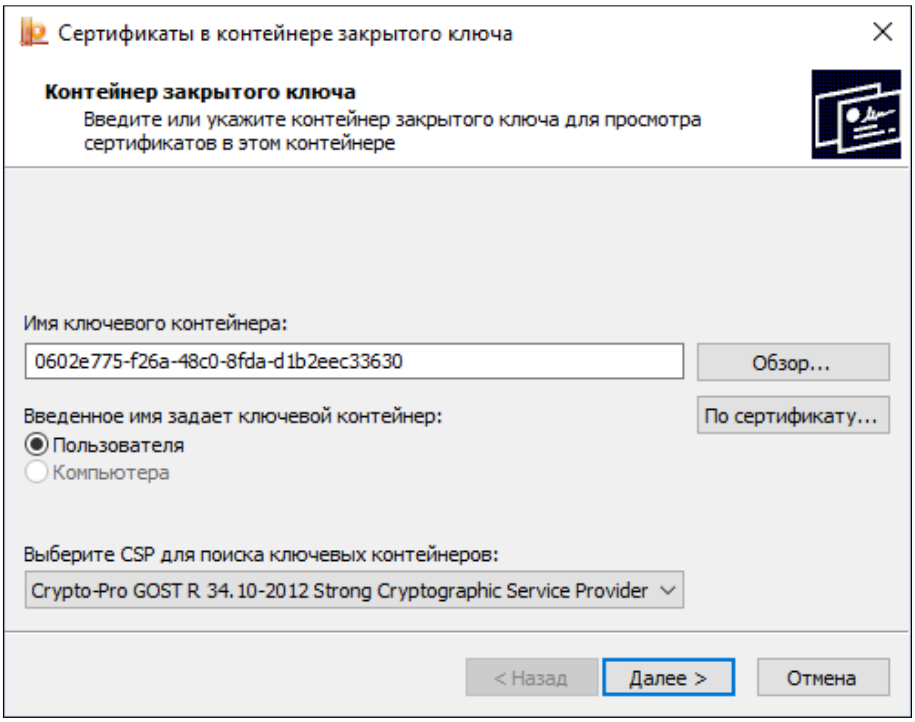


Рис.8.2.4. Просмотр содержимого контейнера

В контейнере содержится сертификат, сведения о котором будут отображены на последнем шаге мастера (рис.8.2.5). Этот сертификат можно установить в систему, нажав на кнопку **Установить**.

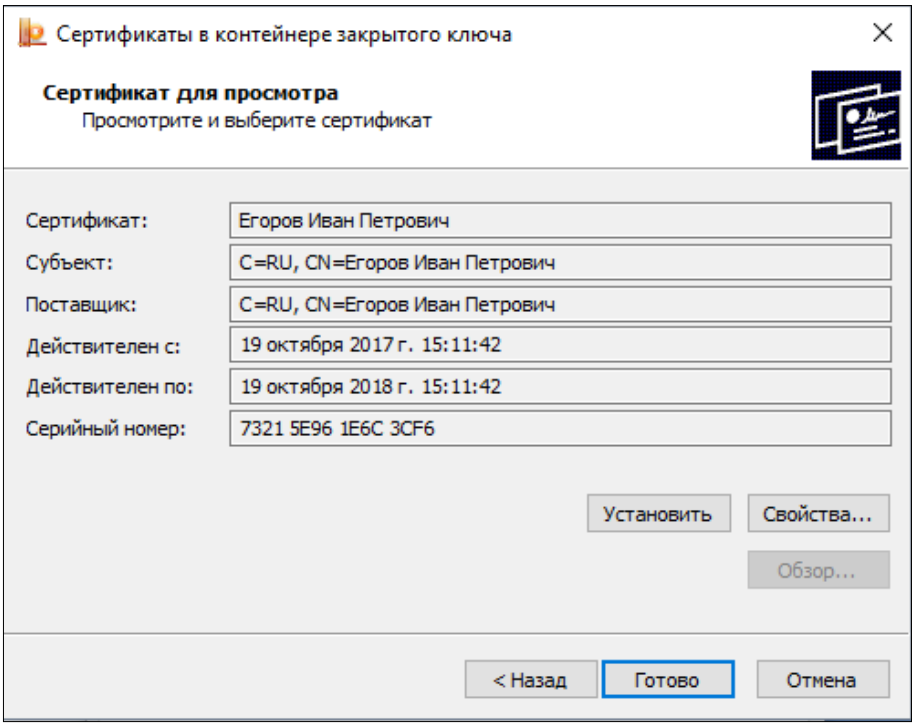


Рис.8.2.5. Сведения о сертификате внутри контейнера

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

– 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. 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)

9.2. 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

9.3. Не запускается КриптоАРМ ГОСТ на Windows.

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

9.4. Не запускается КриптоАРМ ГОСТ на Windows.

Возможно, версия КрипПро CSP ниже 4.

9.5. 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.

9.6. 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.

9.7. 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)"

9.8. Не создается запрос на сертификат на линукс при КриптоПро CSP 4

Актуально для создания самоподписанных сертификатов

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

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

Команда разработки и сопровождения продукта

Селедкин Андрей Евгеньевич

Менеджер по маркетингу, andrey.selyodkin@digt.ru

Компетенции в рамках проекта: изучение узкого сегмента рынка программных продуктов, формирование стратегии развития продукта, организация испытаний на совместимость продукта, вывод продукта на рынок, презентация продукта.

Чесноков Сергей Евгеньевич

Инженер-программист, shesnokov@gmail.com

Компетенции в рамках проекта: планирование процесса разработки продукта. разработка графического пользовательского интерфейса продукта, разработка ядра продукта, сборка продукта для различных платформ, создание технической и пользовательской документации, техническая поддержка продукта

Гаврилов Александр Владимирович

Инженер-программист, alg@digt.ru

Компетенции в рамках проекта: разработка графического пользовательского интерфейса, разработка внешних модулей для криптографических преобразований, интеграция с криптопропровайдерами, сопровождение репозиториев OpenSource-частей проекта, техническая поддержка продукта.

Шалагина Наталья Владимировна

Специалист по тестированию, nsh@digt.ru

Компетенции в рамках проекта: разработка методик тестирования продукта под различными платформами, создание технической и пользовательской документации, техническая поддержка продукта.

Контактная информация

Компания «Цифровые технологии» – российский разработчик и поставщик программного обеспечения в области защиты информации, телекоммуникаций и Интернет-сервисов.

Направление исследований и создания программных продуктов:

- разработка кроссплатформенных решений в области защиты данных, как в виде отдельных собственных продуктов, так и технологических стеков.
- встраивание российских сертифицированных криптографических алгоритмов в информационные системы, независимо от их бизнес-задачи.
- создание систем авторизации и аутентификации пользователей.
- консалтинг в области использования средств криптографической защиты информации (СКЗИ) в государственной и коммерческой среде.

Особое внимание разработчики компании уделяют внедрению и поддержки отечественных стандартов защиты информации, в том числе сертифицированных продуктов.

В случае необходимости получения дополнительной информации по продукту КриптоАРМ ГОСТ, можно обратиться непосредственно к разработчикам продукта или в службу технической поддержки компании – support@trusted.ru.

Контактная информация:

info@trusted.ru

8 (8362) 33-70-50, 8 (499) 705-91-10, 8 (800) 555-65-81

424033, РМЭ, г. Йошкар-Ола, ул. Петрова, д.1, а/я 67