



# КриптоАРМ ГОСТ

Руководство пользователя



## ОГЛАВЛЕНИЕ

Общие сведения о программном продукте .....	5
1.1.1.    Функциональность версии 2.2.0 .....	5
1.1.2.    Поддерживаемые криптопровайдеры .....	6
1.1.3.    Лицензия на программный продукт.....	6
1.1.4.    Доля использования OpenSource проектов .....	6
Системные требования .....	8
Поддерживаемые операционные системы .....	9
1.    Установка программного продукта .....	10
1.1.    Установка на платформу Microsoft Windows .....	10
1.2.    Установка на платформу Linux .....	12
1.3.    Установка на платформу OS X .....	13
2.    Удаление программного продукта.....	18
2.1.    Удаление приложения на платформе MS Windows.....	18
2.2.    Удаление приложения на платформе Linux.....	18
2.3.    Удаление приложения на платформе OS X.....	19
3.    Установка лицензии на программный продукт .....	20
3.1.    Установка лицензии через пользовательский интерфейс.....	20
3.1.1.    Установка постоянной лицензии .....	20
3.2.    Установка лицензии через командную строку .....	22
4.    Установка криптопровайдера КриптоПро CSP .....	23
4.1.    Установка криптопровайдера на платформу MS Windows.....	23
4.2.    Установка криптопровайдера на платформу Linux .....	23
4.2.1.    Установка базовых пакетов скриптом.....	23
4.2.2.    Установка пакетов.....	23
4.2.3.    Установка пакета для модулей TSP и OCSP.....	24
4.2.4.    Установка пакета для графического интерфейса ввода пароля .....	24
4.2.5.    Установка пакетов для работы с ключевыми носителями.....	24
4.2.6.    Установка пакетов для работы с «облачными» сертификатами .....	25
4.3.    Установка криптопровайдера на платформу OS X .....	25
4.4.    Установка лицензии на программный продукт КриптоПро CSP .....	25
4.4.1.    Установка лицензии через пользовательский интерфейс. ....	26
4.4.2.    Установка лицензии через командную строку для ОС Linux и MacOS .....	28
4.4.3.    Установка лицензии через программный интерфейс КриптоПро CSP для ОС Windows .....	28
4.5.    Установка лицензии на модуль TSP.....	29
4.5.1.    Установка лицензии через пользовательский интерфейс. ....	29
4.5.2.    Установка лицензии через командную строку для ОС MacOS.....	31
4.5.3.    Установка лицензии через командную строку для ОС Linux.....	31
4.5.4.    Установка лицензии для ОС Windows .....	31



4.6.	Установка лицензии на модуль OCSP .....	32
4.6.1.	Установка лицензии через пользовательский интерфейс. ....	32
4.6.2.	Установка лицензии через командную строку для ОС MacOS.....	33
4.6.3.	Установка лицензии через командную строку для ОС Linux.....	33
4.6.4.	Установка лицензии для ОС Windows .....	34
5.	Графический пользовательский интерфейс приложения .....	35
5.1.	Начало работы с приложением .....	35
5.2.	Создание электронной подписи .....	36
5.3.	Создание подписи со штампом времени (TSP) .....	41
5.4.	Создание усовершенствованной подписи .....	44
5.5.	Подпись сертификатом DSS.....	48
5.6.	Проверка электронной подписи .....	51
5.7.	Снятие электронной подписи .....	54
5.8.	Добавление подписи .....	56
5.9.	Шифрование файлов.....	57
5.10.	Расшифрование файлов .....	62
5.11.	Управление списком файлов для выполнения операций .....	64
5.12.	Документы .....	67
5.13.	Сертификаты .....	72
5.13.1.	Импорт сертификата из файла .....	74
5.13.2.	Импорт сертификата из DSS.....	78
5.13.3.	Экспорт сертификата в файл.....	80
5.13.4.	Удаление сертификата .....	82
5.13.5.	Создание запроса на сертификат .....	83
5.13.6.	Создание самоподписанного сертификата .....	87
5.13.7.	Получить сертификат через сервис УЦ .....	89
5.13.8.	Списки отзыва сертификатов (COC) .....	96
5.13.9.	Установка сертификата из ключевого контейнера .....	99
5.13.10.	Поиск сертификата .....	101
5.14.	Контакты .....	102
5.15.	О программе .....	106
5.15.1.	О программе .....	107
5.15.2.	Журнал операций .....	108
5.15.3.	Справка.....	112
6.	Диагностика неполадок при запуске приложения .....	112
6.1.	Отсутствует СКЗИ КриптоПро CSP.....	112
6.2.	Отсутствует лицензия на КриптоАРМ ГОСТ.....	112
6.3.	Отсутствует лицензия на КриптоПро CSP .....	113
6.4.	Не обнаружены сертификаты с привязкой к ключевому контейнеру .....	114
6.5.	Не загружен модуль Trusted Crypto.....	116



7.	Включение режима логирования и консоль управления.....	117
7.1.	Отслеживание ошибок на платформе MS Windows.....	117
7.2.	Отслеживание ошибок на платформе Linux .....	119
7.3.	Отслеживание ошибок на платформе OS X .....	120
8.	Управление сертификатами и ключами с помощью командной строки.....	122
8.1.	Перенос контейнера закрытого ключа под требуемую операционную систему .....	122
8.2.	Установка сертификата с токена с сохранением привязки к закрытому ключу .....	124
8.3.	Установка доверенных конечных, промежуточных сертификатов и списка отзыва сертификата.....	129
9.	Часто встречающиеся проблемы.....	130
9.1.	Не загружен модуль trusted-crypto. ОС Windows .....	130
9.2.	Не запускается приложение на Ubuntu 18.04, или другой deb системе (Astra Linux) .....	130
9.3.	Не запускается КриптоАРМ ГОСТ на Windows. ....	130
9.4.	Не запускается КриптоАРМ ГОСТ на Windows. ....	130
9.5.	Не устанавливается лицензия на Windows .....	130
9.6.	Если раньше работало и перестало. ....	130
9.7.	КриптоАРМ ГОСТ 2.0, если на unix системах не работает с КриптоПро 4.....	131
9.8.	Не создается запрос на сертификат на линукс при КриптоПро CSP 4.....	131
	Команда разработки и сопровождения продукта .....	132
	Контактная информация .....	134



## 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<sup>1</sup>.

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.

### 1.1.1. Функциональность версии 2.2.0

Приложение текущей версии рассчитано на выполнение операций:

Электронная подпись	<ul style="list-style-type: none"><li>– электронная подпись произвольных файлов на поддерживаемых платформах;</li><li>– добавление электронной подписи к уже существующим (функция создания соподписи);</li><li>– создание как присоединенной, так и отдельной электронной подписи;</li><li>– поддержка стандарта электронной подписи ГОСТ Р 34.10-2012;</li><li>– создание подписи со штампом времени на подпись и подписываемые данные;</li><li>– создание усовершенствованной подписи.</li></ul>
Шифрование	<ul style="list-style-type: none"><li>– шифрование и расшифрование файлов на поддерживаемых платформах;</li><li>– удаление исходного файла после шифрования;</li><li>– шифрование данных по стандарту PKCS#7/CMS.</li></ul>
Управление сертификатами и ключами	<ul style="list-style-type: none"><li>– отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых криптопровайдеров;</li><li>– проверка корректности выбранного сертификата с построением цепочки доверия и скачиванием актуального списка отзыва;</li><li>– хранение закрытых ключей на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.) при условии использования криптопровайдера КриптоПро CSP;</li></ul>

<sup>1</sup> 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.





---

	<ul style="list-style-type: none"><li>– создание запросов на сертификат;</li><li>– импорт сертификатов с привязкой к закрытому ключу;</li><li>– экспорт сертификатов;</li><li>– удаление сертификатов;</li><li>– импорт сертификатов из DSS.</li></ul>
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

---

### 1.1.2. ПОДДЕРЖИВАЕМЫЕ КРИПТОПРОВАЙДЕРЫ

В приложении осуществляется поддержка криптопровайдера КриптоПро CSP версии 4.0 и выше.

### 1.1.3. 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](#).

### 1.1.4. 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.msi** (где x.x.x – номер версии) для 64-разрядной ОС;

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

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

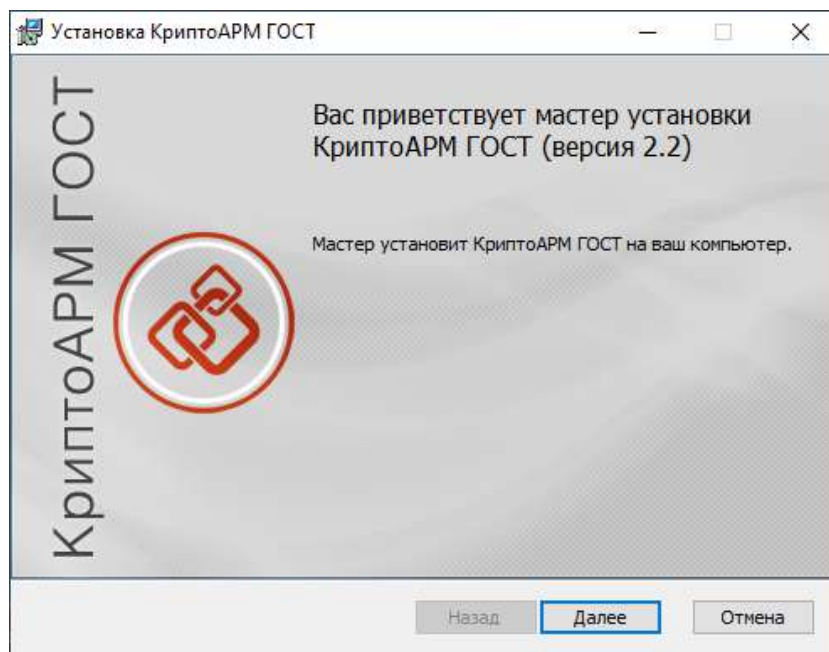


Рис.1.1.1. Начальный шаг мастера установки приложения

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**.

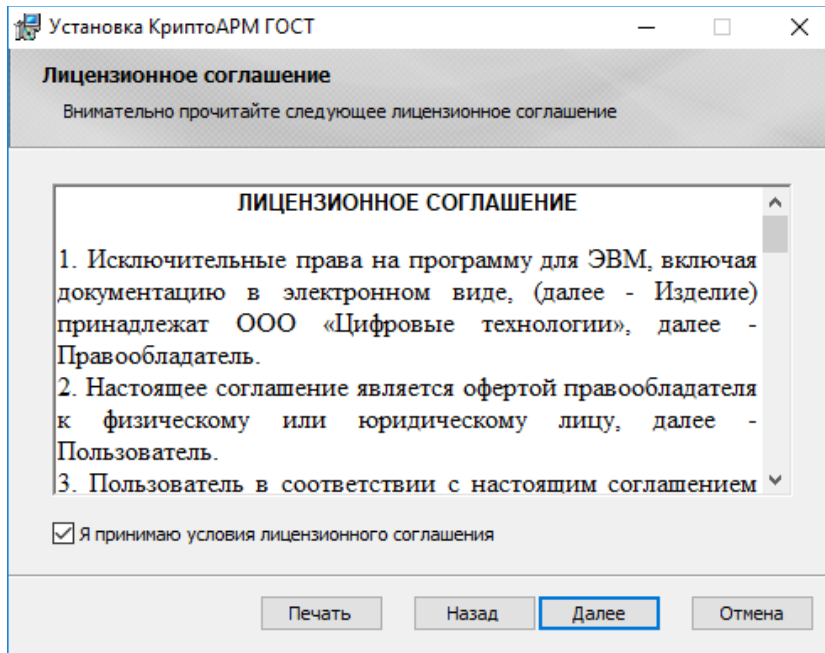


Рис.1.1.2. Условия лицензионного соглашения

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).

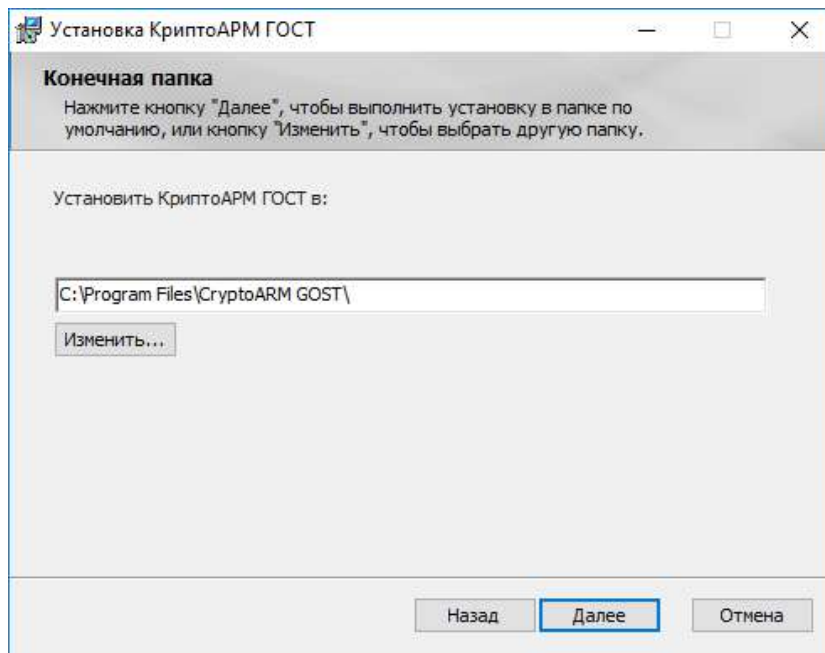


Рис.1.1.3. Выбор каталога установки приложения

На шаге выборочной установки можно отключить создание ярлыка на рабочем столе и установку модулей для создания усовершенствованной подписи (рис. 1.1.4).

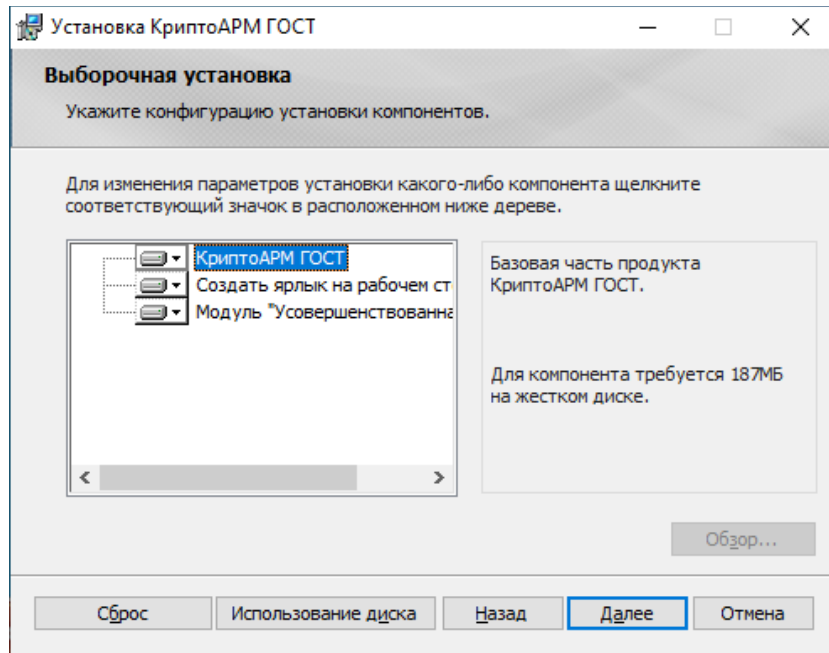


Рис.1.1.4. Выбор компонент для установки

На заключительном шаге мастера нажмите кнопку **Установить** (рис.1.1.5). Установка выполняется с правами администратора.

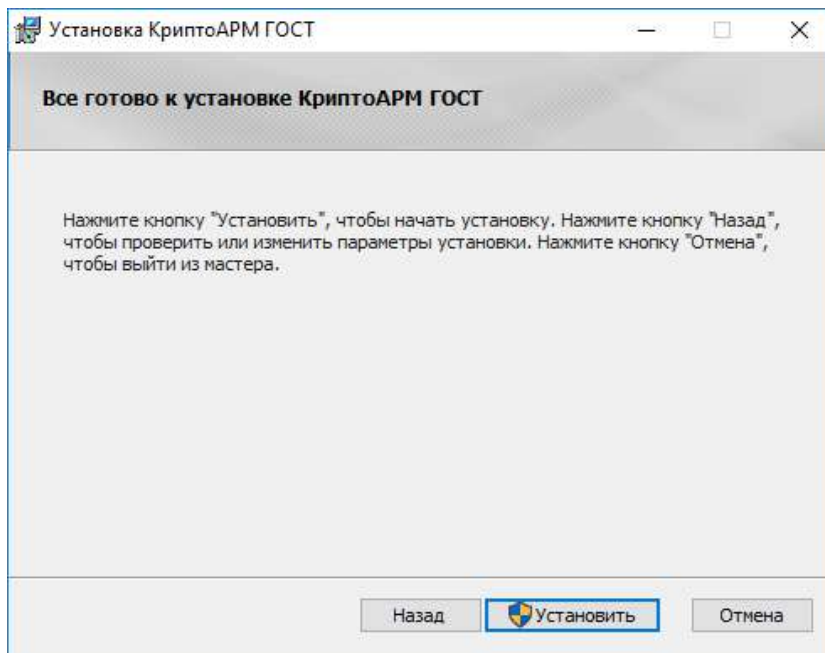


Рис.1.1.5. Выбор каталога установки приложения

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-x64.deb** (где `x.x.x` – номер версии) для 64-разрядных ОС, основанных на DEB.

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

- 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-x64.deb** - для ОС, основанных на Debian (Debian/Ubuntu);

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

После установки приложения в меню появится ярлык КриптоАРМ ГОСТ.

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

### 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).

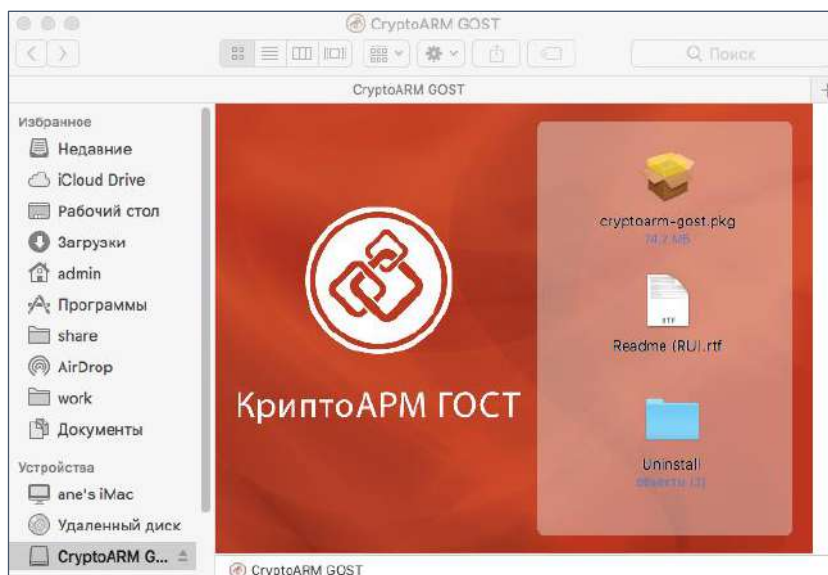


Рис.1.3.1. Состав образа диска

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

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

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

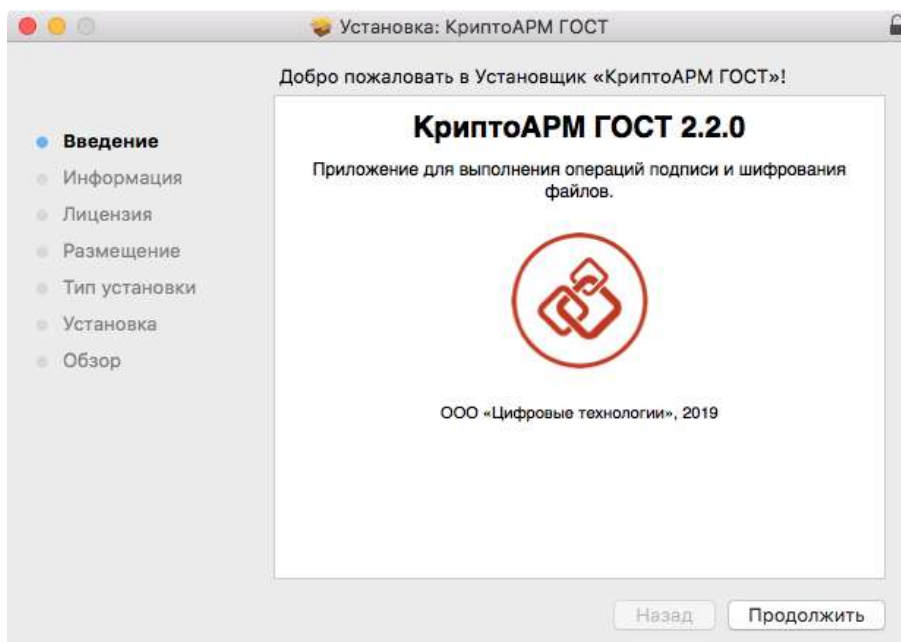


Рис.1.3.2. Начальный шаг мастера установки пакета приложения

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

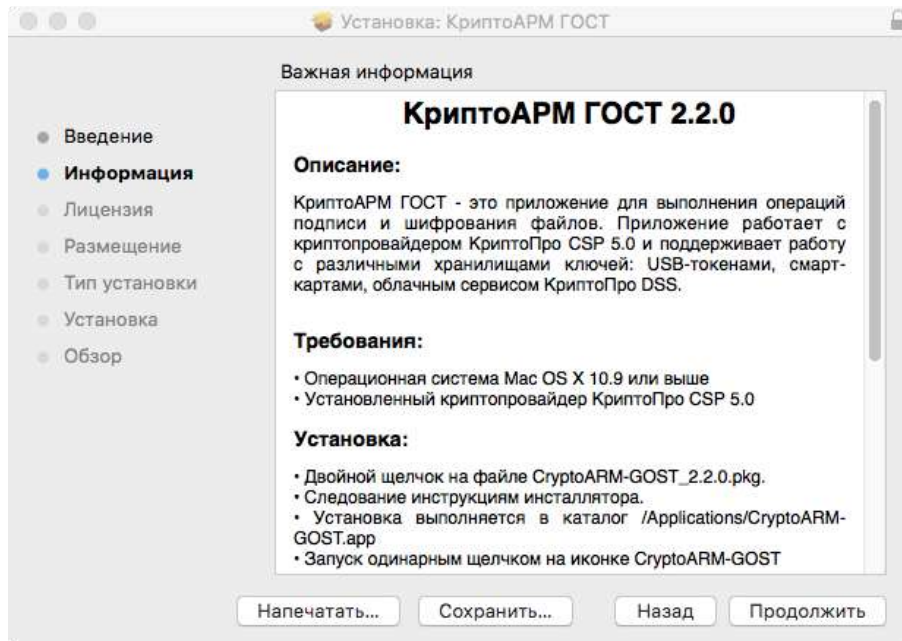


Рис.1.3.3. Просмотр информации о программном продукте

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

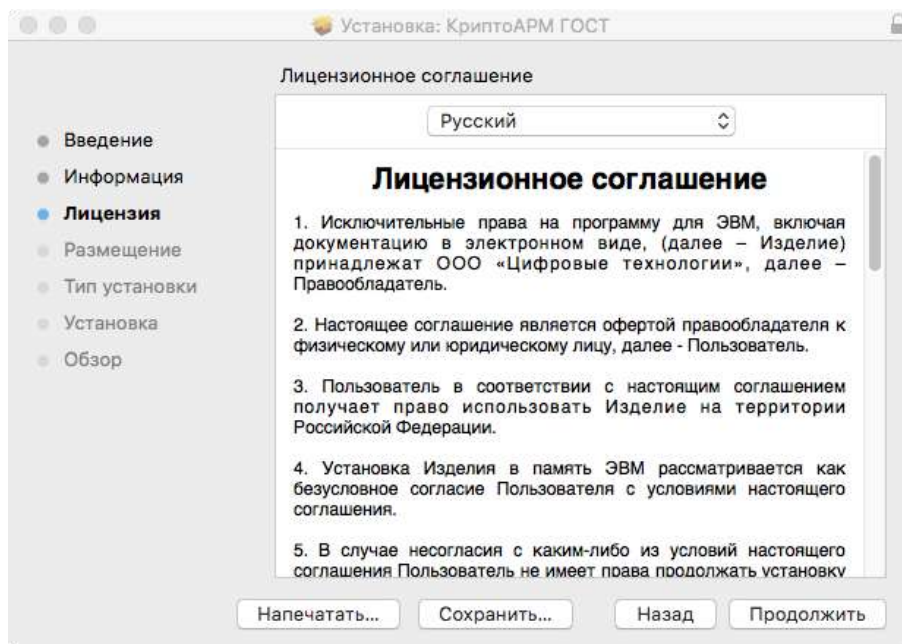


Рис.1.3.4. Просмотр информации о лицензии

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



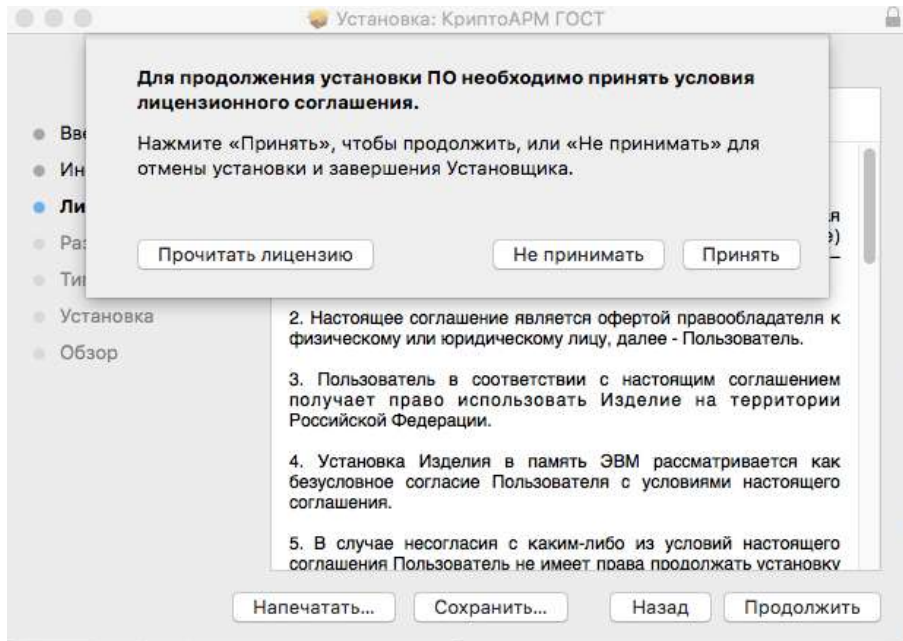


Рис.1.3.5. Соглашение с условиями лицензии

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

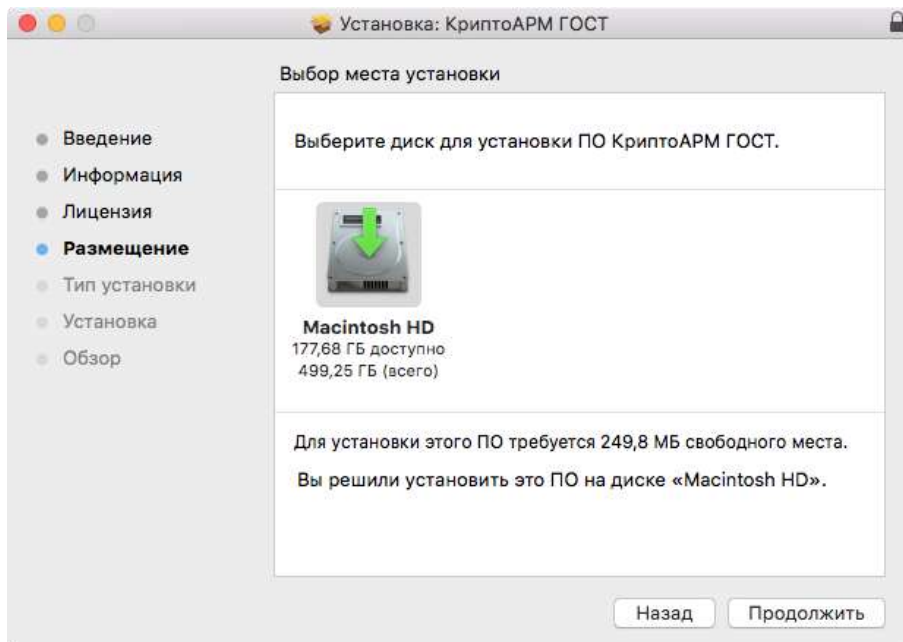


Рис.1.3.6. Информация о размещении приложения на жестком диске

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

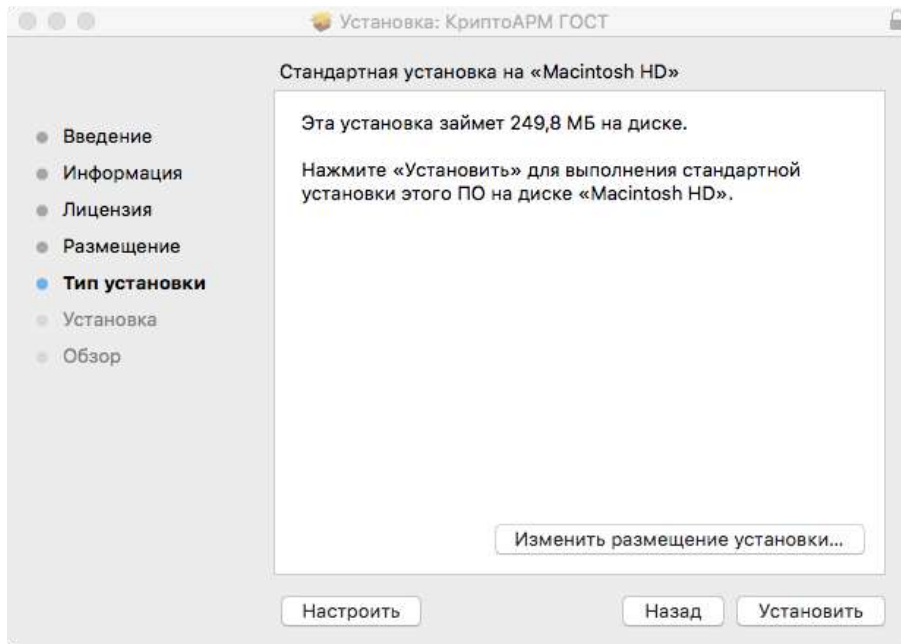


Рис.1.3.7. Подтверждение установки на физический носитель

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

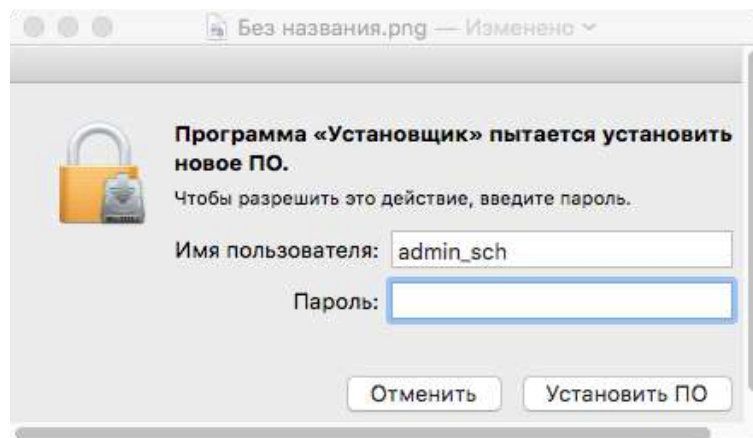


Рис.1.3.8. Информация о размещении приложения на жестком диске

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

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.

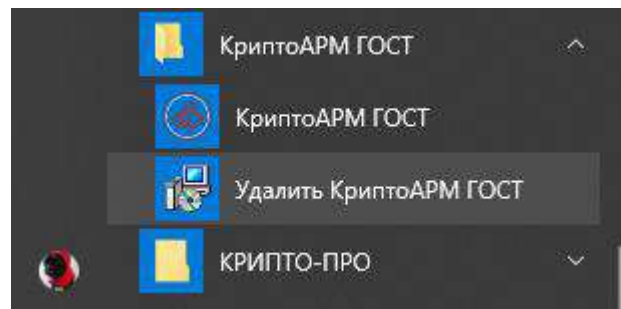


## 2. Удаление программного продукта

### 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) используется скрипт **full\_uninstall\_cryptoarm\_gost**. Затем нужно ввести пароль администратора.

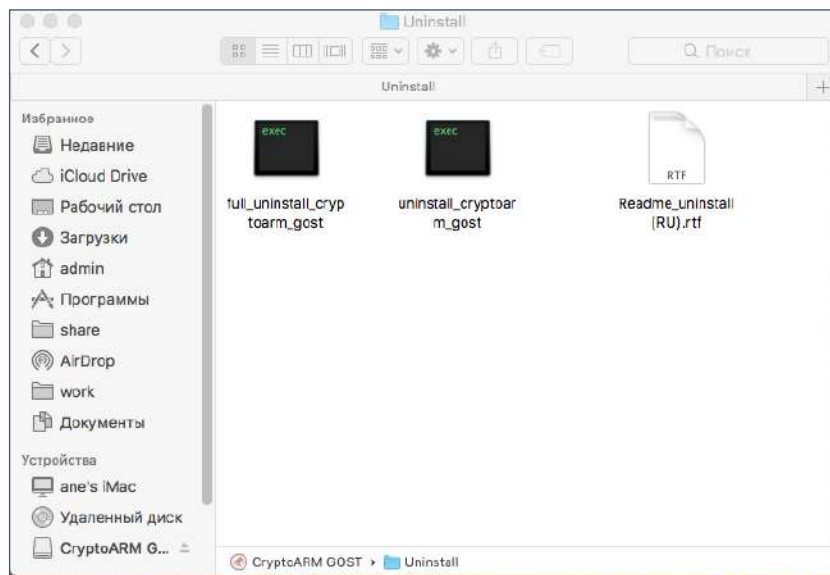


Рис.2.3.1. Каталог скриптов удаления приложения

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 **Лицензии** через пункт **О программе** главного 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 с указанием файла лицензии.

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

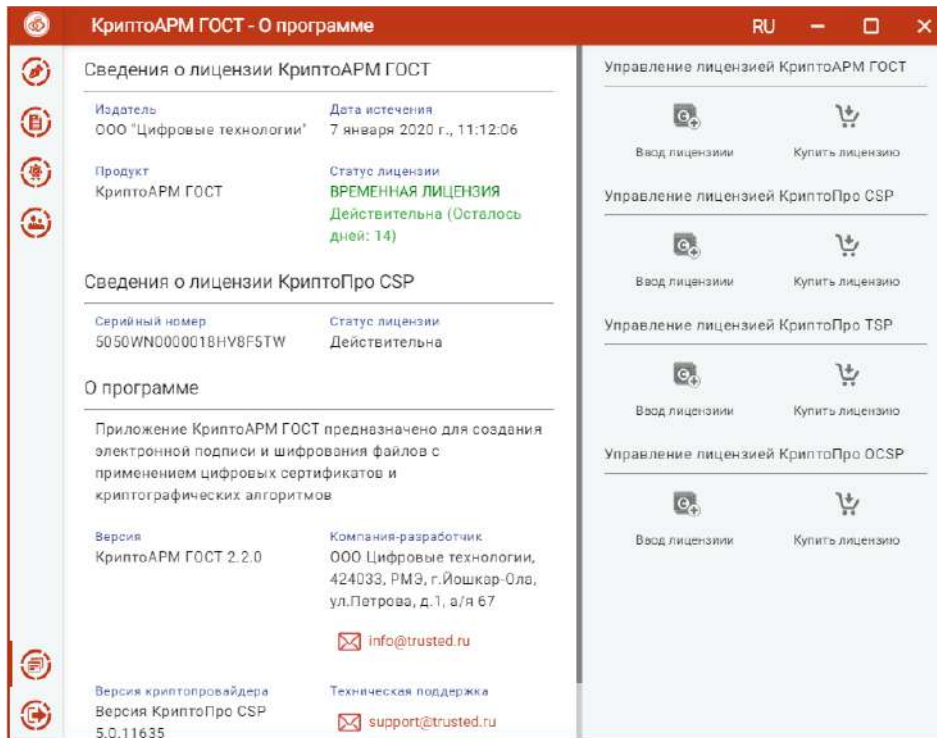


Рис. 3.1.1 Страница ввода лицензионного ключа на программный продукт

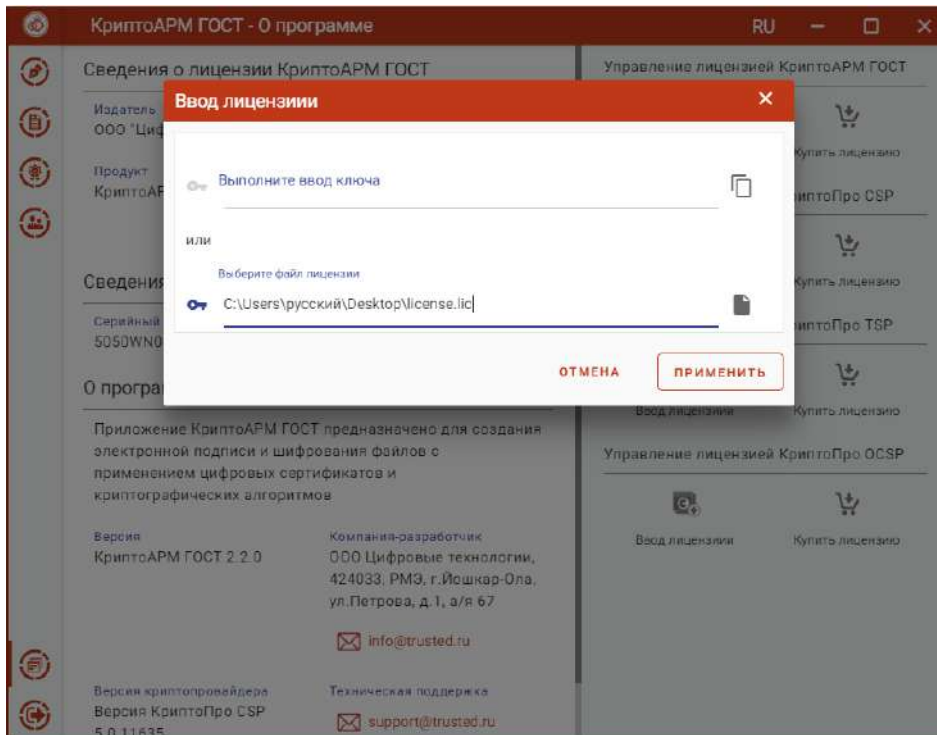


Рис. 3.1.2 Диалоговое окно с выбором варианта ввода лицензионного ключа

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

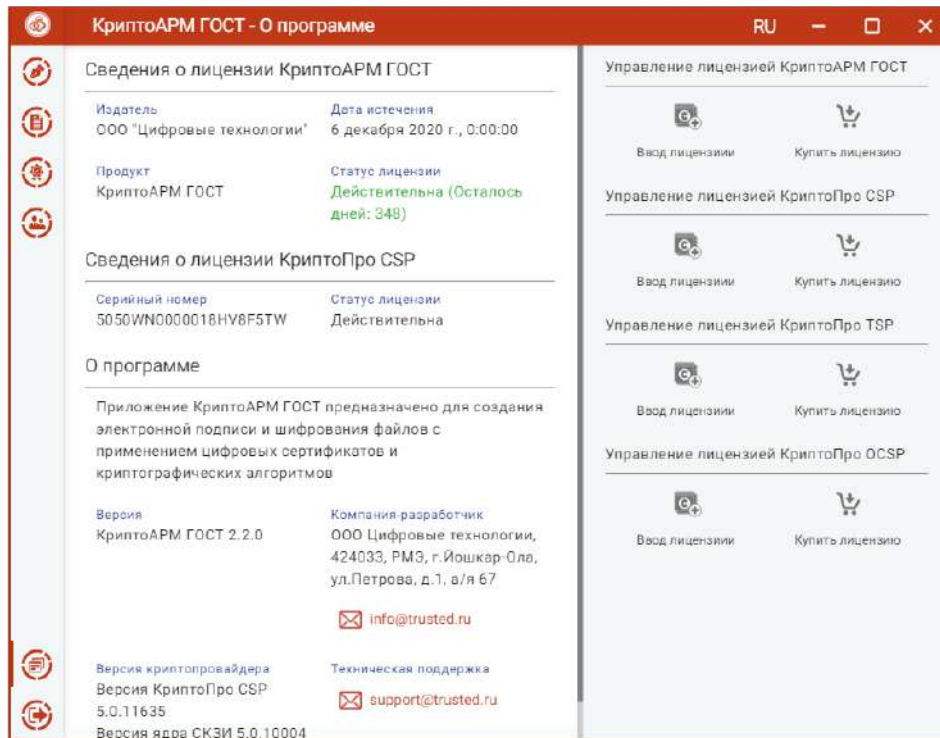


Рис. 3.1.3 Сведения о лицензии

### 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 копирования файла лицензии license.lic в каталог установки:

- Под платформой Windows – каталог  
C:\Users\<имя пользователя>\AppData\Local\Trusted\CryptoARM GOST.
- Под платформой Linux и MacOS – 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 работы приложения КриптоАРМ ГОСТ 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/](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.

#### 4.2.1. УСТАНОВКА БАЗОВЫХ ПАКЕТОВ СКРИПТОМ

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

#### 4.2.2. УСТАНОВКА ПАКЕТОВ

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-cproccsp-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-cproccsp-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
```

#### 4.2.3. УСТАНОВКА ПАКЕТА ДЛЯ МОДУЛЕЙ TSP И OCSP

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

1. Скачать архив **Linux 64 бита** по ссылке <https://www.cryptopro.ru/products/pki/tsp/sdk/downloads> (требуется предварительная регистрация).
2. Распаковать архив.
3. Установить пакет:

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

```
sudo rpm -i cprocsp-pki-x.x.x-amd64-cades.rpm – для RPM ОС
```

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

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

#### 4.2.4. УСТАНОВКА ПАКЕТА ДЛЯ ГРАФИЧЕСКОГО ИНТЕРФЕЙСА ВВОДА ПАРОЛЯ

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

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

#### 4.2.5. УСТАНОВКА ПАКЕТОВ ДЛЯ РАБОТЫ С КЛЮЧЕВЫМИ НОСИТЕЛЯМИ

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

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

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

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

Для ключевого носителя Рутокен:



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

Для ключевого носителя JaCarta:

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

#### 4.2.6. УСТАНОВКА ПАКЕТОВ ДЛЯ РАБОТЫ С «ОБЛАЧНЫМИ» СЕРТИФИКАТАМИ

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

```
sudo dpkg -i ./cprocsp-cptools-gtk- <...>.deb  
sudo dpkg -i ./cprocsp-rdr-cloud-<...>.deb  
sudo dpkg -i ./cprocsp-rdr-cloud-gtk-<...>.deb
```

**Примечание.** Директория расположения утилит КриптоПро CSP /opt/cprocsp/bin/<arch>/, где под <arch> подразумевается 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>.

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

1. Скачать архив **Apple** **MacOS** по ссылке <https://www.cryptopro.ru/products/pki/tsp/sdk/downloads> (требуется предварительная регистрация).
2. Распаковать архив.
3. Установить пакет cprocsp-rki-x.x.x.mpkg, следуя инструкциям на каждом шагу установщика.

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

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

#### 4.4. УСТАНОВКА ЛИЦЕНЗИИ НА ПРОГРАММНЫЙ ПРОДУКТ КРИПТОПРО CSP

Установка программного обеспечения «КриптоПро CSP» без ввода лицензии подразумевает использование временной лицензии с ограниченным сроком действия. Для использования КриптоПро CSP после окончания этого срока пользователь должен ввести серийный номер с бланка лицензии, полученной у организации-разработчика или организации, имеющей права распространения продукта (дилера).



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

#### 4.4.1. УСТАНОВКА ЛИЦЕНЗИИ ЧЕРЕЗ ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС.

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного 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.

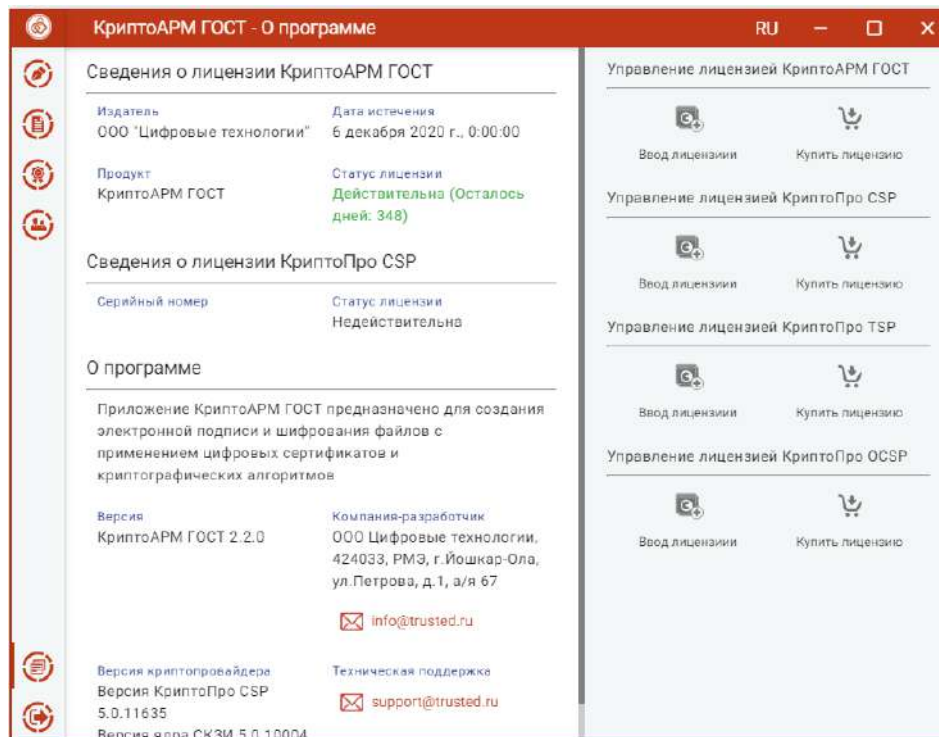




Рис.4.4.1. Страница ввода лицензионного ключа на КриптоПРО CSP

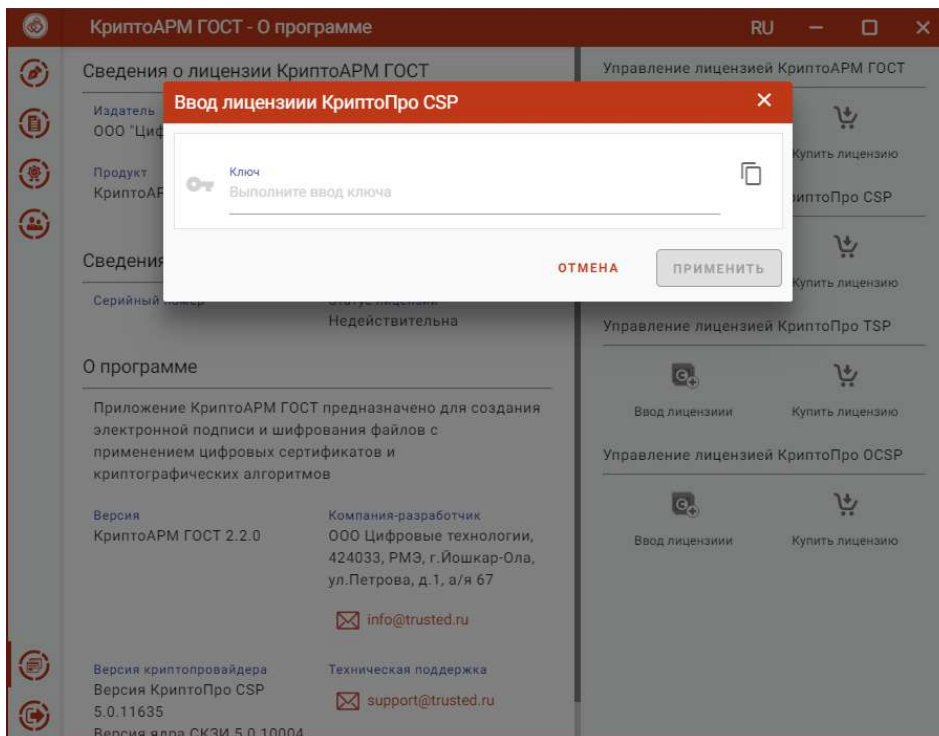
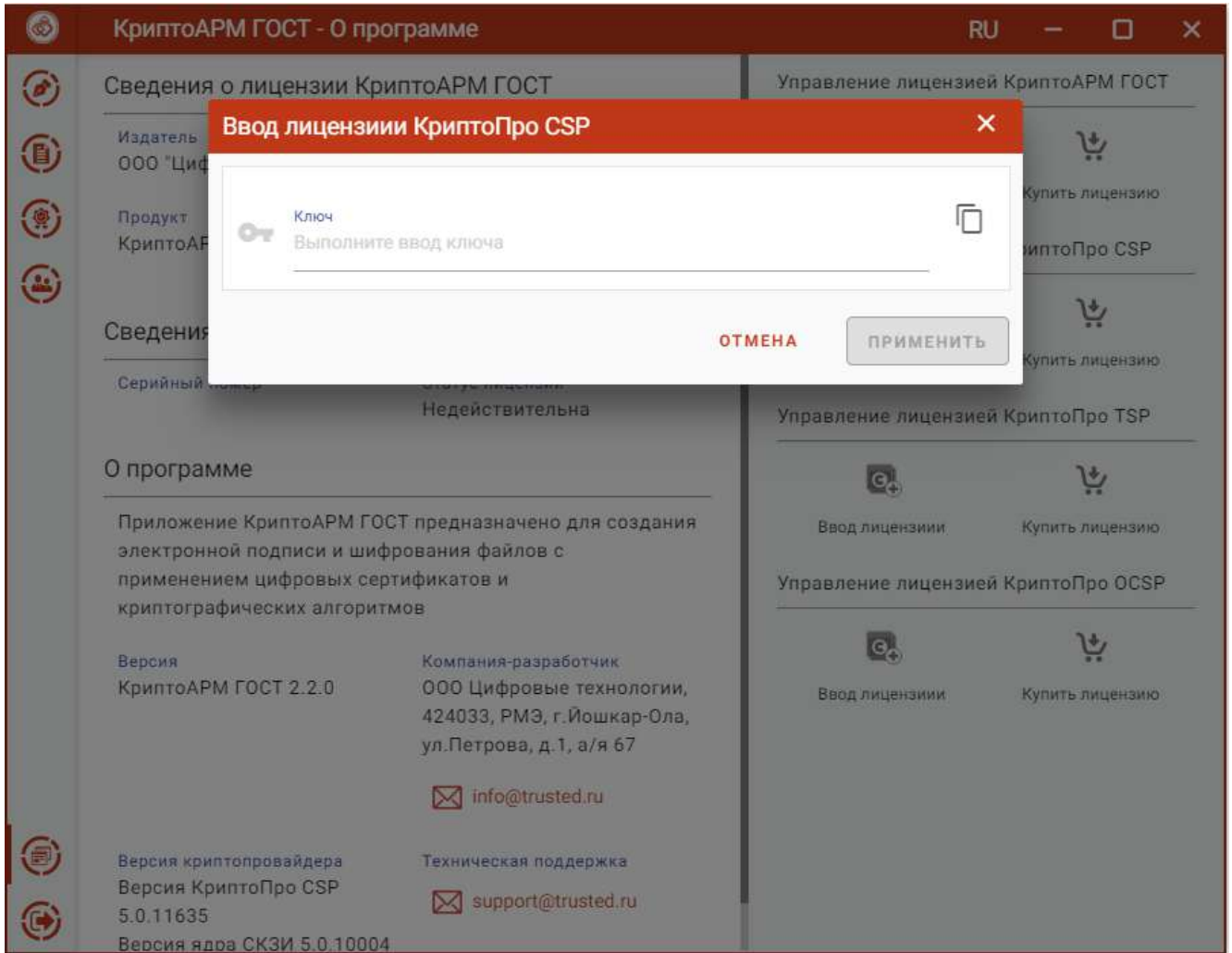


Рис. 4.4.2. Диалоговое окно ввода лицензионного ключа



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

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

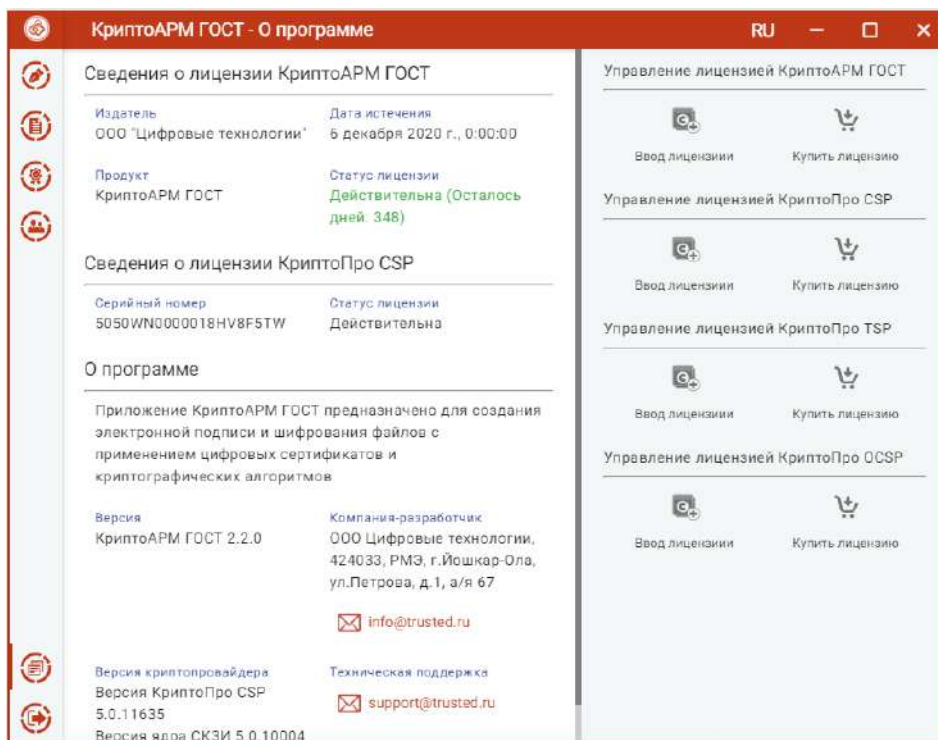


Рис. 4.4.3 Сведения о лицензии

#### 4.4.2. Установка лицензии через командную строку для ОС Linux и MacOS

Установка лицензии на КристоПро 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
```

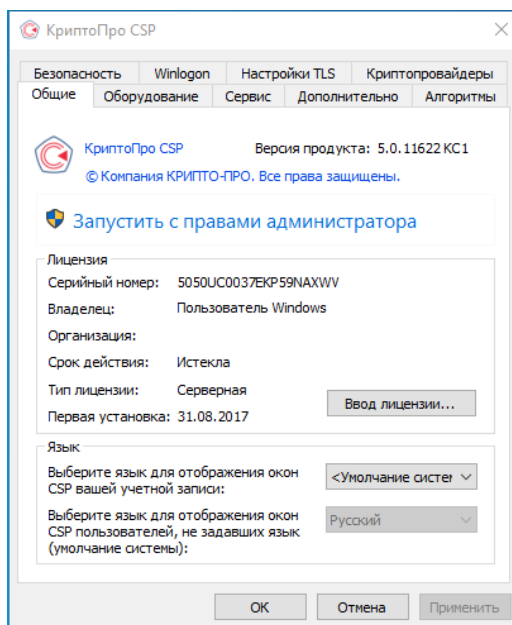
Ввод лицензии производится командой (серийный номер следует вводить с соблюдением регистра символов):

```
# cpconfig -license -set <серийный_номер>
```

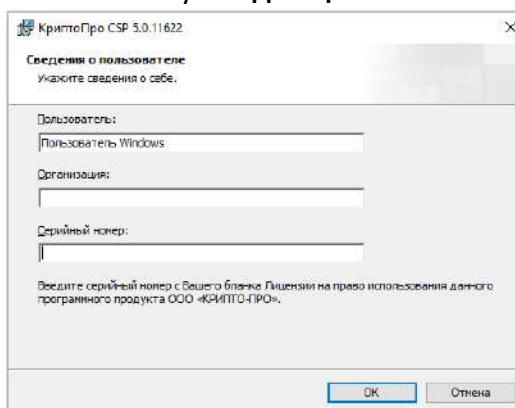
#### 4.4.3. Установка лицензии через программный интерфейс КристоПро CSP для ОС Windows

Для установки лицензии на КристоПро CSP потребуются права администратора.

- Откройте в главном меню **Пуск, Все программы, КРИПТО-ПРО, КристоПро CSP**.



- В открывшемся окне нажмите кнопку **Ввод лицензии**.



- В поле **Серийный номер** введите лицензионный ключ и нажмите **ОК**.

#### 4.5. Установка лицензии на модуль TSP

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

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

##### 4.5.1. Установка лицензии через пользовательский интерфейс.

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения. На открывшейся странице, которая представлена на рис.4.5.1 нажать на кнопку **Установить лицензию** в разделе управления лицензией модуля штампов времени (TSP).

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



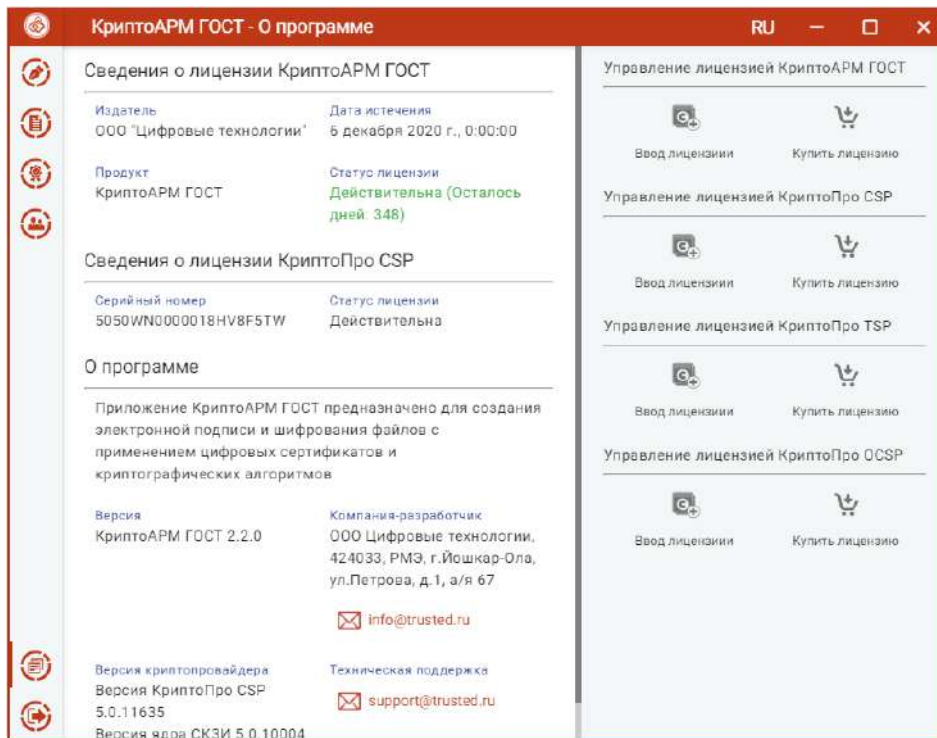


Рис.4.5.1. Страница ввода лицензионного ключа на модуль TSP

В результате должно появиться всплывающее окно ввода лицензии копированием содержимого файла лицензии в текстовое поле (рис. 4.5.2).

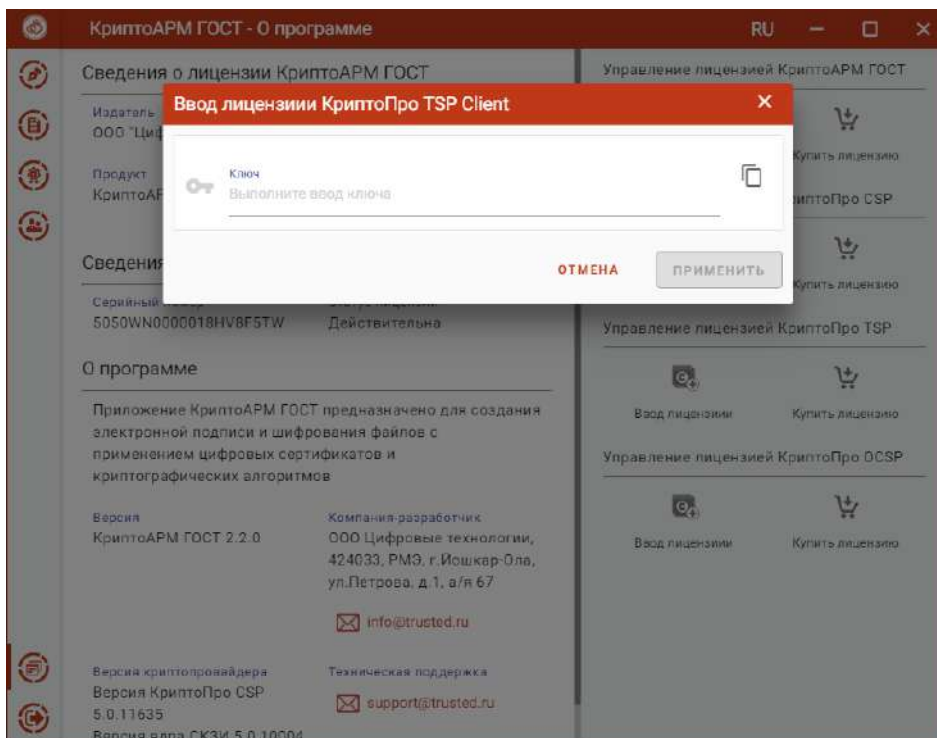


Рис.4.5.2. Окно ввода лицензионного ключа на модуль TSP

При успешной операции должно появиться информационное сообщение.



#### 4.5.2. УСТАНОВКА ЛИЦЕНЗИИ ЧЕРЕЗ КОМАНДНУЮ СТРОКУ ДЛЯ ОС MACOS

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

Просмотр информации о лицензии осуществляется командой:

```
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license
```

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

```
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license -s <серийный_номер>
```

#### 4.5.3. УСТАНОВКА ЛИЦЕНЗИИ ЧЕРЕЗ КОМАНДНУЮ СТРОКУ ДЛЯ ОС LINUX

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

Просмотр информации о лицензии осуществляется командой:

```
/opt/cproscsp/bin/amd64/tsputil license
```

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

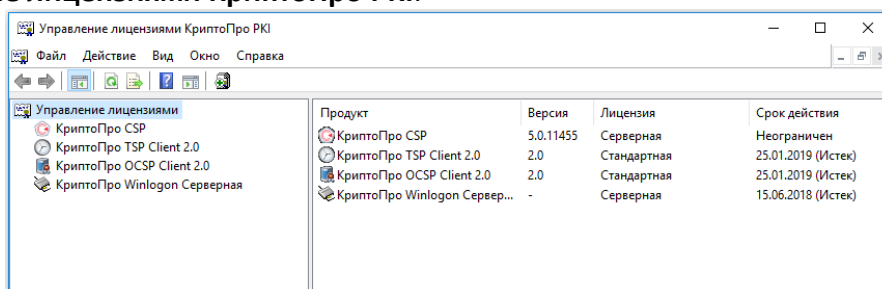
```
/opt/cproscsp/bin/amd64/tsputil license -s <серийный_номер>
```

#### 4.5.4. УСТАНОВКА ЛИЦЕНЗИИ ДЛЯ ОС WINDOWS

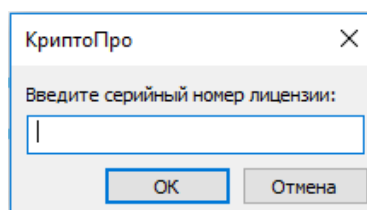
Для установки лицензии на модуль TSP требуются права администратора.

Для ввода лицензий необходимо выполнить следующее:

1. Запустите КриптоПро PKI. Для этого перейдите в меню **Пуск, Программы, КриптоПро, Управление лицензиями КриптоПро PKI**.



2. Перейдите в раздел «КриптоПро TSP Client 2.0», выберите пункт **Действия, Все задачи, Ввести серийный номер**.



3. В открывшемся окне введите серийный номер лицензии и нажмите **ОК**. Если серийный номер введен правильно, то в режиме просмотра информации о лицензиях появится информация о лицензии.



## 4.6. Установка лицензии на модуль OCSP

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

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

### 4.6.1. Установка лицензии через пользовательский интерфейс.

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения. На открывшейся странице, которая представлена на рис.4.6.1 нажать на кнопку **Установить лицензию** в разделе управления лицензией модуля (OCSP).

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

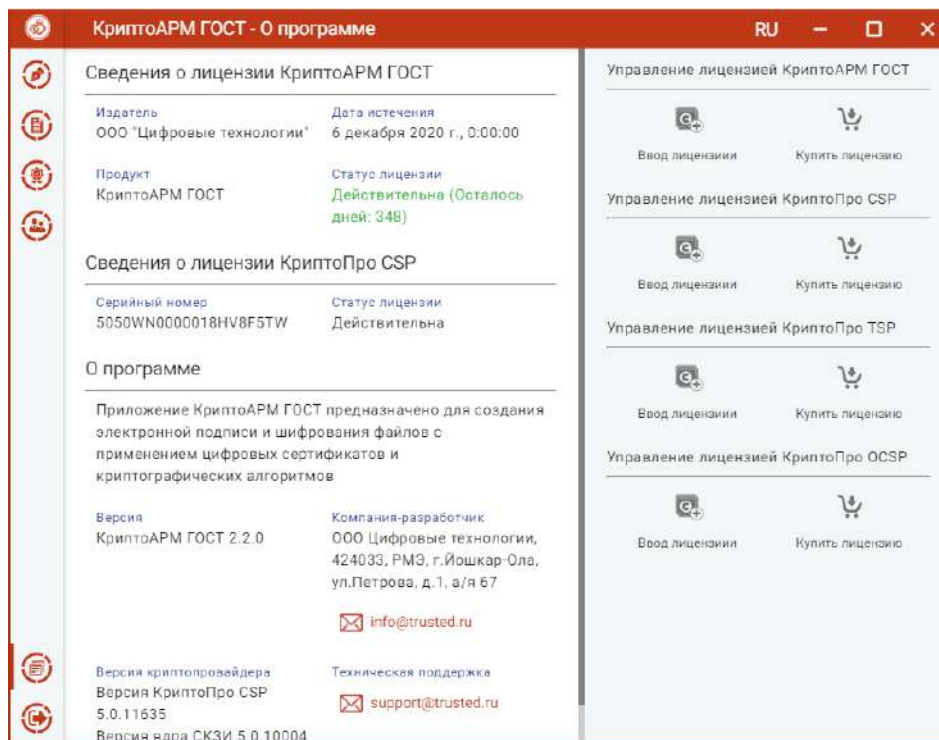


Рис.4.6.1. Страница ввода лицензионного ключа на модуль OCSP

В результате должно появиться всплывающее окно ввода лицензии копированием содержимого файла лицензии в текстовое поле (рис. 4.6.2).

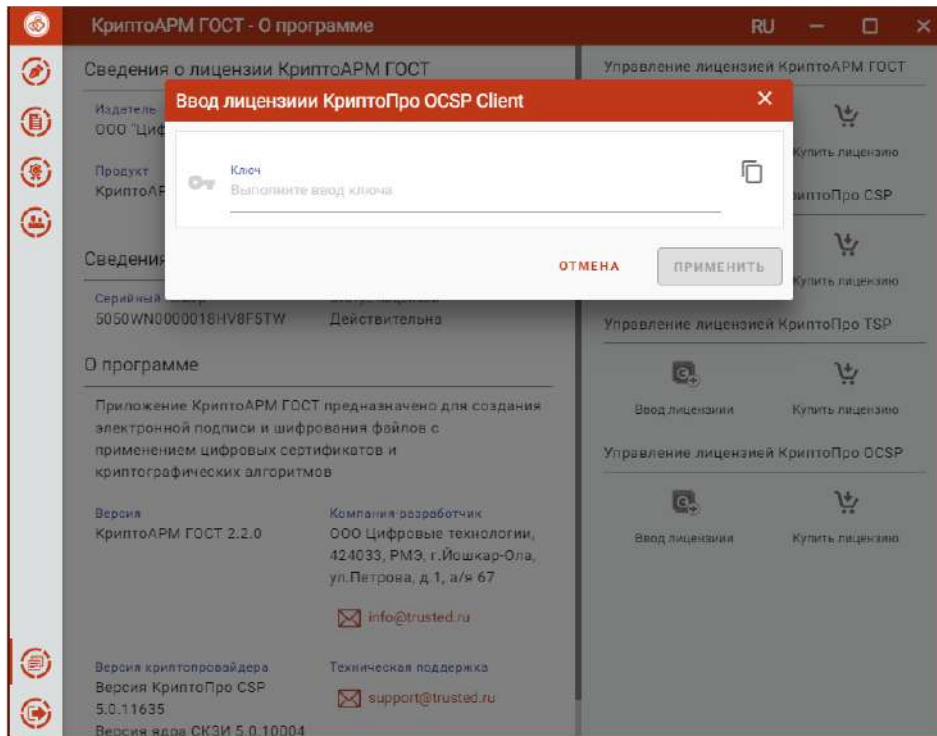


Рис.4.6.2. Окно ввода лицензионного ключа на модуль OSCP

При успешной операции должно появиться информационное сообщение.

#### 4.6.2. Установка лицензии через командную строку для ОС MacOS

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

Просмотр информации о лицензии осуществляется командой:

```
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license
```

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

```
/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license -s <серийный_номер>
```

#### 4.6.3. Установка лицензии через командную строку для ОС Linux

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

Просмотр информации о лицензии осуществляется командой:

```
/opt/cproscsp/bin/amd64/ocsputil license
```

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

```
/opt/cproscsp/bin/amd64/ocsputil license -s <серийный_номер>
```

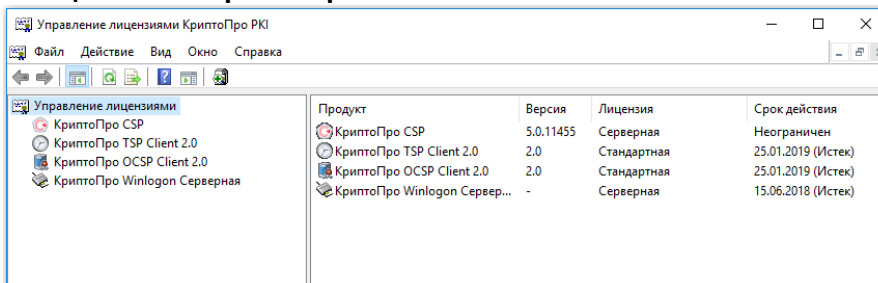


#### 4.6.4. Установка лицензии для ОС WINDOWS

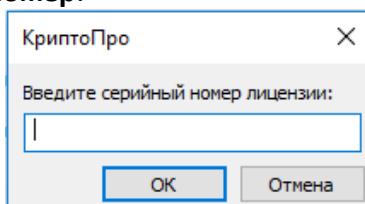
Для установки лицензии на модуль OCSP требуются права администратора.

Для ввода лицензий необходимо выполнить следующее:

1. Запустите КристоПро PKI. Для этого перейдите в меню **Пуск, Программы, КристоПро, Управление лицензиями КристоПро PKI.**



2. Перейдите в раздел «КристоПро OCSP Client 2.0», выберите пункт **Действия, Все задачи, Ввести серийный номер.**



3. В открывшемся окне введите серийный номер лицензии и нажмите **OK**. Если серийный номер введен правильно, то в режиме просмотра информации о лицензиях появится информация о лицензии.



## 5. Графический пользовательский интерфейс приложения

### 5.1. Начало работы с приложением

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

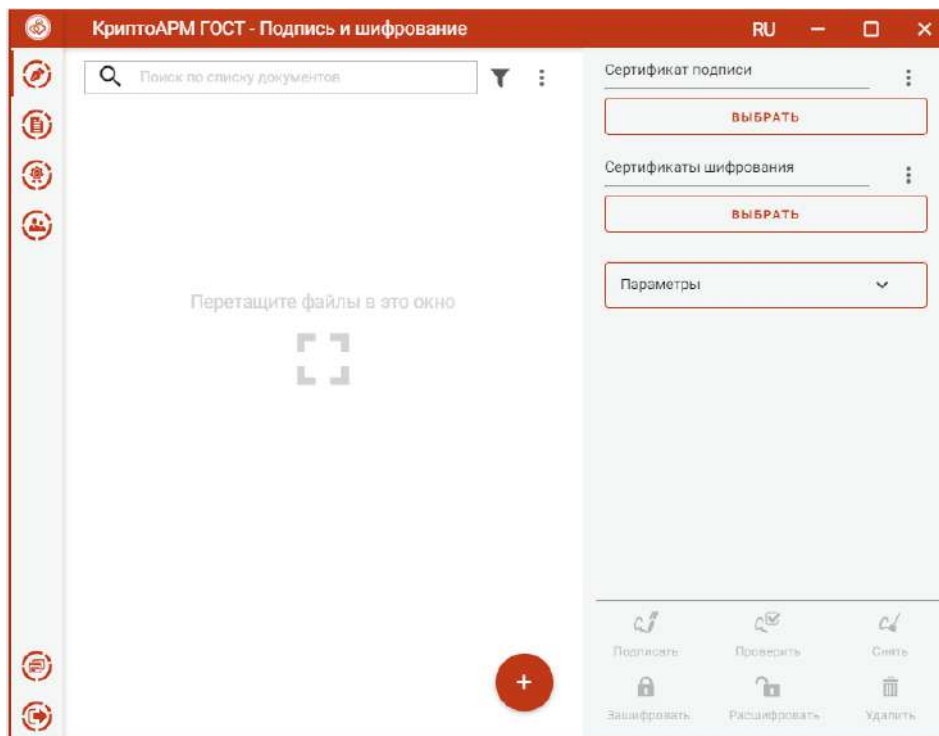


Рис. 5.1.1 Стартовое окно приложения

В левой панели расположены кнопки выбора пунктов меню приложения, через которые можно выполнить переход ко всем представлениям (рис.5.1.2).

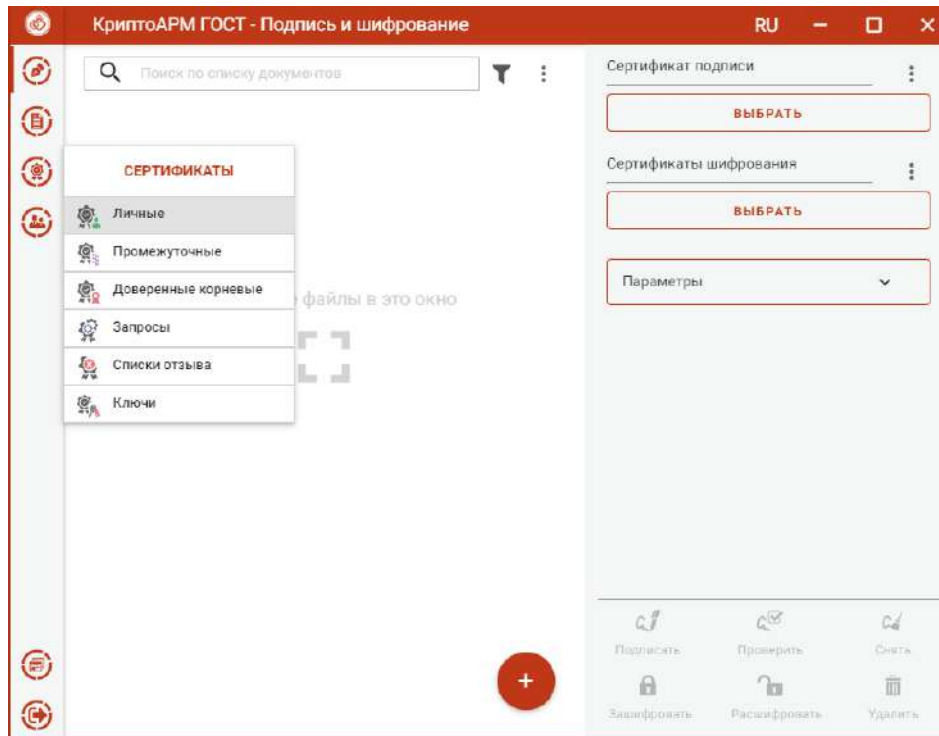


Рис. 5.1.2 Пункт меню Сертификаты с подменю

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 параметры 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 перетаскивая файлы мышкой в область формирования списка файлов для подписи.

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



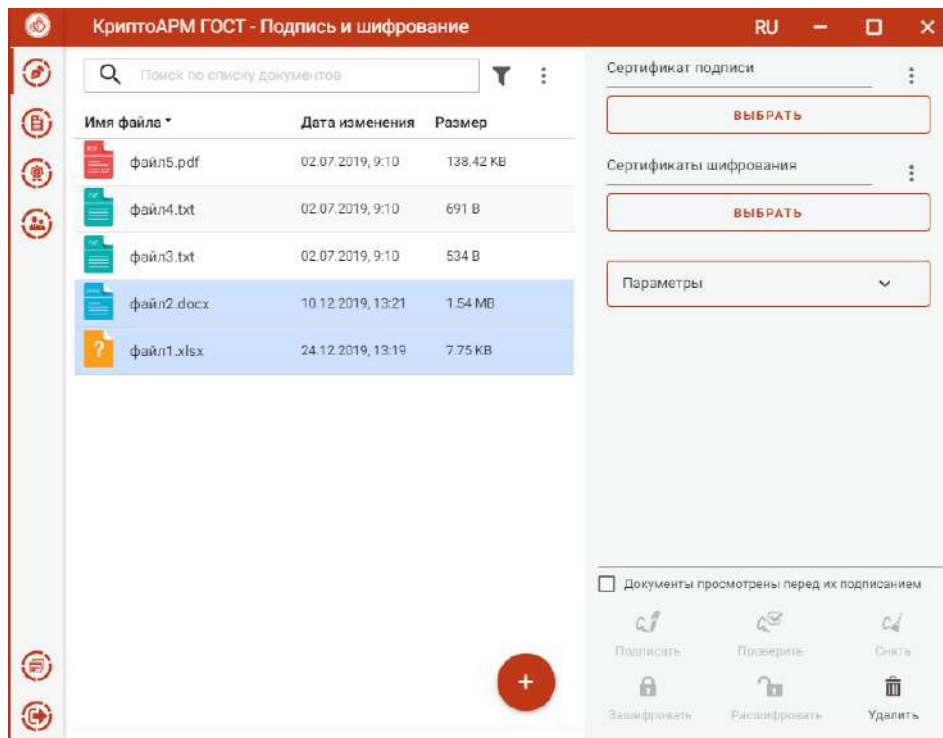


Рис. 5.2.1 Список подписываемых файлов

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

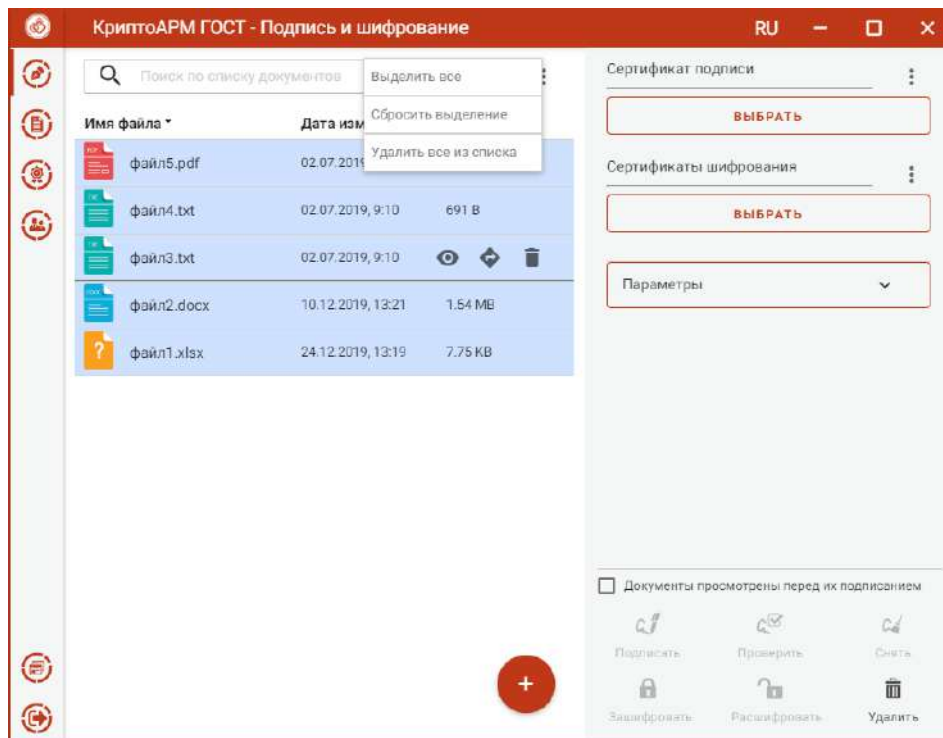


Рис. 5.2.2 Контекстное меню управления списком файлов

**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.5.2.3).

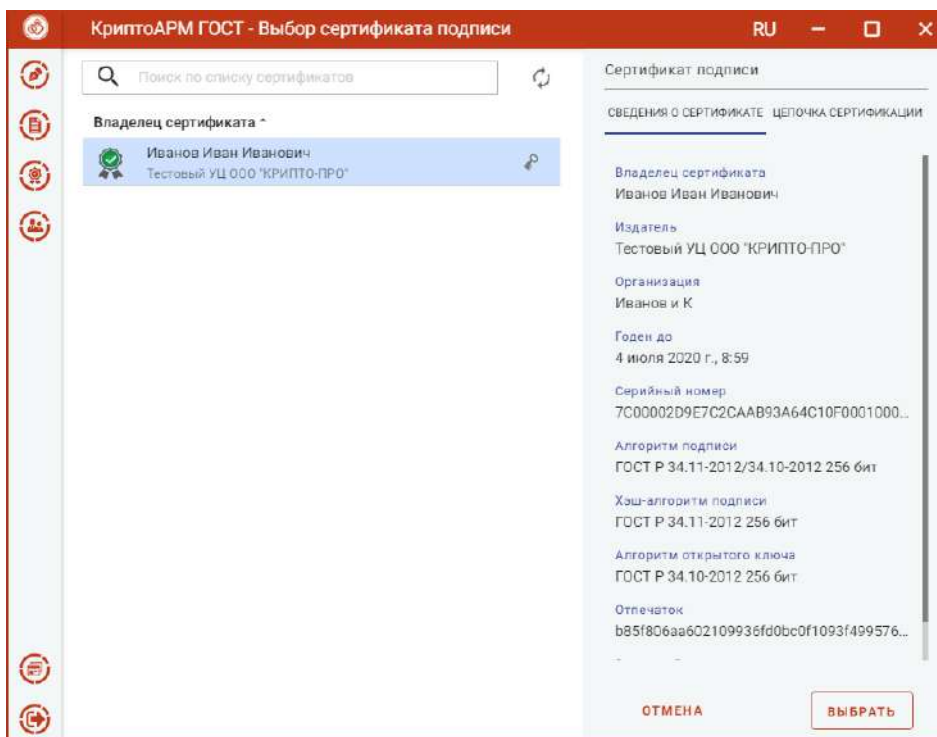


Рис. 5.2.3 Выбор сертификата подписи

Выбор сертификата подписи осуществляется его выделением и нажатием на кнопку **Выбрать**. При следующем запуске приложения данный сертификат будет уже выбран в качестве сертификат подписи.

Сертификат подписи можно изменить с помощью контекстного меню (рис. 5.2.4).

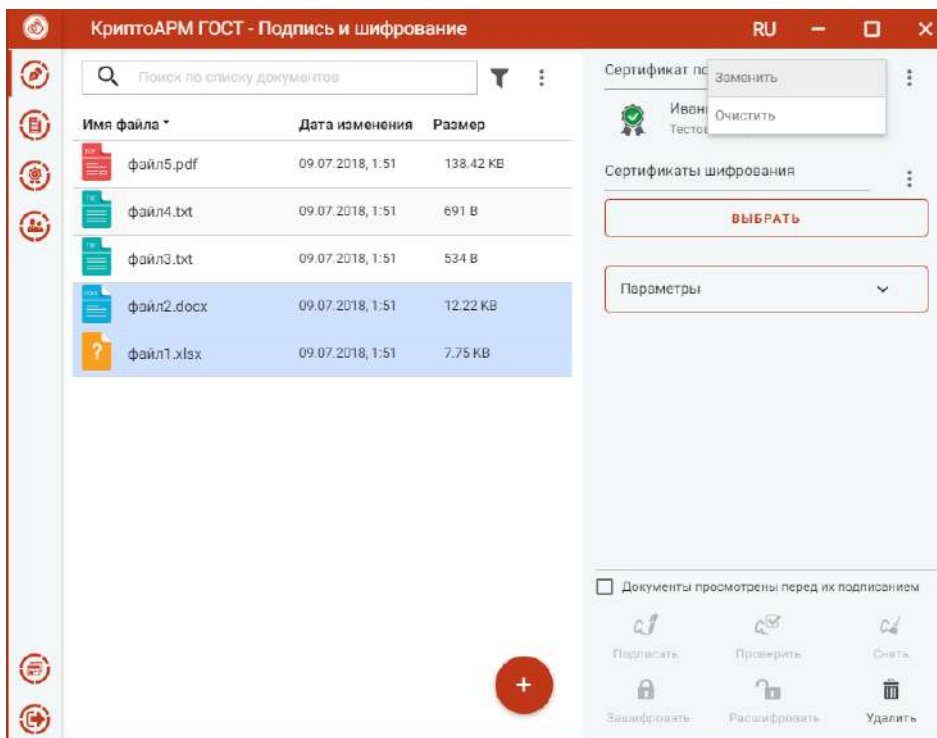


Рис. 5.2.4 Изменение сертификата подписи

Если в хранилище личных сертификатов нет сертификата с закрытым ключом, то можно создать или импортировать сертификат в разделе [Сертификаты](#).



**УСТАНОВКА ПАРАМЕТРОВ ПОДПИСИ.** Параметры подписи задаются в раскрывающемся списке **Параметров** (рис. 5.2.5).

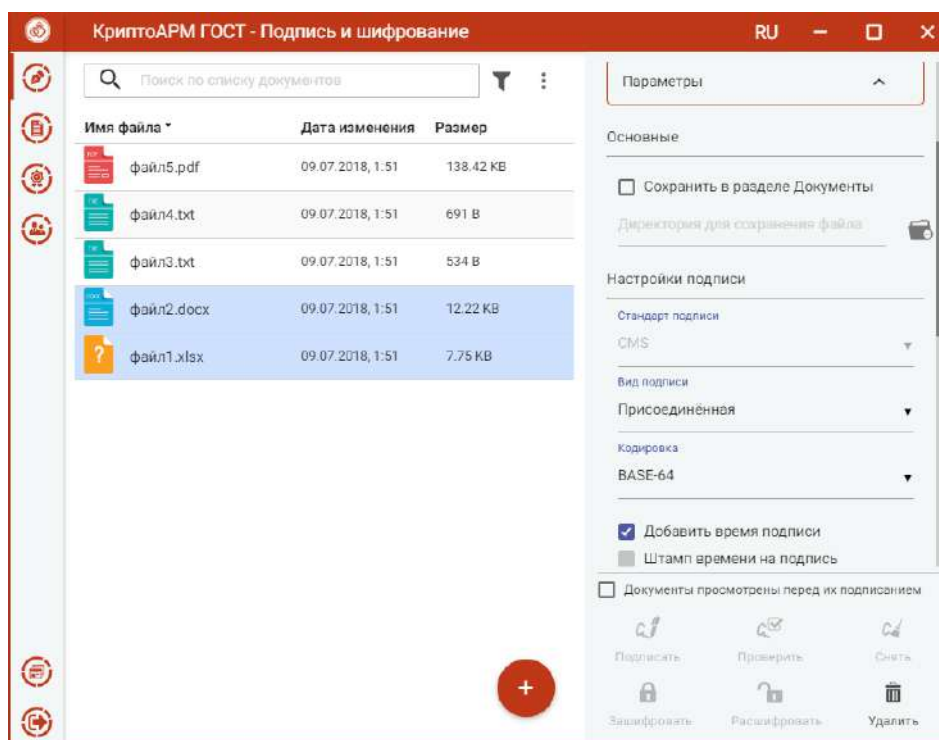


Рис. 5.2.5 Настройка параметров подписи

В параметрах можно настроить:

- **Сохранить в разделе Документы** – при установленном флажке результат операции сохраняется в каталог Documents, расположенный в папке пользователя в каталоге /Trusted/CryptoARM GOST/. Если флаг не установлен и не выбрана директория для сохранения файла, то файл сохраняется рядом с исходным файлом.
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба online статусов OCSP** (подробнее о создании усовершенствованной подписи в пункте «[Создание усовершенствованной подписи](#)»). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client и КриптоПро OCSP Client.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Вид подписи** – присоединённая или отсоединённая.
- **Добавить время подписи** - при установленном флажке в подпись сохраняется время (системное) подписи.
- **Добавлять штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Добавлять штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в

пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client.

**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. 5.2.6).

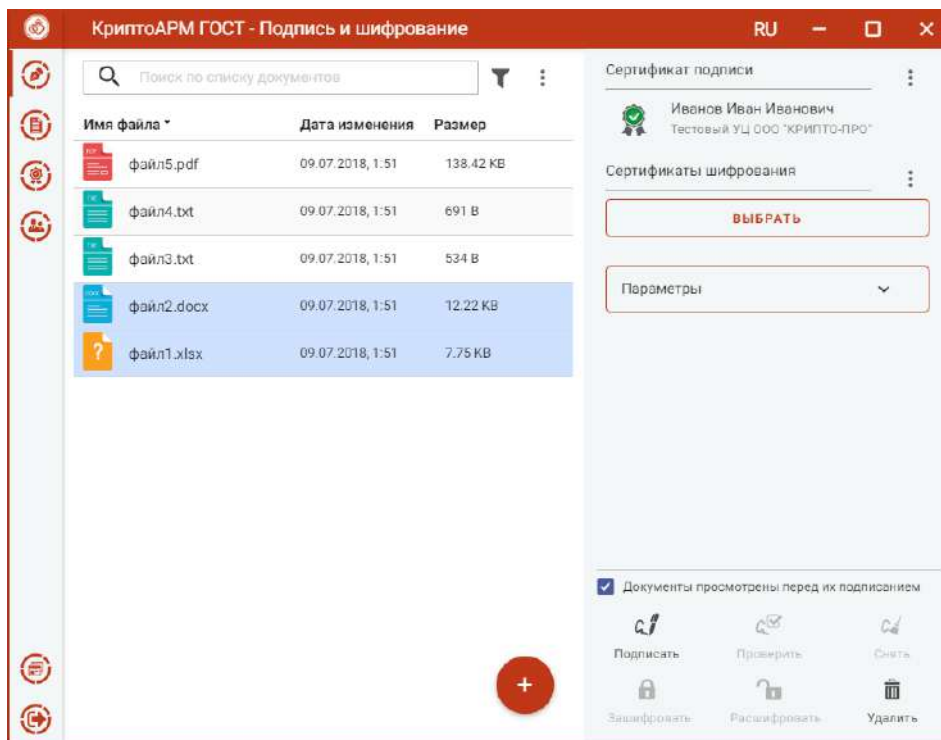


Рис. 5.2.6 Подпись файлов

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. 5.2.7).

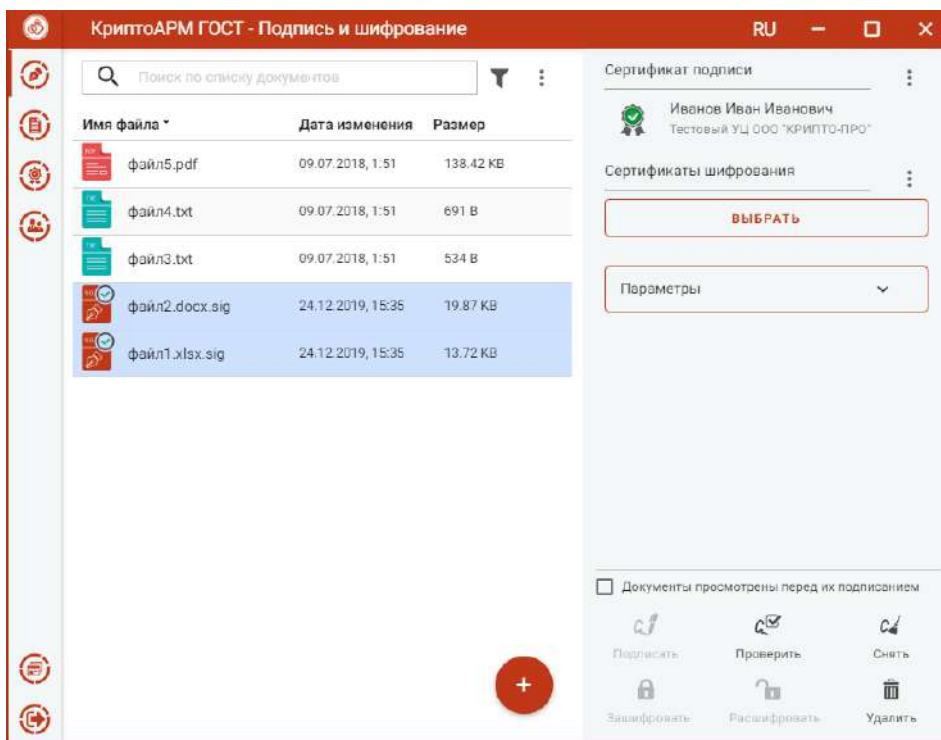


Рис. 5.2.7 Подписанные файлы

### 5.3. Создание подписи со штампом времени (TSP)

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

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

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

- установить флаг **Добавлять штамп времени на подпись**, если требуется поставить штамп на подпись (рис. 5.3.1);
- установить флаг **Добавлять штамп времени на подписываемые данные**, если требуется поставить штамп на данные (рис. 5.3.1);

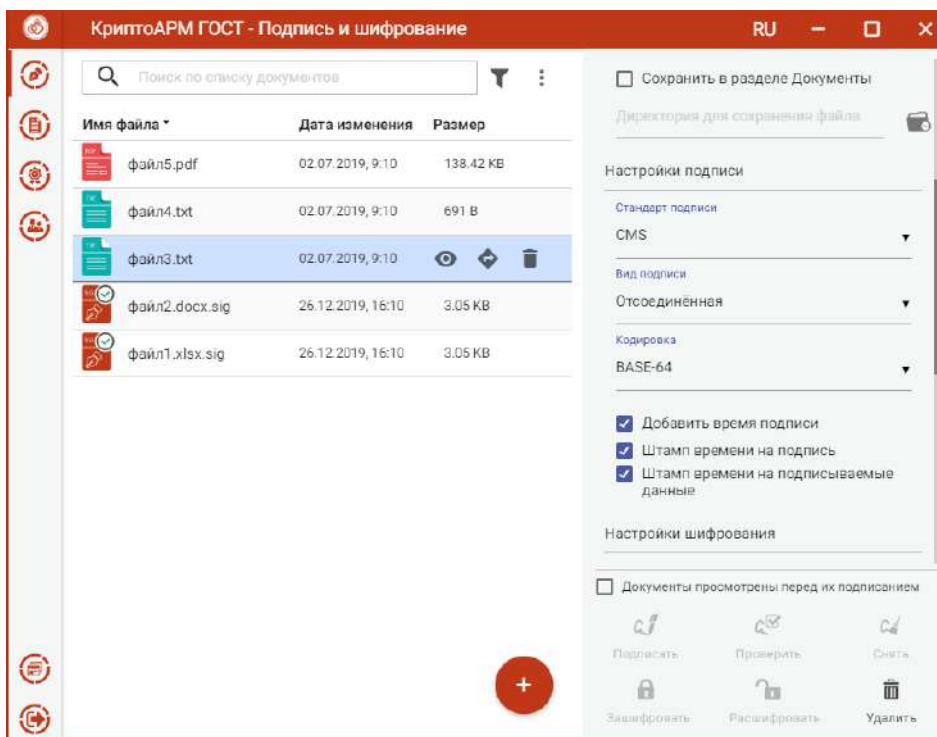


Рис. 5.3.1 Установка флага для добавления штампа времени в подпись

При установленном флаге добавления штампа времени на подпись или на данные необходимо заполнить параметры раздела Служба штампов времени (TSP) (рис. 5.3.2):

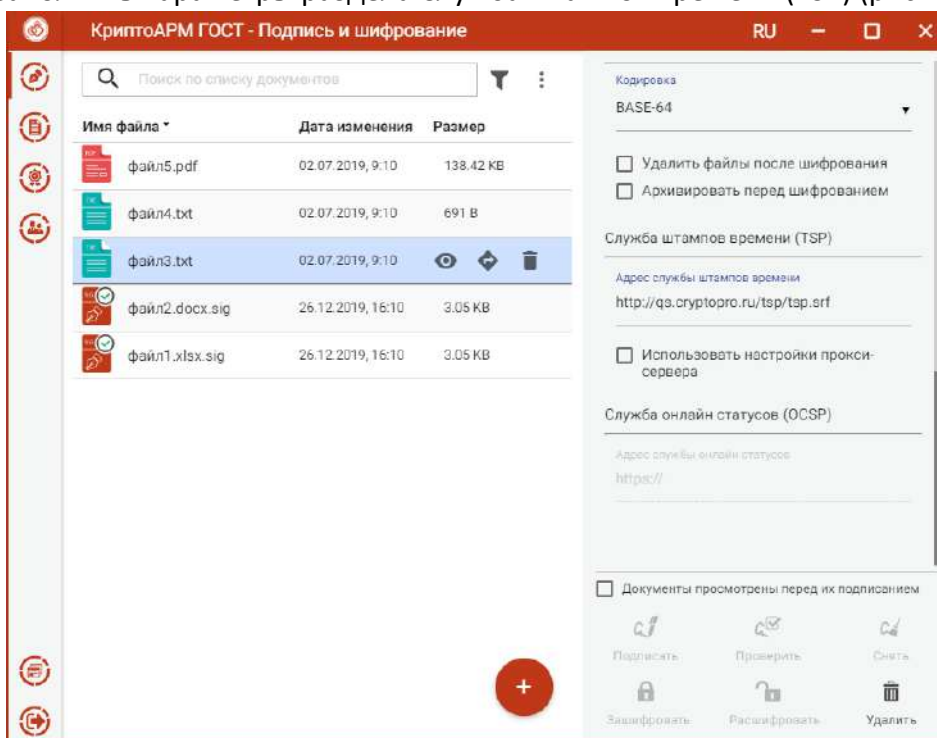


Рис. 5.3.2 Параметры штампов времени

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





**Адрес прокси-сервера, Порт, Логин, Пароль**, которые можно узнать у системного администратора.

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

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** (

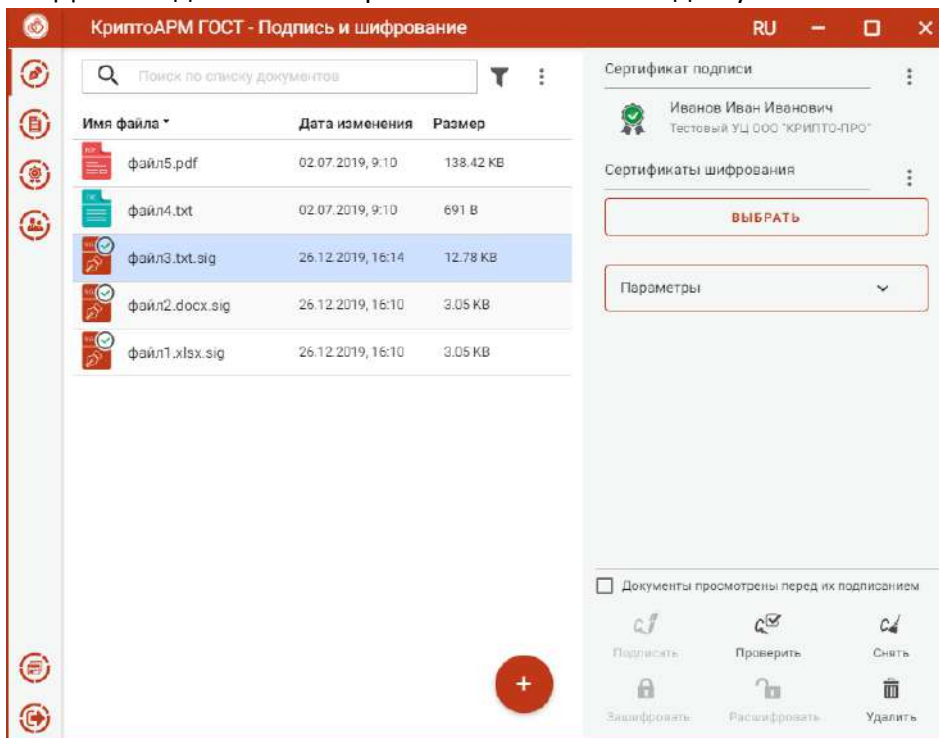


рис. 5.3.3).



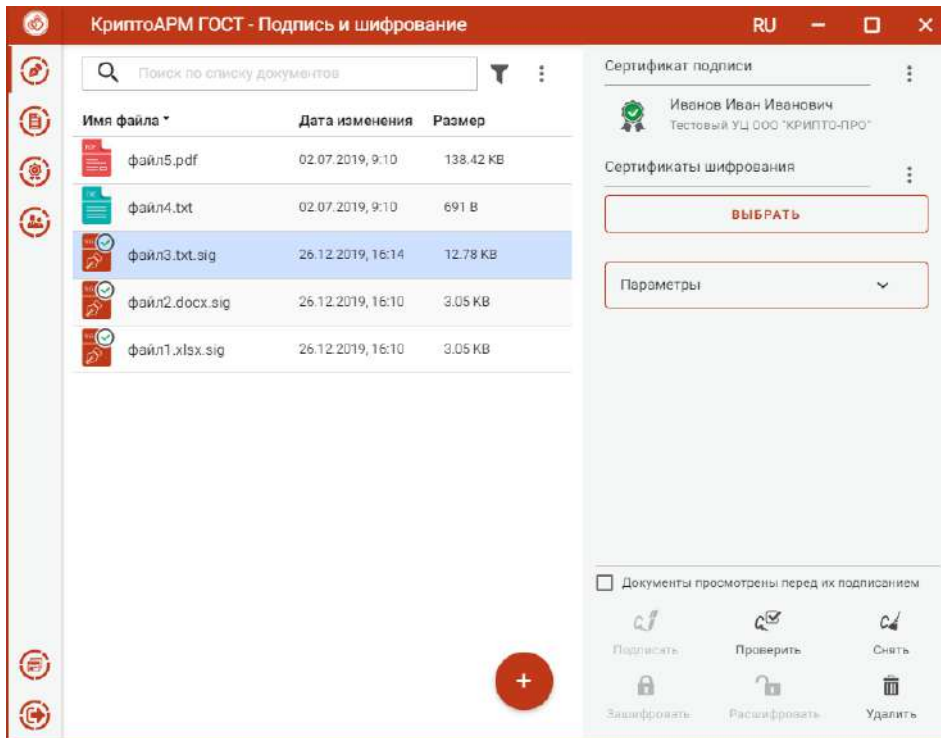


Рис. 5.3.3 Подписанные файлы

При просмотре информации о подписи отображается информация о штампе времени (рис. 5.3.4)

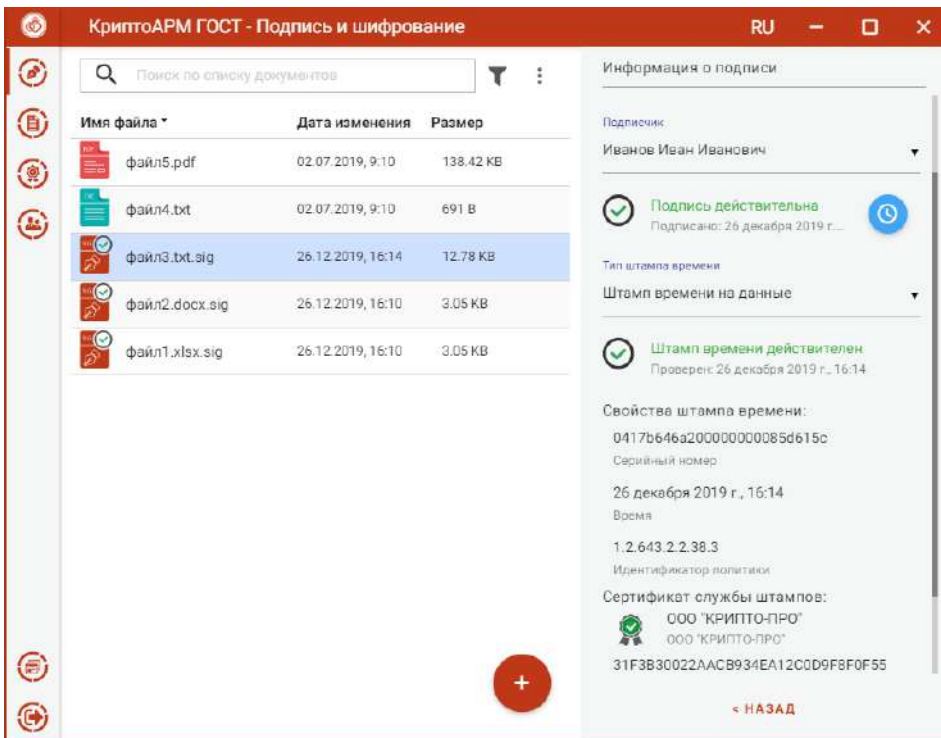


Рис. 5.3.4 Информация о штампе времени при просмотре подписи

#### 5.4. СОЗДАНИЕ УСОВЕРШЕНСТВОВАННОЙ ПОДПИСИ

Усовершенствованная квалифицированная электронная подпись поможет доказать юридическую значимость документа в спорных ситуациях. Например, когда помимо авторства



и целостности документа (которые дает обычная КЭП) необходимо подтвердить, что сертификат был действителен в момент подписания документа.

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

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

Для создания усовершенствованной подписи нужно выбрать подписываемые файлы, сертификат подписи и установить дополнительные параметры:

- Выбрать стандарт подписи **CADES-X Type 1** (рис. 5.4.1);

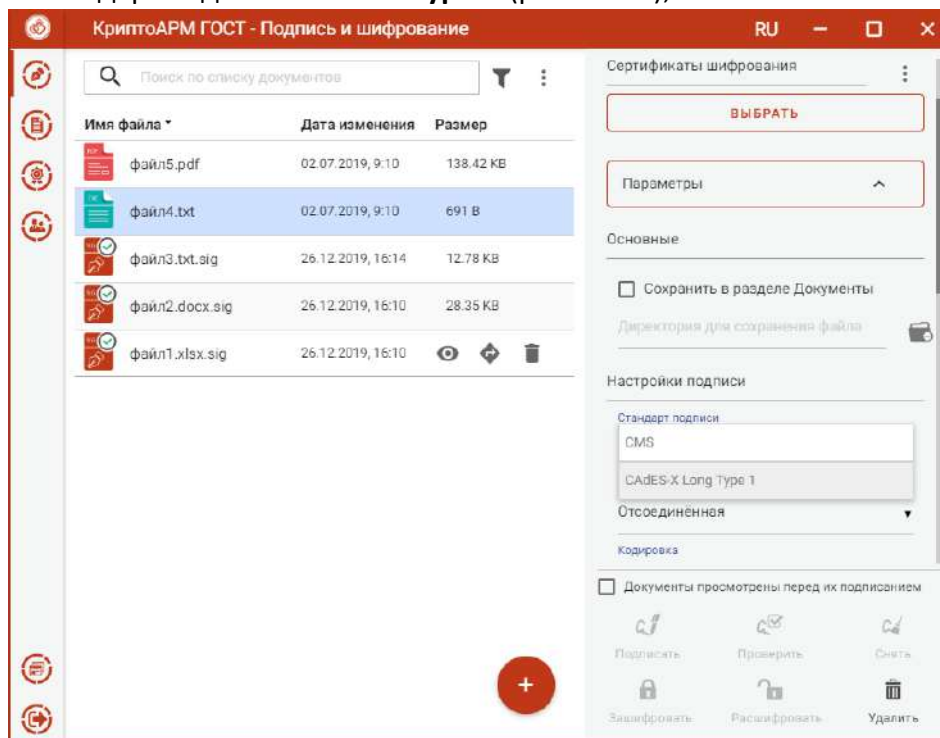


Рис. 5.4.1 Стандарт подписи CADES-X Type 1

- Заполнить параметры раздела **Служба штампов времени (TSP)** (рис. 5.4.2): **Адрес службы штампов времени, Использовать настройки прокси-сервера** (если при подключении к службе TSP используется прокси-сервер)

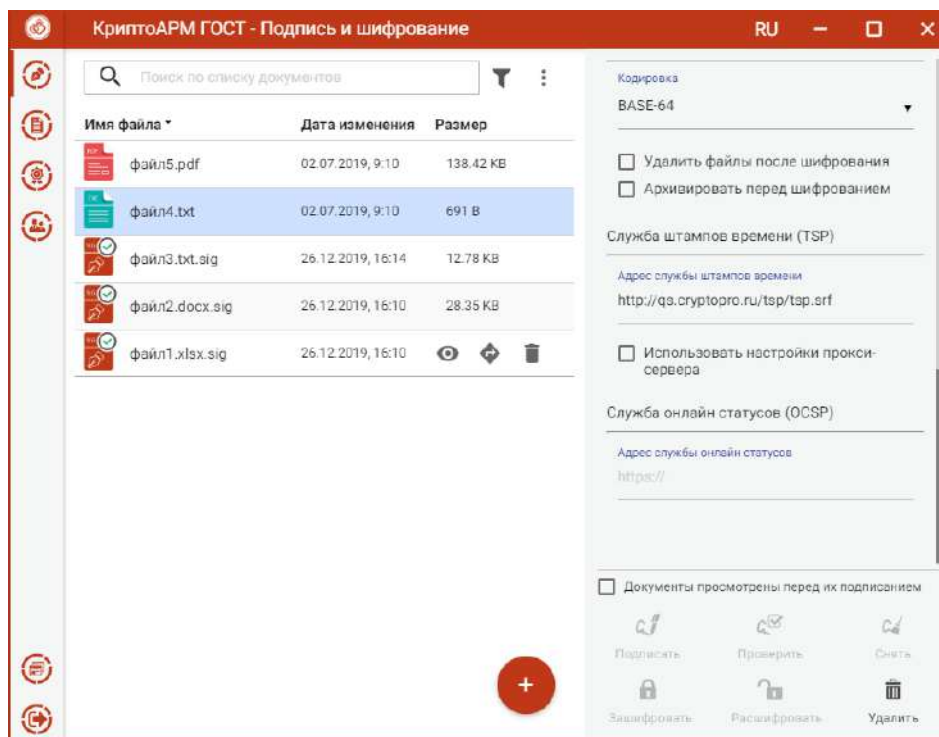


Рис. 5.4.2 Параметры службы штампов времени

– Заполнить параметры раздела **Службы online статусов (OCSP)** (рис. 5.4.2): **Адрес службы online статусов** - необязательный параметр, задается, если в сертификате данное поле не заполнено.

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

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. 5.4.3).

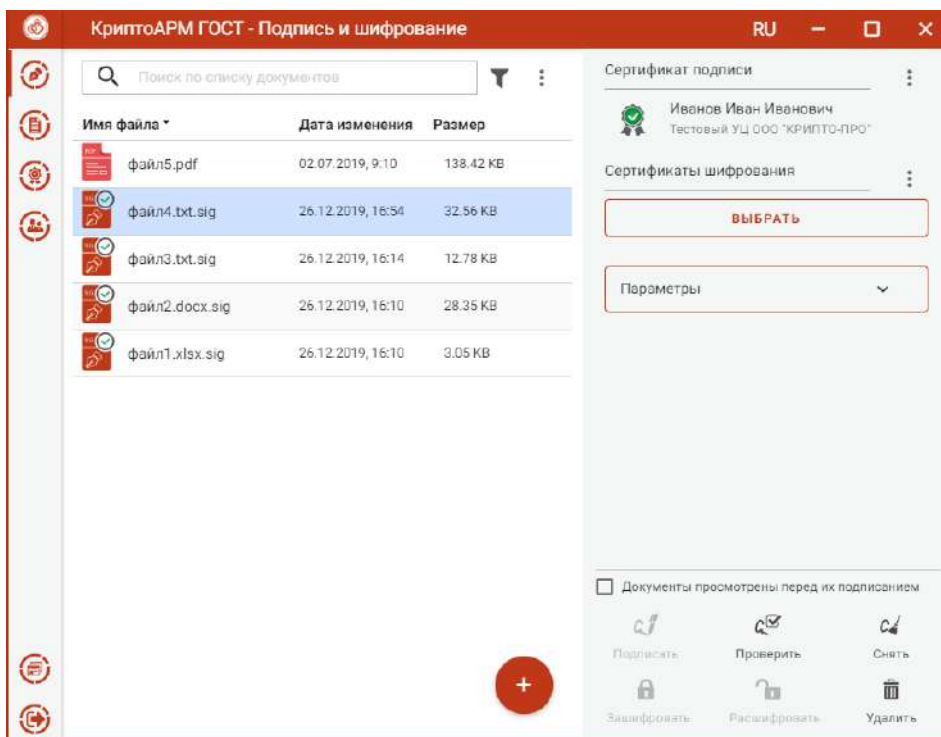


Рис. 5.4.3 Подписанные файлы

При просмотре информации о подписи отображается информация о OSCP ответе (рис. 5.4.4)

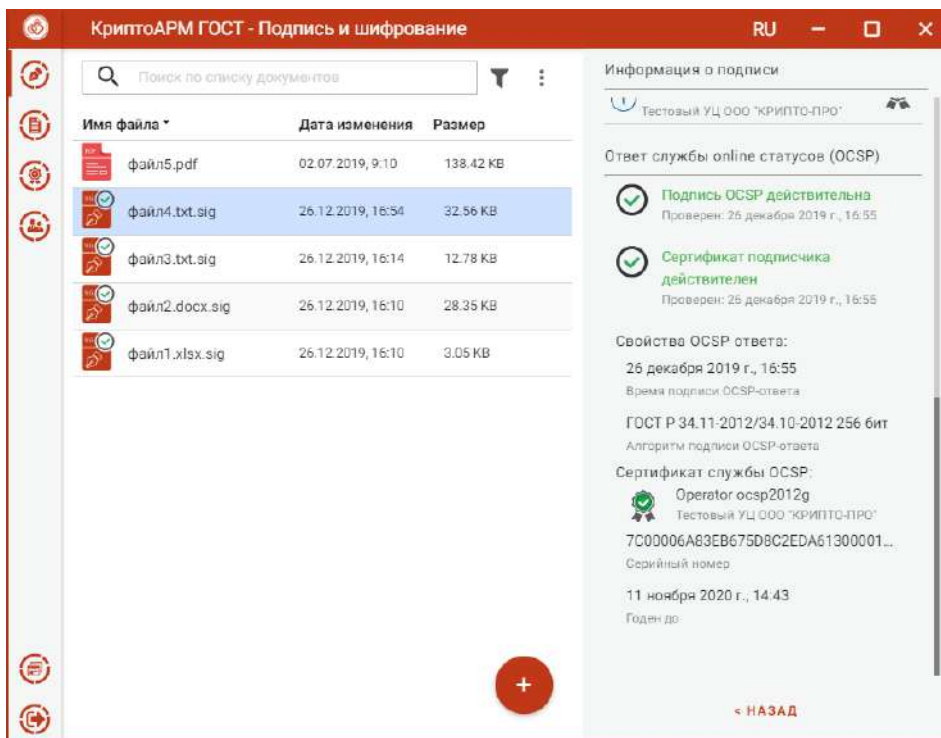


Рис. 5.4.4 Информация об OSCP ответе при просмотре подписи

Информация о штампе времени на подпись (рис. 5.4.5).

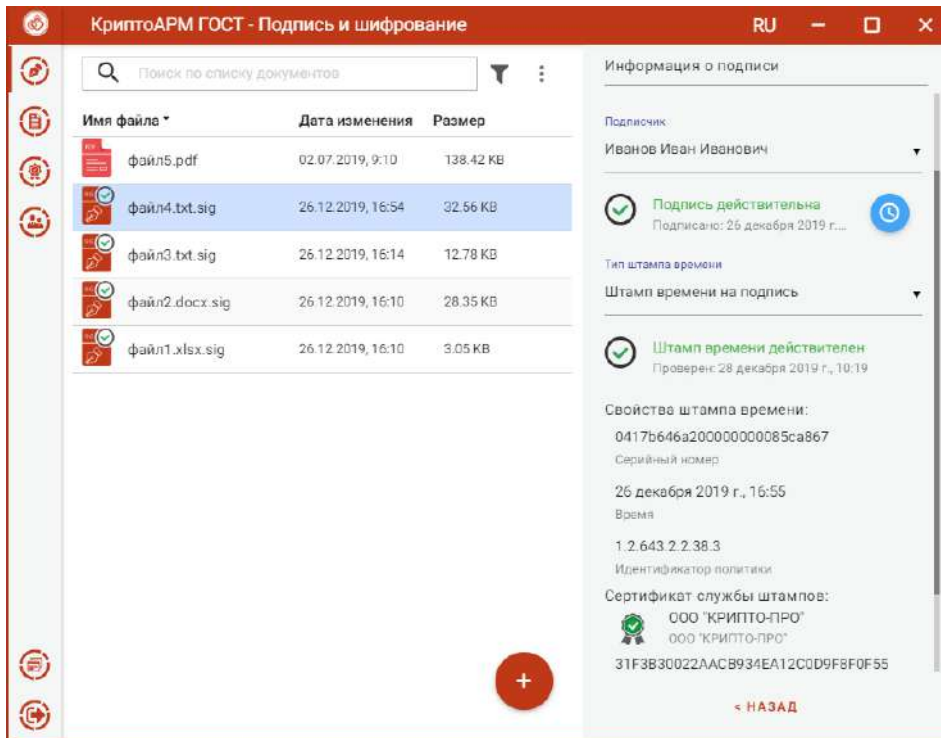


Рис. 5.4.5 Информация об штампе времени на подпись

И информация о доказательствах подлинности (рис. 5.4.6).

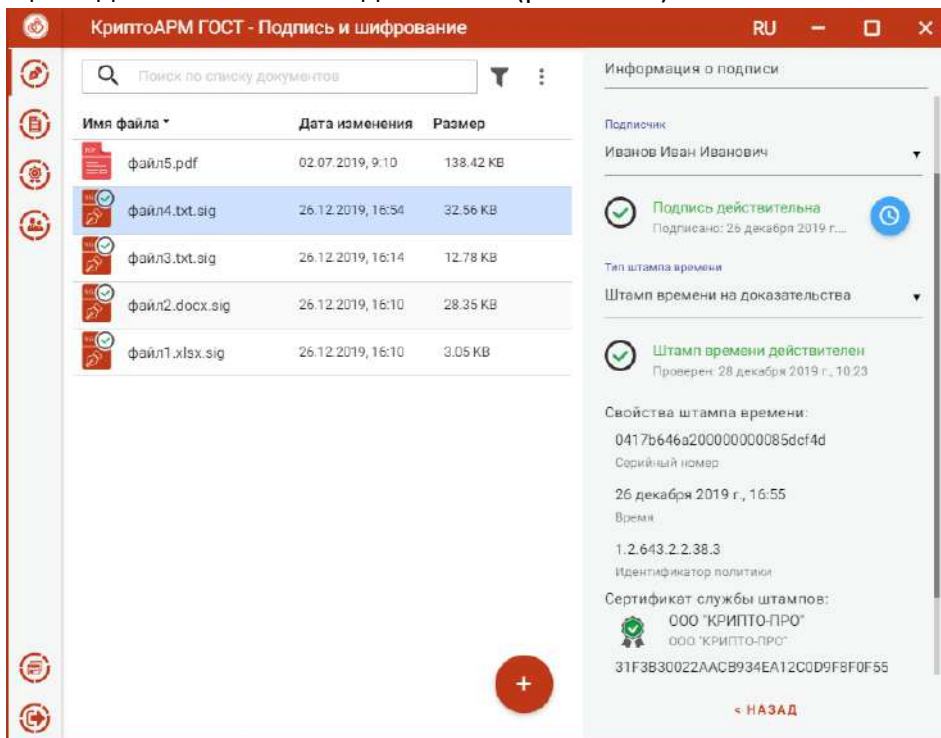


Рис. 5.4.6 Информация о доказательствах подлинности

## 5.5. 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. 5.5.1).

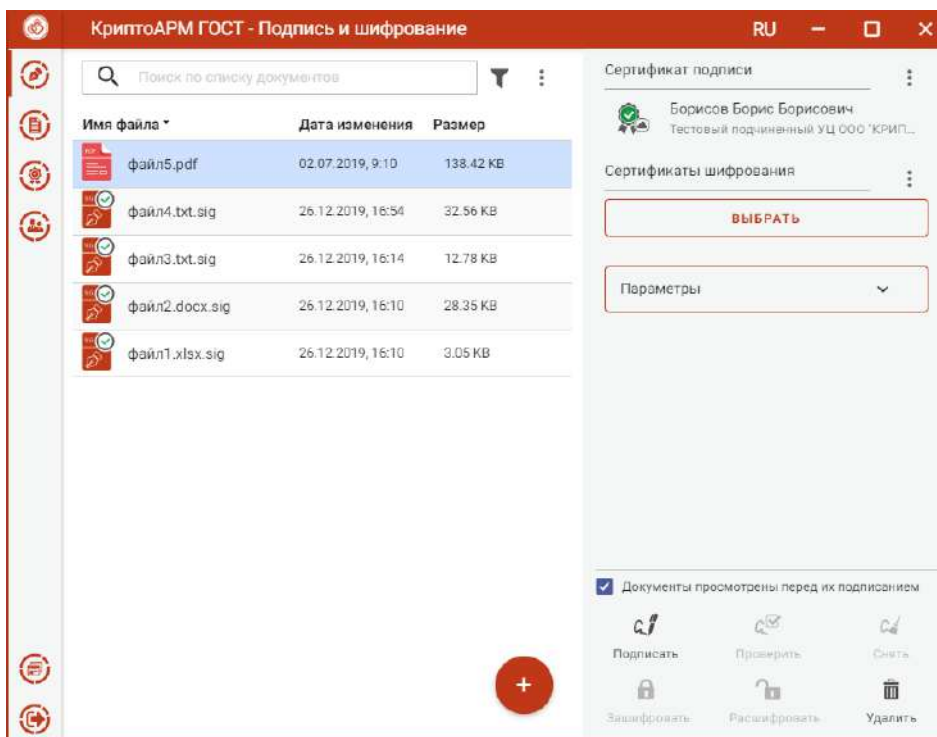


Рис. 5.5.1 Выбор файлов и сертификата для подписи DSS

При нажатии на кнопку **Подписать** открывается окно для ввода пароля для аутентификации на сервисе DSS (рис. 5.5.2), если время действия токена аутентификации истекло. Если токен аутентификации не истек, то данный шаг пропускается.

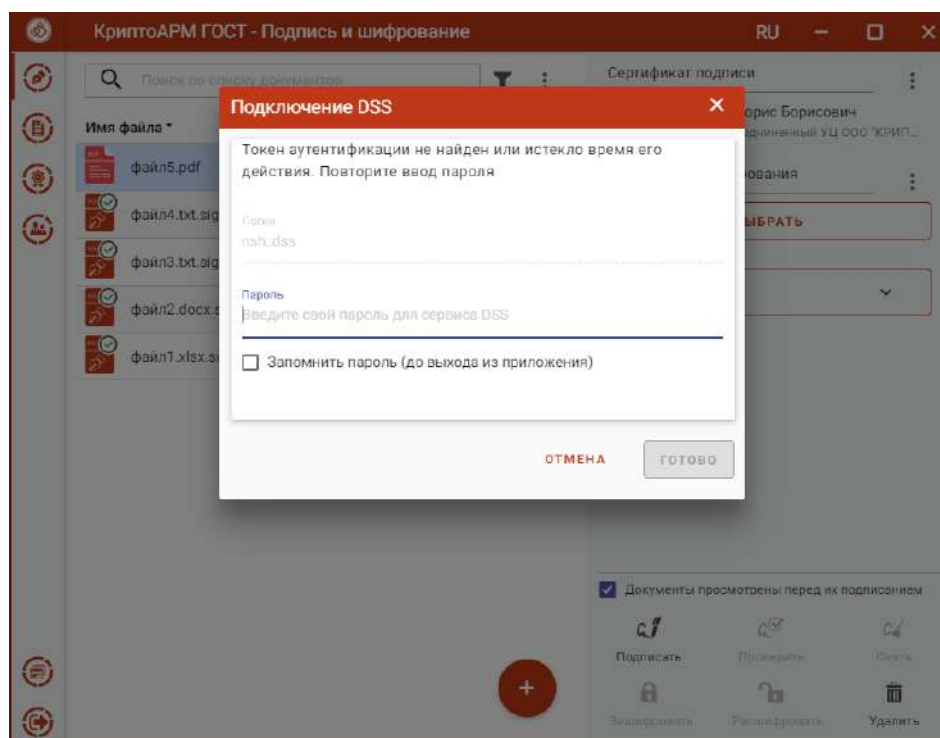


Рис. 5.5.2 Ввод пароля аутентификации на сервисе DSS

При нажатии на кнопку **Готово** открывается окно для ввода пароля к ключевому контейнеру (рис. 5.5.3). Если пароль не задан, то данный шаг пропускается.



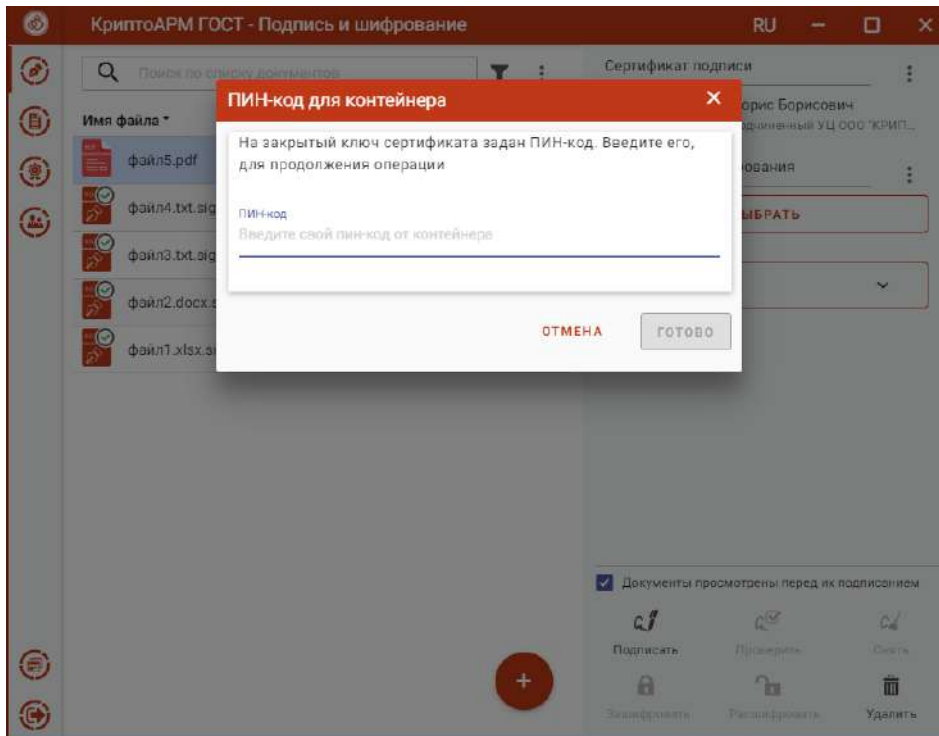


Рис. 5.5.3 Ввод пароля к ключевому контейнеру

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. 5.5.4).

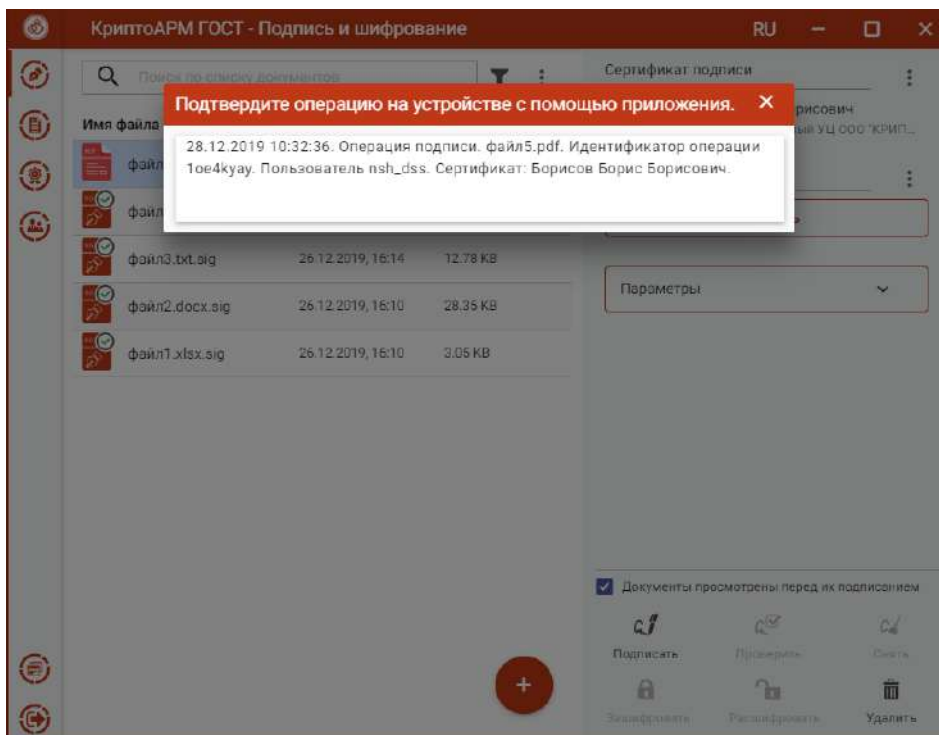


Рис. 5.5.4 Окно ожидания подтверждения операции подписи

После подтверждения операции на устройстве происходит подпись файла.



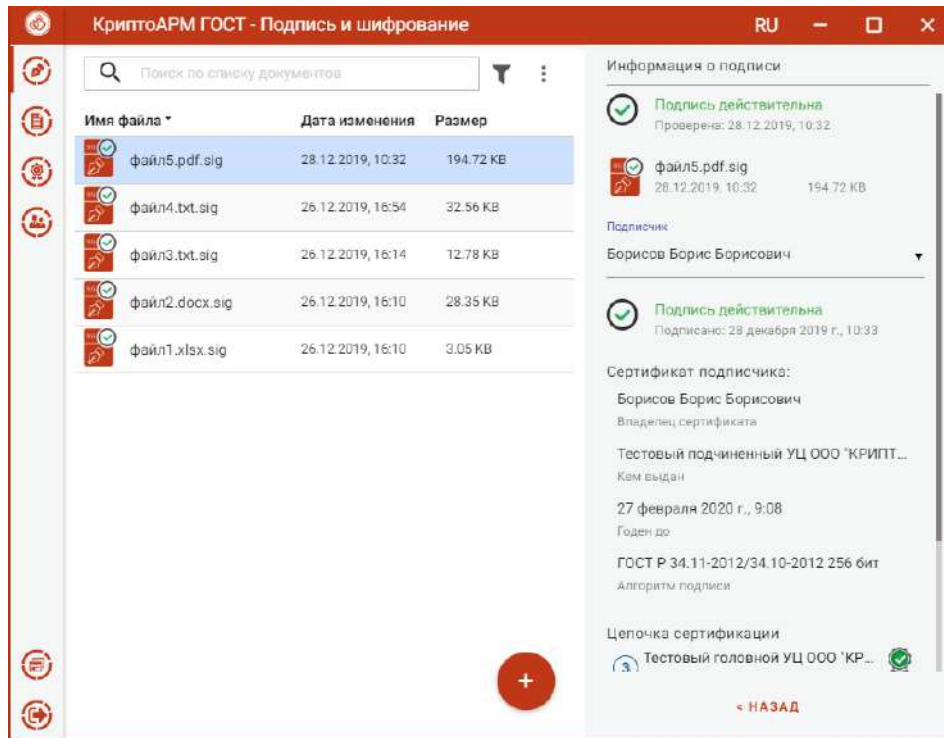


Рис. 5.5.5 Подписанный файл

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

## 5.6. 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. 5.6.1): зеленый - подпись действительна; красный - подпись недействительна.

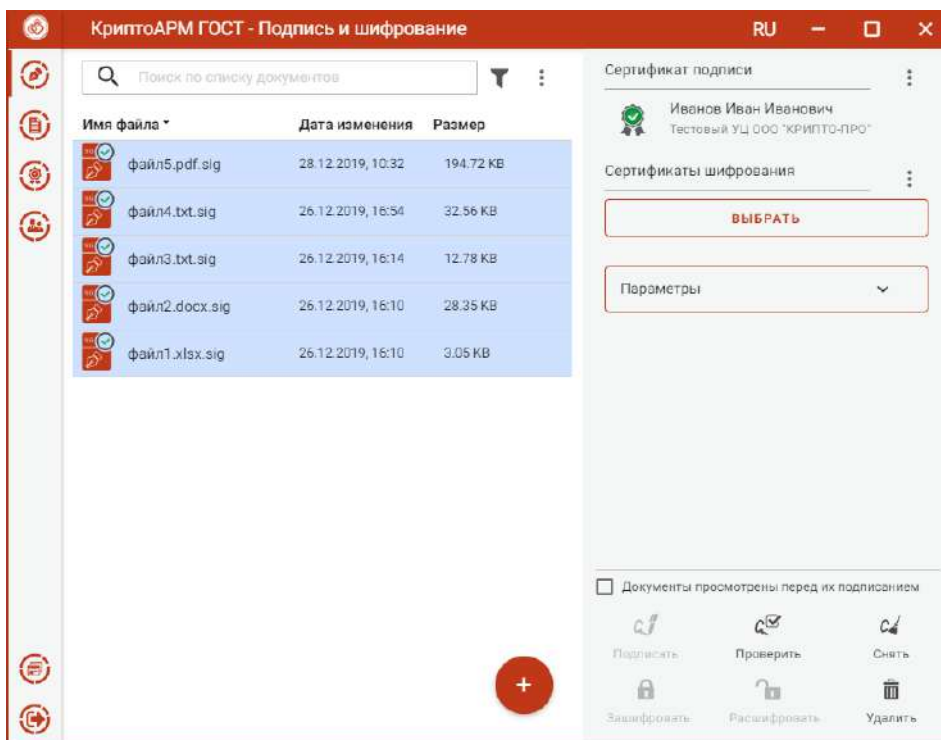


Рис. 5.6.1 Результат проверки подписи файлов

При выделении одного подписанного файла в правой области отображается информация о подписи (рис. 5.6.2).

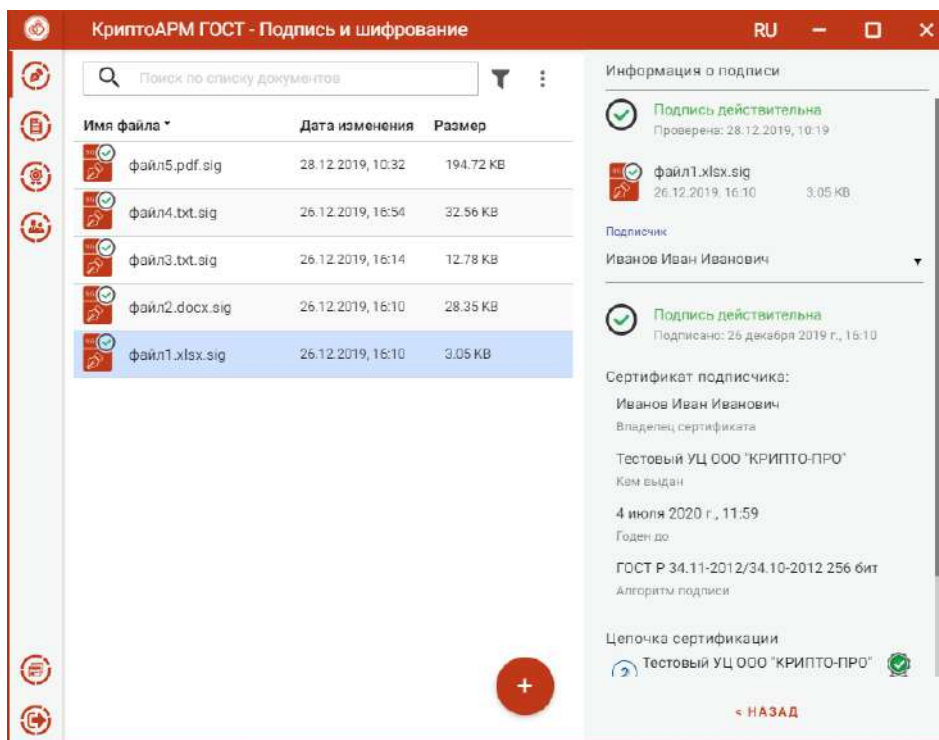


Рис. 5.6.2 Отображение информации о подписи

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

Если документ подписан несколькими подписями (имеет соподписи), то для просмотра информации о подписи нужно в выпадающем списке выбрать подписчика (рис. 5.6.3).

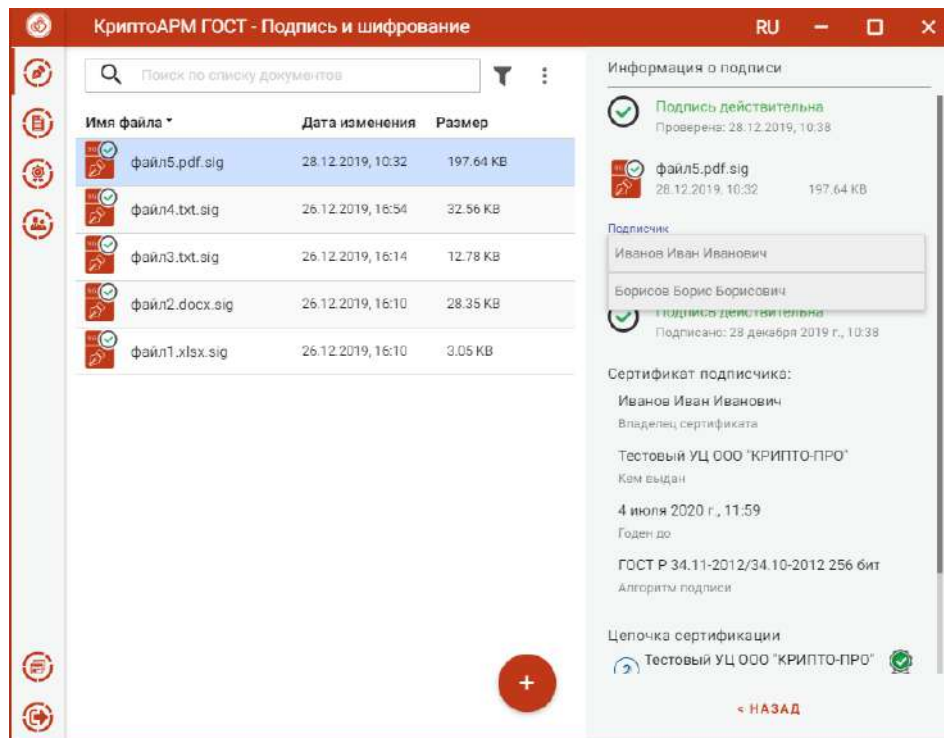


Рис. 5.6.3 Выбор подписчика для просмотра информации о подписи

Если документ подписан подписью со штампом времени, то для просмотра параметров штампа нужно нажать на иконку развернуть информацию и выбрать в выпадающем списке тип штампа времени (рис. 5.6.4).

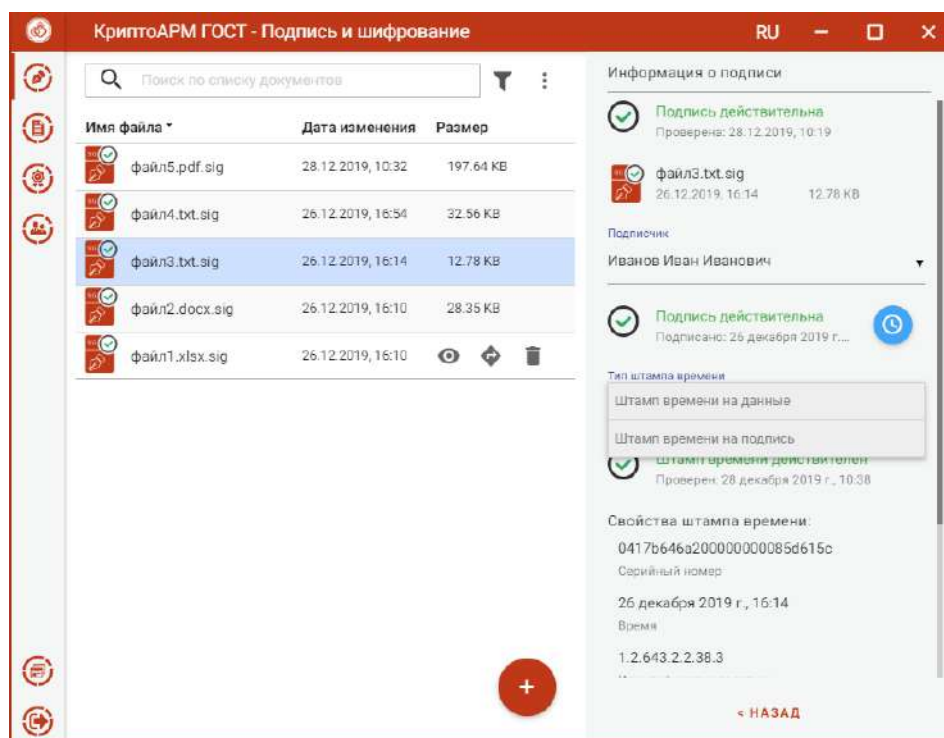


Рис. 5.6.4 Отображение информации о подписи со штампом времени

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

рис. 5.6.5).

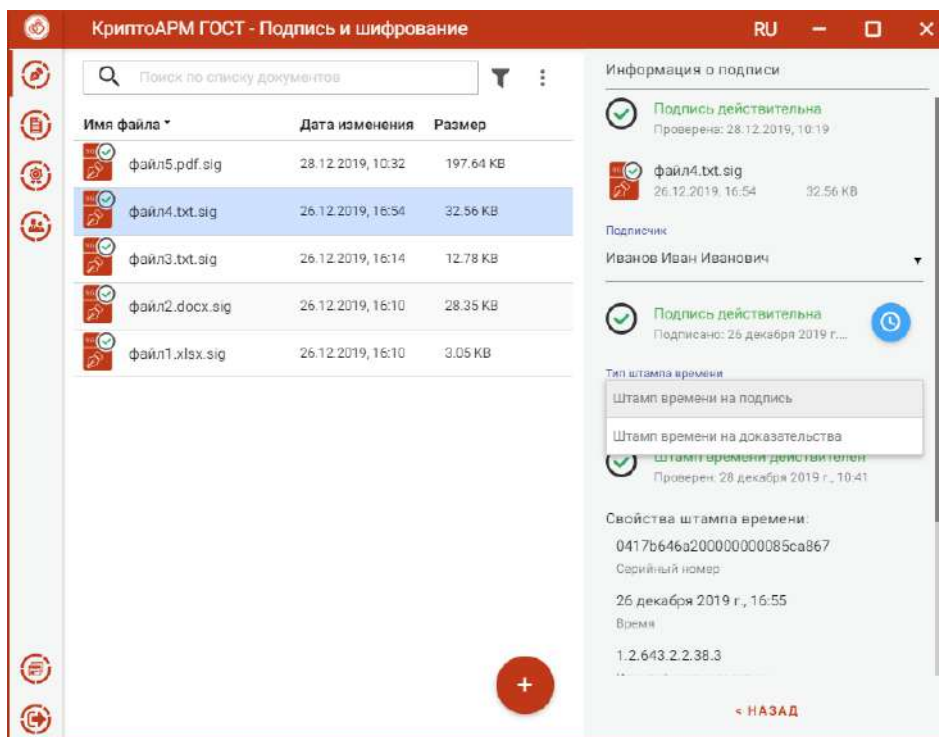


Рис. 5.6.5 Отображение информации о штампах времени усовершенствованной подписи

Информация о OCSP ответе усовершенствованной подписи представлена на рисунке рис. 5.6.6.

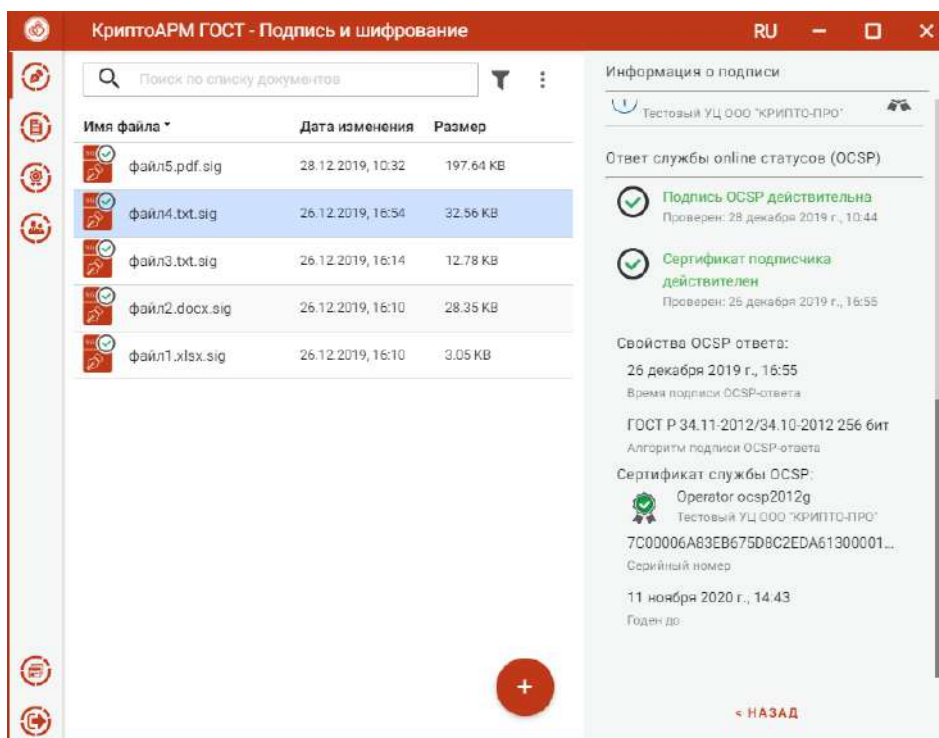


Рис. 5.6.6 Отображение информации о OCSP ответе усовершенствованной подписи

## 5.7. Снятие электронной подписи

Для снятия подписи достаточно выбрать подписанные файлы - файлы с расширением **.sig**, которые содержат электронную подпись и нажать на кнопку **Снять** (рис. 5.7.1).

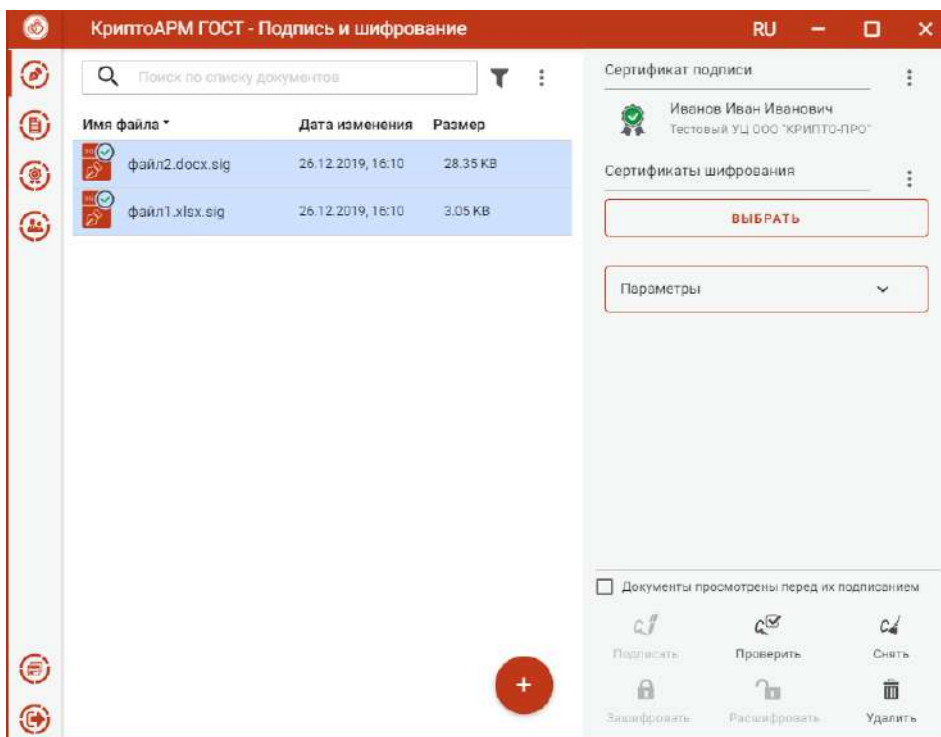


Рис. 5.7.1 Выделенные файлы для снятия подписи

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. 5.7.2).

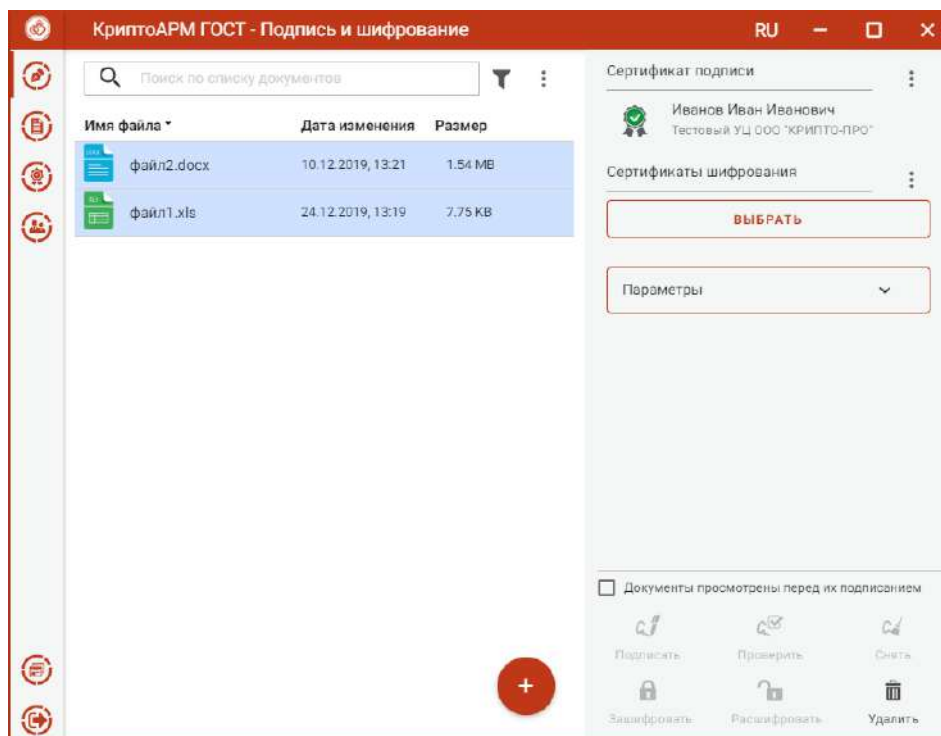


Рис. 5.7.2 Результат снятия подписи с файлов

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



## 5.8. ДОБАВЛЕНИЕ ПОДПИСИ

Приложение КристоАРМ 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. 5.8.1).

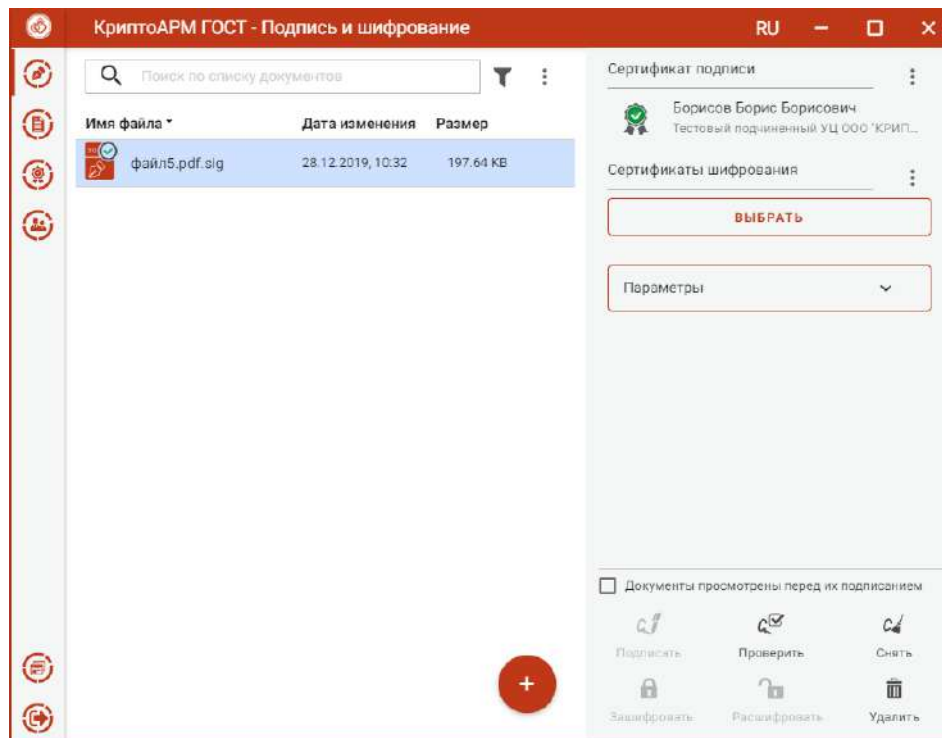


Рис. 5.8.1 Добавление подписи к уже подписанным файлам

Для всех добавленных подписей настройки подписи, такие как кодировка и вид подписи, используются по умолчанию, как для первой подписи. Тип подписи и использование штампов времени можно настроить.

В информации о подписи содержатся сведения о всех подписях. Чтобы посмотреть информацию о конкретном подписчике, нужно выбрать подписчика из выпадающего списка (рис. 5.8.2).



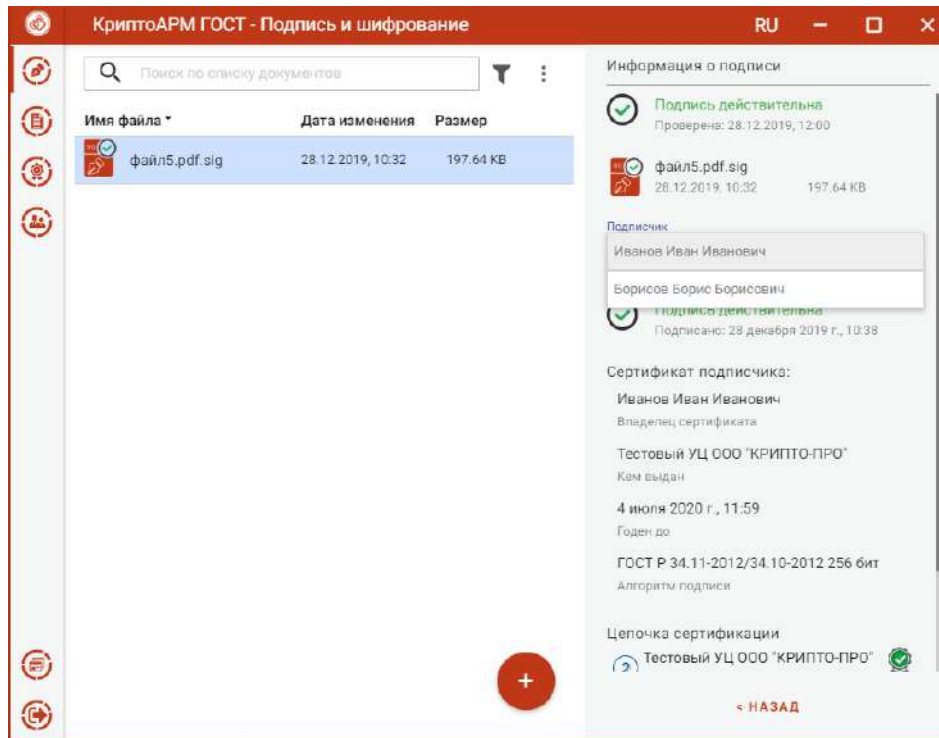


Рис. 5.8.2 Выбор подписчика при просмотре информации о подписи

## 5.9. 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 шифрование одного или группы выбранных файлов. Файлы для шифрования можно добавить двумя способами: через кнопку **Добавить файлы** («+») или перетаскив файлы мышкой в область формирования списка файлов.

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (рис. 5.9.1).



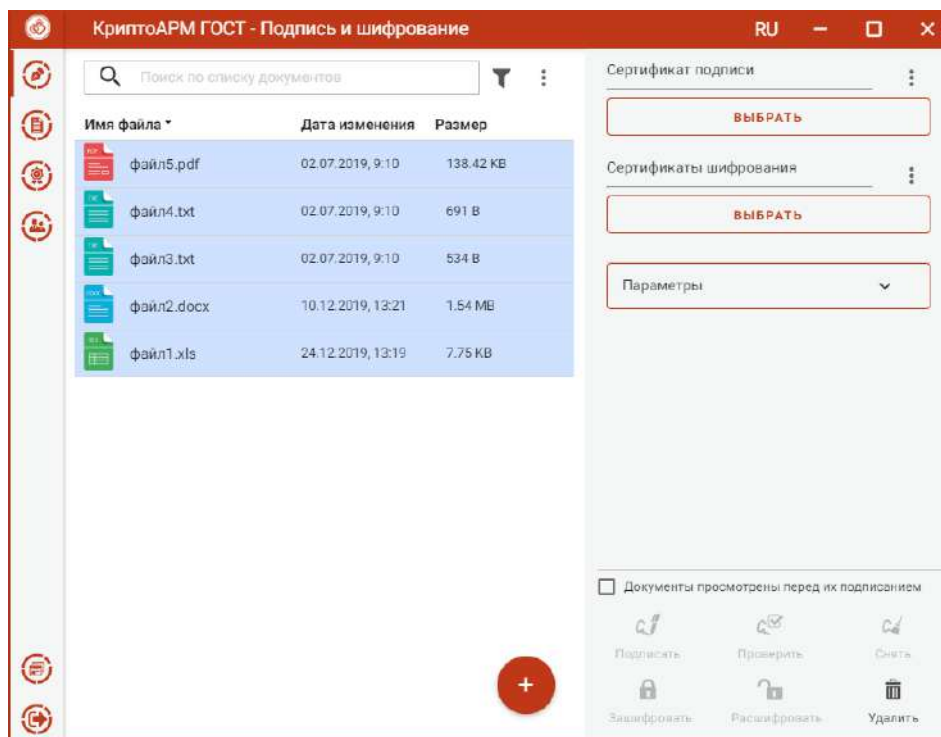


Рис. 5.9.1 Список файлов для шифрования

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (рис. 5.9.2).

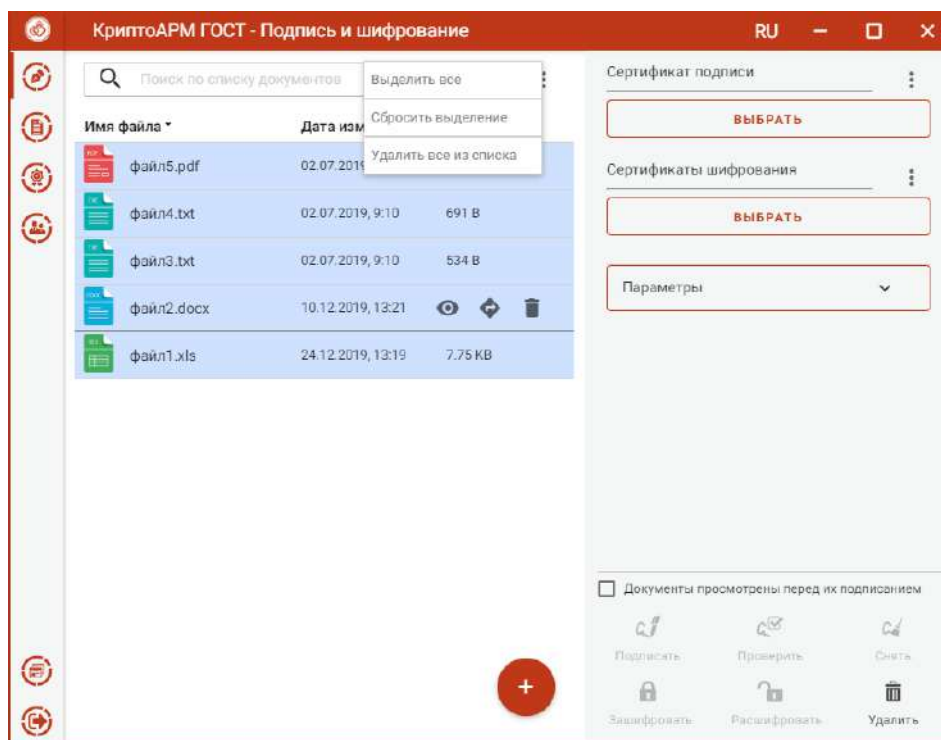


Рис. 5.9.2 Контекстное меню управления списком файлов

**НАСТРОЙКА ПАРАМЕТРОВ ШИФРОВАНИЯ.** Параметры шифрования задаются в раскрывающемся списке **Дополнительных параметров** (рис. 5.9.3).

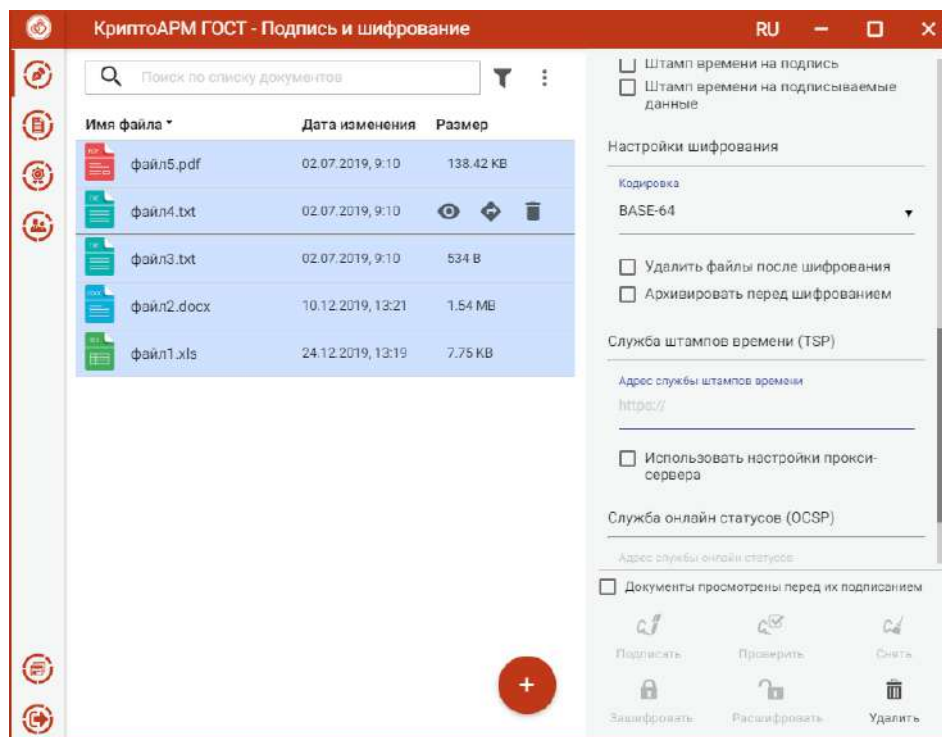


Рис. 5.9.3 Выбор параметров шифрования

В параметрах можно настроить:

- **Сохранить в разделе Документы** – при установленном флажке результат операции сохраняется в каталог Documents, расположенный в папке пользователя в каталоге /Trusted/CryptoARM GOST/. Если флаг не установлен и не выбрана директория для сохранения файла, то файл сохраняется рядом с исходным файлом.
- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Архивировать перед шифрованием** - файлы архивируются (ZIP) перед выполнением операции шифрования. Шифруется созданный ZIP-архив..
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования удаляются из файловой системы в случае успешного завершения операции.

**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. 5.9.4).

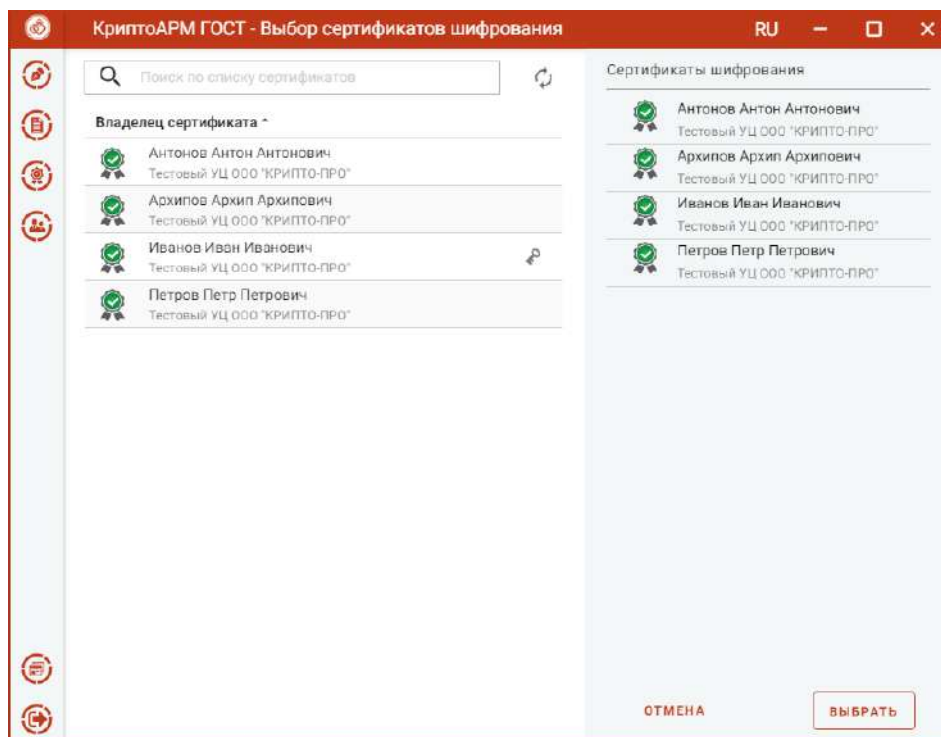


Рис. 5.9.4 Выбор сертификатов шифрования

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 удалить, по ним можно посмотреть детальную информацию, нажав на интересующий сертификат в правой области (рис. 5.9.5).

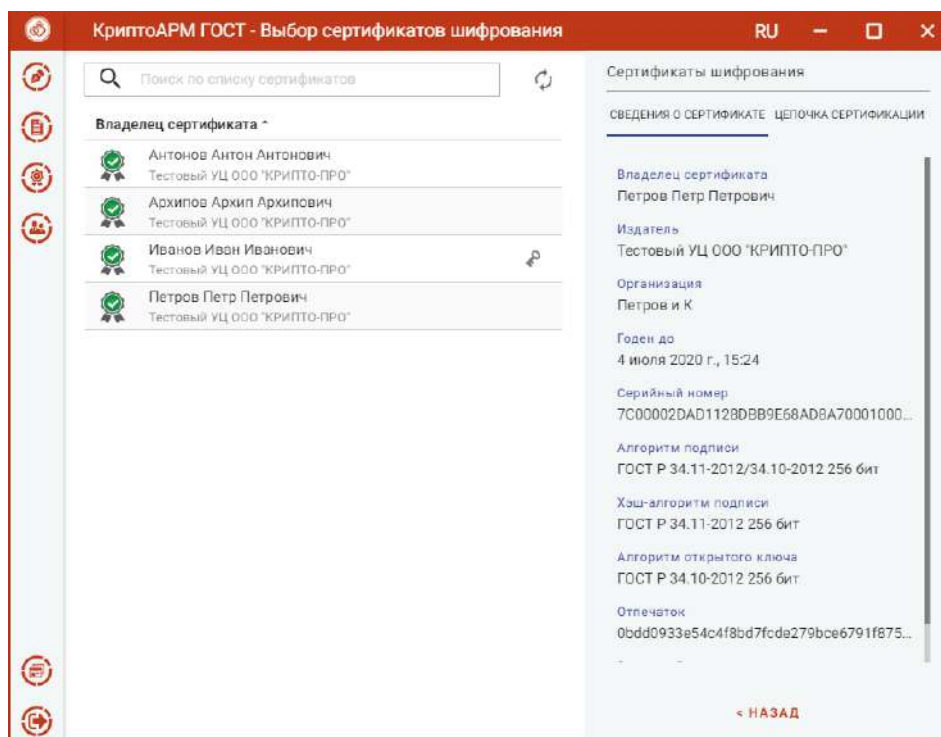


Рис. 5.9.5 Информация о сертификате шифрования

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



Изменить список сертификатов шифрования можно с помощью контекстного меню (рис. 5.9.6). Удалить сертификаты из сформированного списка можно кнопкой **Удалить**.

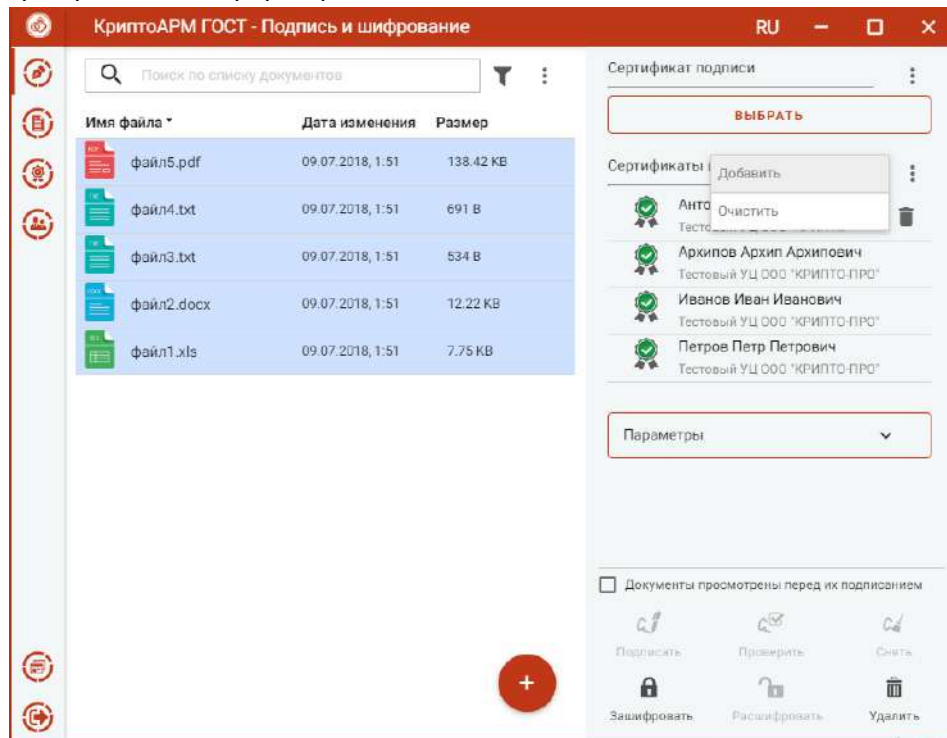


Рис. 5.9.6 Изменение списка сертификатов шифрования

Если список личных сертификатов и сертификатов других пользователей пуст, то можно создать или импортировать сертификат на вкладке [Сертификаты](#).

**ШИФРОВНИЕ ФАЙЛОВ.** При условии выбора сертификатов получателей и файлов в мастере становится доступной кнопка **Зашифровать** (рис. 5.9.7).

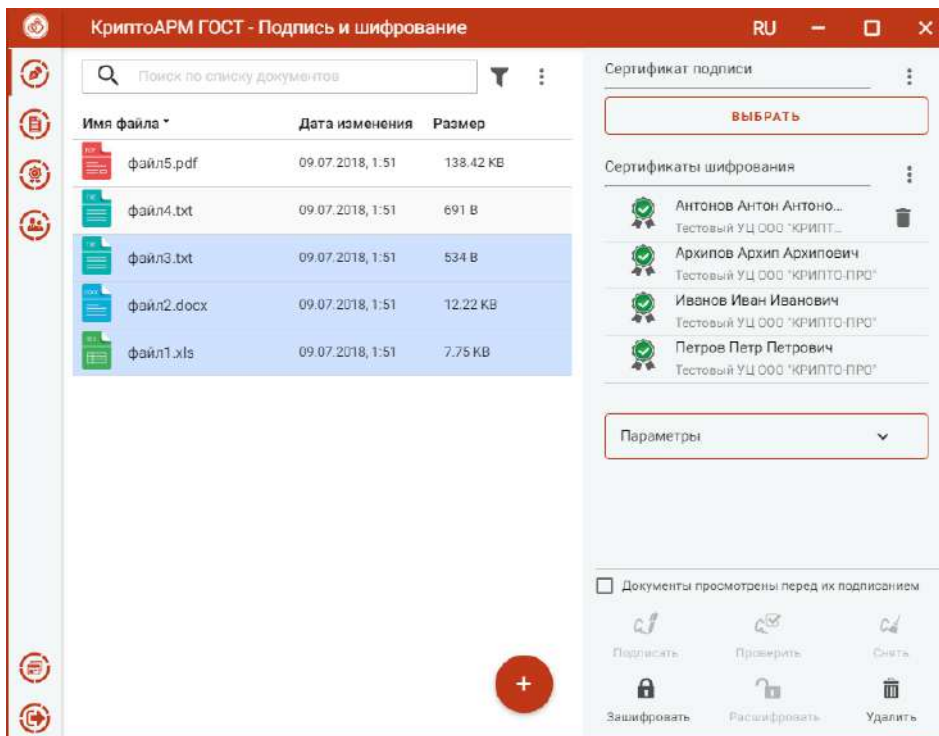


Рис. 5.9.7 Шифрование файлов



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

Если в параметрах 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. 5.9.8).

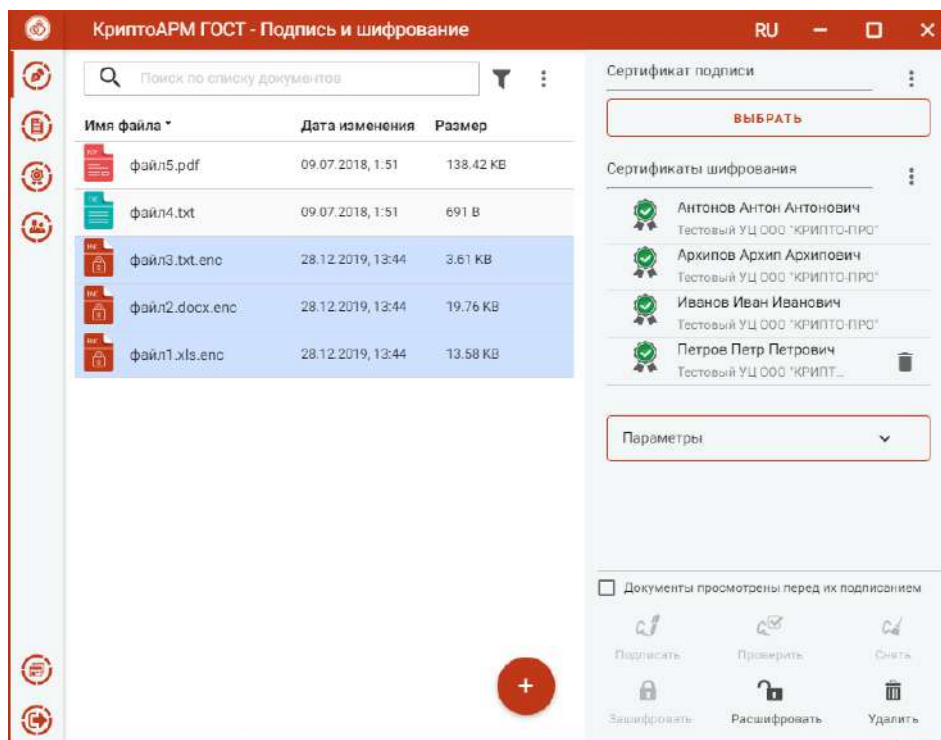


Рис. 5.9.8 Зашифрованные файлы

## 5.10. 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.

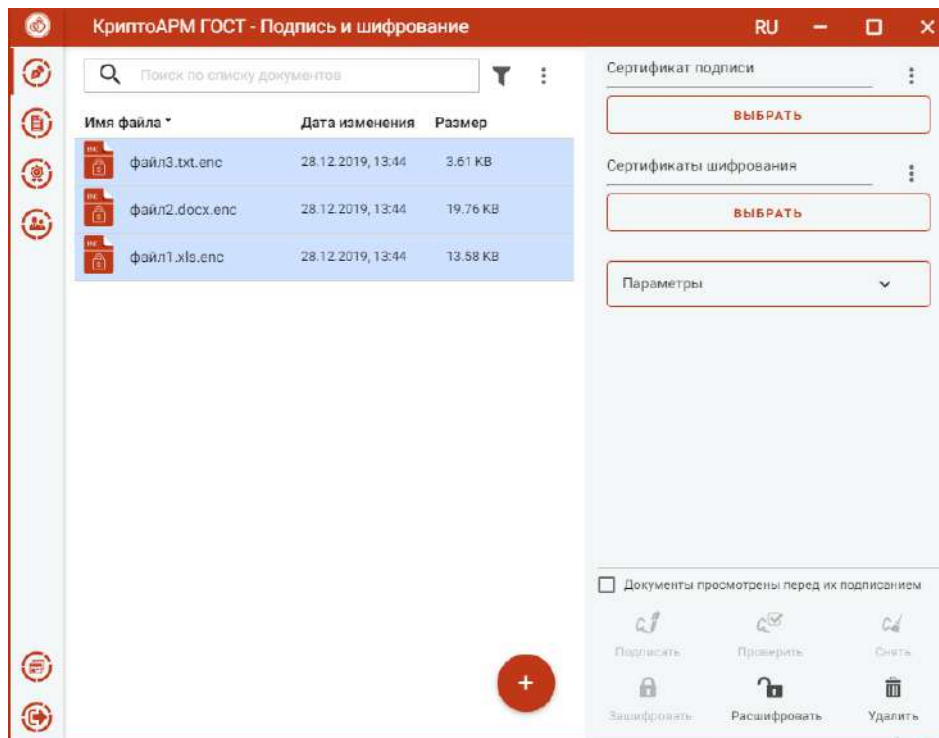


Рис. 5.10.1 Мастер расшифрования файлов

При расшифровании у файлов меняется иконка, наименование, дата создания (рис. 5.10.2). 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**.

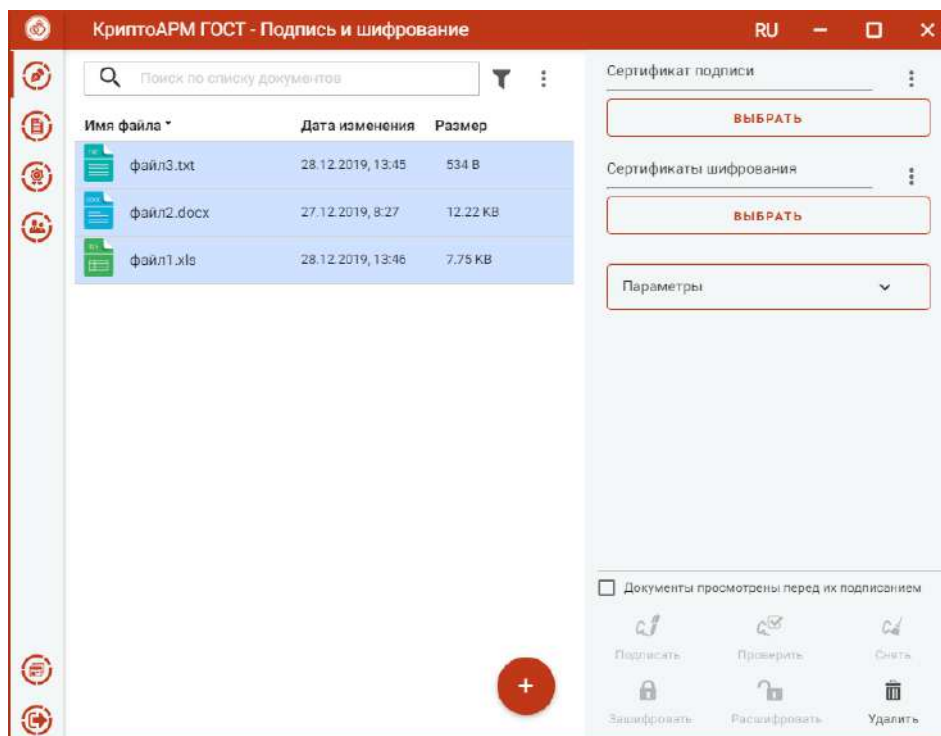


Рис. 5.10.2 Результат операции расшифрования





### 5.11. Управление списком файлов для выполнения операций

Список файлов для выполнения операций представляет собой одноуровневый список (рис. 5.11.1).

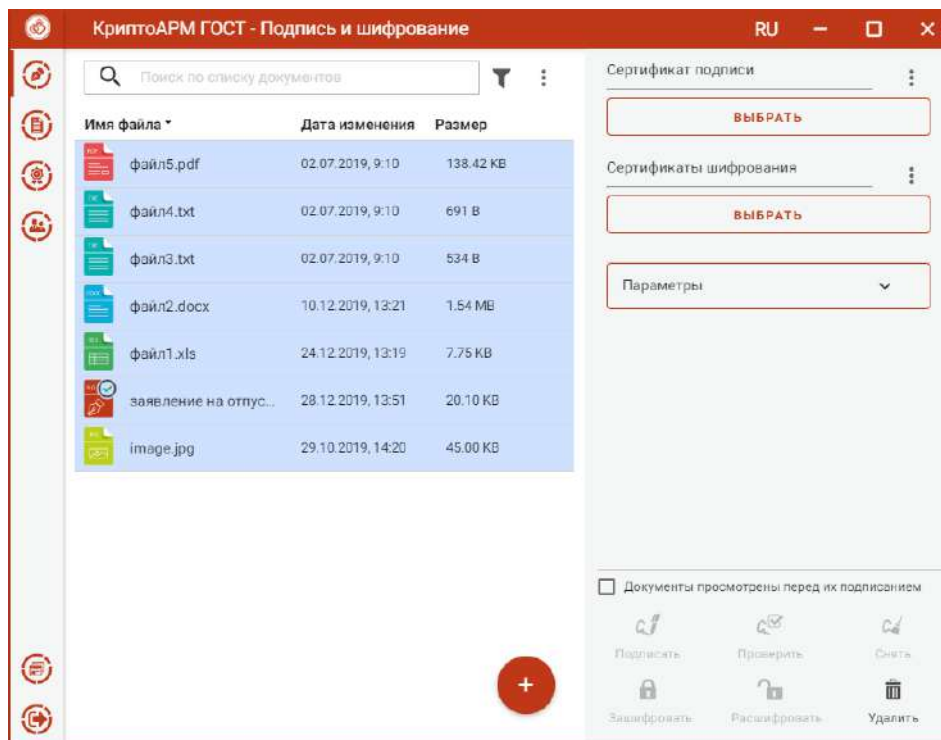


Рис. 5.11.1 Список файлов

Файлы в список можно добавить двумя способами: через кнопку **Добавить файлы** («+») или перетаскивая 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. 5.11.2), 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.



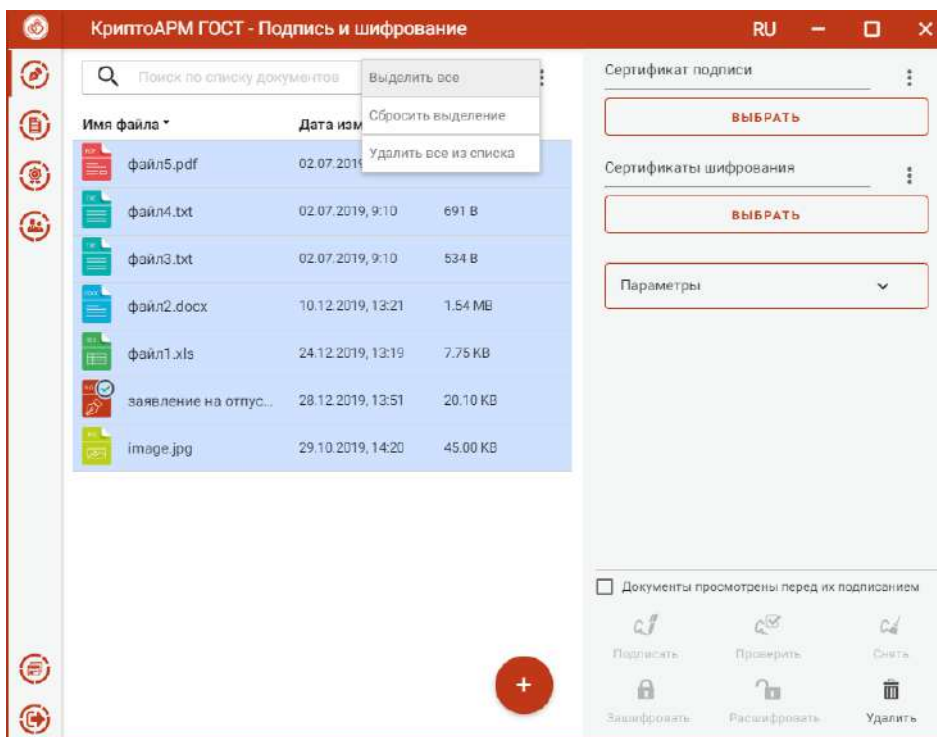


Рис. 5.11.2 Контекстное меню списком файлов

Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши (рис. 5.11.3):

- **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.

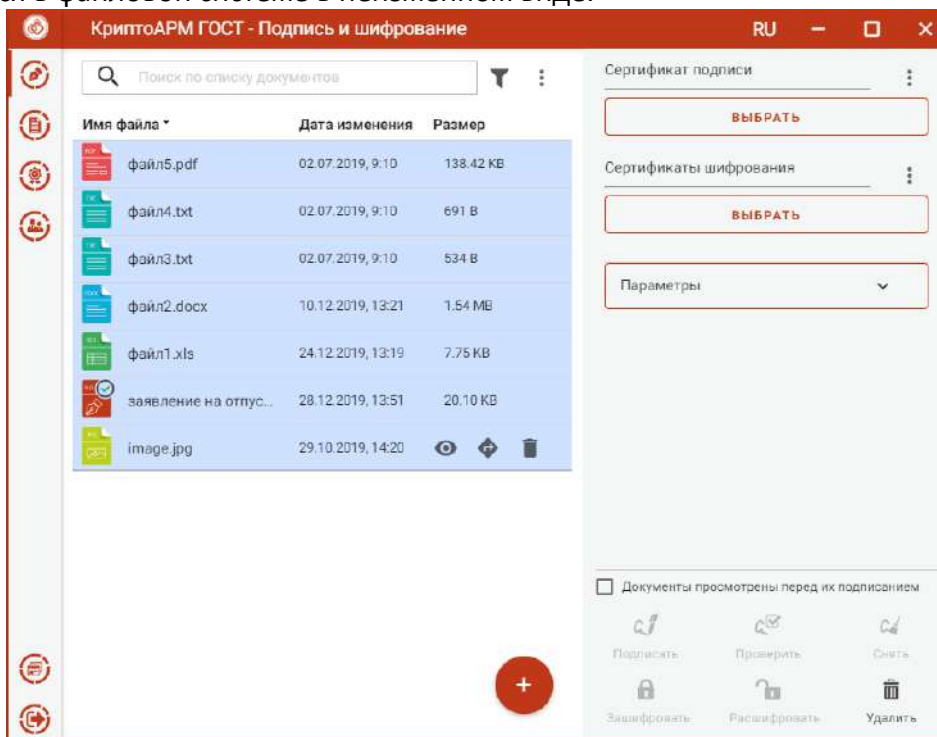


Рис. 5.11.3 Кнопки операций файла



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. 5.11.4)

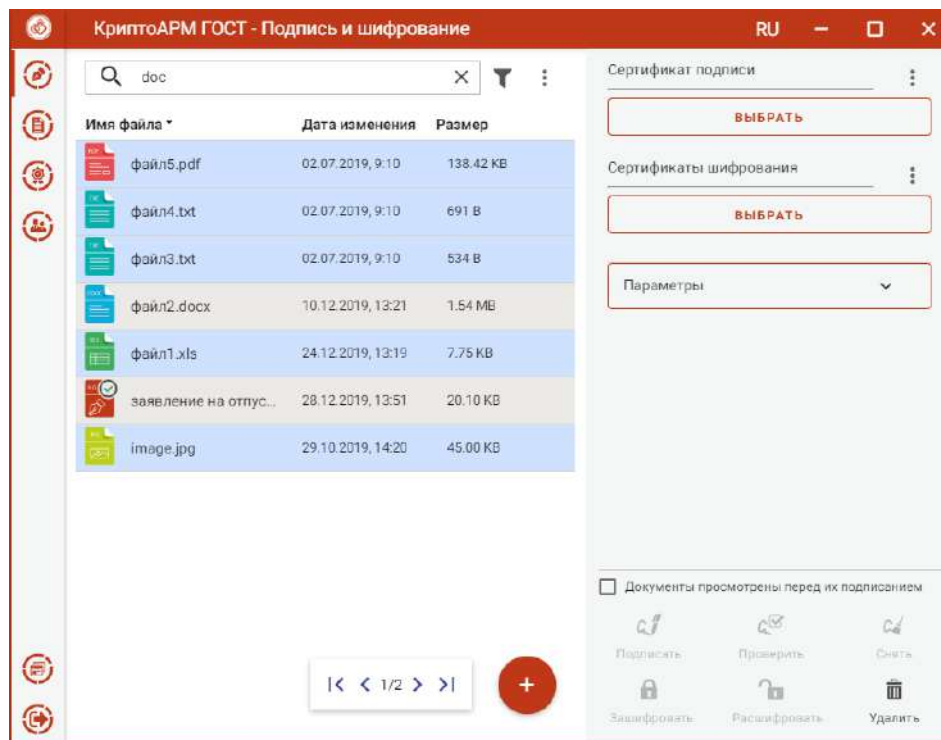


Рис. 5.11.4 Поиск файлов

Список файлов можно отфильтровать, задав настройки фильтрации (рис. 5.11.5).

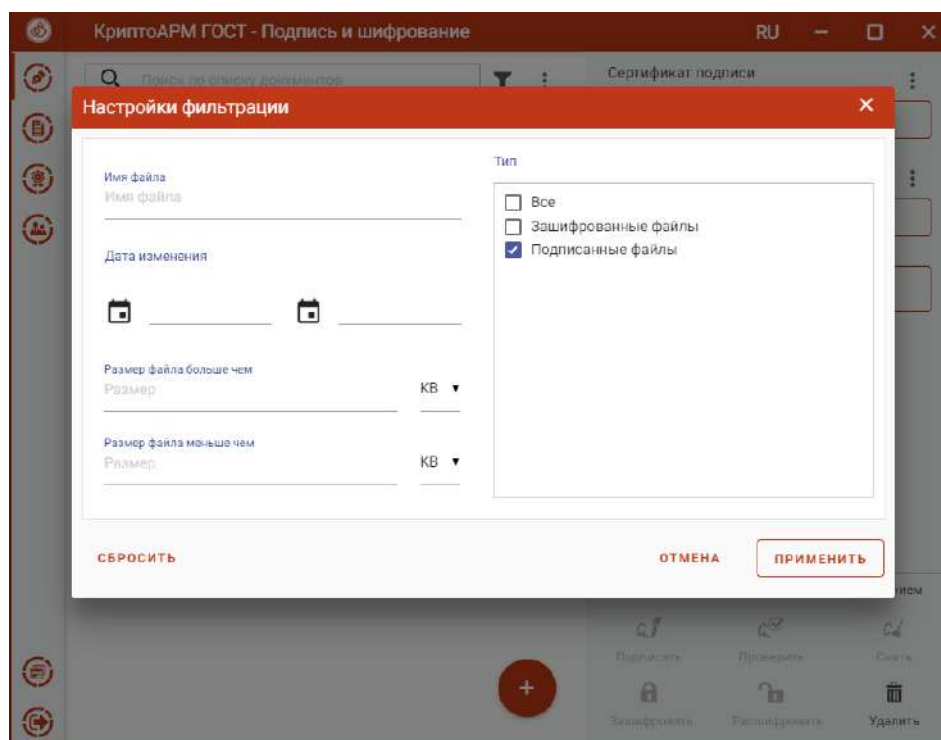


Рис. 5.11.5 Настройки критериев фильтра файлов



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.

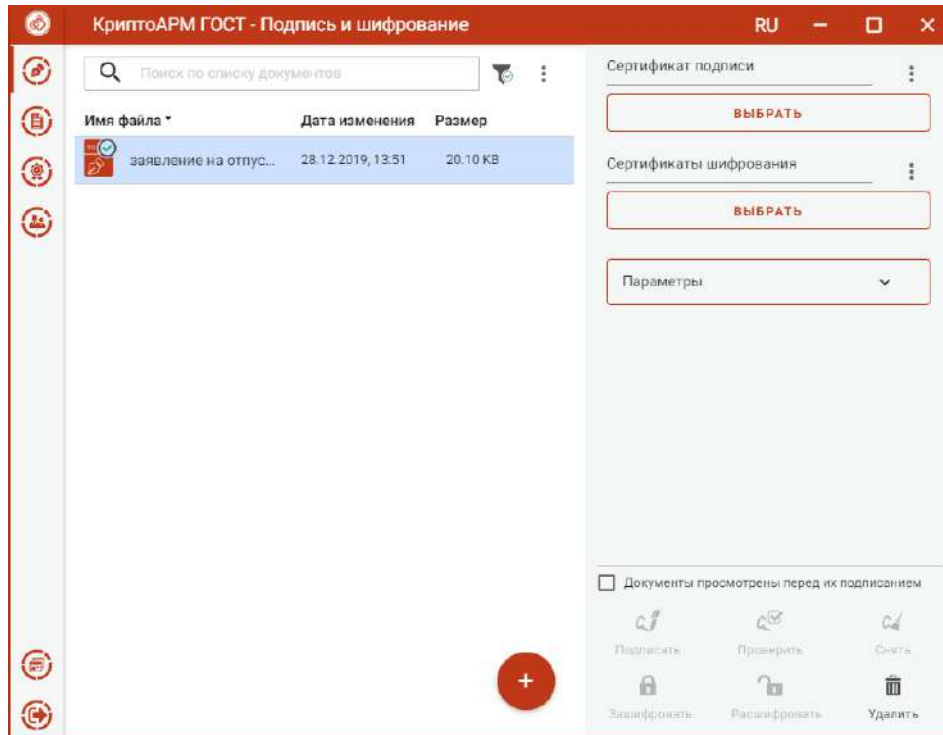


Рис. 5.11.6 Результат применения фильтрации файлов

Для сброса заданных критериев фильтрации служит кнопка «Сбросить» в окне настроек фильтрации (рис. 5.11.5).

## 5.12. 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 **Локальное хранилище** в меню **Документы** (рис. 5.12.1).

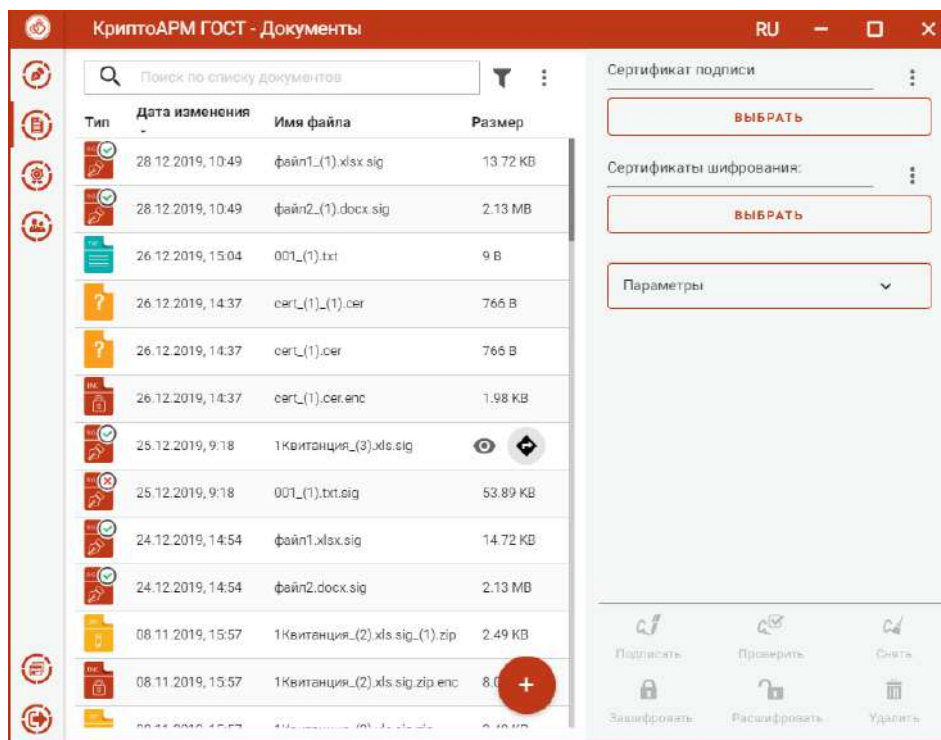


Рис. 5.12.1 Список документов

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. 5.12.2), состоящее из пунктов:

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

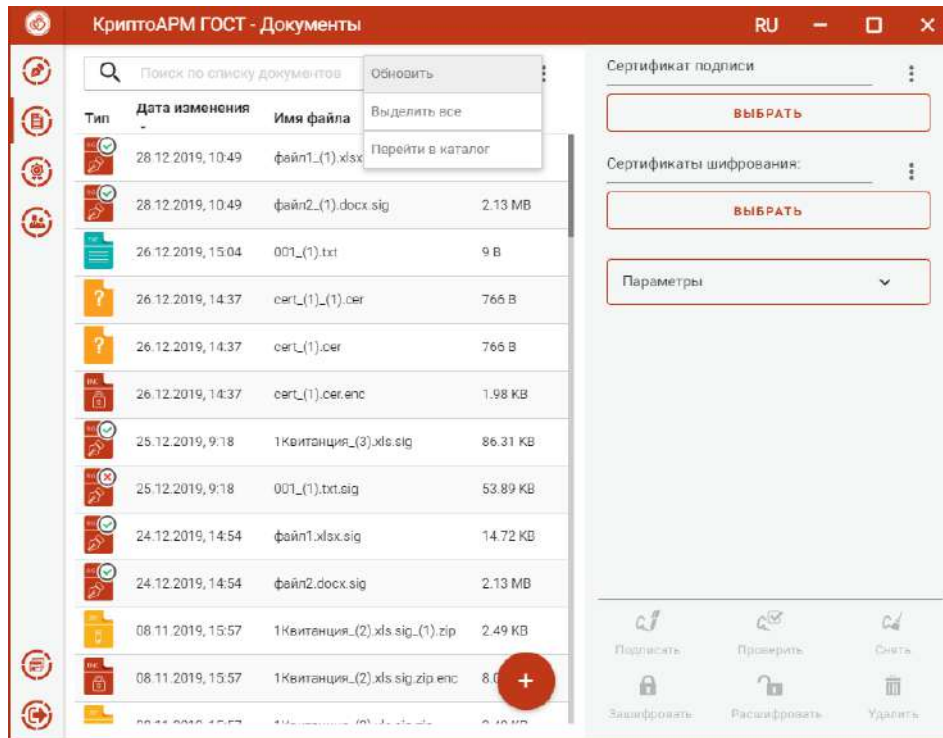


Рис. 5.12.2 Контекстное меню списка Документов

Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши (рис. 5.12.3):

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

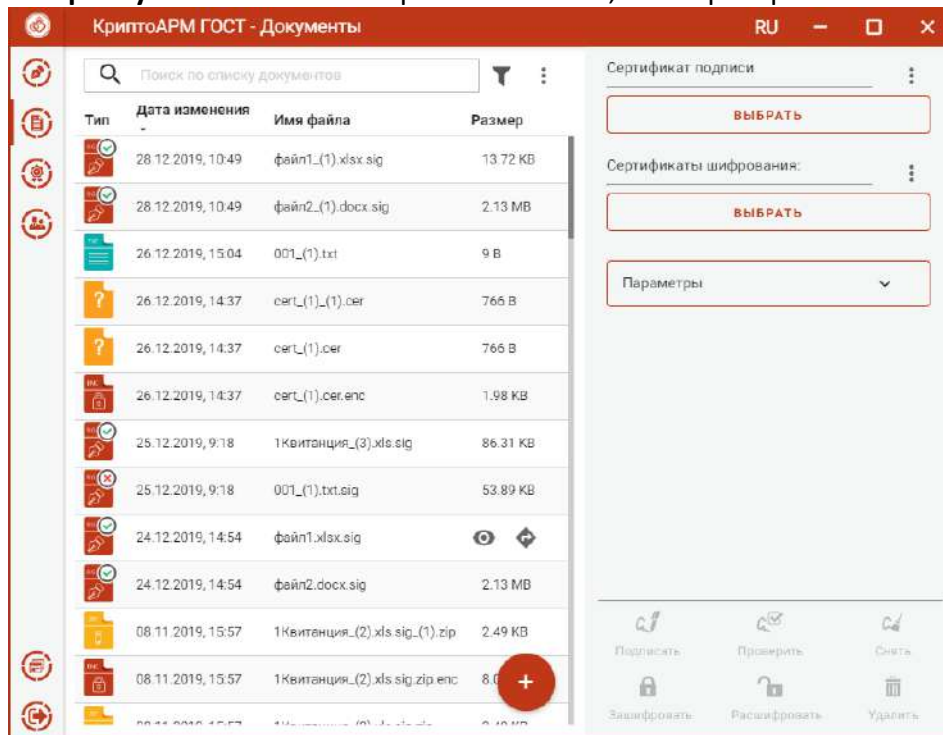


Рис. 5.12.3 Кнопки операций документа

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. 5.12.4)

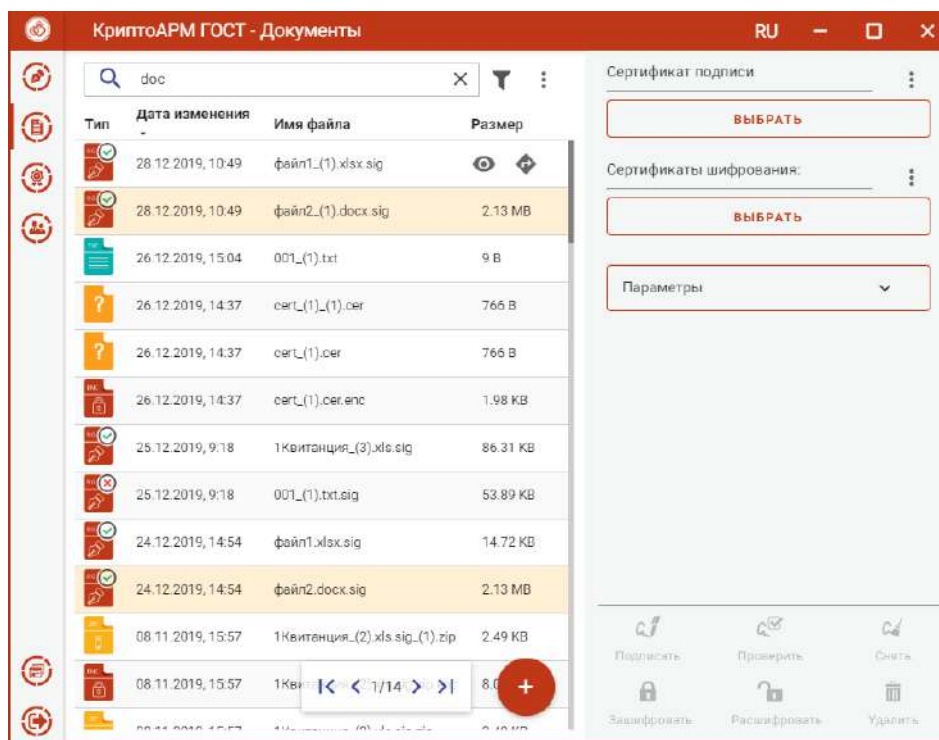


Рис. 5.12.4 Поиск документов

Список документов можно отфильтровать, задав настройки фильтрации (рис. 5.12.5).

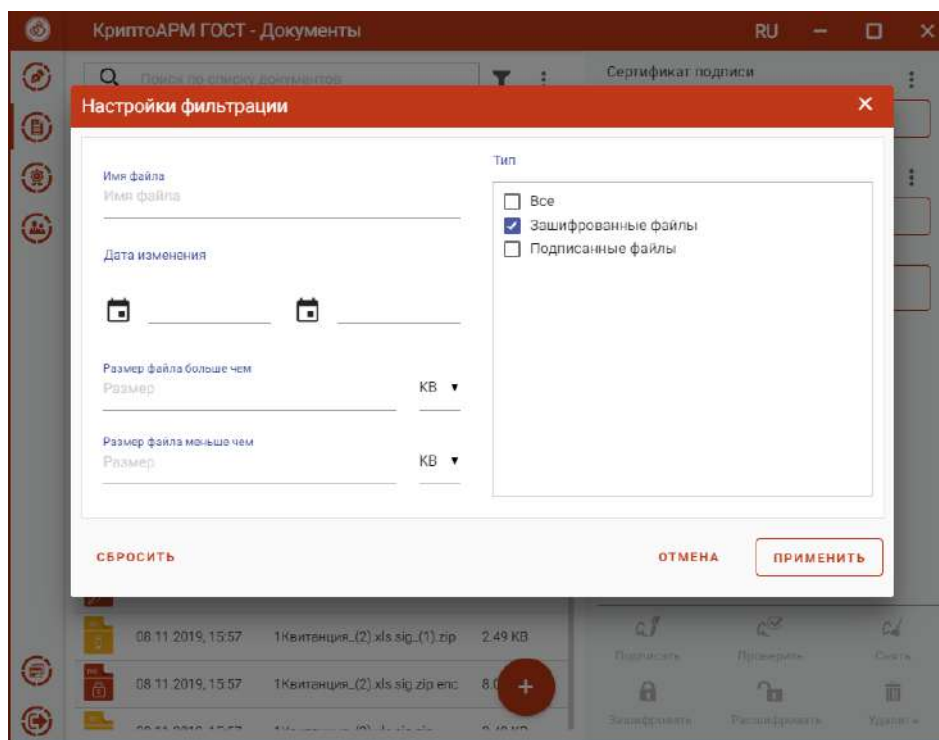


Рис. 5.12.5 Настройки критериев фильтра документов

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.



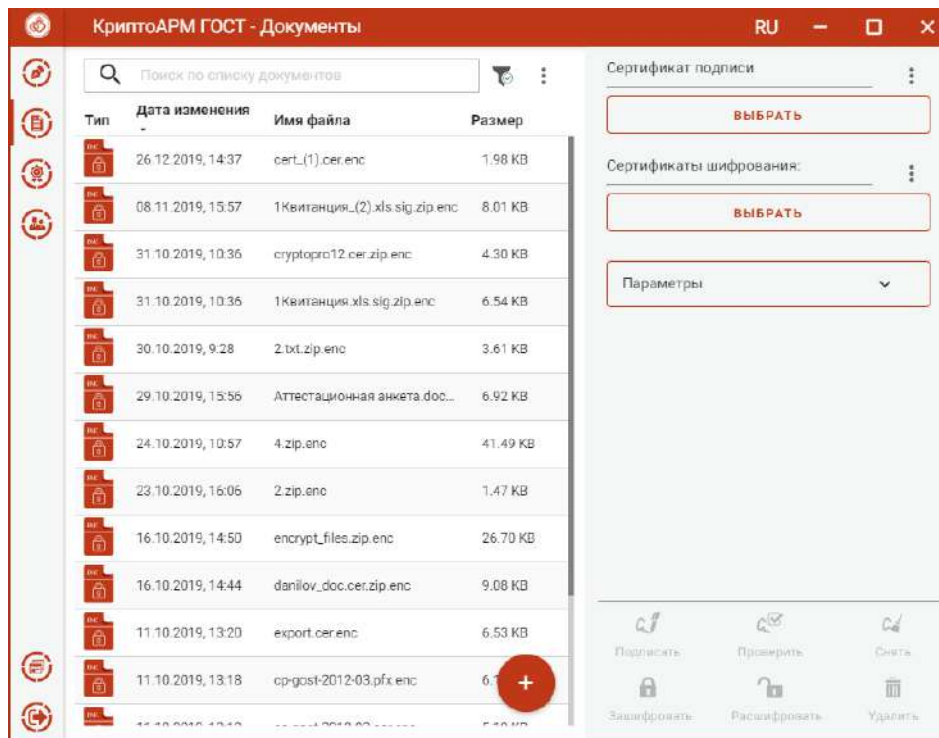


Рис. 5.12.6 Результат применения фильтрации документов

Для сброса заданных критериев фильтрации служит кнопка «Сбросить» в окне настроек фильтрации (рис. 5.12.5).

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. 5.12.7):

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

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

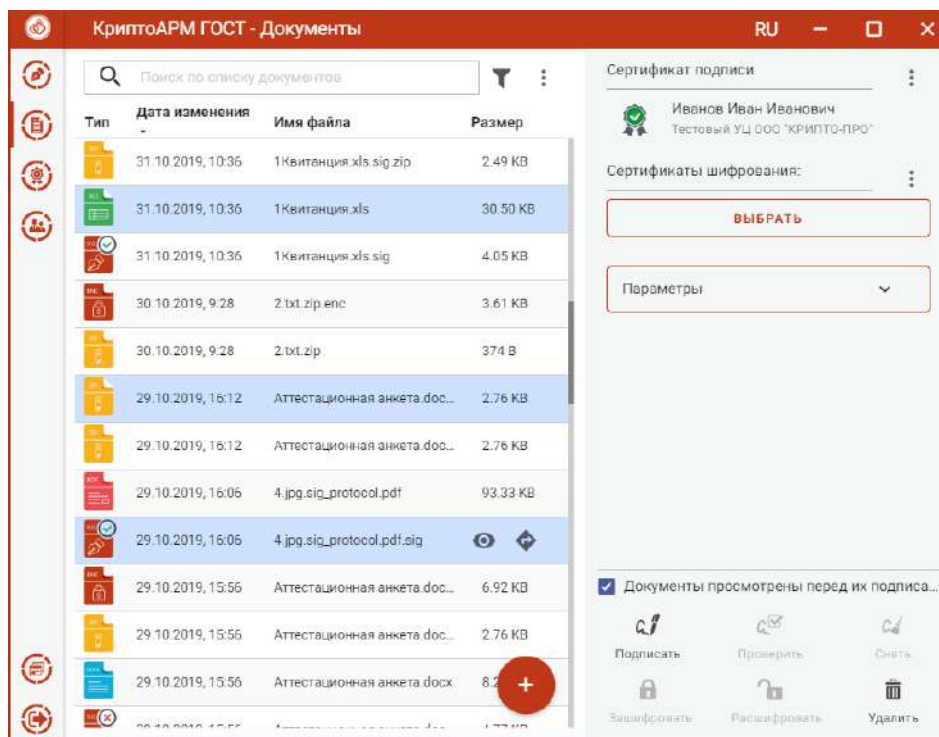


Рис. 5.12.7 Доступные операции для документов

### 5.13. СЕРТИФИКАТЫ

Для управления сертификатами в приложении добавлен отдельный пункт меню **Сертификаты**. При выборе данного пункта открывается список личных сертификатов и подменю с категориям сертификатов (рис. 5.13.1).

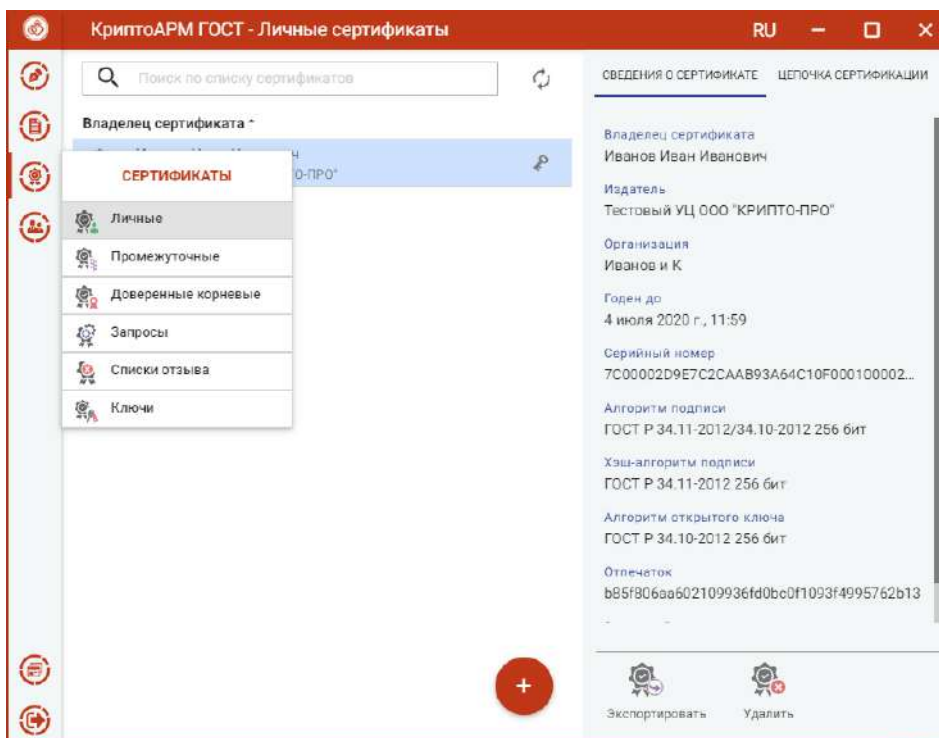


Рис. 5.13.1 Список личных сертификатов с подменю

Подменю содержит пункты:



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

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

При отображении сертификатов, они проверяются на корректность (математическая корректность и построение цепочки доверия). Если к сертификату привязан закрытый ключ, то отображается знак ключа. Облачные сертификаты выделены знаком облака. Возможно появление одного из двух статусов проверки сертификата: сертификат корректный, сертификат не корректный.

После выбора сертификата в списке отображается информация о нем (рис. 5.13.2).

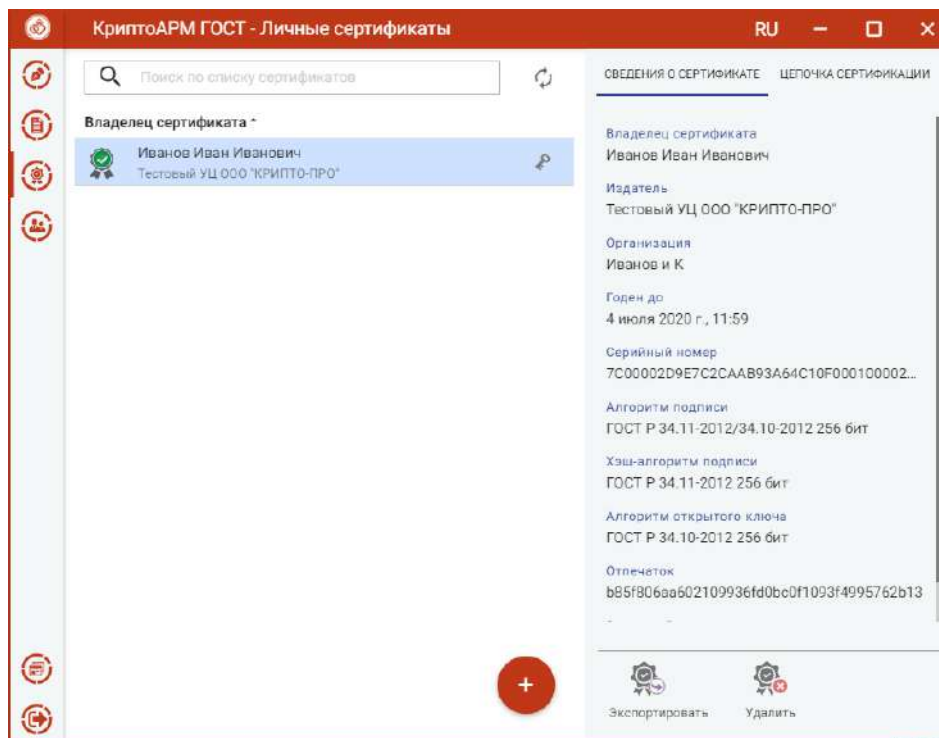


Рис. 5.13.2 Отображение сведений о выбранном сертификате

На вкладке **Цепочка сертификации** отображается общий статус построения цепочки доверия и приводится «дерево» сертификации (рис. 5.13.3).

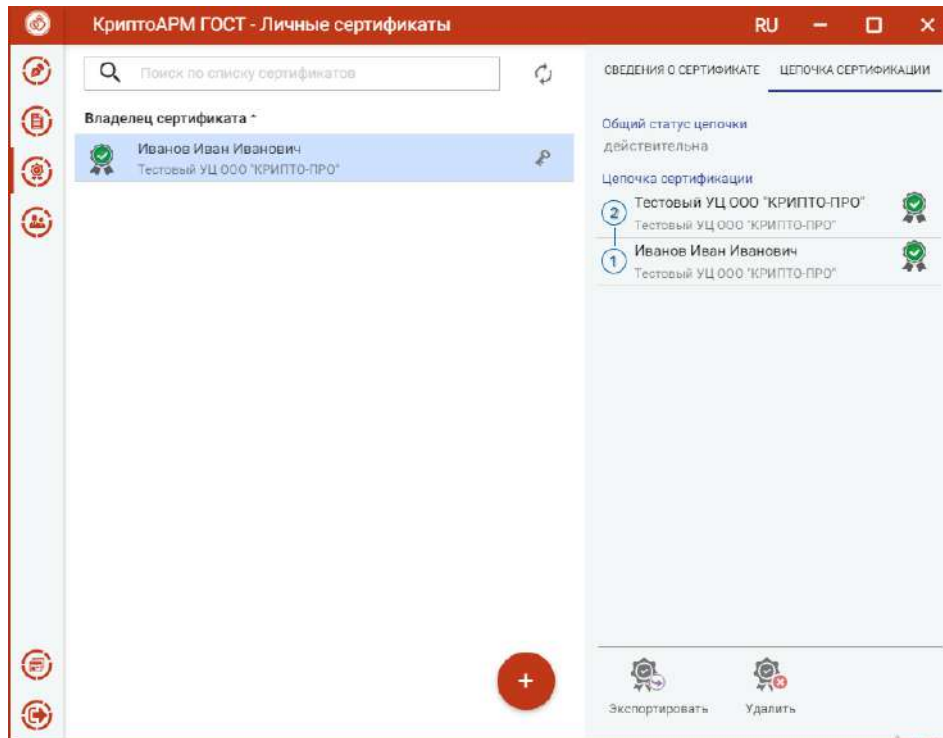


Рис. 5.13.3 Представление цепочки сертификации (цепочки доверия)

### 5.13.1. ИМПОРТ СЕРТИФИКАТА ИЗ ФАЙЛА

**ИМПОРТ ЛИЧНОГО СЕРТИФИКАТА С ПРИВЯЗКОЙ К ЗАКРЫТОМУ КЛЮЧУ.** Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»). В открывшемся окне нужно выбрать операцию **Импорт из файла** (рис. 5.13.4).

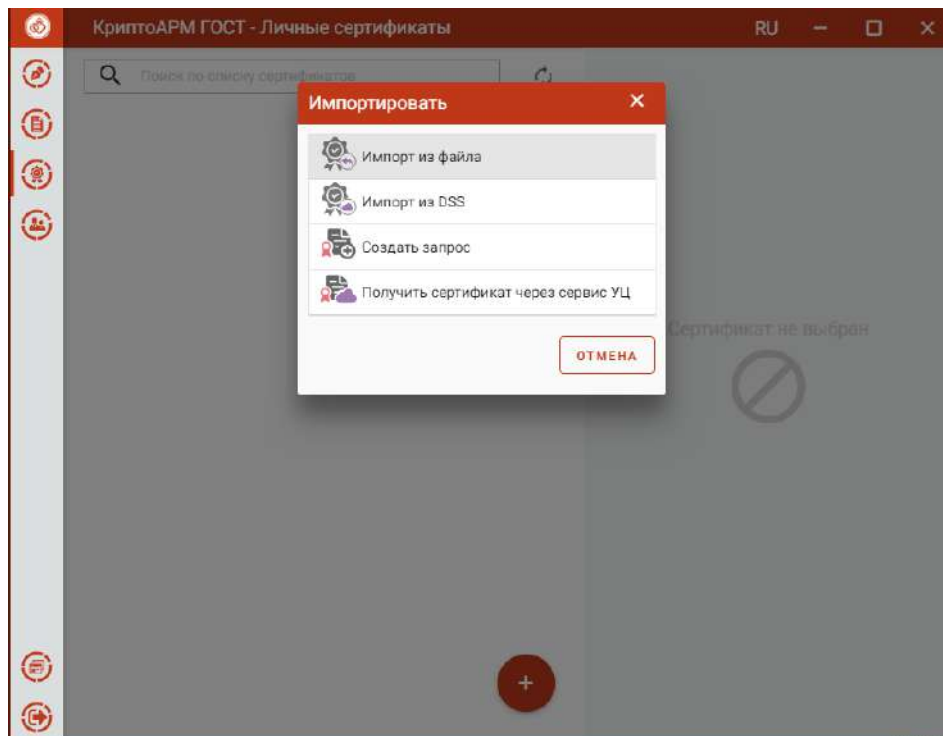


Рис. 5.13.4 Меню выбора способа добавления сертификатов



В появившемся диалоговом окне нужно выбрать файл сертификата. Это может быть файл формата rfx, содержащий ключевую пару (закрытый ключ и сертификат), или обычный сертификат, у которого есть закрытый ключ.

При успешном выполнении операции импорта сертификат автоматически помещается в личные сертификаты (рис. 5.13.5).

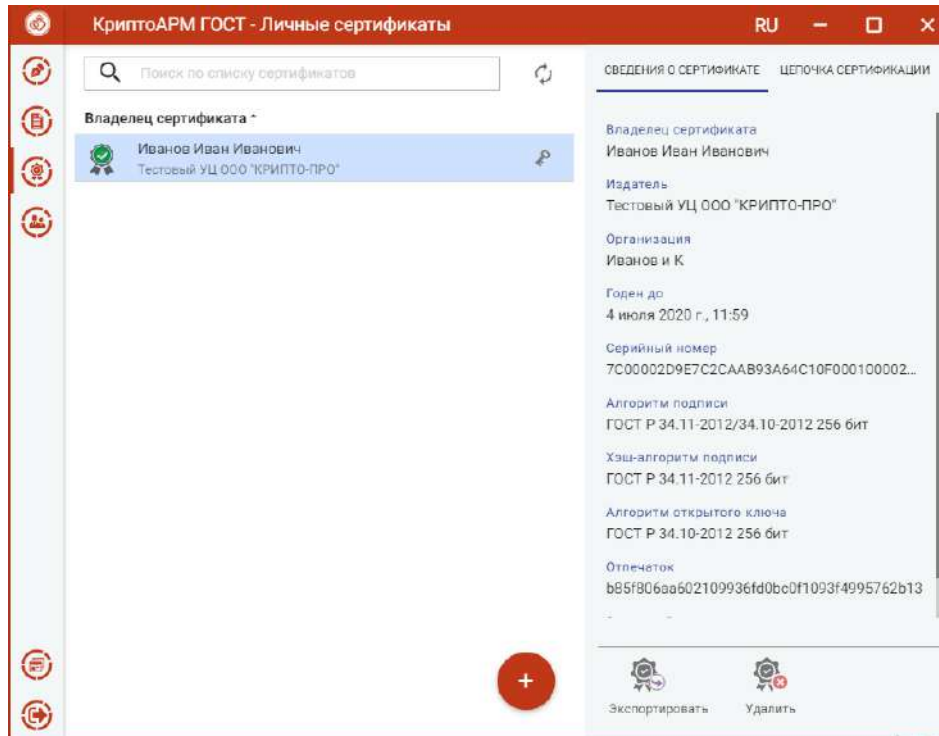


Рис. 5.13.5 Отображение импортированного личного сертификата

Если при импорте не будет найден закрытый ключ, соответствующий сертификату, то возникнет сообщение с предложением установить данный сертификат в подходящее хранилище или принудительно в выбранное (рис. 5.13.6). Если сертификат без закрытого ключа будет установлен в личное хранилище, то данным сертификатом нельзя будет подписывать и расшифровывать файлы.

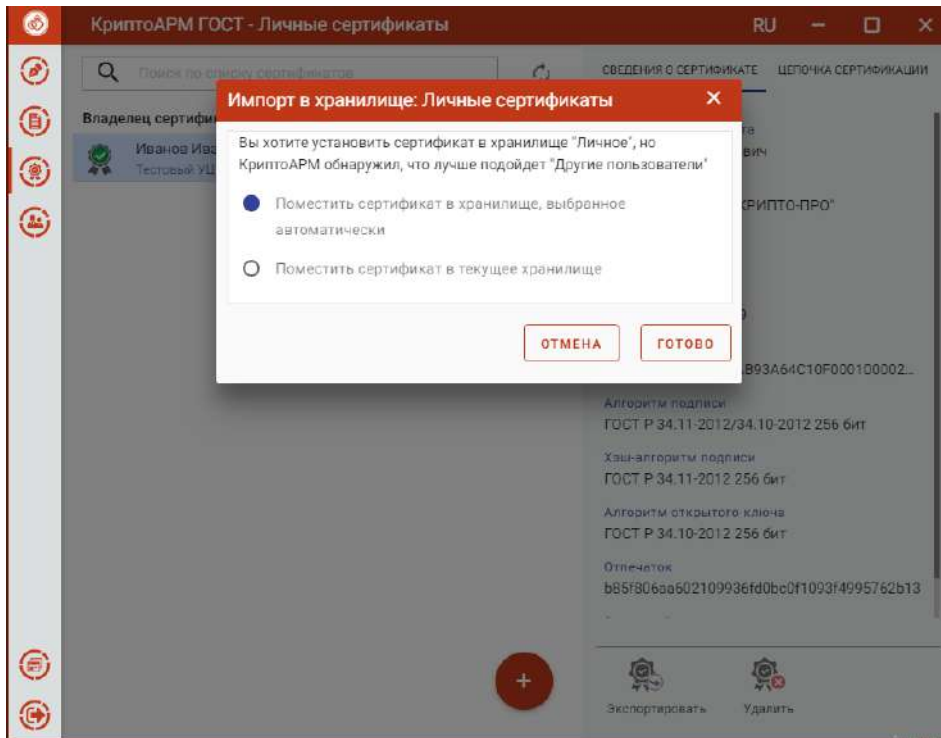


Рис. 5.13.6 Выбор хранилища для установки сертификата

**ИМПОРТ СЕРТИФИКАТА БЕЗ ПРИВЯЗКИ К ЗАКРЫТОМУ КЛЮЧУ.** Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+») и выбора опции **Импорт из файла** (рис. 5.13.7).

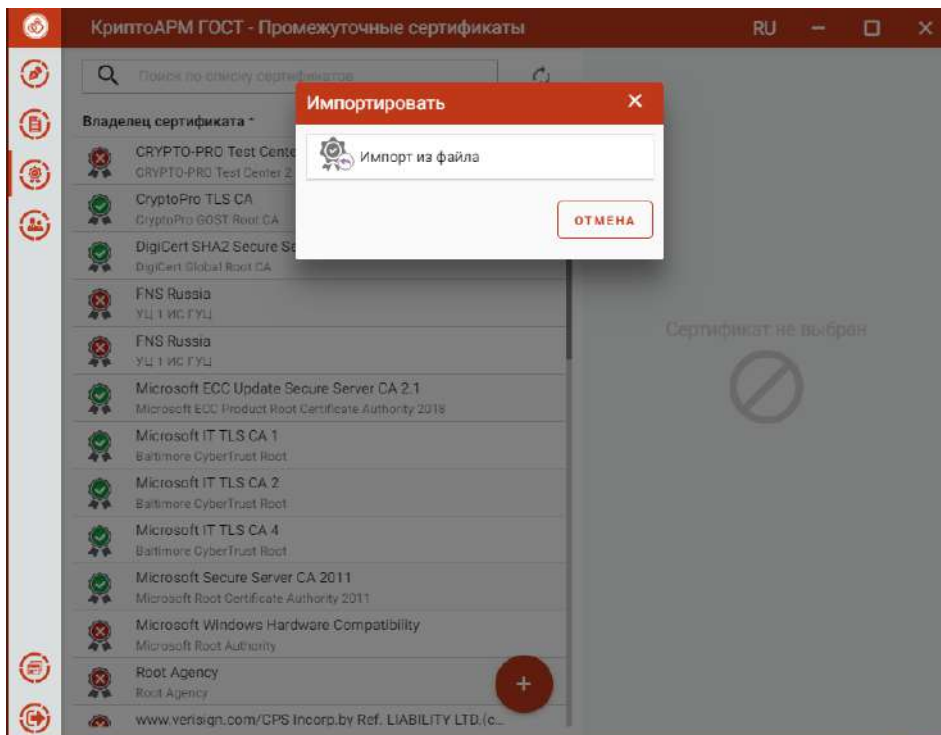


Рис. 5.13.7 Импорт сертификата из файла

В появившемся диалоговом окне нужно выбрать файл сертификата.

При успешном выполнении операции импорта сертификат автоматически помещается в выбранное хранилище (рис. 5.13.8).



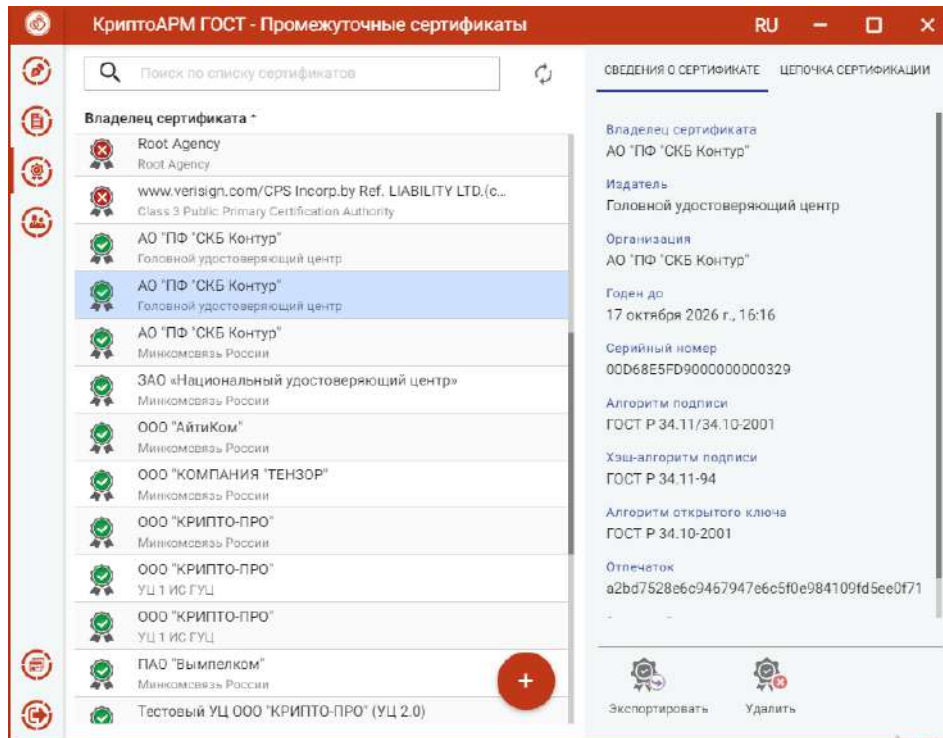


Рис. 5.13.8 Отображение импортированного сертификата

Если при импорте приложение определило, что для данного сертификата лучше подойдет другое хранилище, то возникнет сообщение с предложением установить сертификат в подходящее хранилище или принудительно в выбранное (рис. 5.13.9).

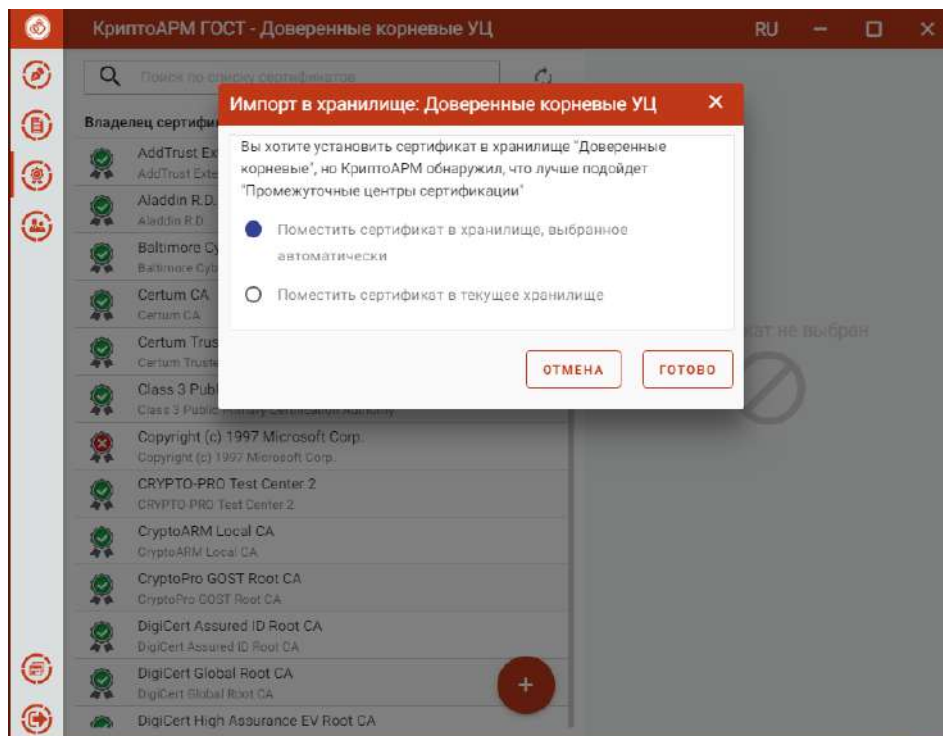


Рис. 5.13.9 Выбор хранилища для установки сертификата



### 5.13.2. ИМПОРТ СЕРТИФИКАТА ИЗ DSS

Для выполнения импорта сертификата из DSS в хранилище можно воспользоваться кнопкой добавления сертификата («+»). В открывшемся окне нужно выбрать операцию **Импорт из DSS** (рис. 5.13.4). Данная опция при импорте доступна только для категории личных сертификатов.

Открывается окно для ввода адресов серверов авторизации и DSS, логина и пароля для аутентификации (рис. 5.13.10).

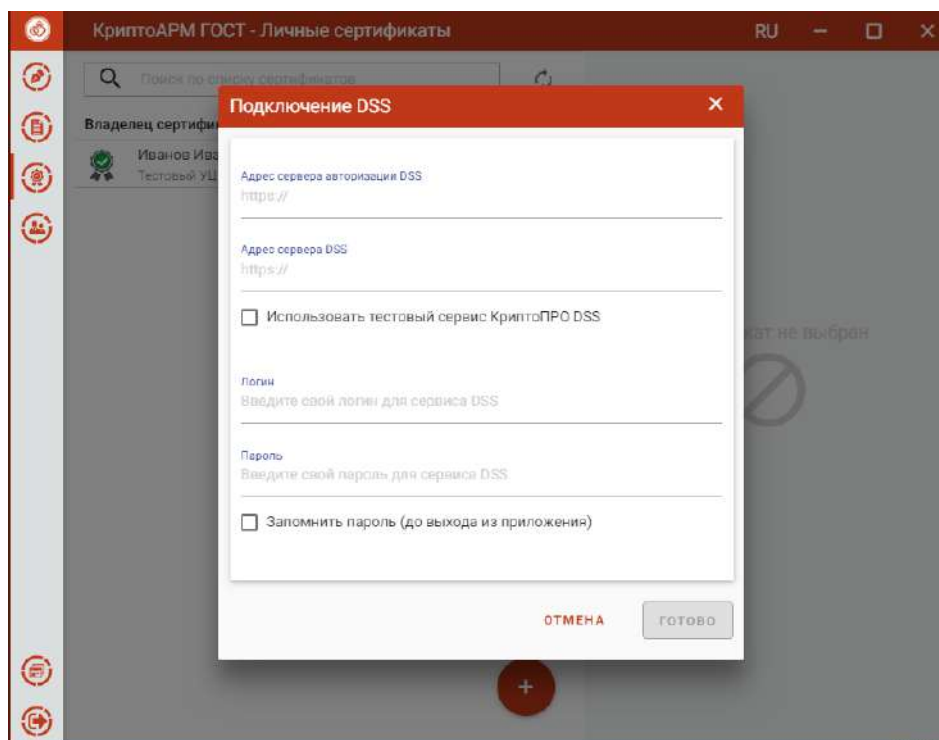


Рис. 5.13.10 Настройка адресов серверов DSS

Если у пользователя в личном кабинете DSS в настройках стоит подтверждение аутентификации по SMS, электронной почте или с помощью мобильного приложения, то при нажатии на кнопку **Готово** появляется сообщение, что операцию нужно подтвердить (рис. 5.13.11). Если нет, то данный шаг пропускается.

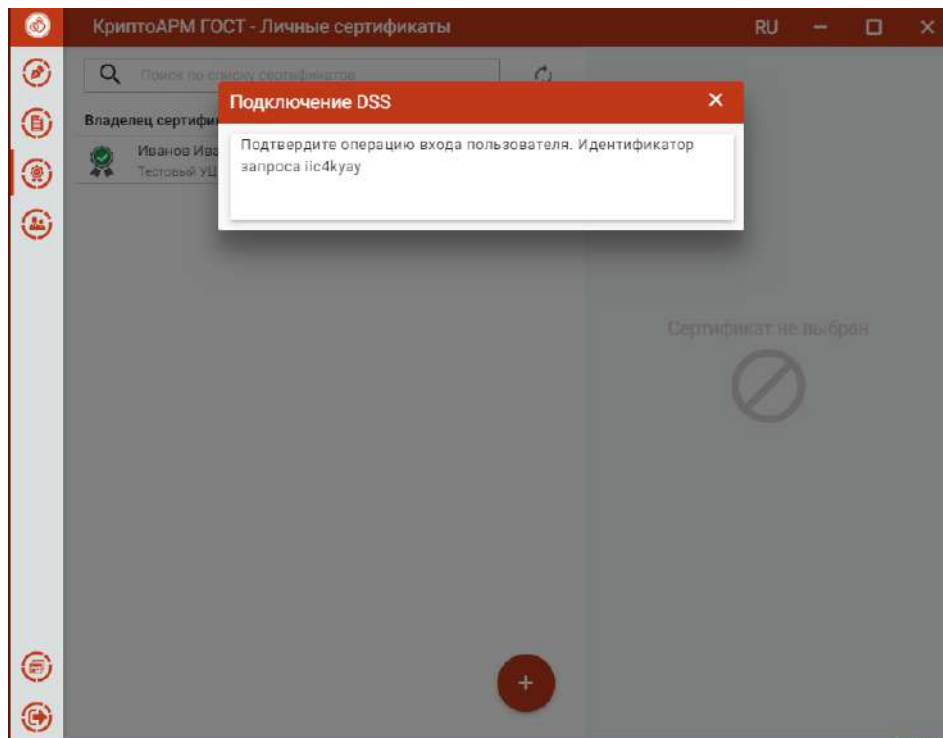


Рис. 5.13.11 Окно запроса подтверждения входа

При успешной аутентификации на следующем шаге сертификаты DSS автоматически помещаются в хранилище личных сертификатов (рис. 5.13.12).

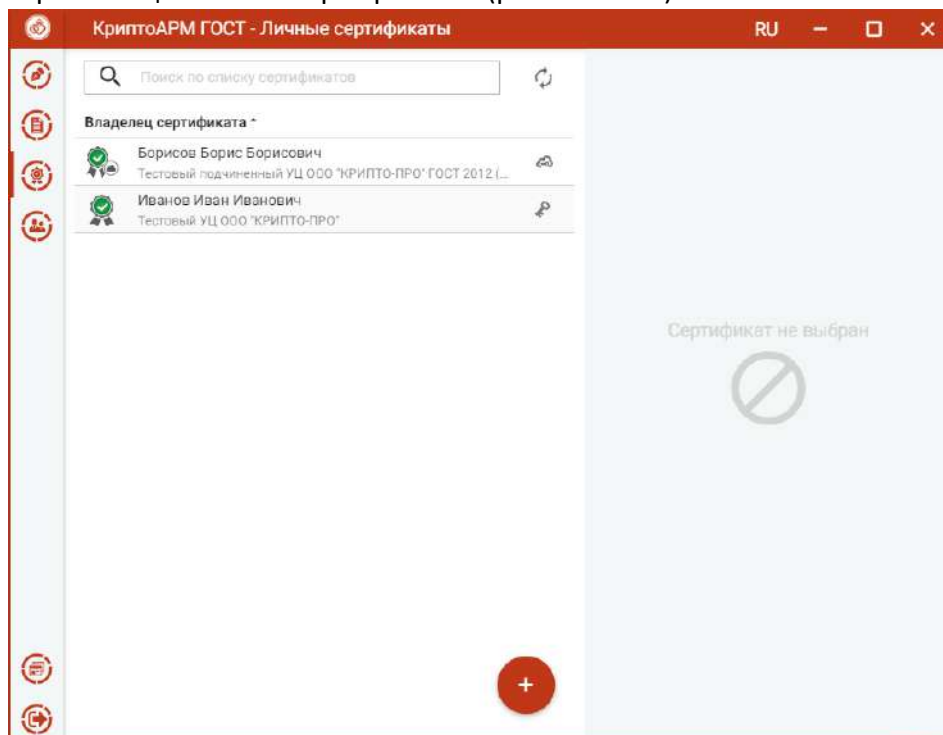


Рис. 5.13.12 Отображение импортированного DSS сертификата

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



### 5.13.3. ЭКСПОРТ СЕРТИФИКАТА В ФАЙЛ

Для экспорта сертификата в файл нужно выделить сертификат и нажать кнопку операции **Экспортировать** (рис. 5.13.13). Если у сертификата экспортируемый закрытый ключ, то такой сертификат можно экспортировать вместе с закрытым ключом.

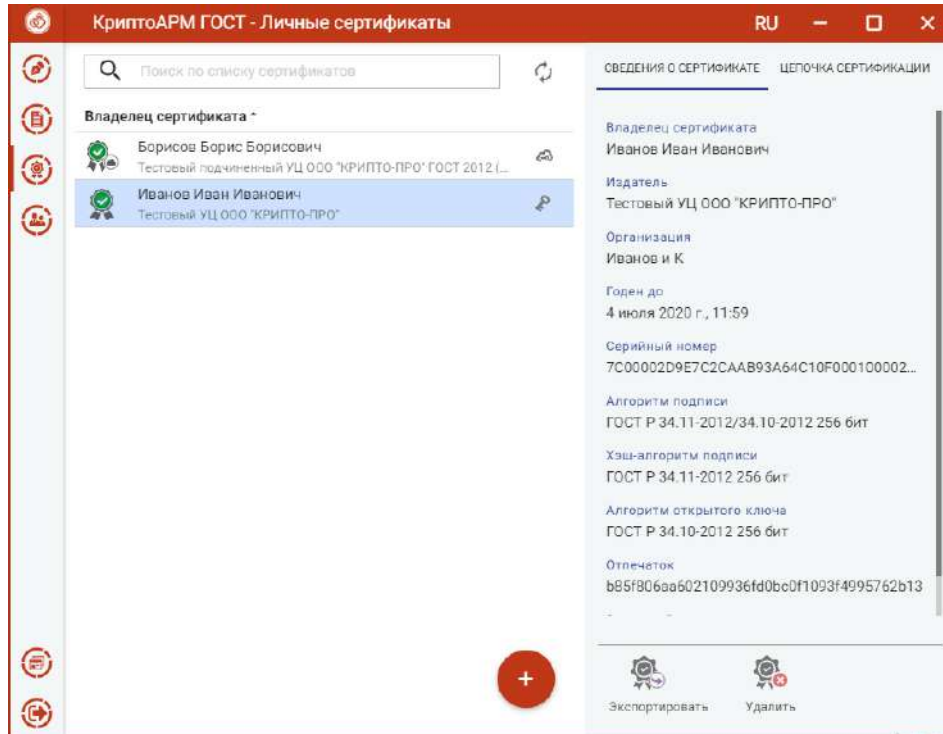


Рис. 5.13.13 Экспорт сертификата

При экспорте сертификата с не экспортируемым закрытым ключом появляется окно, в котором можно выбрать только кодировку файла сертификата (рис. 5.13.14).

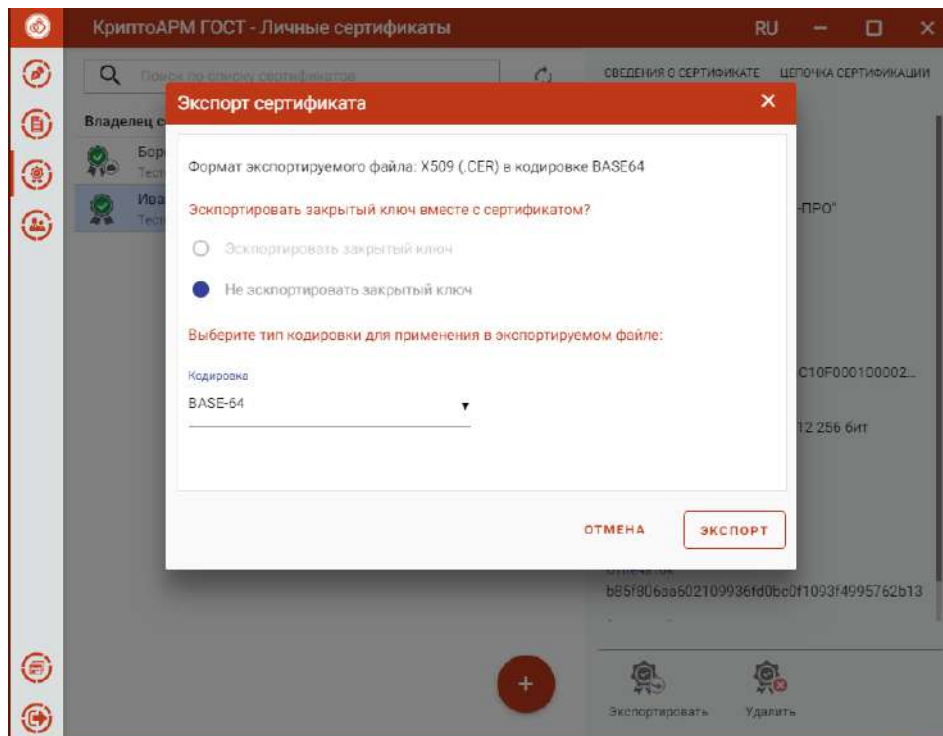


Рис. 5.13.14 Выбор кодировки файла сертификата



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. 5.13.14).
- Экспортировать сертификат вместе с закрытым ключом. В таком случае надо указать пароль для защиты закрытого ключа (рис. 5.13.15).

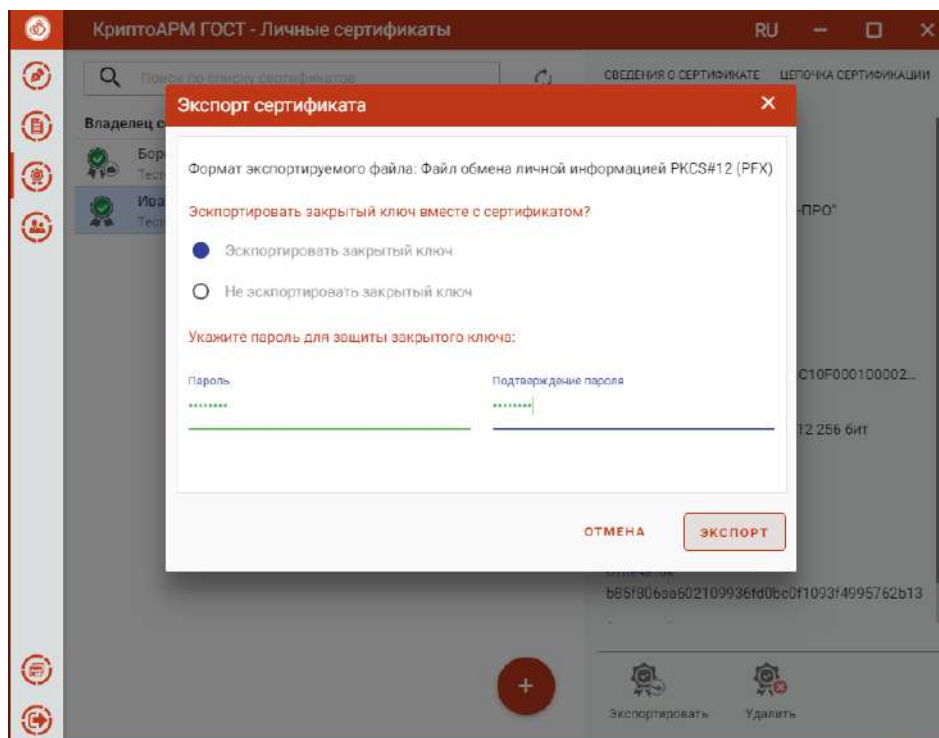


Рис. 5.13.15 Экспорт сертификата вместе с закрытым ключом

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.



#### 5.13.4. УДАЛЕНИЕ СЕРТИФИКАТА

Для удаления сертификата нужно выбрать операцию **Удалить** (рис. 5.13.16).

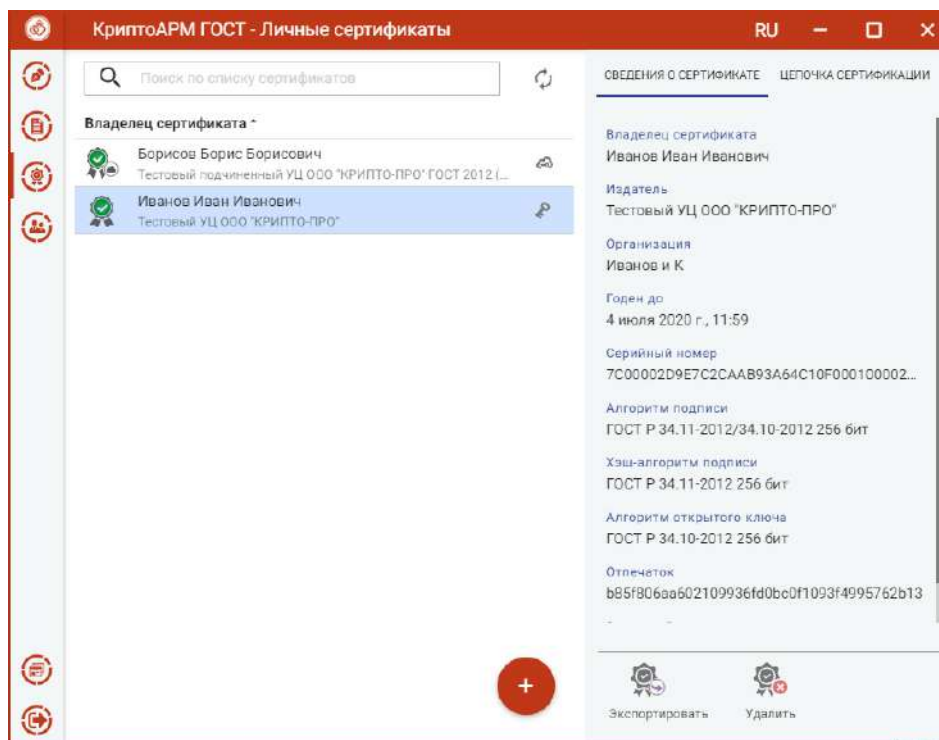


Рис. 5.13.16 Удаление сертификата

В появившемся диалоговом окне нажать **Удалить** для подтверждения удаления (рис. 5.13.17).

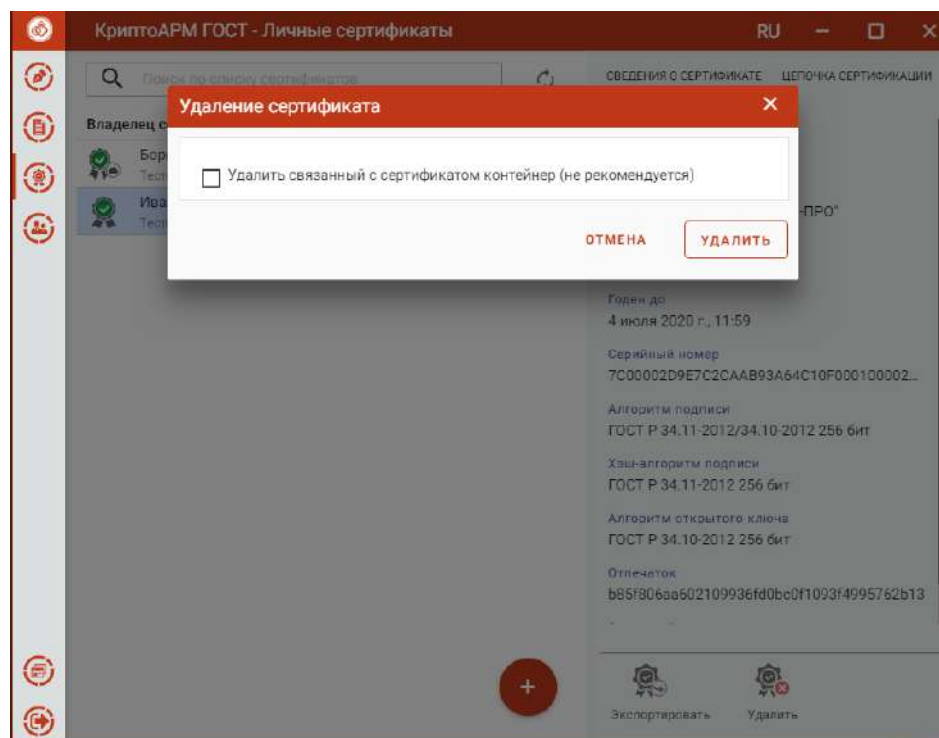


Рис. 5.13.17 Подтверждение удаления сертификата

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.

### 5.13.5. СОЗДАНИЕ ЗАПРОСА НА СЕРТИФИКАТ

Для создания запроса на сертификат в окне добавления сертификата следует выбрать операцию **Создать запрос** (рис. 5.13.18). Создать запрос можно со списка личных сертификатов (рис. 5.13.18) или со списка запросов (рис. 5.13.19)

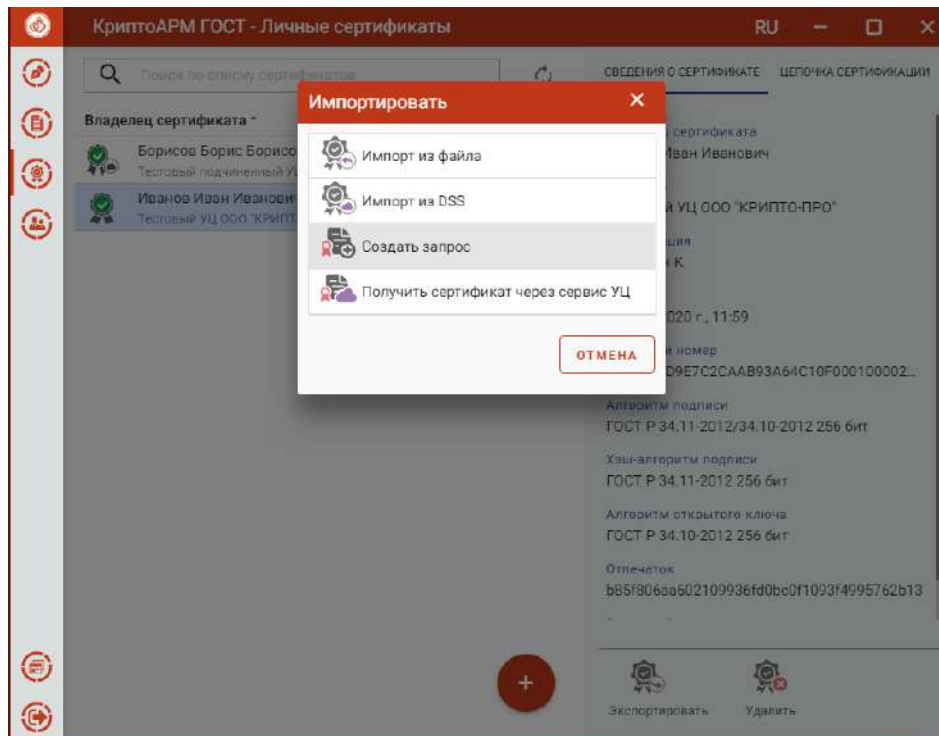


Рис. 5.13.18 Создание запроса на сертификат в списке личных сертификатов

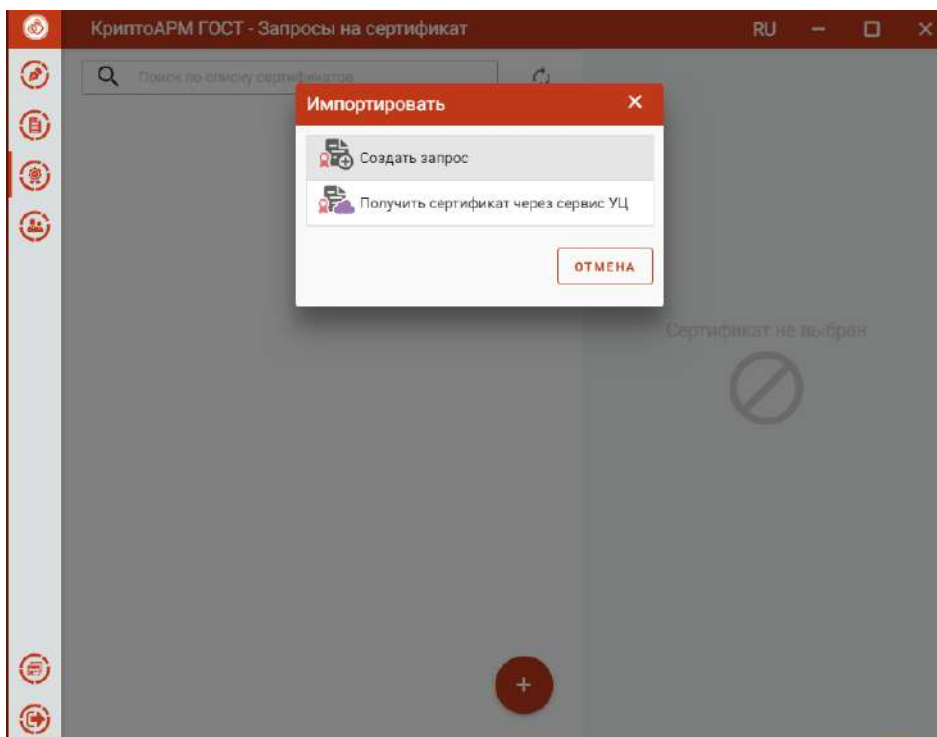


Рис. 5.13.19 Создание запроса на сертификат в списке запросов

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

В параметрах субъекта указывается:

- Шаблон сертификата (рис. 5.13.20);

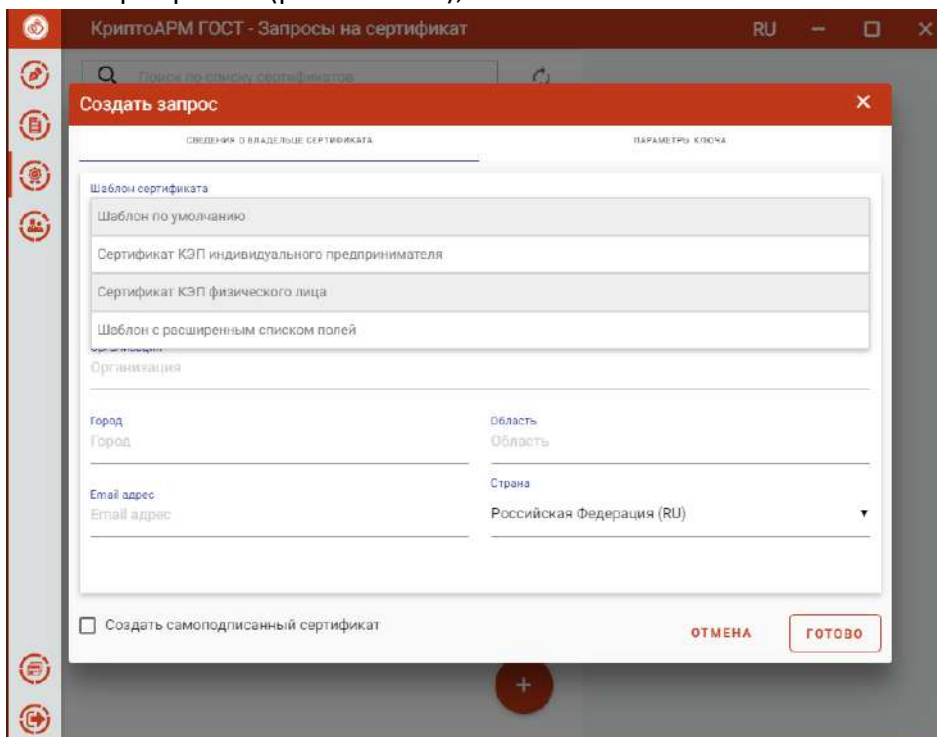


Рис. 5.13.20 Выбор шаблона сертификата

- Основная информация, в которой, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце сертификата (рис. 5.13.21).

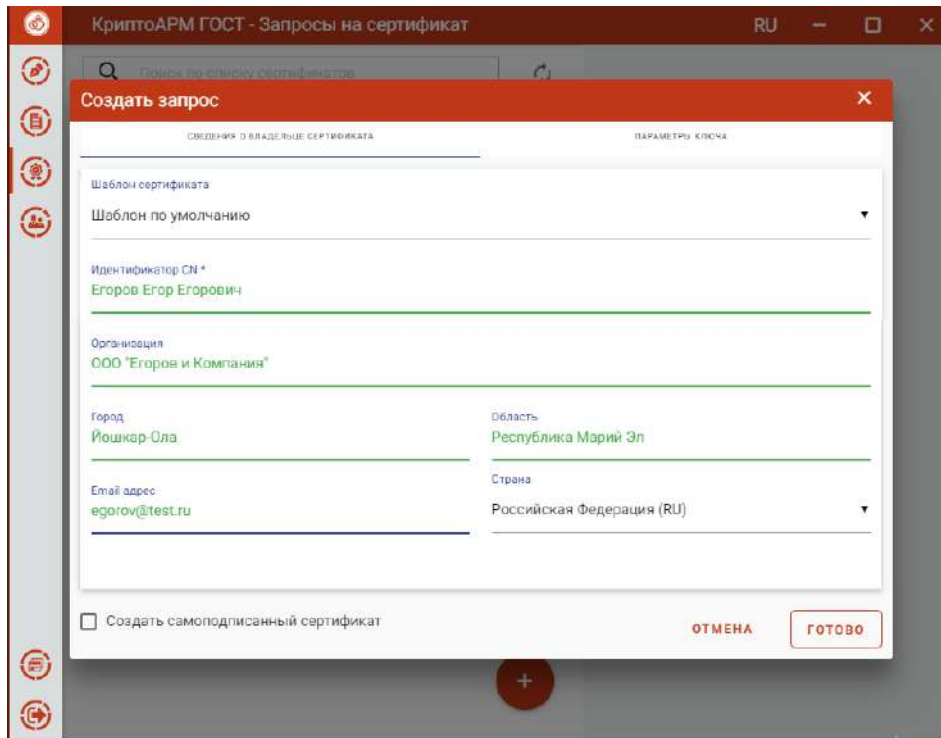


Рис. 5.13.21 Информация о владельце сертификата

- 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. 5.13.22);

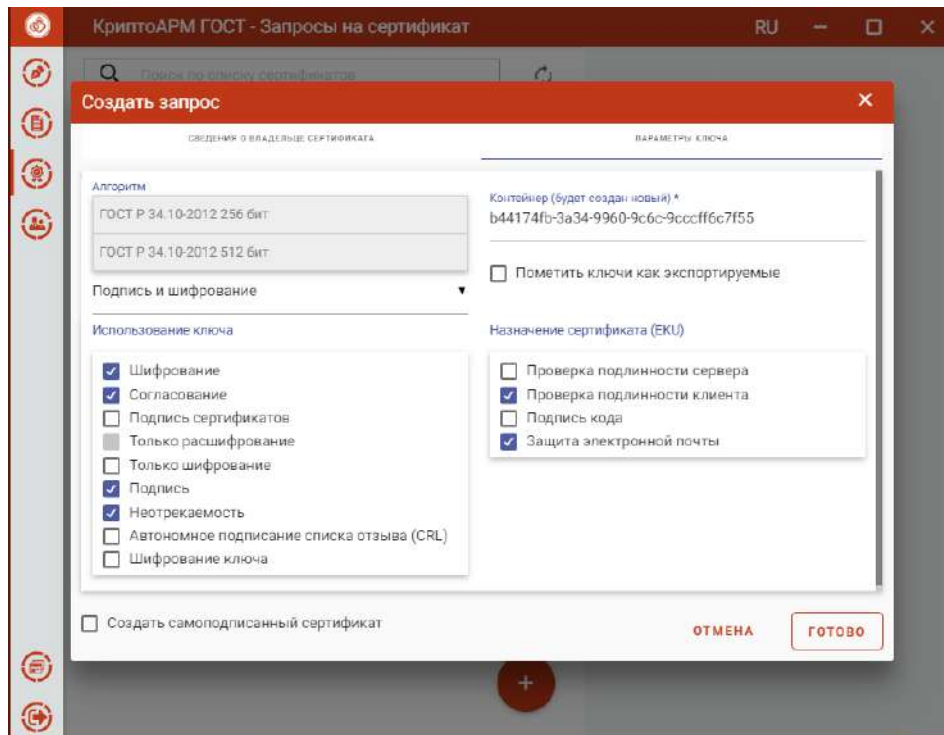


Рис. 5.13.22 Выбор алгоритма ключа

- Назначение ключа (рис. 5.13.23);

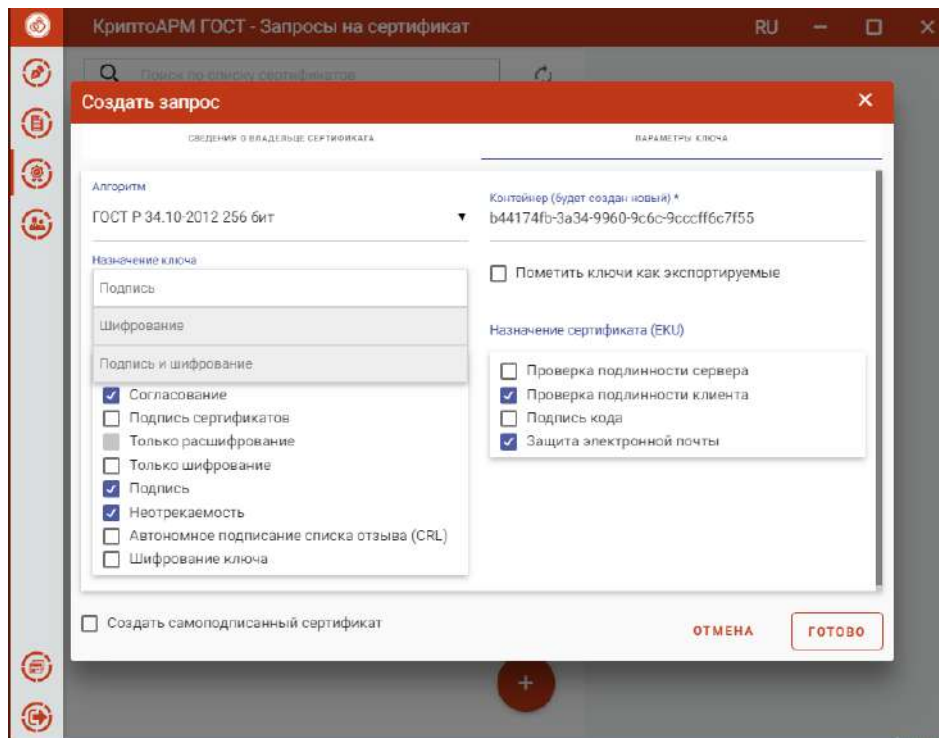


Рис. 5.13.23 Выбор назначения ключа

- Использование ключа (рис. 5.13.24);

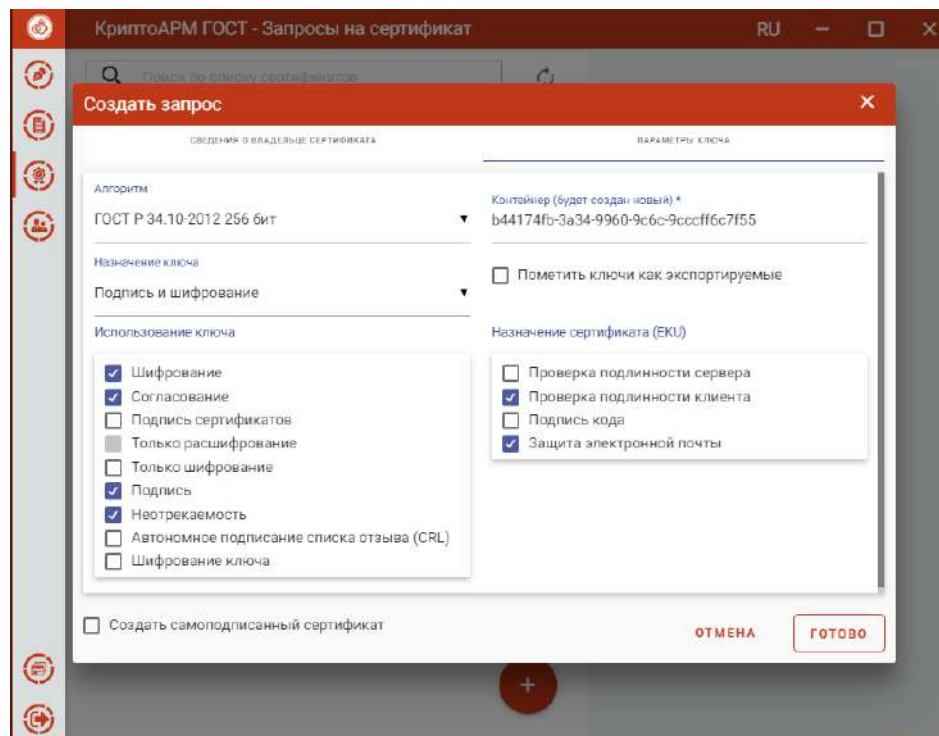


Рис. 5.13.24 Выбор использования ключа

- 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 в подпункте **Запросы** раздела **Сертификаты** (рис. 5.13.25).

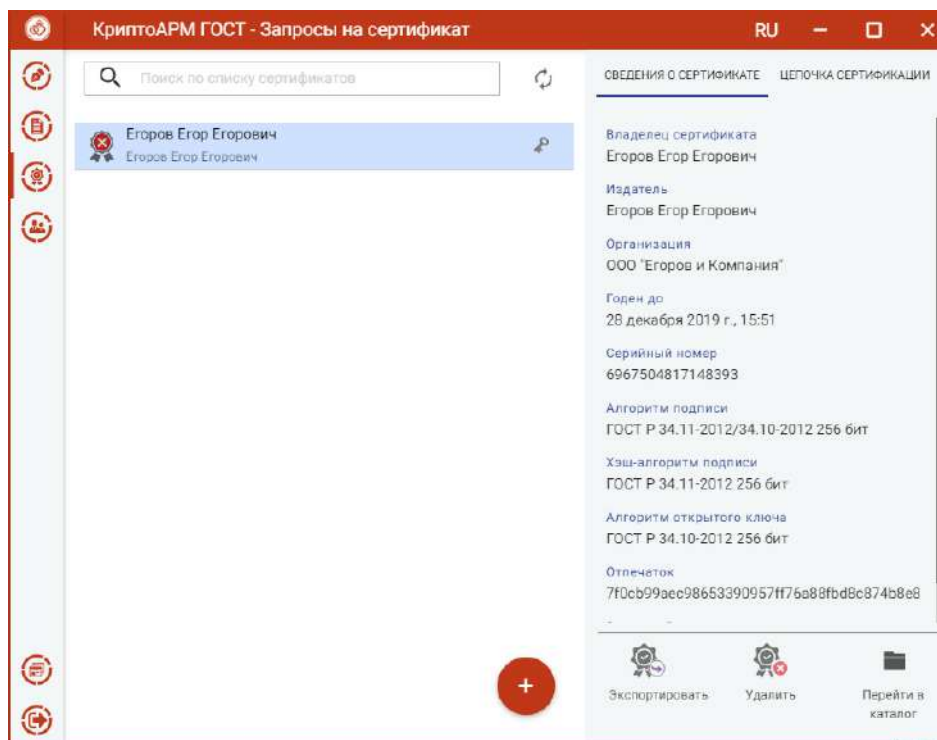


Рис. 5.13.25 Форма просмотра запроса на сертификат

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.

#### 5.13.6. СОЗДАНИЕ САМОПОДПИСАННОГО СЕРТИФИКАТА

Для создания самоподписанного сертификата на форме **Создать запрос** следует поставить флаг **Создание самоподписанного сертификата** (рис. 5.13.26).

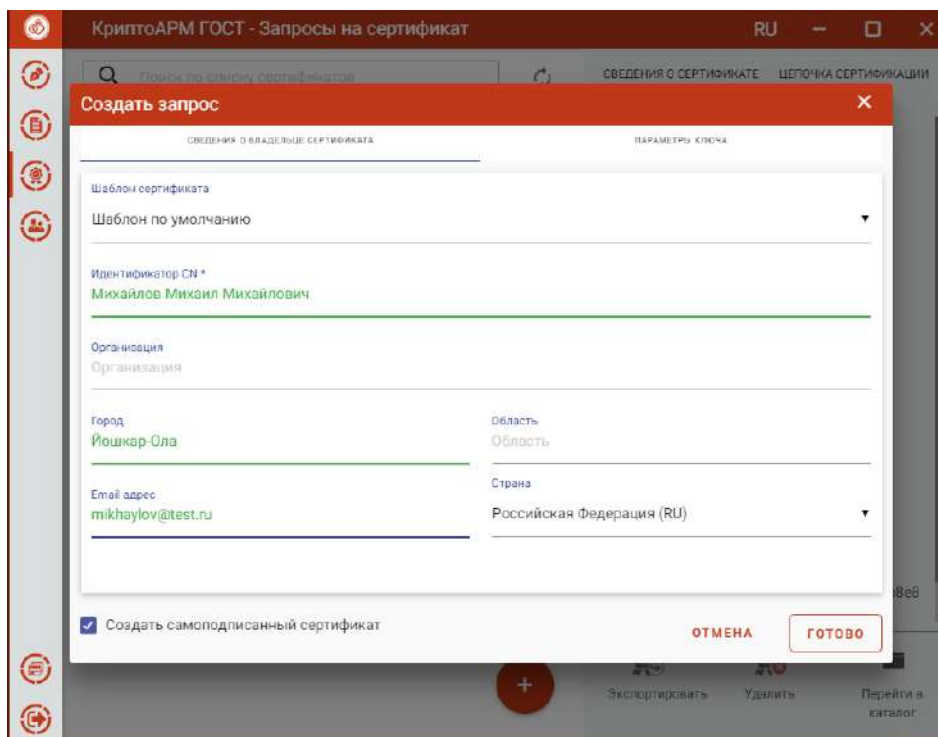


Рис. 5.13.26 Создание самоподписанного сертификата

На основе указанных данных по кнопке **Готово** будет сформирован самоподписанный сертификат. Для сертификата выберите ключевой носитель для хранения контейнера (Реестр, диск, токен). На запрос системы установите пароль на данный контейнер и подтвердите его. После завершения операции возникнет окно с информацией о ее результатах. Сертификат будет в списке Личных сертификатов (рис. 5.13.27)

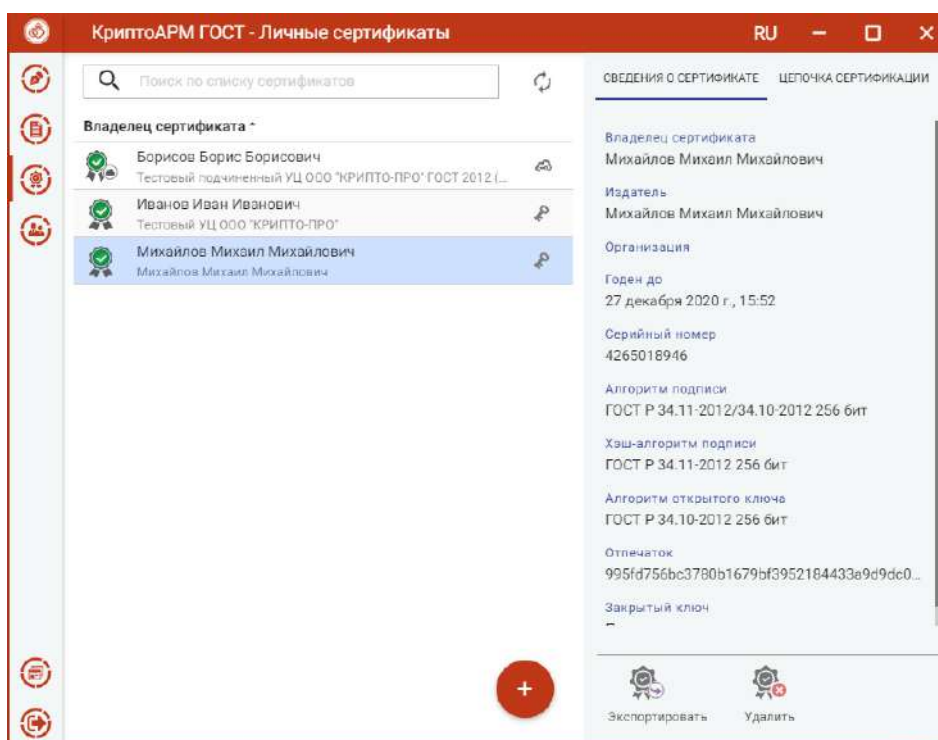


Рис. 5.13.27 Список Личных сертификатов

При генерации самоподписанного сертификата запрос на сертификат не создается.





### 5.13.7. ПОЛУЧИТЬ СЕРТИФИКАТ ЧЕРЕЗ СЕРВИС УЦ

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.

**ДОБАВЛЕНИЕ НОВОГО СЕРВИСА.** Создать подключение можно, выбрав опцию **Получить сертификат через сервис УЦ** при добавлении сертификата в списке личных сертификатов или в списке запросов на сертификат (рис. 5.13.28).

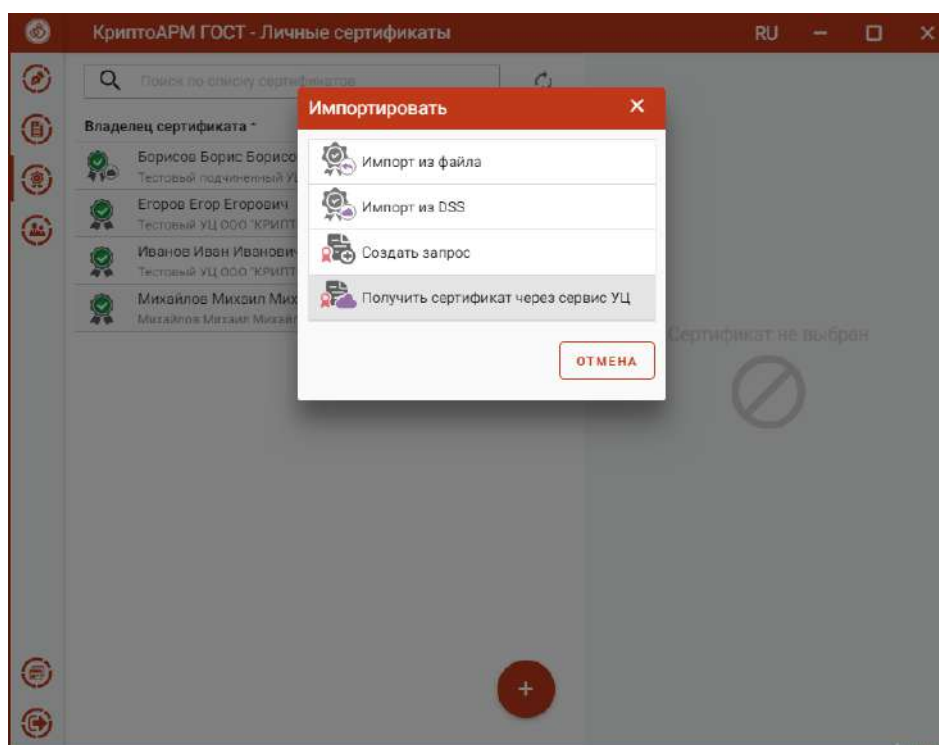


Рис. 5.13.28 Способ добавления подключения.

В открывшемся окне установить флаг **Добавление нового сервиса** и нажать кнопку **Готово** (рис. 5.13.29).

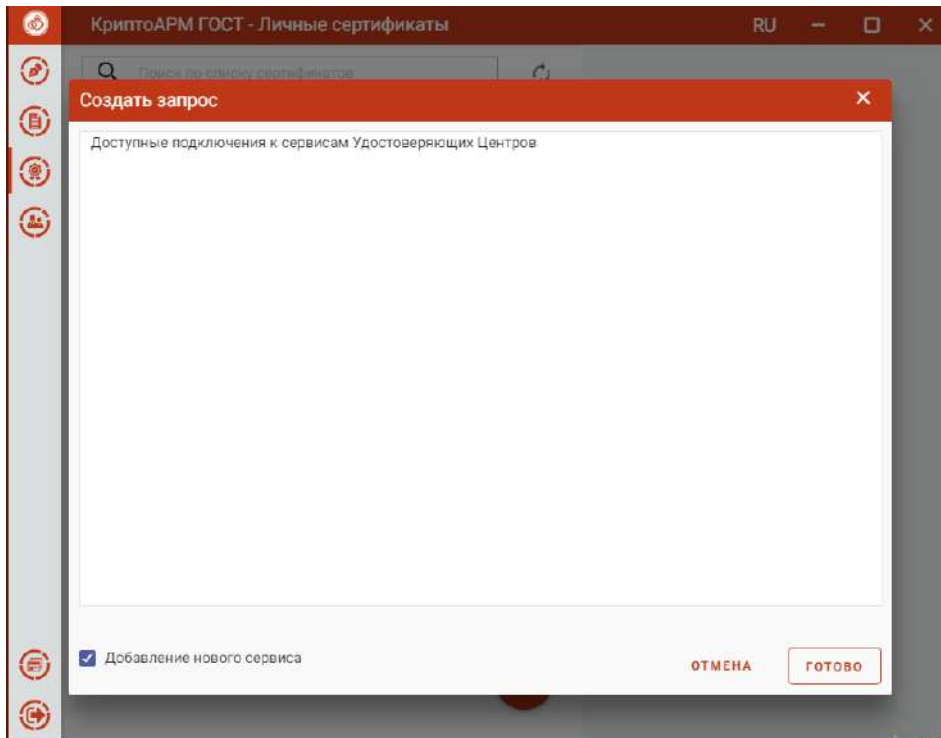


Рис. 5.13.29 Добавление нового сервиса

Еще создать подключение можно, выбрав опцию **Подключить сервис УЦ** при добавлении сертификата в списке доверенных корневых сертификатов (рис. 5.13.30).

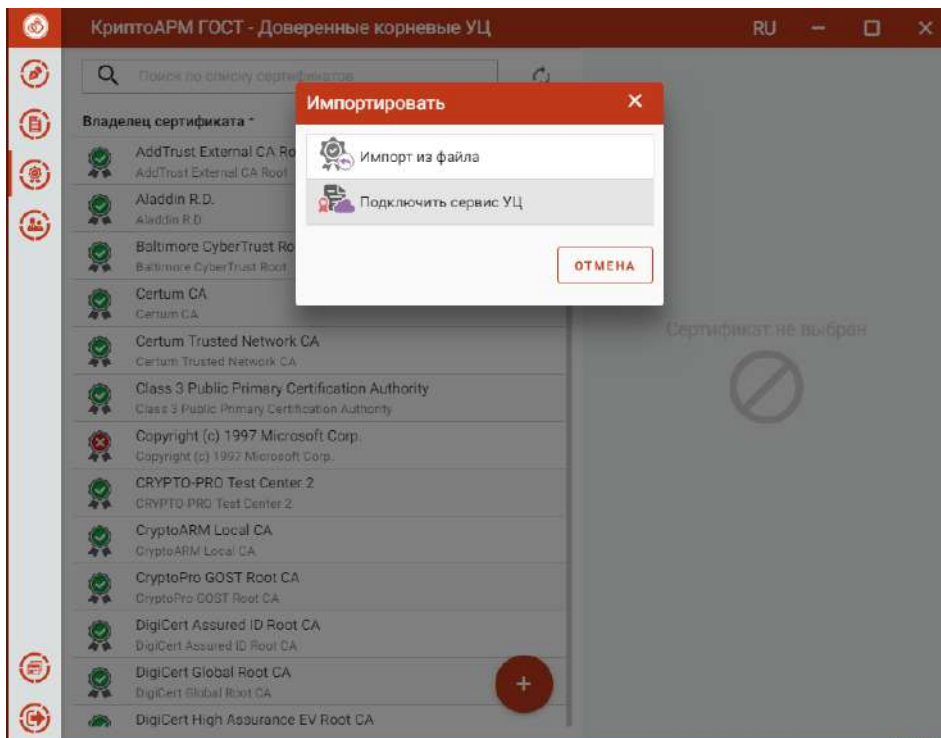


Рис. 5.13.30. Способ добавления подключения

Открывается форма ввода полей для регистрации сервиса (рис. 5.13.31).

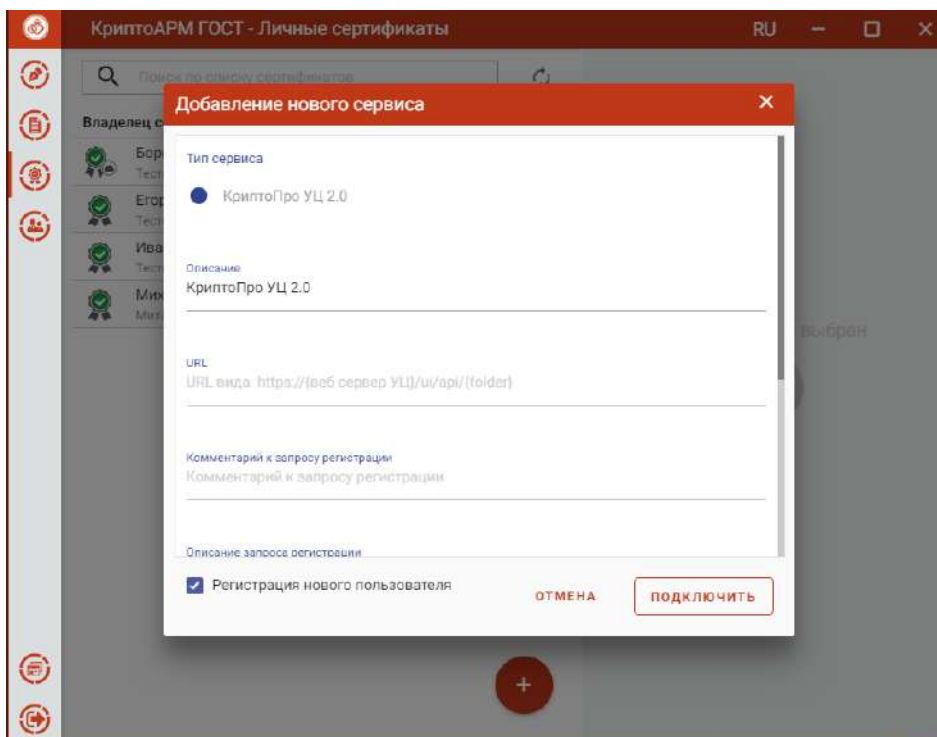


Рис. 5.13.31 Форма ввода полей для создания сервиса

Если пользователь ранее не был не зарегистрирован в УЦ, то для добавления подключения нужно установить галку в поле **Регистрация нового пользователя** и нажать кнопку **Подключить**. На следующем шаге нужно ввести данные для регистрации и нажать **Подключить** (рис. 5.13.32).

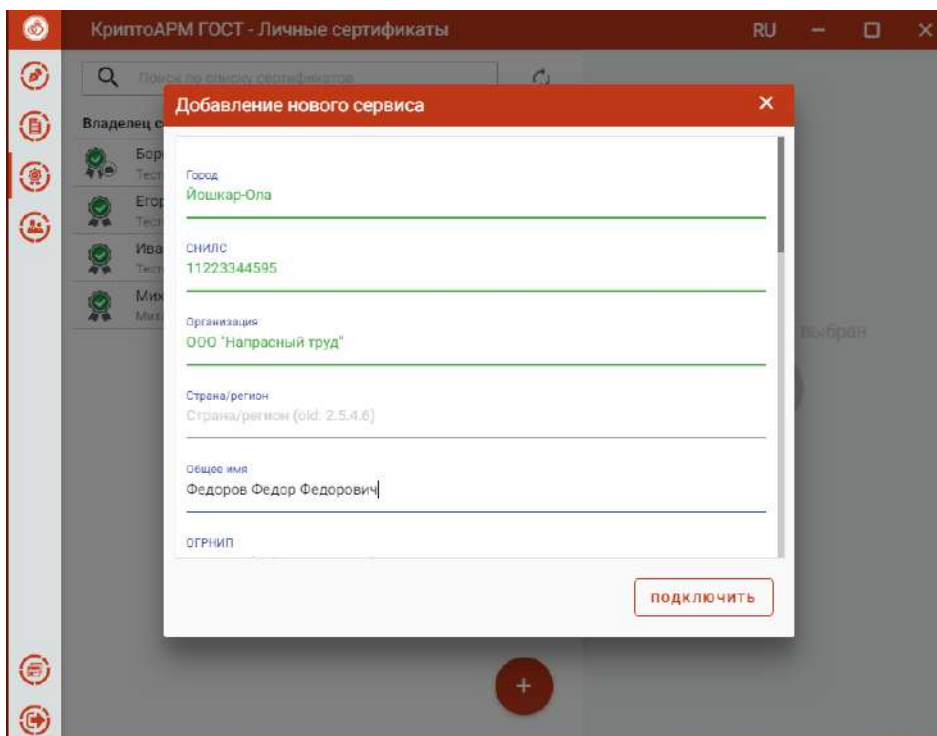


Рис. 5.13.32 Форма регистрации нового пользователя для подключения к УЦ

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).

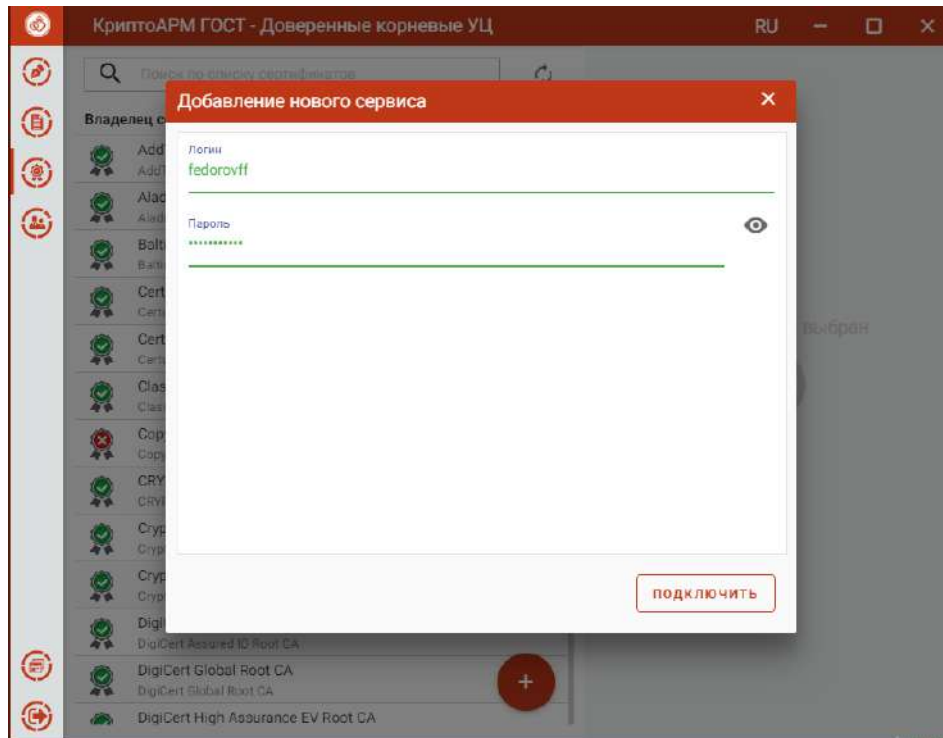


Рис. 5.13.33 Авторизация на сервисе УЦс помощью логина и пароля

После успешной регистрации или авторизации созданное подключение с сервисом по указанному пользователем адресу появляется в списке сервисов при выборе опции **Получение сертификата через сервис УЦ** (рис. 5.13.34).

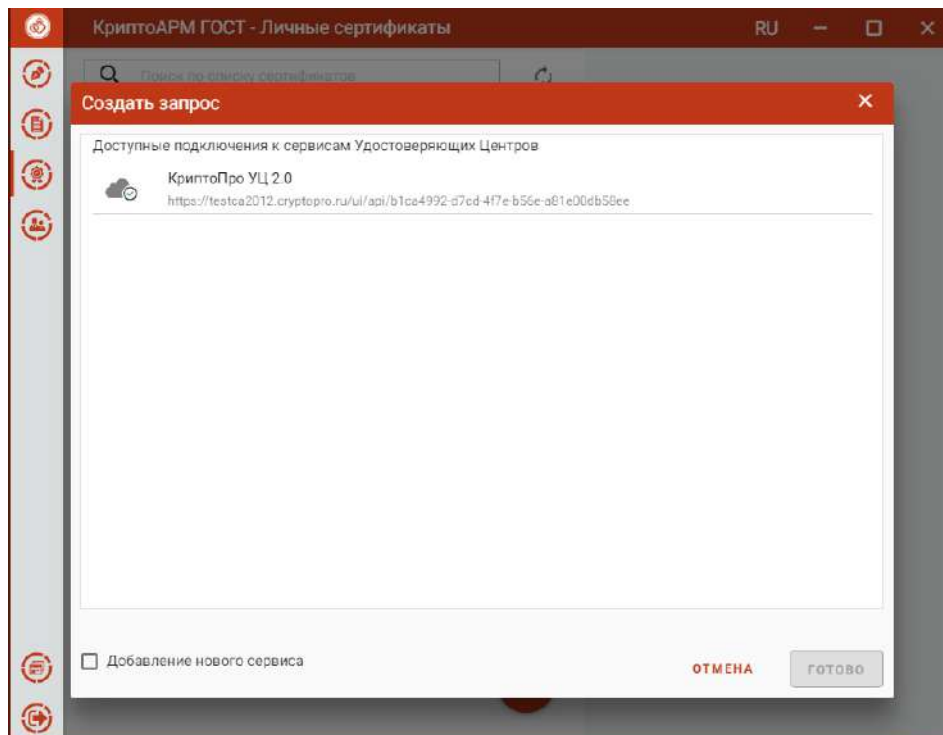



Рис. 5.13.34 Список подключенных сервисов

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.

**СОЗДАНИЕ ЗАПРОСА НА СЕРТИФИКАТ.** Для создания запроса на сертификат нужно выбрав опцию **Получить сертификат через сервис УЦ** при добавлении сертификата в списке личных сертификатов или в списке запросов на сертификат. В открывшемся окне выбрать подключение (рис. 5.13.35) и тип владельца сертификата (рис. 5.13.36).

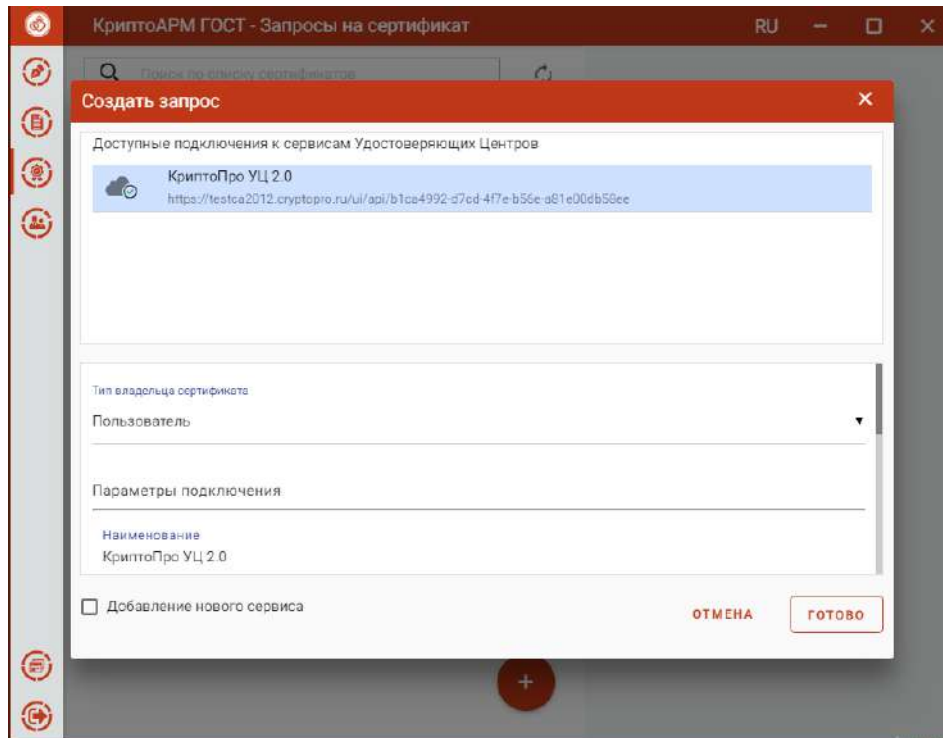


Рис. 5.13.35 Выбор подключения к сервису УЦ

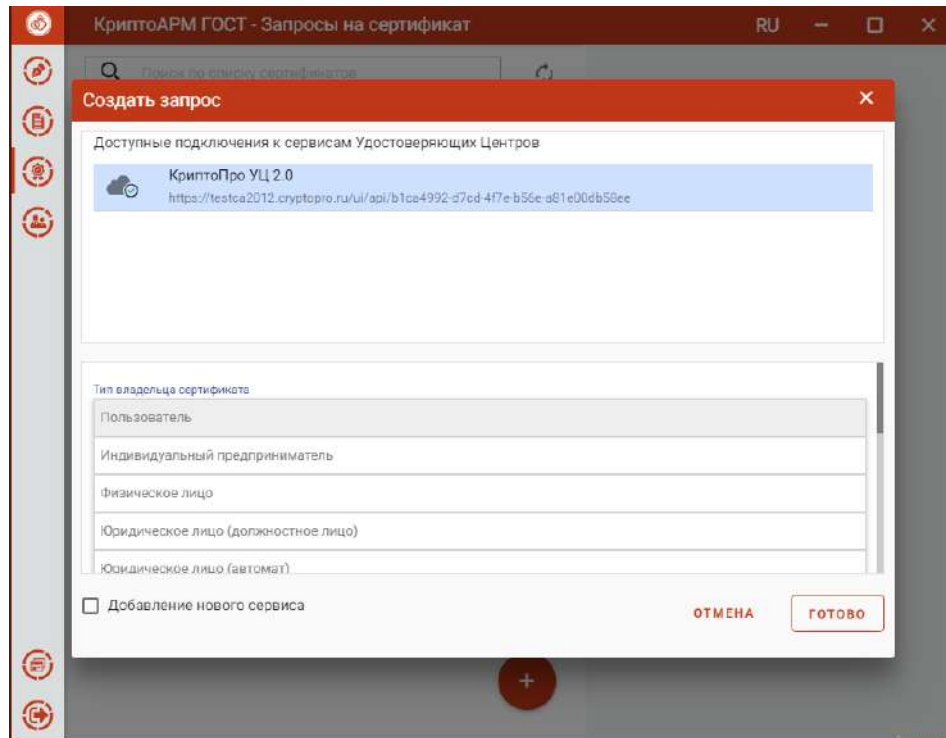


Рис. 5.13.36 Выбор типа владельца сертификата

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).

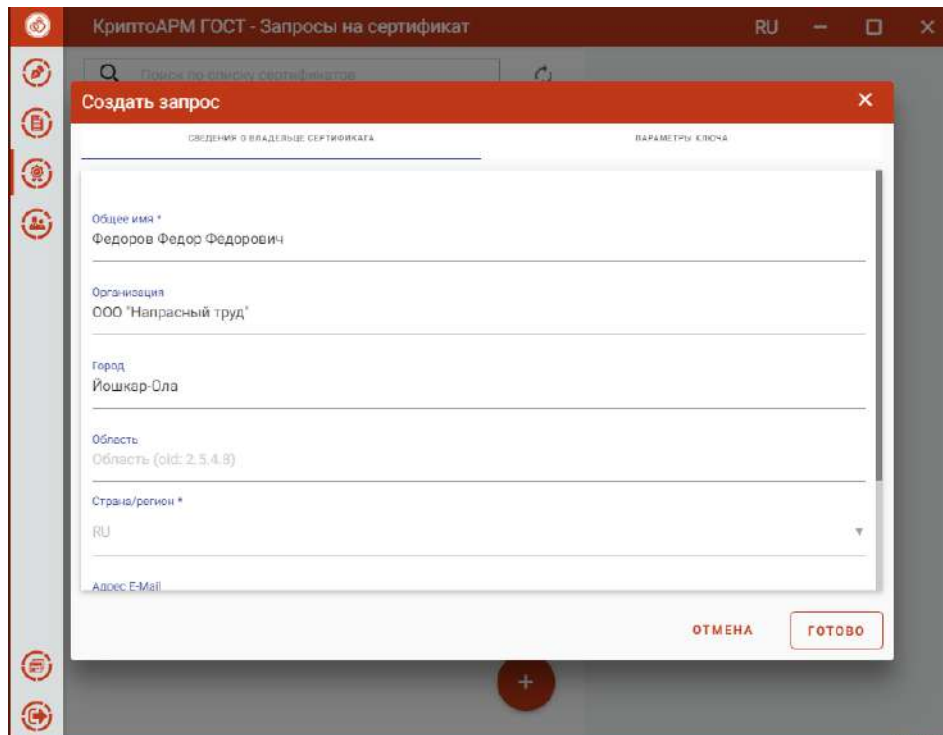


Рис. 5.13.37 Форма создания запроса на сертификат

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** на вкладке управления сертификатами.

**УПРАВЛЕНИЕ ЗАПРОСАМИ НА СЕРТИФИКАТ, СОЗДАНЫМИ ЧЕРЕЗ СЕРВИС УЦ.** Запрос, созданный через подключенный сервис УЦ, сохраняется в раздел **Запросы** (рис. 5.13.38).

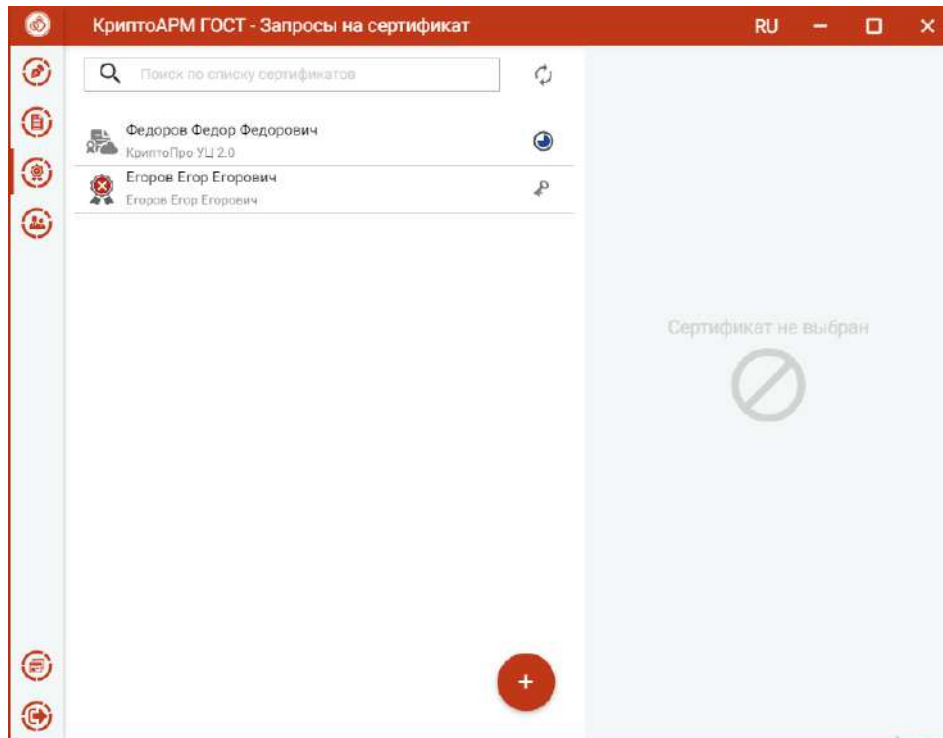


Рис. 5.13.38 Список запросов

Для отображения статуса запроса применяются следующие обозначения:

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

Когда запрос будет обработан Удостоверяющим Центром и выпущен сертификат, при выделении запроса в списке, статус запроса измениться на (рис. 5.13.39), а сертификат установиться в Личное хранилище (рис. 5.13.40).

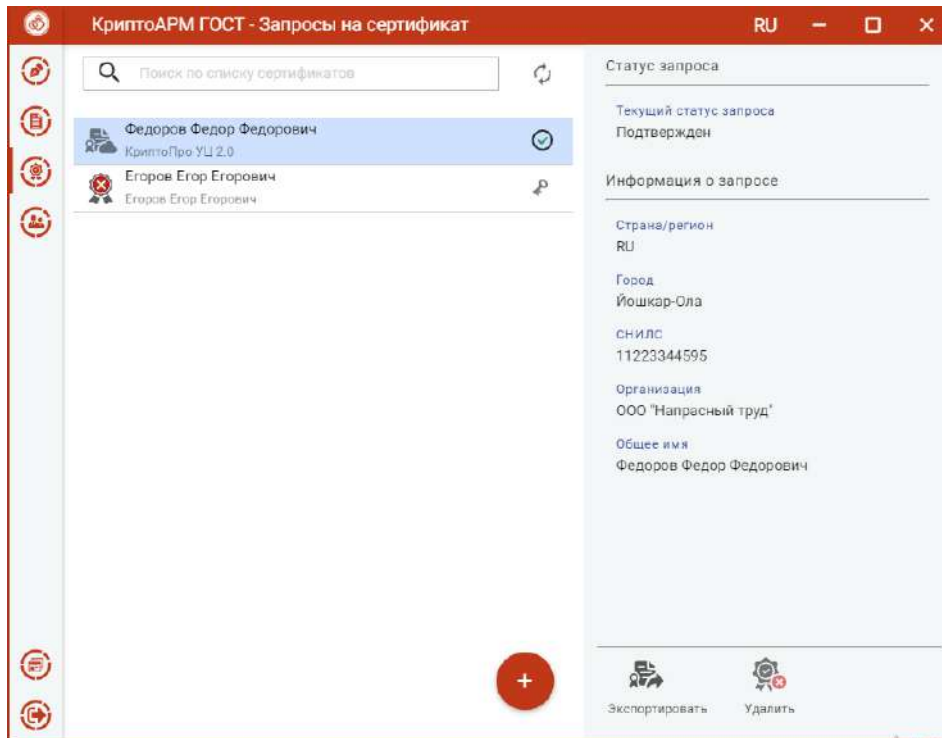


Рис. 5.13.39 Статус запроса, когда сертификат выпущен и установлен в хранилище

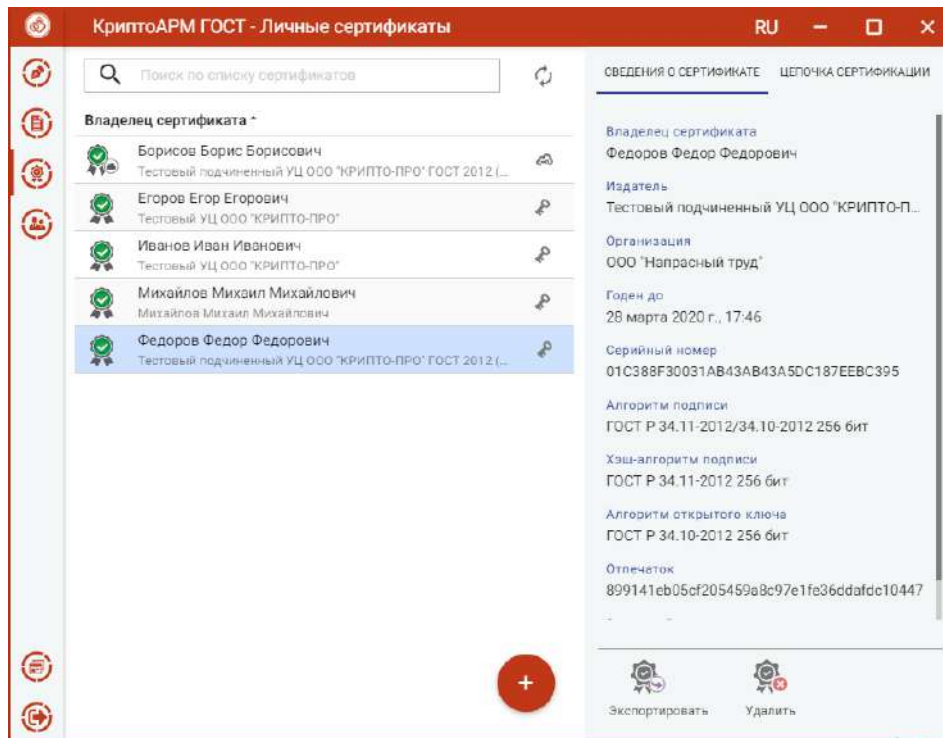


Рис. 5.13.40 Список личных сертификатов

### 5.13.8. Списки отзыва сертификатов (СОС)

Для работы со списками отзыва сертификатов в в пункт меню сертификаты добавлен подпункт **Списки отзыва сертификатов** (рис. 5.13.41).

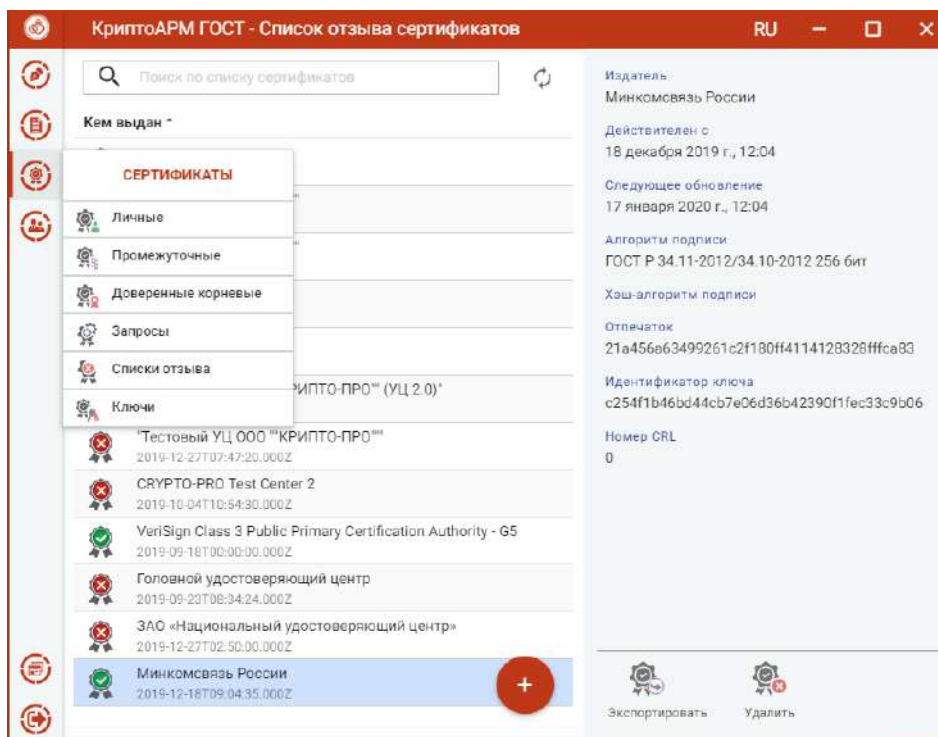


Рис. 5.13.41 Выбор пункт меню для управления списком отзыва

Списки отзыва можно импортировать, экспортировать и удалять.

Для импорта списка отзыва надо нажать кнопку добавления («+») и выбрать опцию **Импорт из файла** (рис. 5.13.42). В открывшемся окне выбрать файл списка отзыва.

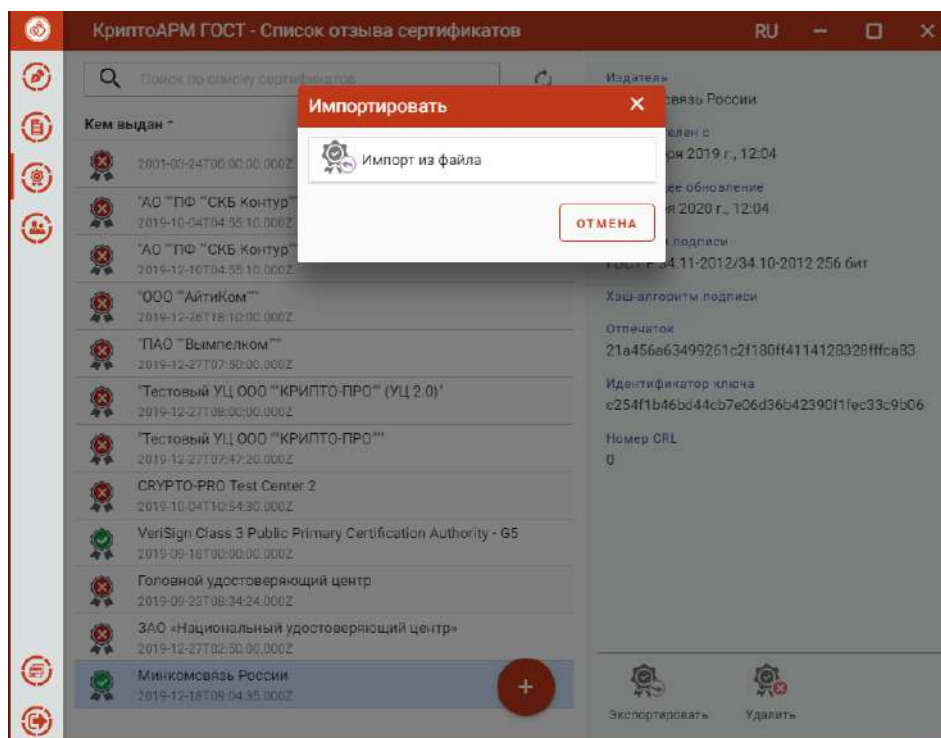


Рис. 5.13.42 Импорт списка отзыва сертификатов

При успешном импорте СОС отображается в разделе **Список отзыва сертификатов** (рис. 5.13.43).

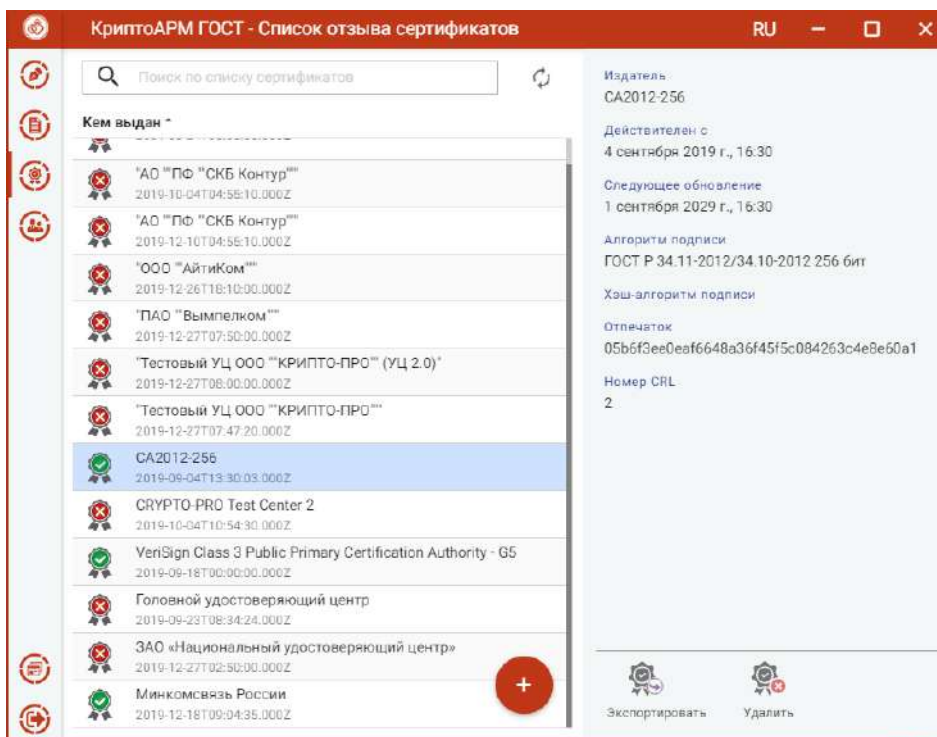


Рис. 5.13.43 Просмотр информации о списке отзыва

**Экспорт СОС.** Для экспорта списка отзыва нужно нажать кнопку **Экспортировать**. Открывается форма выбора кодировки файла (рис. 5.13.44). При нажатии на **Экспорт** следует выбрать директорию для сохранения и задать имя файла СОС.

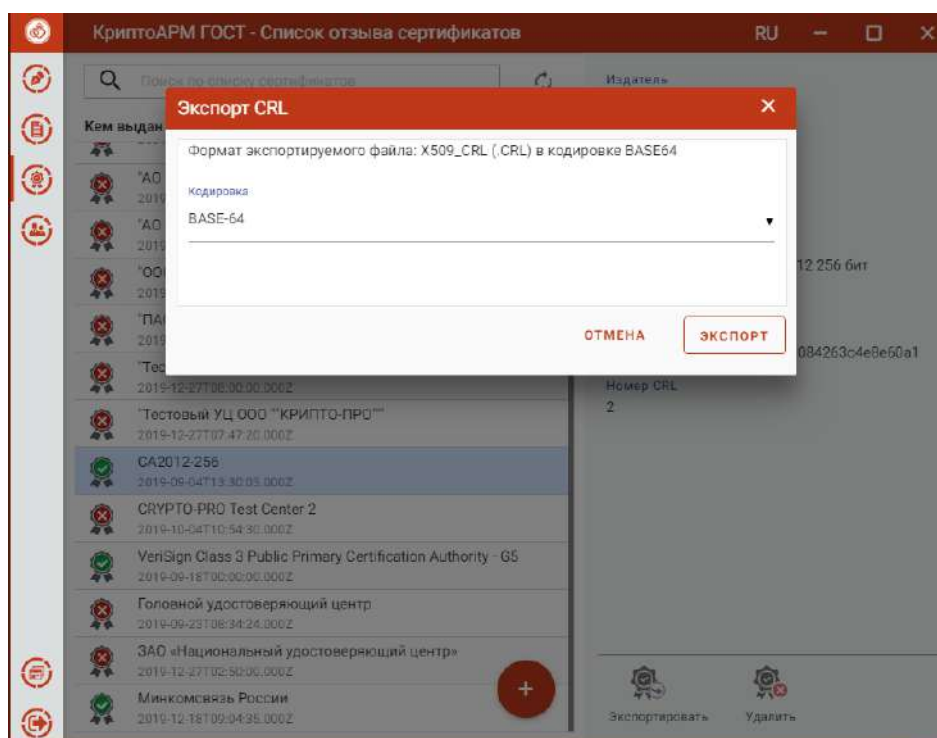


Рис. 5.13.44 Выбор кодировки экспортируемого СОС

**Удаление СОС.** Для удаления СОС надо нажать кнопку **Удалить** и подтвердить удаление в соответствующем окне (рис. 5.13.45).

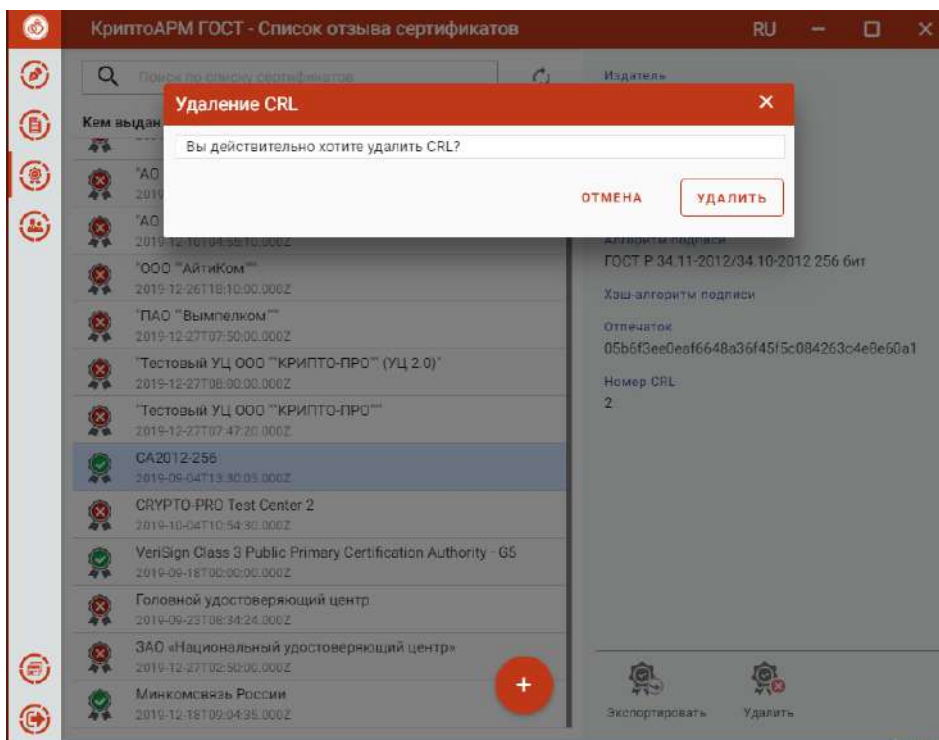


Рис. 5.13.45 Подтверждение удаления СОС

### 5.13.9. УСТАНОВКА СЕРТИФИКАТА ИЗ КЛЮЧЕВОГО КОНТЕЙНЕРА

Для установки сертификата из ключевого контейнера нужно выбрать в меню **Сертификаты** подпункт **Ключи**. В левой области представления отображаются все подключенные хранилища контейнеров закрытых ключей. В правой области отображается информация о сертификате в выделенном контейнере (рис. 5.13.46).

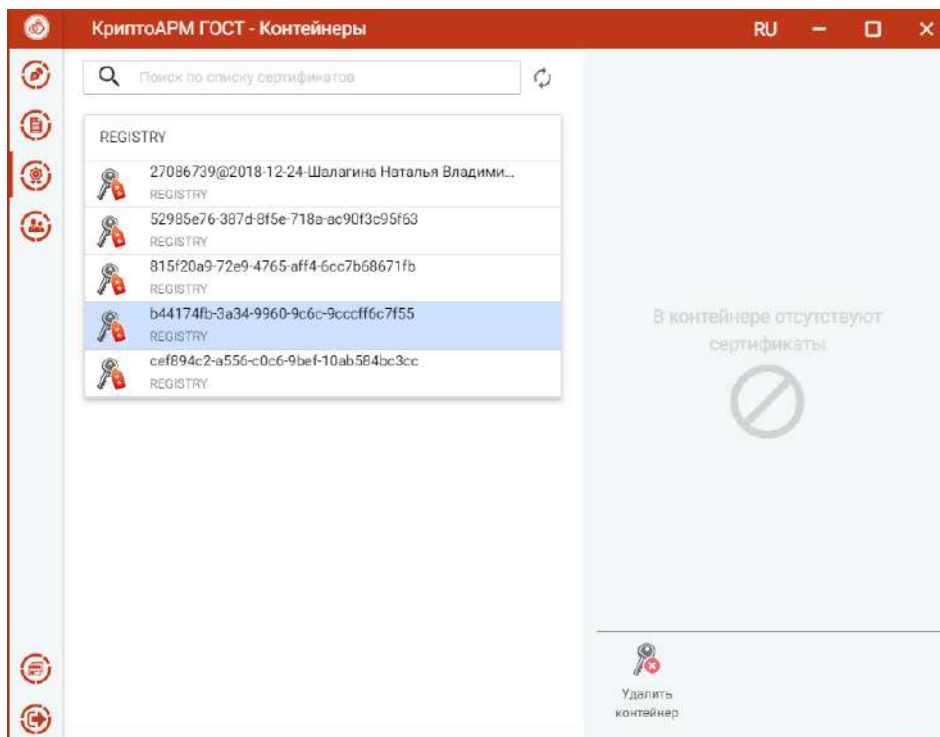


Рис. 5.13.46 Хранилища контейнеров закрытых ключей



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. 5.13.47).

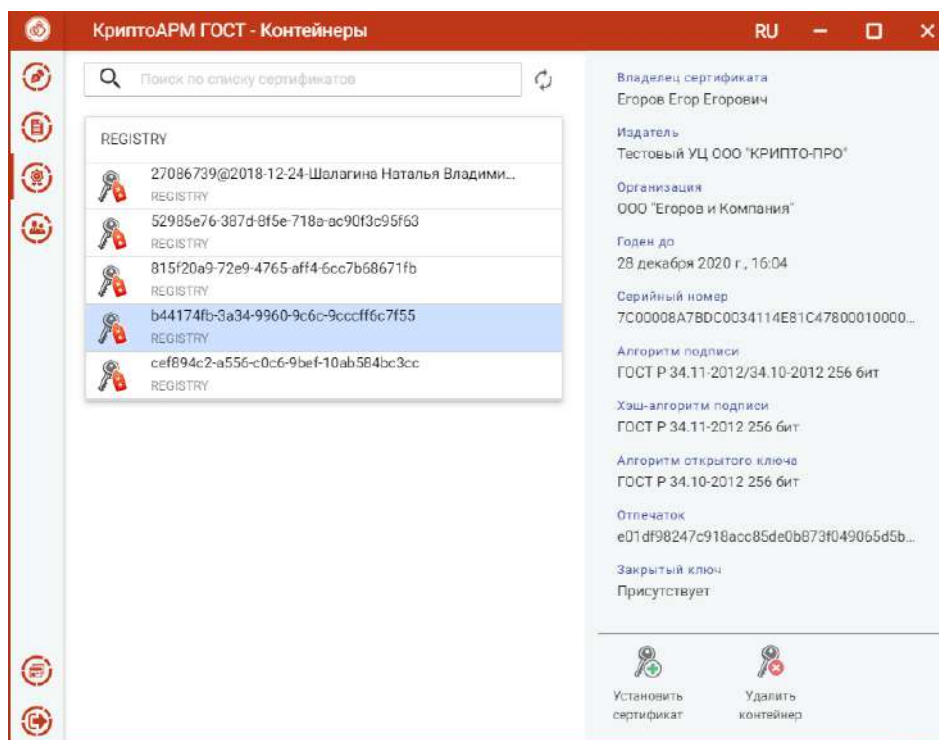


Рис. 5.13.47 Информация о сертификате в контейнере

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. 5.13.48). 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.



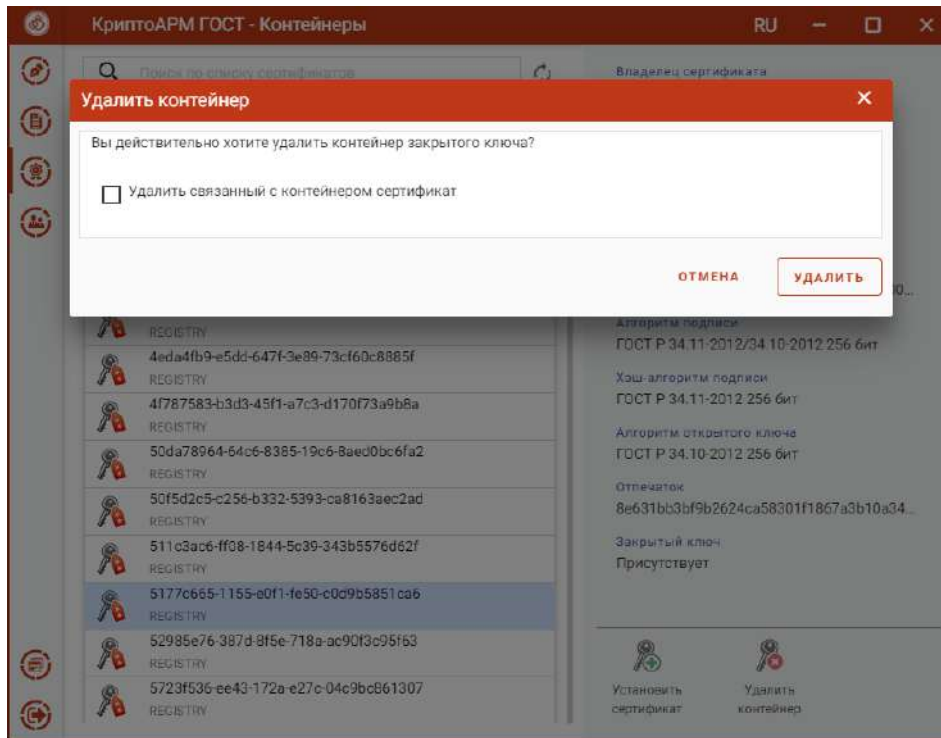


Рис. 5.13.48 Удаление контейнера

В приложении реализован поиск контейнеров по символьному совпадению в названии контейнера (рис. 5.13.49).

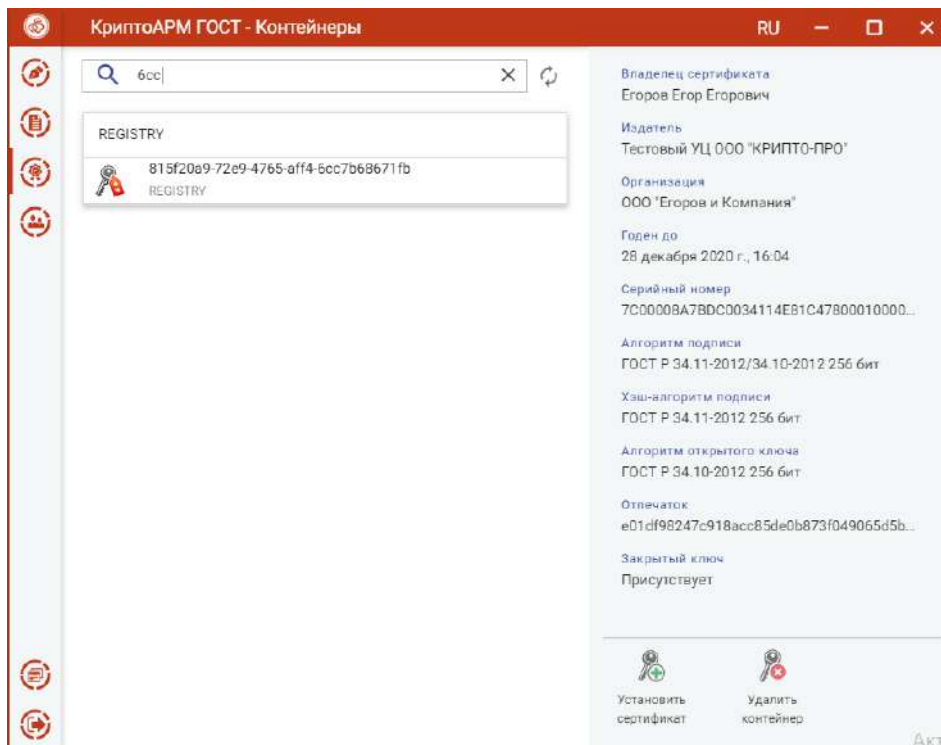


Рис. 5.13.49 Поиск контейнера

### 5.13.10. ПОИСК СЕРТИФИКАТА

В элементах пользовательского интерфейса, где процесс выполнения операции учитывает выбор сертификата из списка, реализована функция поиска сертификатов (рис. 5.13.50). 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 пустым, о чем будет свидетельствовать надпись - «Сертификаты отсутствуют».

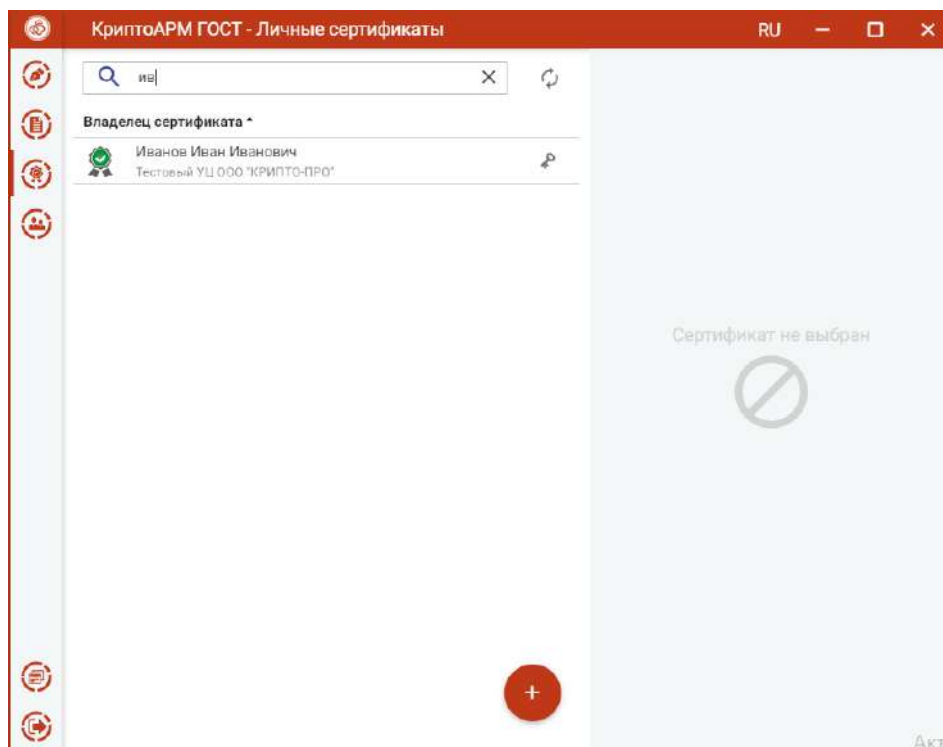


Рис. 5.13.50 Поиск сертификата

## 5.14. Контакты

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

Переход в список контактов происходит при выборе пункта меню **Контакты** (рис. 5.14.1).

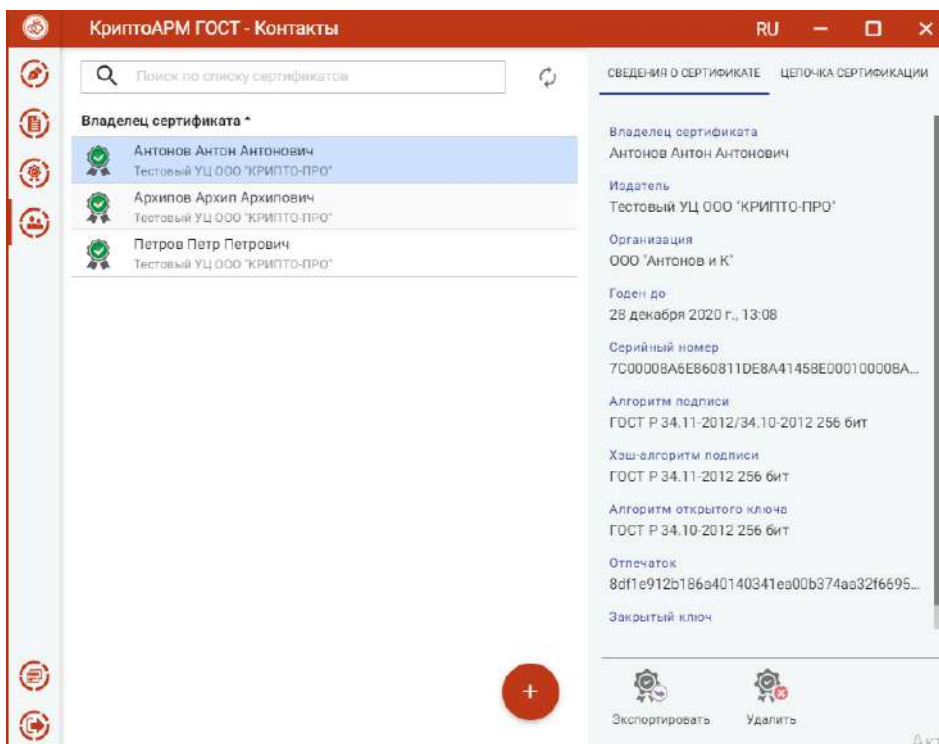


Рис. 5.14.1 Список контактов

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

**ИМПОРТ КОНТАКТА.** Для выполнения импорта нового контакта выполняется кнопкой добавления контакта («+») и выбрать опцию **Импорт из файла** (рис. 5.14.1). В появившемся диалоговом окне нужно выбрать файл сертификата.

При успешном выполнении операции импорта контакт появляется в списке (рис. 5.14.2), а сертификат автоматически помещается в хранилище сертификатов других пользователей.

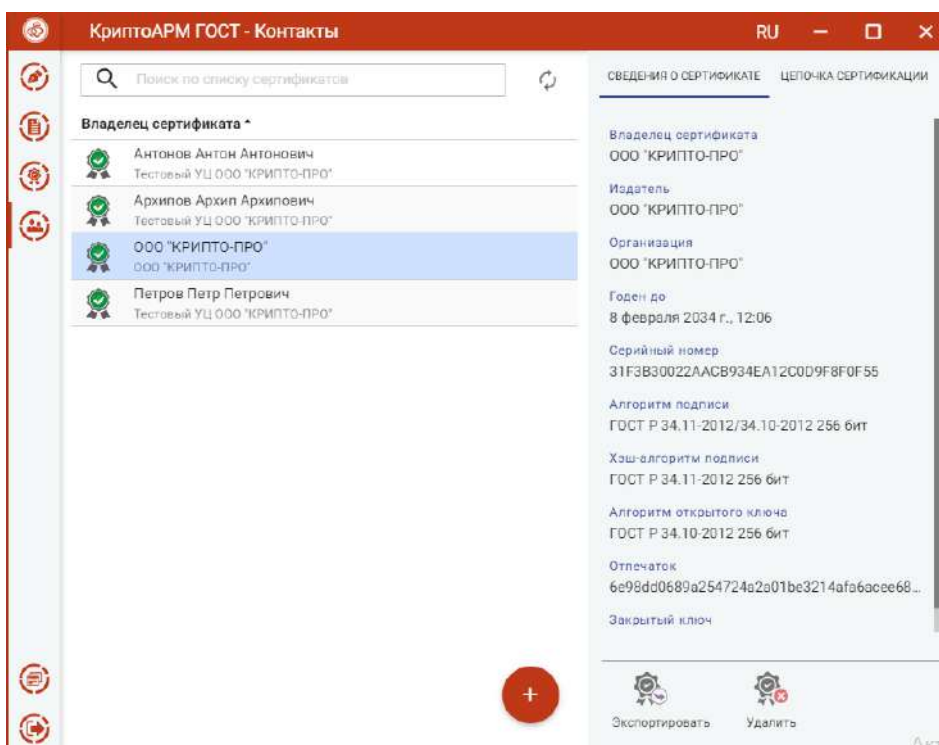


Рис. 5.14.2 Отображение импортированного контакта



**ЭКСПОРТ КОНТАКТА В ФАЙЛ.** Для экспорта контакта в файл нужно выделить контакт и нажать кнопку операции **Экспортировать** (рис. 5.14.3).

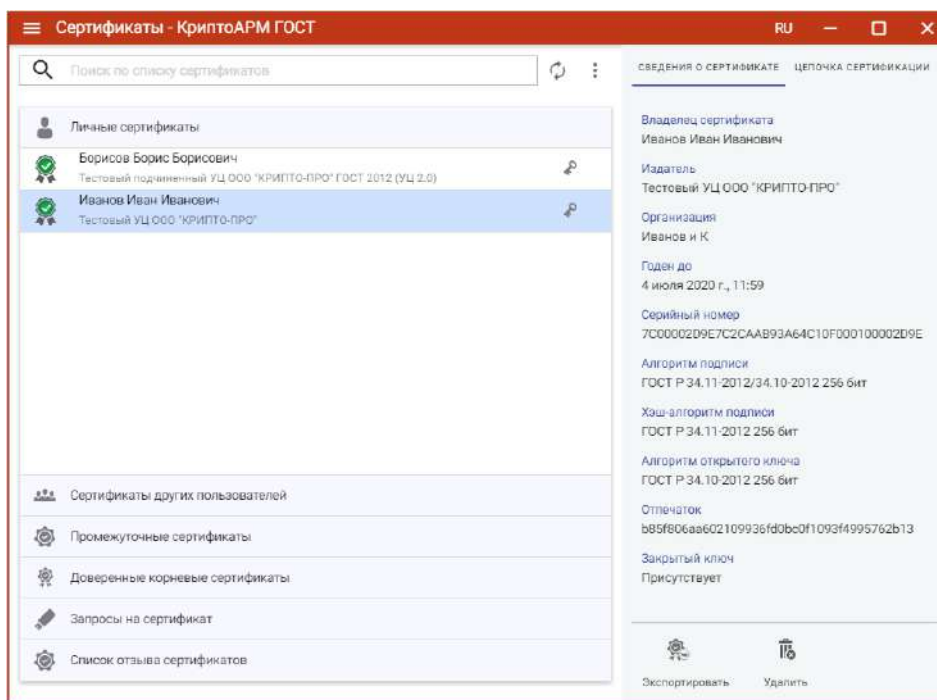


Рис. 5.14.3 Экспорт контакта

При экспорте появляется окно, в котором можно выбрать только кодировку файла сертификата (рис. 5.14.4).

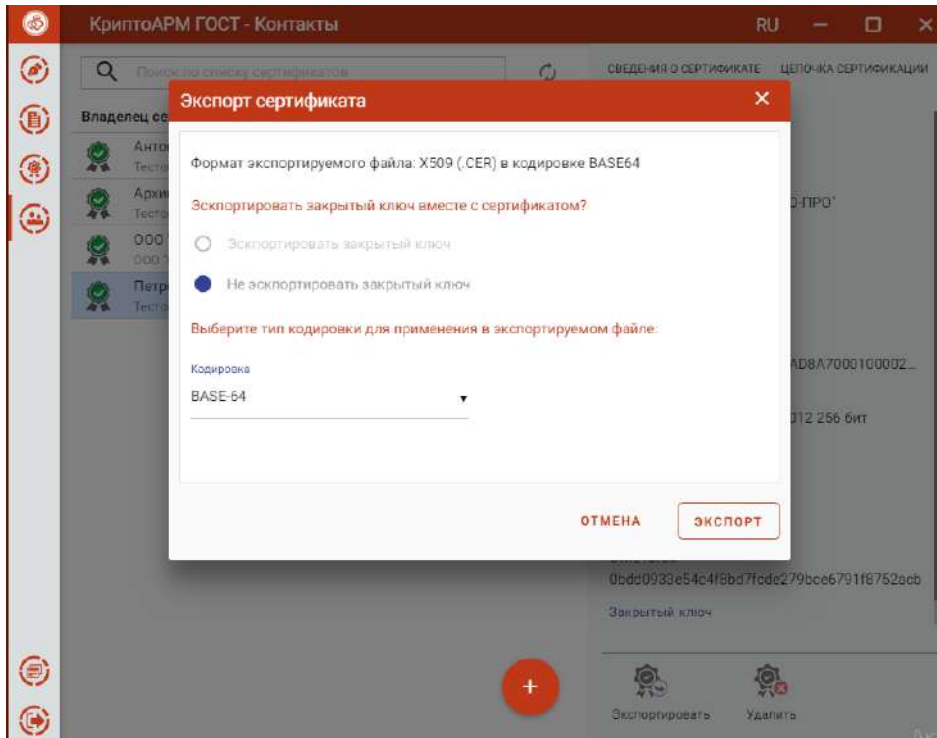


Рис. 5.14.4 Выбор кодировки файла сертификата

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

По окончании операции возникнет сообщение об успешном экспорте сертификата.



**УДАЛЕНИЕ КОНТАКТА** Для удаления сертификата нужно выбрать операцию **Удалить** (рис. 5.14.5).

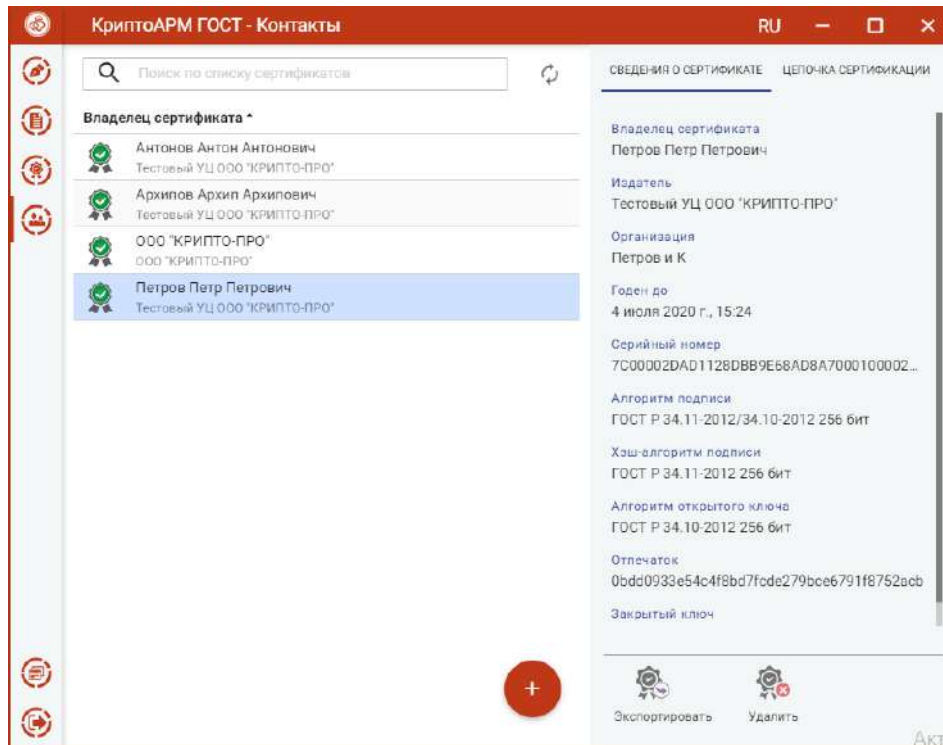


Рис. 5.14.5 Удаление контакта

В появившемся диалоговом окне нажать **Удалить** для подтверждения удаления (рис. 5.14.6).

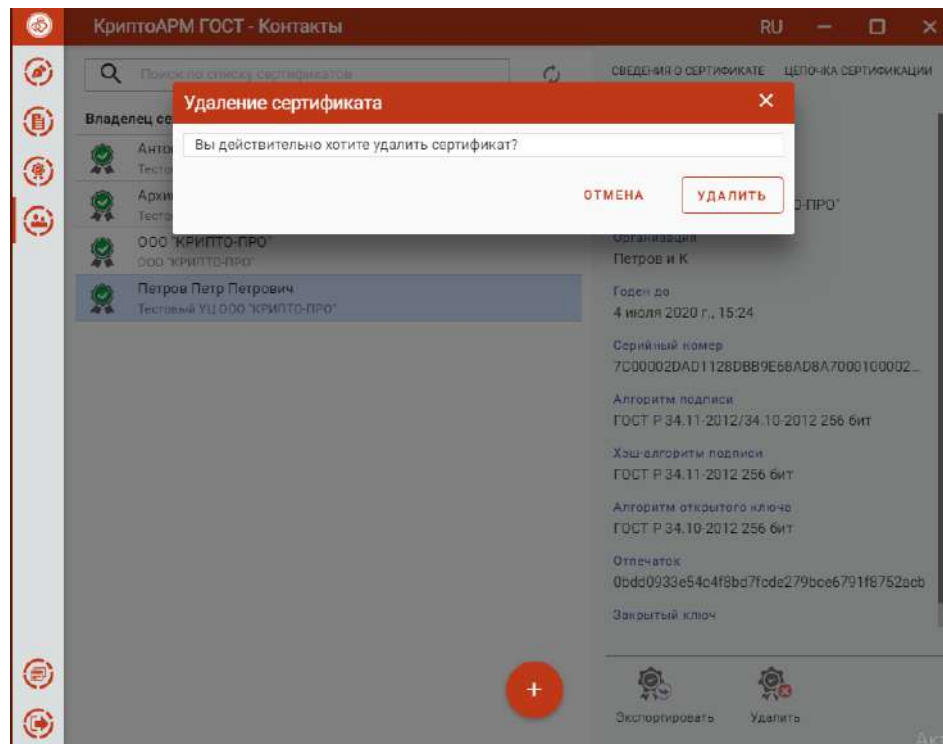


Рис. 5.14.6 Подтверждение удаления контакта

**ПОИСК КОНТАКТА.** Для поиска контакта нужно в строке поиска ввести ключевую фразу (рис. 5.14.7).



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

Чтобы отменить фильтр поиска требуется удалить ключевую фразу или нажать на кнопку Отмена.

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

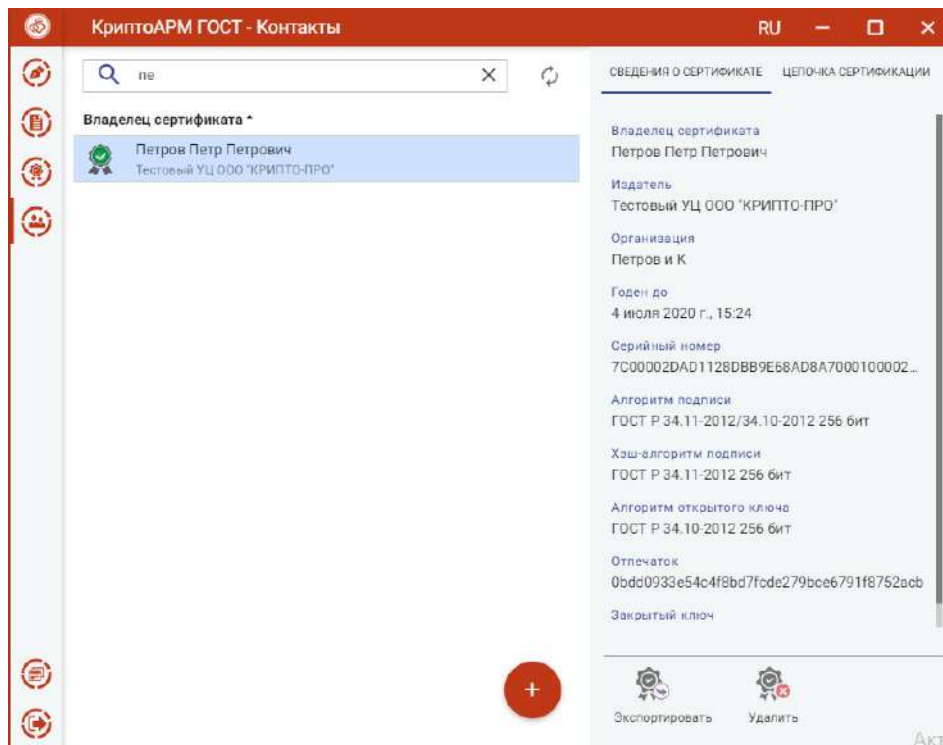


Рис. 5.14.7 Поиск контакта

## 5.15. О ПРОГРАММЕ

Пункт меню **О программе** содержит подпункты:

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



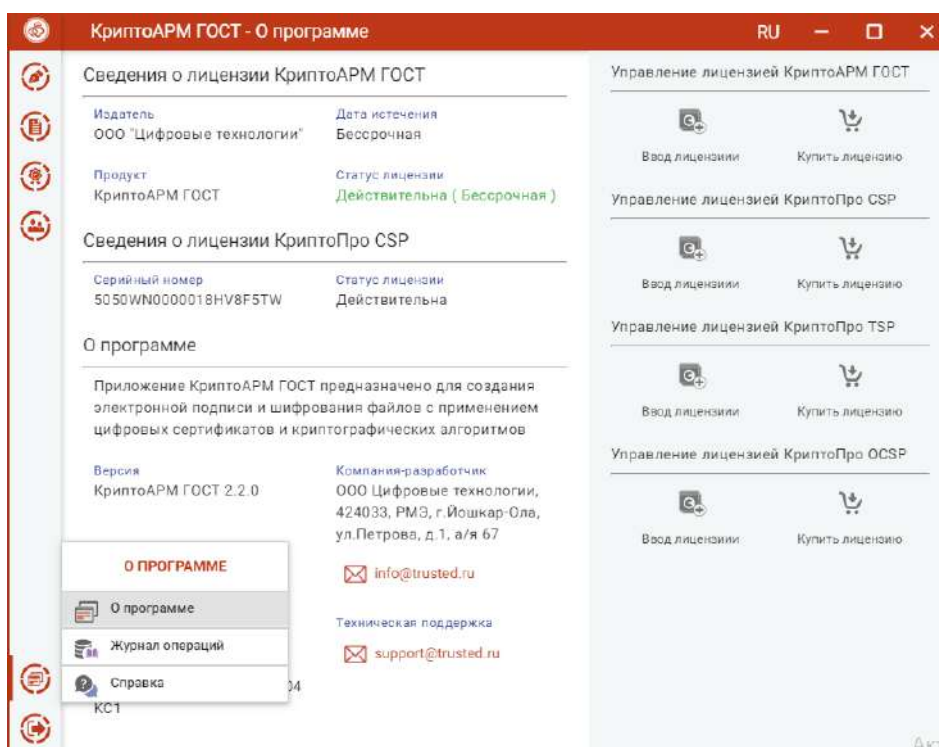


Рис. 5.15.1 Меню О программе

### 5.15.1. 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 подпункт **О программе** (рис. 5.15.2).

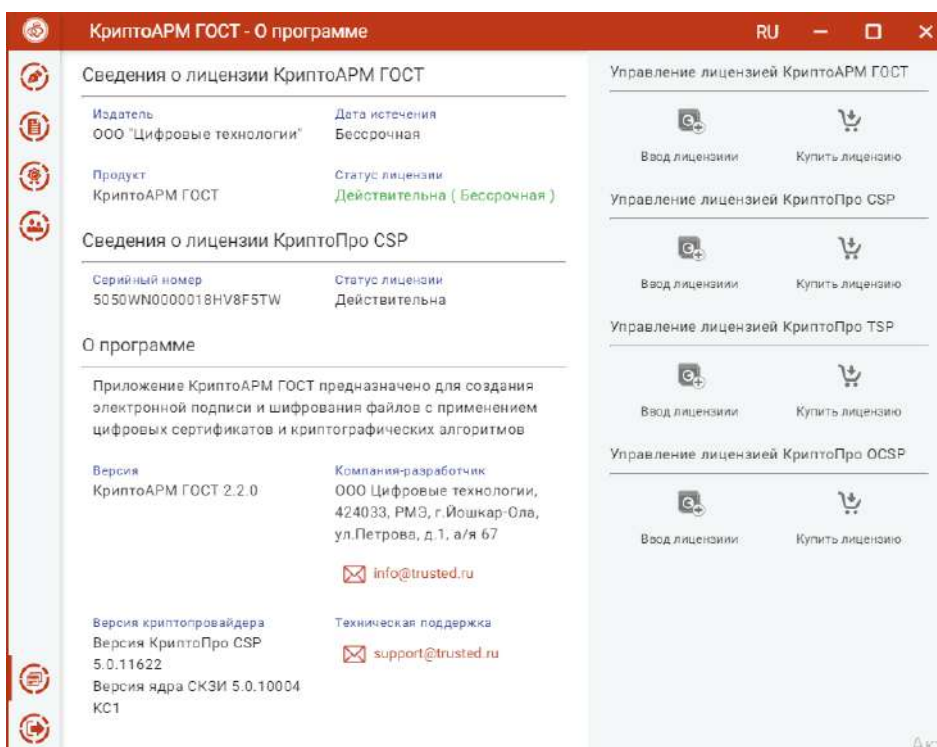


Рис. 5.15.2 Информация о программе



### 5.15.2. Журнал ОПЕРАЦИЙ

Журнал операций предназначен для отображения операций, выполняемых пользователем (рис. 5.15.3).

Дата и время *	Операция	Пользователь	Объект операции	Статус
28.12.2019, 16:23	Удаление сертифик...	Админ	CN=Минкомсвязь России > Null	✓
28.12.2019, 16:23	Импорт сертификата	Админ	CN=Минкомсвязь России > Null	✓
28.12.2019, 16:22	Удаление сертифик...	Админ	CN=Шалагина Наталья Владимировна > Null	✓
28.12.2019, 16:22	Импорт сертификата	Админ	CN=Шалагина Наталья Владимировна > Null	✓
28.12.2019, 16:22	Удаление сертифик...	Админ	CN=АО "ПФ "СКБ Контур" > Null	✓
28.12.2019, 16:22	Импорт сертификата	Админ	CN=АО "ПФ "СКБ Контур" > Null	✓
28.12.2019, 16:21	Импорт сертификата	Админ	CN=ООО "КРИПТО-ПРО" > Null	✓
28.12.2019, 16:04	Импорт сертификата	Админ	CN=Егоров Егор Егорович > Null	✓
28.12.2019, 16:02	Удаление контейнера	Админ	REGISTRY\q2222-1 > Null	✓
28.12.2019, 16:02	Удаление контейнера	Админ	REGISTRY\q2222 > Null	✓
28.12.2019, 16:00	Импорт CRL	Админ	CN=CA2012-256 > Null	✓
28.12.2019, 15:52	Импорт сертификата	Админ	CN=Михайлов Михаил Михайлович > Null	✓
28.12.2019, 15:52	Импорт сертификата	Админ	CN=Михайлов Михаил Михайлович > Null	✓

Рис. 5.15.3 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. 5.15.4)

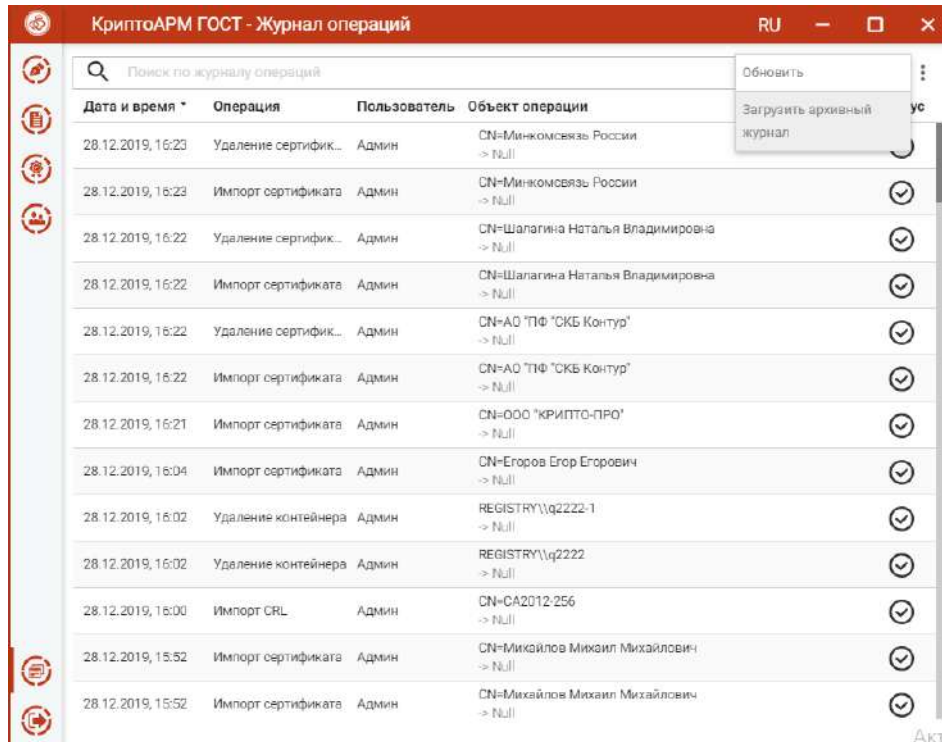


Рис. 5.15.4 Контекстное меню журнала операций

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. 5.15.5)

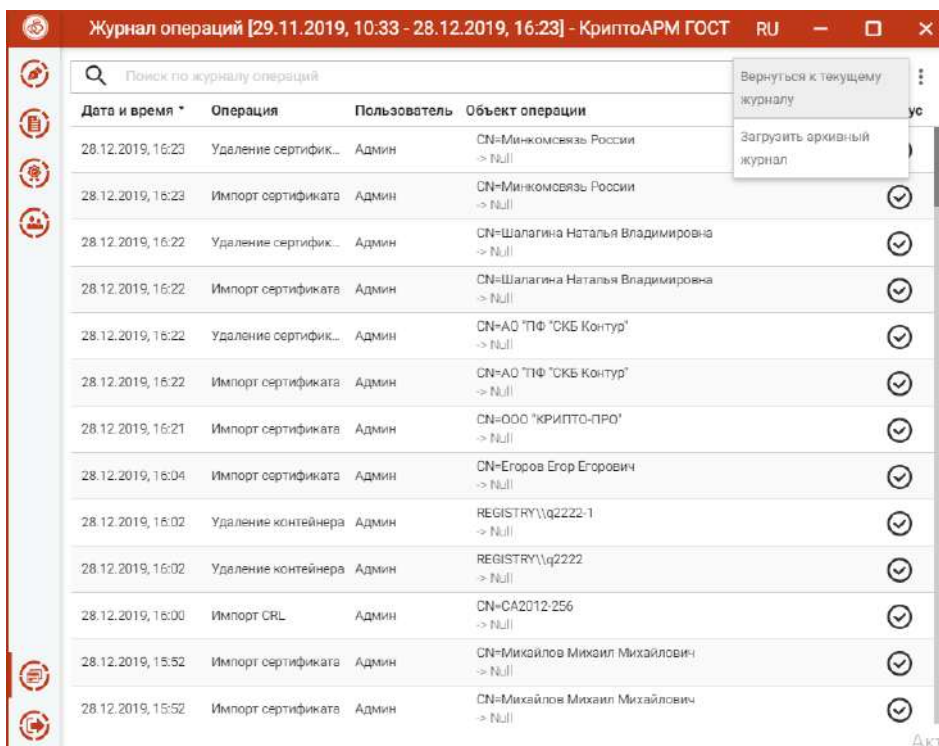


Рис. 5.15.5 Контекстное меню архивного журнала операций

**ПОИСК ЗАПИСЕЙ В ЖУРНАЛЕ ОПЕРАЦИЙ.** В приложении реализован поиск записей журнала операций по символному совпадению (рис. 5.15.6)

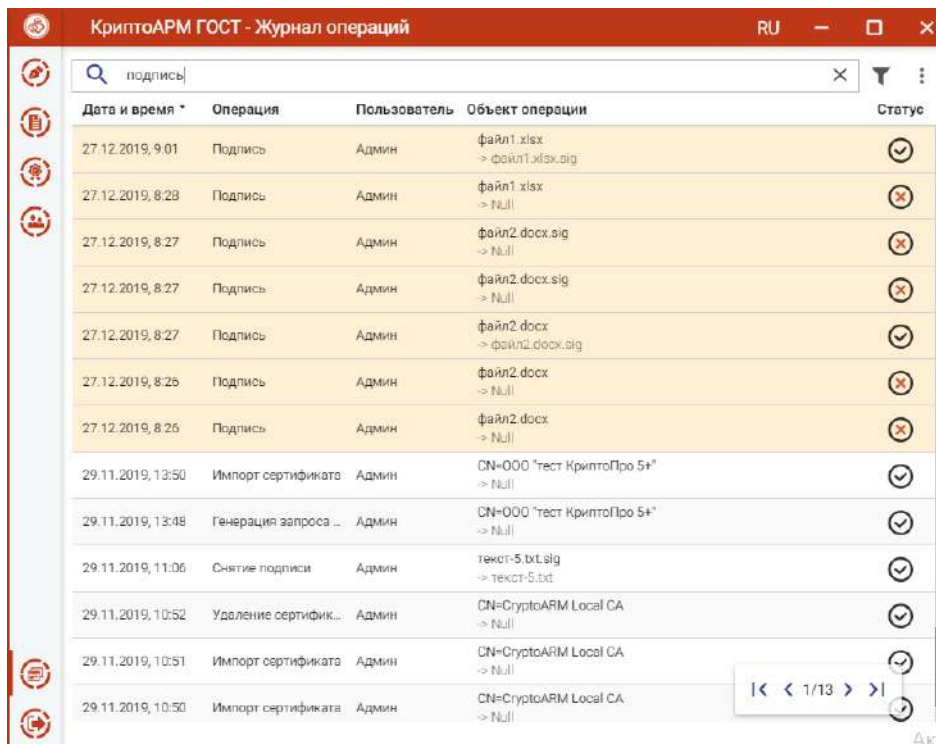


Рис. 5.15.6 Поиск записей в журнале операций

**ФИЛЬТРАЦИЯ ЖУРНАЛА ОПЕРАЦИЙ.** Для открытия окна настроек критериев фильтра на панели управления имеется кнопка, при нажатии на которую открывается окно настроек фильтрации (рис. 5.15.7).

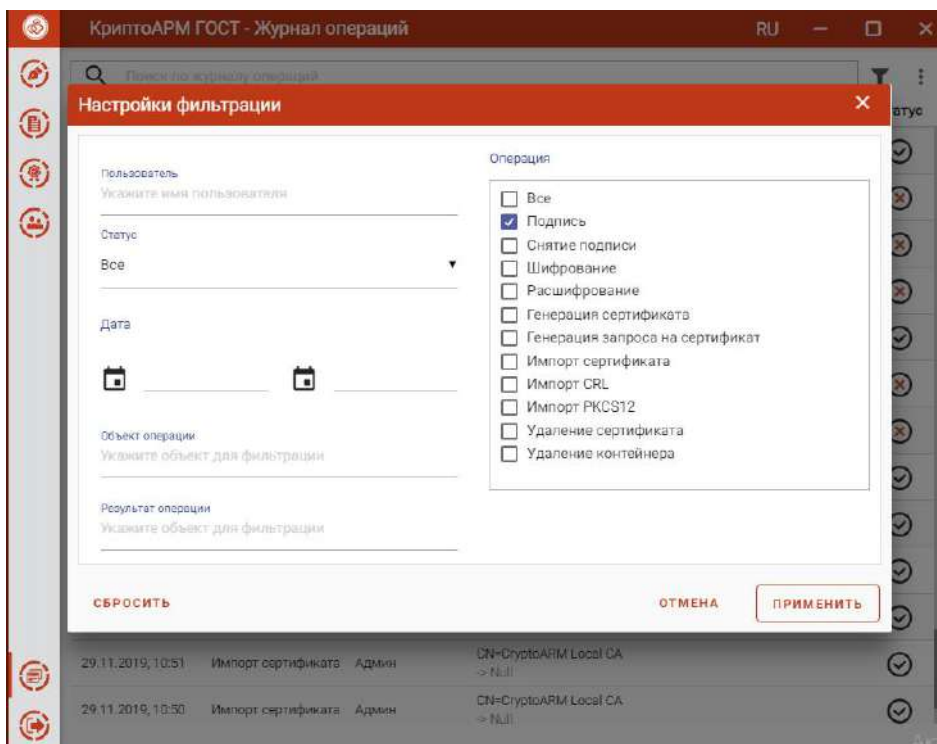


Рис. 5.15.7 Настройки критериев фильтра журнала операций

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. 5.15.8).

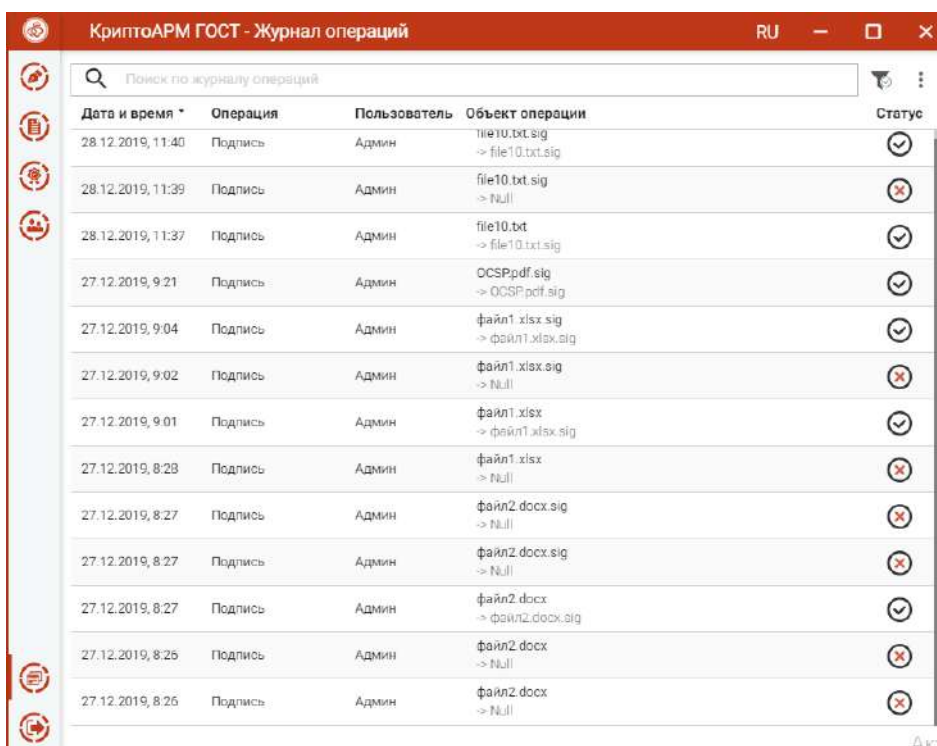


Рис. 5.15.8 Результат применения фильтрации журнала операций

Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации (рис. 5.15.7).





### 5.15.3. СПРАВКА

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

## 6. Диагностика неполадок при запуске приложения

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

### 6.1. Отсутствует СКЗИ КриптоПро CSP

Приложение КриптоАРМ ГОСТ не работает без установленного в системе СКЗИ КриптоПро CSP. В таком случае при запуске приложения будет предупреждающее сообщение (рис. 6.1.1)

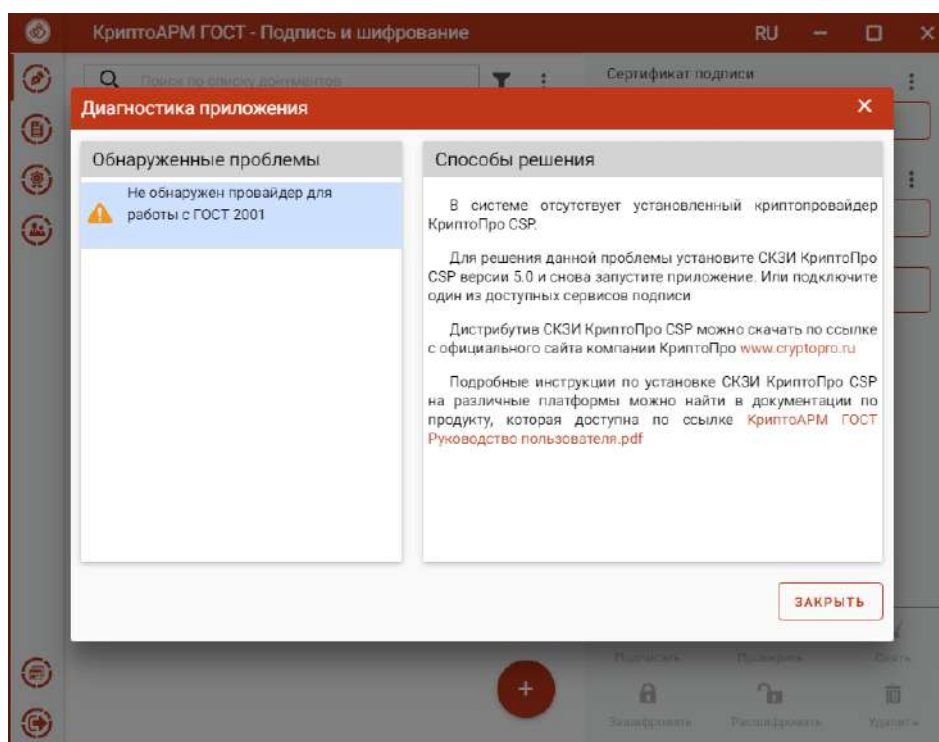


Рис. 6.1.1 Сообщение об отсутствии СКЗИ КриптоПро CSP

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).



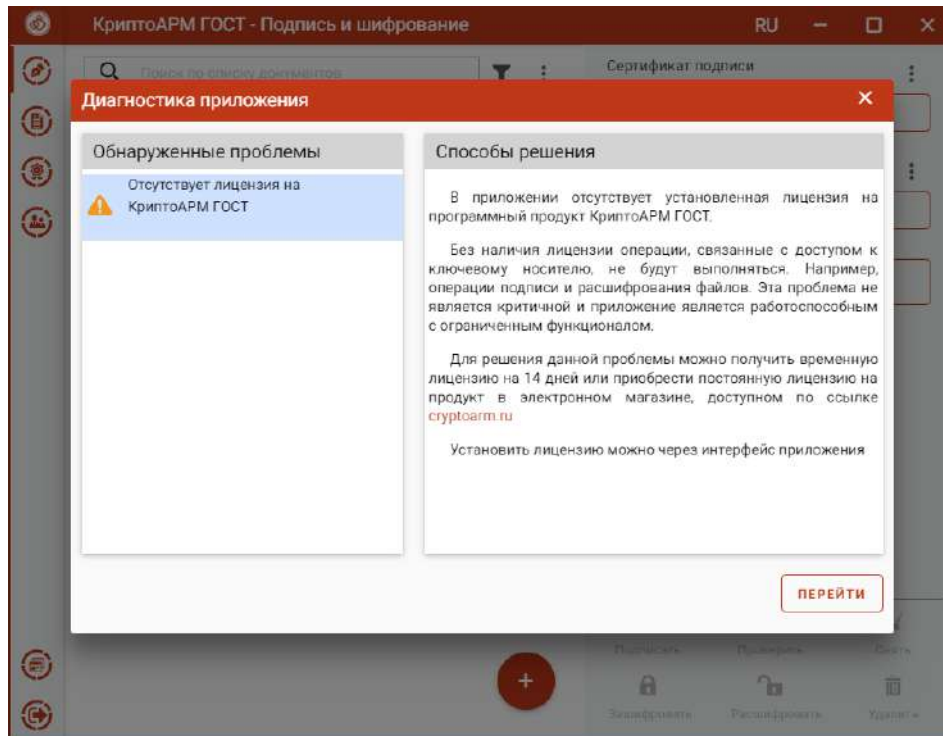


Рис. 6.2.1 Сообщение об отсутствии лицензии на КриптоАРМ ГОСТ

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).

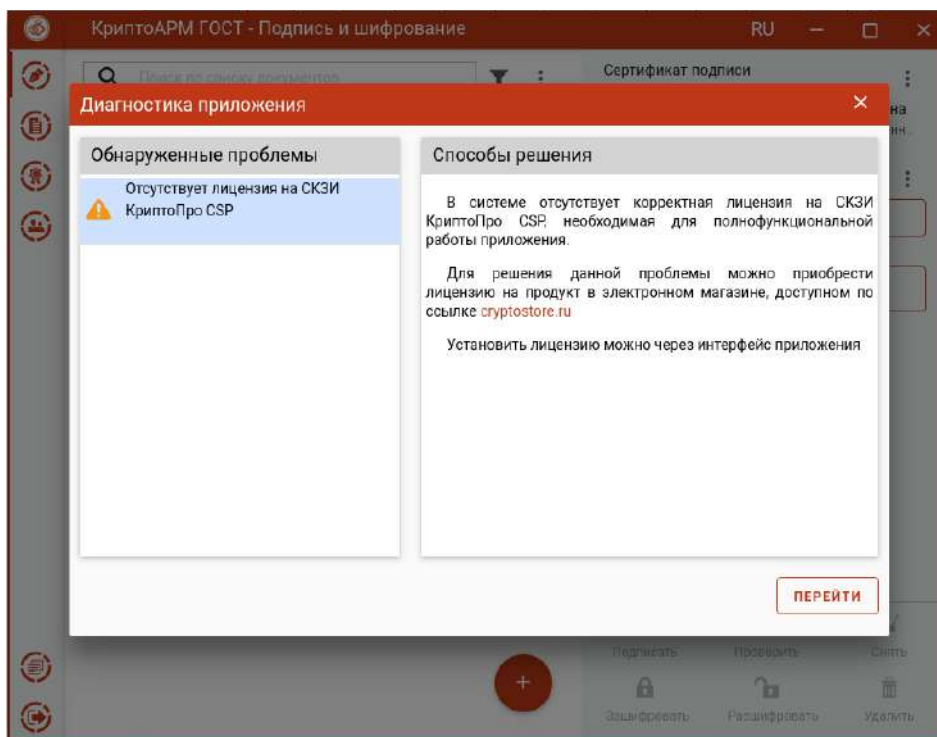


Рис. 6.3.1 Сообщение об отсутствии лицензии на КриптоПро CSP

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)

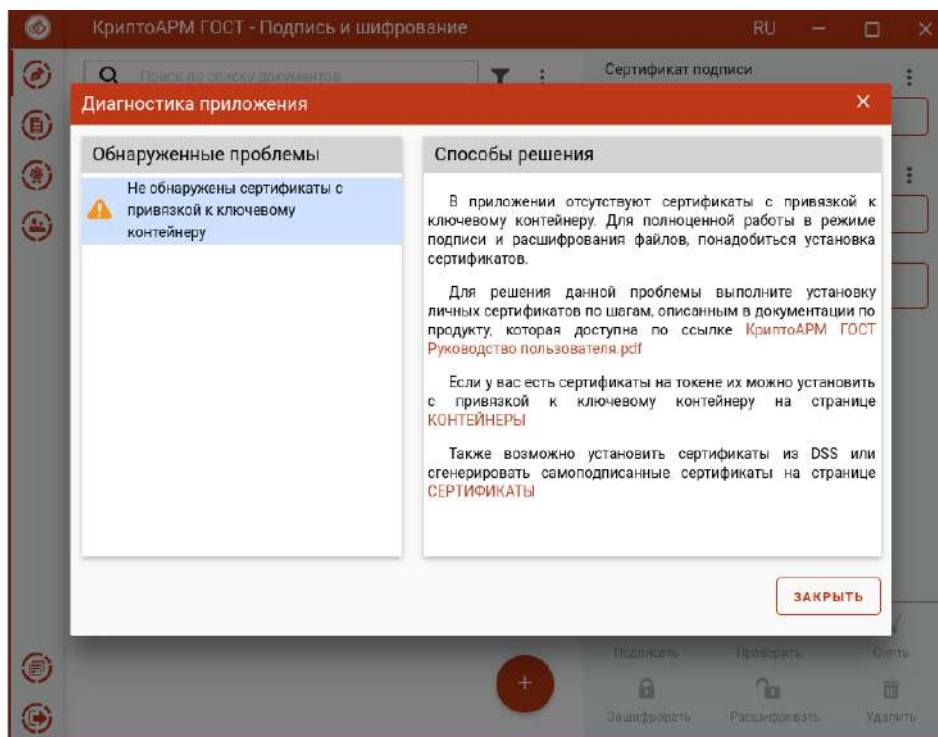


Рис. 6.4.1 Сообщение об отсутствии сертификатов с привязкой к закрытому ключу

Добавить личный сертификат можно несколькими способами:

- установить со стороннего носителя;
- установить из DSS;
- 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 **Ключи**, 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 **Ключи**.

Установить сертификат из DSS можно, перейдя по ссылке на страницу **Сертификаты**, выбрав опцию добавления **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 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)

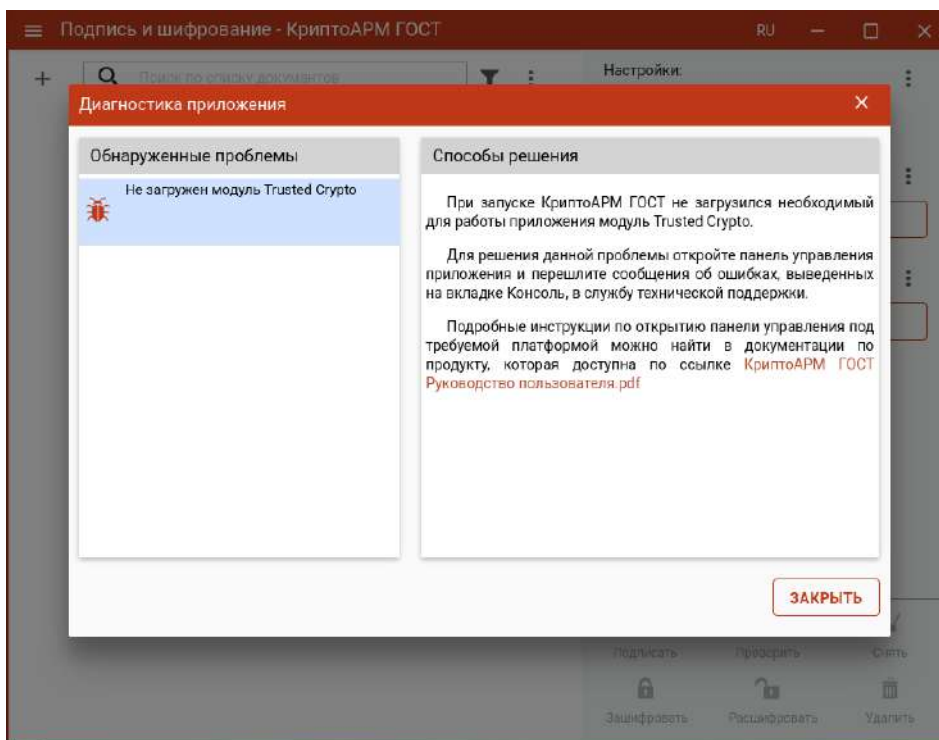


Рис. 6.5.1 Сообщение об ошибке в модуле Trusted Crypto

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.

## 6.6. ОТСУТСТВУЮТ УСТАНОВЛЕННЫЕ МОДУЛИ КРИПТОПРО TSP CLIENT 2.0/OCSP CLIENT 2.0

При отсутствии модулей КриптоПро TSP Client 2.0 или КриптоПро OCSP Client 2.1 возникает информационное сообщение (рис. 6.5.1)

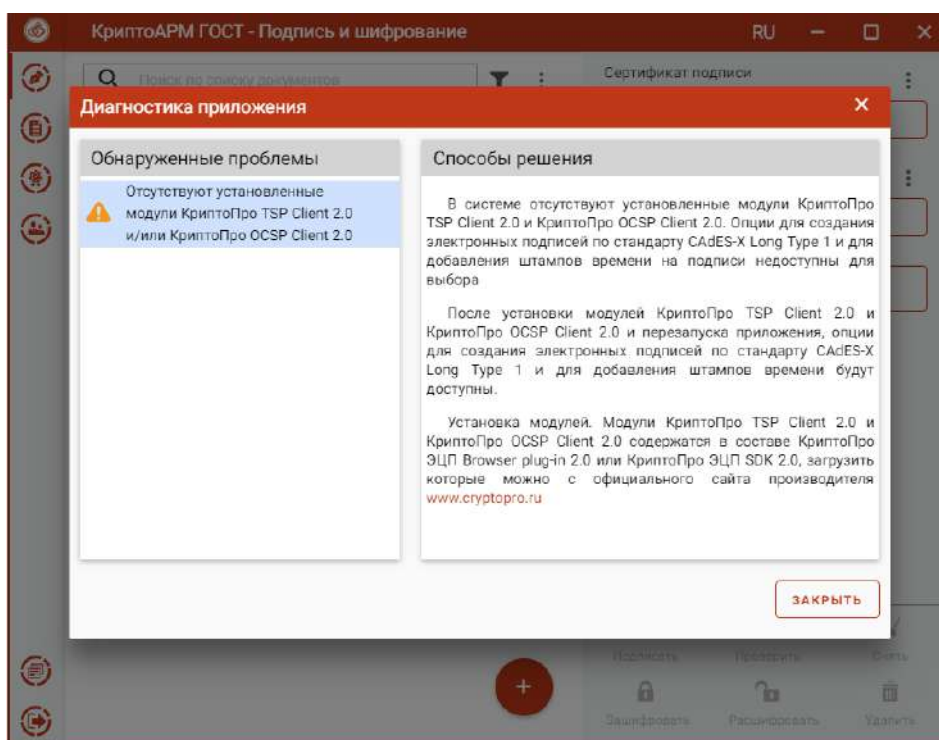


Рис. 6.5.1 Сообщение об ошибке в модуле Trusted Crypto

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

Как установить данные модули описано в пункте установки КриптоПро CSP.

## 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 подразделах.

### 7.1. ОТСЛЕЖИВАНИЕ ОШИБОК НА ПЛАТФОРМЕ MS WINDOWS

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

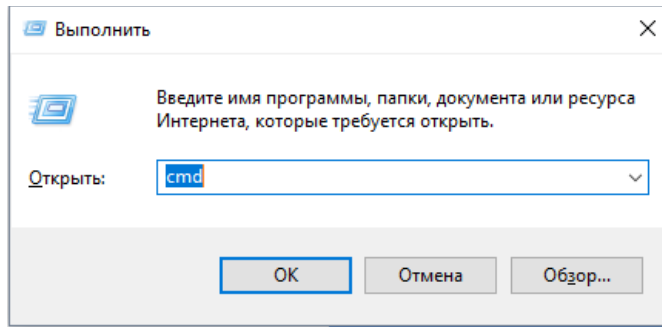


Рис. 7.1.1. Диалог для запуска приложений

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

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

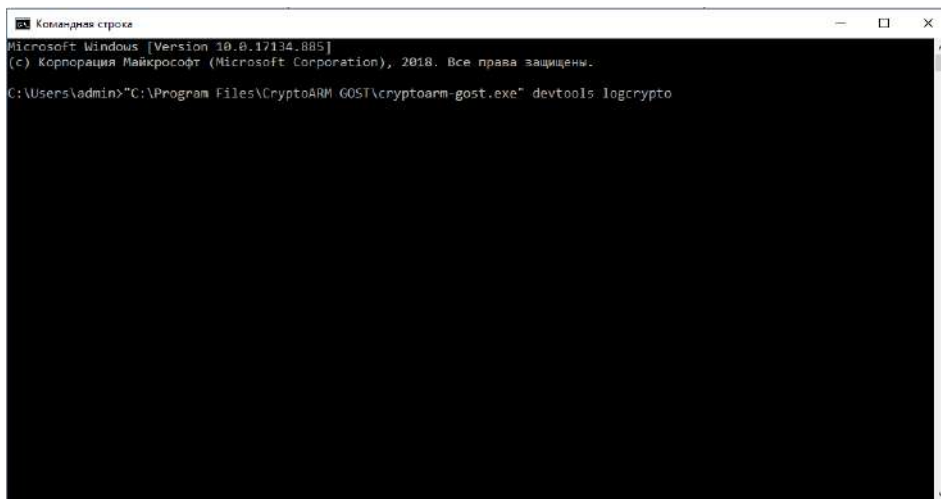


Рис. 7.1.2. Диалог командной строки

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.

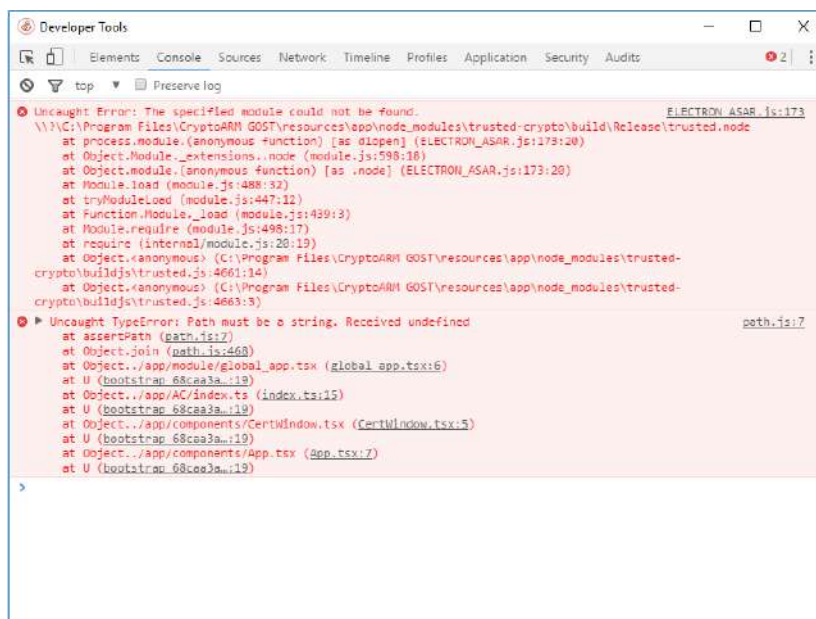


Рис. 7.1.3. Окно с вкладкой консоли управления





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
```

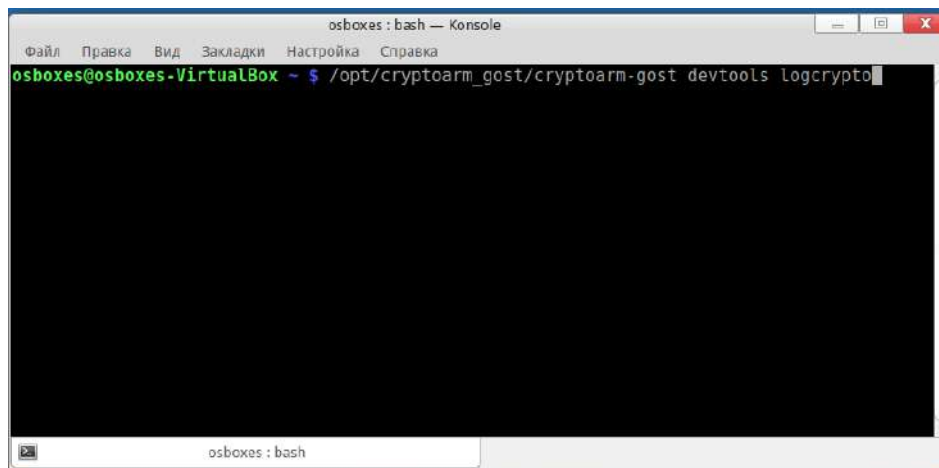


Рис. 7.2.1. Окно терминала

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

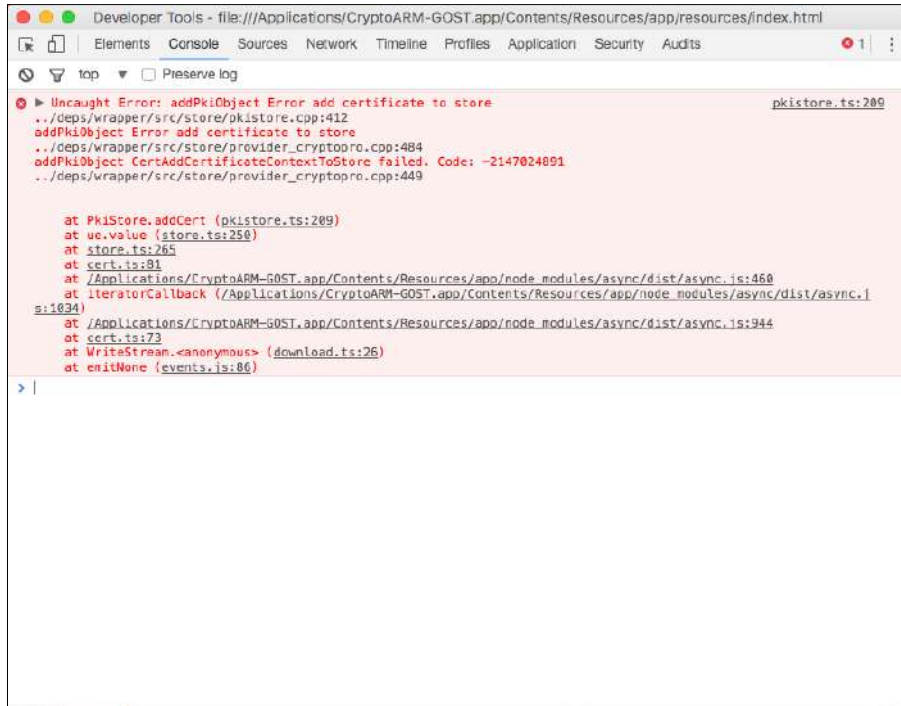
Для получения доступа к дополнительной панели управления приложением и включением режима логирования, в терминале ОС OS X ввести команду (рис. 7.3.1):

**`/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).



```
Developer Tools - file:///Applications/CryptoARM-GOST.app/Contents/Resources/app/resources/index.html
Elements Console Sources Network Timeline Profiles Application Security Audits
top Preserve log
Uncaught Error: addPkiObject Error add certificate to store pkistore.ts:209
  ..deps/wrapper/src/store/pkistore.cpp:412
  addPkiObject Error add certificate to store
  ..deps/wrapper/src/store/provider_cryptoarm.cpp:484
  addPkiObject CertAddCertificateContextToStore failed. Code: -2147024891
  ..deps/wrapper/src/store/provider_cryptoarm.cpp:449

  at PkiStore.addCert (pkistore.ts:209)
  at ue.value (store.ts:250)
  at store.ts:265
  at cert.ts:81
  at /Applications/CryptoARM-GOST.app/Contents/Resources/app/node_modules/async/dist/async.js:460
  at iteratorCallback (/Applications/CryptoARM-GOST.app/Contents/Resources/app/node_modules/async/dist/async.js:1034)
  at /Applications/CryptoARM-GOST.app/Contents/Resources/app/node_modules/async/dist/async.js:944
  at cert.ts:73
  at WriteStream.<anonymous> (download.ts:26)
  at emitNone (events.js:86)
> |
```

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 находиться 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/cproscsp/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/cproscsp/bin/<arch>/csptest -keyset -enum_cont -fqcn -verifycontext
```

Привязать сертификат к закрытому ключу можно командой

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

Выполнить проверку привязки сертификата к закрытому ключу можно через команду

```
/opt/cproscsp/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 КриптоПро CSP. В появившемся диалоге перейти на вкладку **Сервис**, как показано на рис.8.2.1.

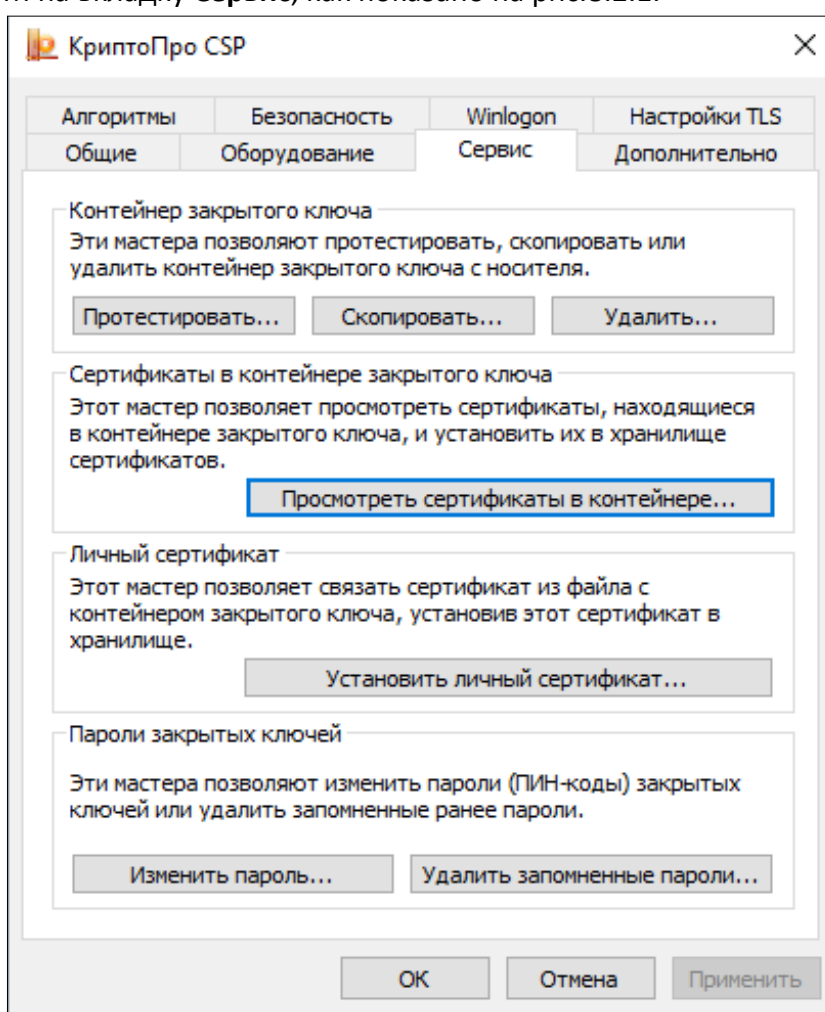


Рис.8.2.1. Диалог настроек криптопровайдера. Вкладка Сервис

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



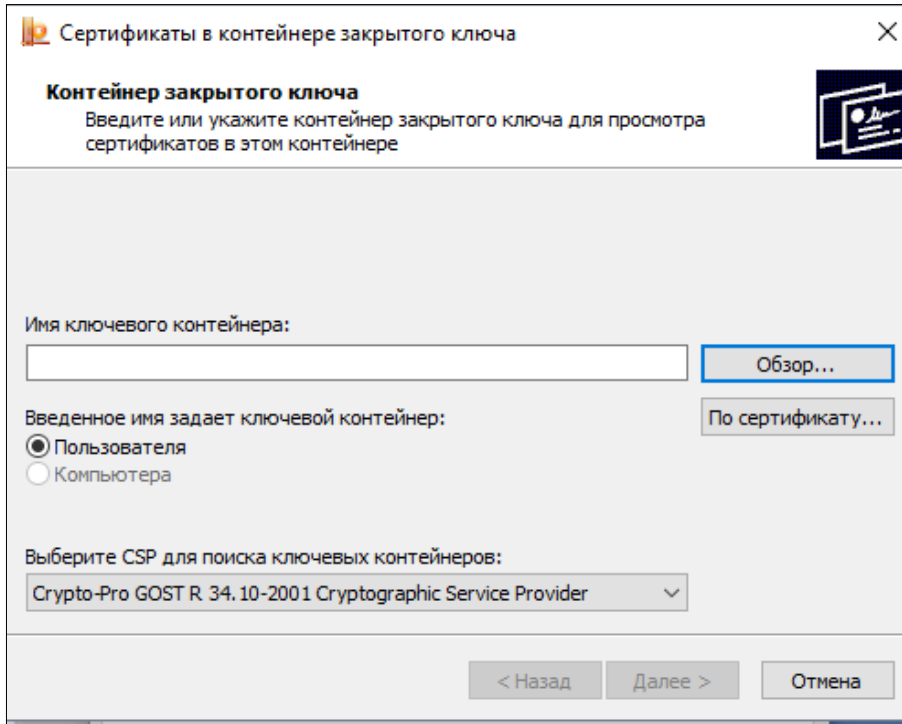


Рис.8.2.2. Диалог поиска ключевого контейнера

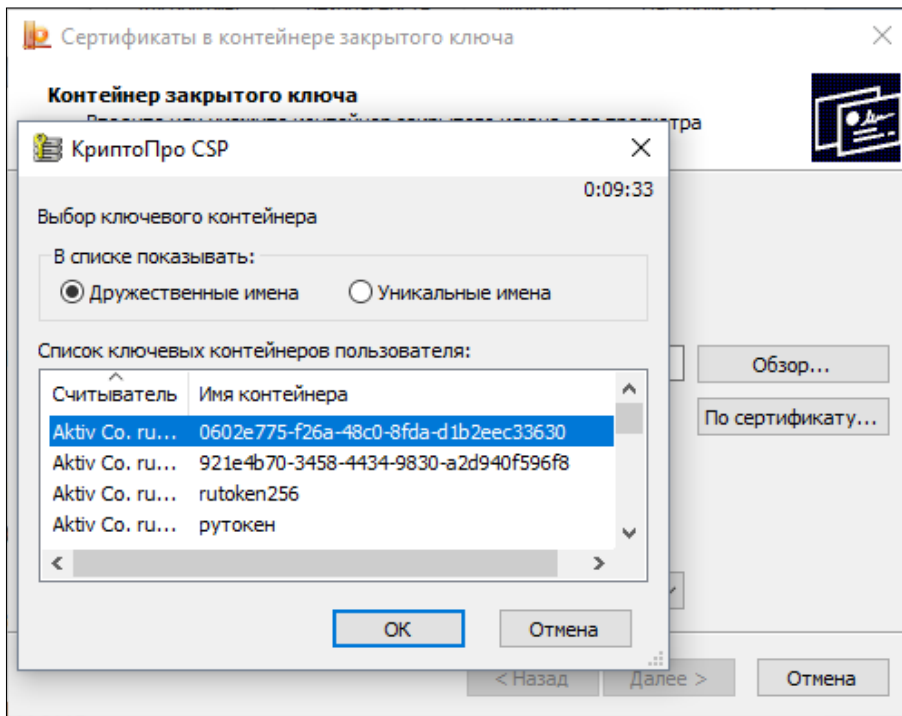


Рис.8.2.3. Выбор ключевого контейнера

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

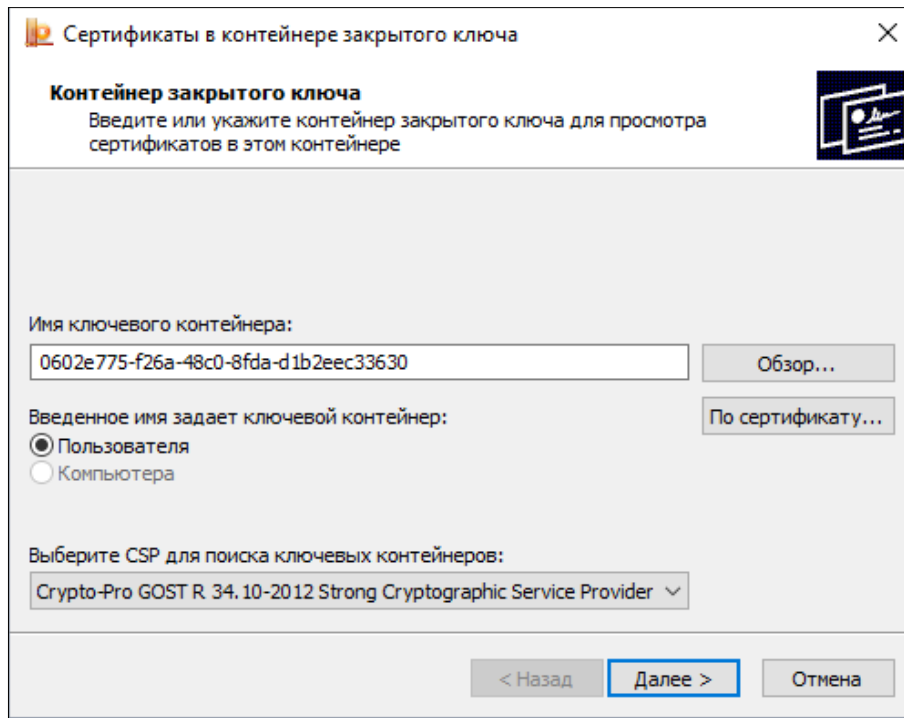


Рис.8.2.4. Просмотр содержимого контейнера

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**.

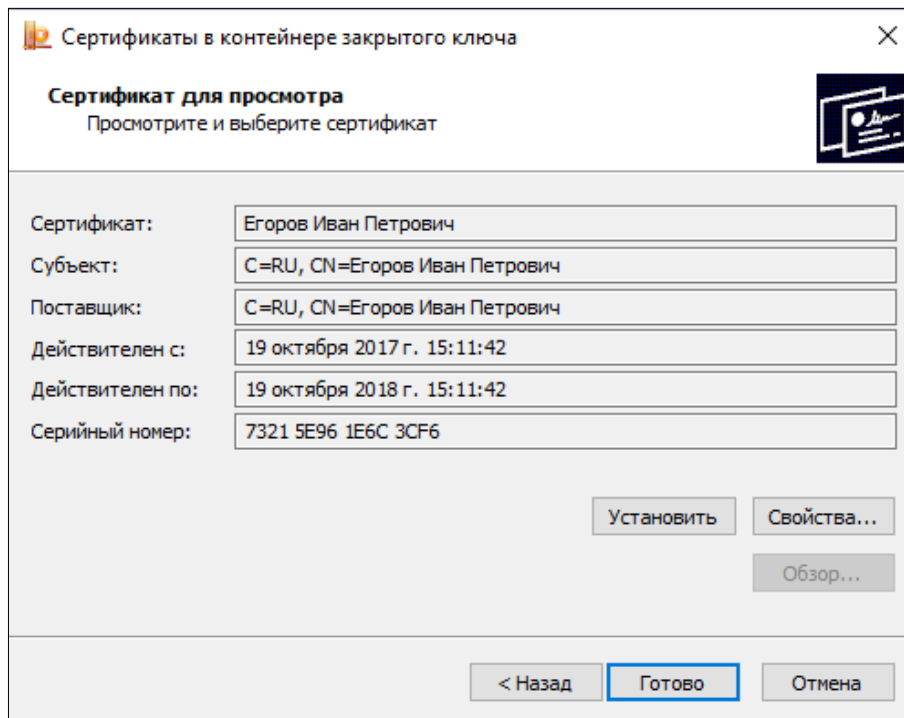


Рис.8.2.5. Сведения о сертификате внутри контейнера

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/cproccsp/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/cproccsp/sbin/<arch>/cpconfig -hardware reader -add "имя_устройства", где  
в кавычках указывается имя устройства. Например, sudo  
/opt/cproccsp/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/cproccsp/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/cproccsp/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/cproccsp/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/cprosp/sbin/cpconfig -hardware reader -add "имя_устройства", где в кавычках указывается имя устройства. Например, sudo /opt/cprosp/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/cprosp/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/cprosp/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/cprosp/bin/<arch>/certmgr -inst -cert -file <название файла корневого сертификата>.cer -store uRoot
```

- Установка цепочки промежуточных сертификатов

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

- Установка списка отозванных сертификатов

```
/opt/cprosp/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 DEV 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@dig.t.ru](mailto:andrey.selyodkin@dig.t.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](mailto: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@dig.t.ru](mailto:alg@dig.t.ru)

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

### **Шалагина Наталья Владимировна**

Специалист по тестированию, [nsh@dig.t.ru](mailto:nsh@dig.t.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 поддержке отечественных стандартов защиты информации, в том числе сертифицированных продуктов.

В случае необходимости получения дополнительной информации по продукту КристоАРМ ГОСТ, можно обратиться непосредственно к разработчикам продукта или в службу технической поддержки компании – [support@trusted.ru](mailto:support@trusted.ru).

Контактная информация:



[info@trusted.ru](mailto: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