Цифровые технологии

КриптоАРМ ГОСТ · Архив

Документация продукта

Релиз Архивное руководство

Исходная документация на CryptoARM.ru

Редакция от 25.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Архив 5

Исходные оглавления

- Содержание 6
- Общие сведения 8
- Работа с программой 10
- Инструкции 11
- Часто задаваемые вопросы 12

Общие сведения

- Поддерживаемые операционные системы, криптопровайдеры 13
- Где скачать дистрибутив КриптоАРМ ГОСТ 14
- Как установить КриптоАРМ ГОСТ на платформу Microsoft Windows 15
- Как установить КриптоАРМ ГОСТ на платформу Linux 20
- Как установить КриптоАРМ ГОСТ на платформу OS X 21
- Как удалить КриптоАРМ ГОСТ на платформе MS Windows 27
- Как удалить КриптоАРМ ГОСТ на платформе Linux 28
- Как удалить КриптоАРМ ГОСТ на платформе OS X 29
- Где приобрести лицензию на право использования программы 30
- Как установить лицензию на КриптоАРМ ГОСТ 31
- Временная лицензия, что в нее входит, срок действия 34
- Установка криптопровайдера на платформу MS WINDOWS 35
- Установка криптопровайдера на платформу LINUX 39
- Установка криптопровайдера на платформу OS X 41
- Инструкция по диагностике рабочего места 47
- Каталог Документы 56
- Журнал операций 61
- Перенос контейнера закрытого ключа под требуемую операционную систему 64
- Установка сертификата с токена с сохранением привязки к закрытому ключу 66
- Установка доверенных корневых, промежуточных сертификатов и списка отзыва сертификата 75
- Отсутствует СКЗИ КриптоПро CSP 84
- Отсутствует лицензия на КриптоАРМ ГОСТ 85

Не загружен модуль Trusted Crypto 86
Документация КриптоАРМ ГОСТ 91

Работа с программой

Начальная страница 92
Создание электронной подписи 94
Установка параметров подписи 98
Проверка электронной подписи 101
Снятие электронной подписи 106
Добавление подписи 108
Как зашифровать файлы с помощью КриптоАРМ ГОСТ 111
Как расшифровать файлы с помощью КриптоАРМ ГОСТ 118
Создание подписи со штампом времени (TSP) 121
Создание усовершенствованной подписи 124
Управление параметрами операций 128
Архивирование файлов 133
Операции с сертификатами и ключами 137
Импорт сертификата из файла 140
Импорт сертификата из DSS 145
Экспорт сертификата в файл 148
Удаление сертификата 151
Создание запроса на сертификат 153
Создание самоподписанного сертификата 160
Списки отзыва сертификатов 162
Установка сертификата из ключевого контейнера 166
Подпись сертификатом DSS 169
Включение режима логирования и консоль управления 173
Отслеживание ошибок на платформе MS Windows 174
Отслеживание ошибок на платформе Linux 176
Отслеживание ошибок на платформе OS X 178

Инструкции

Как подписать и подать проектную документацию в Главгосэкспертизу 180
Как подписать документы в МоемСкладе мобильной электронной подписью 182
Как обмениваться документами с электронной подписью 194

Как отправить запрос в Удостоверяющий центр и получить сертификат электронной подписи ... 208
Как подписать документы мобильной подписью Билайн в КриптоАРМ ГОСТ ... 225
Что нужно для юридически значимого ЭДО ... 235
Как проверить подлинность электронной подписи на документе ... 237
Как установить сертификат из DSS (облачную подпись) в КриптоАРМ ГОСТ ... 241
Как подписать исковое заявление через ГАС “Правосудие” и “Мой арбитр” ... 246
Как подписать документ электронной подписью в КриптоАРМ ГОСТ ... 261
Как подписать межевой план электронной подписью и загрузить его на сайт Росреестра . 269
Как нотариально заверить документы в КриптоАРМ ГОСТ ... 277
Как подписать госконтракт электронной подписью ... 285
Как подписать запрос предложения электронной подписью ... 293
Как подписать котировочную заявку электронной подписью ... 301
Как подписать декларацию в ФСРАР ... 309

Часто задаваемые вопросы

Ошибка при записи в файл во время установки лицензии ... 321
Не устанавливается КриптоАРМ ГОСТ на MacOS ... 324
При выполнении операции произошла ошибка ... 326
В полях сертификата вместо букв знаки вопроса ... 328
Не запускается КриптоАРМ ГОСТ на Windows или запускается, но висит белым окном ... 330
Не обнаружены сертификаты с привязкой к ключевому контейнеру ... 332
Не удалось получить сертификат сервиса при открытии КриптоАРМ ГОСТ по ссылке с внешнего сервиса ... 334
Сертификат недействительный ... 336

Открыть статью на сайте

КриптоАРМ ГОСТ

Архивное руководство.

- Содержание
- Общие сведения
- Работа с программой
- Инструкции
- Часто задаваемые вопросы

Открыть статью на сайте

Содержание

Архив. КриптоАРМ ГОСТ.

Общие сведения

Установка и настройка КриптоАРМ ГОСТ

- Поддерживаемые операционные системы, криптопровайдеры
- Где скачать дистрибутив КриптоАРМ ГОСТ
- Как установить КриптоАРМ ГОСТ на платформу Microsoft Windows
- Как установить КриптоАРМ ГОСТ на платформу Linux
- Как установить КриптоАРМ ГОСТ на платформу OS X
- Как удалить КриптоАРМ ГОСТ на платформе MS Windows
- Как удалить КриптоАРМ ГОСТ на платформе Linux
- Как удалить КриптоАРМ ГОСТ на платформе OS X
- Где приобрести лицензию на право использования программы
- Как установить лицензию на КриптоАРМ ГОСТ?
- Временная лицензия, что в нее входит, срок действия
- Установка криптопровайдера на платформу MS WINDOWS
- Установка криптопровайдера на платформу LINUX
- Установка криптопровайдера на платформу OS X

Графический пользовательский интерфейс приложения

- Каталог Документы
- Журнал операций

Как установить сертификат

- Перенос контейнера закрытого ключа под требуемую операционную систему
- Установка сертификата с токена с сохранением привязки к закрытому ключу
- Установка доверенных коневых, промежуточных сертификатов и списка отзыва сертификата

Диагностика неполадок при запуске приложения

- Отсутствует СКЗИ КриптоПро CSP
- Отсутствует лицензия на КриптоАРМ ГОСТ
- Не загружен модуль Trusted Crypto

Работа с программой

- Начальная страница
- Создание электронной подписи
- Установка параметров подписи
- Проверка электронной подписи
- Снятие электронной подписи
- Добавление подписи
- Как зашифровать файлы с помощью КриптоАРМ ГОСТ
- Как расшифровать файлы с помощью КриптоАРМ ГОСТ
- Создание подписи со штампом времени (TSP)
- Создание усовершенствованной подписи
- Управление параметрами операций
- Архивирование файлов
- Операции с сертификатами и ключами
  - Импорт сертификата из файла
  - Импорт сертификата из DSS
  - Экспорт сертификата в файл
  - Удаление сертификата
  - Создание запроса на сертификат
  - Создание самоподписанного сертификата
  - Списки отзыва сертификатов
  - Установка сертификата из ключевого контейнера
- Подпись сертификатом DSS
- Включение режима логирования и консоль управления
  - Отслеживание ошибок на платформе MS Windows
  - Отслеживание ошибок на платформе Linux
  - Отслеживание ошибок на платформе OS X

Часто задаваемые вопросы

- Ошибка при записи в файл во время установки лицензии
- Не устанавливается КриптоАРМ ГОСТ на MacOS
- При выполнении операции произошла ошибка
- В полях сертификата вместо букв знаки вопроса
- Не запускается КриптоАРМ ГОСТ на Windows или запускается, но висит белым окном
- Не обнаружены сертификаты с привязкой к ключевому контейнеру
- Не удалось получить сертификат сервиса при открытии КриптоАРМ ГОСТ по ссылке с внешнего сервиса
- Сертификат недействительный

Открыть статью на сайте

Общие сведения

Архив. КриптоАРМ ГОСТ.

Установка и настройка КриптоАРМ ГОСТ

- Поддерживаемые операционные системы, криптопровайдеры
- Где скачать дистрибутив КриптоАРМ ГОСТ
- Как установить КриптоАРМ ГОСТ на платформу Microsoft Windows
- Как установить КриптоАРМ ГОСТ на платформу Linux
- Как установить КриптоАРМ ГОСТ на платформу OS X
- Как удалить КриптоАРМ ГОСТ на платформе MS Windows
- Как удалить КриптоАРМ ГОСТ на платформе Linux
- Как удалить КриптоАРМ ГОСТ на платформе OS X
- Где приобрести лицензию на право использования программы
- Как установить лицензию на КриптоАРМ ГОСТ?
- Временная лицензия, что в нее входит, срок действия
- Установка криптопровайдера на платформу MS WINDOWS
- Установка криптопровайдера на платформу LINUX
- Установка криптопровайдера на платформу OS X

Графический пользовательский интерфейс приложения

- Каталог Документы
- Журнал операций

Как установить сертификат

- Перенос контейнера закрытого ключа под требуемую операционную систему
- Установка сертификата с токена с сохранением привязки к закрытому ключу
- Установка доверенных коневых, промежуточных сертификатов и списка отзыва сертификата

Диагностика неполадок при запуске приложения

- Отсутствует СКЗИ КриптоПро CSP
- Отсутствует лицензия на КриптоАРМ ГОСТ
- Не загружен модуль Trusted Crypto

Работа с программой

- Начальная страница

- Создание электронной подписи
- Установка параметров подписи
- Проверка электронной подписи
- Снятие электронной подписи
- Добавление подписи
- Как зашифровать файлы с помощью КриптоАРМ ГОСТ
- Как расшифровать файлы с помощью КриптоАРМ ГОСТ
- Создание подписи со штампом времени (TSP)
- Создание усовершенствованной подписи
- Управление параметрами операций
- Архивирование файлов
- Операции с сертификатами и ключами
  - Импорт сертификата из файла
  - Импорт сертификата из DSS
  - Экспорт сертификата в файл
  - Удаление сертификата
  - Создание запроса на сертификат
  - Создание самоподписанного сертификата
  - Списки отзыва сертификатов
  - Установка сертификата из ключевого контейнера
- Подпись сертификатом DSS
- Включение режима логирования и консоль управления
  - Отслеживание ошибок на платформе MS Windows
  - Отслеживание ошибок на платформе Linux
  - Отслеживание ошибок на платформе OS X

Часто задаваемые вопросы

- Ошибка записи в файл при установке лицензии
- Не устанавливается КриптоАРМ ГОСТ на MacOS
- При выполнении операции произошла ошибка
- В полях сертификата вместо букв знаки вопроса
- Не запускается КриптоАРМ ГОСТ на Windows или запускается, но висит белым окном
- Не обнаружены сертификаты с привязкой к ключевому контейнеру
- Не удалось получить сертификат сервиса при открытии КриптоАРМ ГОСТ по ссылке с внешнего сервиса
- Сертификат недействительный

Открыть статью на сайте

Работа с программой

Архив. КриптоАРМ ГОСТ.

- Начальная страница
- Создание электронной подписи
- Установка параметров подписи
- Проверка электронной подписи
- Снятие электронной подписи
- Добавление подписи
- Как зашифровать файлы с помощью КриптоАРМ ГОСТ
- Как расшифровать файлы с помощью КриптоАРМ ГОСТ
- Создание подписи со штампом времени (TSP)
- Создание усовершенствованной подписи
- Управление параметрами операций
- Архивирование файлов
- Операции с сертификатами и ключами
- Импорт сертификата из файла
- Импорт сертификата из DSS
- Экспорт сертификата в файл
- Удаление сертификата
- Создание запроса на сертификат
- Создание самоподписанного сертификата
- Списки отзыва сертификатов
- Установка сертификата из ключевого контейнера
- Подпись сертификатом DSS

Включение режима логирования и консоль управления

- Отслеживание ошибок на платформе MS Windows
- Отслеживание ошибок на платформе Linux
- Отслеживание ошибок на платформе OS X

> Часто задаваемые вопросы
>
> - Ошибка при записи в файл

Открыть статью на сайте

Инструкции

Архив. КриптоАРМ ГОСТ.

- Как подписать исковое заявление через ГАС “Правосудие” и “Мой арбитр”
- Как подписать декларацию в ФСРАР
- Как подписать котировочную заявку электронной подписью
- Как подписать запрос предложения электронной подписью
- Как подписать госконтракт электронной подписью
- Как нотариально заверить документы в КриптоАРМ ГОСТ
- Как подписать межевой план электронной подписью и загрузить его на сайт Росреестра
- Как подписать документ электронной подписью в КриптоАРМ ГОСТ
- Как подписать и подать проектную документацию в Главгосэкспертизу
- Как установить сертификат из DSS (облачную подпись) в КриптоАРМ ГОСТ
- Как проверить подлинность электронной подписи на документе
- Что нужно для юридически значимого ЭДО
- Как подписать документы мобильной подписью Билайн в КриптоАРМ ГОСТ
- Как отправить запрос в Удостоверяющий центр и получить сертификат электронной подписи
- Как обмениваться документами с электронной подписью
- Как подписать документы в "МоемСкладе" мобильной электронной подписью

Открыть статью на сайте

Часто задаваемые вопросы

Архив. КриптоАРМ ГОСТ.

- Ошибка записи в файл при установке лицензии
- Не устанавливается КриптоАРМ ГОСТ на MacOS
- При выполнении операции произошла ошибка
- В полях сертификата вместо букв знаки вопроса
- Не запускается КриптоАРМ ГОСТ на Windows или запускается, но висит белым окном
- Не обнаружены сертификаты с привязкой к ключевому контейнеру
- Не удалось получить сертификат сервиса при открытии КриптоАРМ ГОСТ по ссылке с внешнего сервиса
- Сертификат недействительный

Открыть статью на сайте

Поддерживаемые операционные системы, криптопровайдеры

Архив. КриптоАРМ ГОСТ.

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

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.

Открыть статью на сайте

Где скачать дистрибутив КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ.

Скачать КриптоАРМ ГОСТ можно с сайта https://cryptoarm.ru/.

Нажмите на кнопку Скачать БЕСПЛАТНО для загрузки программы. При первой установке на рабочем месте активируется бесплатный период сроком на 14 дней.

Открыть статью на сайте

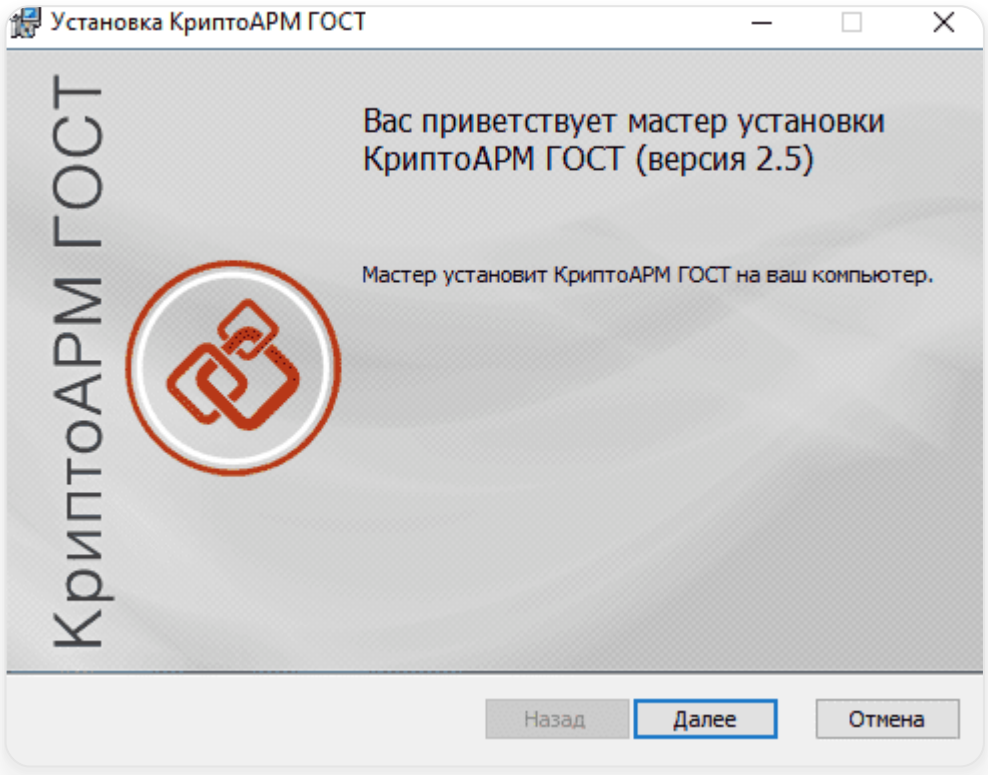
Как установить КриптоАРМ ГОСТ на платформу Microsoft Windows

Архив. КриптоАРМ ГОСТ.

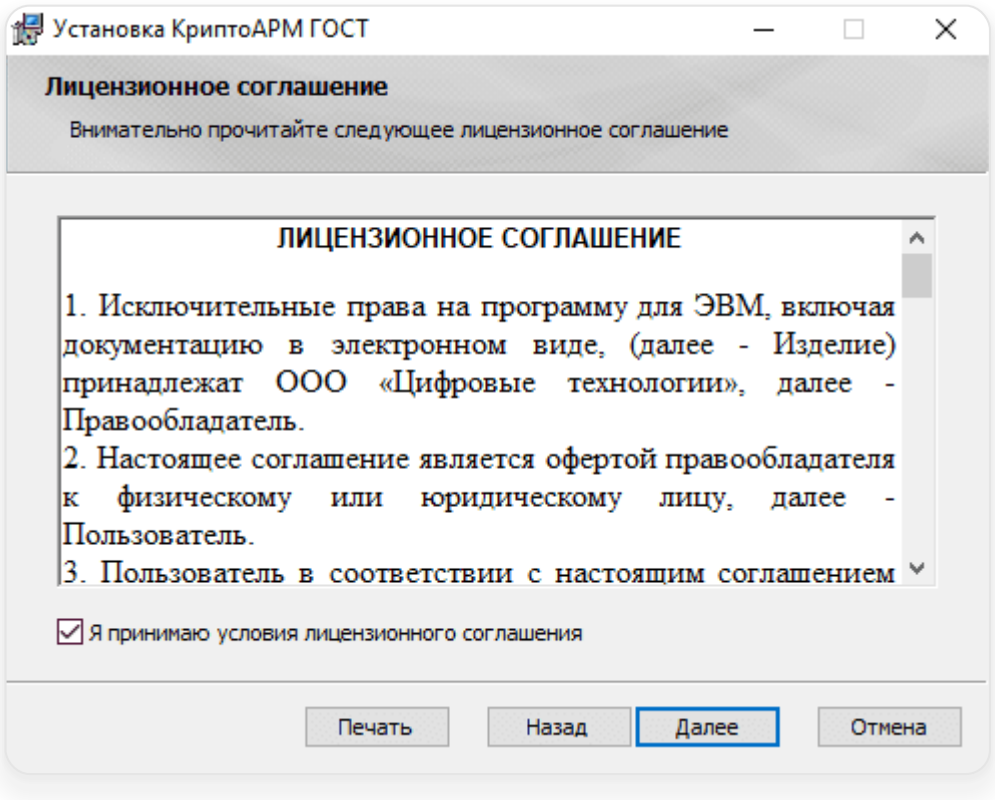
Для установки приложения КриптоАРМ ГОСТ на платформу Microsoft Windows предлагаются два дистрибутива – под 64-битную и 32-битную платформы. В зависимости от выбранной разрядности запустите на исполнение файл:

CryptoARM_GOST_vx.x.x_x64.exe (где x.x.x – номер версии) для 64-разрядной ОС;
CryptoARM_GOST _vx.x.x_x86.exe (где x.x.x – номер версии) для 32-разрядной ОС).

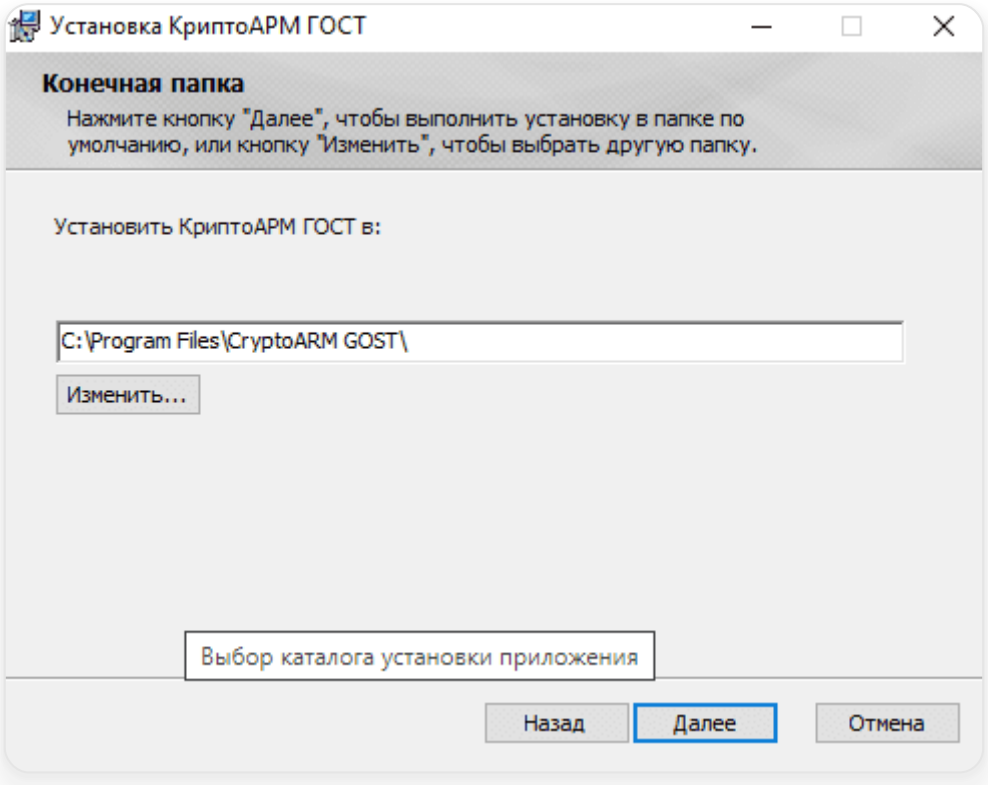
1. При запуске исполняемого файла открывается мастер установки приложения КриптоАРМ ГОСТ:



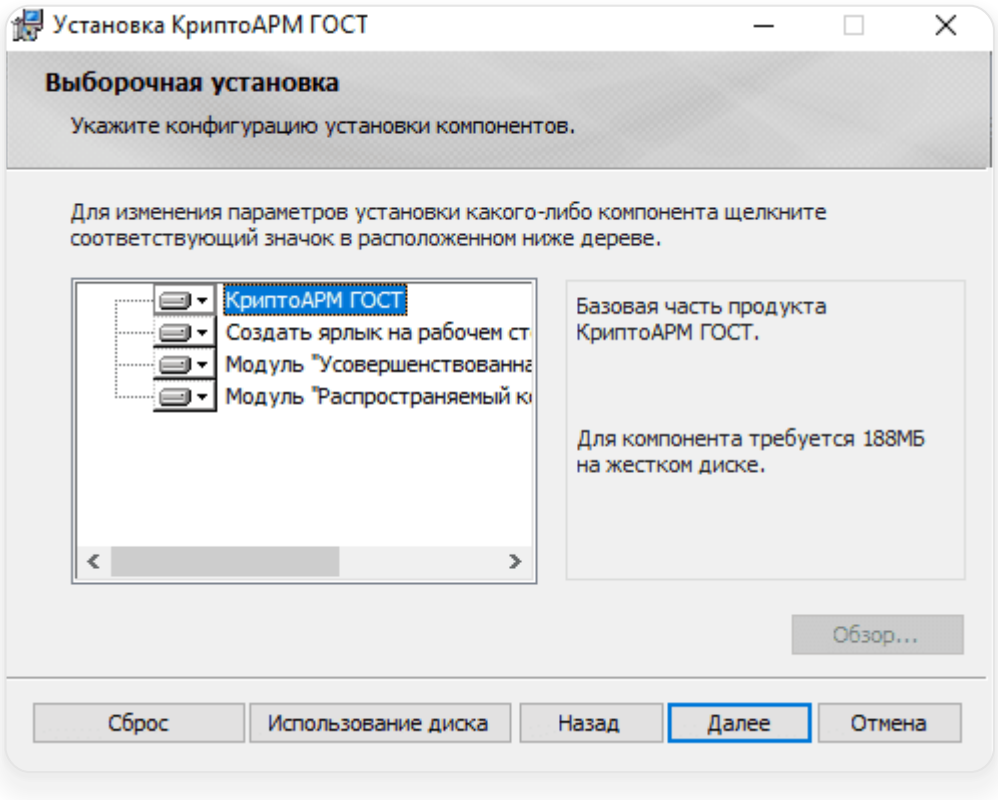
2. По кнопке **Далее** происходит переход на следующий шаг, где предлагается ознакомиться с условиями лицензионного соглашения. В случае согласия нужно **принять условия** и перейти к следующему шагу мастера, нажав кнопку **Далее**.



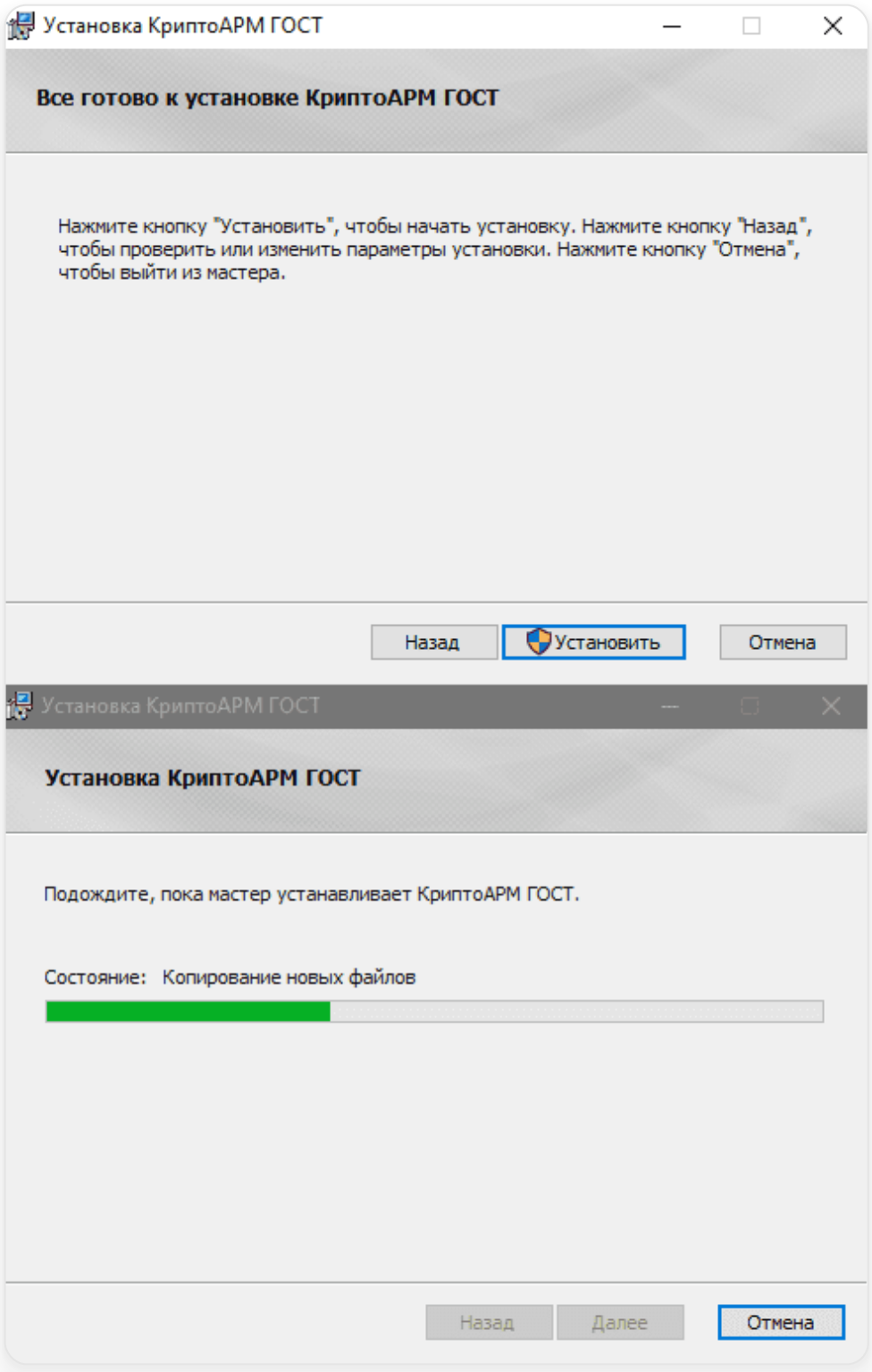
3. На следующем шаге мастера можно выбрать каталог для установки КриптоАРМ ГОСТ (по умолчанию приложение устанавливается в каталог C:\Program Files\CryptoARM GOST\).



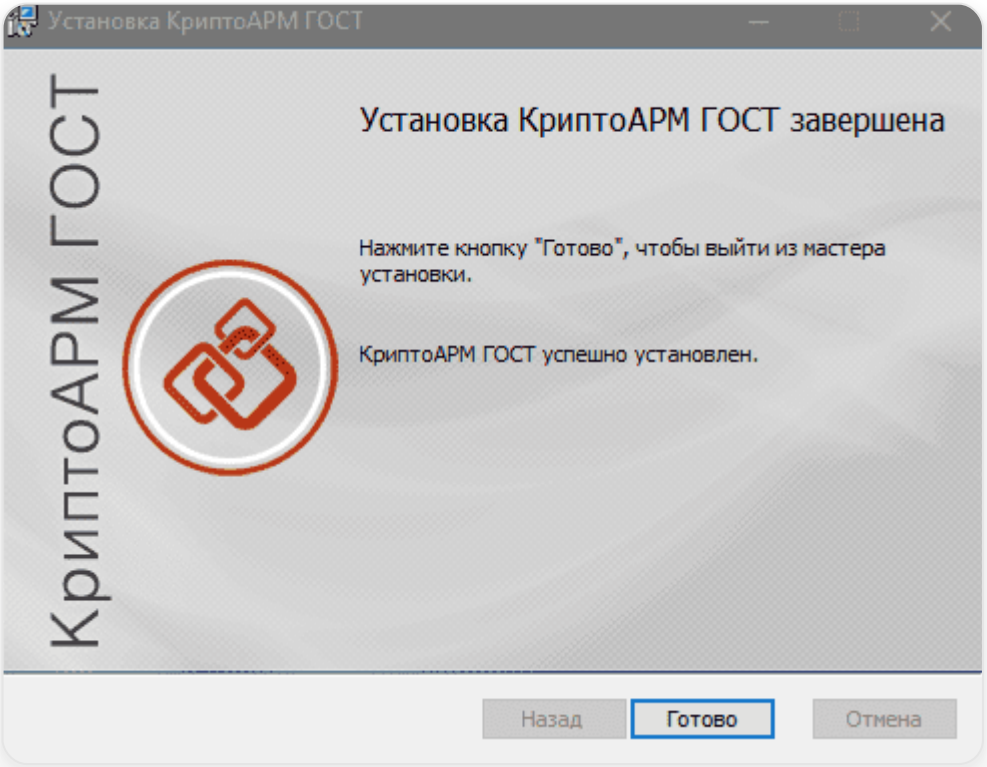
4.На шаге выборочной установки можно отключить создание ярлыка на рабочем столе и установку модулей для создания усовершенствованной подписи.



5. На заключительном шаге мастера по кнопке **Установить** выполняется установка. Нужны права администратора.



6. Закрыть окно установки, нажав **Готово**.



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 C:\Program Files\CryptoARM GOST) будут размещаться файлы приложения КриптоАРМ ГОСТ.

Открыть статью на сайте

Как установить КриптоАРМ ГОСТ на платформу Linux

Архив. КриптоАРМ ГОСТ.

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).

С помощью командной строки нужно запустить терминал и ввести команду:

- **sudo dpkg -i cryptoarm-gost-vx.x.x-x64.deb** — для ОС, основанных на Deb;
- **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.

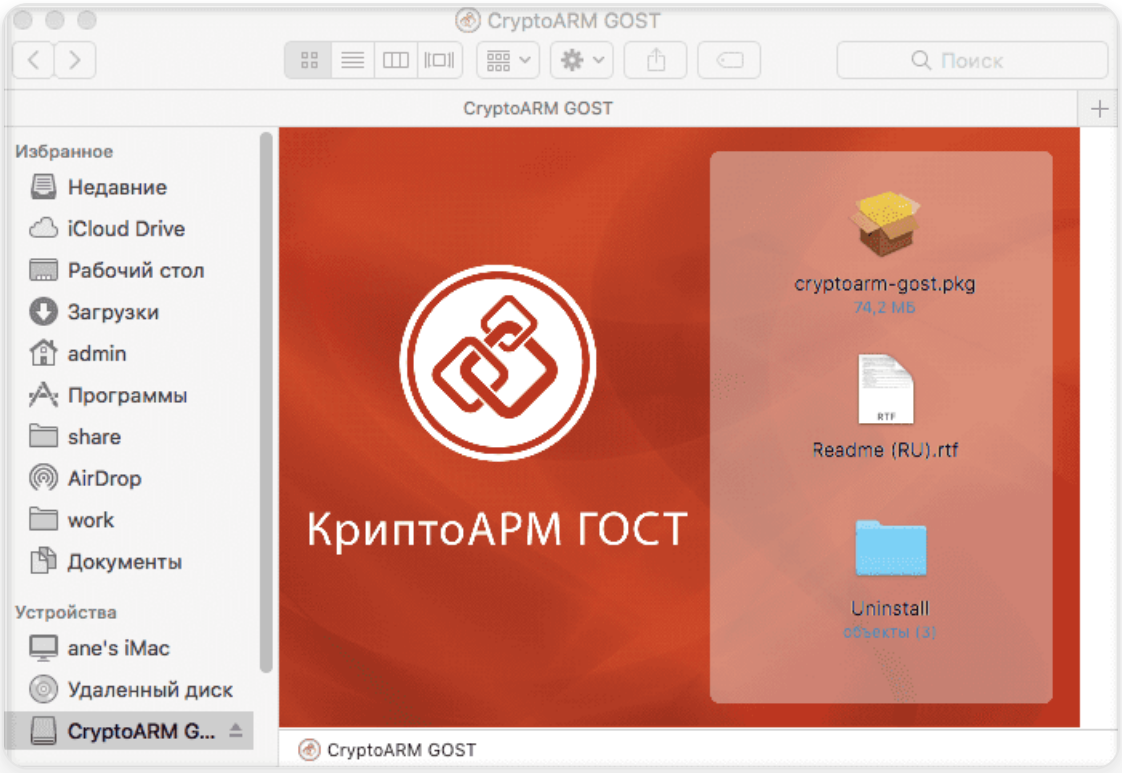
Открыть статью на сайте

Как установить КриптоАРМ ГОСТ на платформу OS X

Архив. КриптоАРМ ГОСТ.

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.

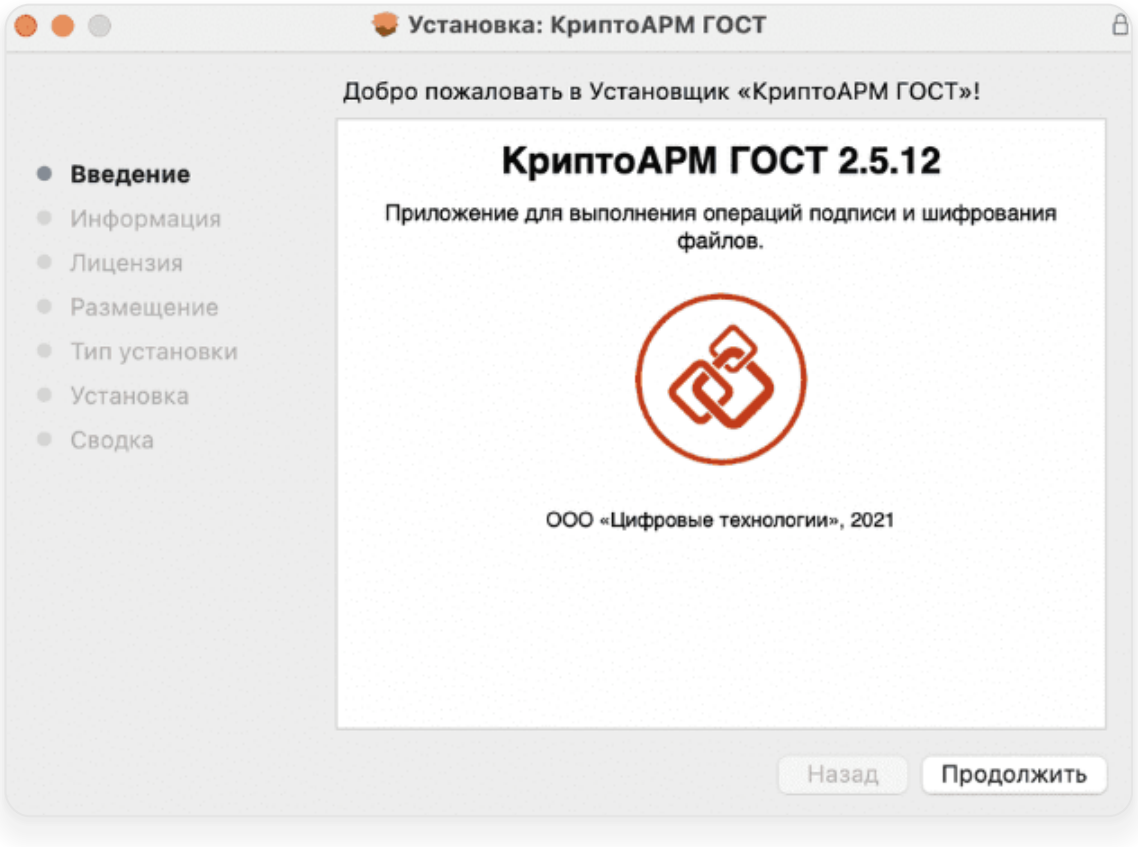
1. Для установки пакета через графический интерфейс откройте двойным щелчком образ диска с дистрибутивом **cryptoarm-gost-vx.x.x-x64.dmg** (где x.x.x – номер версии). При этом у вас может возникнуть уведомление системы безопасности, что файл является вредоносным ПО. Решение этой проблемы описано в инструкции.



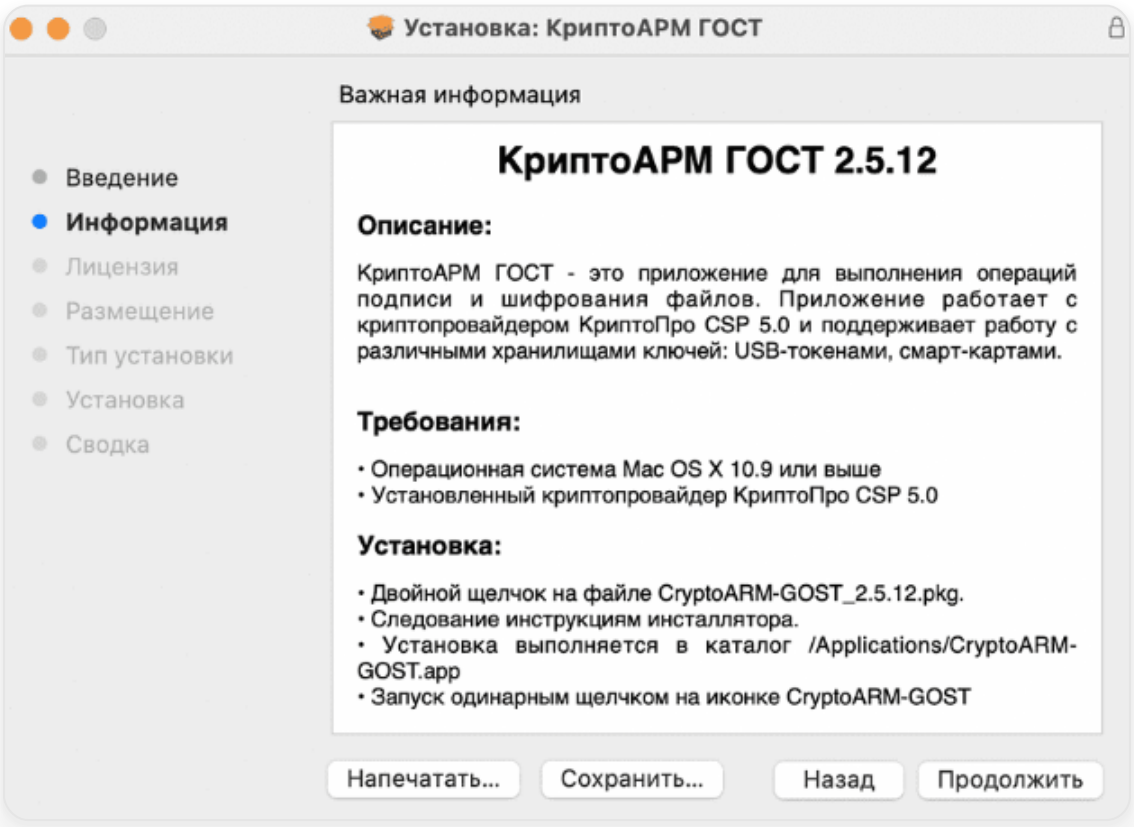
2. Для установки программы КриптоАРМ ГОСТ запустите на исполнение файл **cryptoarm-gost-vx.x.x-64.pkg** (где x.x.x – номер версии).

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).

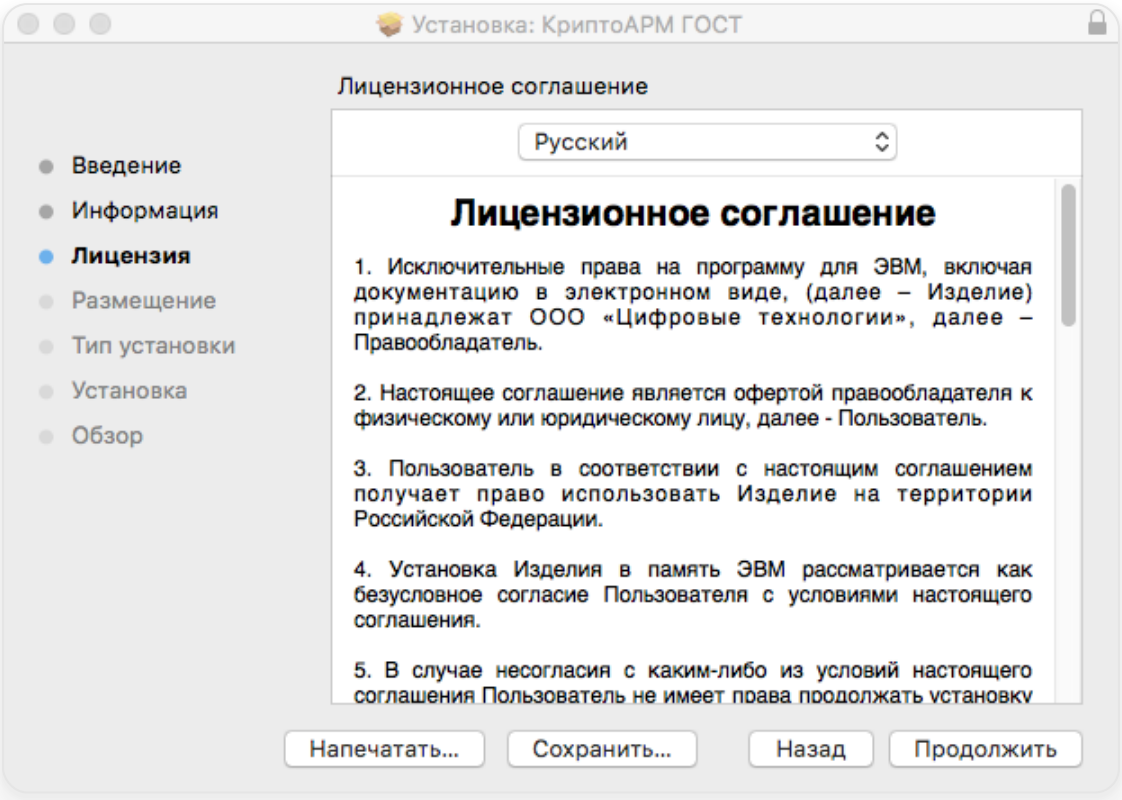
3. Откроется мастер установки КриптоАРМ ГОСТ. Для продолжения установки следует нажать кнопку **Продолжить**. На каждом шаге можно вернуться на предыдущий шаг нажатием **Назад**.



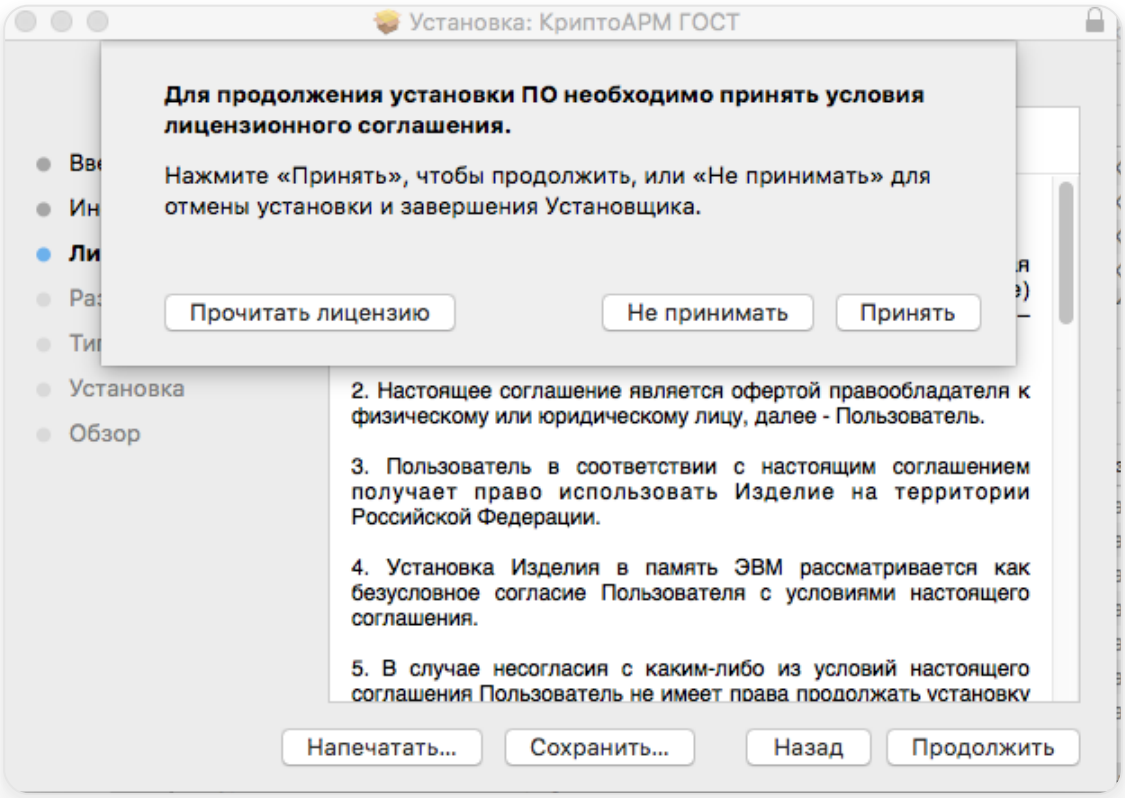
4. На следующем шаге предоставляется описание программы, которое можно распечатать или сохранить в файл. По кнопке **Продолжить** происходит переход на следующий шаг.



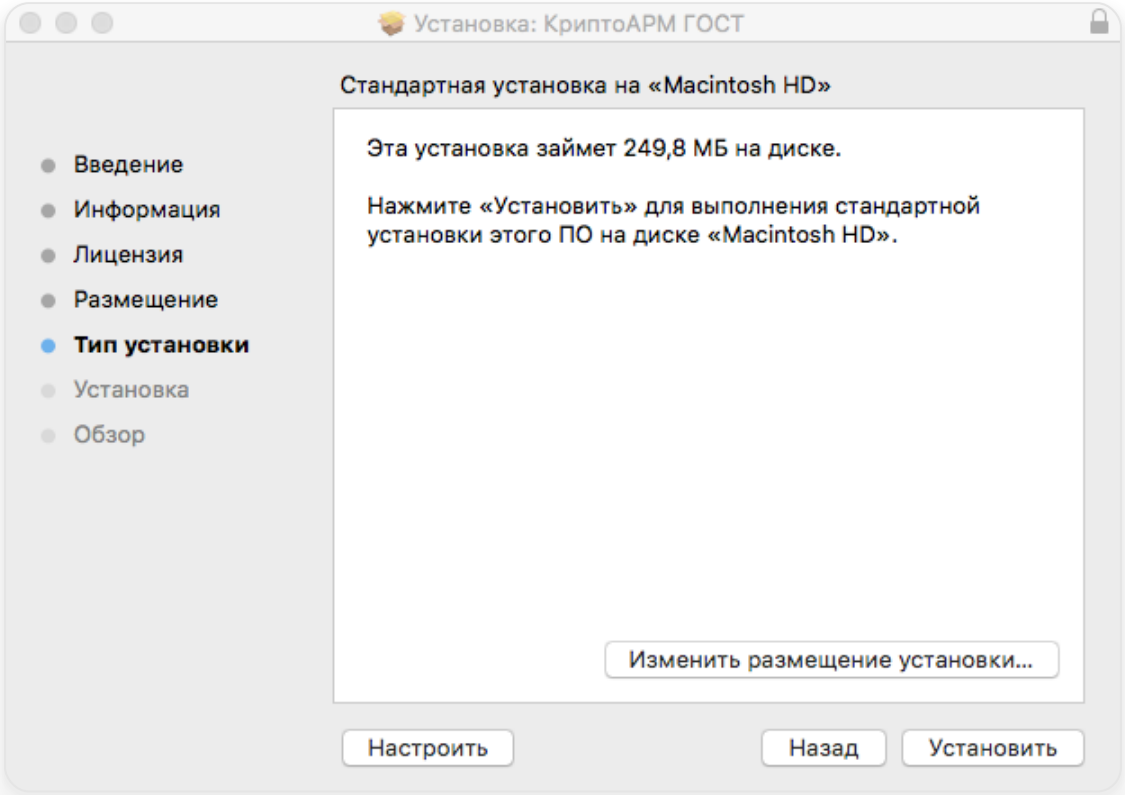
5. На этапе ознакомления с условиями лицензионного соглашения их можно распечатать или сохранить в файл.



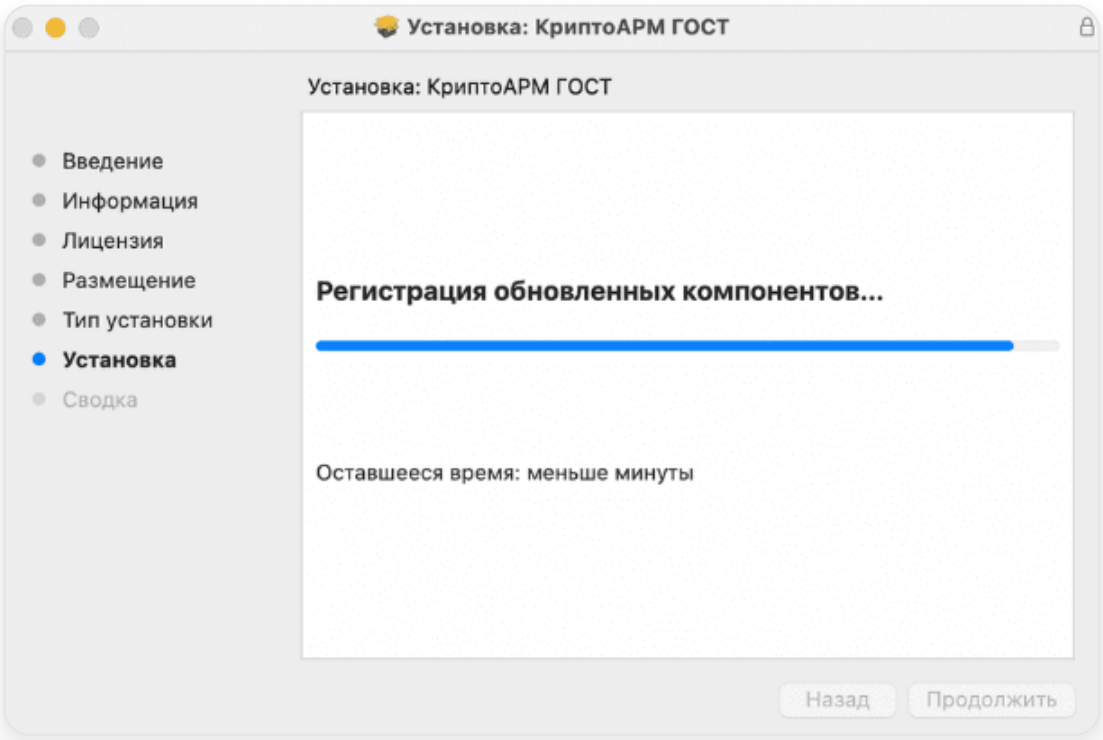
Принять условия лицензионного соглашения можно, нажав кнопку **Принять**. Установка продолжения продолжается. По кнопке **Не принимать** происходит отмена установки.



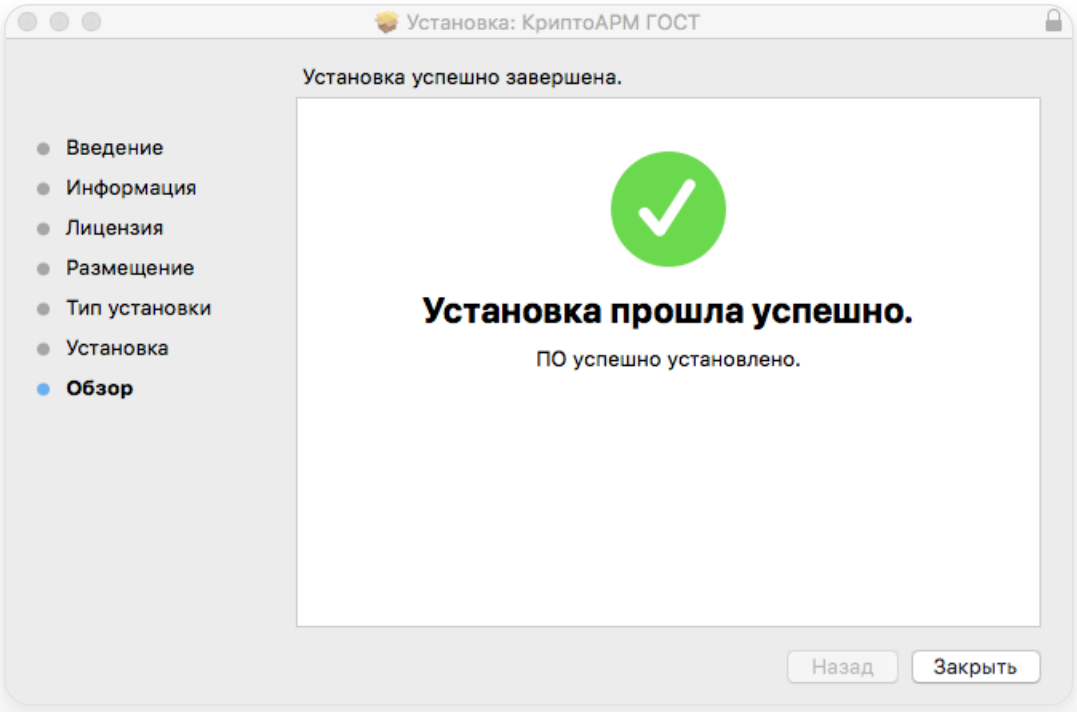
6. На последнем шаге мастера надо нажать кнопку **Установить** для завершения установки.



7. На запрос нужно **ввести** пароль администратора и нажать **Установить ПО**. Начнется установка программы на компьютер.



8. По окончании установки нужно нажать кнопку **Закрыть**.



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

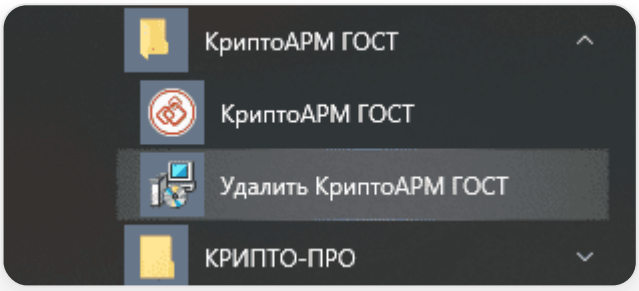
Открыть статью на сайте

Как удалить КриптоАРМ ГОСТ на платформе MS Windows

Архив. КриптоАРМ ГОСТ.

Удалить приложение КриптоАРМ ГОСТ можно следующим образом:

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



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.

Открыть статью на сайте

Как удалить КриптоАРМ ГОСТ на платформе Linux

Архив. КриптоАРМ ГОСТ.

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

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

2. Второй способ удаления основан на запуске команд в терминале:

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

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

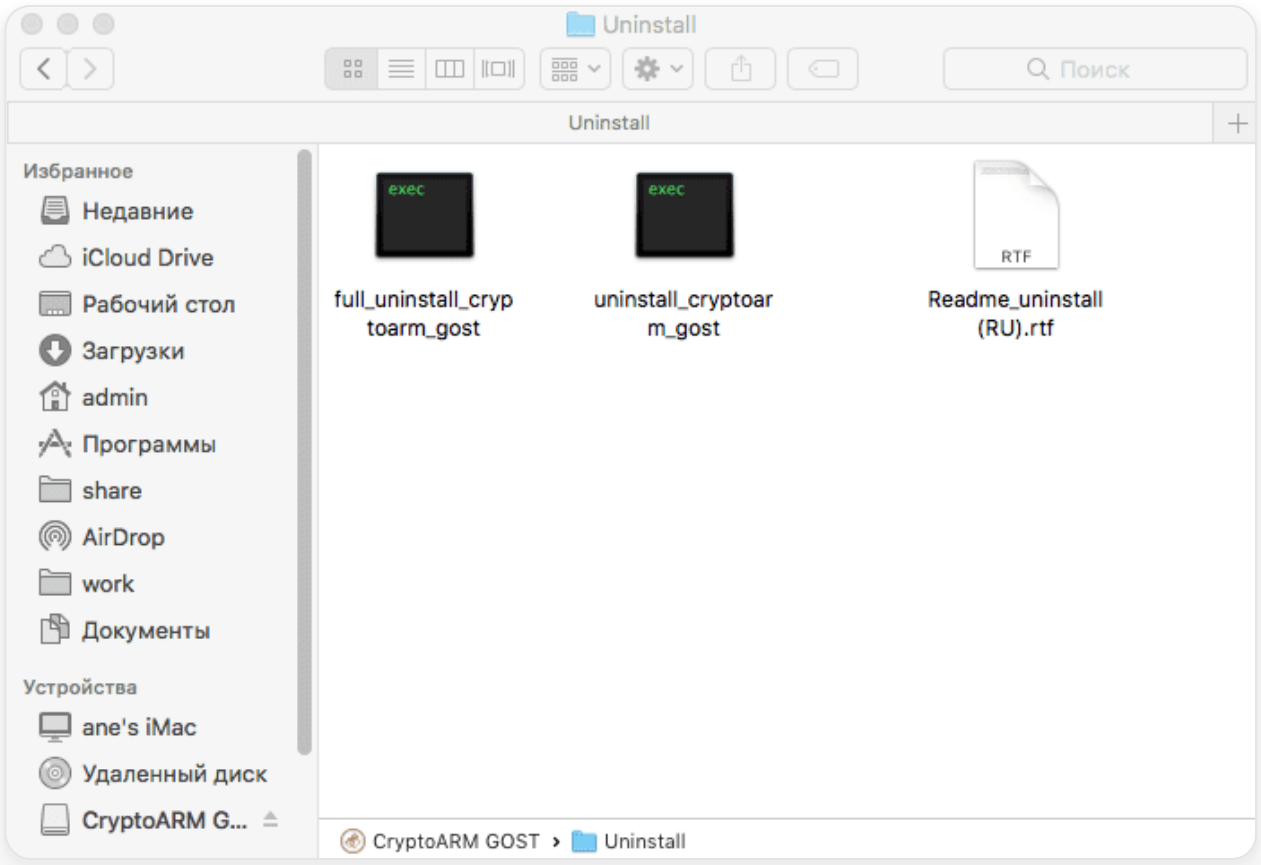
После выполнения команды приложение будет удалено из операционной системы.

Открыть статью на сайте

Как удалить КриптоАРМ ГОСТ на платформе OS X

Архив. КриптоАРМ ГОСТ.

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



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

Открыть статью на сайте

Где приобрести лицензию на право использования программы

Архив. КриптоАРМ ГОСТ.

Купить программу «КриптоАРМ ГОСТ» вы можете:

- Непосредственно в компании "Цифровые технологии". Для покупки товаров нажмите на кнопку **Магазин** в верхней части сайта cryptoarm.ru. Ознакомьтесь с инструкцией как оформить заказ или позвоните по телефону +7 (8362) 33-70-50. Если у вас возникнут вопросы, то вы можете написать на sales@cryptoarm.ru или задать их менеджеру в онлайн-чате, доступном в правом нижнем углу сайта.
- У официальных партнеров компании "Цифровые технологии" (ИТ-разработчики, удостоверяющие центры, системные интеграторы, интернет-магазины). Полный список региональных компаний-партнеров и их контактную информацию вы найдете на сайте в разделе "Партнеры".

Открыть статью на сайте

Как установить лицензию на КриптоАРМ ГОСТ

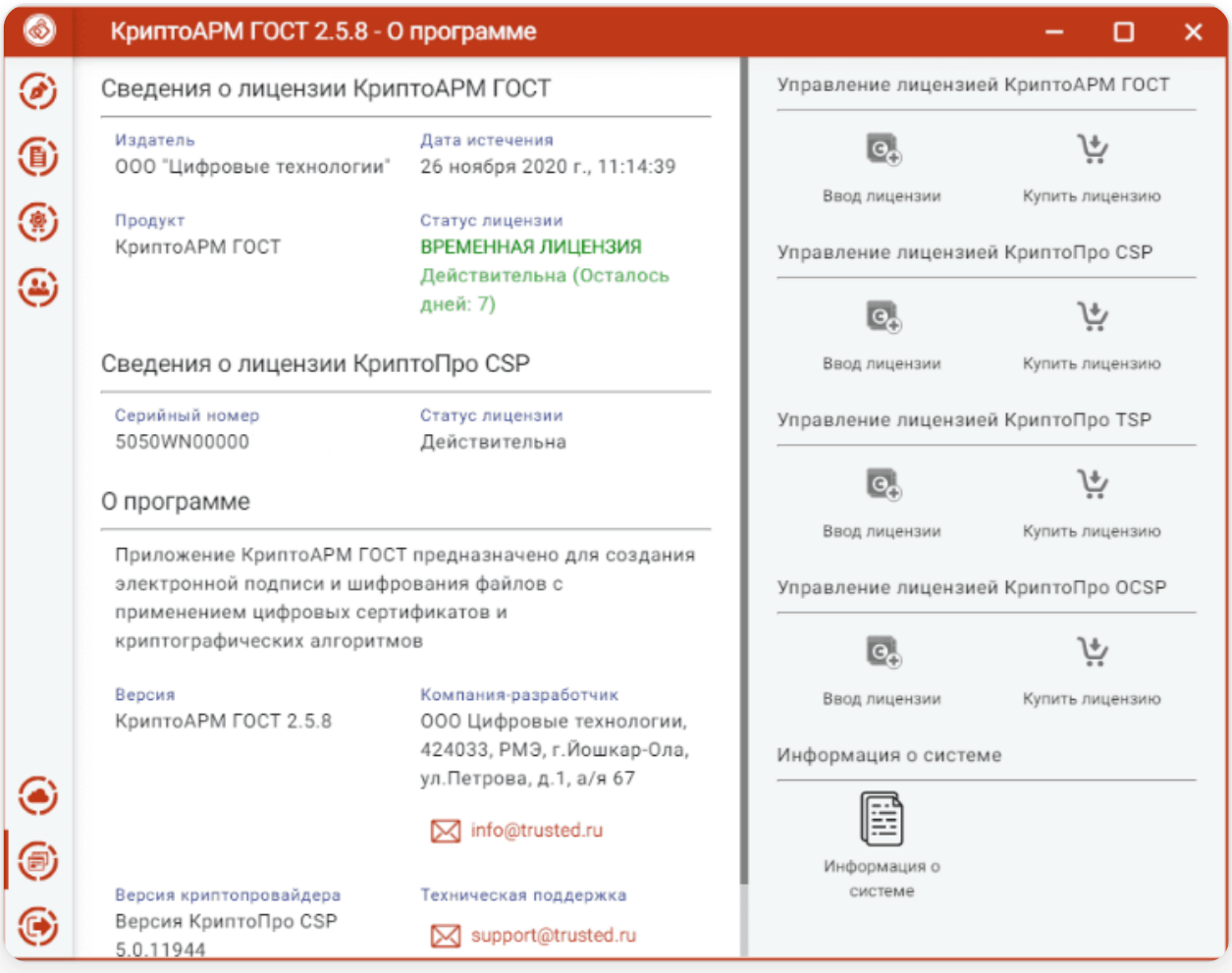
Архив. КриптоАРМ ГОСТ.

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

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

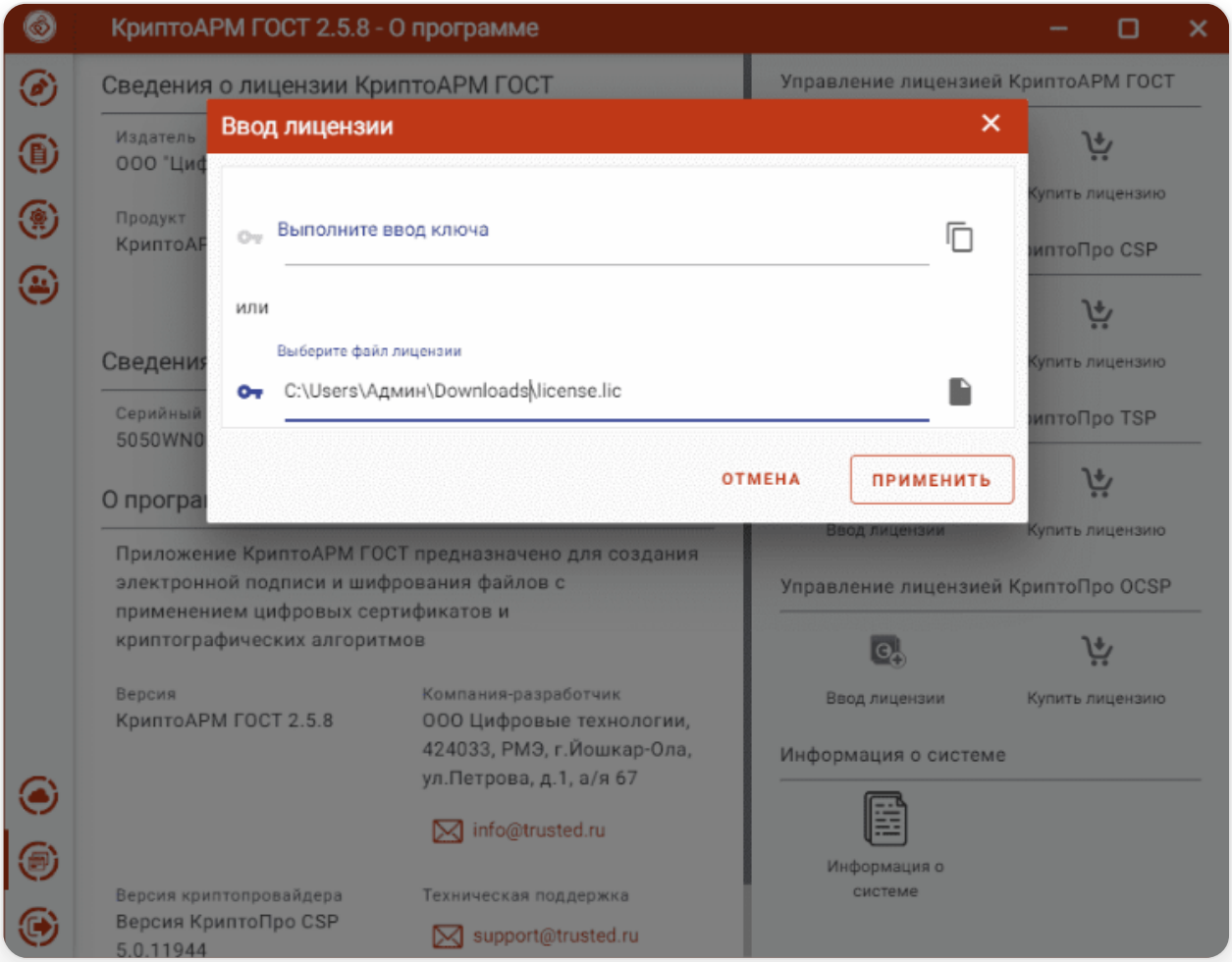
УСТАНОВКА ЛИЦЕНЗИИ ЧЕРЕЗ ПОЛЬЗОВАТЕЛЬСКИЙ ИНТЕРФЕЙС

Для установки лицензии нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения.



На открывшейся странице нажать на кнопку **Ввод лицензии** в разделе управления лицензией КриптоАРМ ГОСТ. В результате должно появиться всплывающее окно ввода лицензии, предполагающее выполнение действия одним из двух способов:

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



Необходимо ввести лицензию удобным способом и нажать **Применить**.

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

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

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

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 – 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.

Открыть статью на сайте

Временная лицензия, что в нее входит, срок действия

Архив. КриптоАРМ ГОСТ.

В течение 14 дней с момента установки КриптоАРМ ГОСТ работает в режиме с максимальным набором функциональных возможностей.

Ознакомительная версия НЕ для коммерческого использования. По истечении 14 дней программа автоматически переключается на версию, которая имеет ряд ограничений по сравнению с полнофункциональной версией, а именно - функционал программы будет ограничен. КриптоАРМ ГОСТ без постоянной лицензии выполняет только проверку подписанных файлов.

Открыть статью на сайте

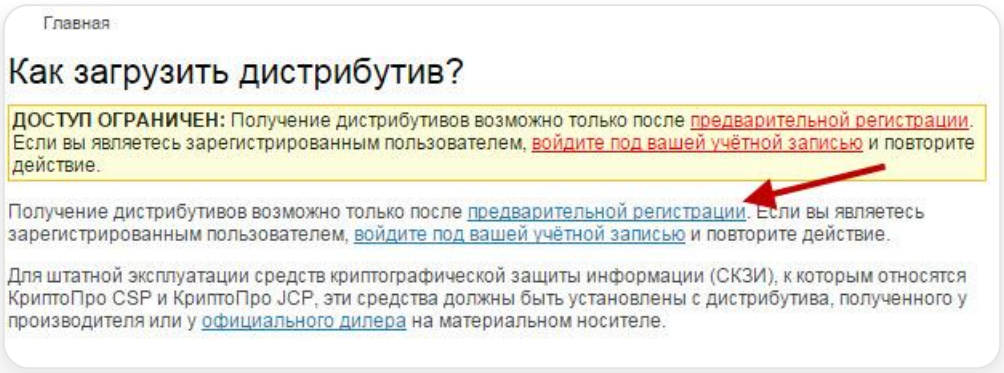
Установка криптопровайдера на платформу MS WINDOWS

Архив. КриптоАРМ ГОСТ.

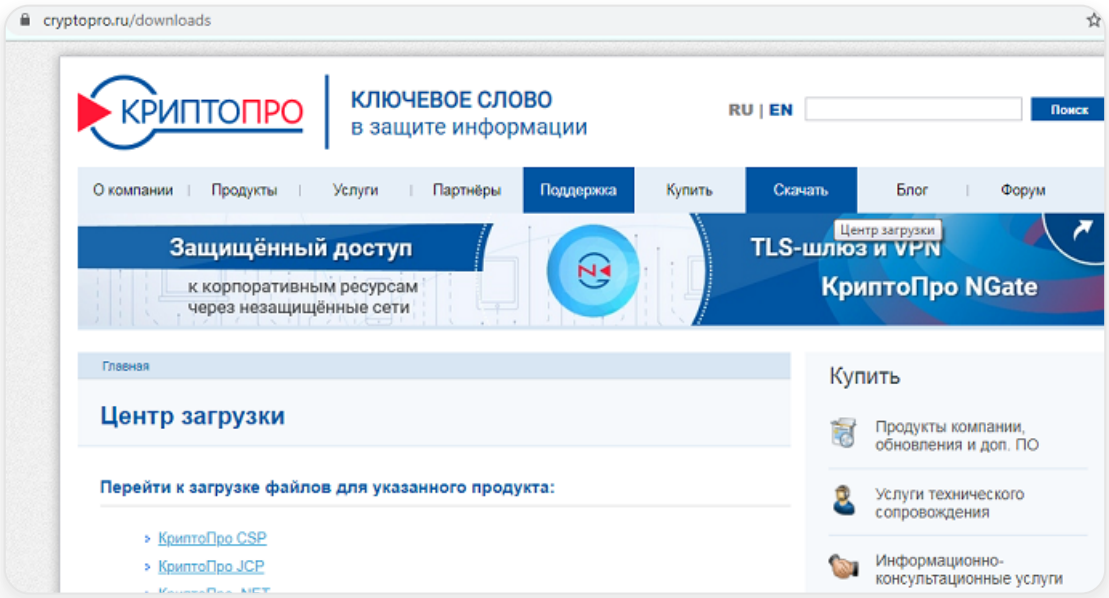
Скачать КриптоПро CSP можно с сайта разработчика - компании "КриптоПРО" по ссылке: **https://www.cryptopro.ru/downloads**.

На этом сайте понадобится пройти регистрацию так как криптопровайдер является средством криптографической защиты информации, а значит его распространение подлежит учету в соответствующих органах.

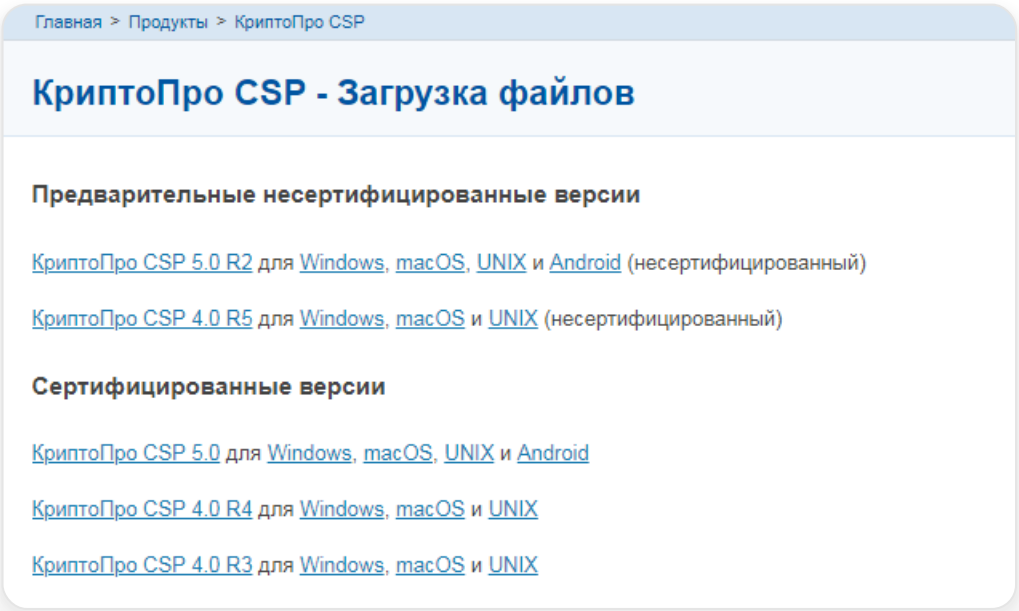
Нажмите на ссылку "**Предварительная регистрация**" и заполните форму из множества полей. После заполнения формы и регистрации, от вас потребуют согласиться с лицензионным соглашением, а затем все-таки получите возможность скачать дистрибутив программы.



Выберите на сайте раздел Центр загрузки (**Скачать**) и в списке нажмите на КриптоПро CSP.



По нажатию на ссылку **Windows** произойдет загрузка дистрибутива.

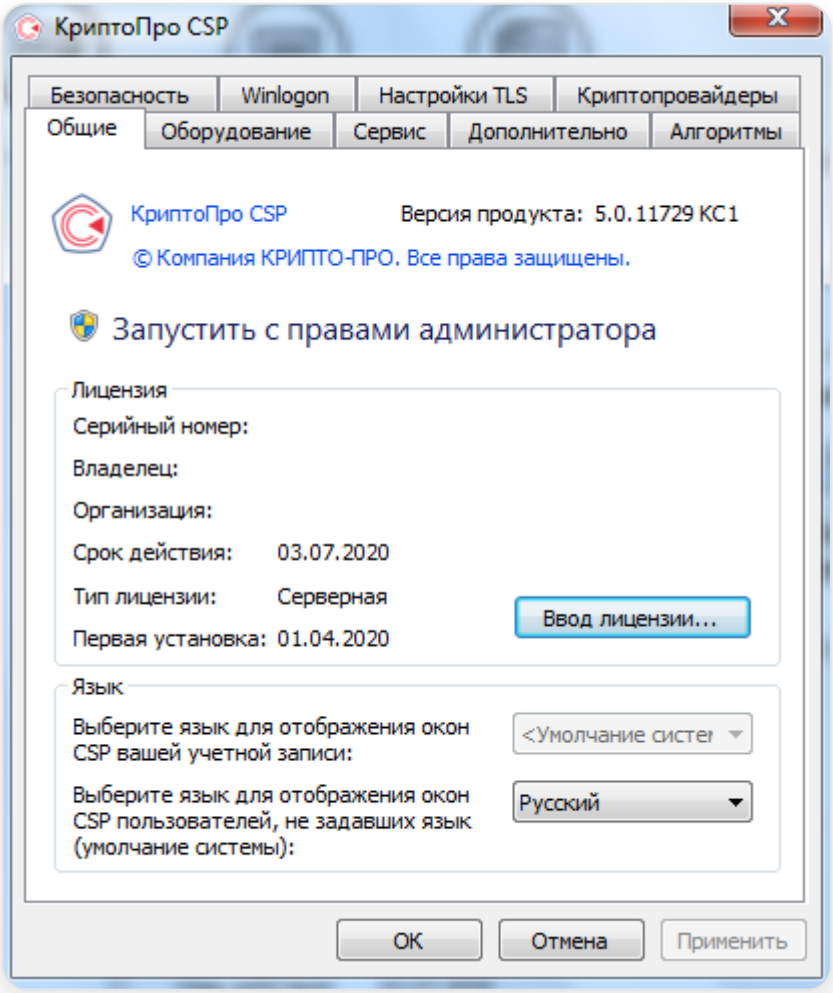


Далее нужно будет запустить установщик. Никаких дополнительный действий не потребуется, если возникнет оповещение безопасности, нужно будет разрешить программе внести изменения на вашем компьютере.

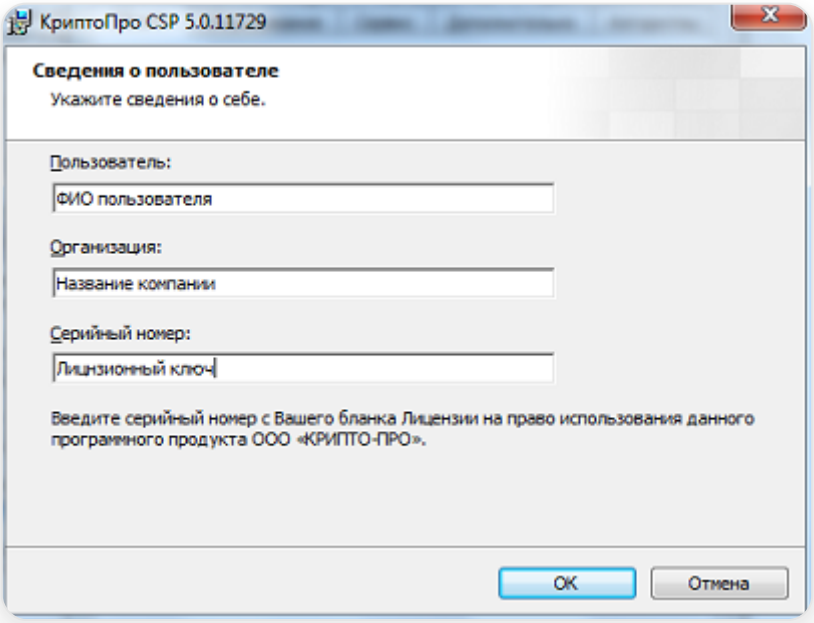
Инсталляция программы происходит в автоматическом режиме и не требует участия пользователя.

По завершению установки, если вы приобрели лицензионный ключ для КриптоПро CSP, внесите его в программу.
Для этого пройдите в меню **Пуск - Все программы - КриптоПро - КриптоПро CSP**. На вкладке

Общие в программе есть кнопка **Ввод лицензии**.



В открывшемся окне внесите данные пользователя, организации и лицензионный ключ, нажмите **OK**. Все программа активирована.


КриптоПро CSP 5.0.11729
Сведения о пользователе
Укажите сведения о себе.
Пользователь:
ФИО пользователя
Организация:
Название компании
Серийный номер:
Лицензионный ключ
Введите серийный номер с Вашего бланка Лицензии на право использования данного программного продукта ООО «КРИПТО-ПРО».
OK
Отмена

Открыть статью на сайте

Установка криптопровайдера на платформу LINUX

Архив. КриптоАРМ ГОСТ.

Установка криптопровайдера

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

Примечание: Директория расположения утилит КриптоПро CSP

/opt/cprocsp/bin/\<arch>/, где под \<arch> подразумеваться один из следующих идентификаторов платформы: - ia32 - для 32-разрядных систем; - amd64 - для 64-разрядных систем.

Установка базовых пакетов скриптом

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

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

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

Установка пакета для модулей TSP и OCSP

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

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

Распаковать архив.

Установить пакет:

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

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

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

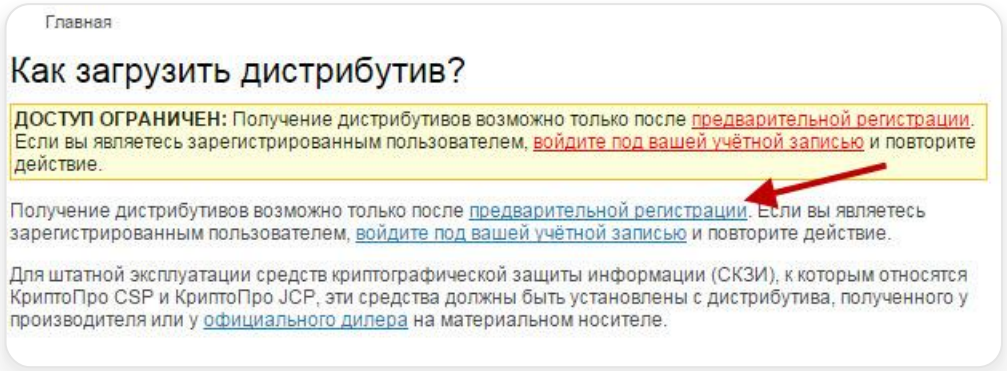
Открыть статью на сайте

Установка криптопровайдера на платформу OS X

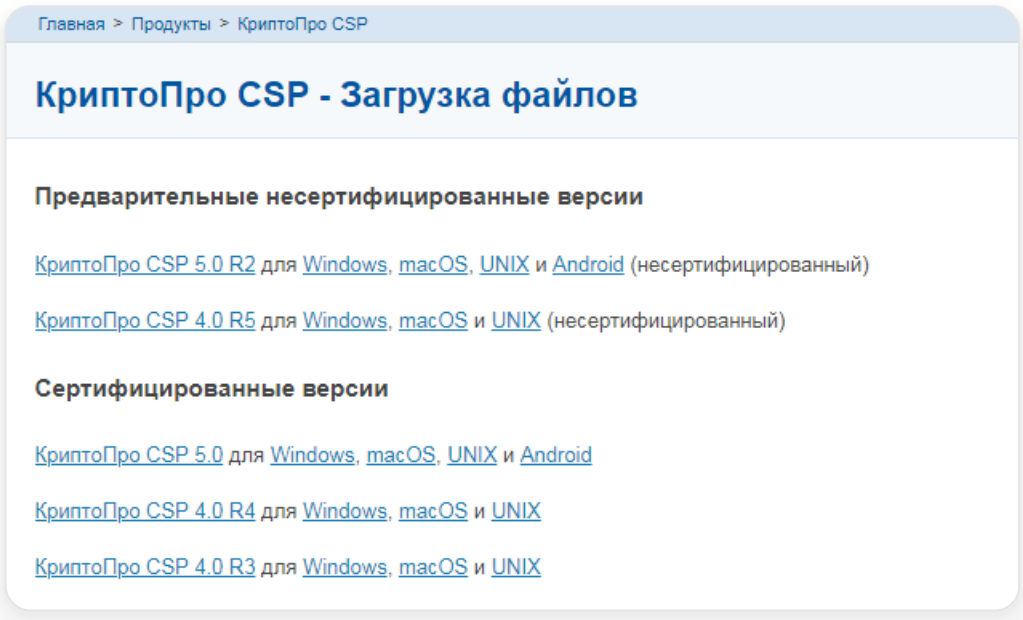
Архив. КриптоАРМ ГОСТ.

Загрузить дистрибутив программы можно на сайте https://www.cryptopro.ru/downloads после предварительной регистрации. Нажмите на предварительную регистрацию, заполните форму.

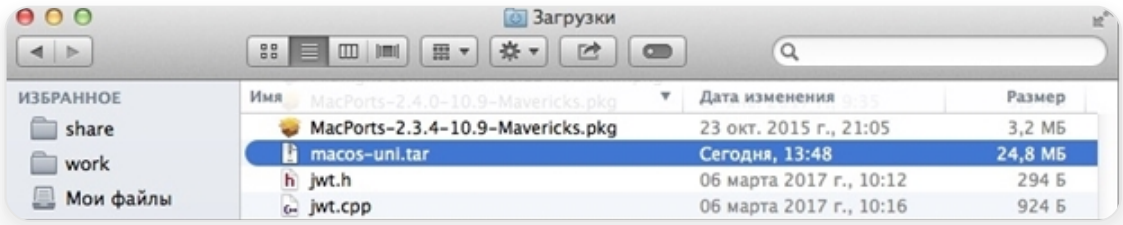
После регистрации вы увидите страницу с лицензионным соглашением. Ознакомившись с правилами и условиями нажмите внизу экрана кнопку **Я согласен** для перехода в раздел загрузки дистрибутивов.



Выбрав нужный вариант КриптоПро CSP, нажмите на ссылку macOs, произойдет загрузка установочного файла.



Процесс установки предельно прост. Кликните по загруженному файлу, загрузка начнется автоматически. После ее завершения двойным щелчком распакуйте загруженный файл **macos-uni.tar.**

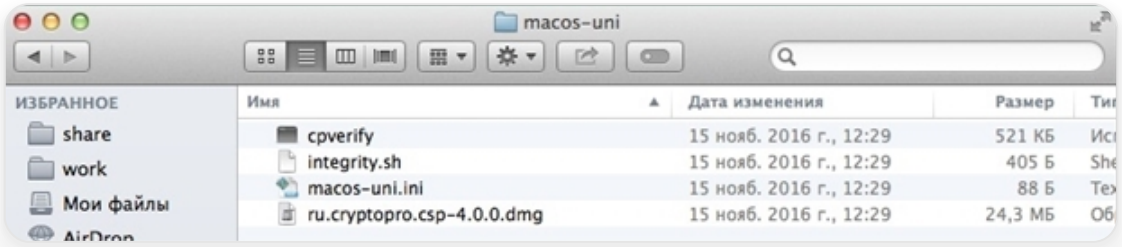


Войдите в распакованную папку. Установка ПО осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo.

СКЗИ КриптоПро CSP требует следующей последовательности установки: сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

В ОС Mac OS X для установки ПО применяются пакеты (packages). Пакет – архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды.

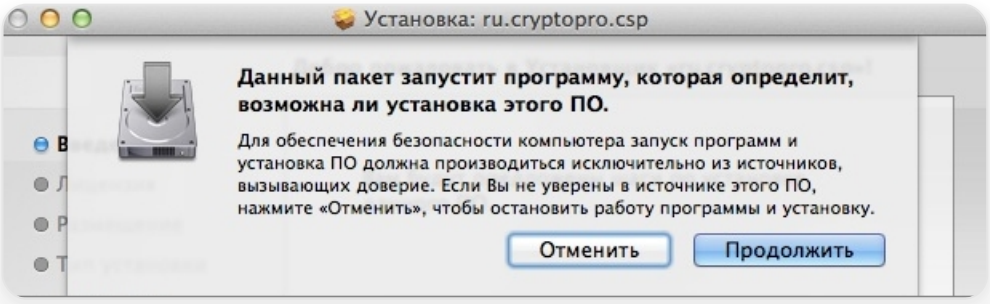
Дистрибутив поставляется в упакованном виде, имеет формат .dmg и представляет собой образ диска, содержащий пакет. Для установки пакета откройте двойным щелчком образ диска с дистрибутивом (dmg).



Запустите установку, выбрав в контекстном меню **Открыть**.

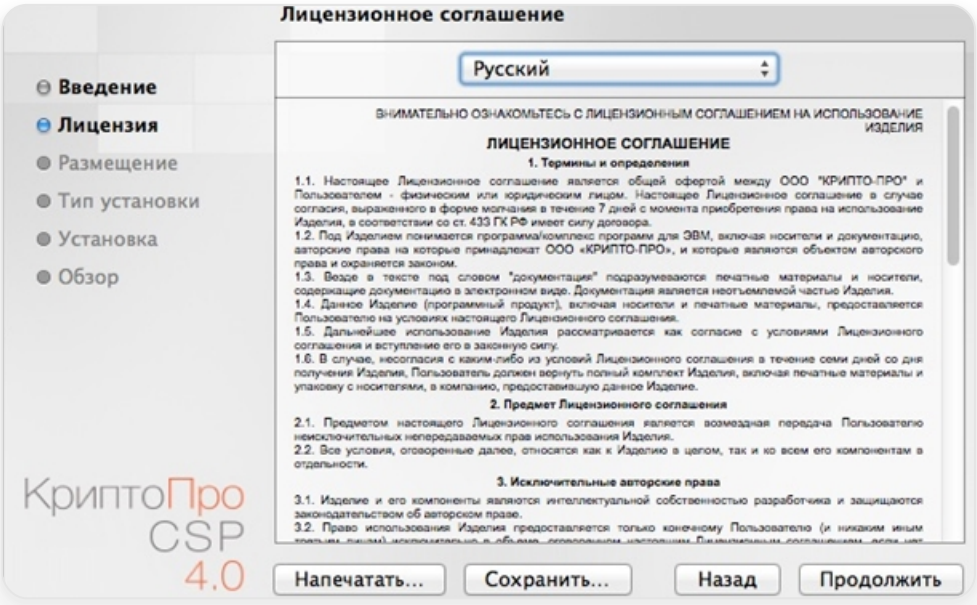


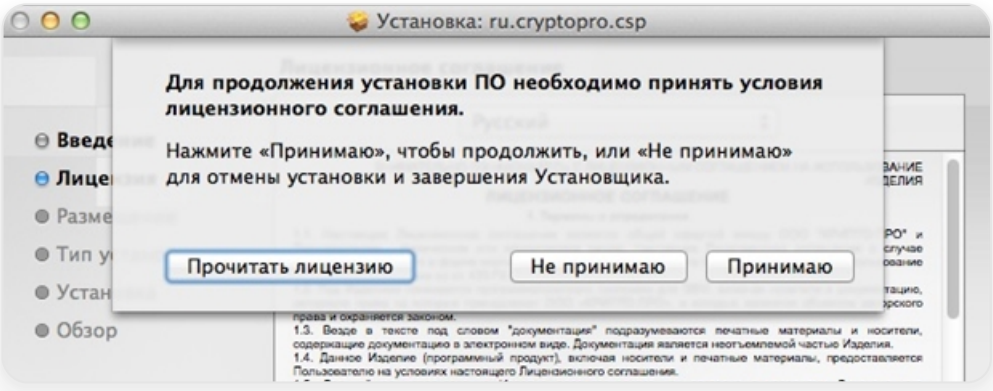
В окне-предупреждении нажмите **Продолжить**.



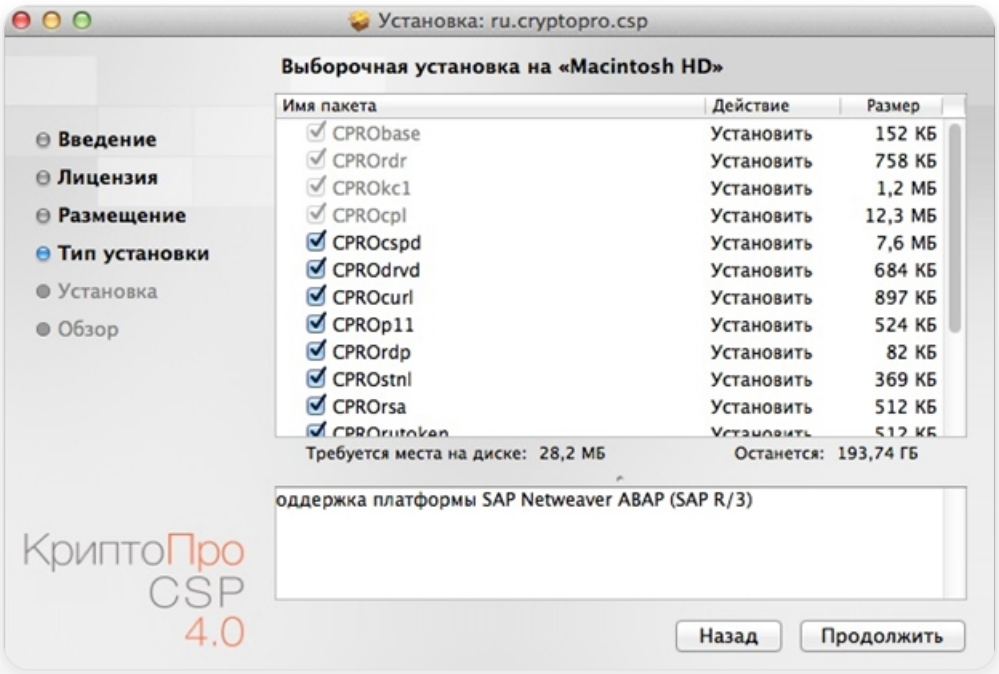
Для установки следуйте указаниям мастера.

Ознакомьтесь с лицензионным соглашением и продолжите установку. Нажмите **Принимаю**.

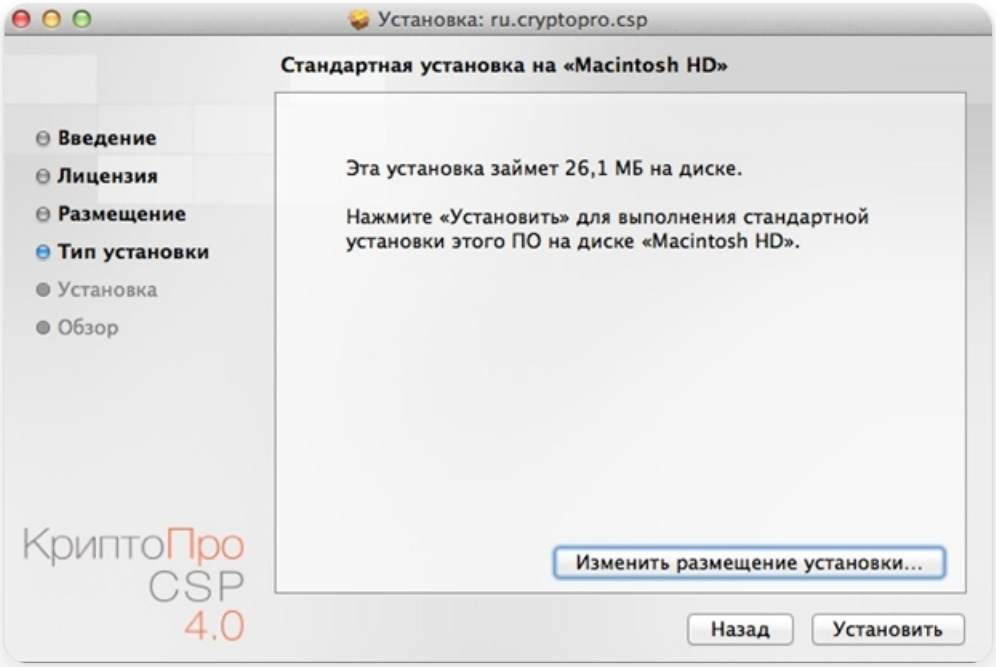




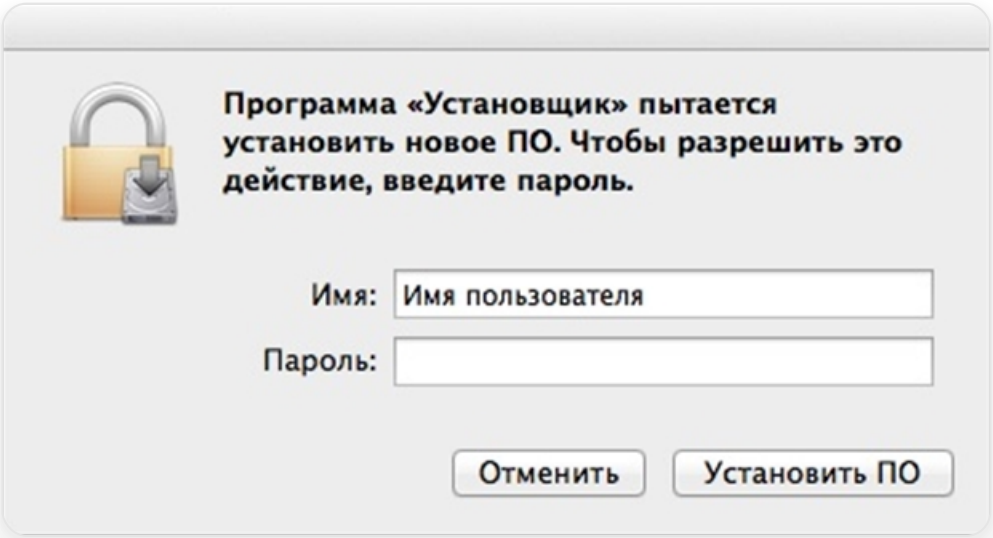
На следующем шаге выберете все установочные пакеты и нажмите **Продолжить**.



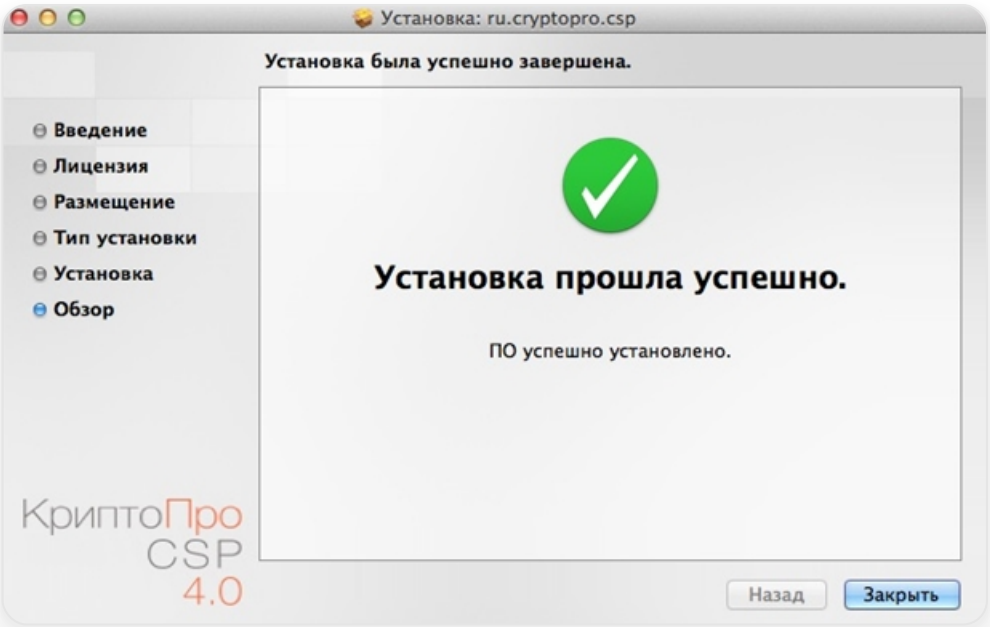
Нажмите **Установить**.



Введите имя и пароль пользователя, имеющего права администратора или учётной записи root. Начнется процесс установки.



Установка закончена. Закройте Установщик.



После первой установки КриптоПро CSP предоставляется временная лицензия на срок до 90 дней. Но если ранее программа уже устанавливалась или срок действия временной лицензии истек, то следует приобрести и установить лицензионный ключ.

Для активации лицензионного ключа выполните команду:

sudo /opt/cprocsp/sbin/cpconfig -license -set <серийный_номер>



Серийный номер лицензионного ключа следует вводить с соблюдением регистра символов.

Установка установка КриптоПро CSP 4.0 на Mac OS X 10 на этом завершена.

Установка пакета для модулей TSP и OCSP

Для создания подписи со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP.
Скачать архив Apple MacOS по ссылке КриптоПро ЭЦП SDK 2.0 (требуется предварительная регистрация).

Открыть статью на сайте

Инструкция по диагностике рабочего места

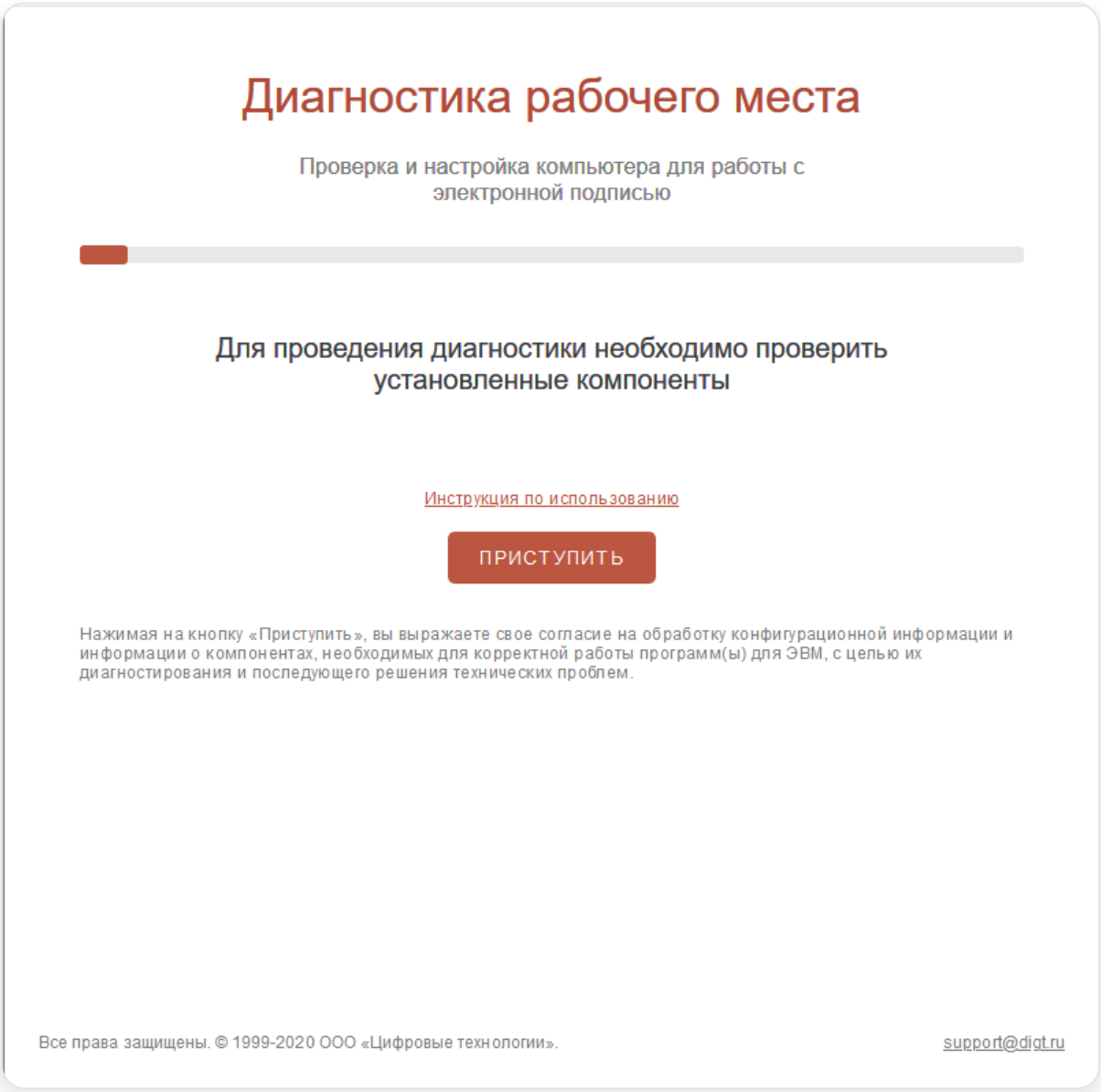
Архив. КриптоАРМ ГОСТ.

Описание

Web-приложение “Диагностика рабочего места” позволяет проверить готовность рабочего места к работе с электронной подписью. Действия поделены на этапы, выполнив которые, пользователь получит настроенное рабочее место.

Последовательность этапов диагностики

Перейдя на портал диагностики, пользователь видит следующее окно:

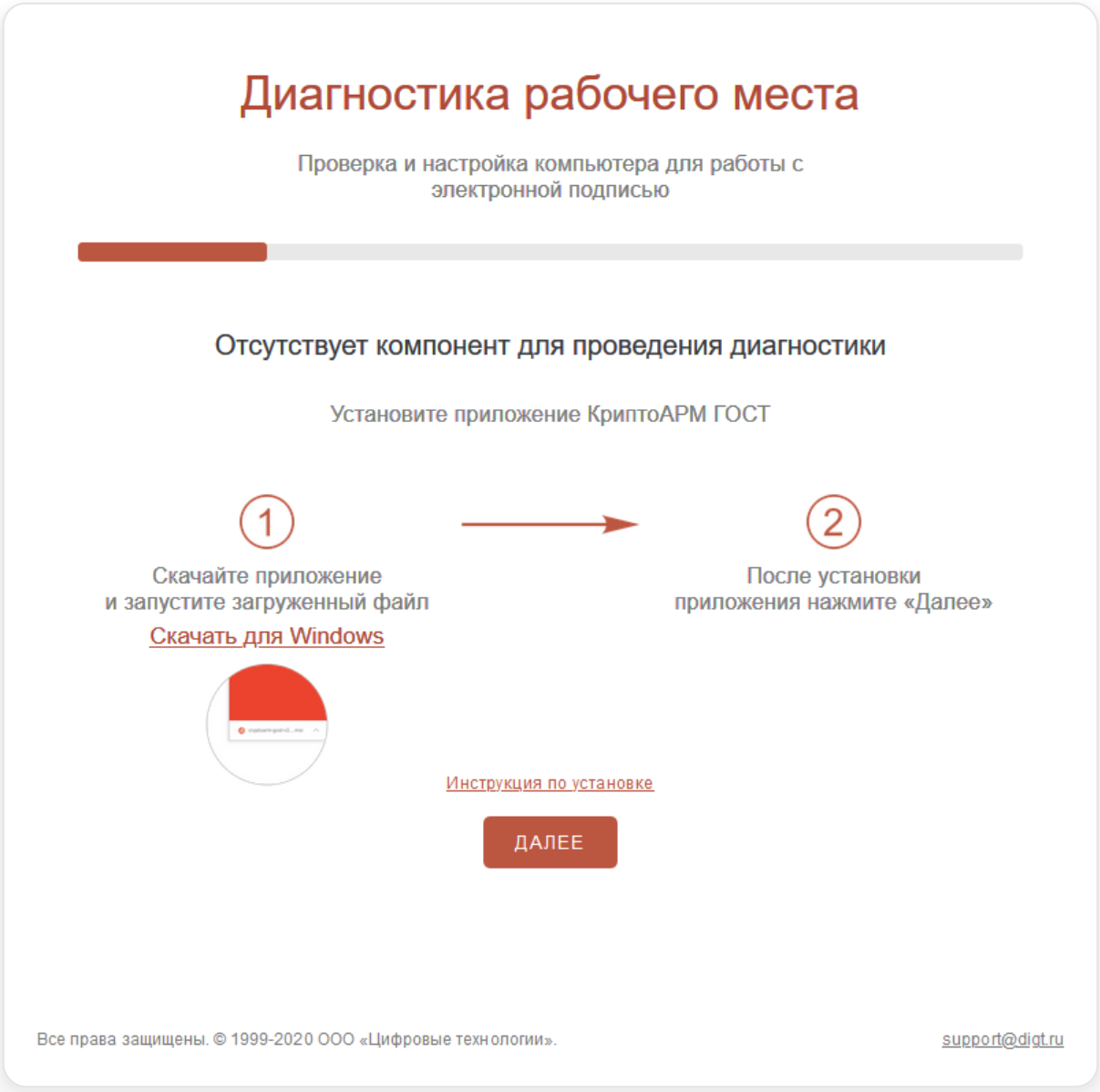


Нажатие кнопки “Приступить” запускает процесс диагностики. При этом проверяется:

- Наличие приложения КриптоАРМ ГОСТ (версии не ниже 2.5.3)
- Наличие криптопровайдера КриптоПро CSP
- Наличие действующих лицензий на КриптоАРМ ГОСТ и КриптоПро CSP
- Наличие действующих личных сертификатов

Отсутствует КриптоАРМ ГОСТ

Если на рабочем месте пользователя отсутствует КриптоАРМ ГОСТ, то будет предложено его скачать и установить:

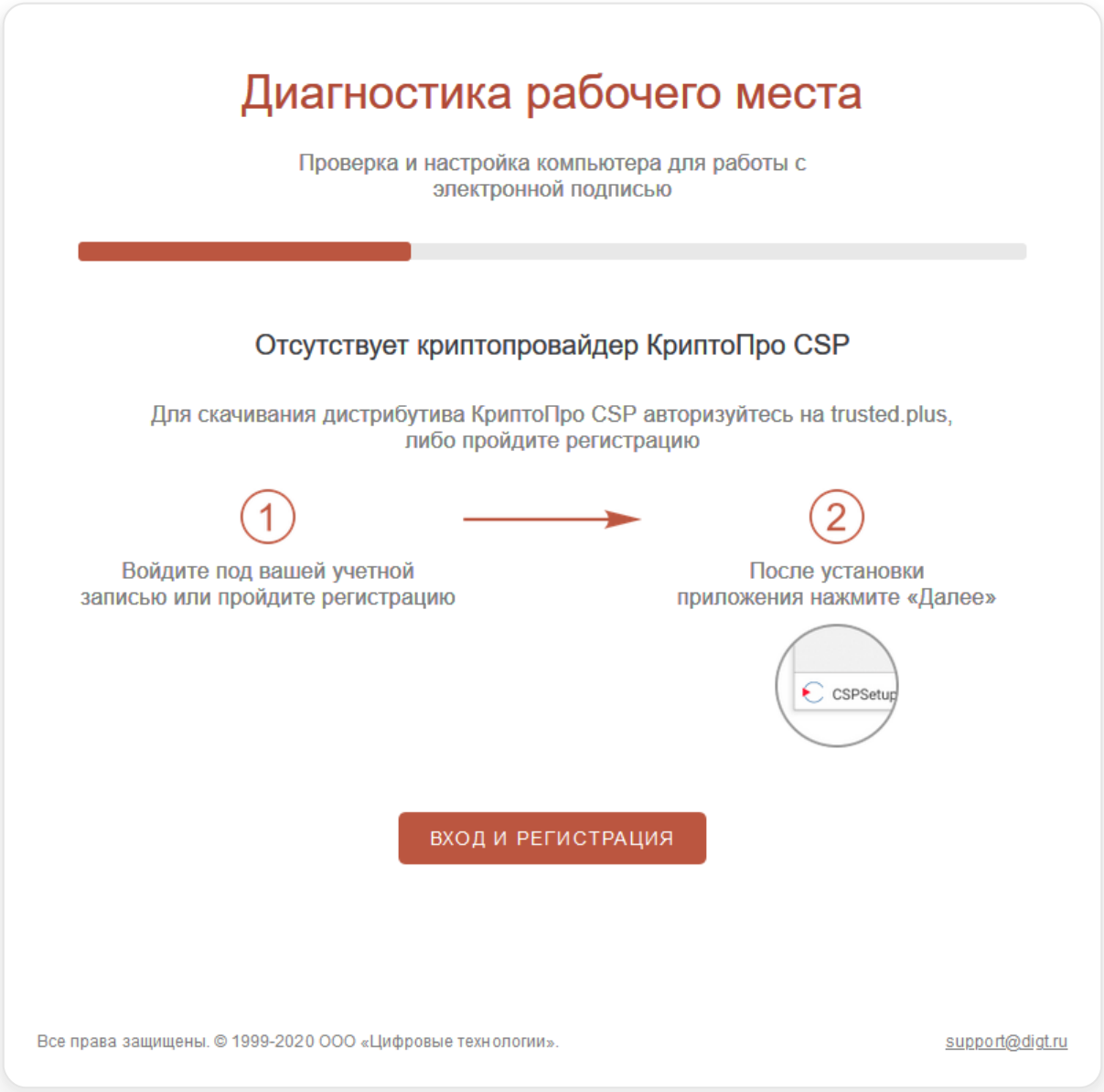


После установки приложения на рабочем месте, требуется нажать кнопку “Далее”.

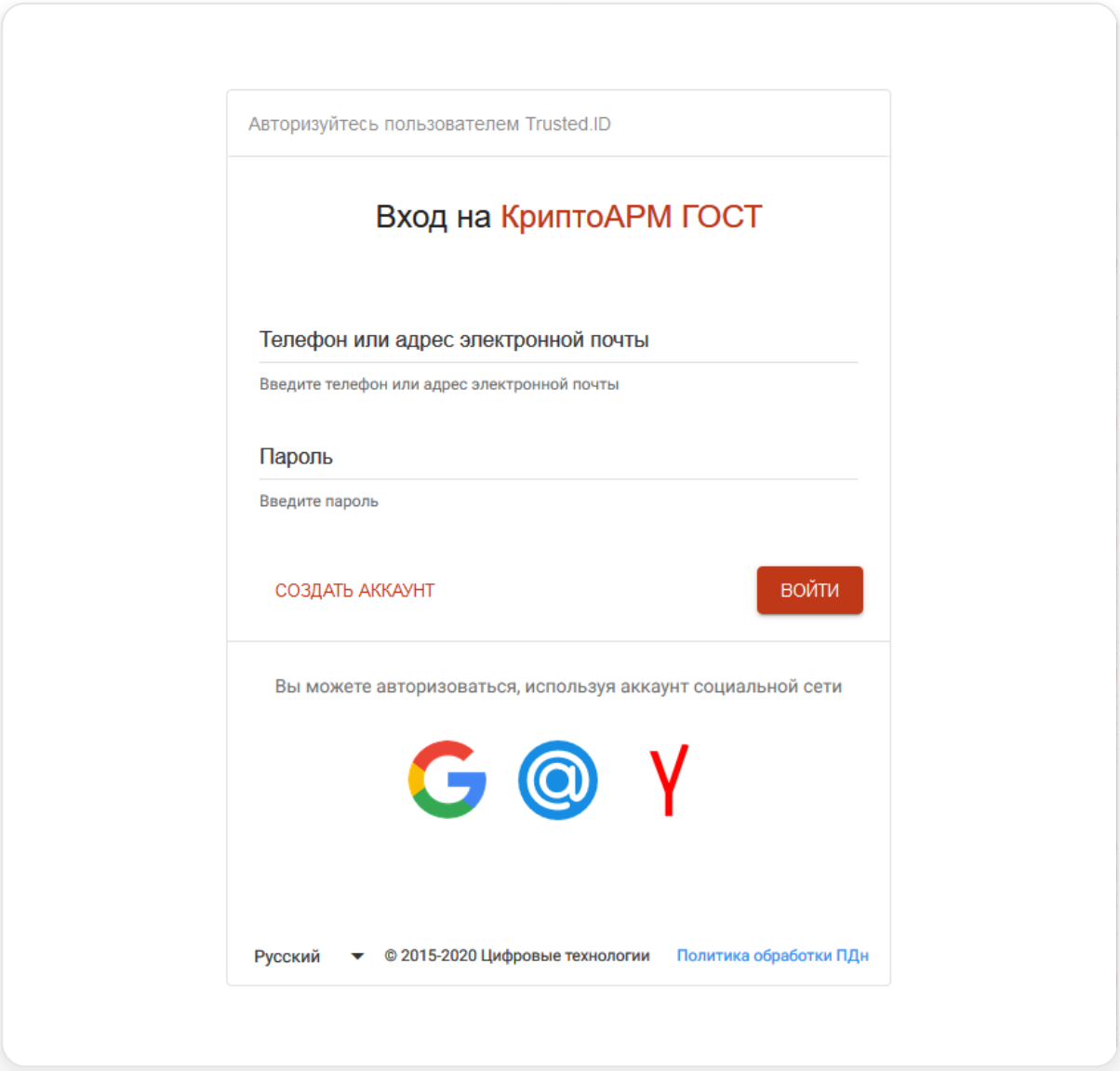
Отсутствует КриптоПро CSP

Если на рабочем месте пользователя отсутствует КриптоПро CSP, то будет предложено его скачать и установить. Для скачивания дистрибутивов CSP необходимо авторизоваться.

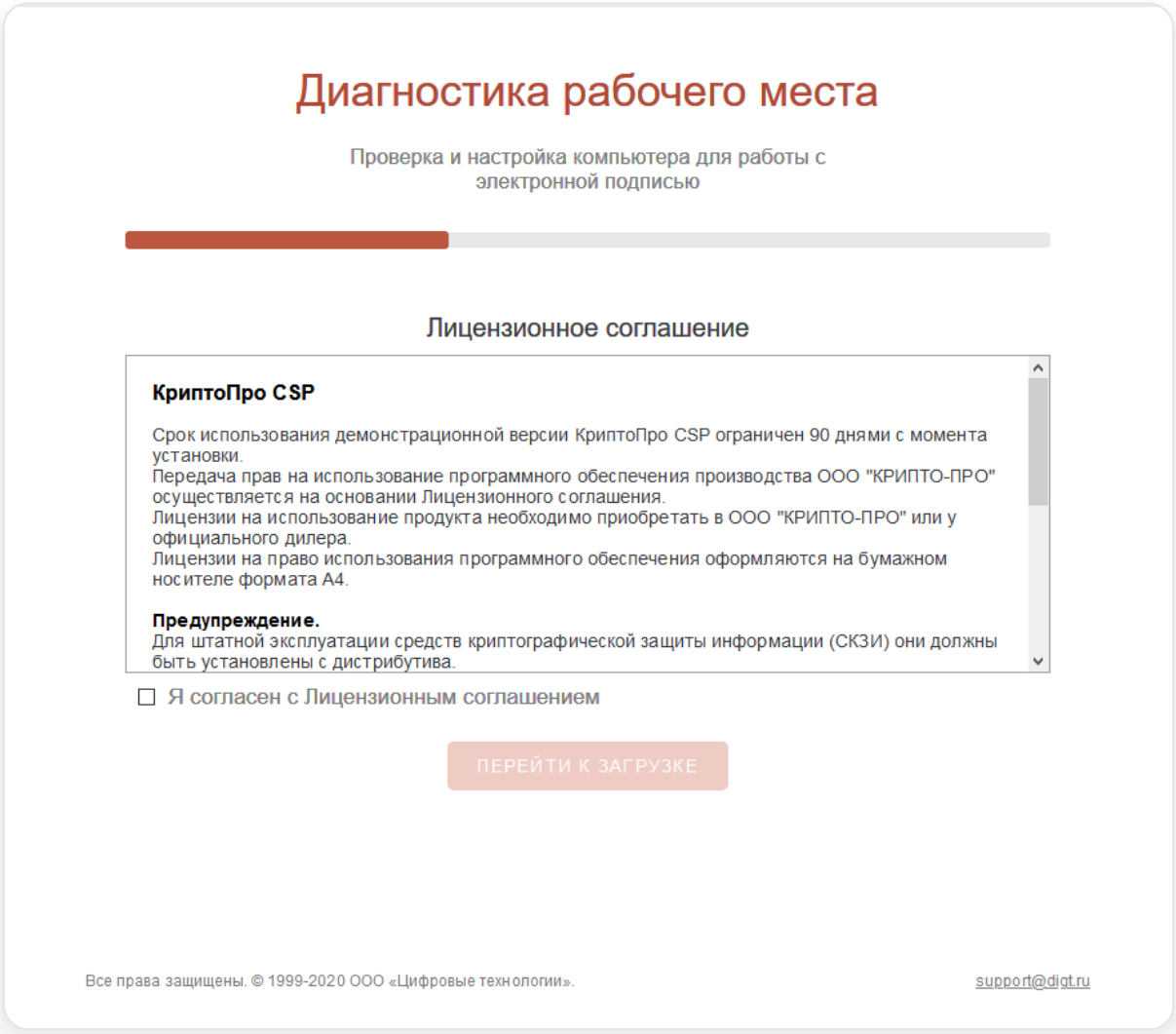
Сообщение об отсутствии КриптоПро CSP:



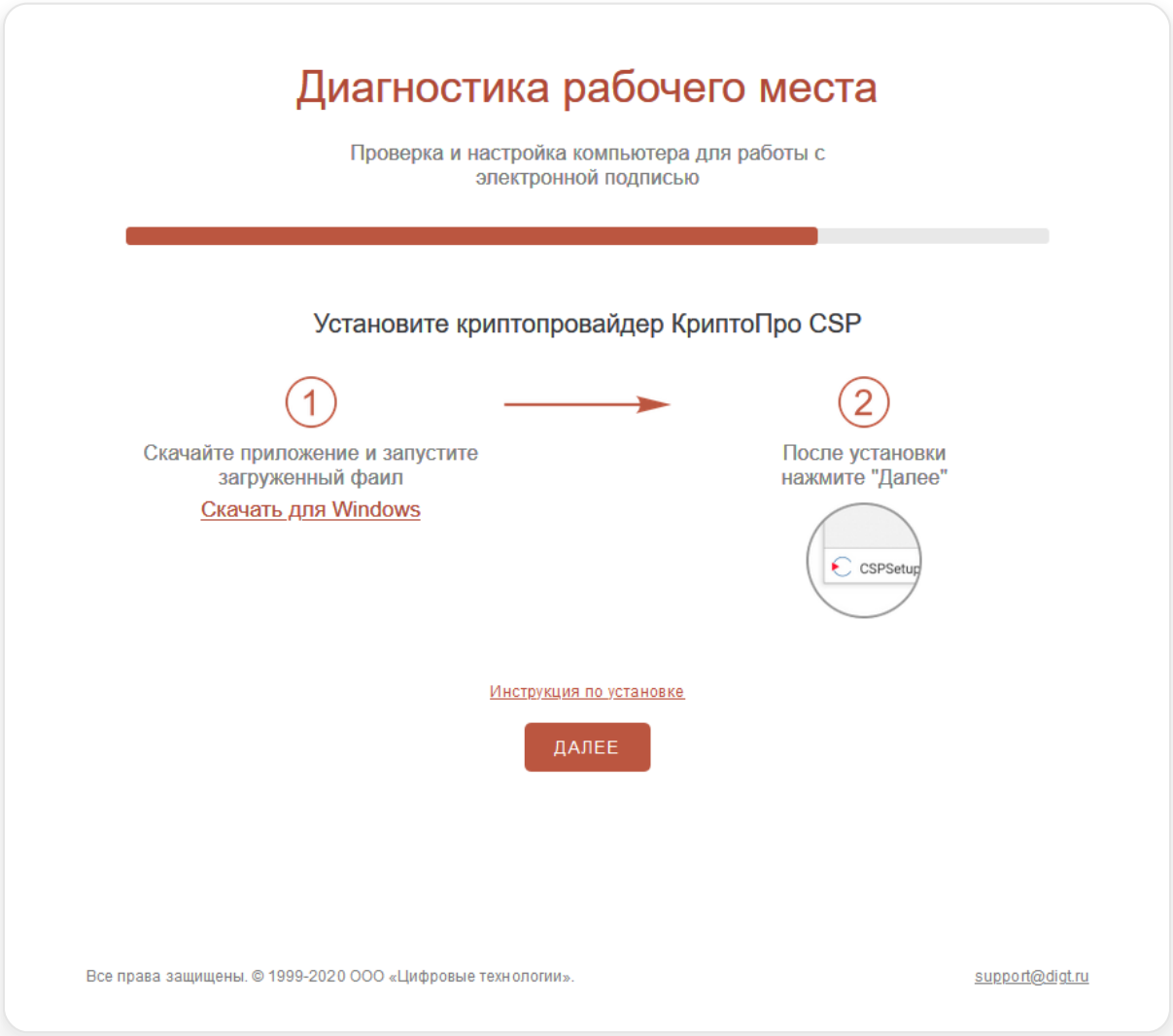
Авторизация через сервис Trusted.ID:



После успешной авторизации необходимо принять лицензионное соглашение:

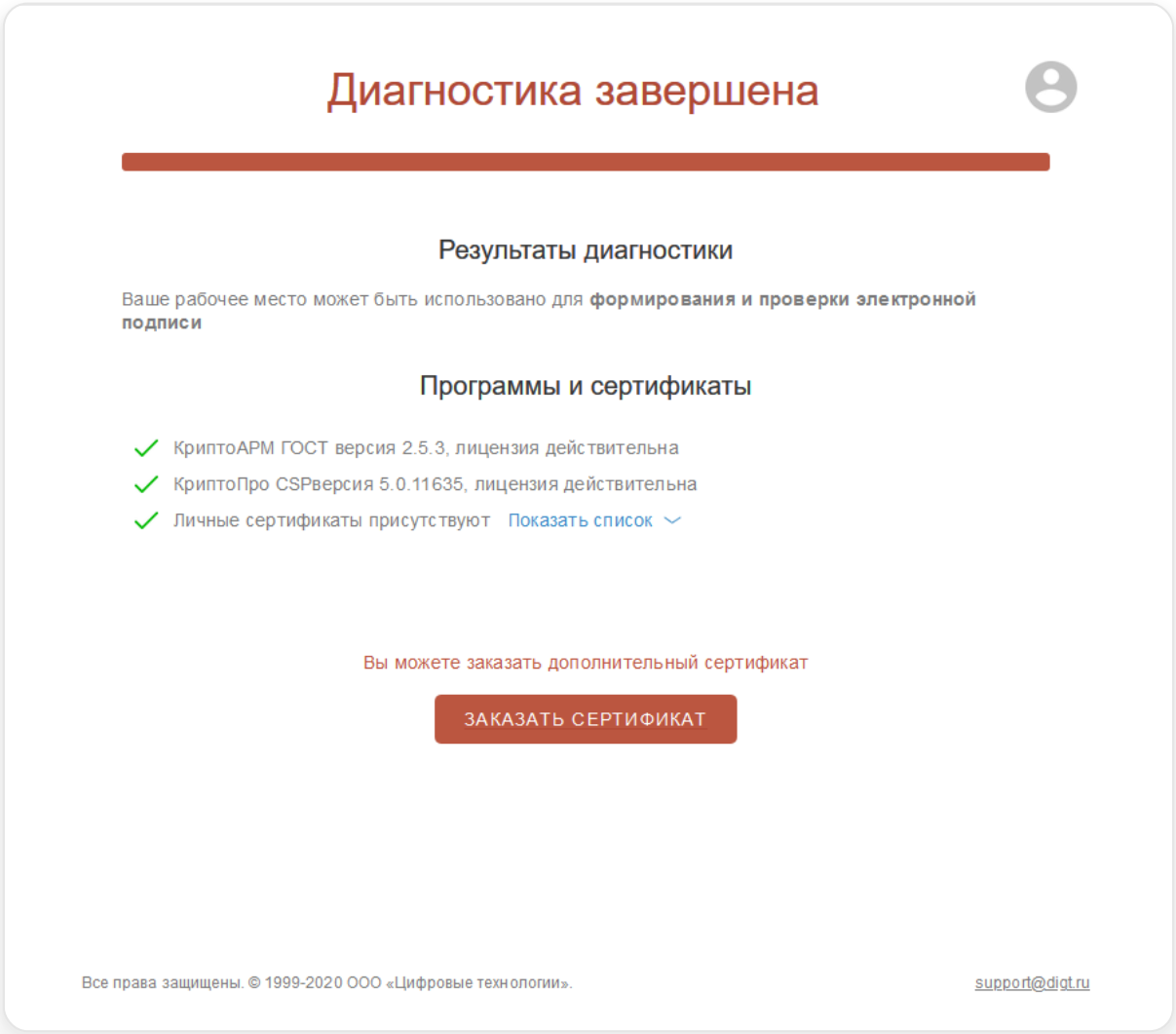


Скачивание и установка КриптоПро CSP:

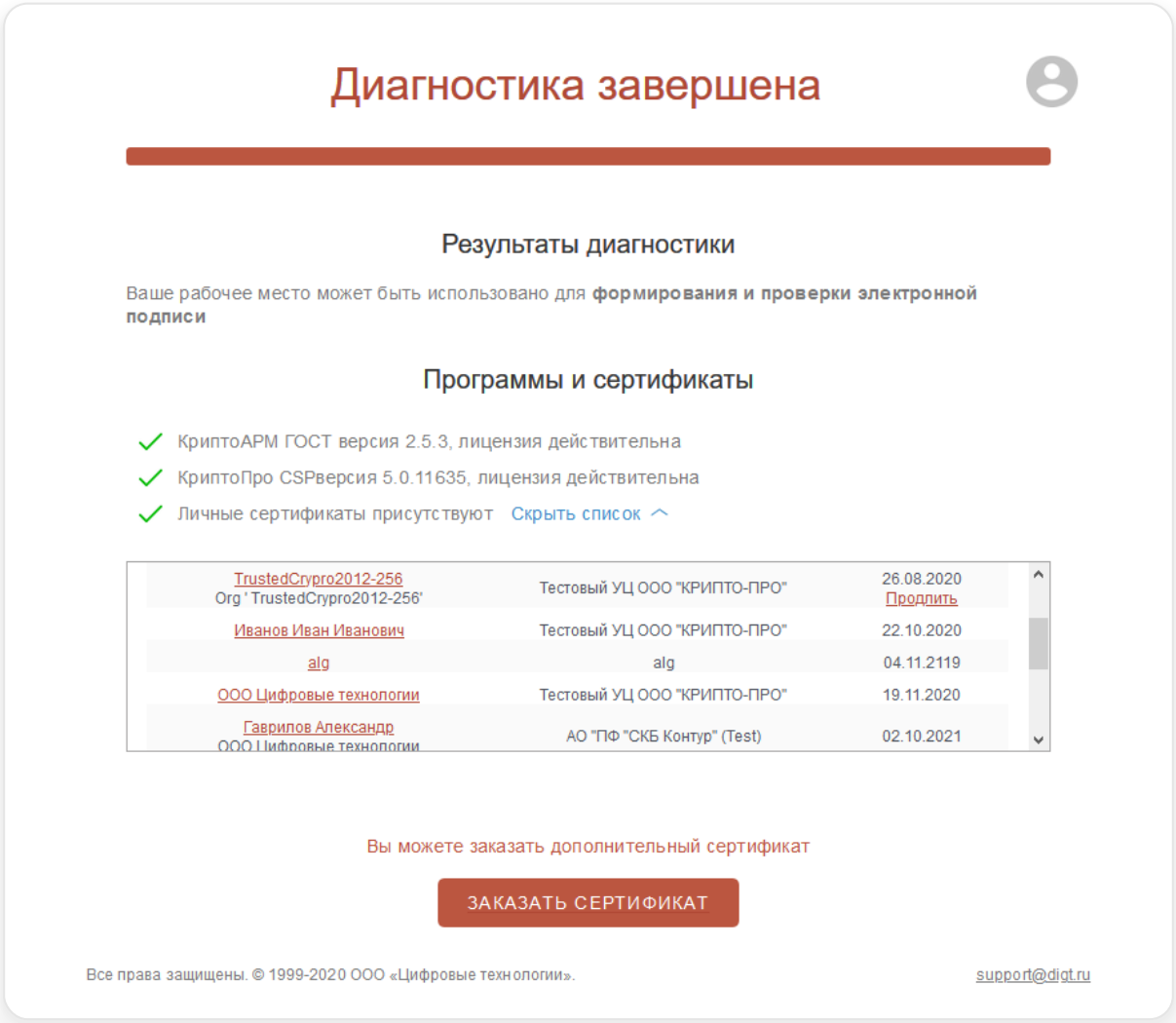


Результаты диагностики

После установки КриптоАРМ и КриптоПро выполняется проверка лицензий на продукты и наличие действующих сертификатов. В случае если рабочее место готово к подписи отображается окно вида:



Для просмотра списка сертификатов следует развернуть таблицу. Для сертификатов, у которых скоро истечет срок действия, доступна опция продления. Кроме этого, можно заказать дополнительный сертификат, нажав советующую кнопку и воспользовавшись сервисом подбора КЭП.

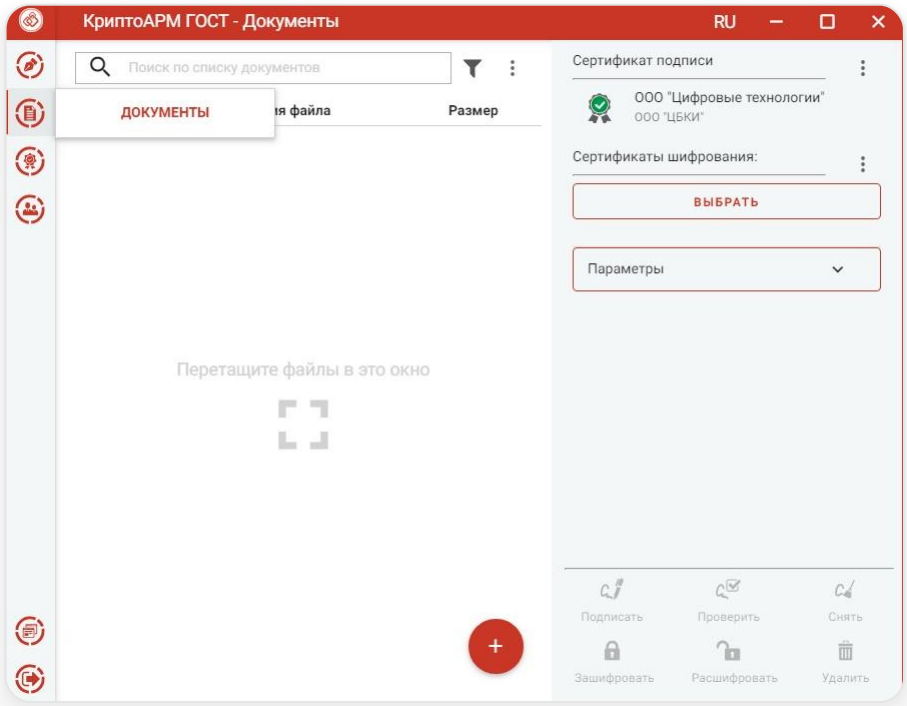

Диагностика завершена
Результаты диагностики
Ваше рабочее место может быть использовано для формирования и проверки электронной подписи
Программы и сертификаты
КриптоАРМ ГОСТ версия 2.5.3, лицензия действительна
КриптоПро CSPверсия 5.0.11635, лицензия действительна
Личные сертификаты присутствуют
Скрыть список
TrustedCrypro2012-256
Org ' TrustedCrypro2012-256'
Тестовый УЦ ООО "КРИПТО-ПРО"
26.08.2020
Продлить
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
22.10.2020
alg
alg
04.11.2119
ООО Цифровые технологии
Тестовый УЦ ООО "КРИПТО-ПРО"
19.11.2020
Гаврилов Александр
ООО Цифровые технологии
АО "ПФ "СКБ Контур" (Test)
02.10.2021
Вы можете заказать дополнительный сертификат
ЗАКАЗАТЬ СЕРТИФИКАТ
Все права защищены. © 1999-2020 ООО «Цифровые технологии».
support@digt.ru

Открыть статью на сайте

Каталог Документы

Архив. КриптоАРМ ГОСТ.

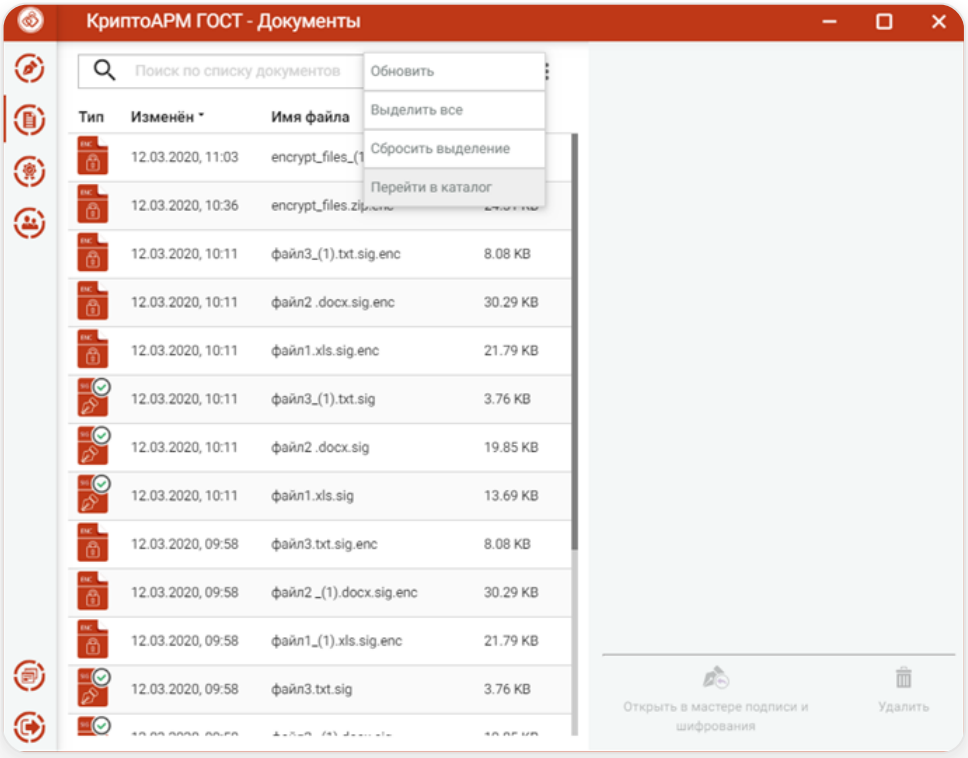
Для сохранения копии результатов выполнения операций подписи, снятия подписи, архивирования, шифрования и расшифрования используется каталог **Документы**. Каталог с документами располагается в каталоге пользователя в папке \.Trusted\CryptoARM GOST\Documents\. Просмотреть документы в каталоге можно,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



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

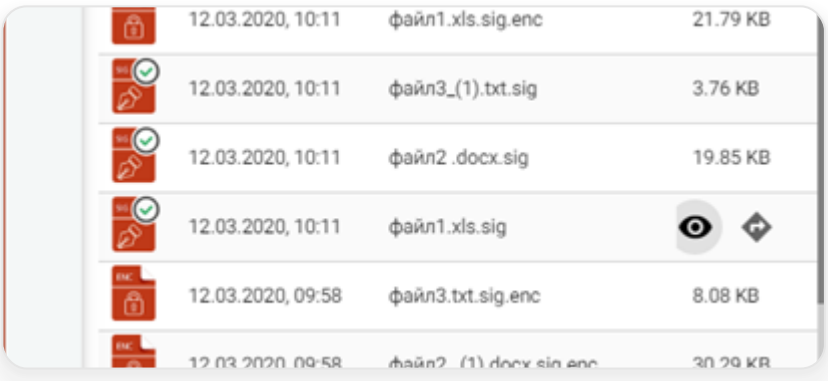
Для списка доступно контекстное меню, состоящее из пунктов:

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

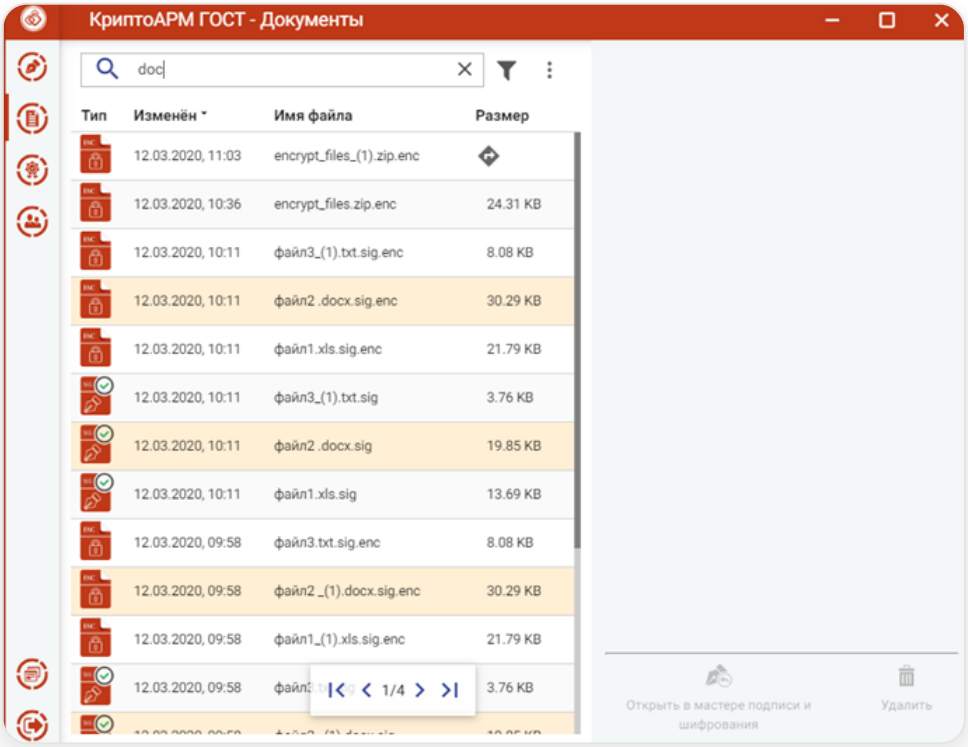


Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши:

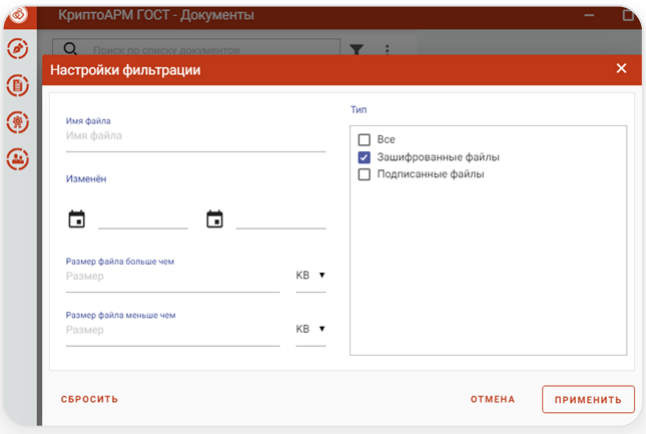
- Просмотр - выполняется открытие файла через приложение, которое ассоциировано с его расширением. Не доступно для зашифрованных файлов;
- Перейти к файлу - выполняется открытие каталога, в котором располагается файл.

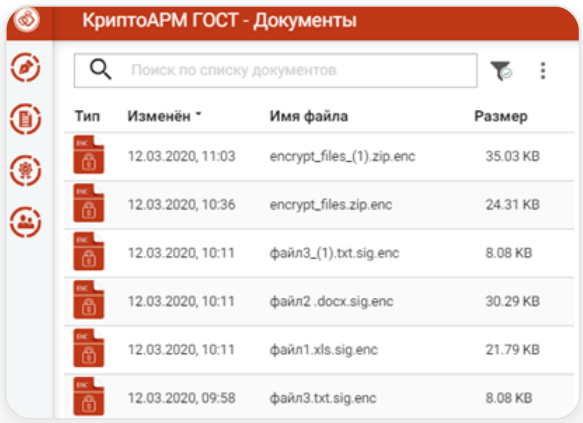


В приложении реализован поиск документов по символьному совпадению.



Список документов можно отфильтровать, задав настройки фильтрации.
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.



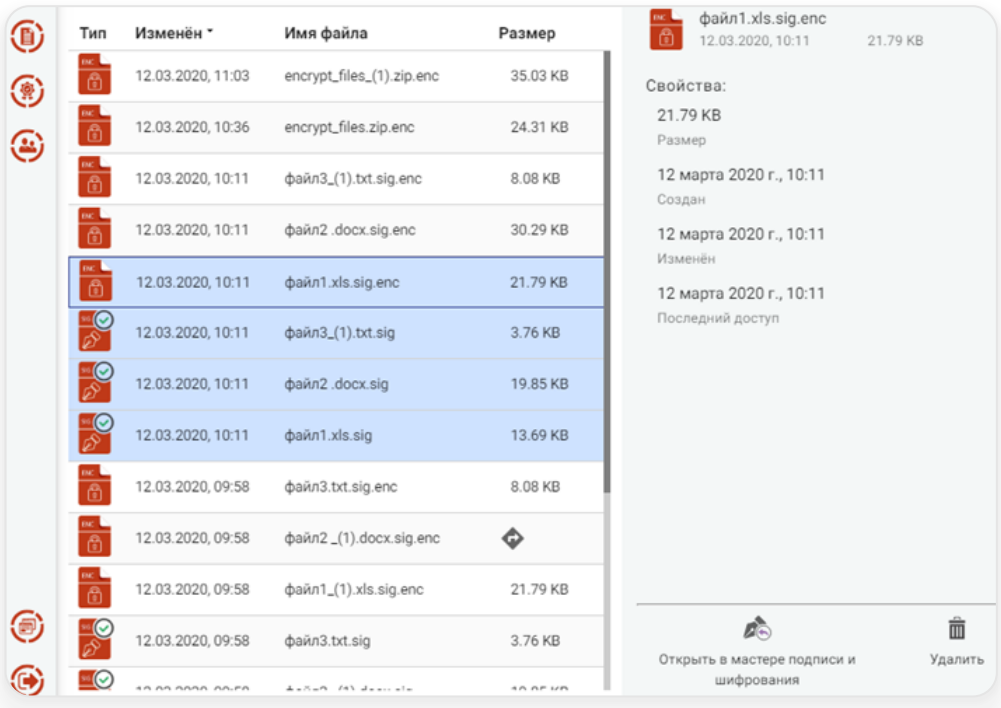


Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации.

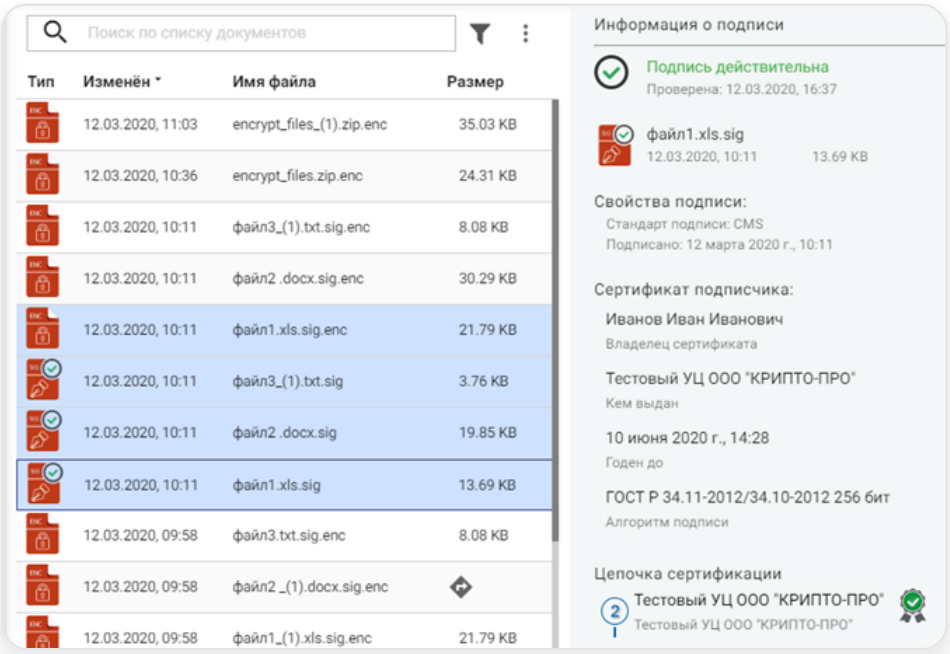
Для списка файлов в разделе Документы доступны операции:

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

При выделении документов в списке в правой области отображается информация о последнем выделенном документе.



Для подписанных файлов отображается информация о подписи.


Поиск по списку документов
Тип
Изменён
Имя файла
Размер
12.03.2020, 11:03 encrypt_files_(1).zip.enc 35.03 KB
12.03.2020, 10:36 encrypt_files.zip.enc 24.31 KB
12.03.2020, 10:11 файл3_(1).txt.sig.enc 8.08 KB
12.03.2020, 10:11 файл2 .docx.sig.enc 30.29 KB
12.03.2020, 10:11 файл1.xls.sig.enc 21.79 KB
12.03.2020, 10:11 файл3_(1).txt.sig 3.76 KB
12.03.2020, 10:11 файл2 .docx.sig 19.85 KB
12.03.2020, 10:11 файл1.xls.sig 13.69 KB
12.03.2020, 09:58 файл3.txt.sig.enc 8.08 KB
12.03.2020, 09:58 файл2 _(1).docx.sig.enc
12.03.2020, 09:58 файл1_(1).xls.sig.enc 21.79 KB
Информация о подписи
Подпись действительна
Проверена: 12.03.2020, 16:37
файл1.xls.sig
12.03.2020, 10:11 13.69 KB
Свойства подписи:
Стандарт подписи: CMS
Подписано: 12 марта 2020 г., 10:11
Сертификат подписчика:
Иванов Иван Иванович
Владелец сертификата
Тестовый УЦ ООО "КРИПТО-ПРО"
Кем выдан
10 июня 2020 г., 14:28
Годен до
ГОСТ Р 34.11-2012/34.10-2012 256 бит
Алгоритм подписи
Цепочка сертификации
2
Тестовый УЦ ООО "КРИПТО-ПРО"
Тестовый УЦ ООО "КРИПТО-ПРО"

Открыть статью на сайте

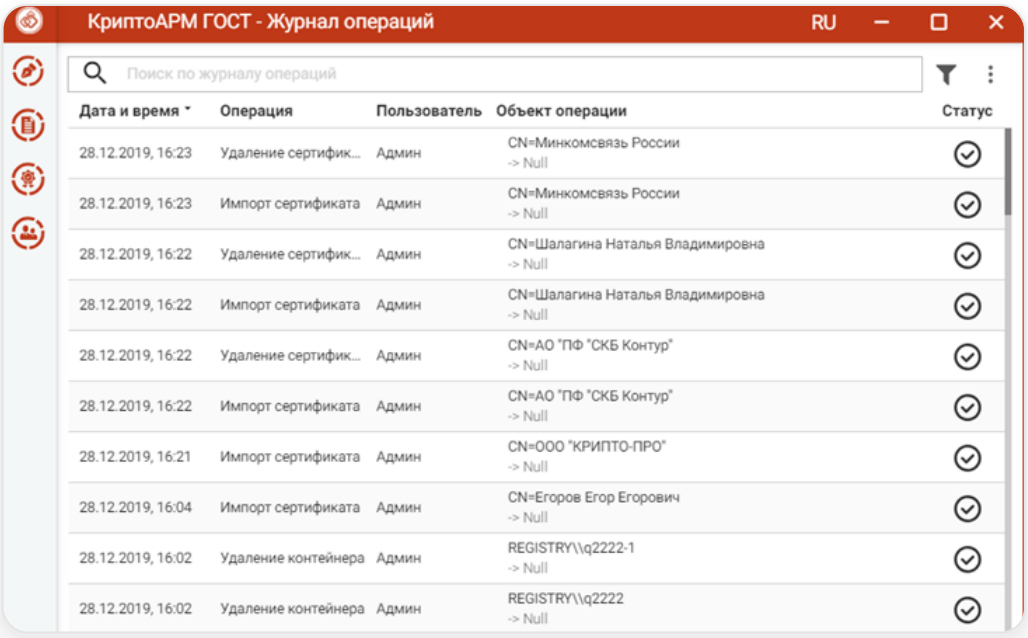
Журнал операций

Архив. КриптоАРМ ГОСТ.

Журнал операций предназначен для отображения операций, выполняемых пользователем.

В нем 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.

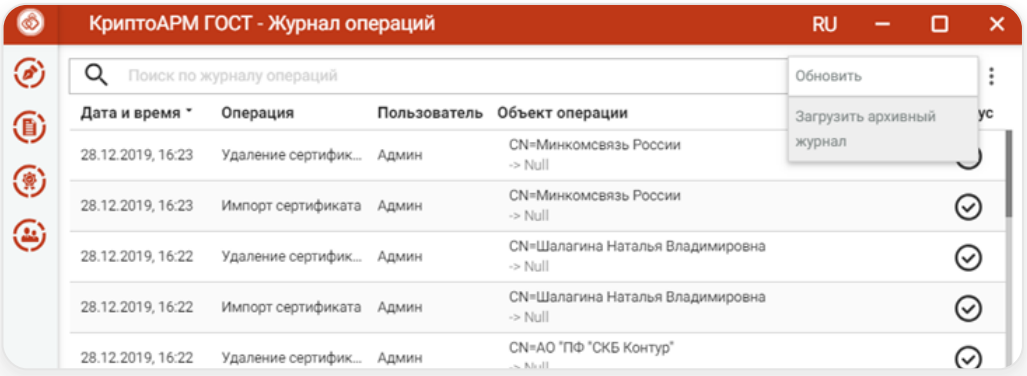


Текущая версия журнала операций записывается в файл **cryptoarm_gost_operations[порядковый номер журнала].log**, который находится в папке пользователя в директории \.Trusted\CryptoARM_Gost\ под Windows и \.Trusted\CryptoARM_Gost\ под OSX и Linux.

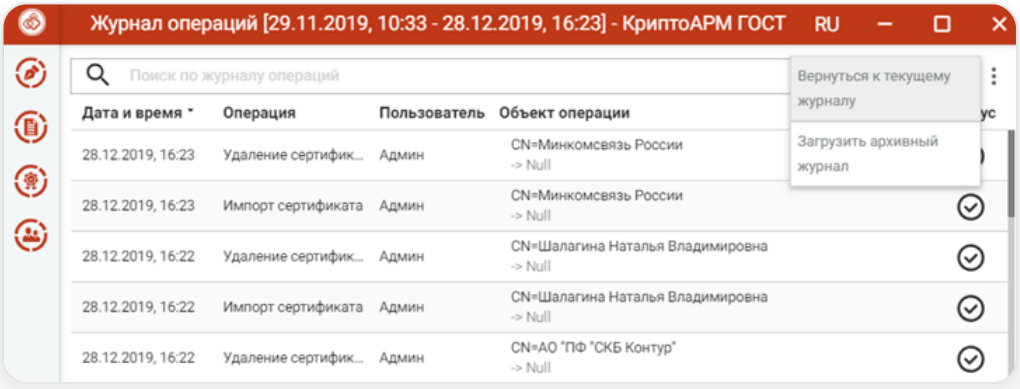
По мере накопления записей в журнале операций выполняется автоматический переход к новому файлу журнала со следующим порядковым номером.

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.

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

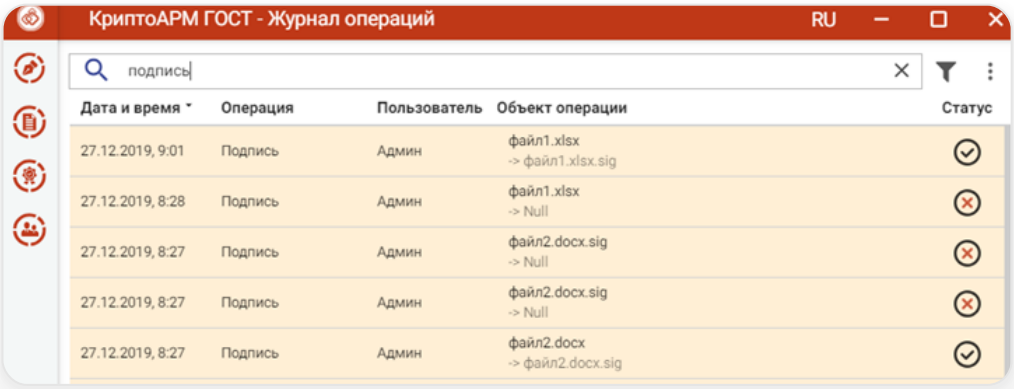


Для возврата к текущему журналу операций используется пункт контекстного меню архивного журнала **Вернуться к текущему журналу**.



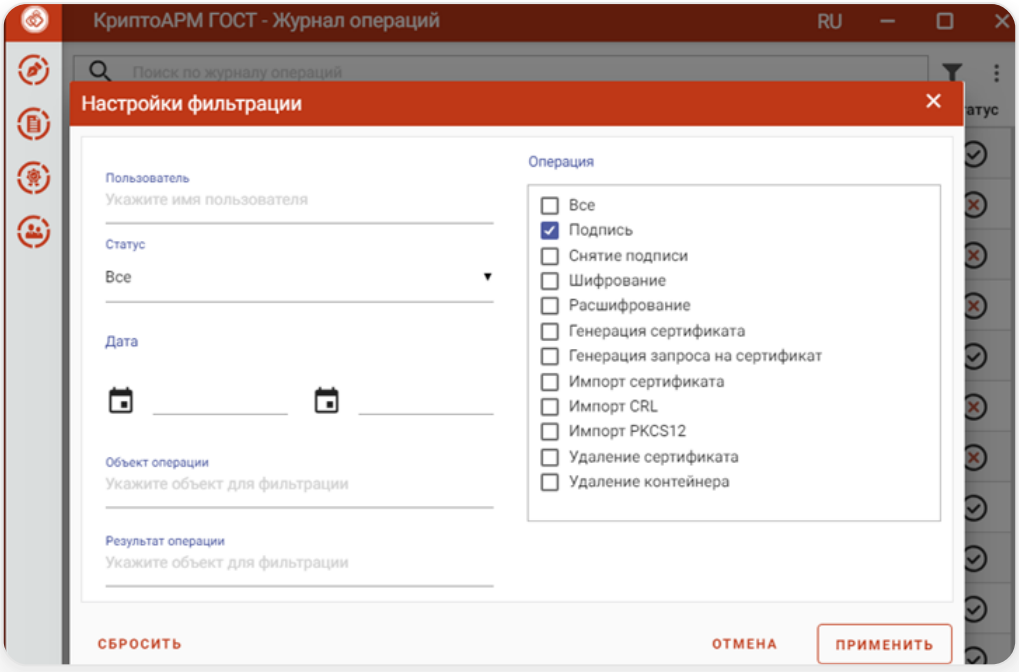
Поиск записей в журнале операций

В приложении реализован поиск записей журнала операций по символьному совпадению. К примеру, вы хотите найти все операции подписи сделанные за время работы программы. Для этого в окне поиска нужно задать значение "подпись".



Фильтрация журнала операций

Для открытия окна настроек критериев фильтра на панели управления имеется кнопка, при нажатии на которую открывается окно настроек фильтрации.
Применение фильтрации выполняется по нажатию кнопки **Применить**. В зависимости от выставленных критериев фильтра в журнале остаются только те записи, которые удовлетворяют (суммарно) этим критериям.



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

Открыть статью на сайте

Перенос контейнера закрытого ключа под требуемую операционную систему

Архив. КриптоАРМ ГОСТ.

Для примера рассмотрим наиболее часто встречающуюся задачу переноса контейнера закрытого ключа из операционной системы Windows под Linux или OS X.

Если в операционной системе Windows сертификат и закрытый ключ могут находится в локальном хранилище Crypto API, то для работы под операционными системами Linux или OS X его нужно импортировать в специальное системное хранилище.



Важно, чтобы у закрытого ключа должен быть установлен флаг «Экспортируемый»

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

В операционной системе Windows скопировать контейнер закрытого ключа можно следующим образом:

1. Откройте приложение КриптоПро CSP и перейдите на вкладку **Сервис**.
2. На вкладке выберите команду **Скопировать контейнер закрытого ключа**.
3. Введите пароль для ключевого контейнера и задайте имя ключевого контейнера (например, test).
4. Сохраните контейнер на диск или флешку.
5. 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 сертификата под операционными системами Linux (OS X) выполните следующие действия.

1. Скопируйте контейнер закрытого ключа (директорию /test/ в формате 8.3) и файл сертификата (test.cer) из корня дискеты или флешки в директорию **/var/opt/cprocsp/keys/имя_пользователя**.

2. При этом необходимо проследить чтобы: владельцем файлов был пользователь, в директории с именем которого расположен контейнер (от его имени будет осуществляться работа с ключами); на директорию с ключами были выставлены права, разрешающие владельцу всё, остальным ничего; на файлы были выставлены права, разрешающие владельцу по крайней мере чтение и запись, остальным ничего.

Проверить, отображается ли контейнер можно командой
/opt/cprocsp/bin//csptest -keyset -enum_cont -fqcn -verifycontext

Привязать сертификат к закрытому ключу можно командой
/opt/cprocsp/bin//certmgr -inst -store uMy -file /var/opt/cprocsp/keys/<сертификат>.cer -cont '\\.\HDIMAGE\test' –pin ***

Выполнить проверку привязки сертификата к закрытому ключу можно через команду
/opt/cprocsp/bin//certmgr -list -store uMy

В результате выполнения предыдущей команды должно быть выведено сообщение

PrivateKey Link: Yes. Container: HDIMAGE\\test.000\.

В приведенных выше командах подразумевается один из следующих идентификаторов платформы: ia32 - для 32-разрядных систем Linux; amd64 - для 64- разрядных систем Linux; не указывается - для OS X.

Открыть статью на сайте

Установка сертификата с токена с сохранением привязки к закрытому ключу

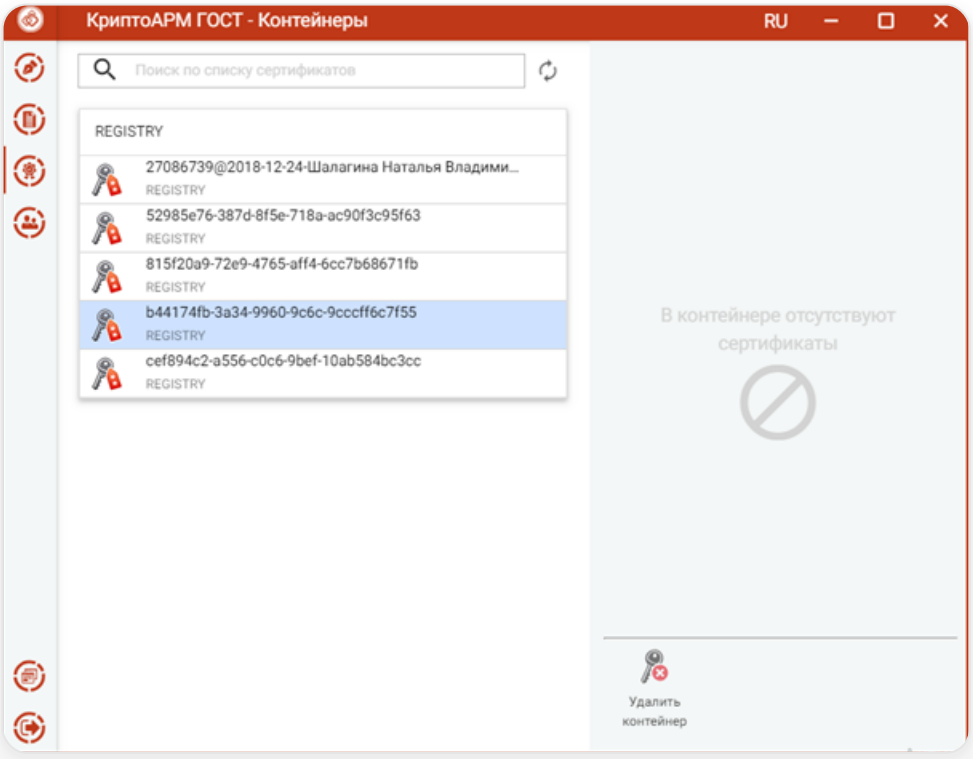
Архив. КриптоАРМ ГОСТ.

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.

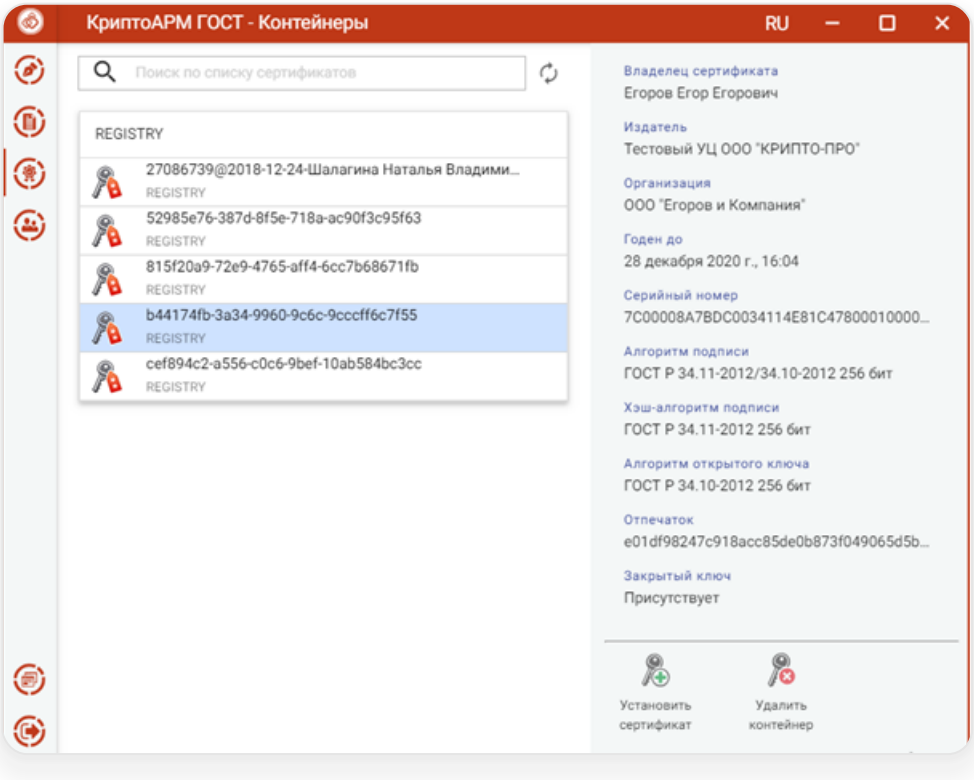
Установка сертификата из ключевого контейнера в КриптоАРМ ГОСТ на Windows.

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.



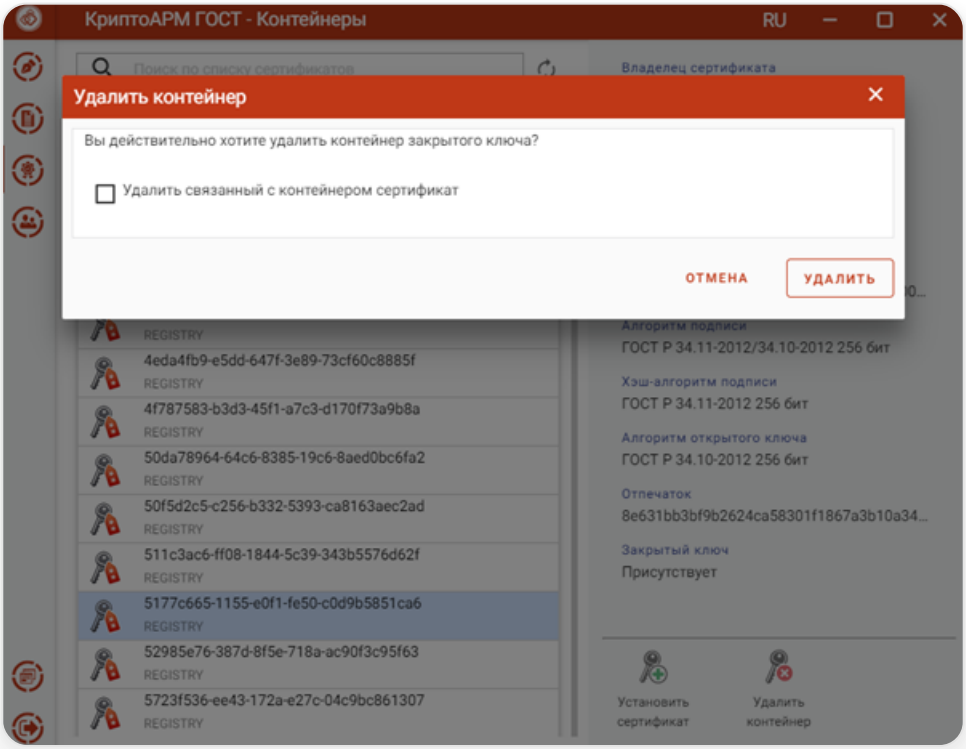
В каждом из хранилищ отображаются контейнеры закрытых ключей. В случае отсутствия контейнеров в хранилище, оно может быть скрыто как пустое.

После выбора контейнера отображается информация о находящемся в нем сертификате.



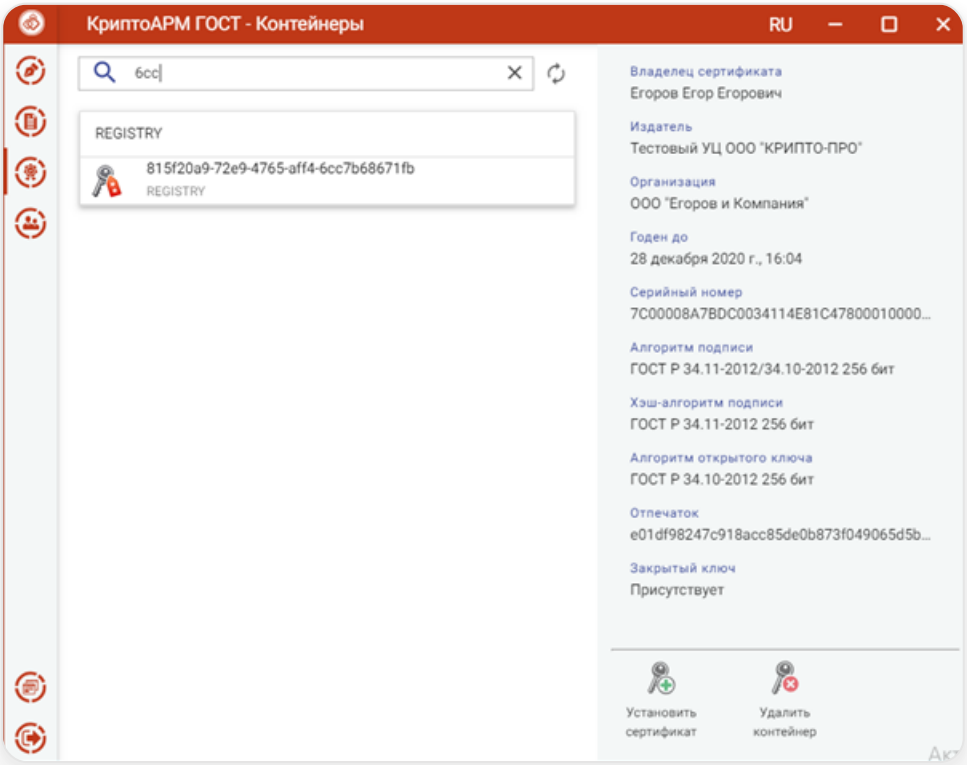
По кнопке **Установить сертификат** происходит установка сертификата в Личное хранилище сертификатов. Данный сертификат становится доступен для выполнения операций подписи, шифрования и расшифрования.

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



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.

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

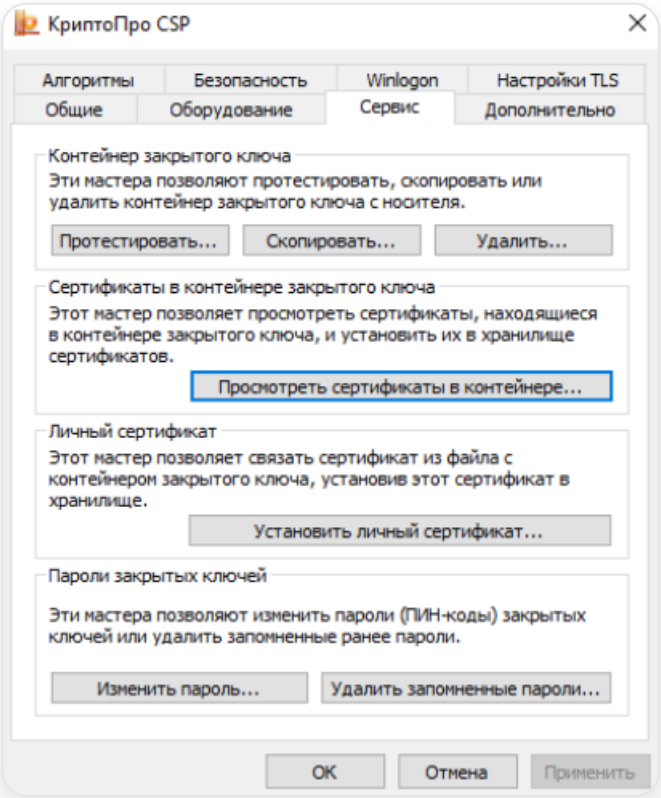


Установка сертификата с помощью программы КриптоПРО CSP.

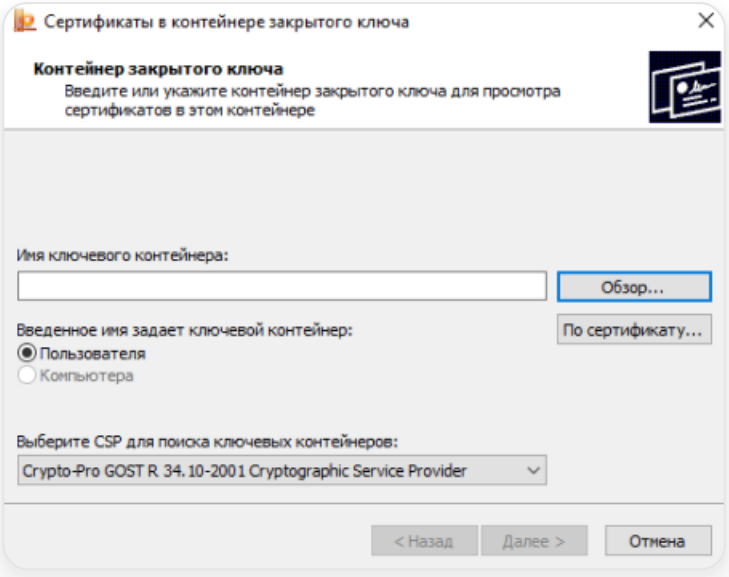
Установка с помощью программы КриптоПРО CSP отличается в операционных системах Windows, Linux и OS X.

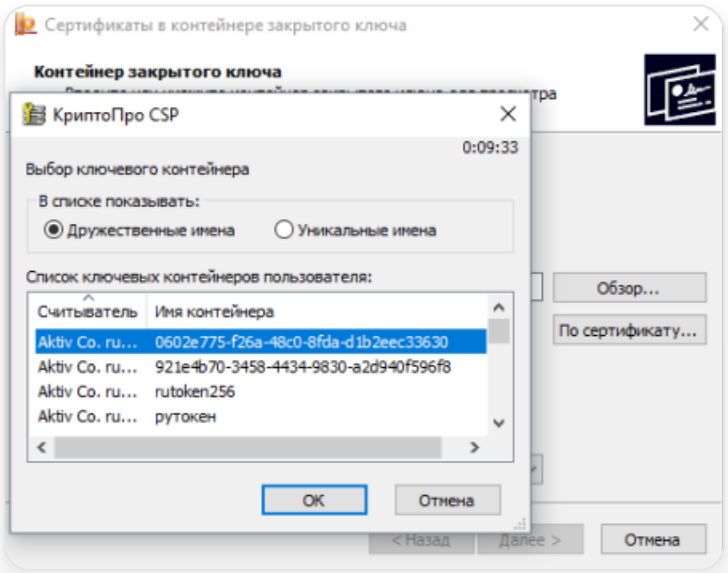
- Установка на операционной системе Windows выполняется следующим образом.

Нужно подключить токен (например, Рутокен) и открыть программу КритоПро CSP. В появившемся диалоге перейти на вкладку **Сервис** и нажать на кнопку **Просмотреть сертификаты в контейнере.**

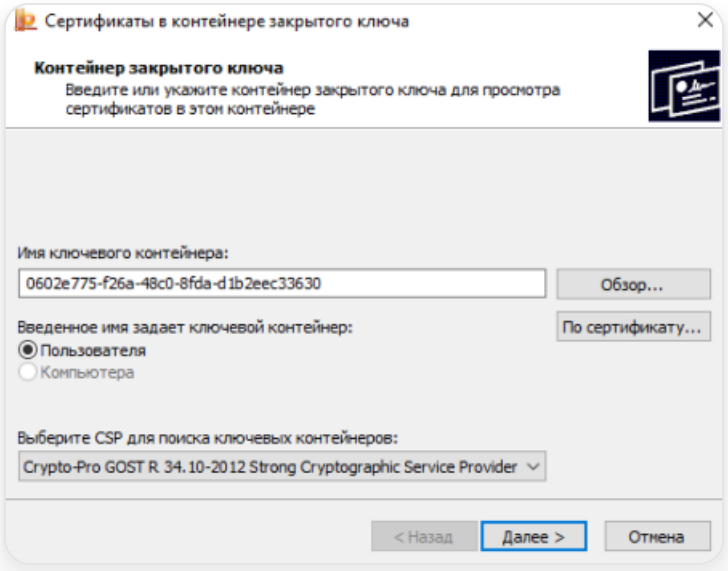


Далее нажать **Обзор** и выбрать контейнер.

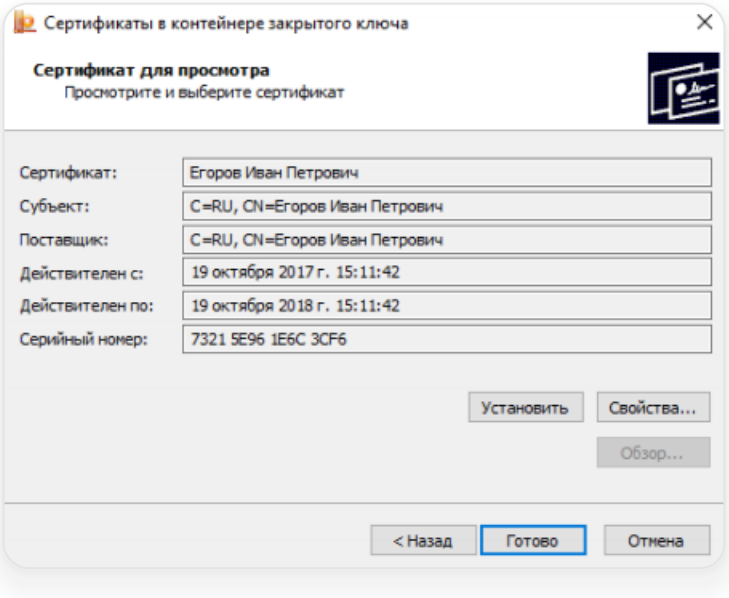




После выбора контейнера нажать кнопку **Далее.**



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



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

Установка сертификата на Linux

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

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

В результате получаем имя устройства, например,

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

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

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

Далее нужно ввести команду:

sudo /opt/cprocsp/sbin/<arch>/cpconfig -hardware reader -add "имя_устройства", где в кавычках указывается имя устройства. Например, **sudo /opt/cprocsp/sbin/amd64/cpconfig -hardware reader -add "Aktiv Rutoken ECP"**

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

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

Для просмотра контейнеров на токене можно ввести команду

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

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

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

Затем требуется ввести для копирования сертификата с токена

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

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

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

Установка сертификата на OS X

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

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

В результате получаем имя устройства, например,

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

Затем требуется ввести команду

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

add "Aktiv Rutoken ECP"

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

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

Для просмотра контейнеров на токене ввести команду: **/opt/cprocsp/bin/csptest -keys -verifyc -enu –fq -u**

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

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

Ввести или вставить команду для копирования сертификата с токена

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

В кавычках должно быть имя Вашего устройства и уникальное имя контейнера (справа от символа |).

В терминале должна вывестись информация об установленном Вами сертификате.

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

Открыть статью на сайте

Установка доверенных корневых, промежуточных сертификатов и списка отзыва сертификата

Архив. КриптоАРМ ГОСТ.

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).

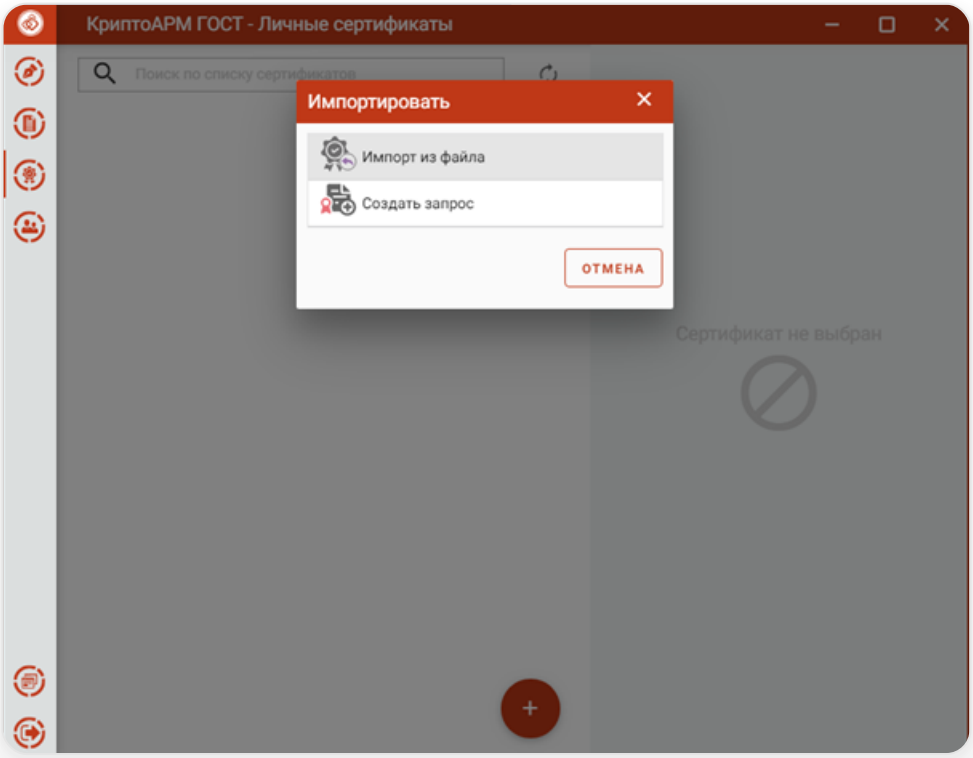
Для получения корневых и промежуточных сертификатов нужно обратиться в удостоверяющий центр.

Установить сертификаты можно через программный интерфейс приложения КриптоАРМ ГОСТ или с помощью команд программы КриптоПРО CSP.

Установка сертификата через КриптоАРМ ГОСТ:

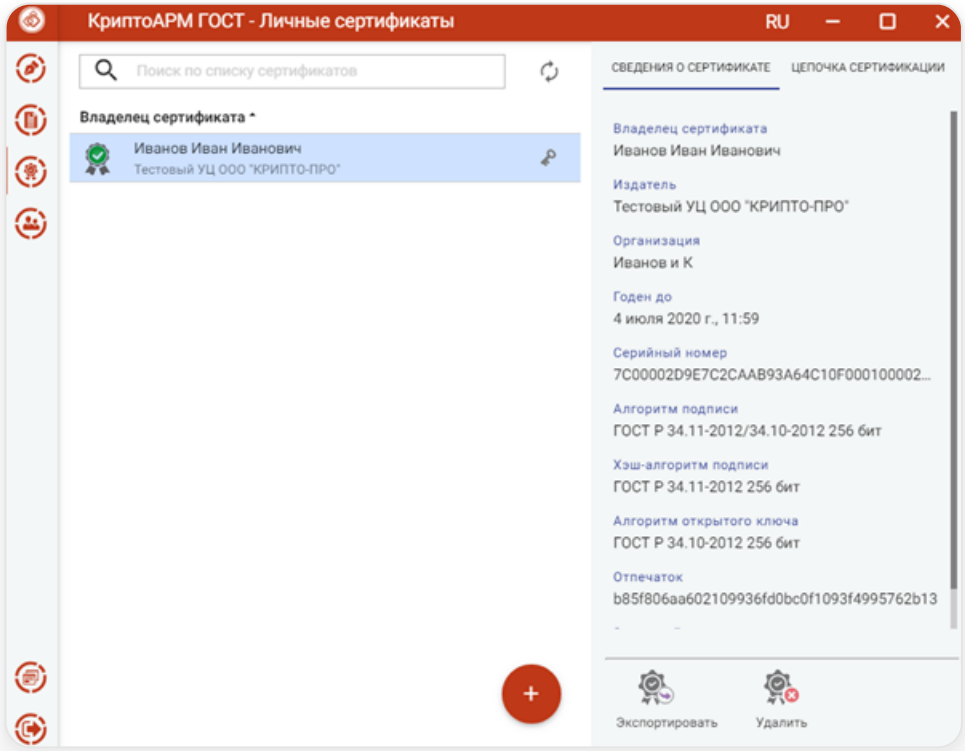
- Импорт личного сертификата с привязкой к закрытому ключу.

Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»). В открывшемся окне нужно выбрать операцию **Импорт из файла**

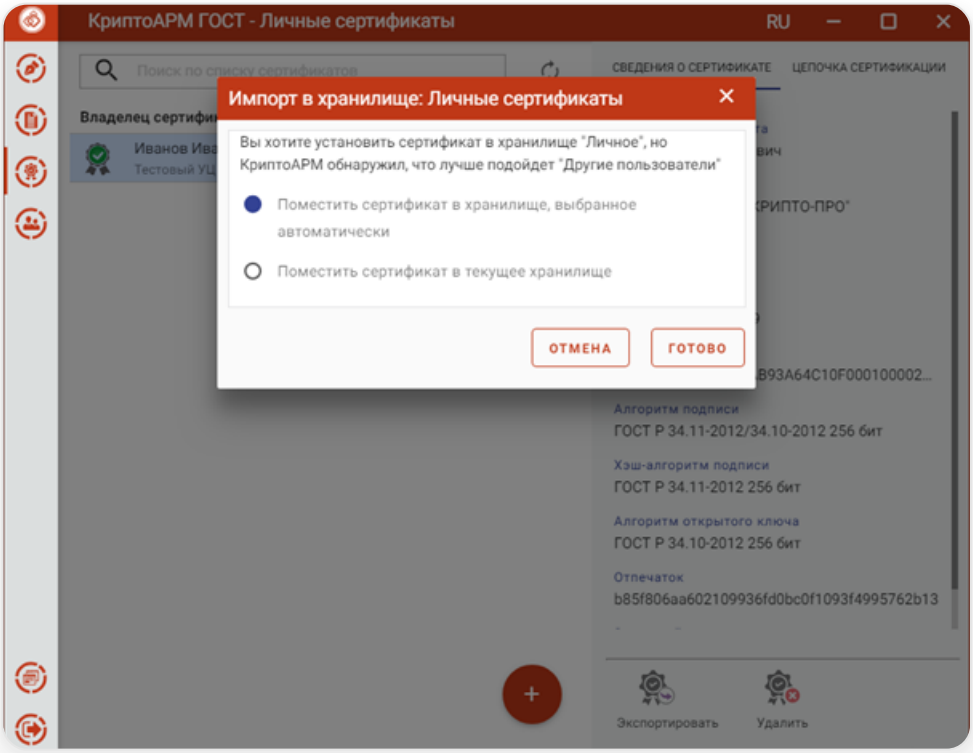


В появившемся диалоговом окне нужно выбрать файл сертификата. Это может быть файл формата pfx, содержащий ключевую пару (закрытый ключ и сертификат), или обычный сертификат, у которого есть закрытый ключ.

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



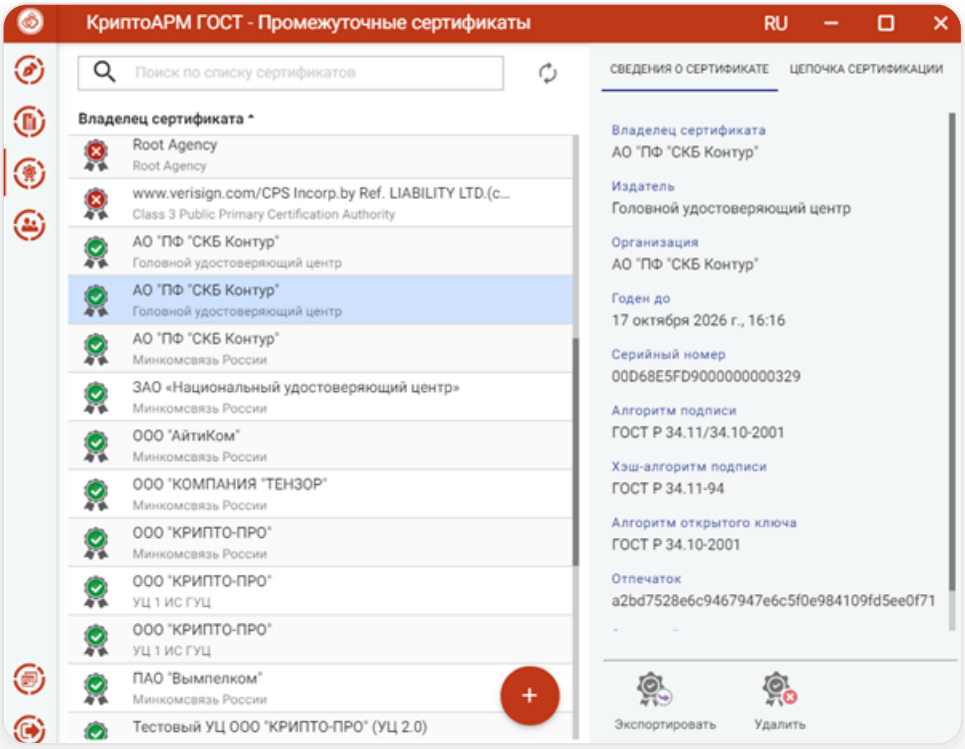
Если при импорте не будет найден закрытый ключ, соответствующий сертификату, то возникнет сообщение с предложением установить данный сертификат в подходящее хранилище или принудительно в выбранное. Если сертификат без закрытого ключа будет установлен в личное хранилище, то данным сертификатом нельзя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



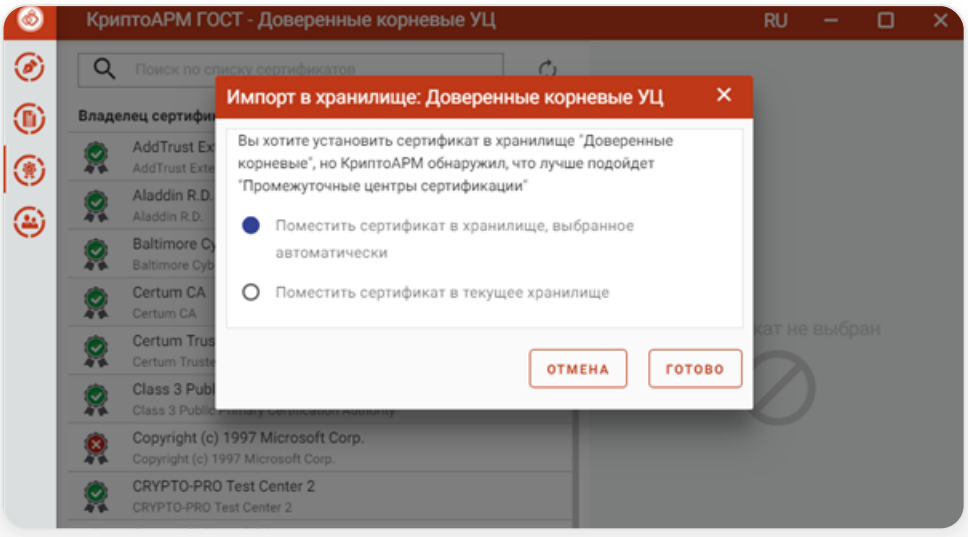
- Импорт сертификата без привязки к закрытому ключу.

Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»)и выбора опции **Импорт из файла**

В появившемся диалоговом окне нужно выбрать файл сертификата.
При успешном выполнении операции импорта сертификат автоматически помещается в выбранное хранилище.



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.



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

Установка корневого сертификата удостоверяющего центра

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

для OS X: /opt/cprocsp/bin/certmgr -inst -store uRoot -file пробел и перетащить в терминал файл сертификата в формате crt

То есть не только название файла должно быть, а полный путь к нему. Проще всего это сделать перетаскиванием файла непосредственно в терминал.

– Установка цепочки промежуточных сертификатов

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

Установка списка отозванных сертификатов

/opt/cprocsp/bin/<arch>/certmgr -inst -crl -file пробел и перетащить в терминал файл списка отзыва в формате crl

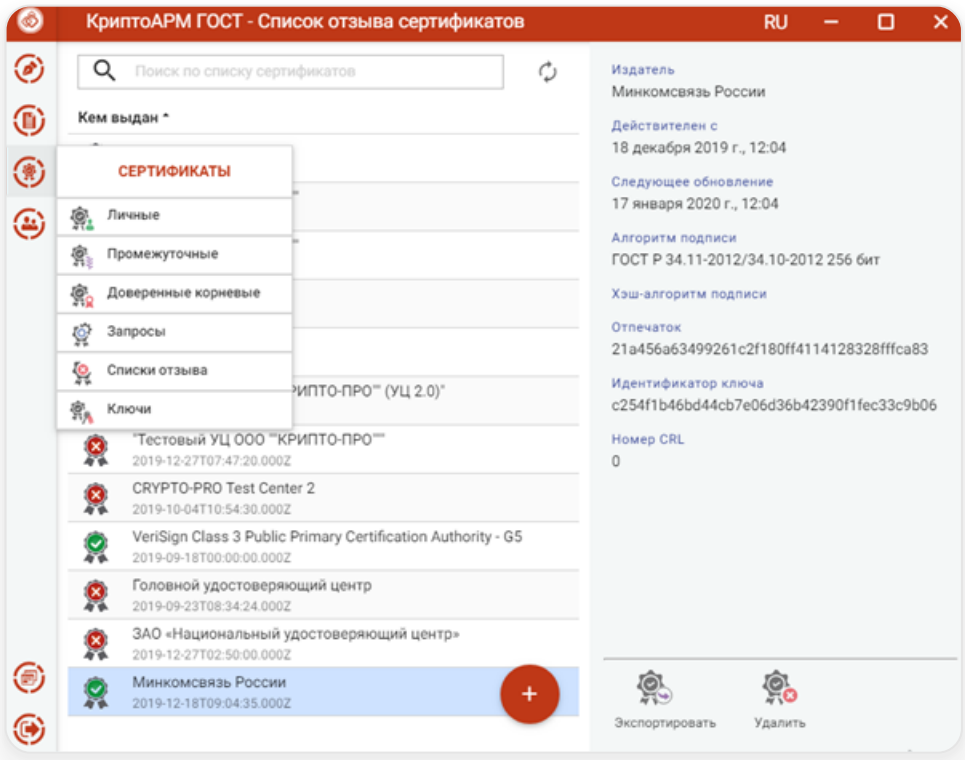
В приведенных выше командах под <arch>подразумевается один из следующих идентификаторов платформы:

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

После импорта сертификата или списка отзыва перезапустите программу нажав кнопку Выход.

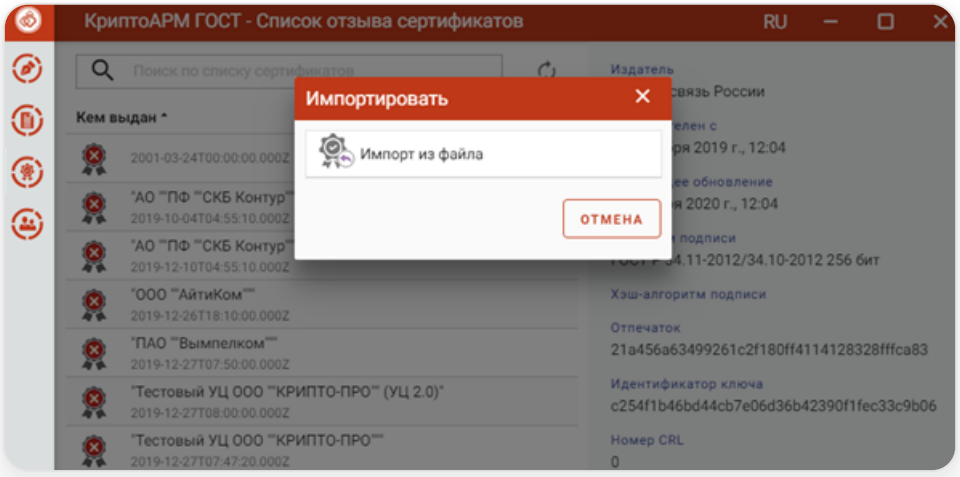
Списки отзыва сертификатов (COC)

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

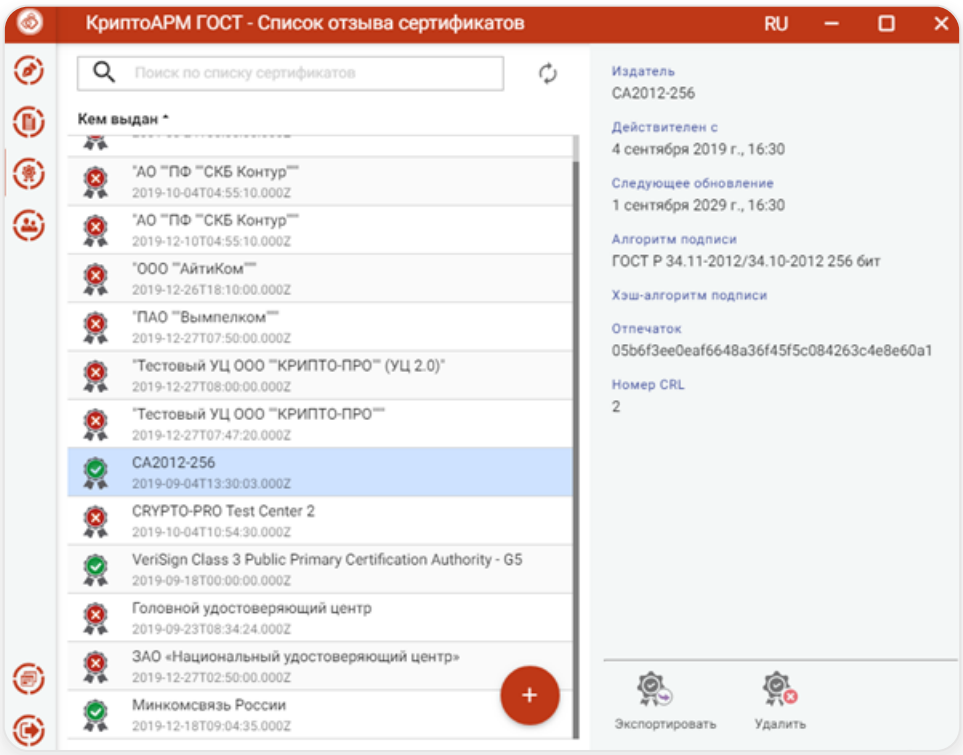


Списки отзыва можно импортировать, экспортировать и удалять.

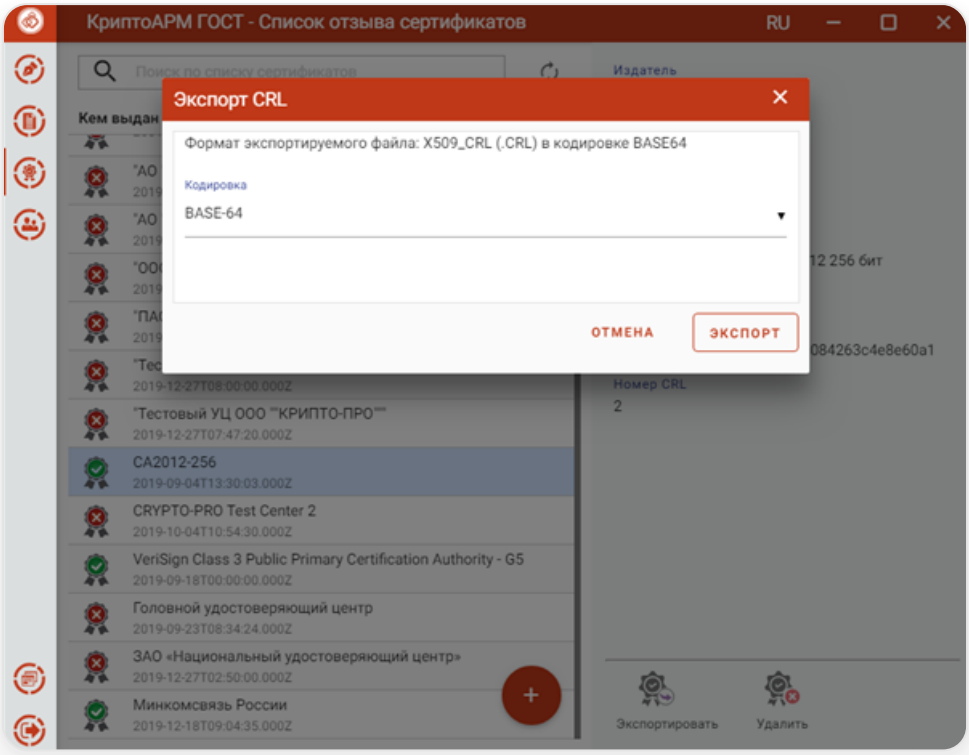
Для импорта списка отзыва надо нажать кнопку добавления («+») и выбрать опцию **Импорт из файла**. В открывшемся окне выбрать файл списка отзыва.



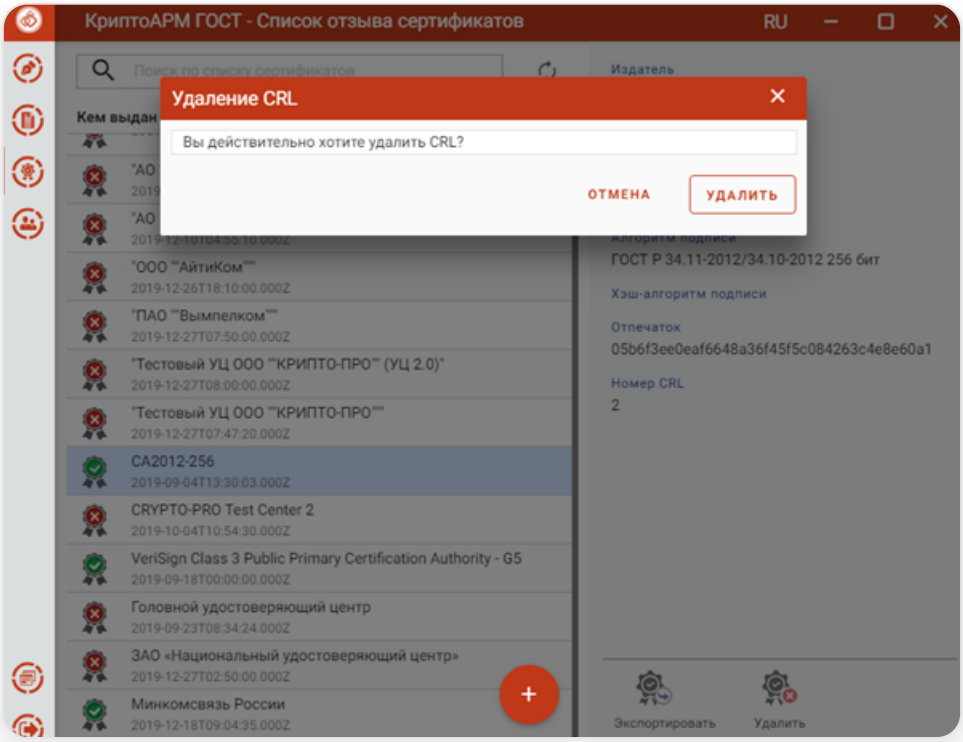
При успешном импорте COC отображается в разделе Список отзыва сертификатов.



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



Для удаления COC надо нажать кнопку **Удалить** и подтвердить удаление в соответствующем окне.


КриптоАРМ ГОСТ - Список отзыва сертификатов
RU
Поиск по списку сертификатов
Кем выдан
Удаление CRL
Вы действительно хотите удалить CRL?
ОТМЕНА
УДАЛИТЬ
"ООО ""АйтиКом"""
2019-12-26T18:10:00.000Z
"ПАО ""Вымпелком"""
2019-12-27T07:50:00.000Z
"Тестовый УЦ ООО ""КРИПТО-ПРО"" (УЦ 2.0)"
2019-12-27T08:00:00.000Z
"Тестовый УЦ ООО ""КРИПТО-ПРО"""
2019-12-27T07:47:20.000Z
CA2012-256
2019-09-04T13:30:03.000Z
CRYPTO-PRO Test Center 2
2019-10-04T10:54:30.000Z
VeriSign Class 3 Public Primary Certification Authority - G5
2019-09-18T00:00:00.000Z
Головной удостоверяющий центр
2019-09-23T08:34:24.000Z
ЗАО «Национальный удостоверяющий центр»
2019-12-27T02:50:00.000Z
Минкомсвязь России
2019-12-18T09:04:35.000Z
Издатель
ГОСТ Р 34.11-2012/34.10-2012 256 бит
Хэш-алгоритм подписи
Отпечаток
05b6f3ee0eaf6648a36f45f5c084263c4e8e60a1
Номер CRL
2
Экспортировать
Удалить

Открыть статью на сайте

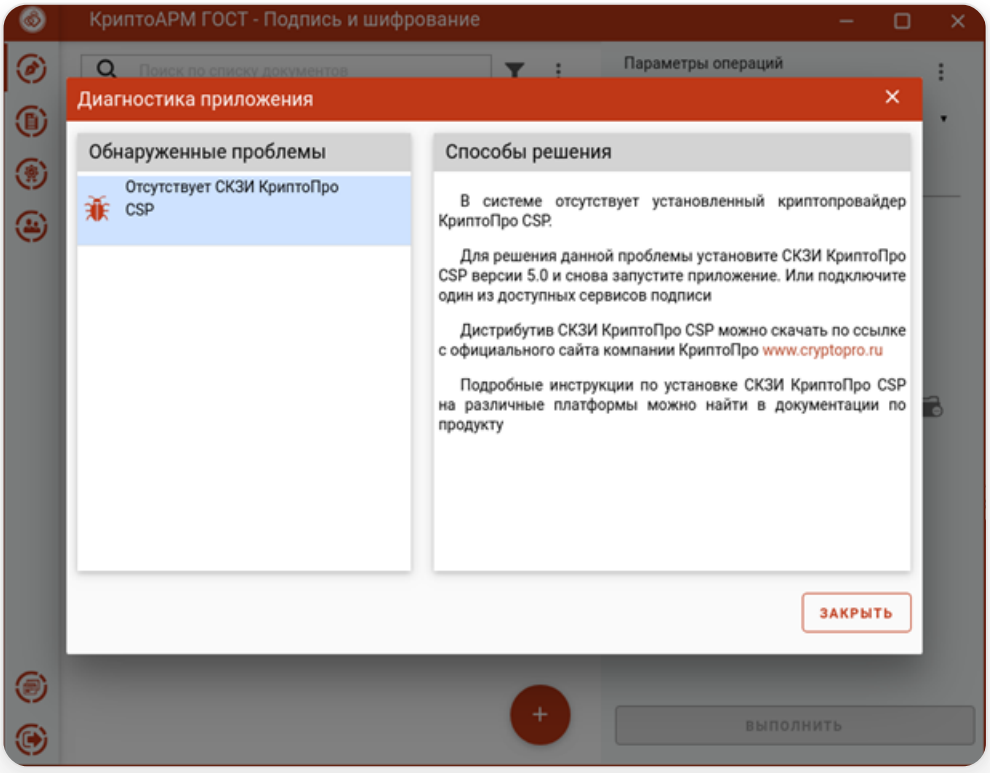
Отсутствует СКЗИ КриптоПро CSP

Архив. КриптоАРМ ГОСТ.

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

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.



Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

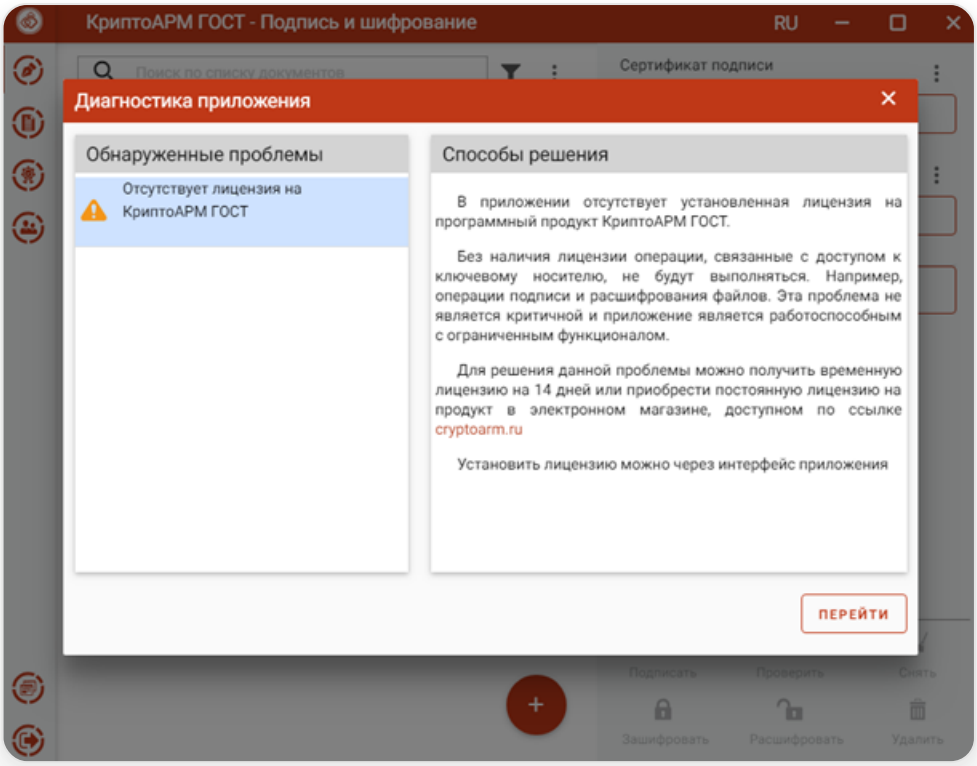
Требуется установка криптопровайдера КриптоПро CSP.

Открыть статью на сайте

Отсутствует лицензия на КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ.

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



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

При закрытии мастера диагностики приложение остается работоспособным, но с ограниченным функционалом.

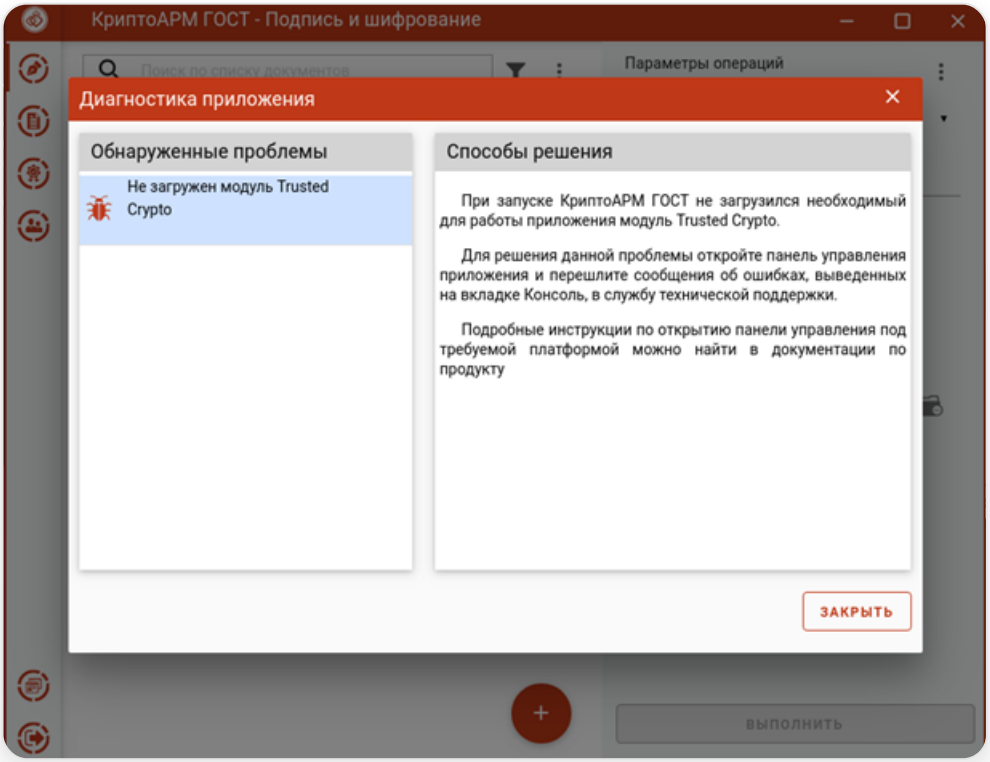
Без лицензии не будут выполняться операции, связанные с доступом к закрытому ключу (например, подпись и расшифрование).

Открыть статью на сайте

Не загружен модуль Trusted Crypto

Архив. КриптоАРМ ГОСТ.

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



Дальнейшая работа приложения невозможна. Приложение можно только закрыть.

В Windows для устранения данного уведомления нужно установить Распространяемый пакет Visual C++ для Visual Studio 2015, 2017, 2019 и 2022. Если установка этих библиотек не помогла, проверьте, установлены ли устаревшие сборки Visual C++, удалите их.

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.

Запуск программы в консольном режиме и включение логирования рассмотрим далее.

Включение режима логирования и консоль управления

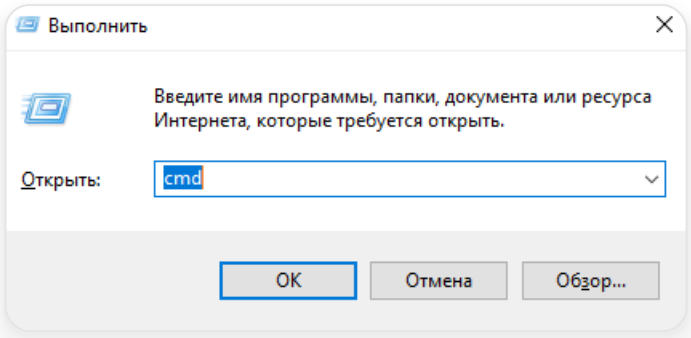
Приложение КриптоАРМ ГОСТ построено на основе браузера, в котором исполняются скрипты, написанные на языке JavaScript и отображается интерфейс приложения. Ошибки, которые возникают при работе интерфейсной части приложения, связанные с проблемами подключения модулей и других компонент можно отследить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

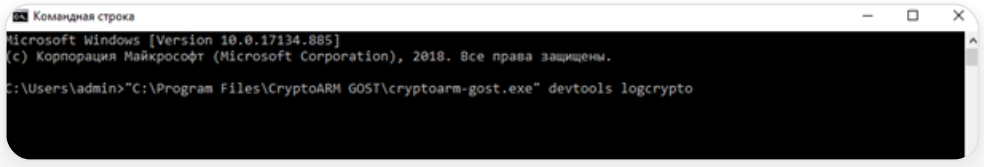
1. Отслеживание ошибок на платформе MS Windows

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

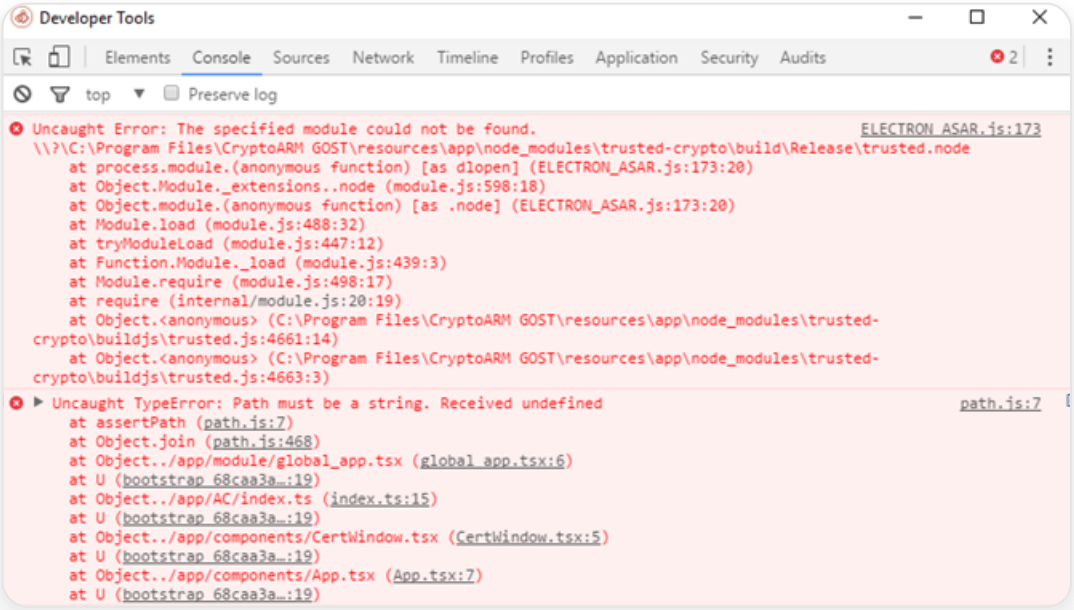


В открывшемся окне ввести команду запуска приложения КриптоАРМ ГОСТ

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



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



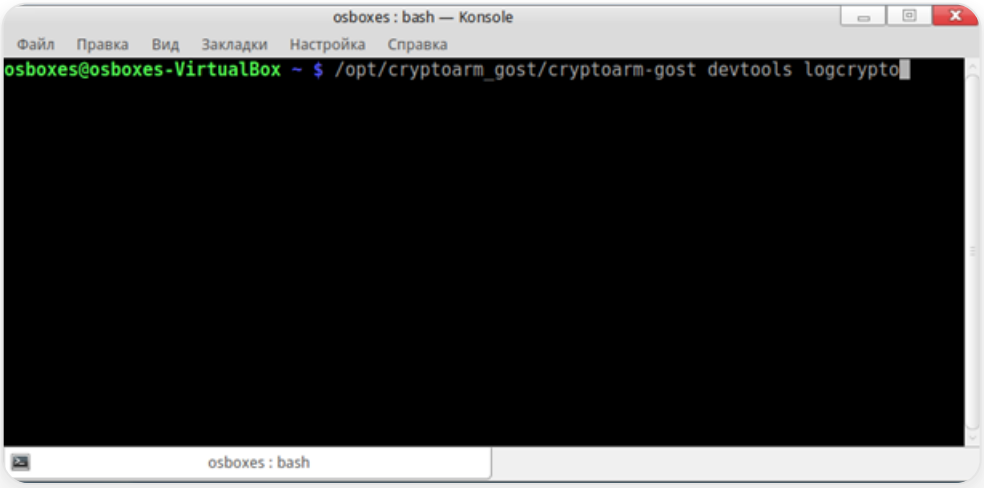
При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

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

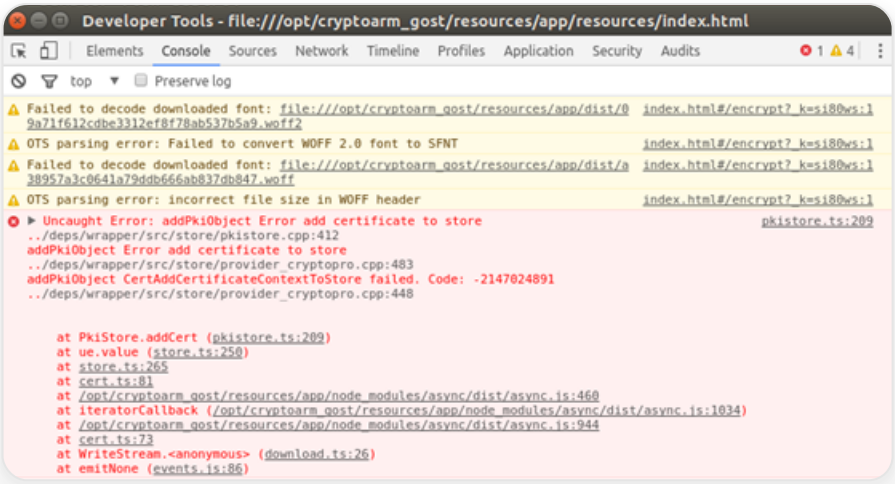
2. Отслеживание ошибок на платформе LINUX

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

/opt/cryptoarm_gost/cryptoarm-gost devtools logcrypto



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



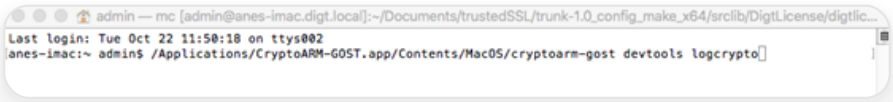
При выполнении операции, приводящей к ошибке, в открывшемся дополнительном окне управления на вкладке Console отобразится текст ошибки.

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

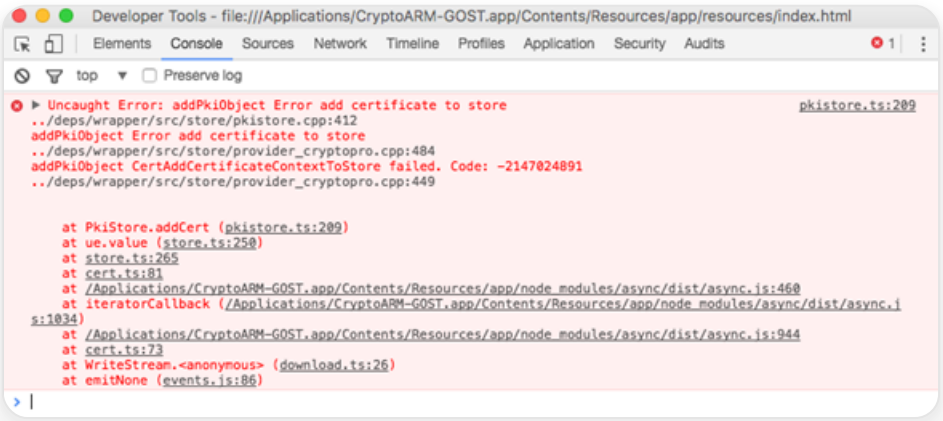
3. Отслеживание ошибок на платформе OS X

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

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



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



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**.

Открыть статью на сайте

Документация КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ.

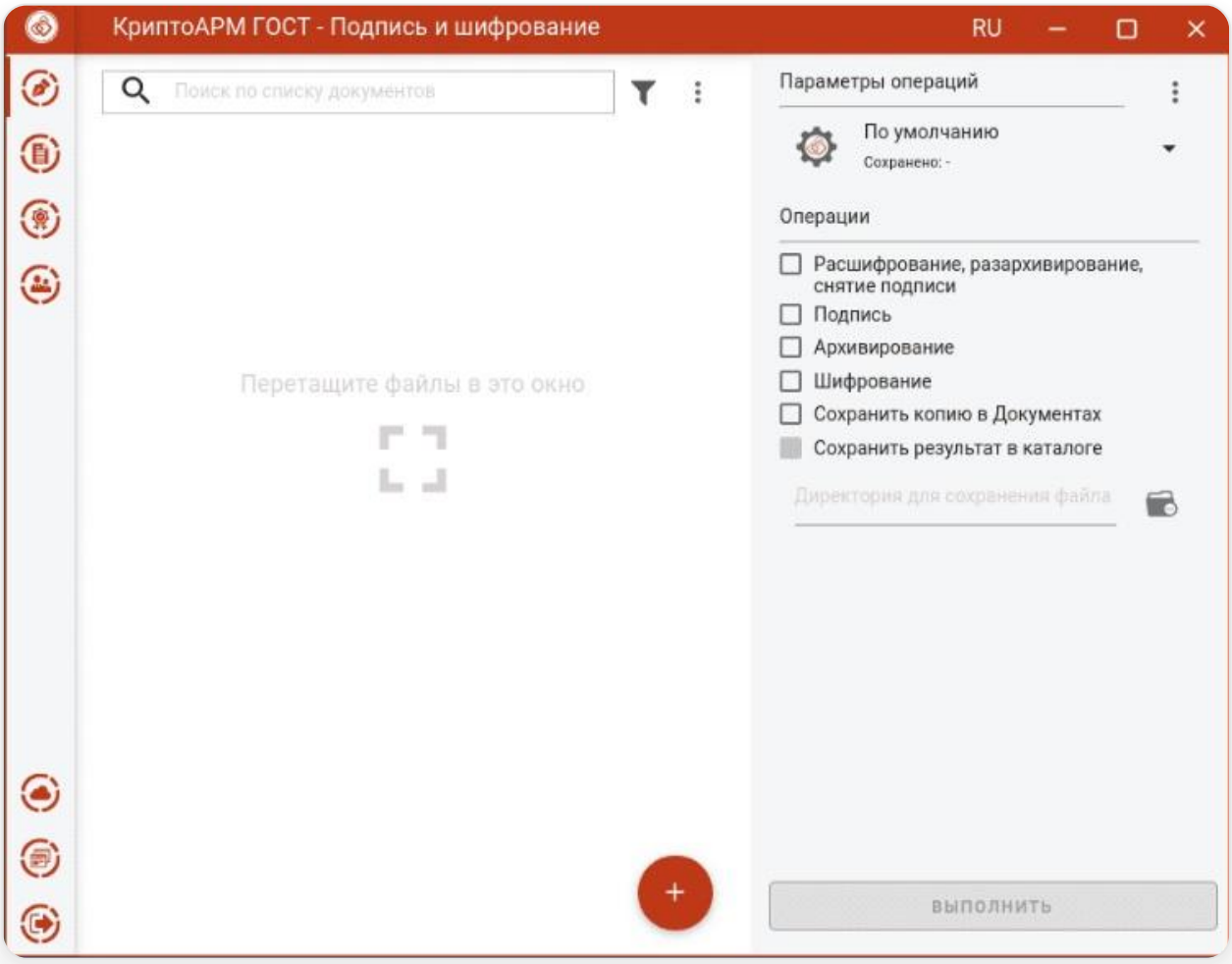
Документация КриптоАРМ ГОСТ

Открыть статью на сайте

Начальная страница

Архив. КриптоАРМ ГОСТ.

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



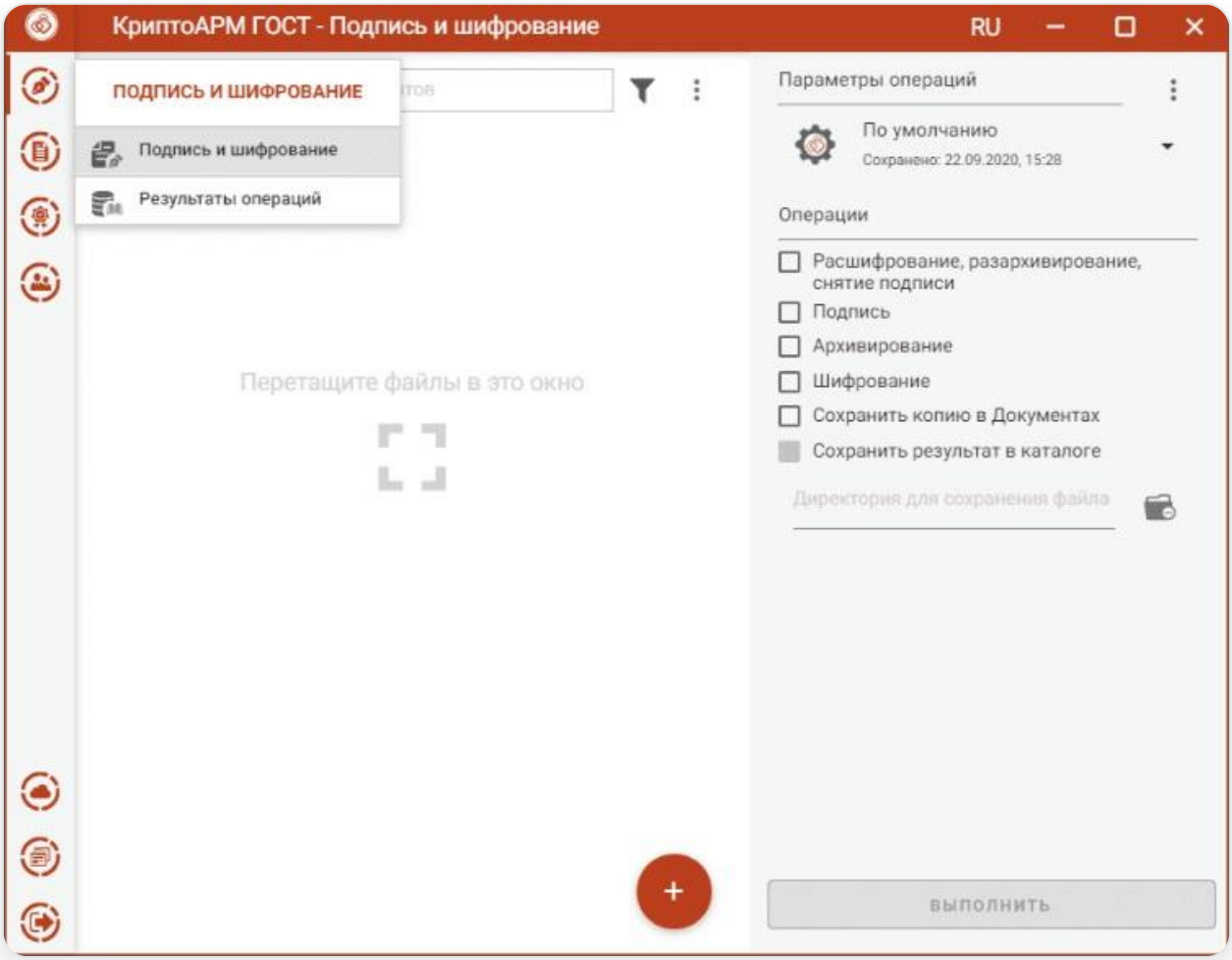
Левая рабочая часть окна предназначена для управления списком файлов; в правой части располагается панель выбора **Параметров операций**, переключатель **Операций** и кнопка **Выполнить.**

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

- **Расшифрование, разархивирование, снятие подписи** – опция для выполнения обратных операций. Для выполнения обратных операций не требуется установка дополнительных параметров.

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

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



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

Открыть статью на сайте

Создание электронной подписи

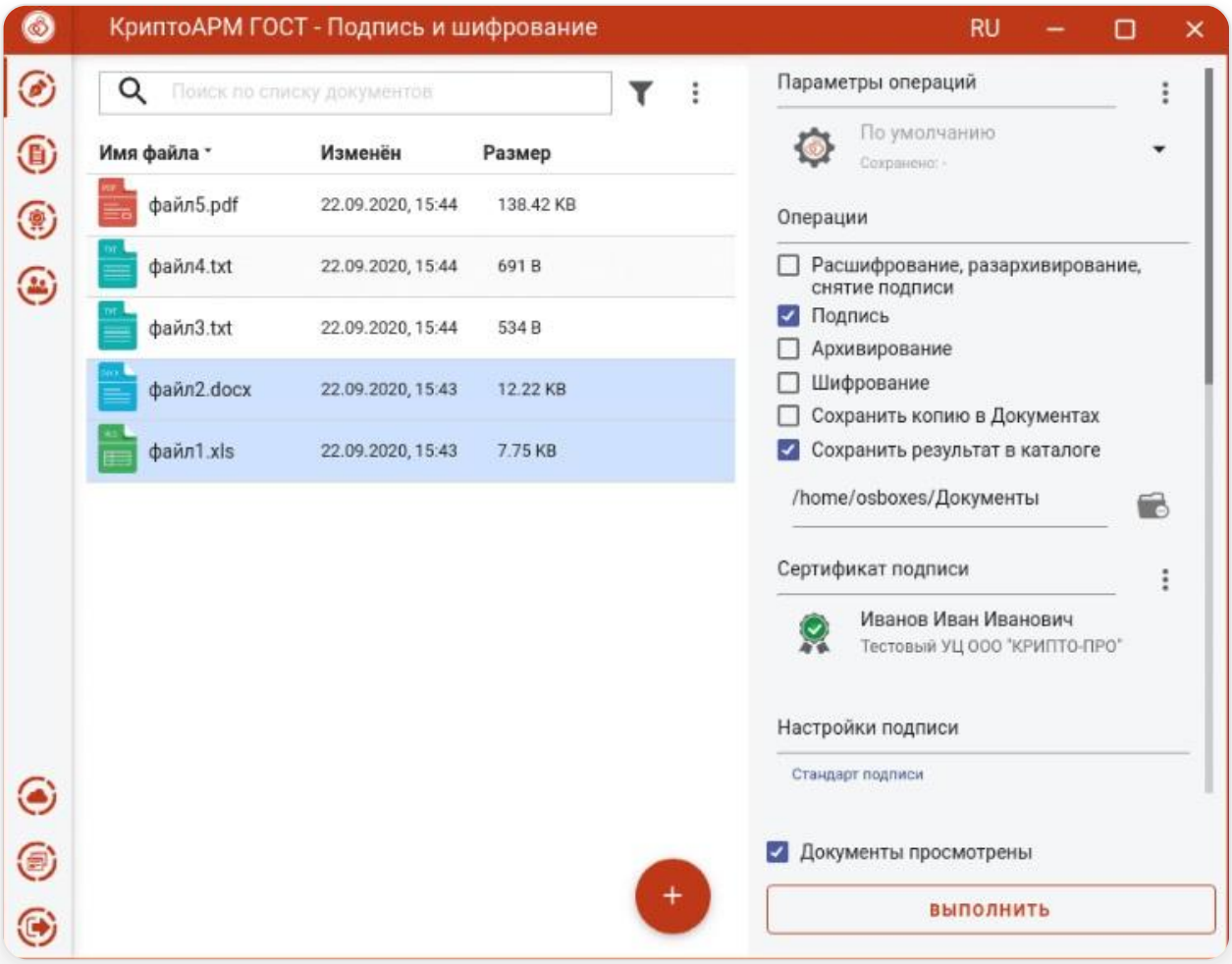
Архив. КриптоАРМ ГОСТ.

Подписать файлы можно на странице **Подпись и шифрование**. Для этого нужно:

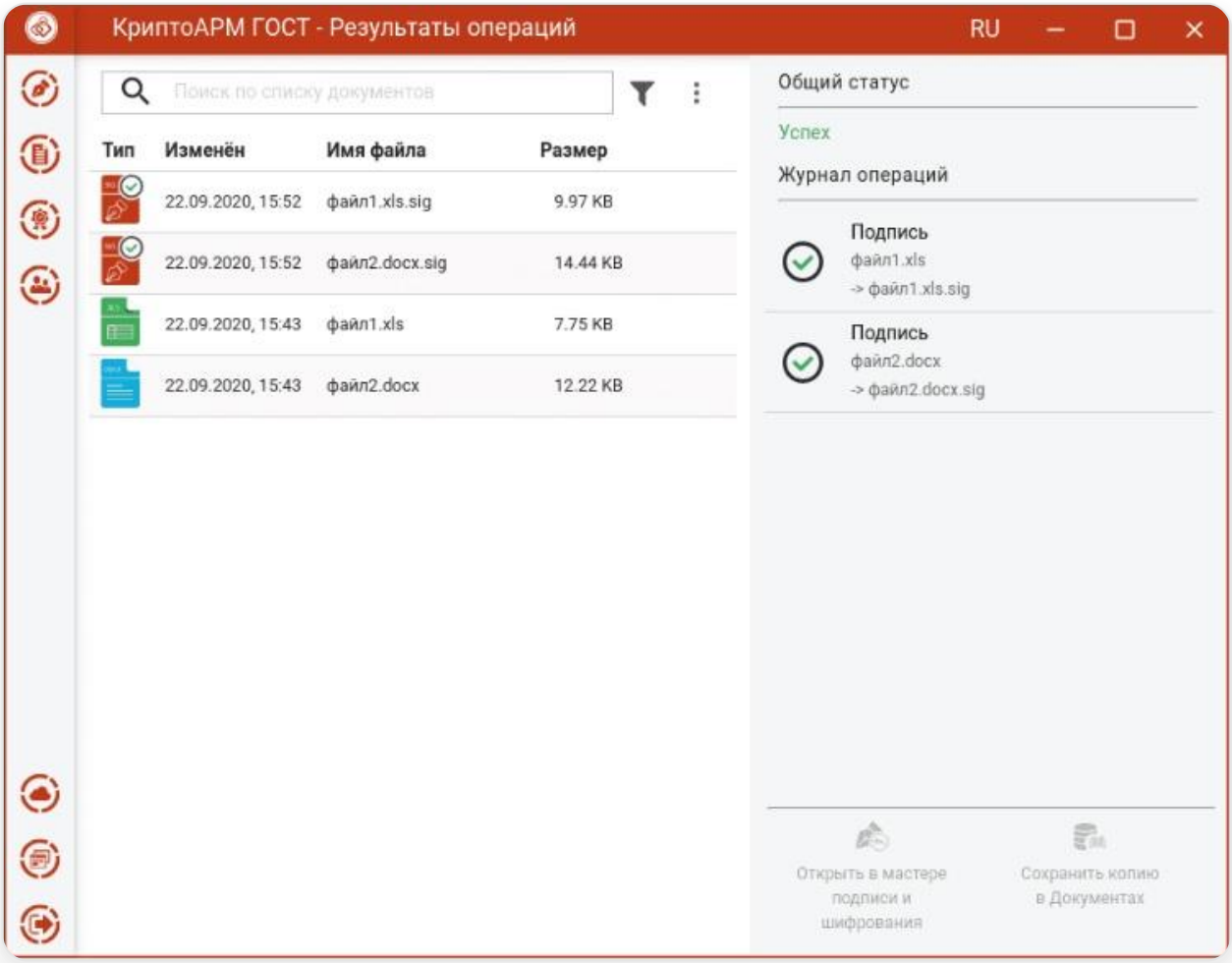
- выбрать подписываемые файлы,
- задать параметры подписи (подробнее в разделе **Установка параметров подписи**);
- выбрать сертификат подписи (подробнее в разделе **Выбор сертификата подписи**).

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

Подписать можно любые файлы, кроме зашифрованных.



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



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

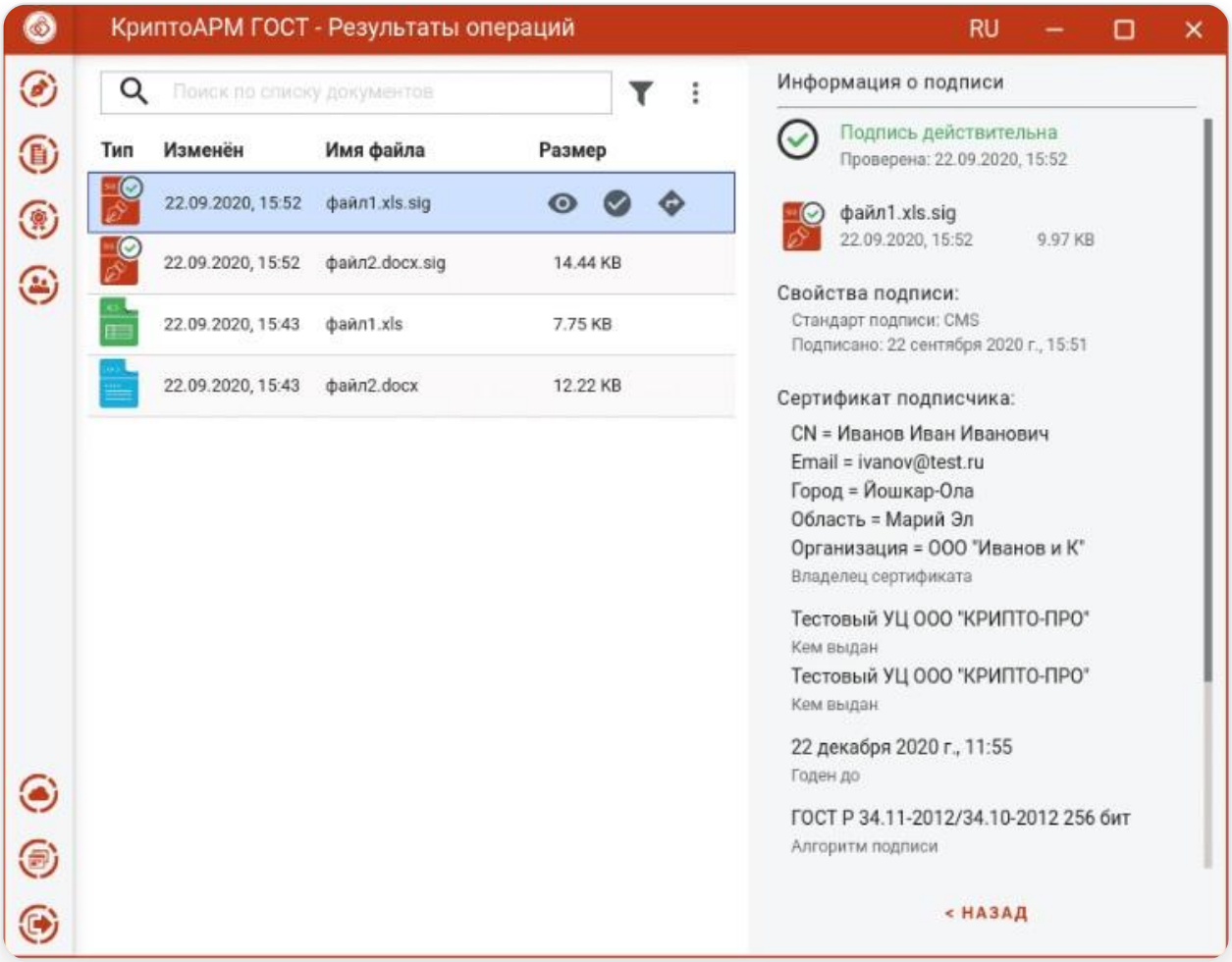
Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученного после операции файла сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Файлы из данного каталога доступны в пункте меню **Документы**.

Подпись проверяется автоматически.

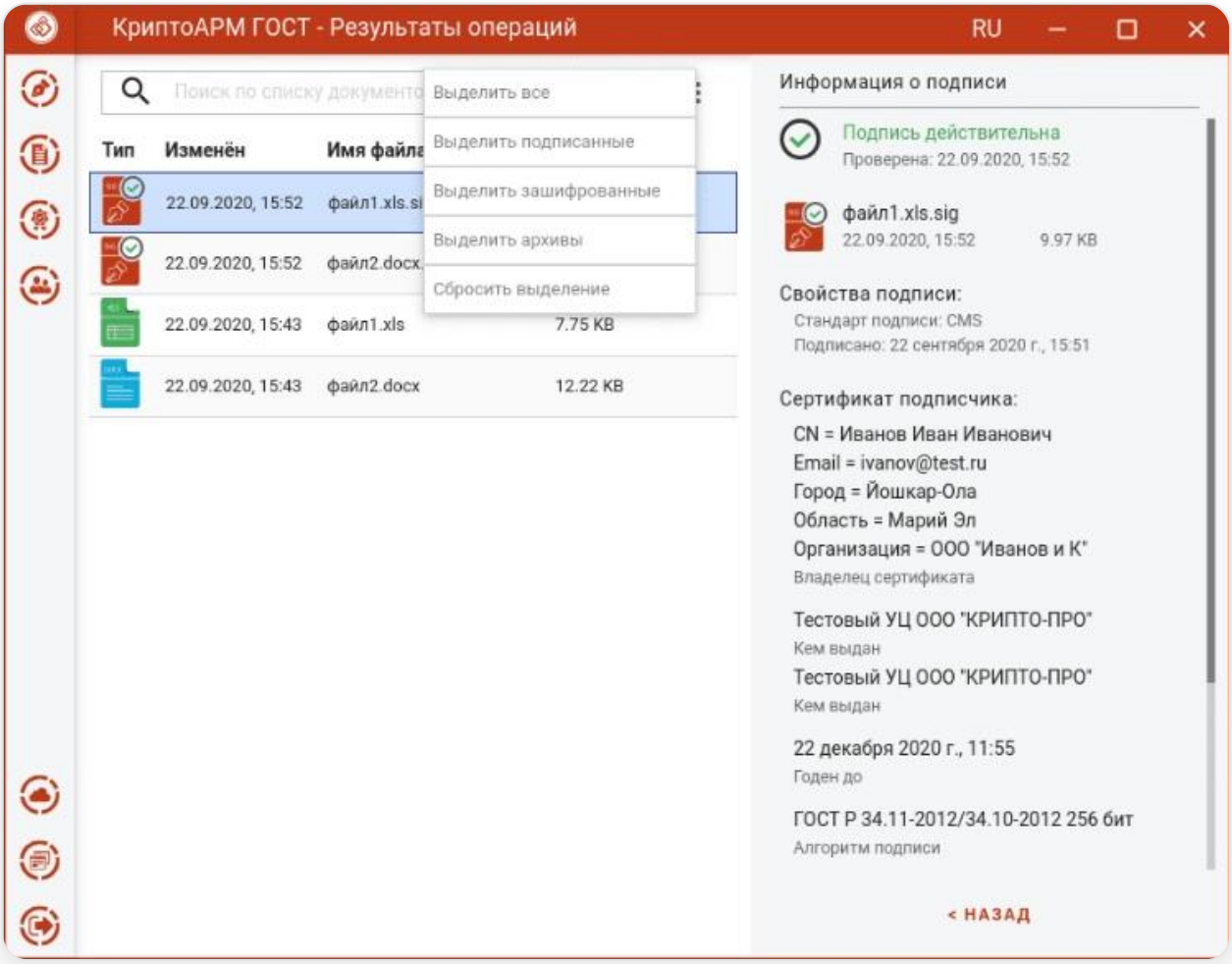
Для просмотра информации о подписи нужно выделить один файл в списке.

Для каждого документа доступны операции:

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



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



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

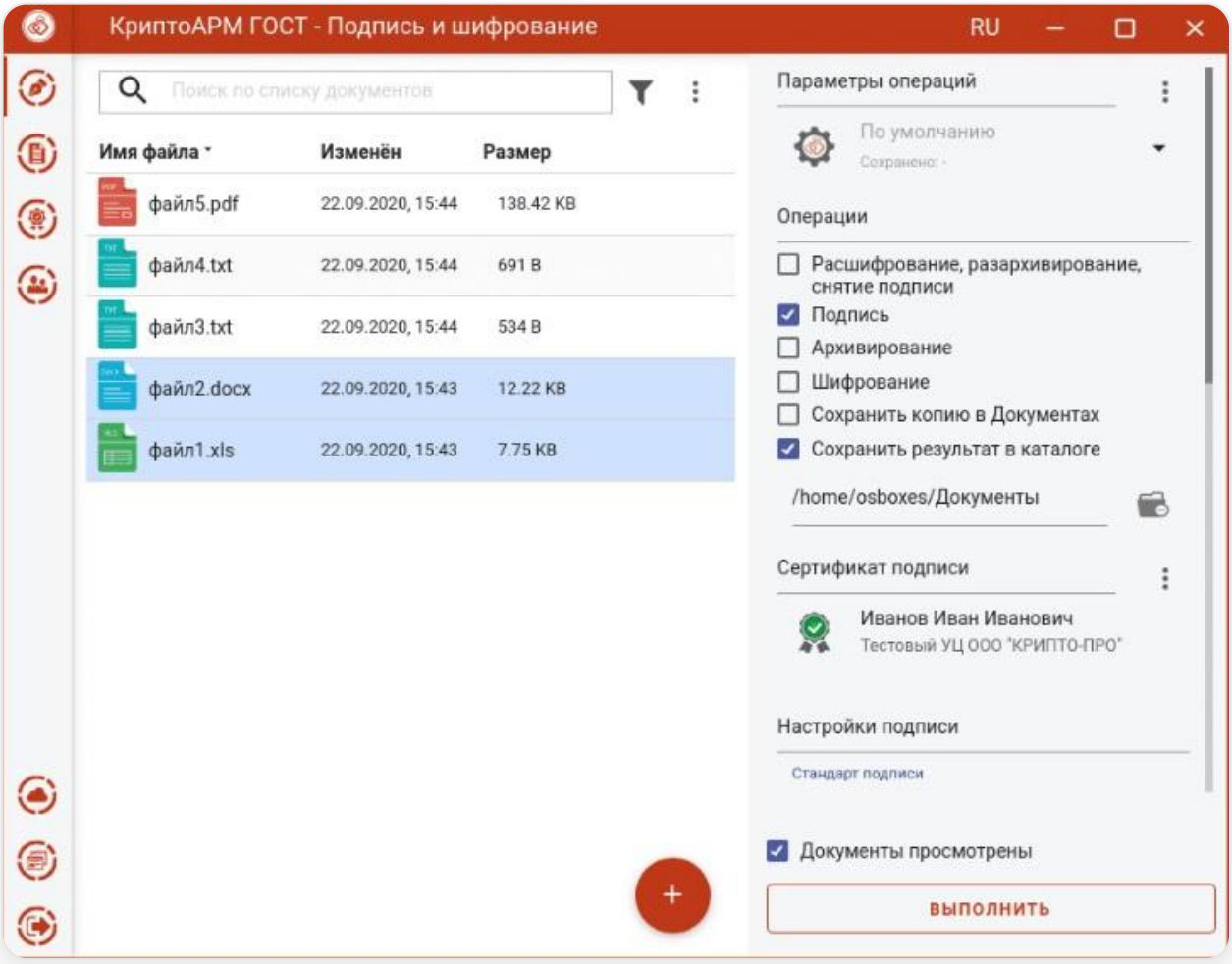
После выполнения операции мастер **Подписи и шифрования** очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения и доступны в меню **Подпись и шифрование - Результаты операций**.

Открыть статью на сайте

Установка параметров подписи

Архив. КриптоАРМ ГОСТ.

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

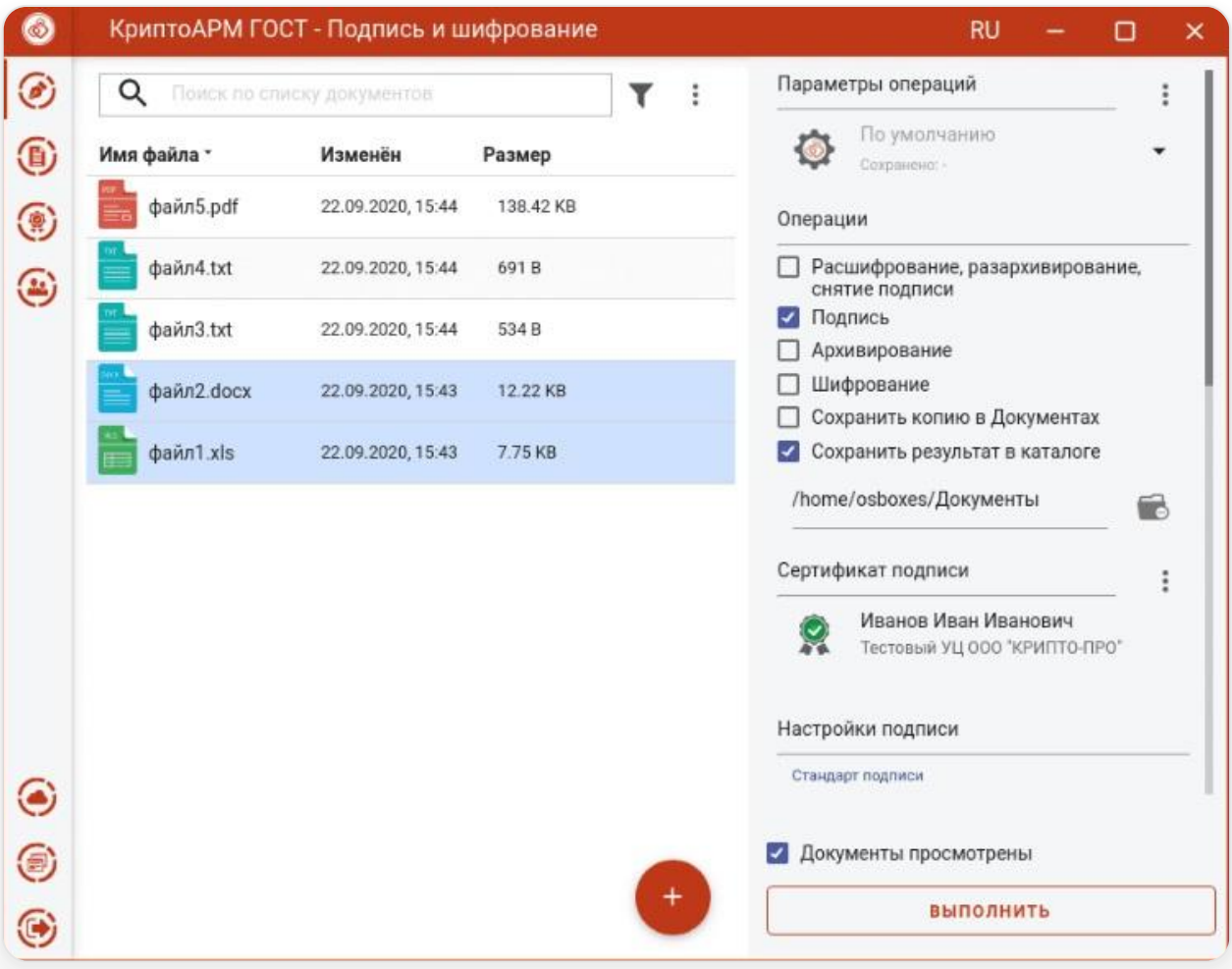


В параметрах можно настроить:

- **Сертификат подписи** – личный сертификат с закрытым ключом.
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 - для усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее в разделе **Создание усовершенствованной подписи**). Стандарт подписи CAdES-X Long Type 1 доступен только при установленных модулях КриптоПро TSP Client и КриптоПро OCSP Client.
- **Вид подписи** – присоединённая или отсоединённая.

- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробно в разделе **Создание подписи со штампом времени**). Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробно в разделе **Создание подписи со штампом времени**). Данная опция доступна только при установленном модуле КриптоПро TSP Client.

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



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

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

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

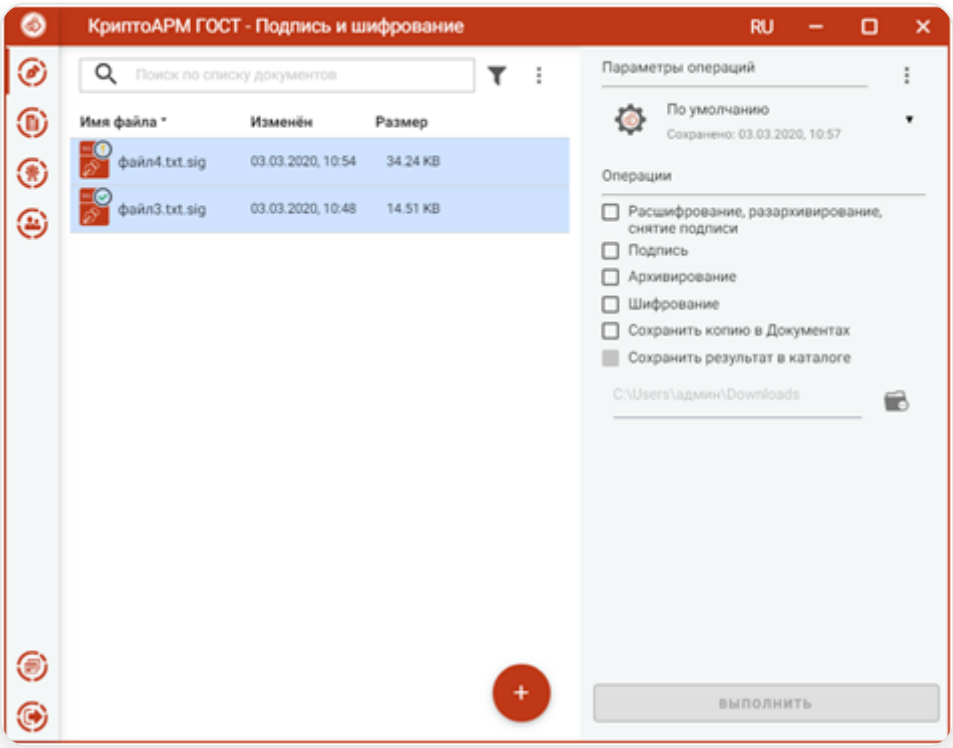
Открыть статью на сайте

Проверка электронной подписи

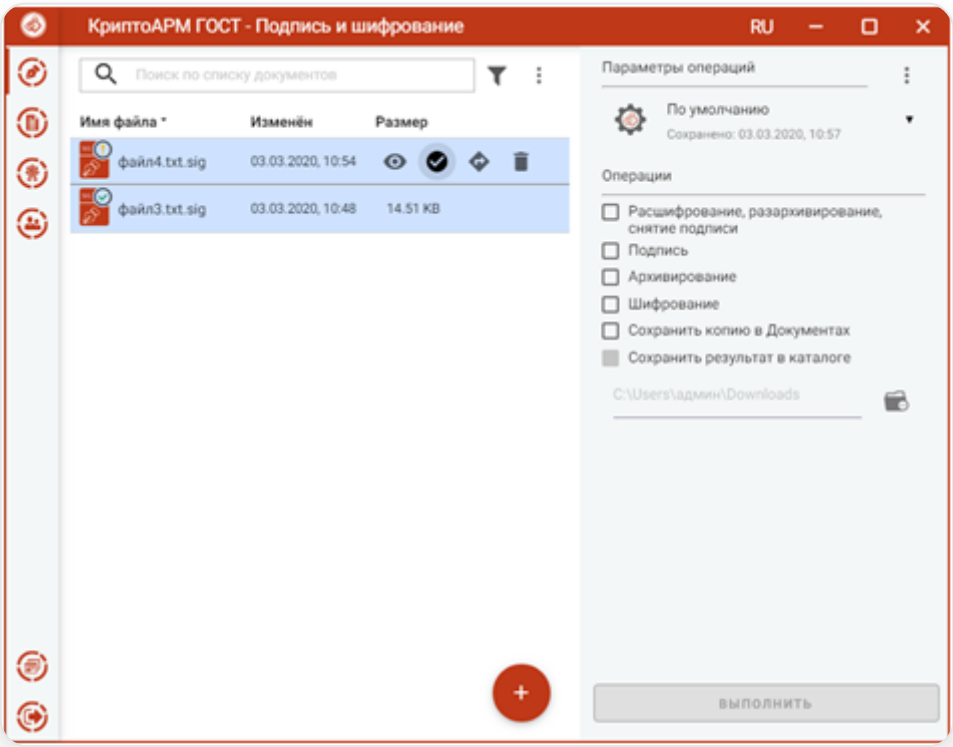
Архив. КриптоАРМ ГОСТ.

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

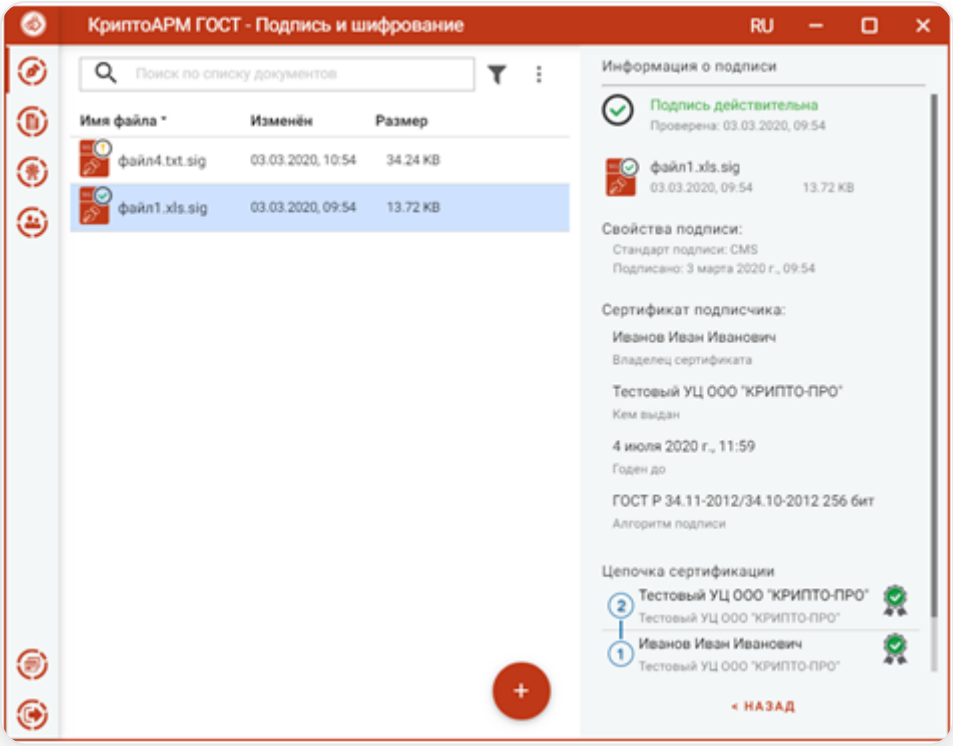
Результат проверки подписей отображается в виде общего сообщения и цветового индикатора на иконке для каждого файла: зеленый - подпись действительна; красный - подпись недействительна.



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

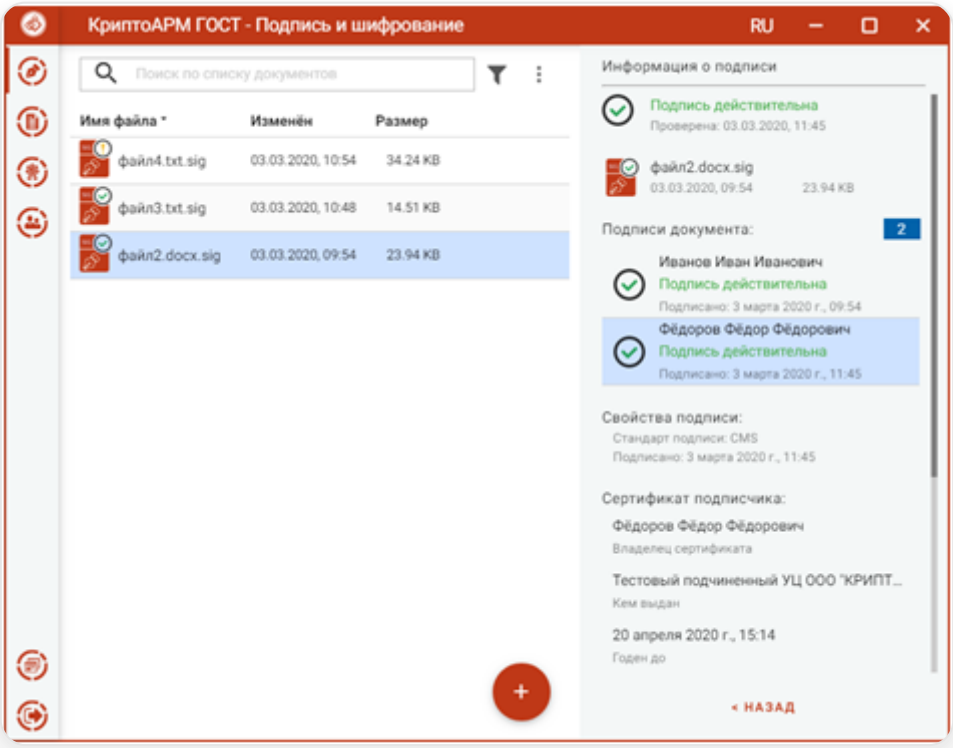


При выделении одного подписанного файла в правой области отображается информация о подписи.

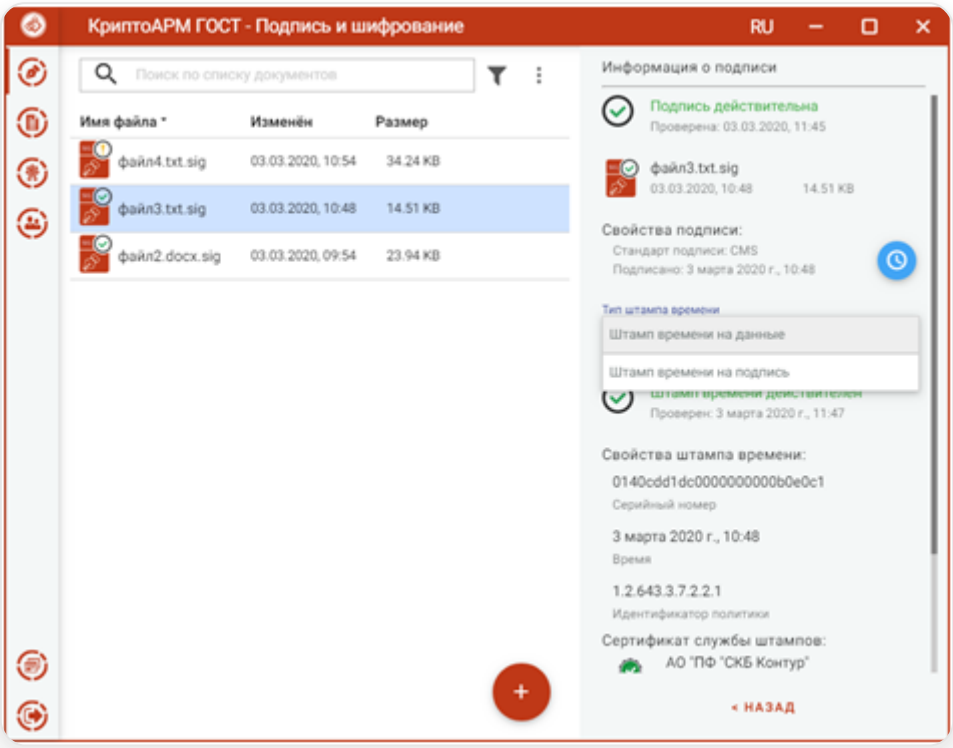


По кнопке **Назад** информация о подписи закрывается и происходит возврат к операциям.

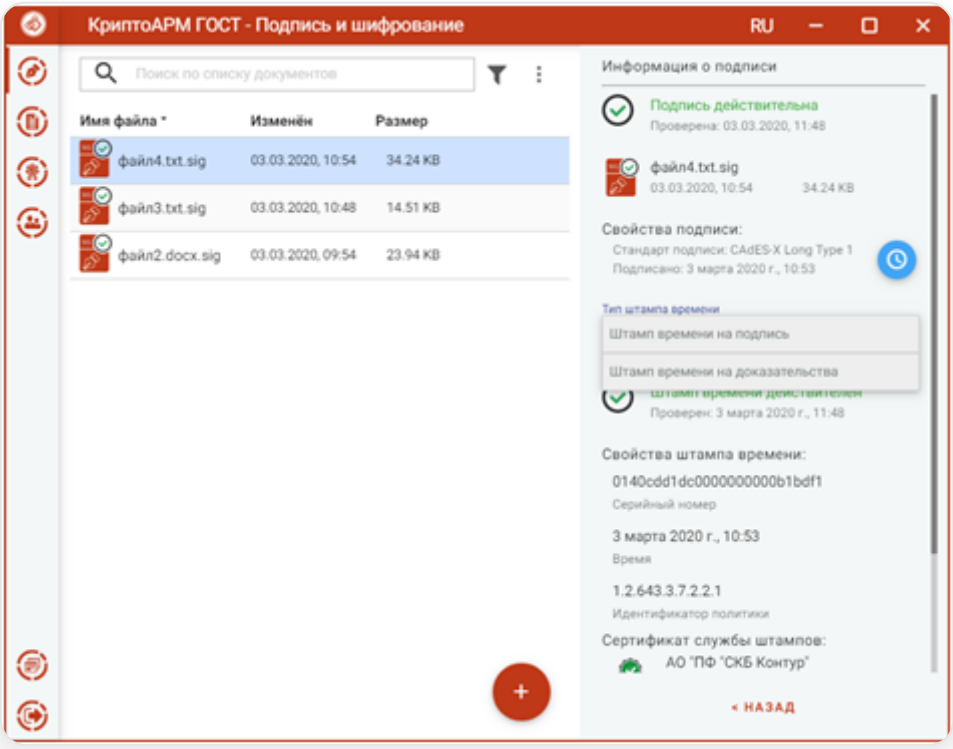
Если документ подписан несколькими подписями (имеет соподписи), то для просмотра информации о подписи нужно в списке выбрать подписчика.



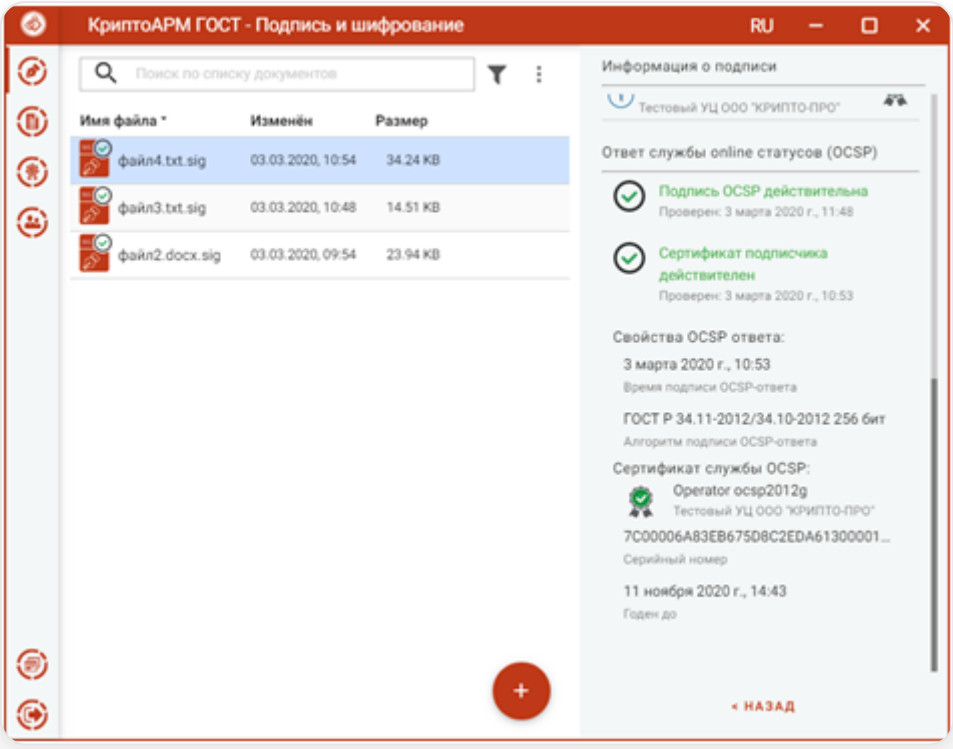
Если документ подписан подписью со штампом времени, то для просмотра параметров штампа нужно нажатием на иконку развернуть информацию и выбрать в выпадающем списке тип штампа времени.



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



Информация об OCSP ответе усовершенствованной подписи представлена на рисунке ниже:

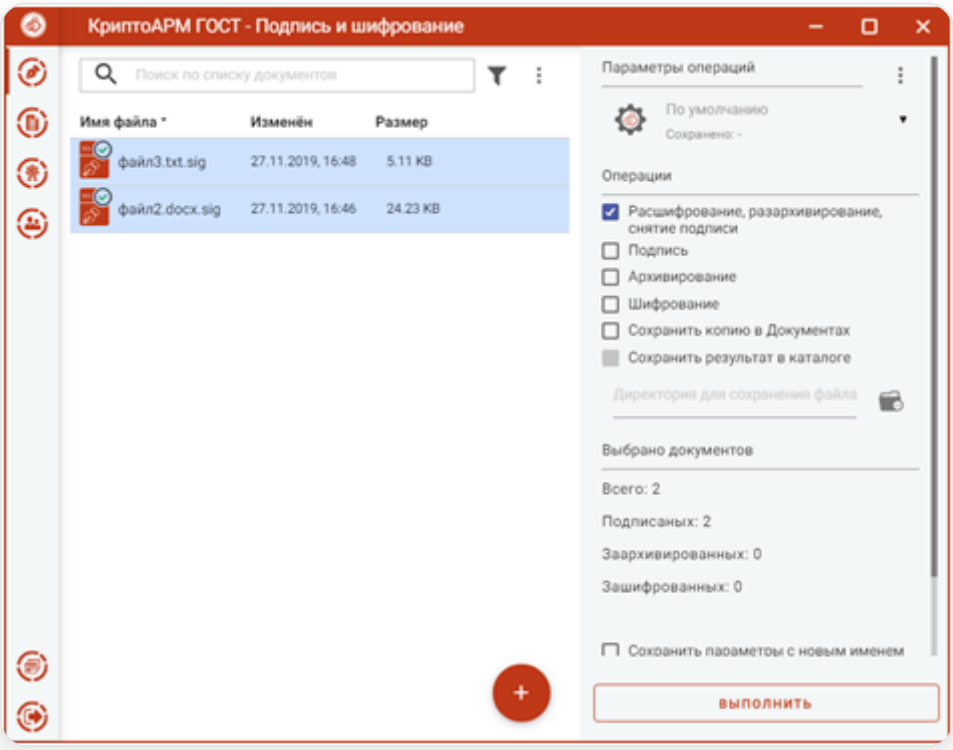


Открыть статью на сайте

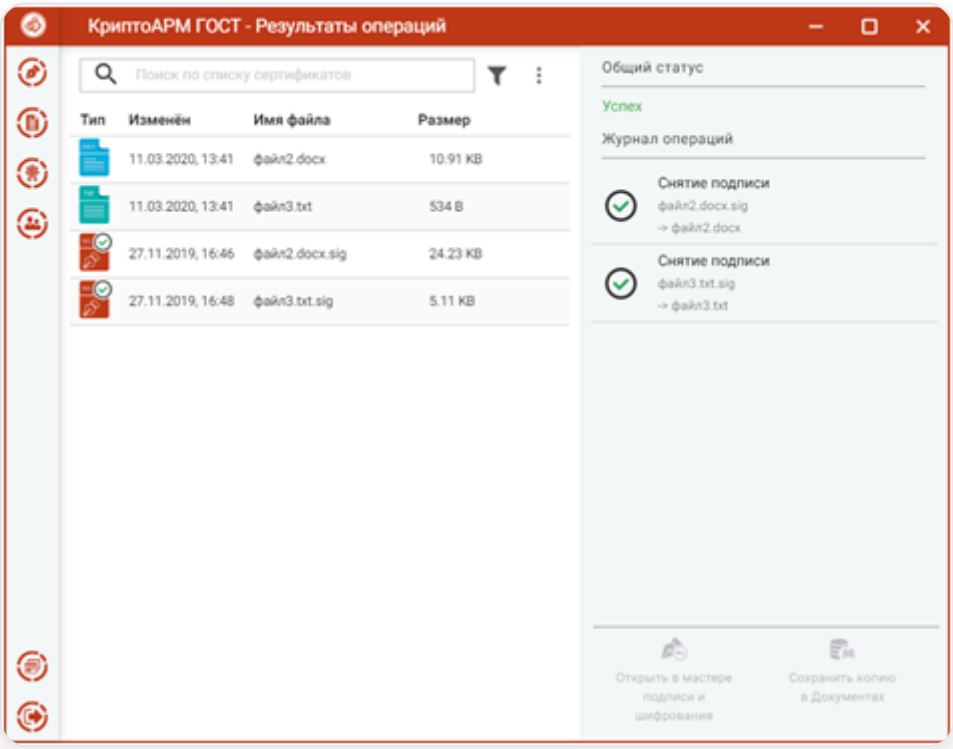
Снятие электронной подписи

Архив. КриптоАРМ ГОСТ.

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



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



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

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

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

У отделенной подписи при выполнении операции снятия подписи возникает сообщение об ошибке, в окне **Результаты операций** отображаются только подписанные файлы.

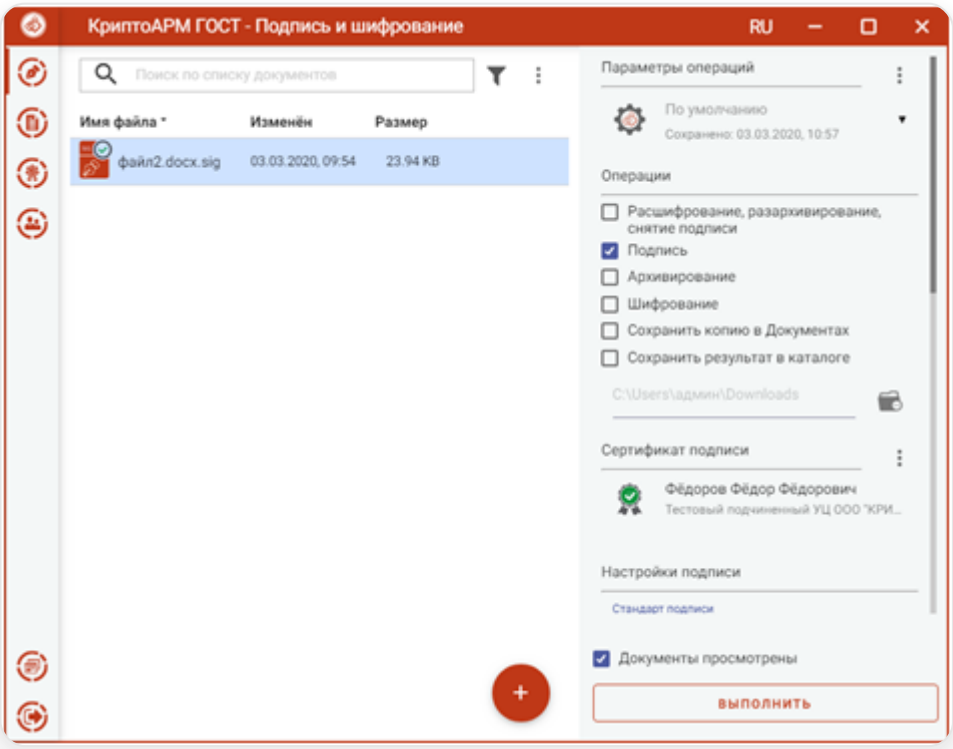
Открыть статью на сайте

Добавление подписи

Архив. КриптоАРМ ГОСТ.

Приложение КриптоАРМ ГОСТ позволяет добавлять электронные подписи к уже подписанному файлу.

Для добавления подписи нужно выбрать файлы, содержащие электронную подпись (файлы с расширением **.sig**), установить опцию **Подпись**, задать сертификат подписи, и установить флаг, что документы просмотрены перед подписанием.



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

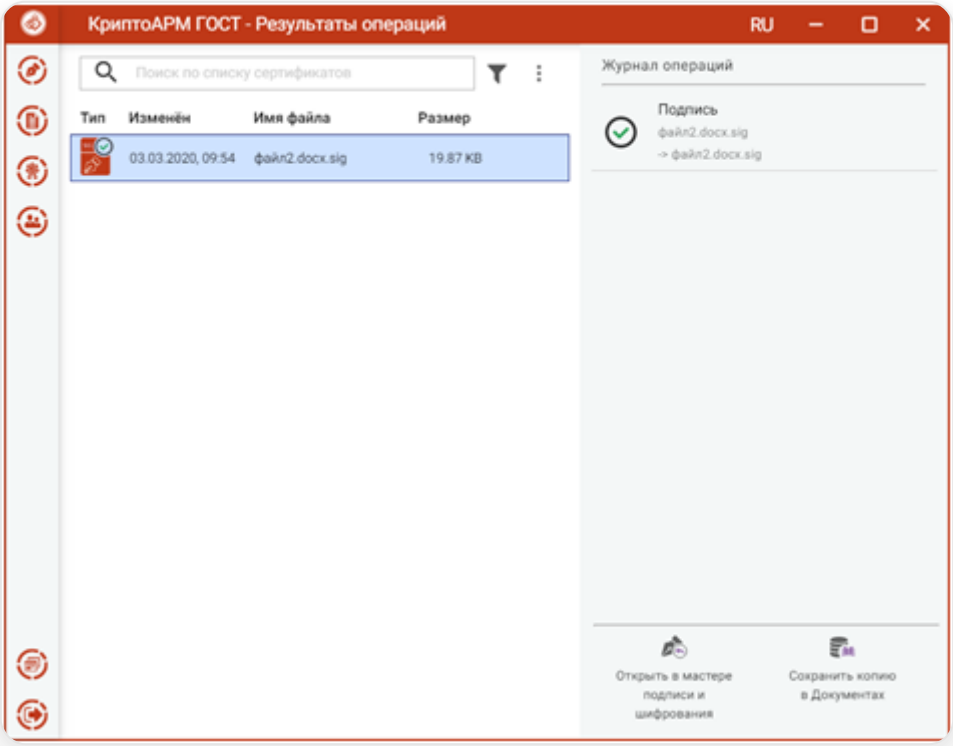
Тип подписи и использование штампов времени можно настроить.

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

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

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

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



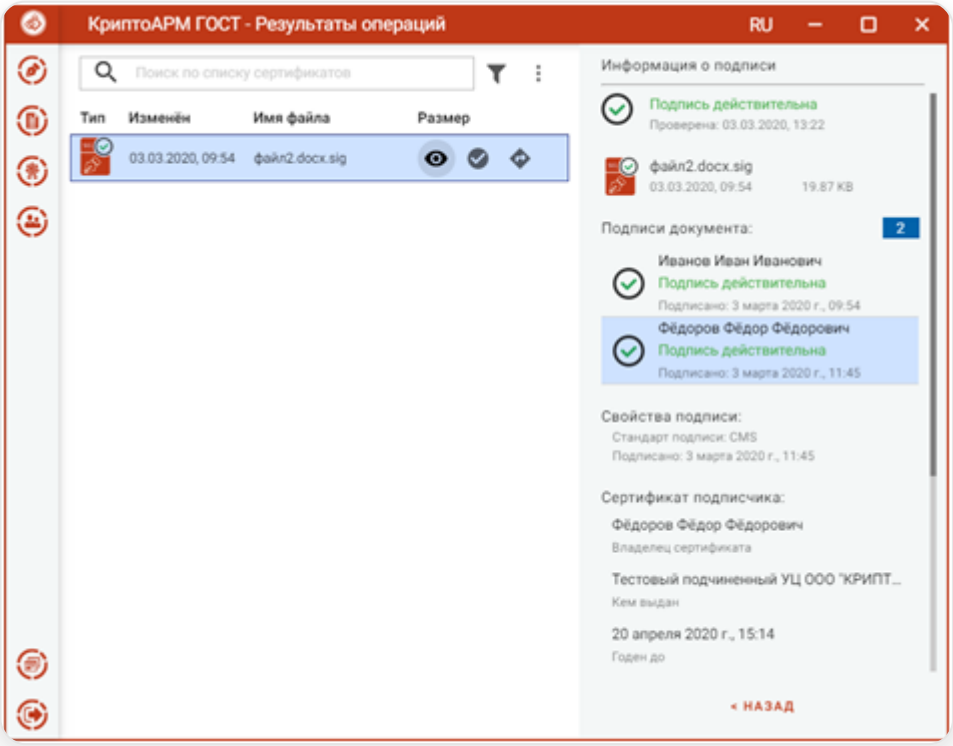
Подписанные файлы сохраняются в заданном каталоге, если в операциях был выбран каталог для сохранения результатов, или в каталоге расположения исходного файла, если в операциях не был установлен флаг **Сохранить результат в каталоге**. Если в операциях был установлен флаг **Сохранить копию в Документах**, то копия полученного после операции файла сохраняется в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Документы из данного каталога доступны в пункте меню **Документы**.

Для подписанного документа доступны операции:

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

При выделении подписного файла открывается информация о подписи, содержащая сведения о всех подписях. Чтобы посмотреть информацию о конкретном подписчике, нужно выбрать

подписчика из списка.



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

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

Открыть статью на сайте

Как зашифровать файлы с помощью КриптоАРМ ГОСТ

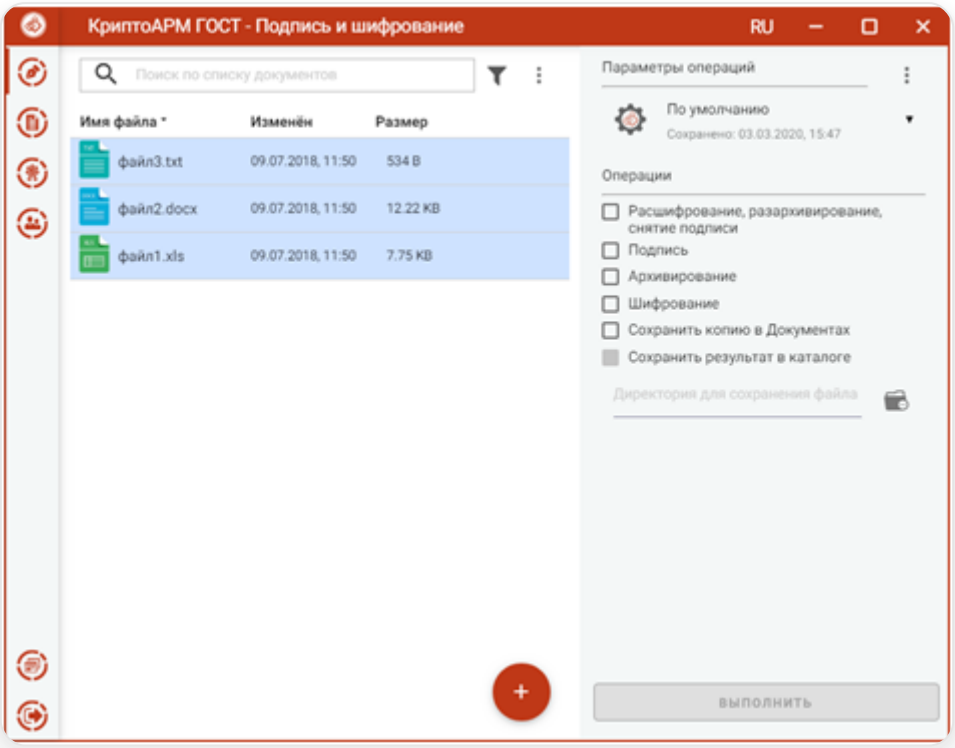
Архив. КриптоАРМ ГОСТ.

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

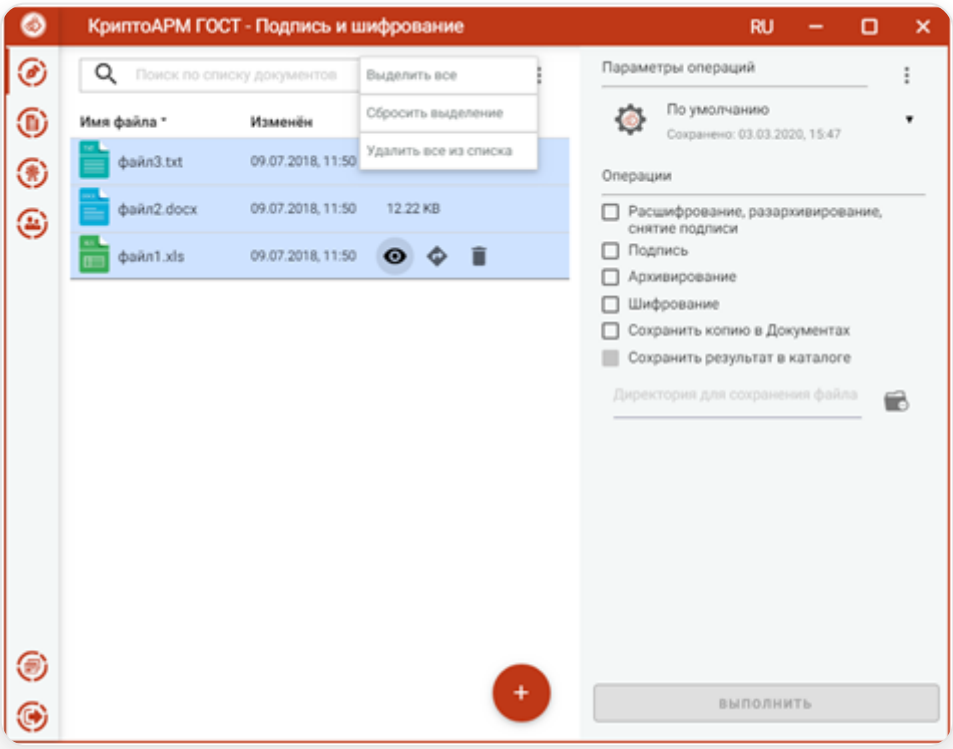
1. Выбор файлов для шифрования.

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

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

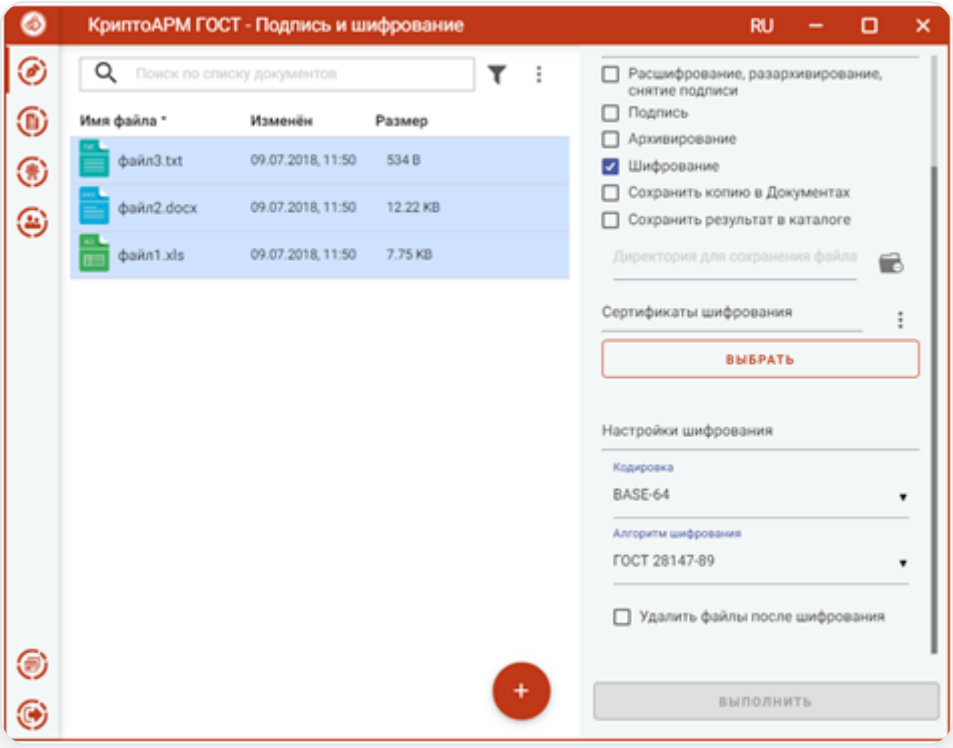


Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла.



2.Настройка параметров шифрования.

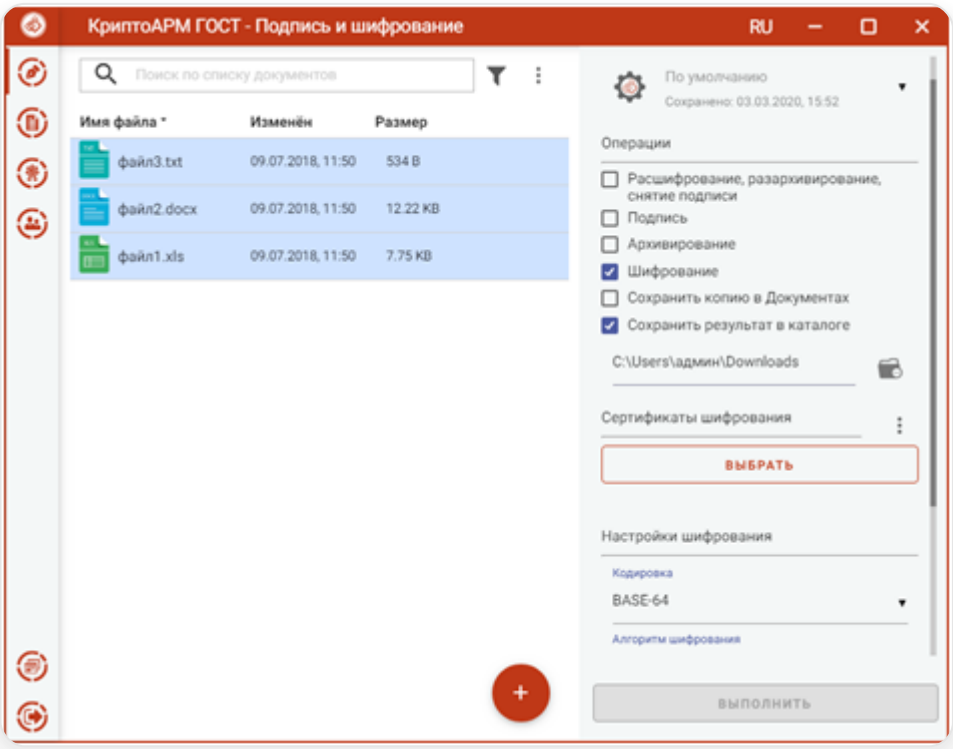
Для доступа к настройке параметров шифрования в разделе Операции необходимо выбрать опцию **Шифрование**.



В параметрах можно настроить:

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

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

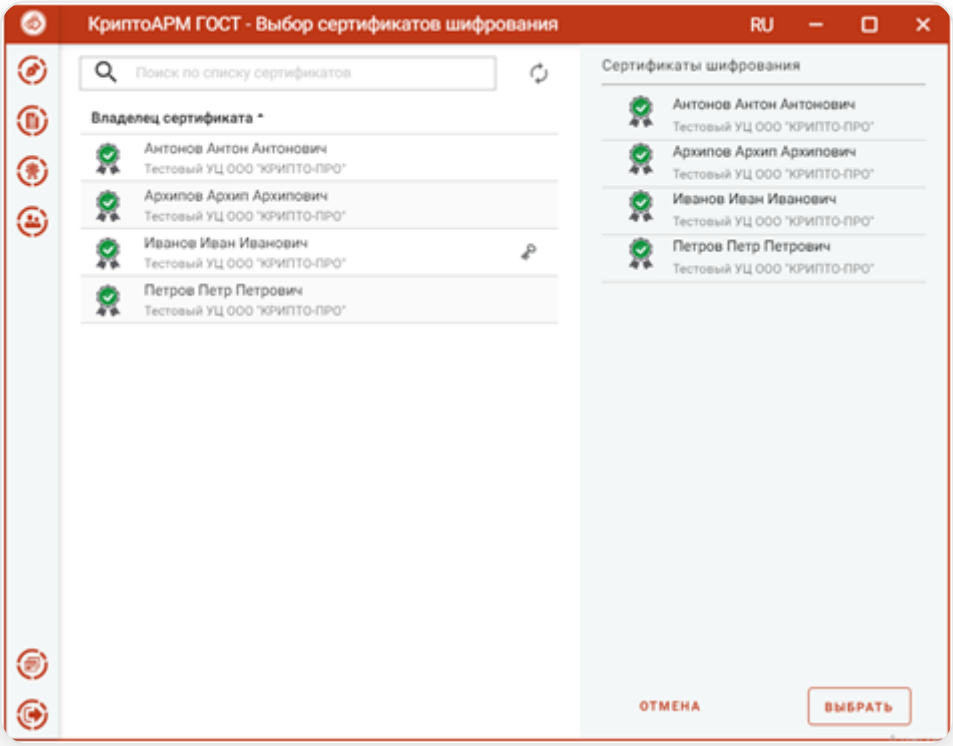


Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Документы из данного каталога доступны в пункте меню **Документы**.

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

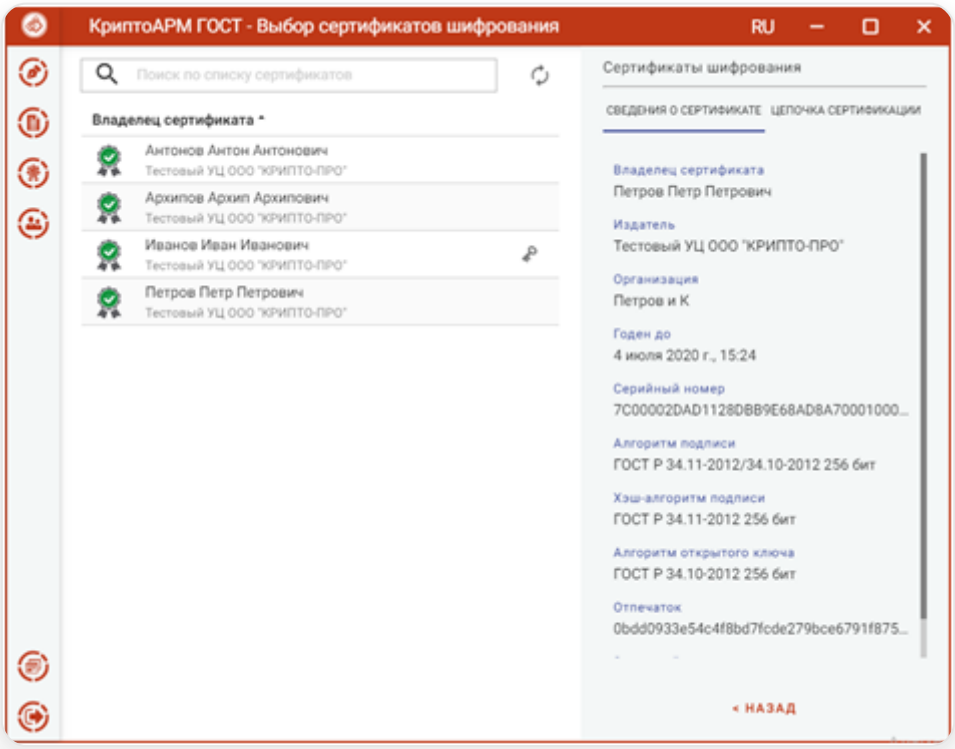
3. Выбор сертификатов шифрования.

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



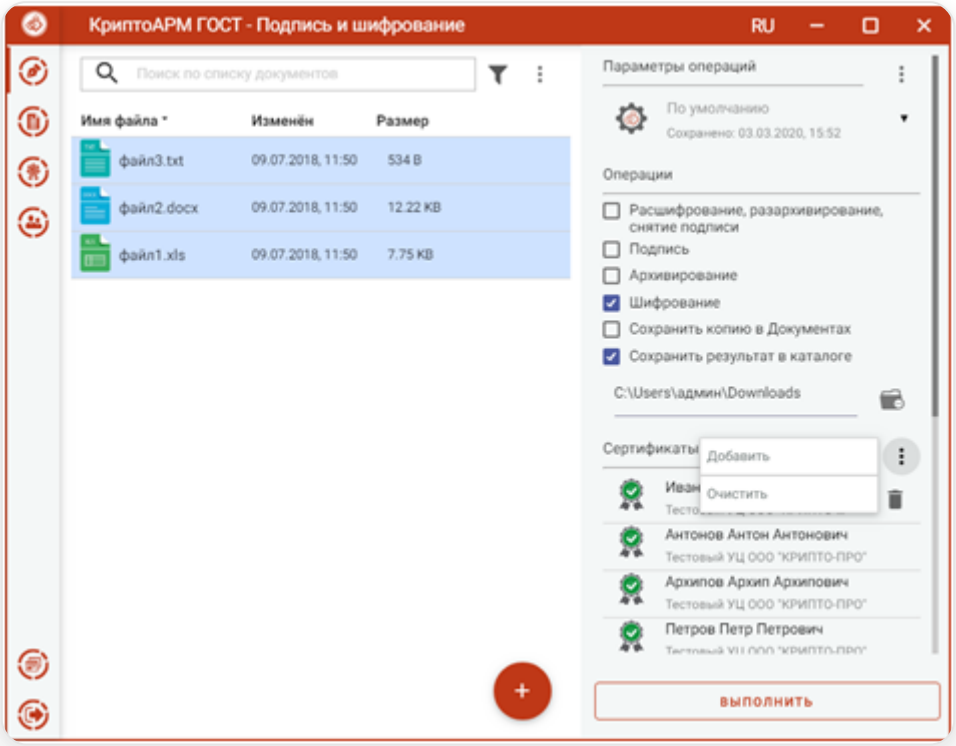
В списке сертификатов допускается выбор нескольких сертификатов, так как число получателей может быть различным.

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



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

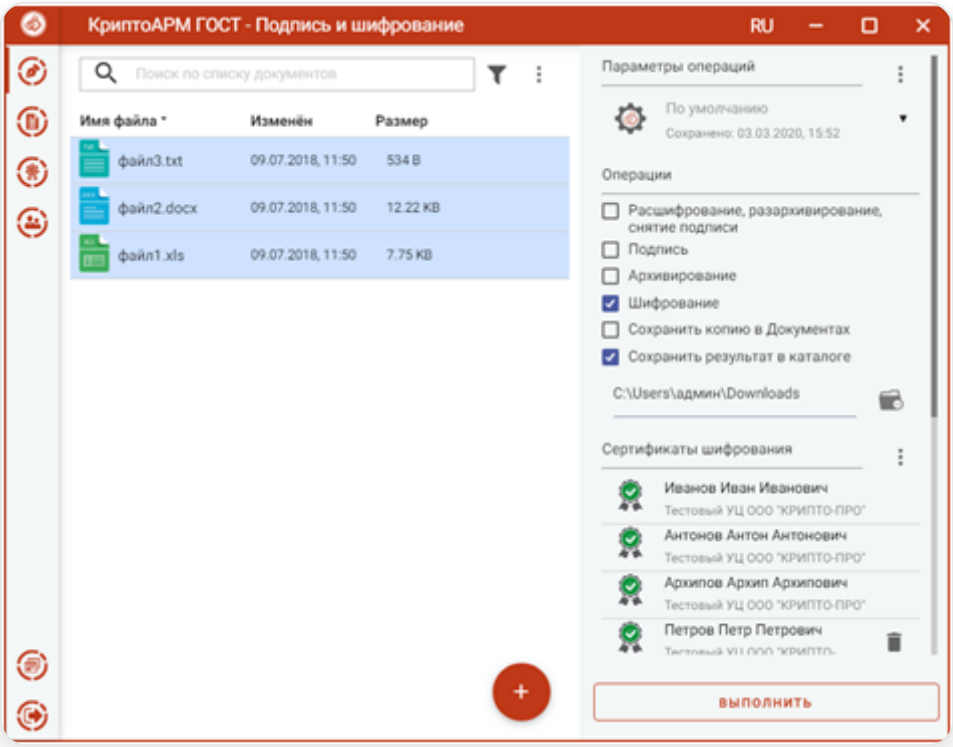
Изменить список сертификатов шифрования можно с помощью контекстного меню. Удалить сертификаты из сформированного списка можно кнопкой **Удалить**.



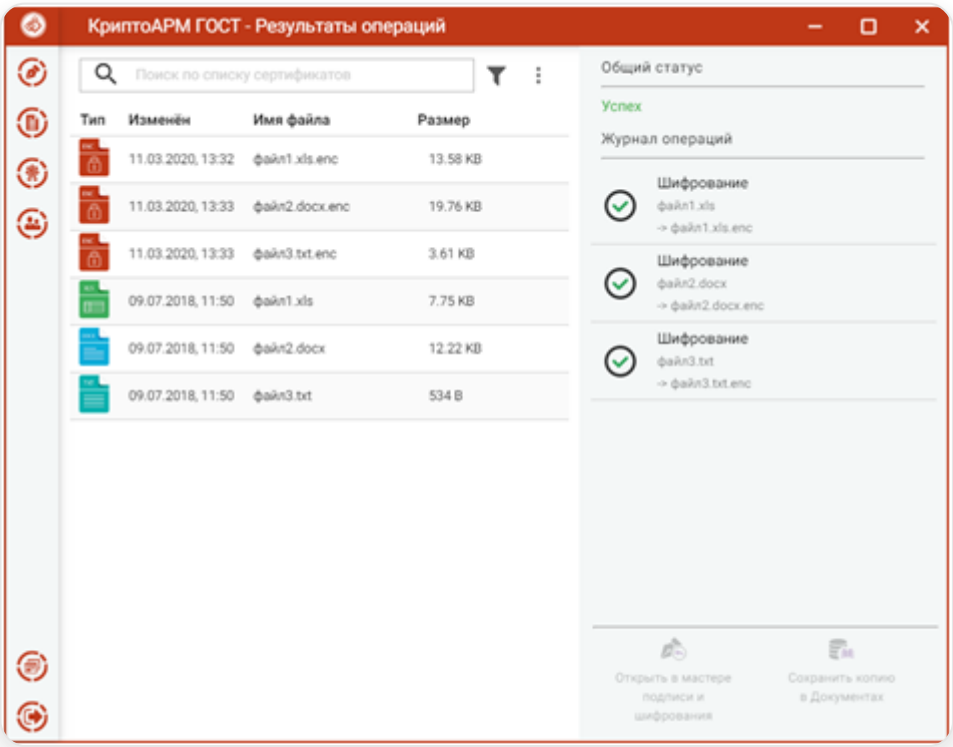
Если список сертификатов других пользователей пуст, то можно создать или импортировать сертификат на вкладке **Контакты**.

4. Шифрование файлов.

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



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



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

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

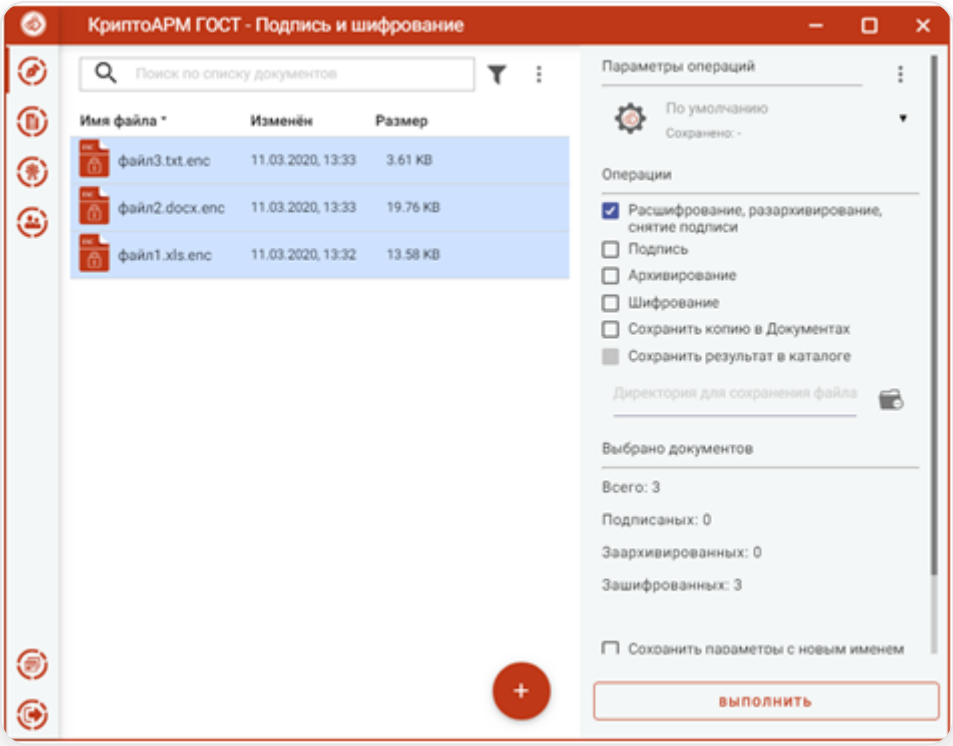
После выполнения операции мастер подписи и шифрования очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения. Результаты последней операции доступны в меню **Подпись и шифрование - Результаты операции**.

Открыть статью на сайте

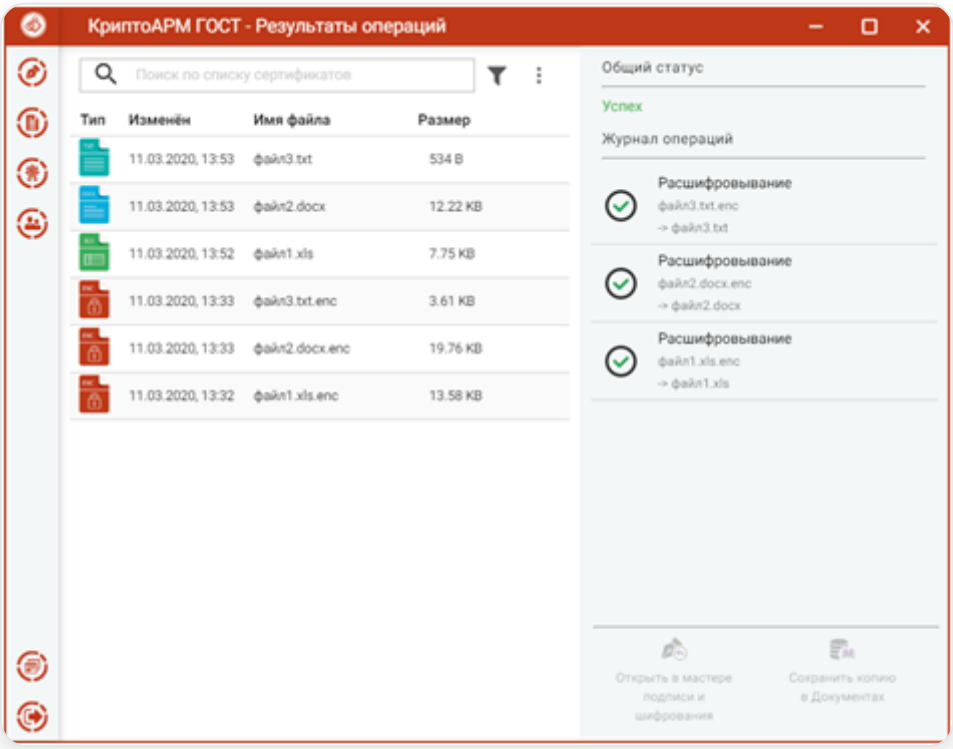
Как расшифровать файлы с помощью КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ.

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



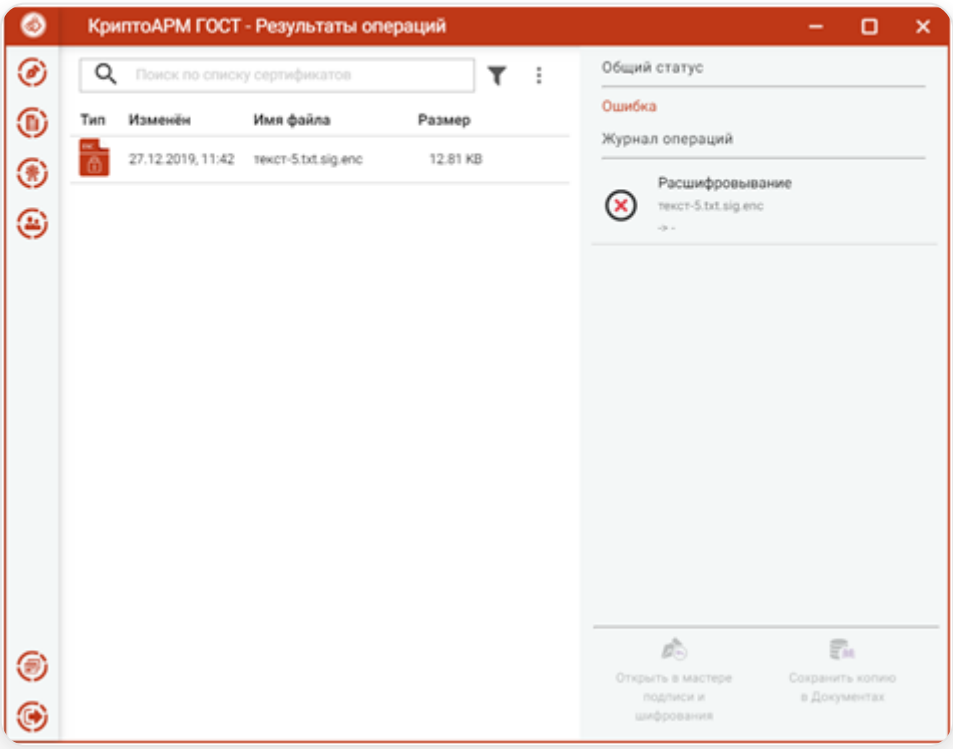
Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций**.



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

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

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


КриптоАРМ ГОСТ - Результаты операций
Поиск по списку сертификатов
Тип
Изменён
Имя файла
Размер
27.12.2019, 11:42
текст-5.txt.sig.enc
12.81 KB
Общий статус
Ошибка
Журнал операций
Расшифровывание
текст-5.txt.sig.enc
-> -
Открыть в мастере подписи и шифрования
Сохранить копию в Документах

Открыть статью на сайте

Создание подписи со штампом времени (TSP)

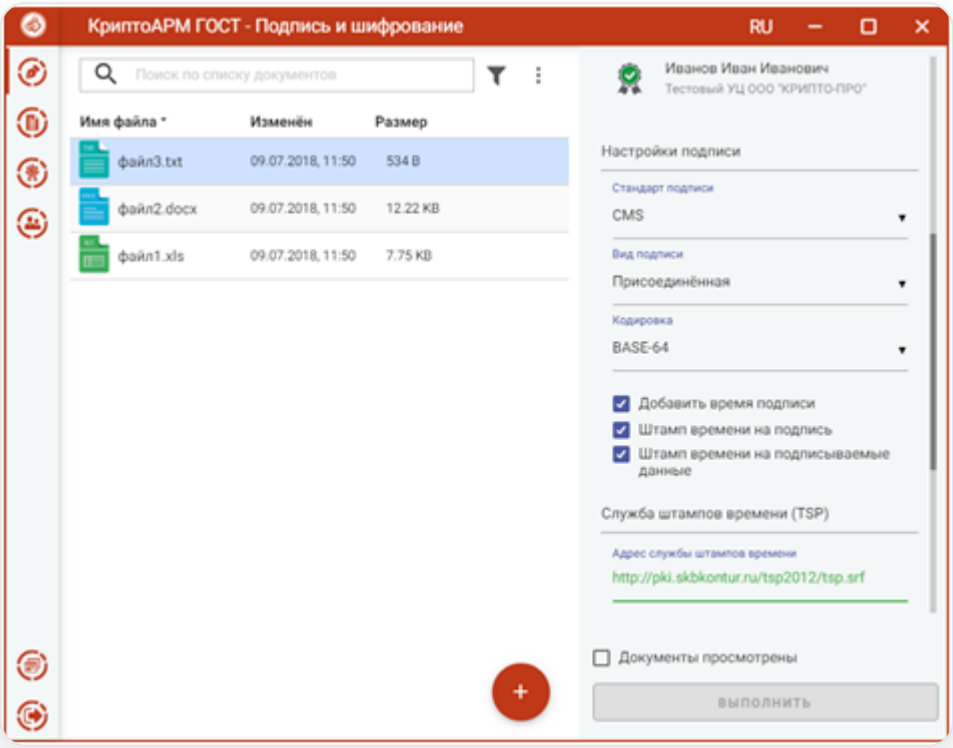
Архив. КриптоАРМ ГОСТ.

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(КриптоПро TSP Client.).

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

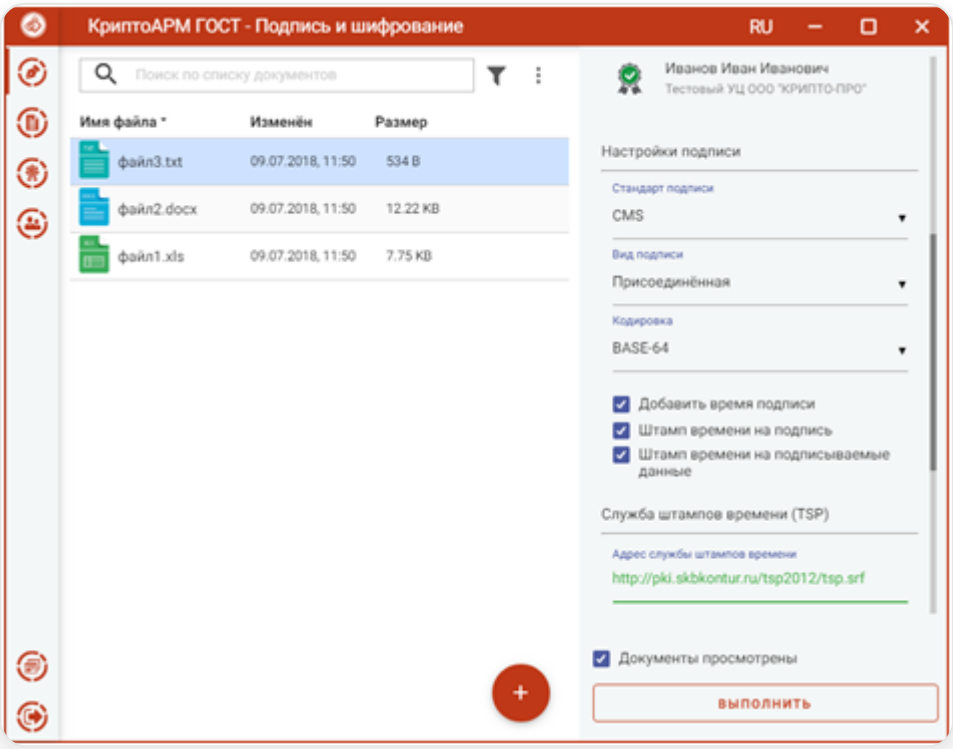
- установить флаг **Добавлять штамп времени на подпись**, если требуется поставить штамп на подпись;
- установить флаг **Добавлять штамп времени на подписываемые данные**, если требуется поставить штамп на данные;



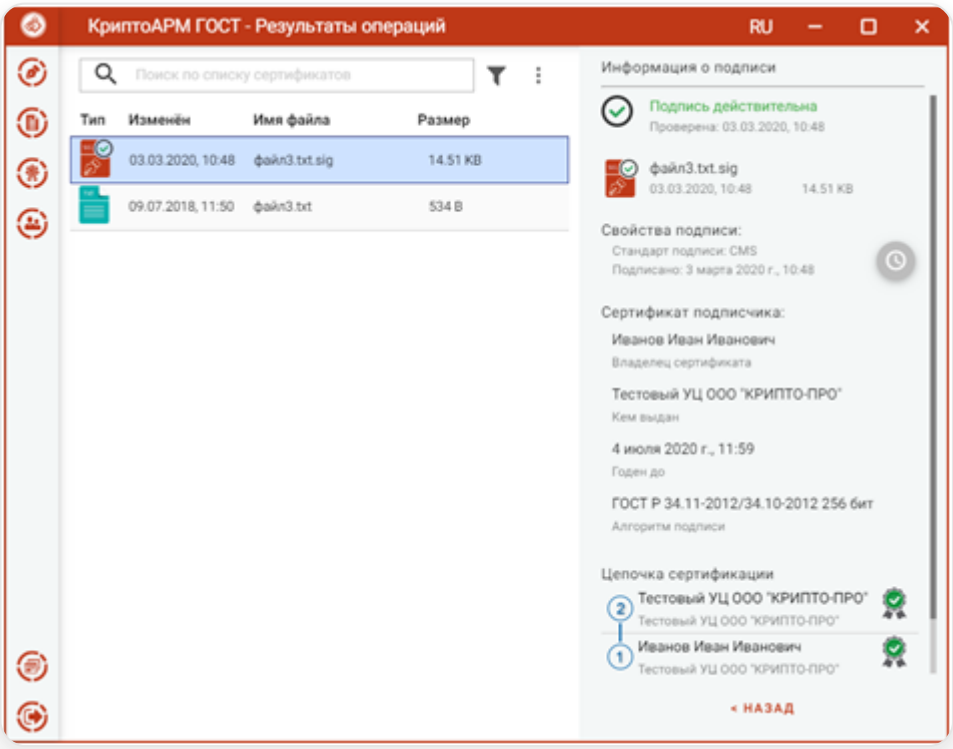
При установленном флаге добавления штампа времени на подпись или на данные необходимо заполнить параметры раздела **Служба штампов времени** (TSP):

- **Адрес службы штампов времени** - адрес службы штампов времени можно узнать у поставщика сертификата. 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.

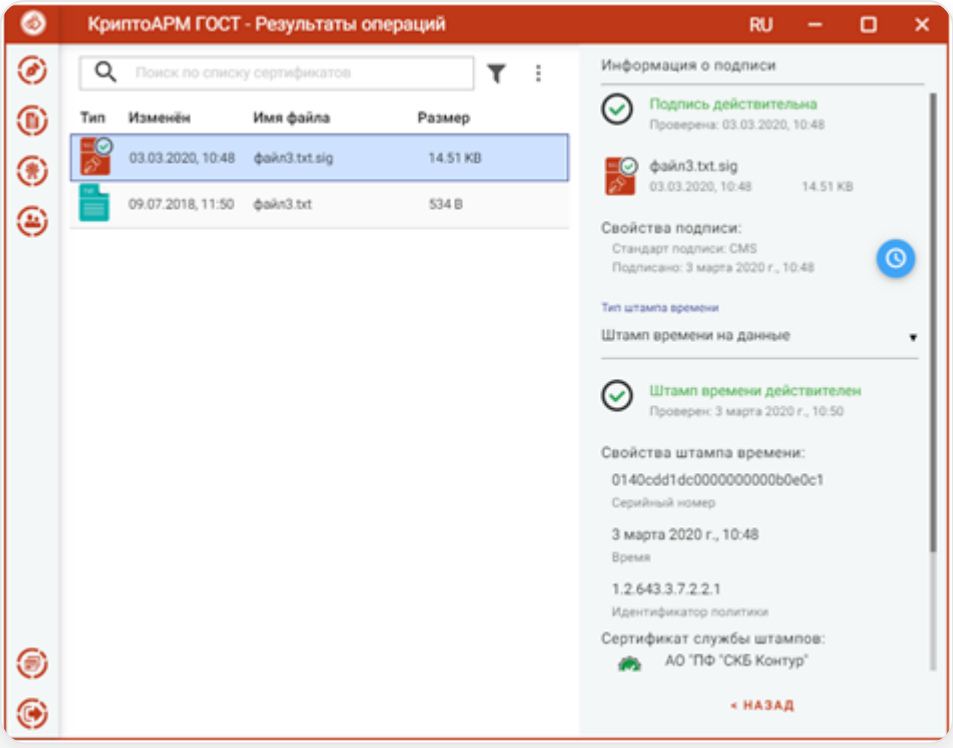
После заполнения параметров подписи и установки флага, что файлы просмотрены перед их подписанием, становится доступна кнопка **Выполнить**.



Нажатие на кнопку **Выполнить** запускает процесс подписи. Исходные документы (оригиналы) и результаты операции подписи отображаются в отдельном мастере **Результаты операций**. Причем, после выполнения операции мастер подписи и шифрования очищается от добавленных в него файлов.



При просмотре информации о подписи отображается информация о штампе времени.



Открыть статью на сайте

Создание усовершенствованной подписи

Архив. КриптоАРМ ГОСТ.

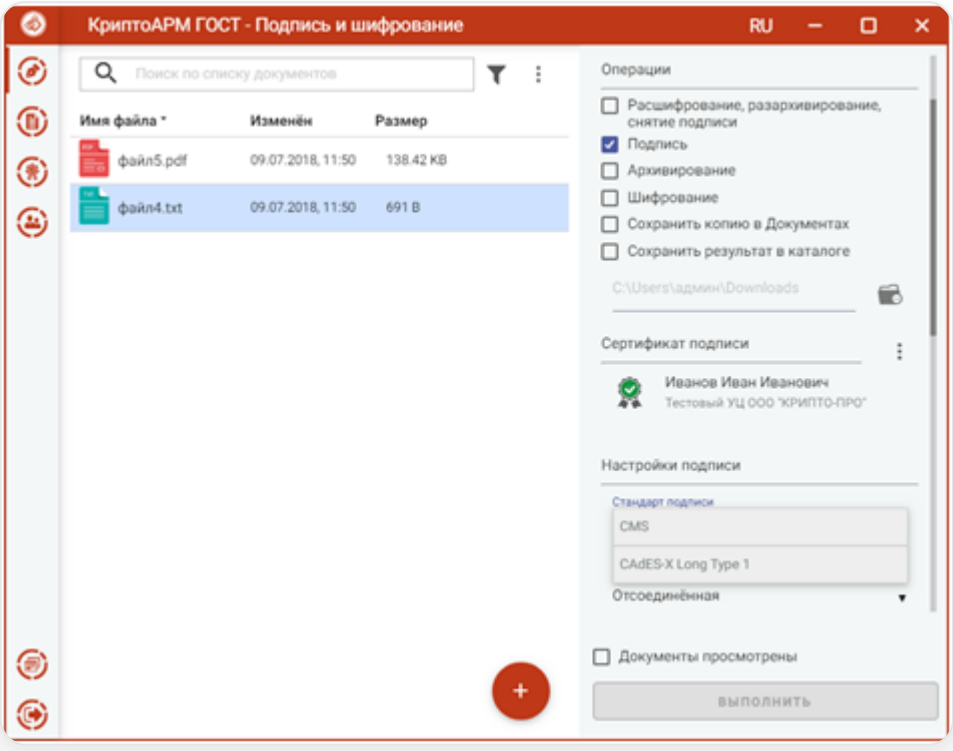
Усовершенствованная квалифицированная электронная подпись поможет доказать юридическую значимость документа в спорных ситуациях. Например, когда помимо авторства и целостности документа (которые дает обычная КЭП) необходимо подтвердить, что сертификат был действителен в момент подписания документа.

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).

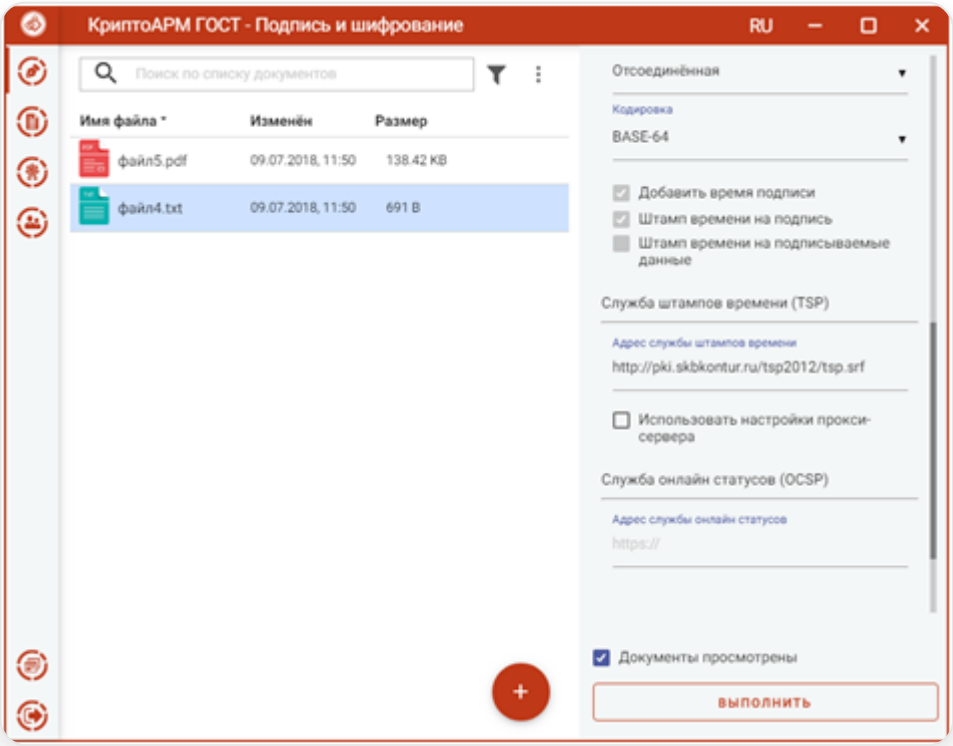
Создание усовершенствованной подписи возможно только при установленных модулях TSP Client и OCSP Client и лицензий на них (КриптоПро TSP Client. и КриптоПро OCSP Client).

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

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



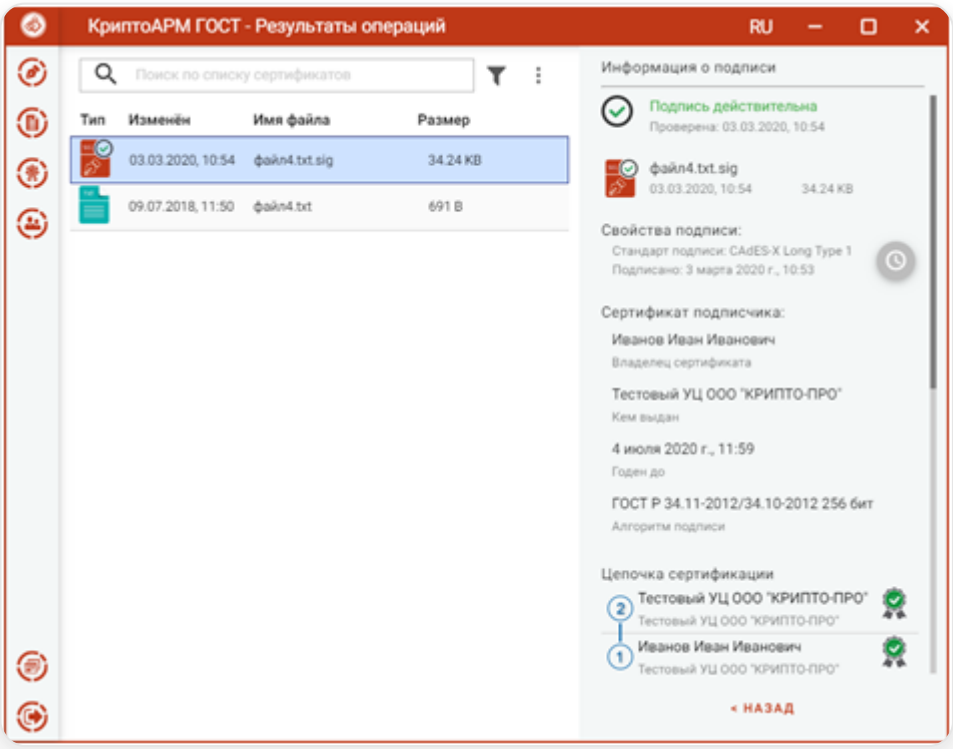
- Заполнить параметры раздела **Служба штампов времени (TSP)**: **Адрес службы штампов времени, Использовать настройки прокси-сервера** (если при подключении к службе TSP используется прокси-сервер)



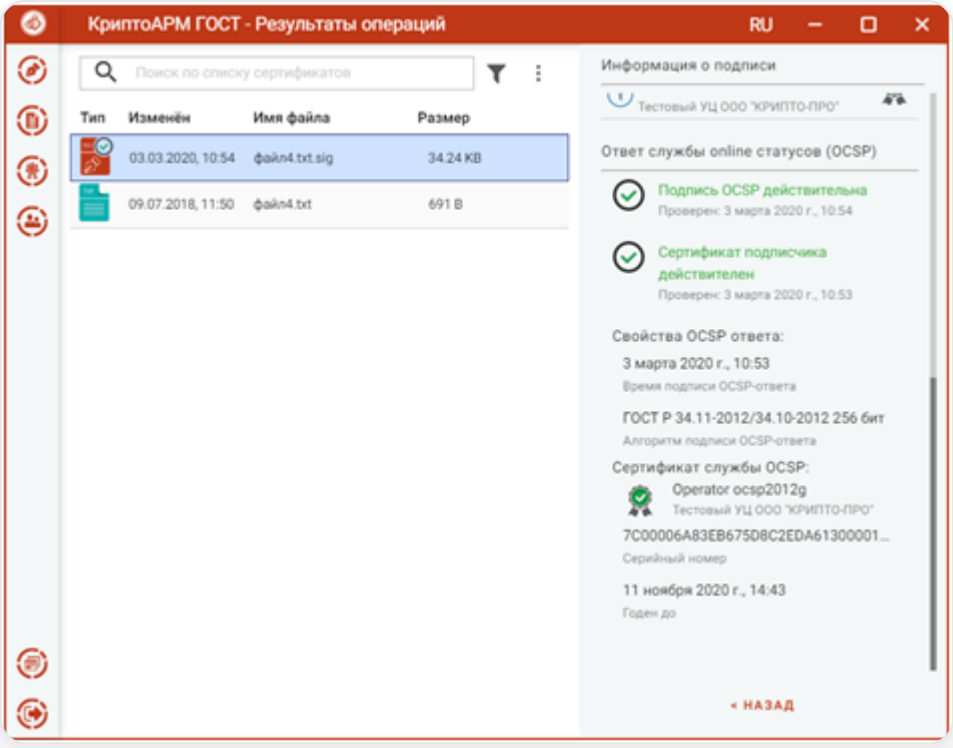
- Заполнить параметры раздела **Службы online статусов** (OCSP): **Адрес службы online статусов** - необязательный параметр, задается, если в сертификате данное поле не заполнено.

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

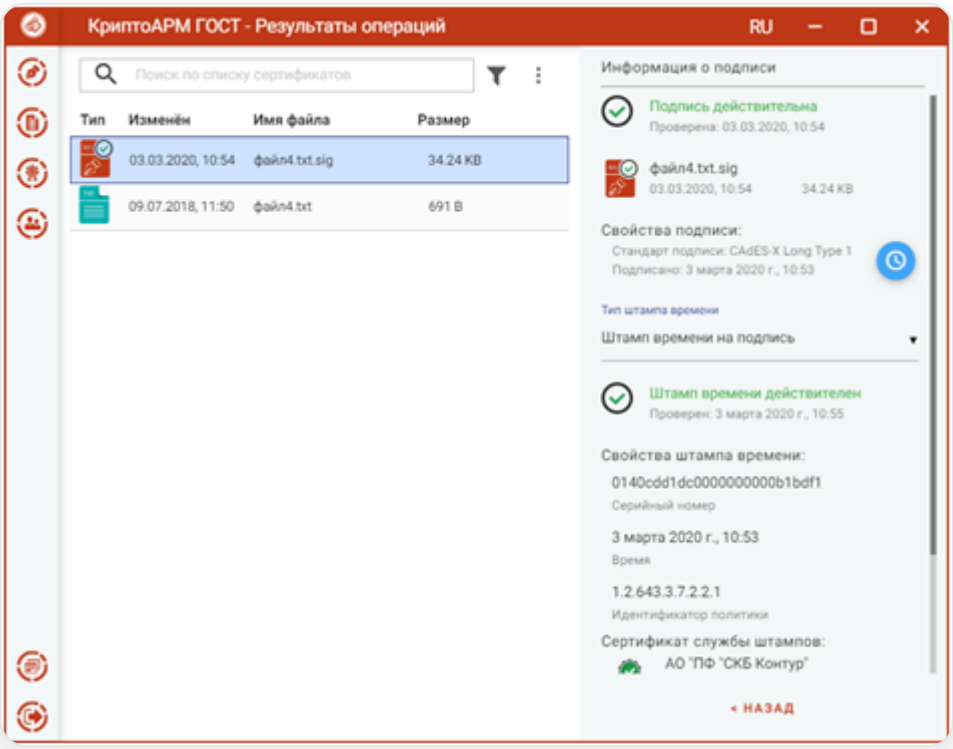
Нажатие на кнопку **Выполнить** запускает процесс подписи. Исходные документы (оригиналы) и результаты операции подписи отображаются в отдельном мастере **Результаты операций**.



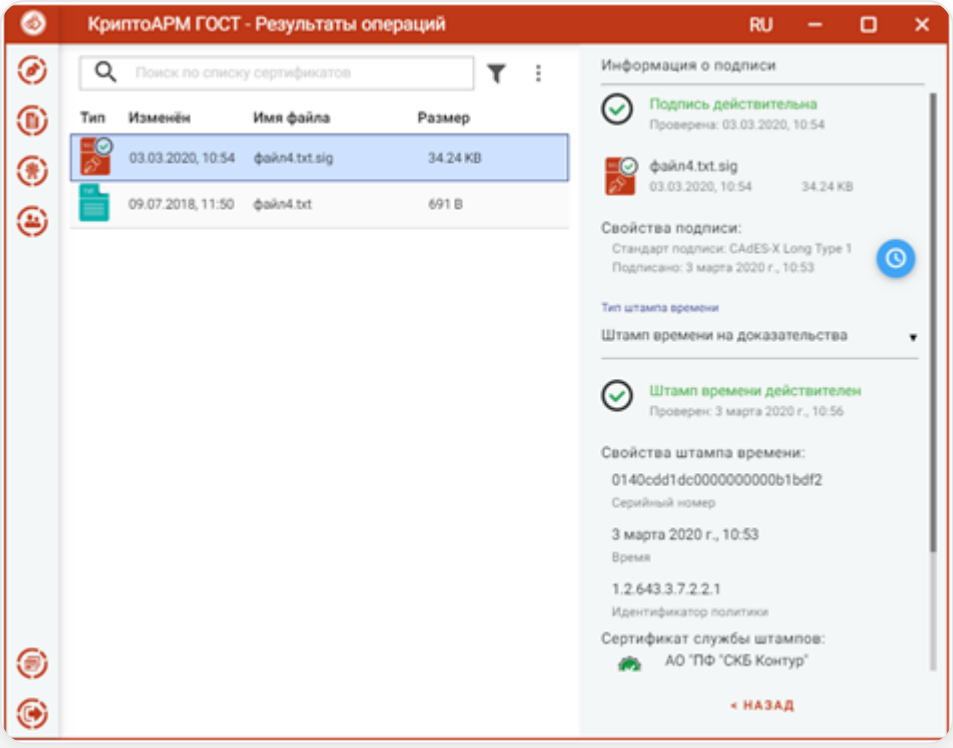
При просмотре информации о подписи отображается информация о OCSP ответе.



Информация о штампе времени на подпись.



И информация о доказательствах подлинности.



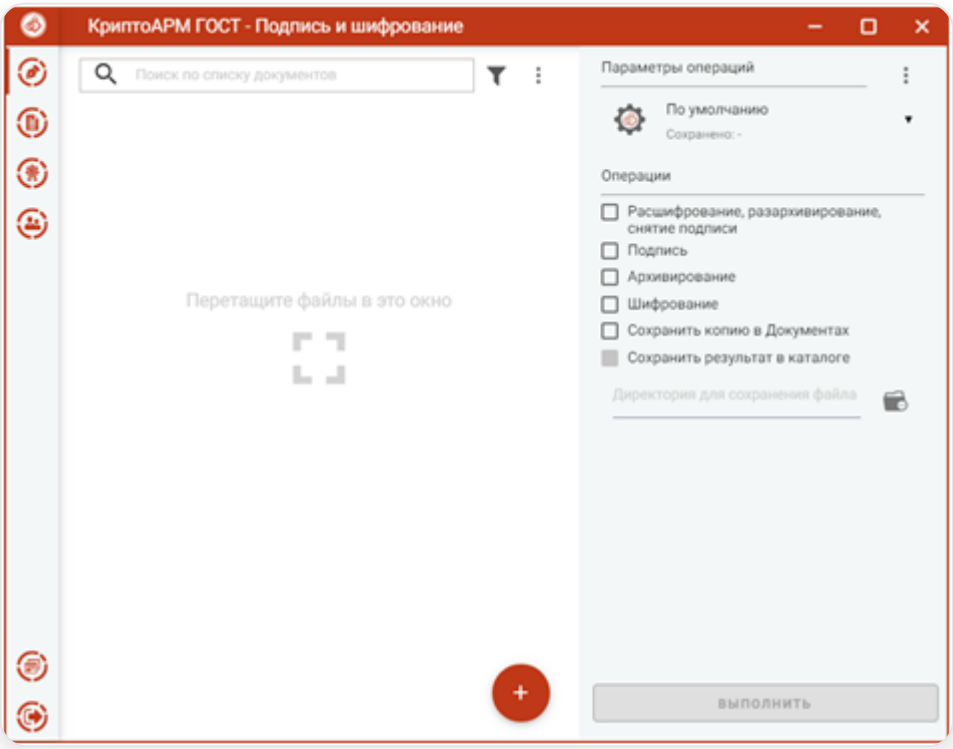
Открыть статью на сайте

Управление параметрами операций

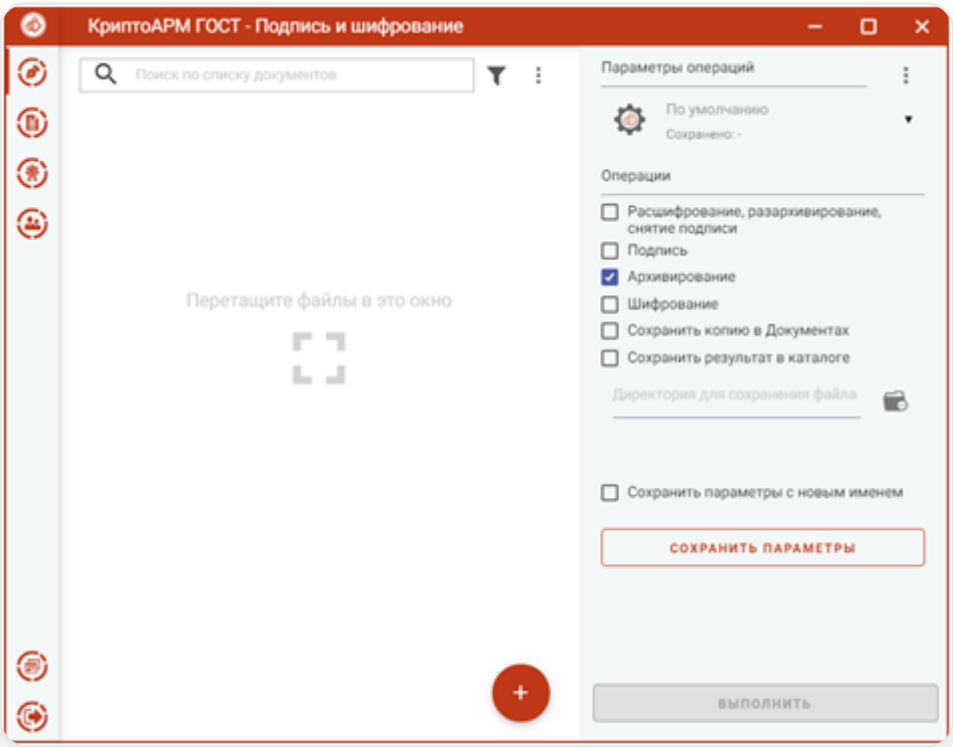
Архив. КриптоАРМ ГОСТ.

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

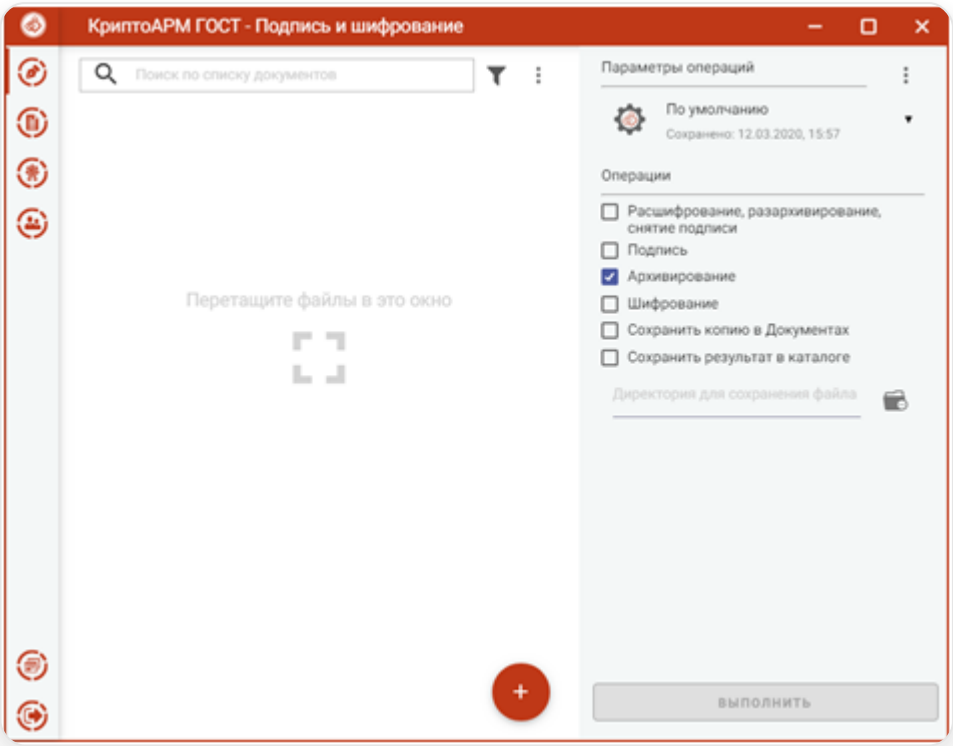
При первом запуске приложения создаются параметры «По умолчанию» с пустыми опциями операций и параметров операций.



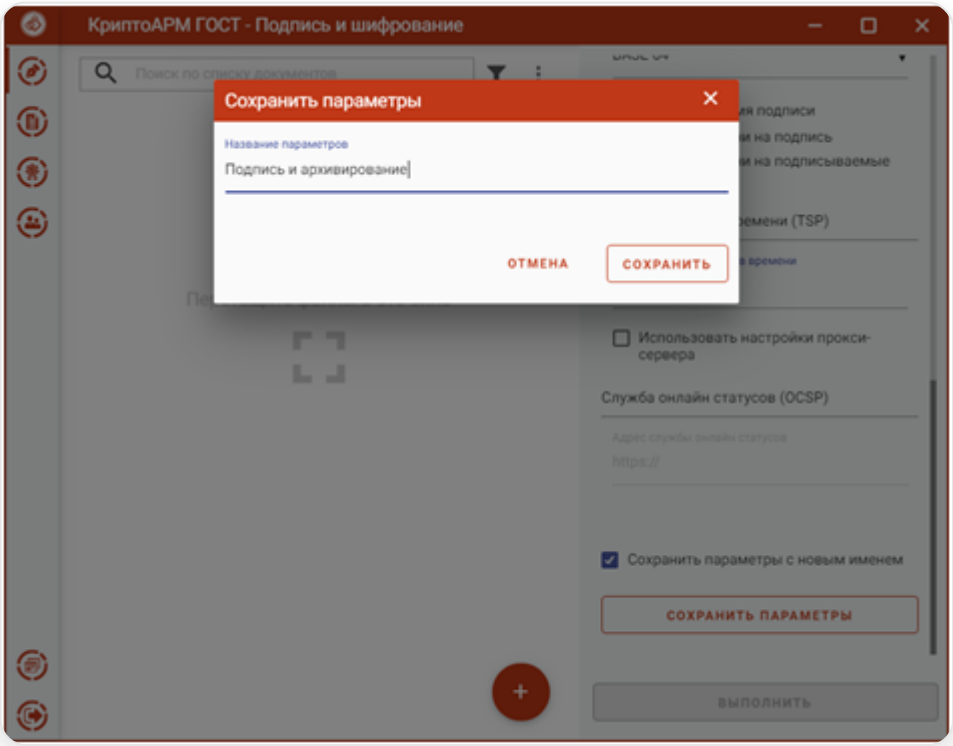
При любом изменении опции операций или параметров операции становится доступна кнопка сохранения изменений **Сохранить параметры**.



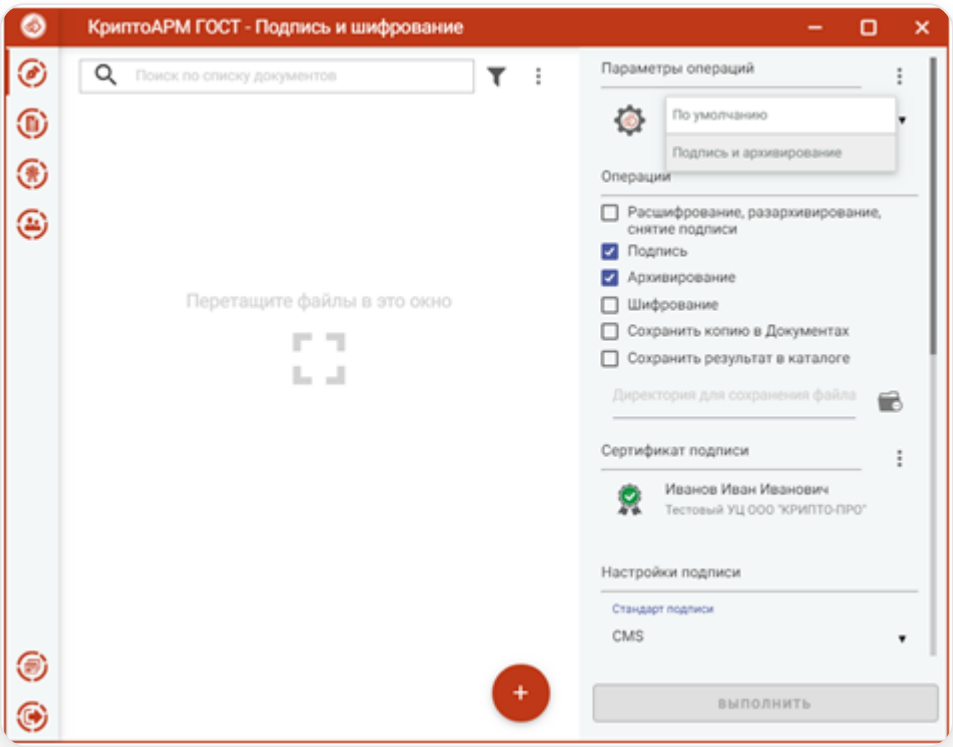
При нажатии на кнопку происходит сохранение выбранных параметров в текущие параметры операций. Кнопка **Сохранить параметры** скрывается до изменений.



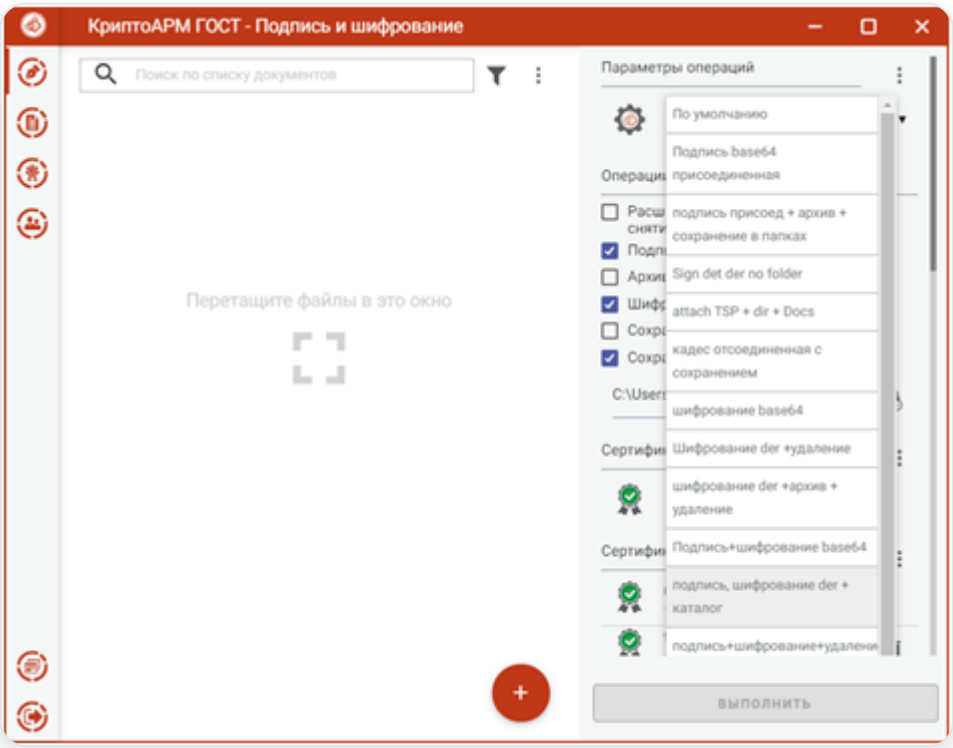
Если выбрать опцию **Сохранить параметры с новым именем** и нажать кнопку **Сохранить параметры**, то открывается окно ввода названия параметров операций.



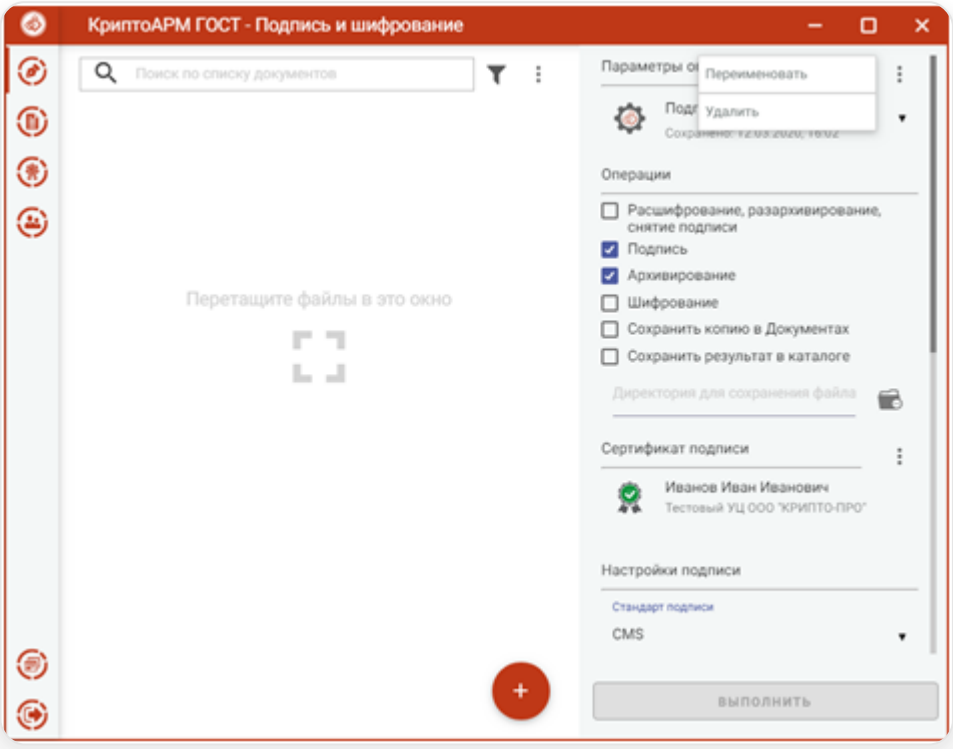
По кнопке **Сохранить** происходит сохранение выбранных параметров в параметры операций с заданным именем. Выбрать параметры операций можно в выпадающем списке из ранее сохраненных параметров.



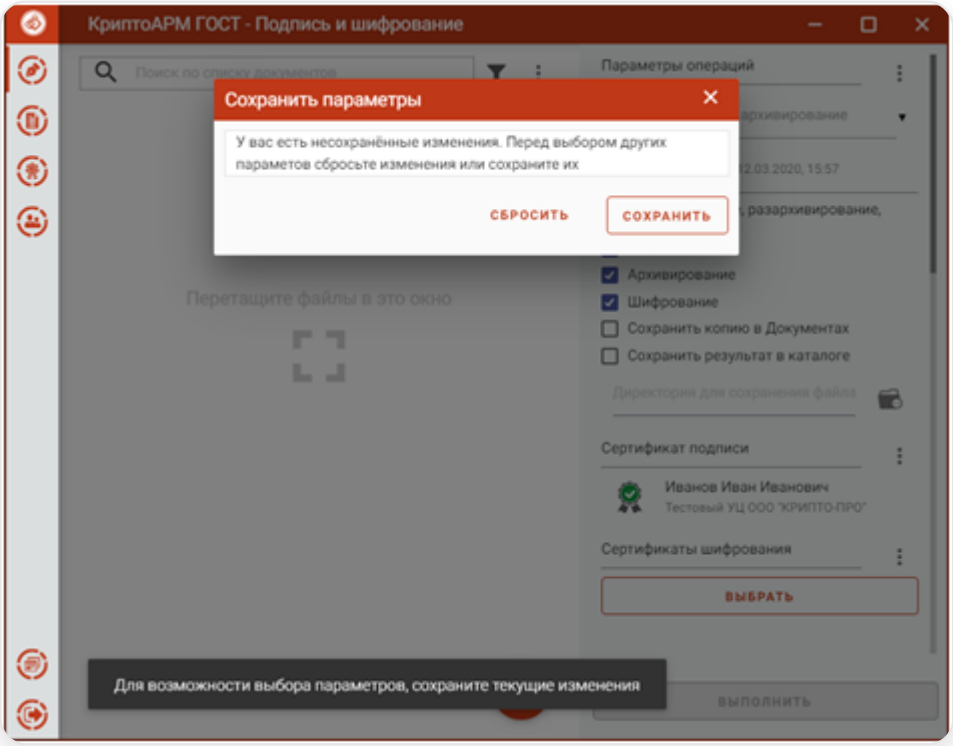
Можно настроить несколько параметров операций и выбирать нужные из списка.



Параметры операций можно переименовать или удалить через контекстное меню Параметров операций.



Если в параметрах операций были сделаны изменения и не сохранены, то при попытке выбрать другие параметры из выпадающего списка или при закрытии приложения появляется окно с предложением сохранить сделанные изменения, сбросить изменения или закрыть без сохранения.

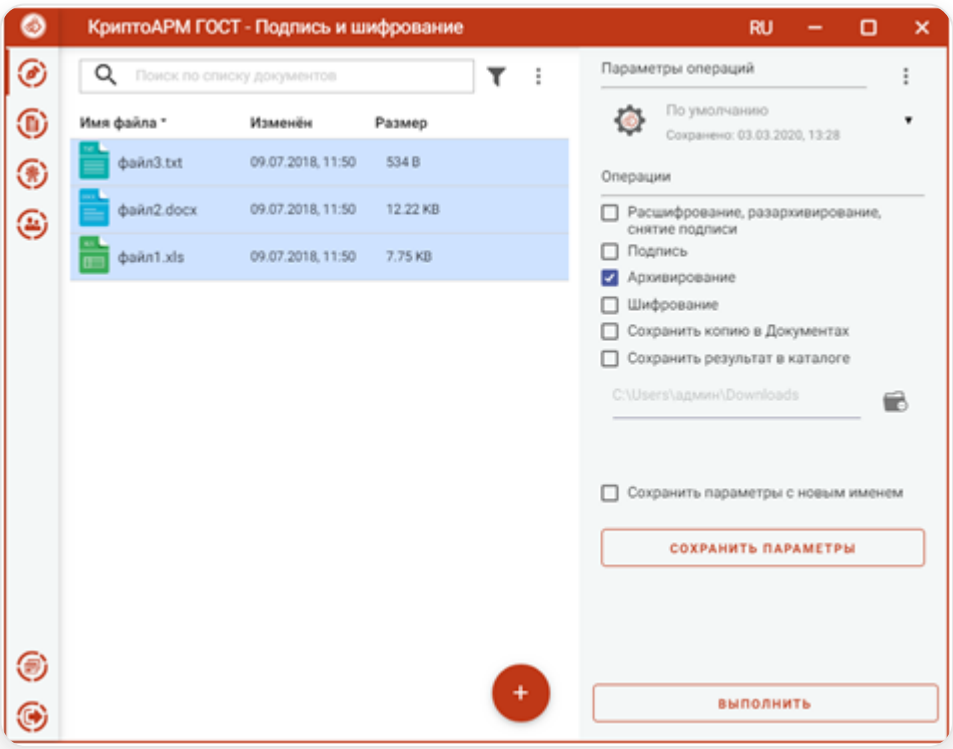


Открыть статью на сайте

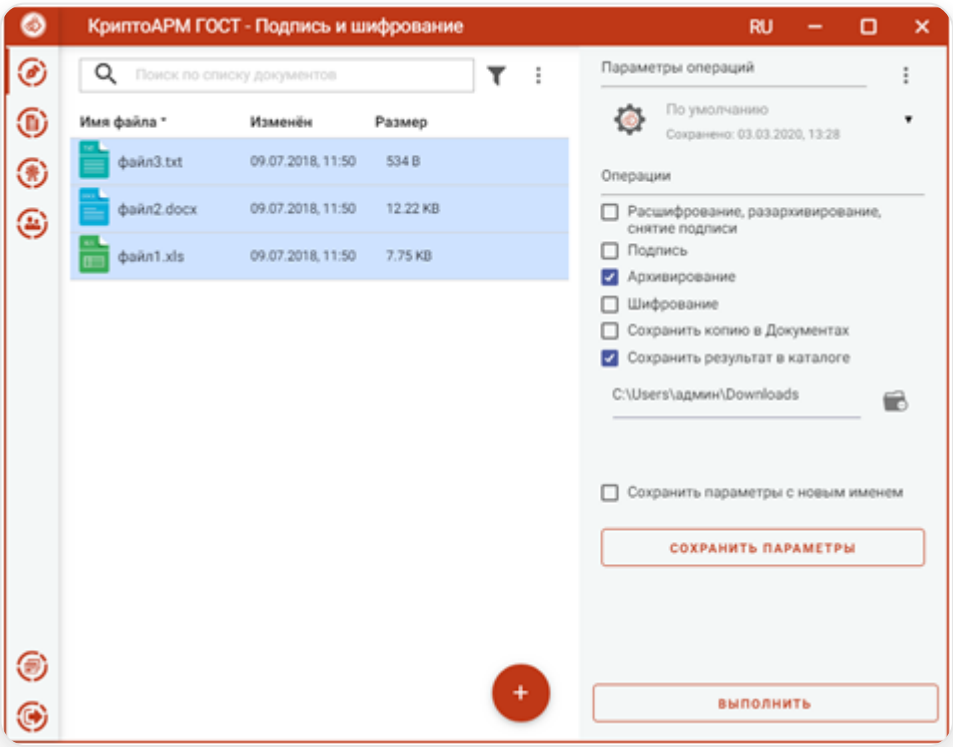
Архивирование файлов

Архив. КриптоАРМ ГОСТ.

Для архивирования файлов нужно выбрать файлы и опцию **Архивирование**.



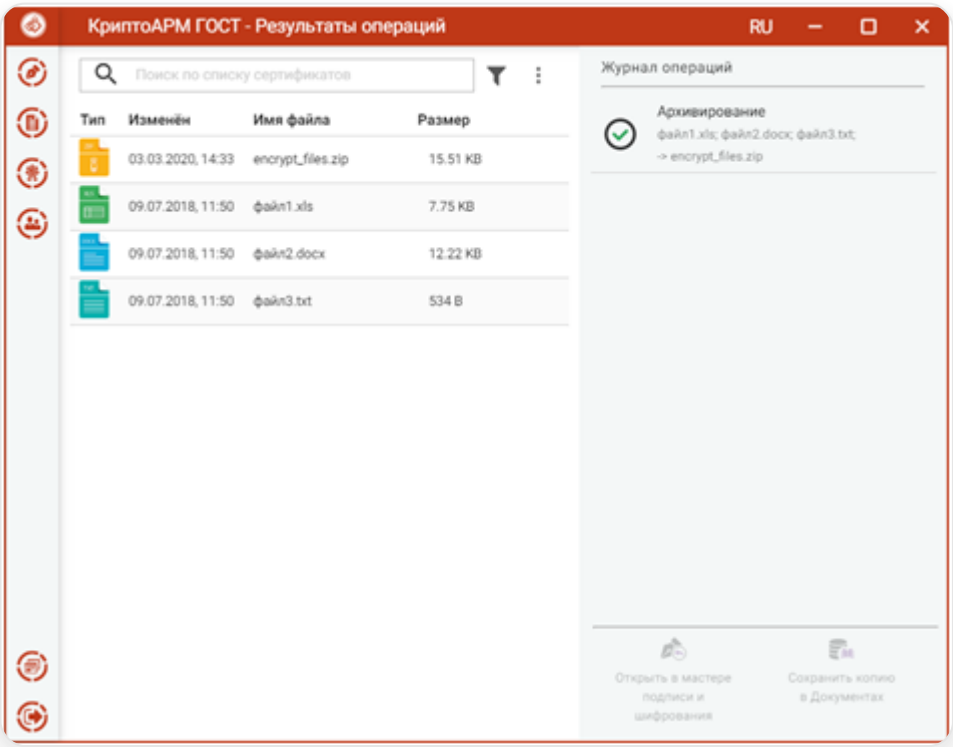
Можно задать каталог для сохранения архива документов, выбрав в операциях опцию **Сохранить результат в каталоге**. При установке флага становится доступно поле выбора каталога.



Если флаг не установлен, то полученный архив сохраняется во временную папку TEMP, расположенную в каталоге пользователя в папке ./Trusted/CryptoARM GOST/.

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге ./Trusted/CryptoARM GOST/. Документы из данного каталога доступны в пункте меню **Документы**.
Выбранные параметры архивирования можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте Управление параметрами операции.

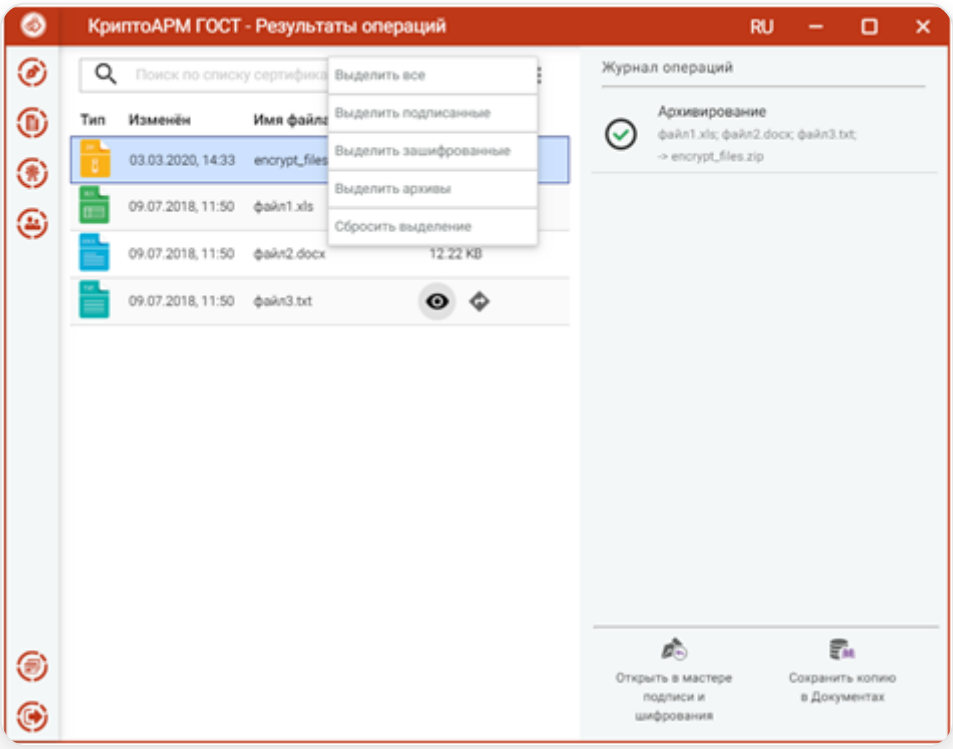
При нажатии на кнопку **Выполнить** происходит архивирование выбранных файлов. Исходные файлы и полученный архив отображаются в отдельном мастере **Результаты операций**.



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

Для каждого документа доступны операции:

- **Просмотр** - выполняется открытие файла через приложение, которое ассоциировано с его расширением. Для подписанных файлов открывается оригинал документа.
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл.



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

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

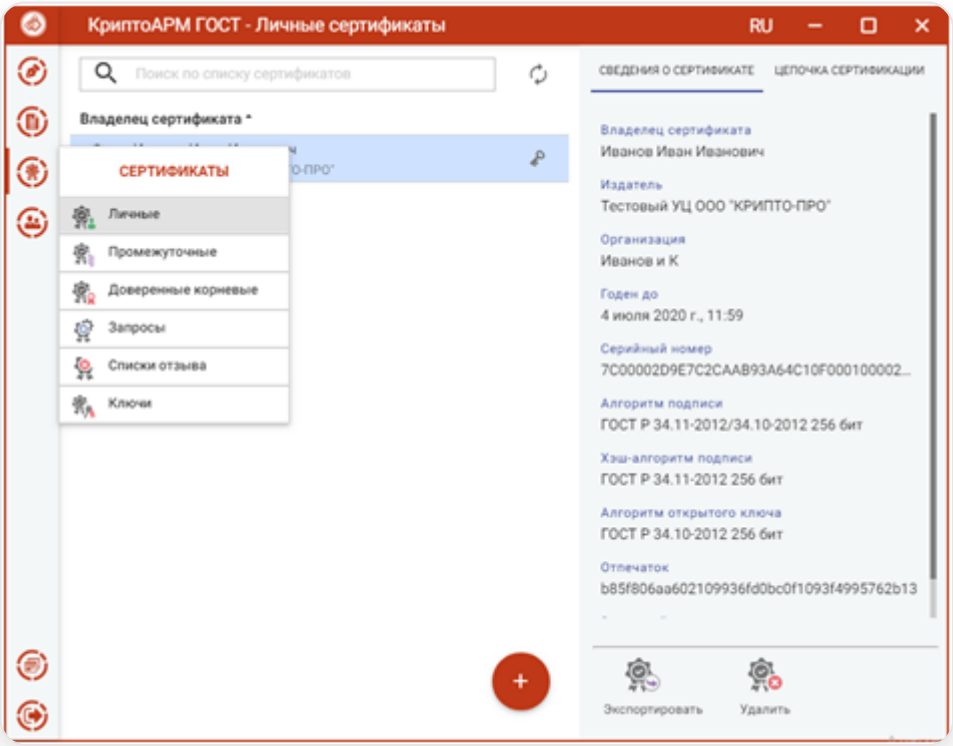
После выполнения операции мастер подписи и шифрования очищается от добавленных в него файлов. Результаты операций сохраняются до выполнения следующей операции или до закрытия приложения. Результаты последней операции доступны в меню **Подпись и шифрование - Результаты операции**.

Открыть статью на сайте

Операции с сертификатами и ключами

Архив. КриптоАРМ ГОСТ.

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

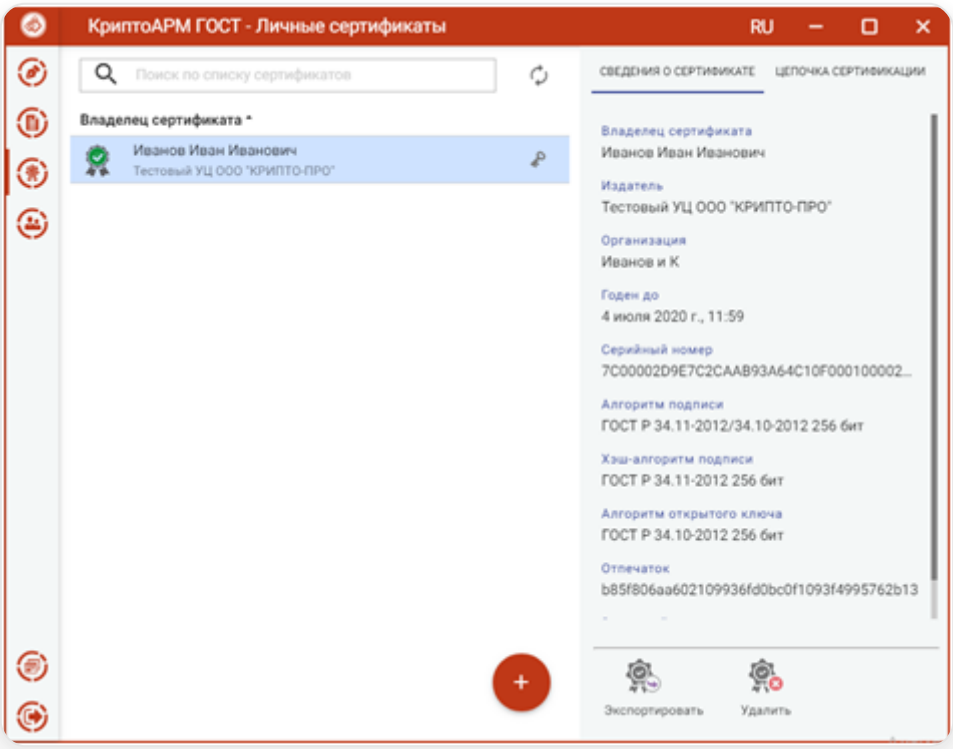


- **Личные** – для управления личными сертификатами, у которых есть привязка к закрытому ключу;
- **Промежуточные** - для управления промежуточными сертификатами;
- **Корневые доверенные** - для управления доверенными корневыми сертификатами;
- **Запросы** – для управлениями запросами на сертификат;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

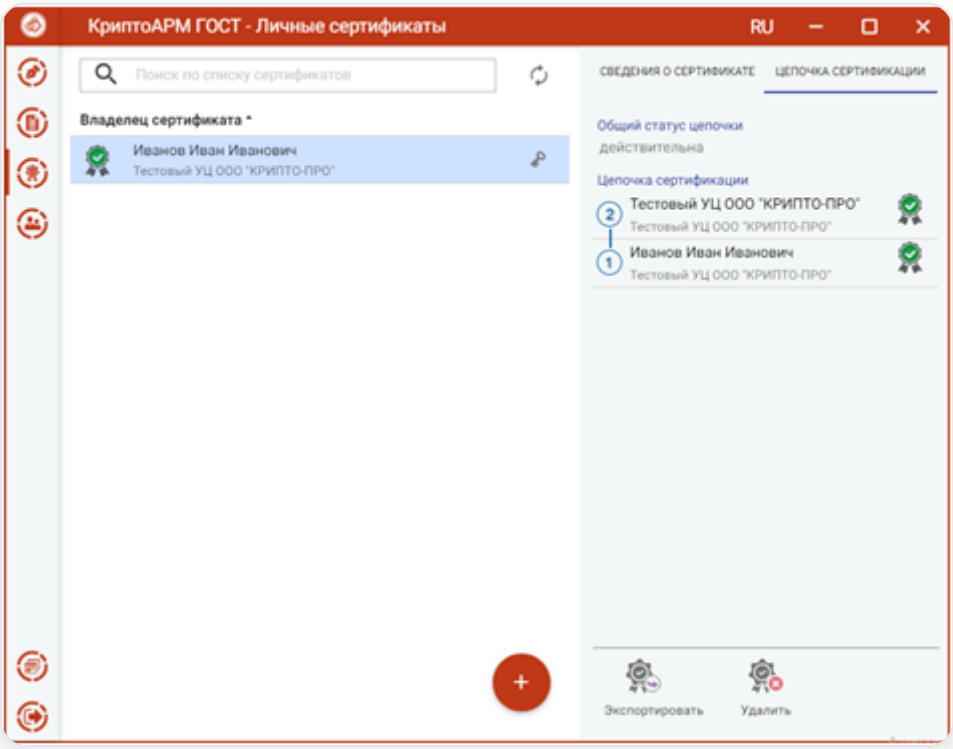
В левой области представления отображается список сертификатов выбранного раздела, в правой области отображается информация о выделенном сертификате.

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.



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


КриптоАРМ ГОСТ - Личные сертификаты
RU
Поиск по списку сертификатов
Владелец сертификата
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
СВЕДЕНИЯ О СЕРТИФИКАТЕ
ЦЕПОЧКА СЕРТИФИКАЦИИ
Общий статус цепочки
действительна
Цепочка сертификации
2
Тестовый УЦ ООО "КРИПТО-ПРО"
Тестовый УЦ ООО "КРИПТО-ПРО"
1
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
Экспортировать
Удалить

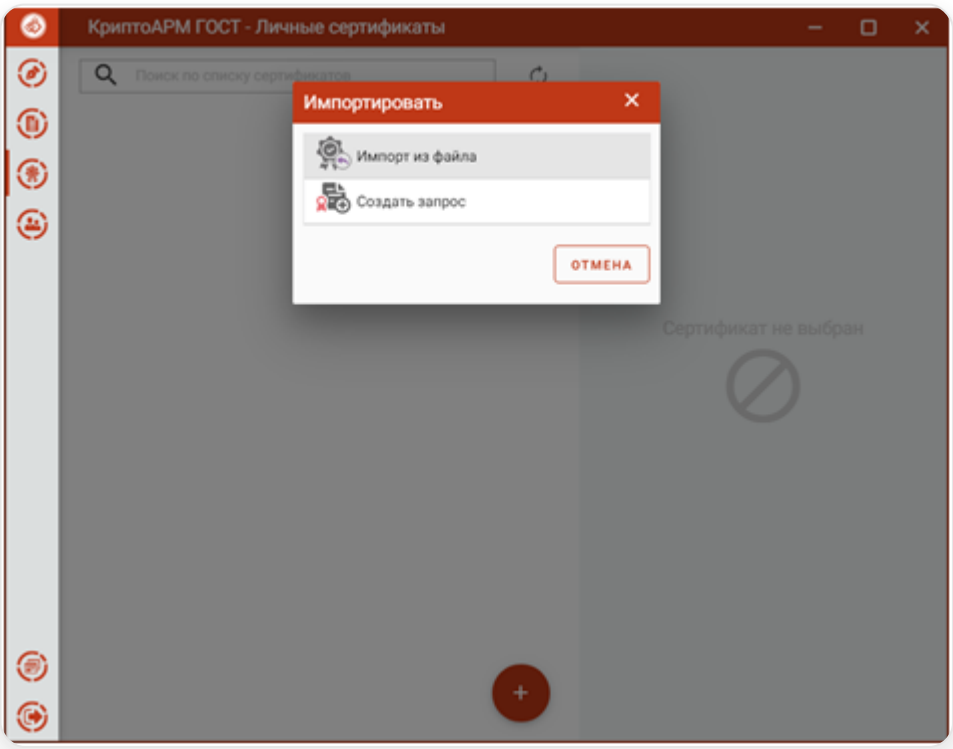
Открыть статью на сайте

Импорт сертификата из файла

Архив. КриптоАРМ ГОСТ.

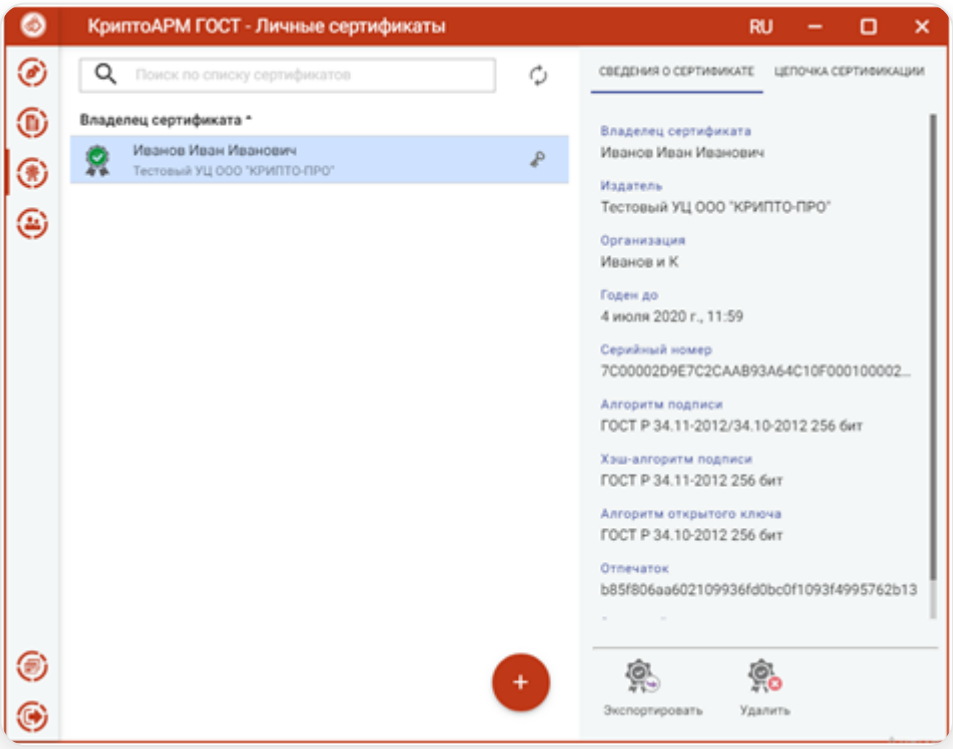
Импорт личного сертификата с привязкой к закрытому ключу.

Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»). В открывшемся окне нужно выбрать операцию **Импорт из файла**.

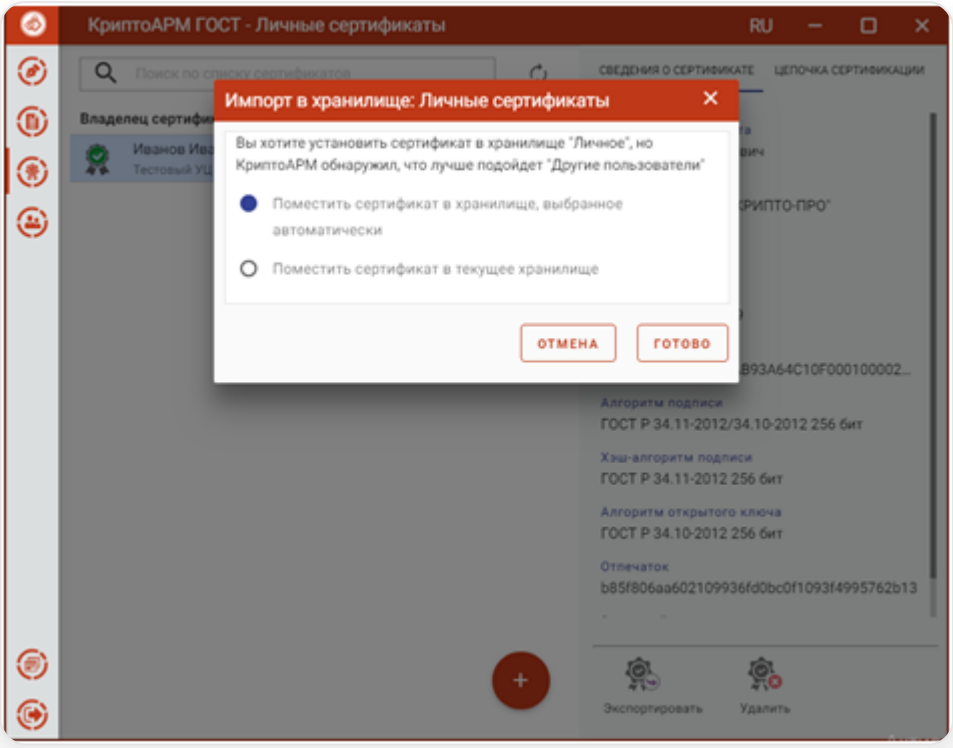


В появившемся диалоговом окне нужно выбрать файл сертификата. Это может быть файл формата pfx, содержащий ключевую пару (закрытый ключ и сертификат), или обычный сертификат, у которого есть закрытый ключ.

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



Если при импорте не будет найден закрытый ключ, соответствующий сертификату, то возникнет сообщение с предложением установить данный сертификат в подходящее хранилище или принудительно в выбранное.

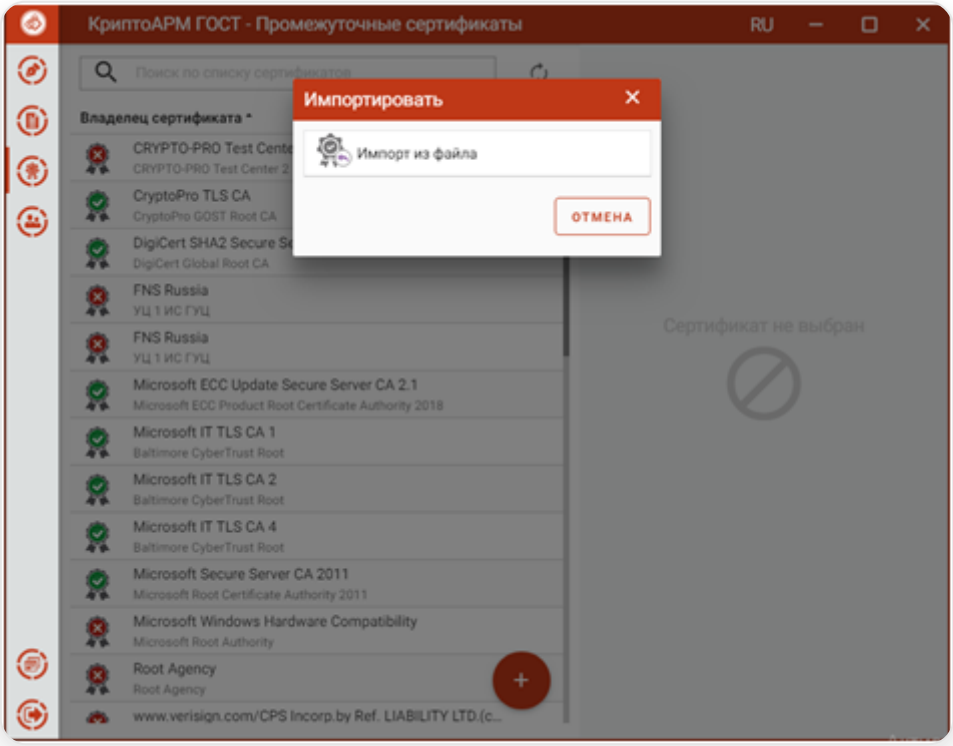


Если сертификат без закрытого ключа будет установлен в личное хранилище, то данным

сертификатом нельзя будет подписывать и расшифровывать файлы.

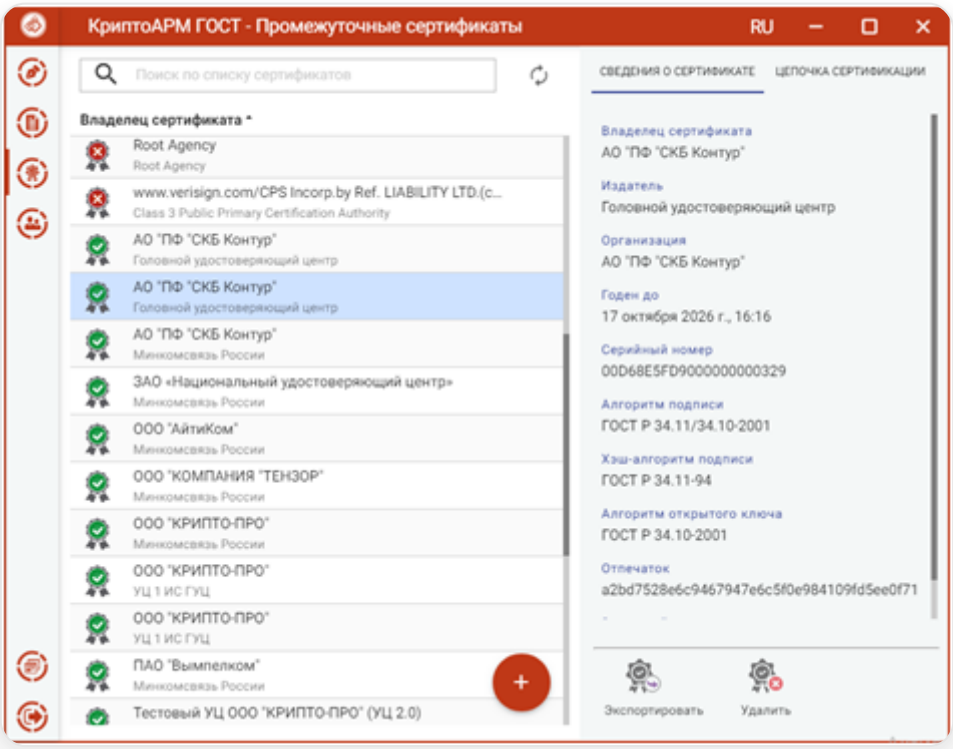
Импорт сертификата без привязки к закрытому ключу.

Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»)и выбора опции **Импорт из файла**.

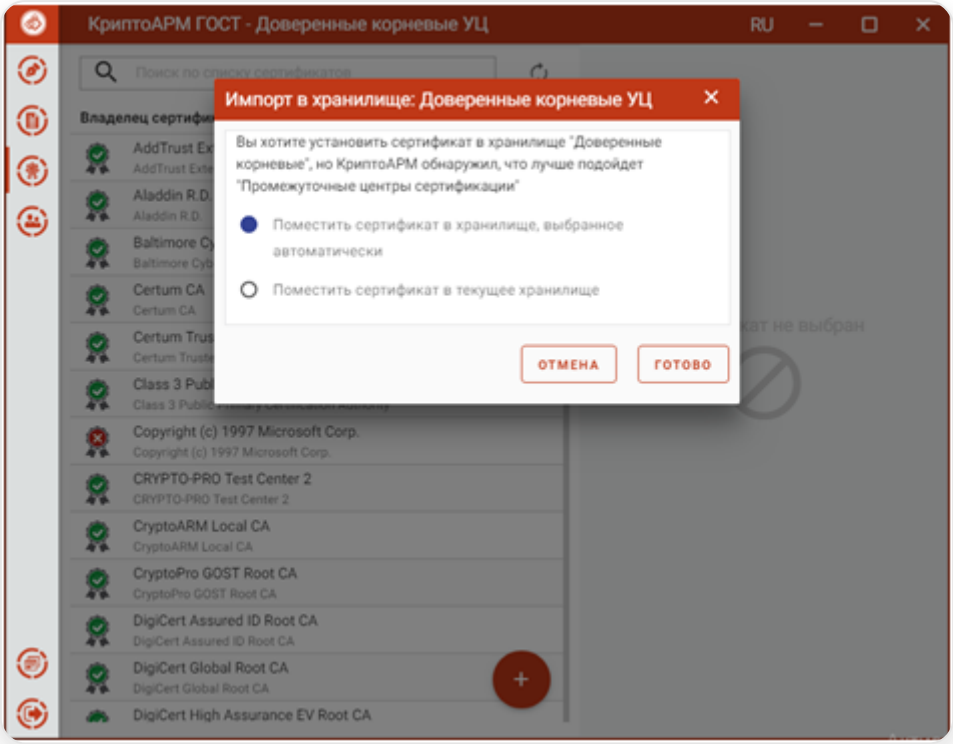


В появившемся диалоговом окне нужно выбрать файл сертификата.

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



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.

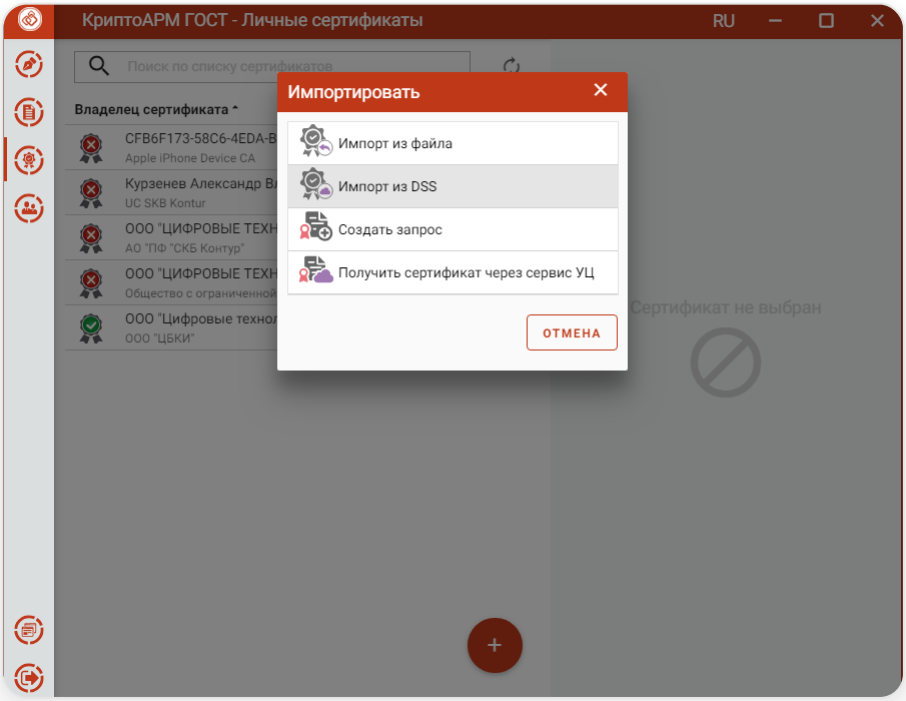


Открыть статью на сайте

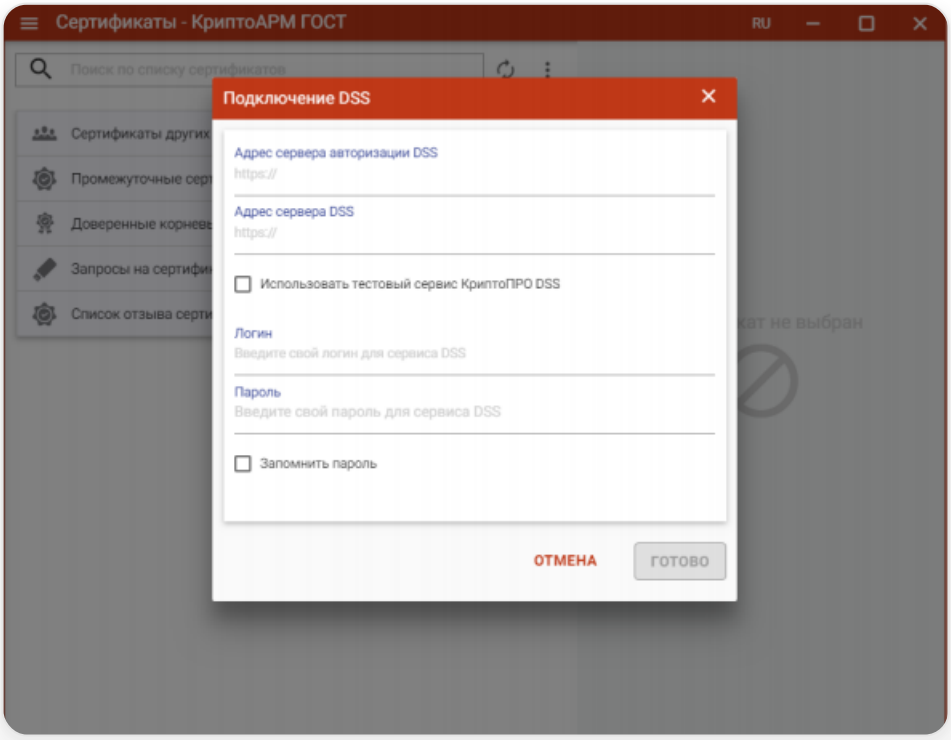
Импорт сертификата из DSS

Архив. КриптоАРМ ГОСТ.

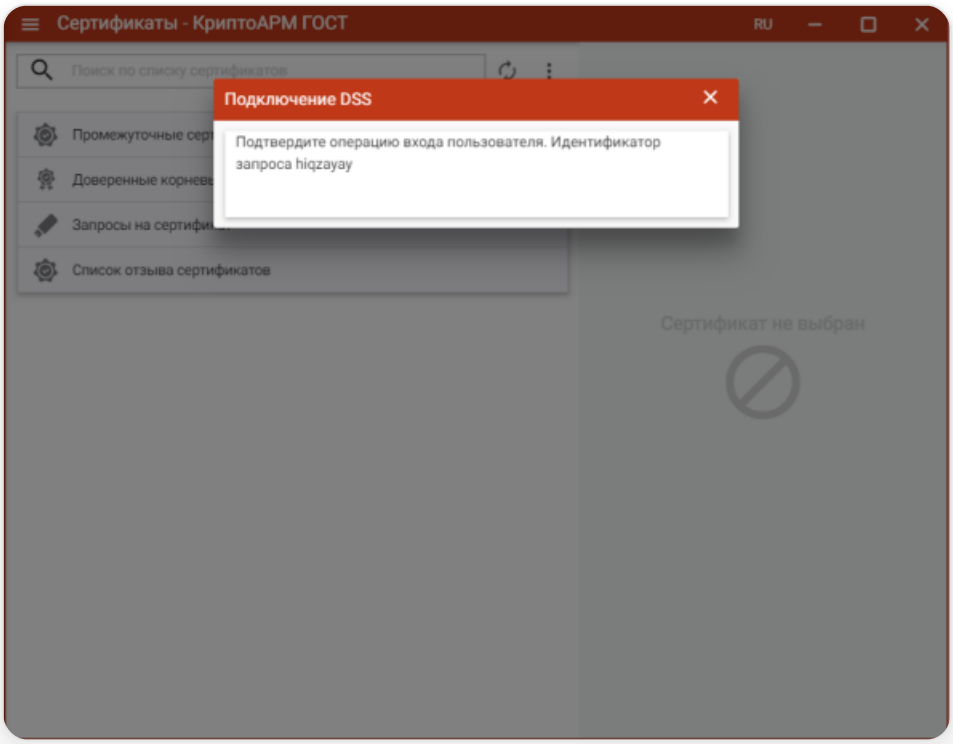
Выполнение импорта сертификата из DSS в хранилище выполняется кнопкой добавления сертификата ("+"), в открывшемся окне нужно выбрать операцию **Импорт из DSS.**



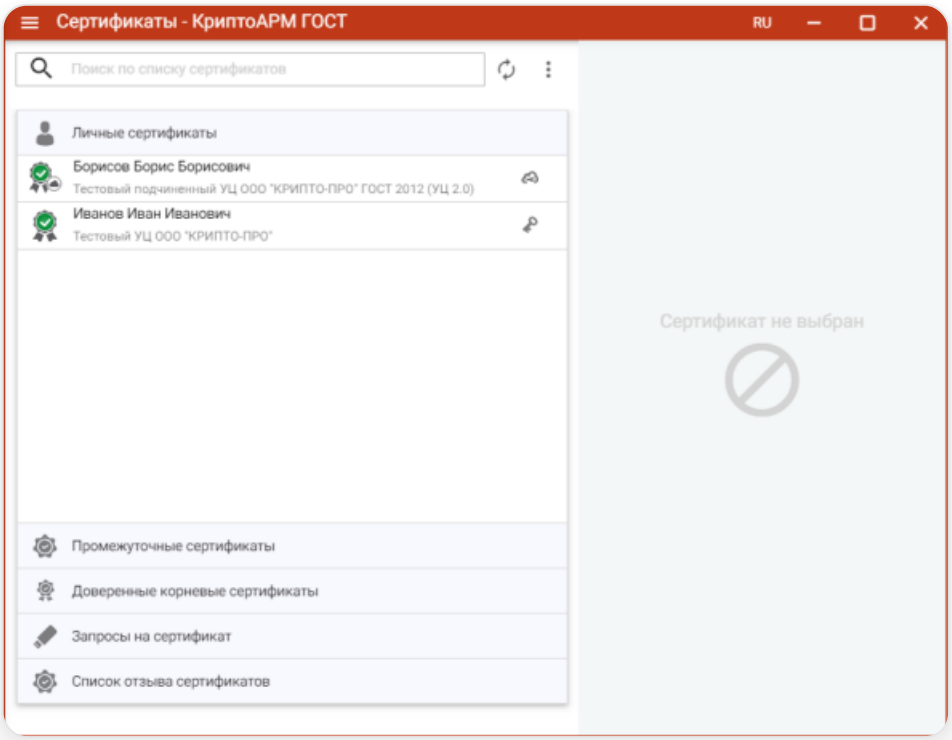
Открывается окно для ввода адресов серверов авторизации и DSS, логина и пароля для аутентификации.



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



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



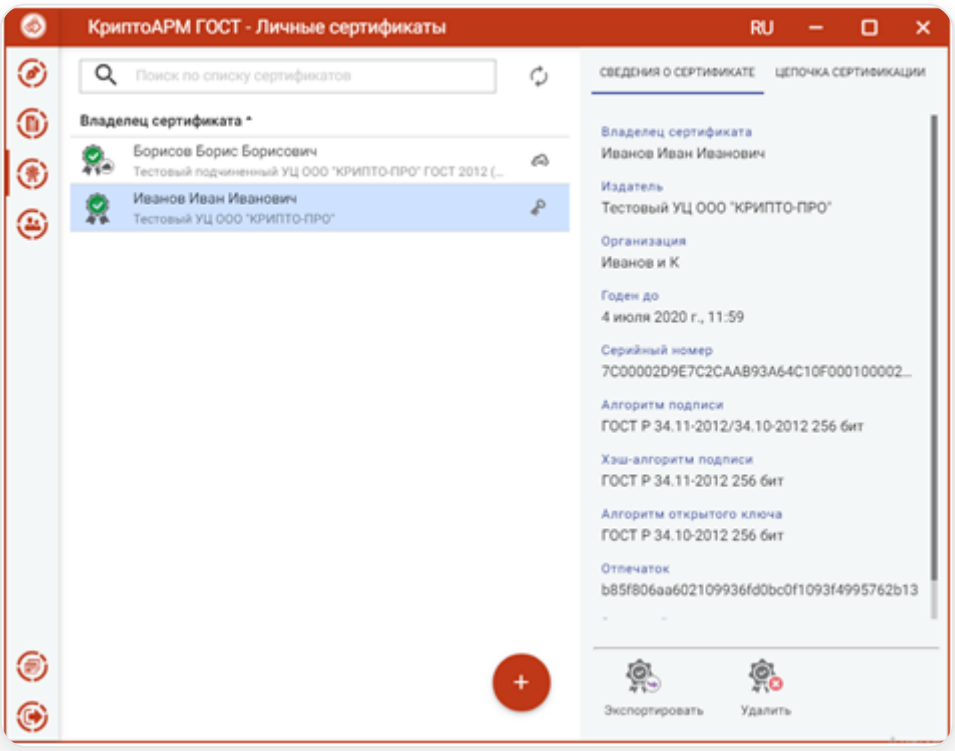
Сертификаты DSS отличаются от сертификатов, хранящихся локально, индикатором «облако».

Открыть статью на сайте

Экспорт сертификата в файл

Архив. КриптоАРМ ГОСТ.

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

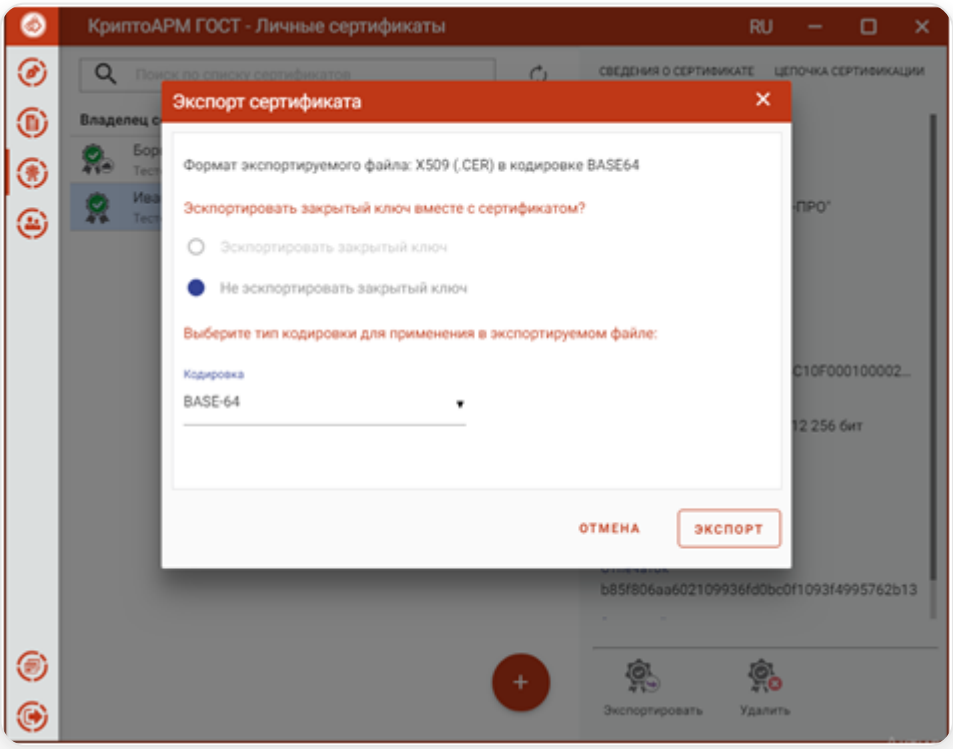


При экспорте сертификата с не экспортируемым закрытым ключом появляется окно, в котором можно выбрать только кодировку файла сертификата.

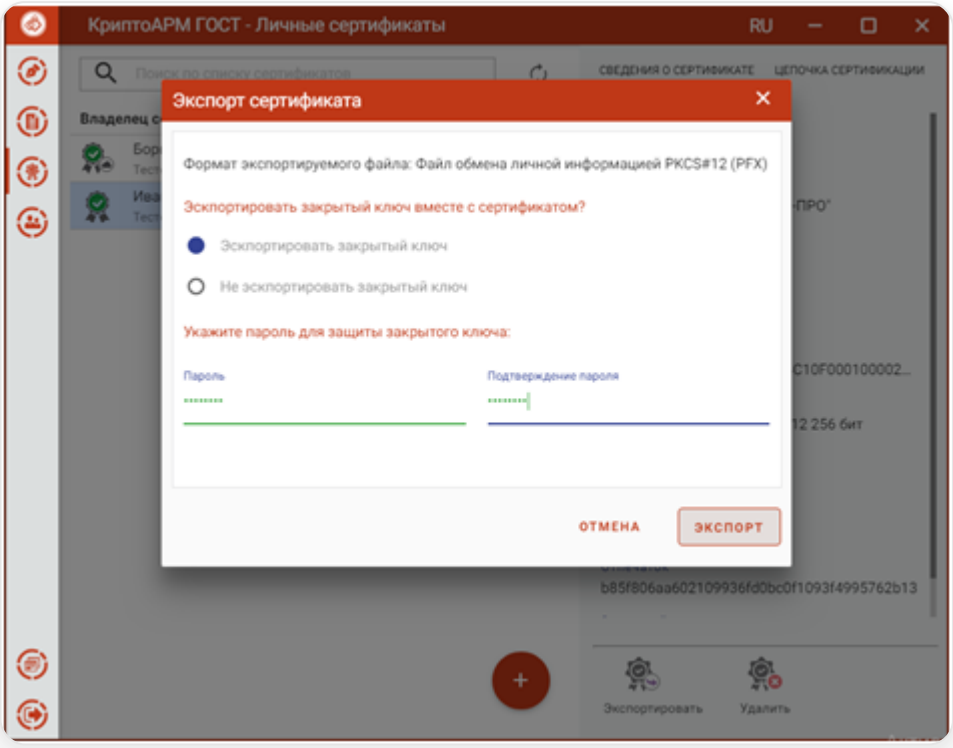
После нажатия кнопки **Экспорт**, в появившемся диалогом окне указать путь и имя файла, куда будет сохранен сертификат (по умолчанию, файл export.cer).

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.



- Экспортировать сертификат вместе с закрытым ключом. В таком случае надо указать пароль для защиты закрытого ключа



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.

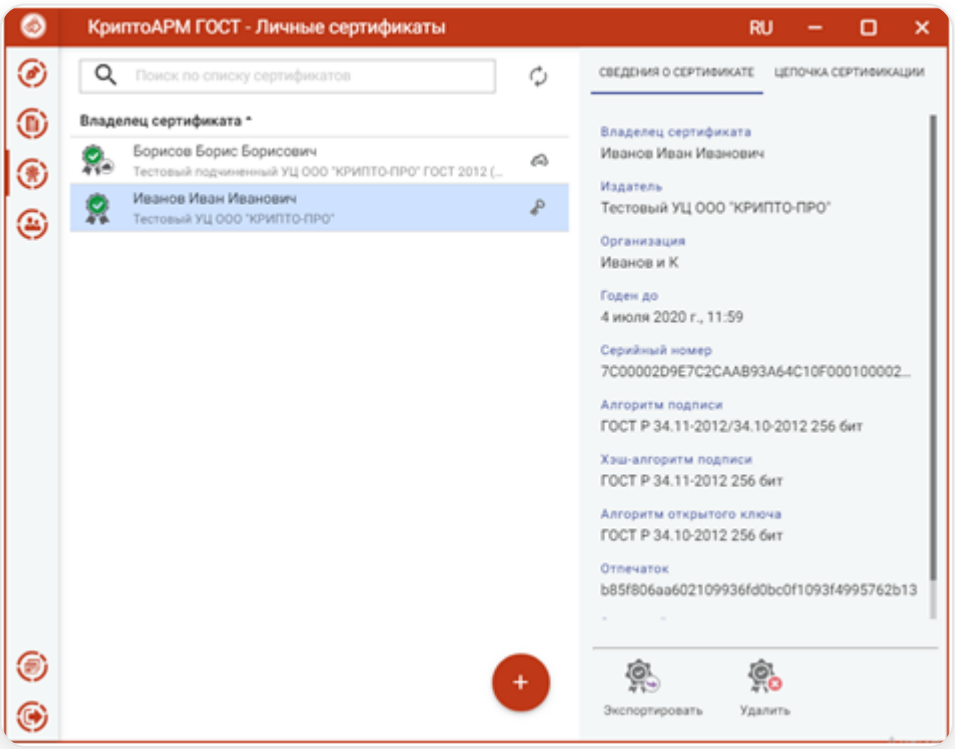
Примечание: если контейнер экспортируемого сертификата защищен паролем, то при экспорте сертификата вместе с закрытым ключом необходимо будет вводить пароль к ключевому контейнеру.

Открыть статью на сайте

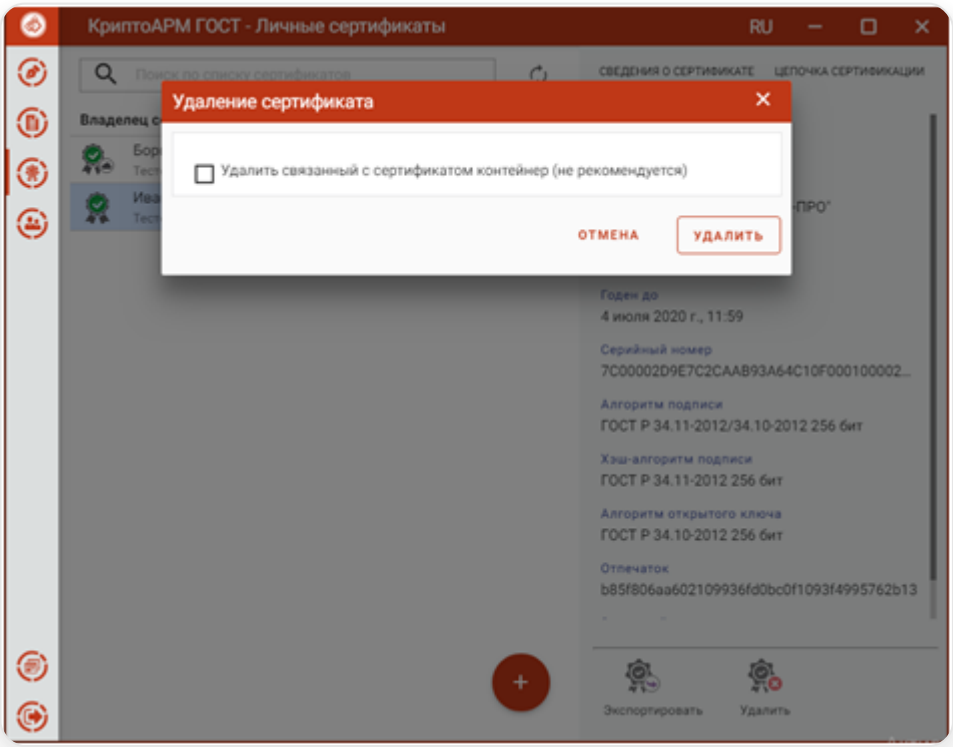
Удаление сертификата

Архив. КриптоАРМ ГОСТ.

Для удаления сертификата нужно выбрать операцию **Удалить**.



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



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

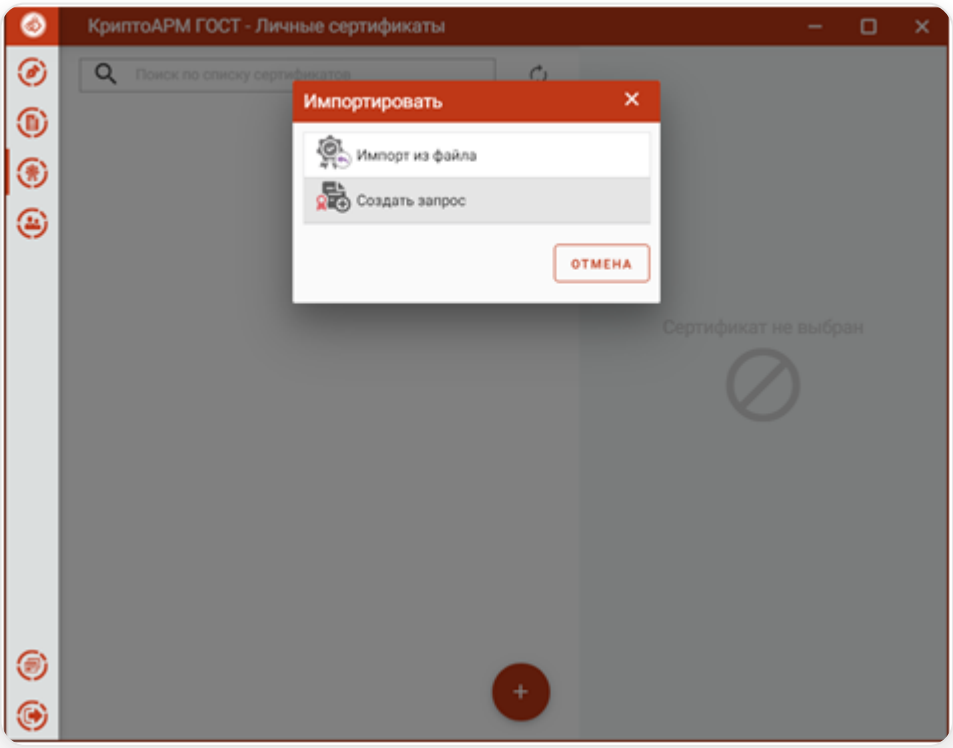
Примечание: Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.

Открыть статью на сайте

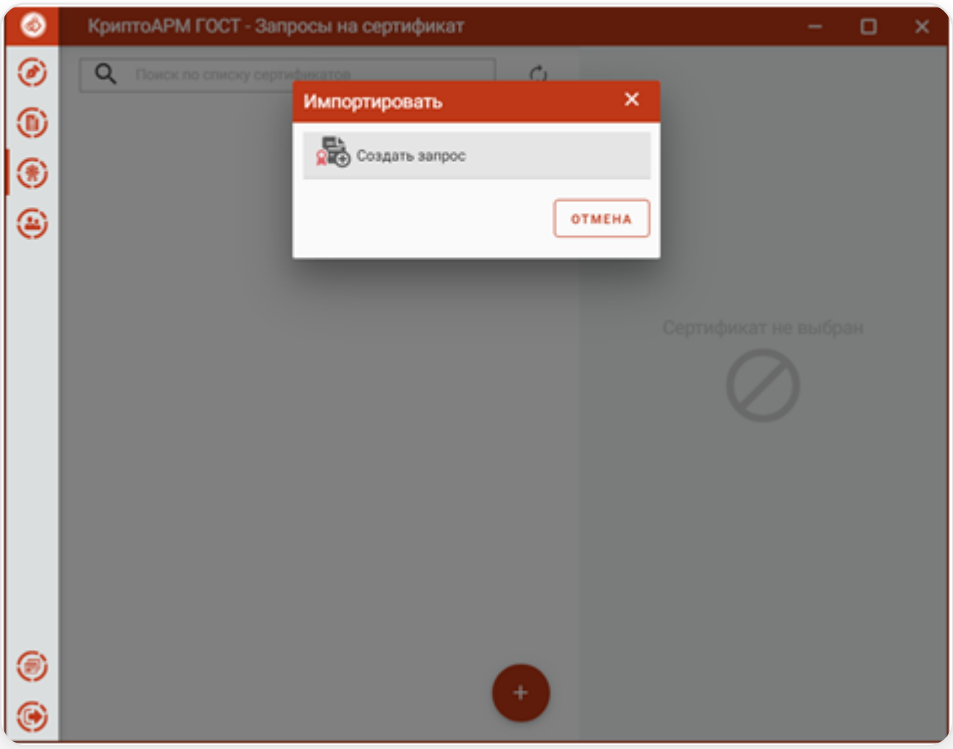
Создание запроса на сертификат

Архив. КриптоАРМ ГОСТ.

Для создания запроса на сертификат в окне добавления сертификата следует выбрать операцию **Создать запрос**.



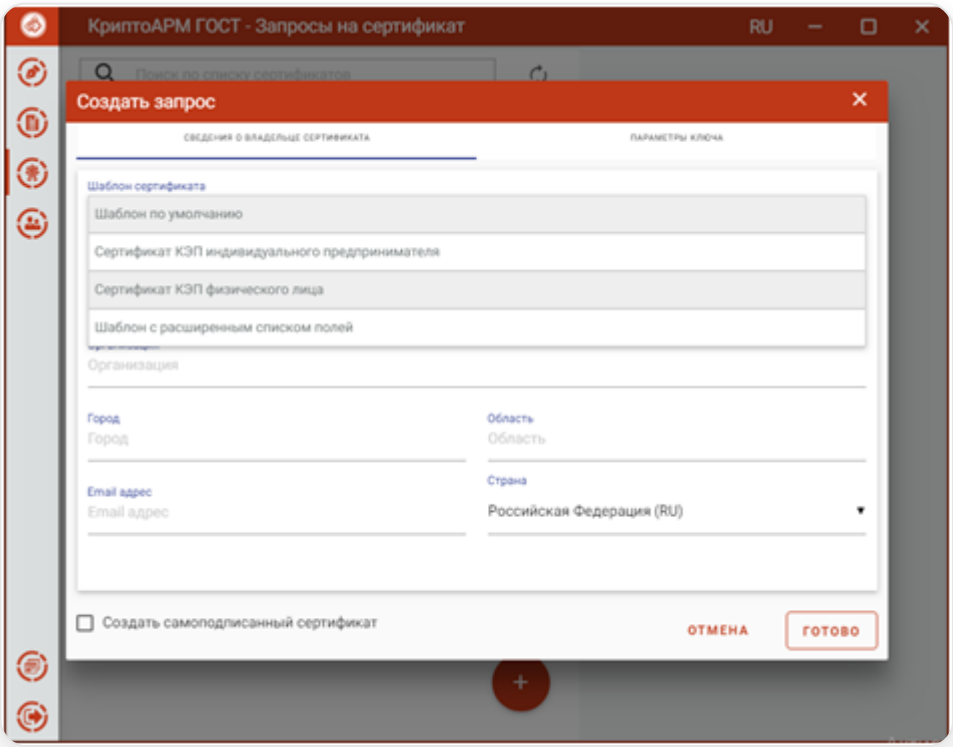
Создать запрос можно со списка личных сертификатов или со списка запросов.



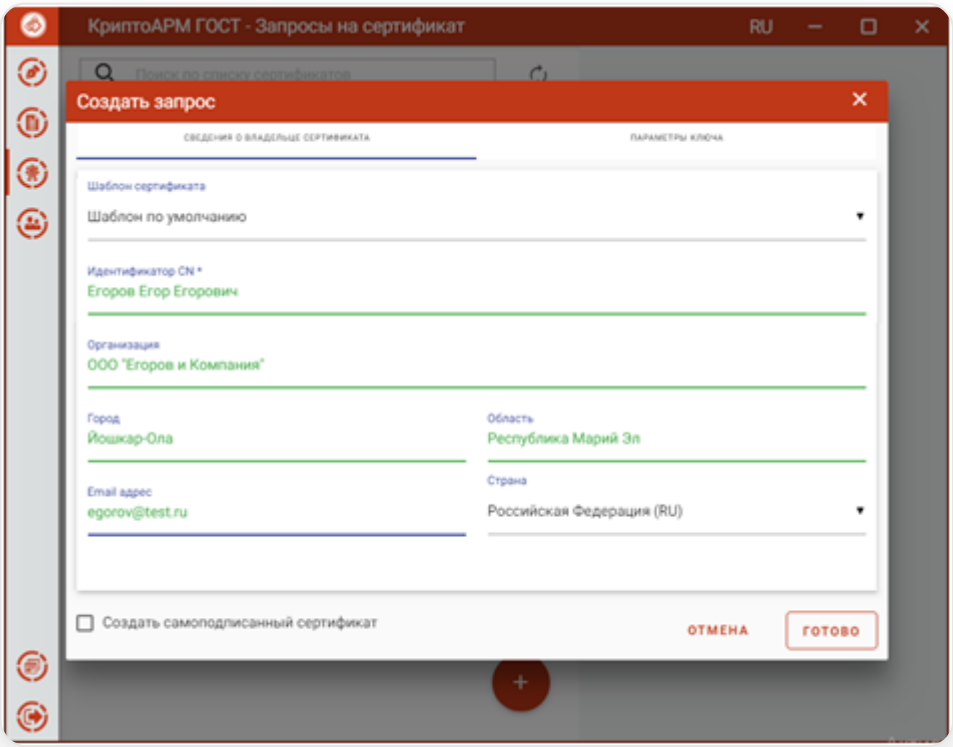
Опции необходимых сведений для генерации запроса распределены на две вкладки: **Сведения о владельце сертификата** и **Параметры ключа**.

В параметрах субъекта указывается:

- Шаблон сертификата



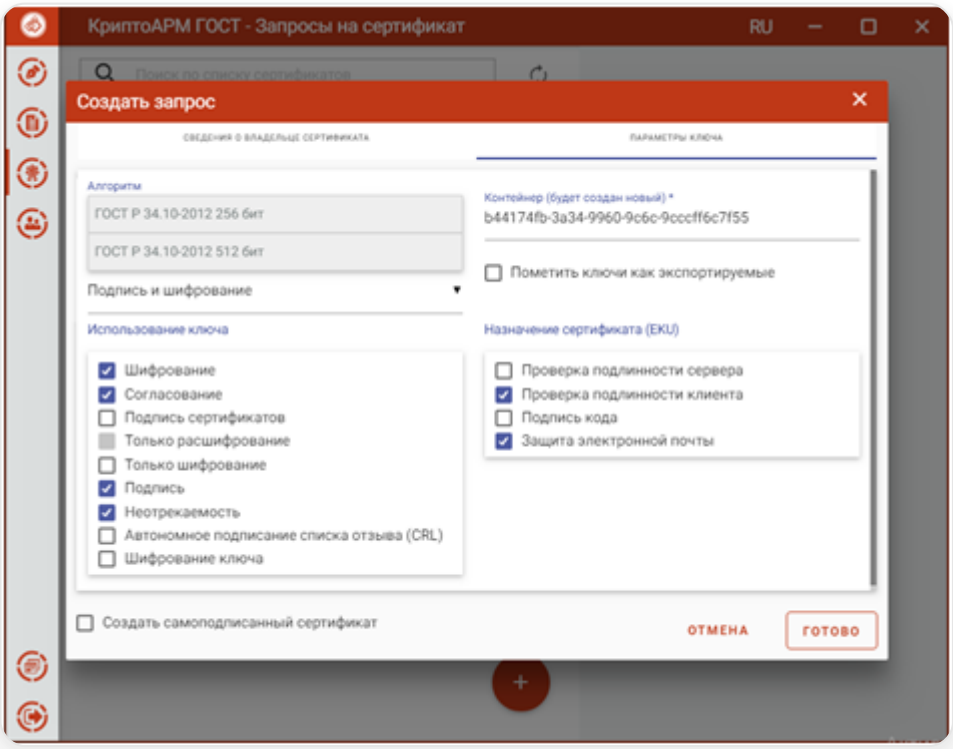
- Основная информация, в которой, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце сертификата



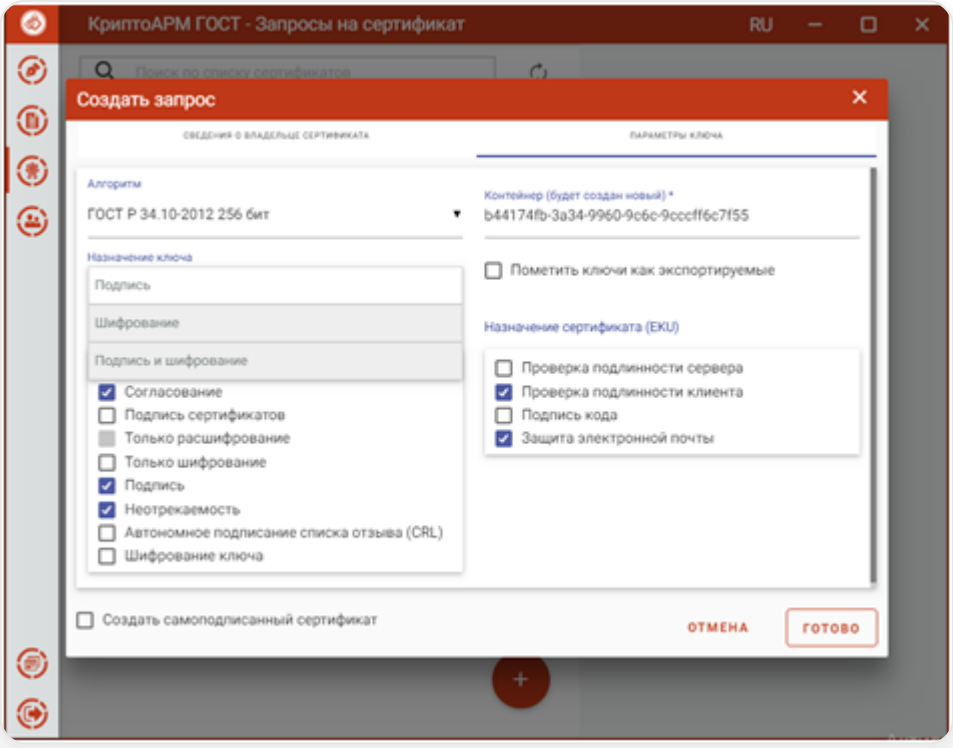
- При установке флага **Создать самоподписанный сертификат** происходит создание сертификата и его автоматическая установка в личное хранилище пользователя. Запросы на самоподписанные сертификаты не создаются.

В параметрах ключа указывается:

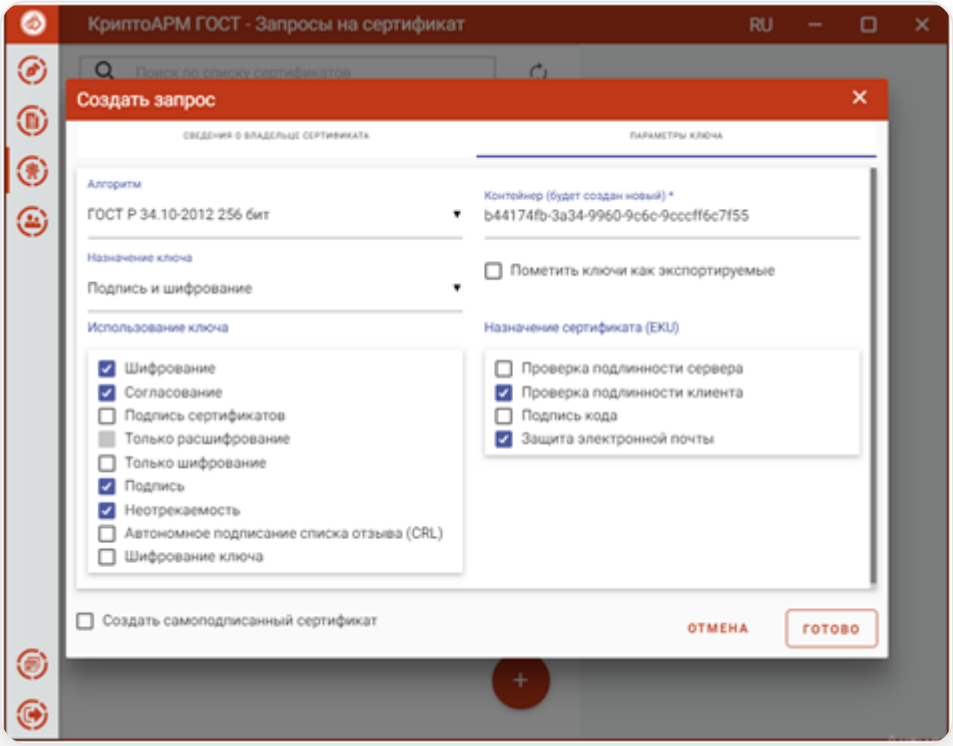
- Алгоритм ключа



- Назначение ключа



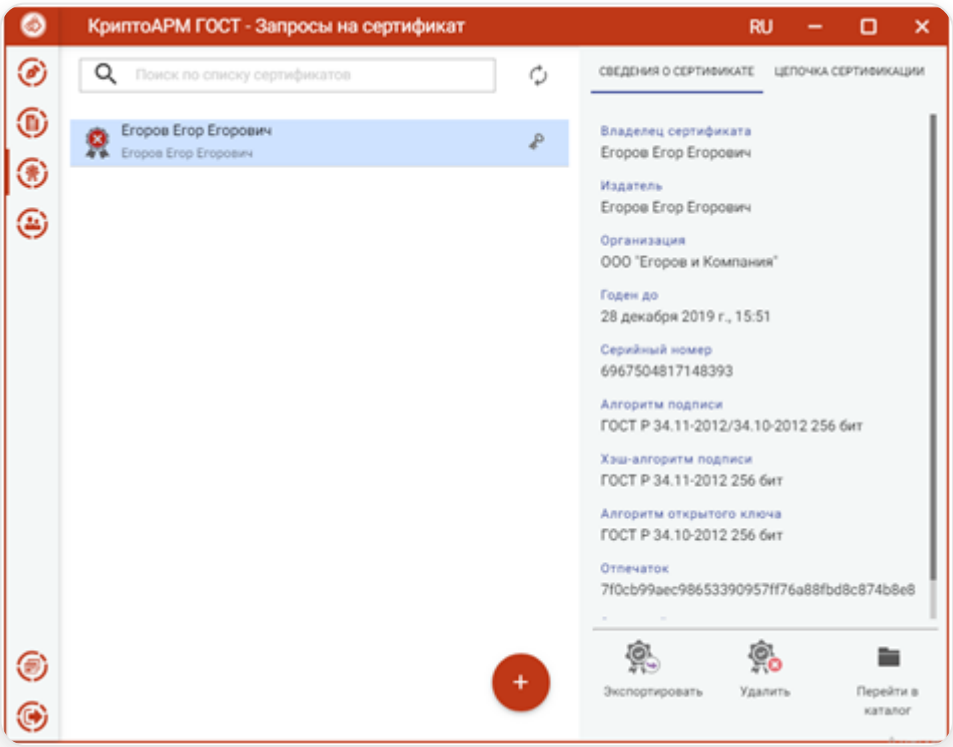
- Использование ключа



- 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**.



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.

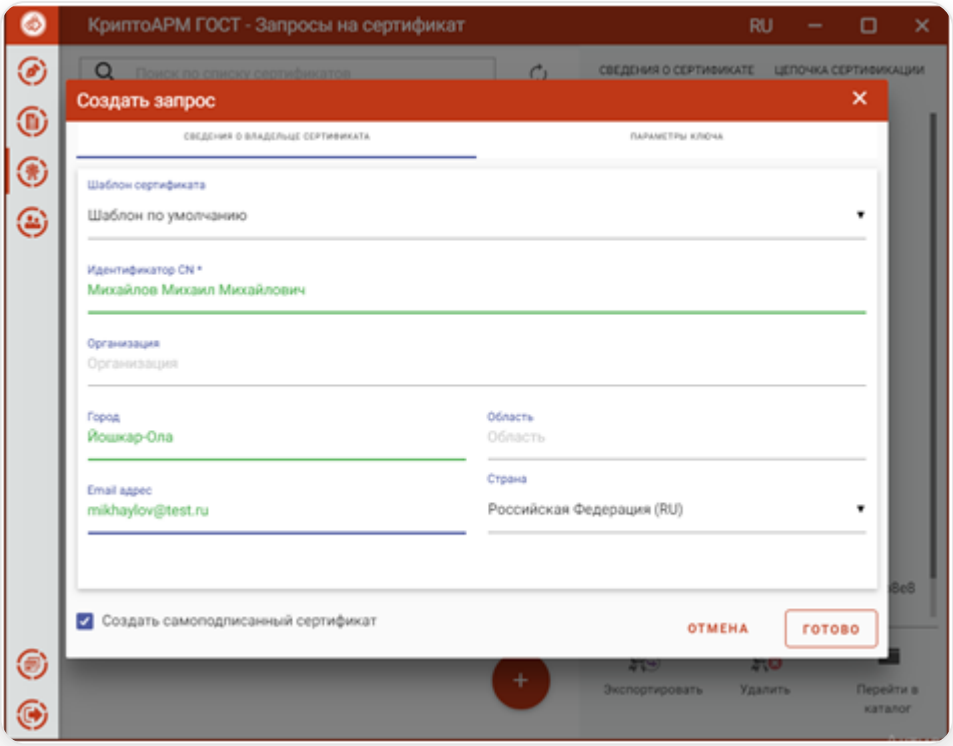
Созданный файл запроса на сертификат следует направить на рассмотрение в Удостоверяющий центр (УЦ). Полученный из УЦ сертификат следует импортировать для работы с данным сертификатом в приложении.

Открыть статью на сайте

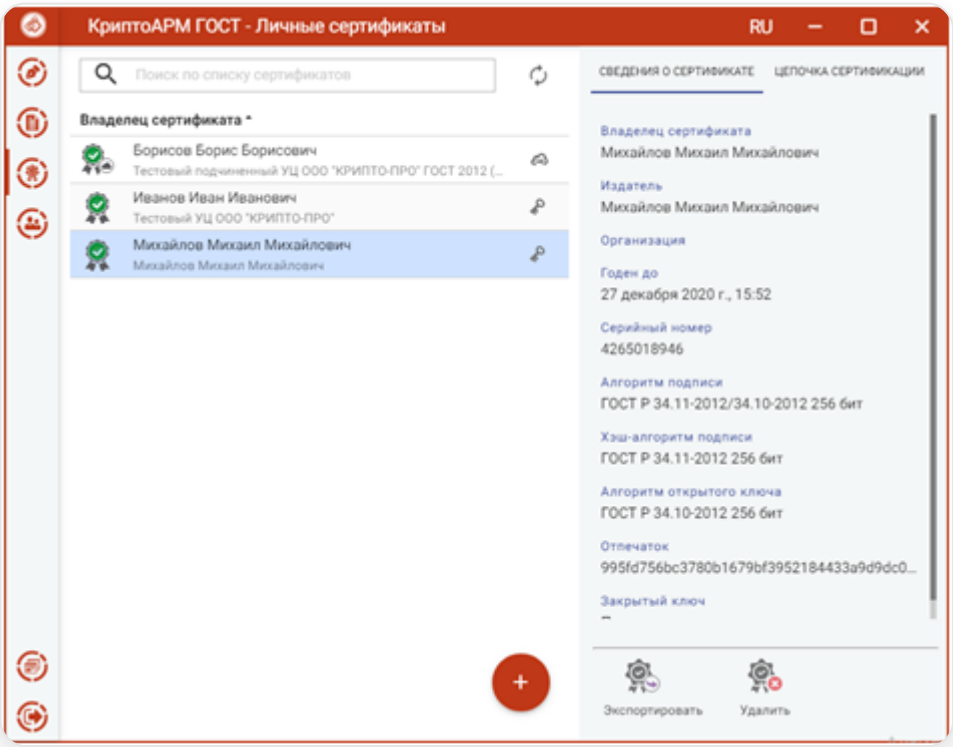
Создание самоподписанного сертификата

Архив. КриптоАРМ ГОСТ.

Для создания самоподписанного сертификата на форме **Создать запрос** следует поставить флаг **Создание самоподписанного сертификата.**



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



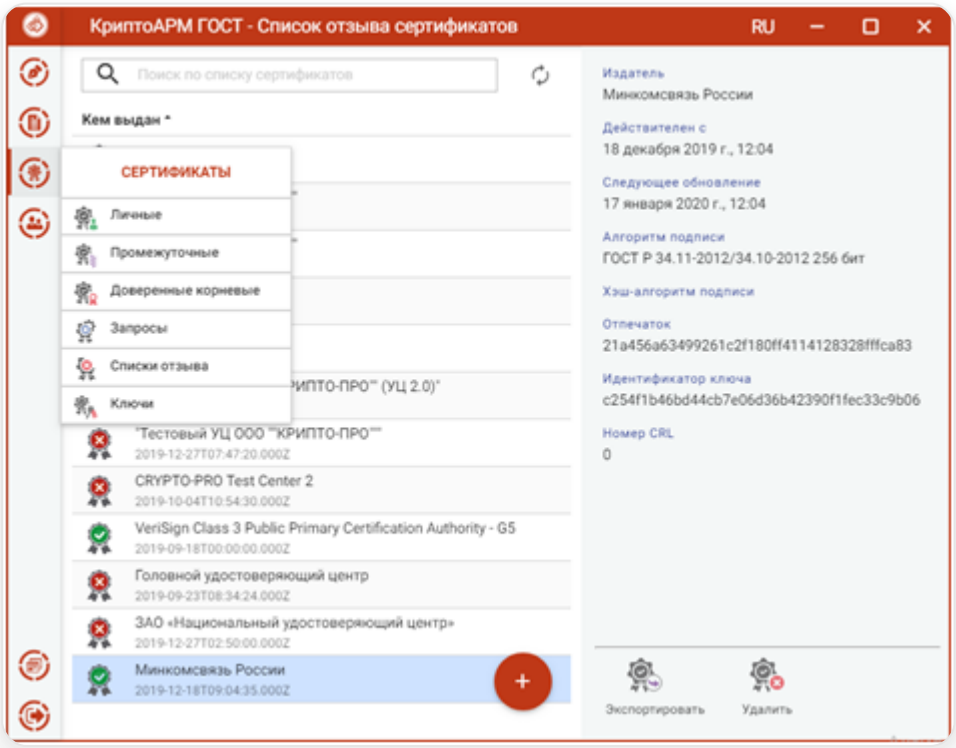
При генерации самоподписанного сертификата запрос на сертификат не создается.

Открыть статью на сайте

Списки отзыва сертификатов

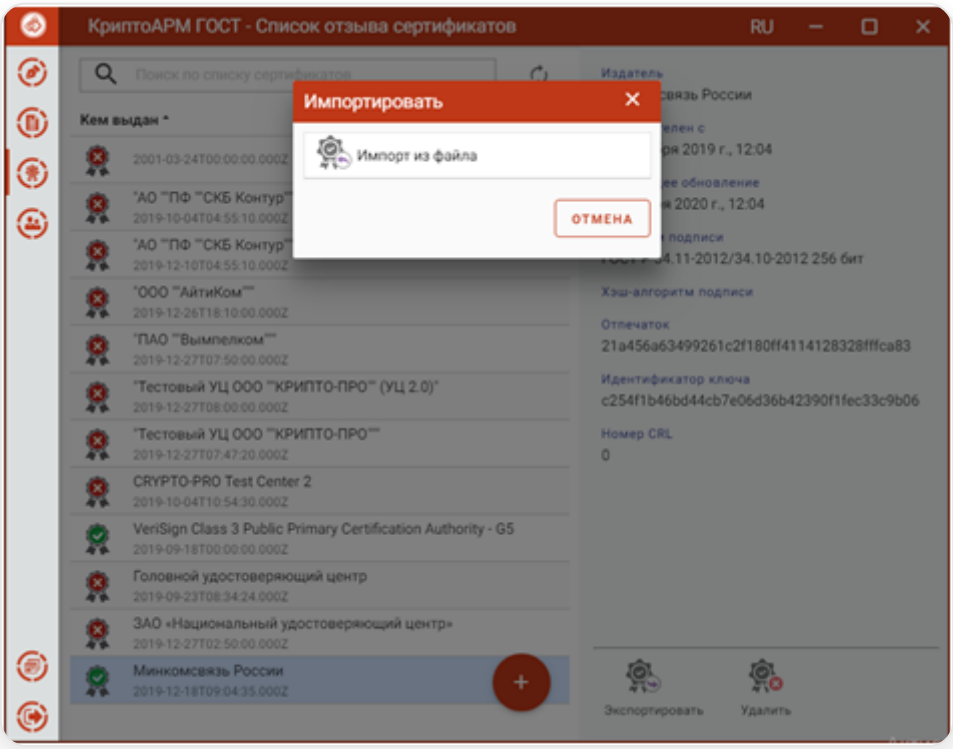
Архив. КриптоАРМ ГОСТ.

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

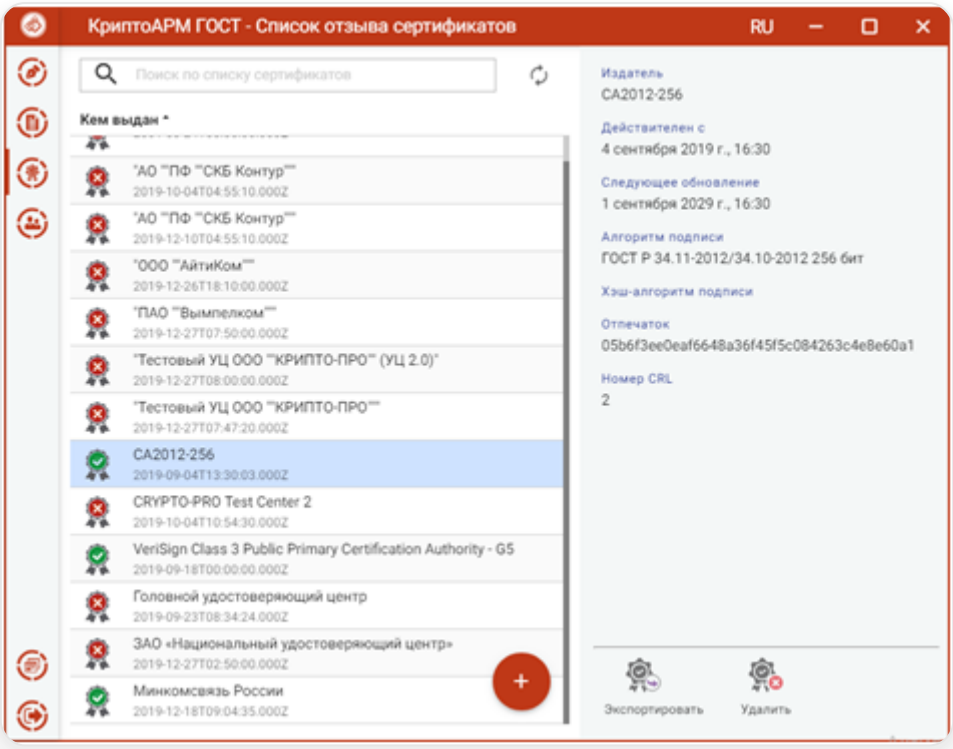


Списки отзыва можно импортировать, экспортировать и удалять.

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

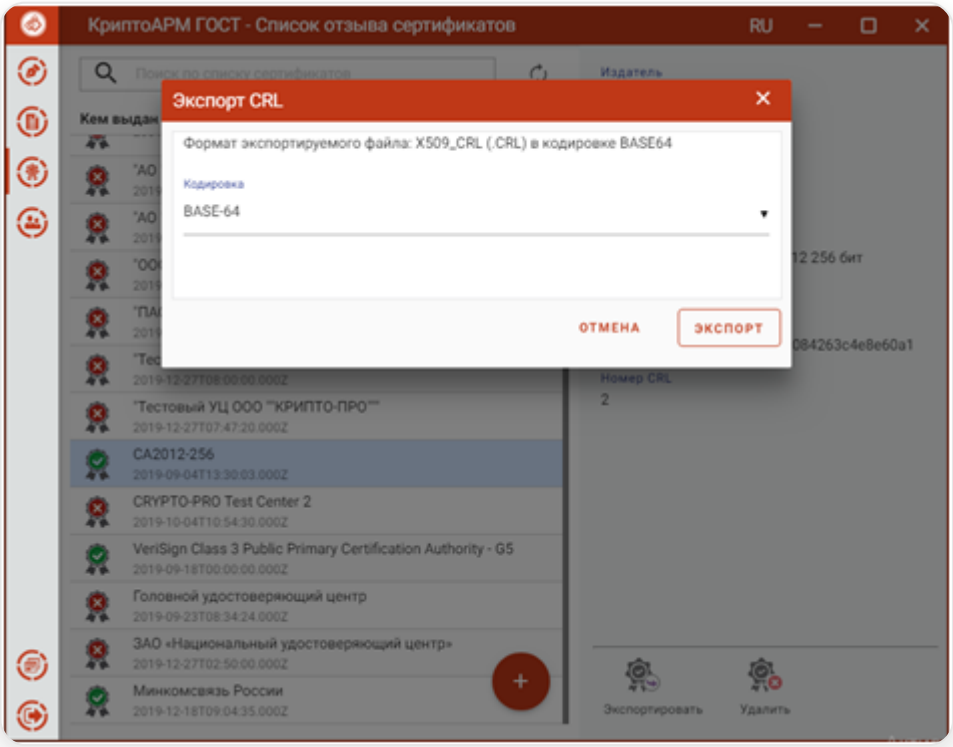


При успешном импорте COC отображается в разделе **Список отзыва сертификатов**.



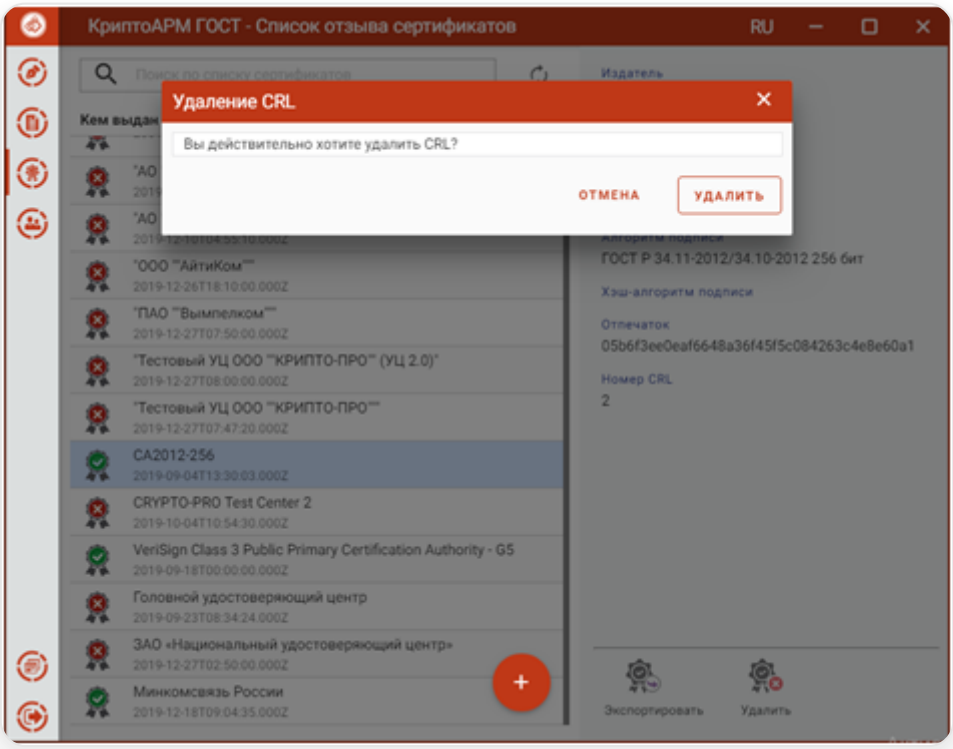
Экспорт списка отзыва сертификатов.

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



Удаление списка отзыва сертификатов.

Для удаления COC надо нажать кнопку **Удалить** и подтвердить удаление в соответствующем окне.

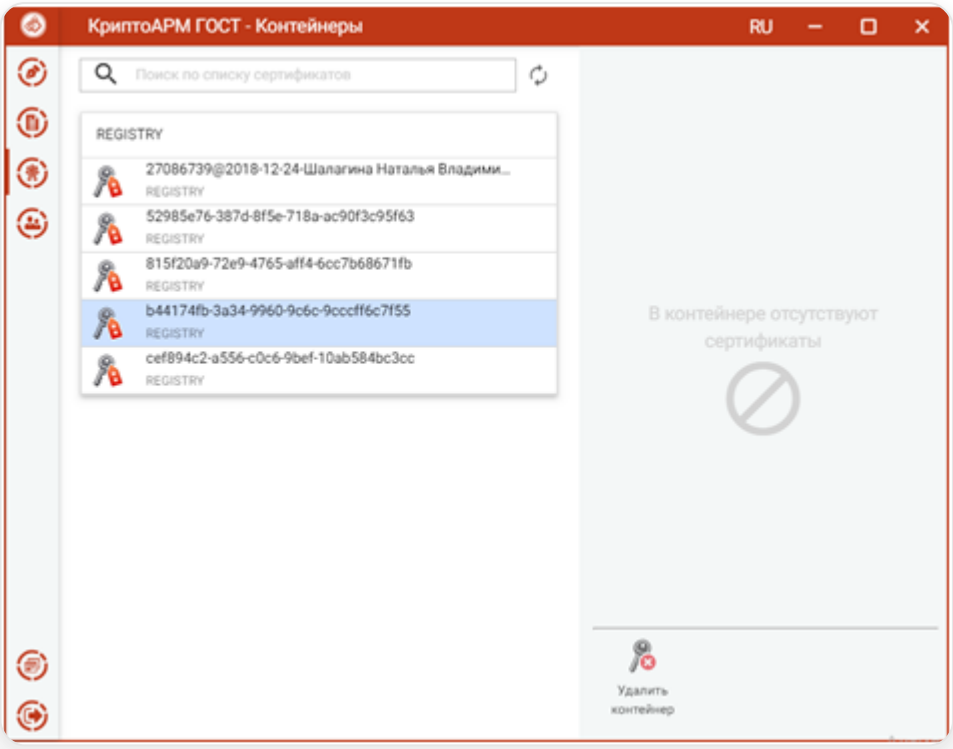

КриптоАРМ ГОСТ - Список отзыва сертификатов
RU
Удаление CRL
Вы действительно хотите удалить CRL?
ОТМЕНА
УДАЛИТЬ
Издатель
ГОСТ Р 34.11-2012/34.10-2012 256 бит
Хэш-алгоритм подписи
Отпечаток
05b6f3ee0eaf6648a36f45f5c084263c4e8e60a1
Номер CRL
2
Экспортировать
Удалить

Открыть статью на сайте

Установка сертификата из ключевого контейнера

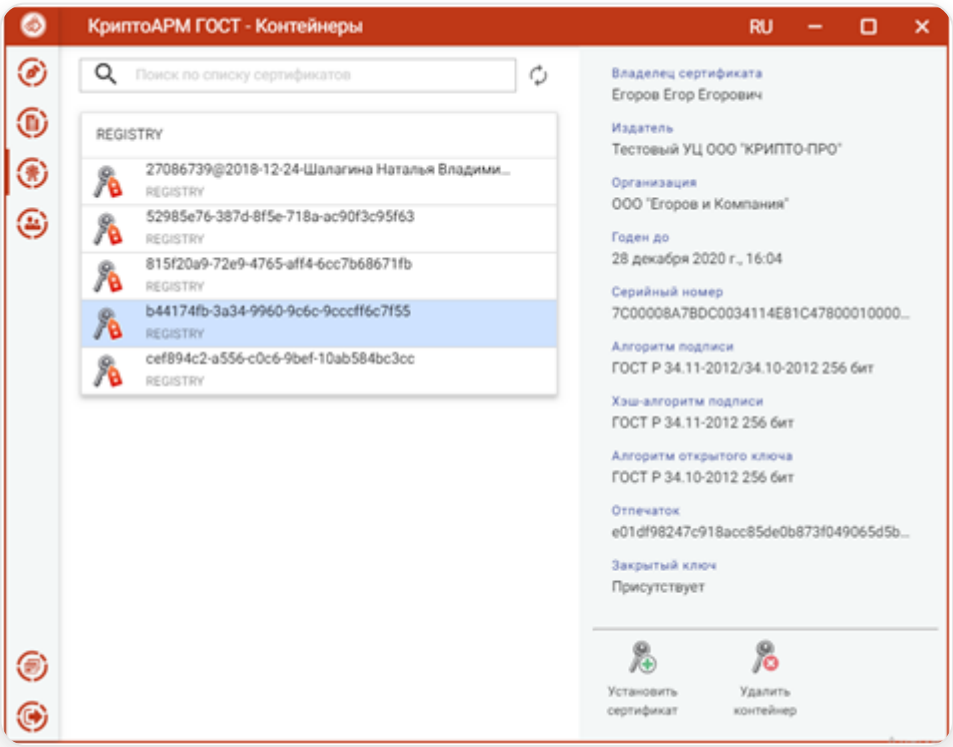
Архив. КриптоАРМ ГОСТ.

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.



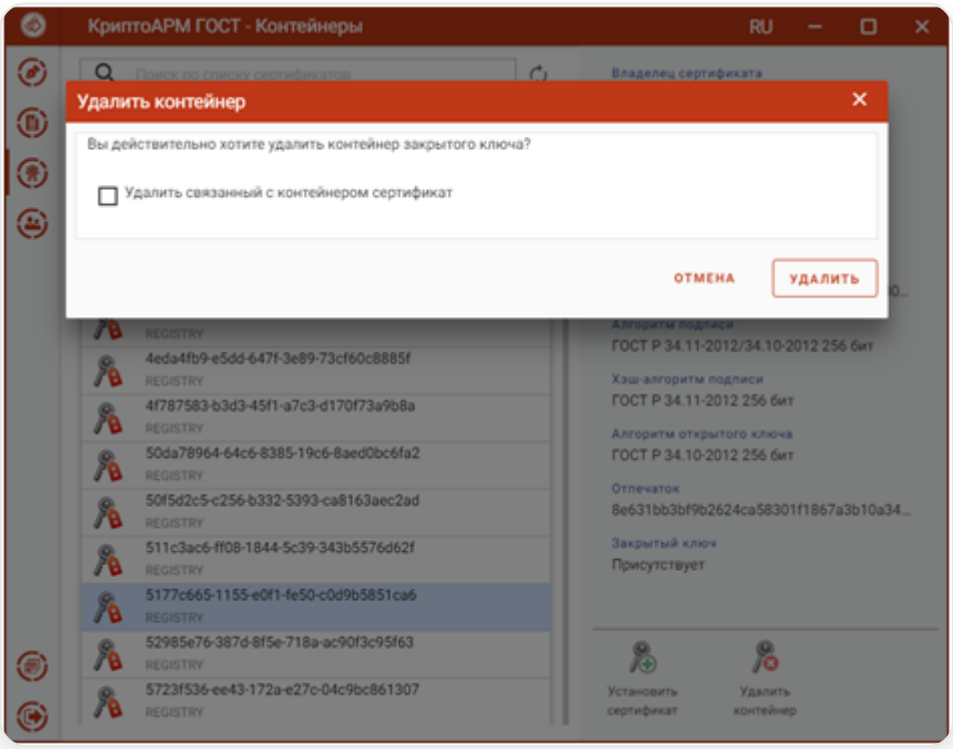
В каждом из хранилищ отображаются контейнеры закрытых ключей. В случае отсутствия контейнеров в хранилище, оно может быть скрыто как пустое.

После выбора контейнера отображается информация о находящемся в нем сертификате.

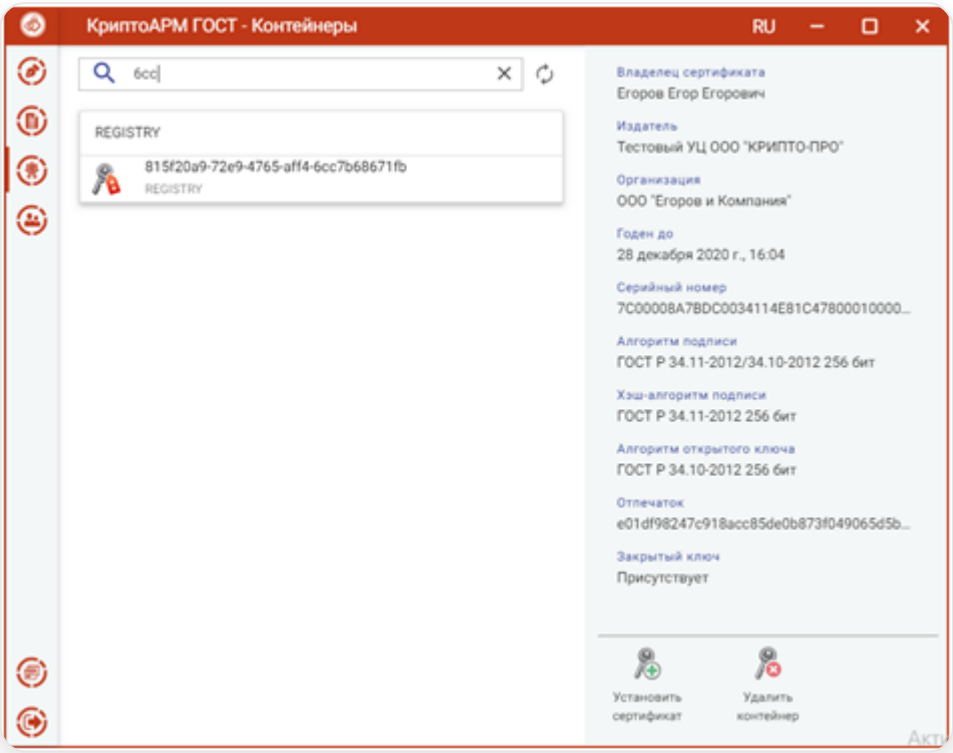


По кнопке **Установить сертификат** происходит установка сертификата в Личное хранилище сертификатов. Данный сертификат становится доступен для выполнения операций подписи, шифрования и расшифрования.

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



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

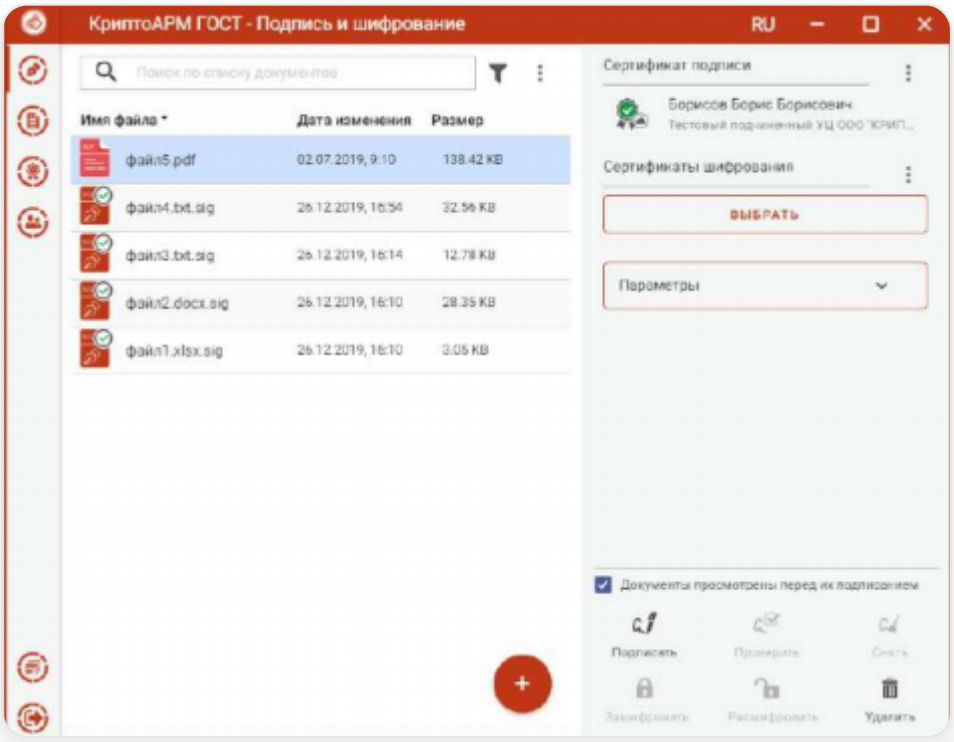


Открыть статью на сайте

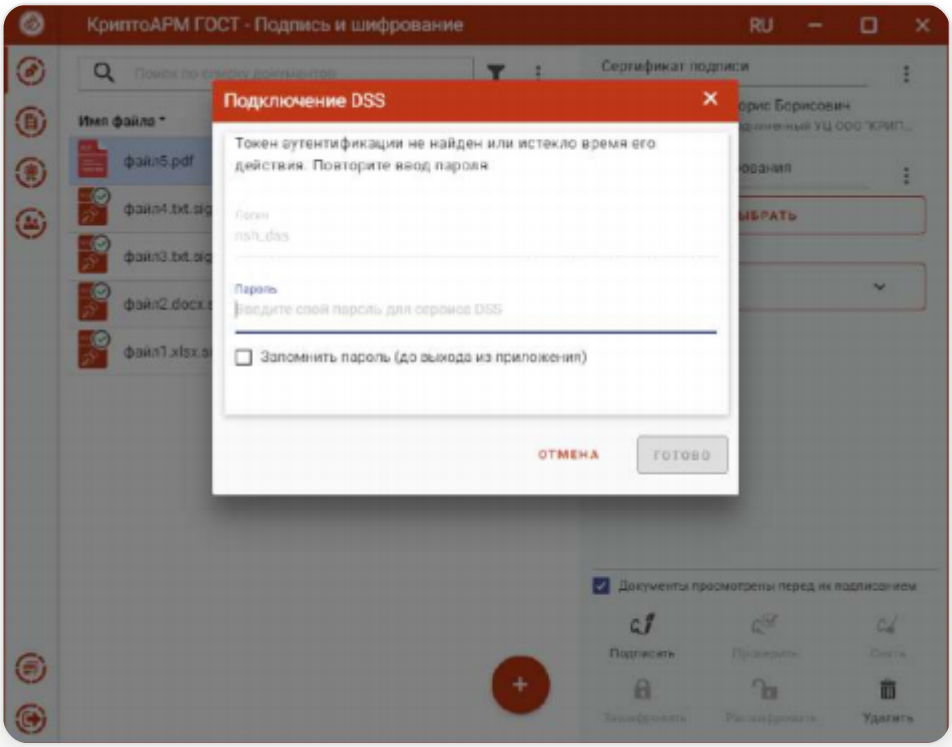
Подпись сертификатом DSS

Архив. КриптоАРМ ГОСТ.

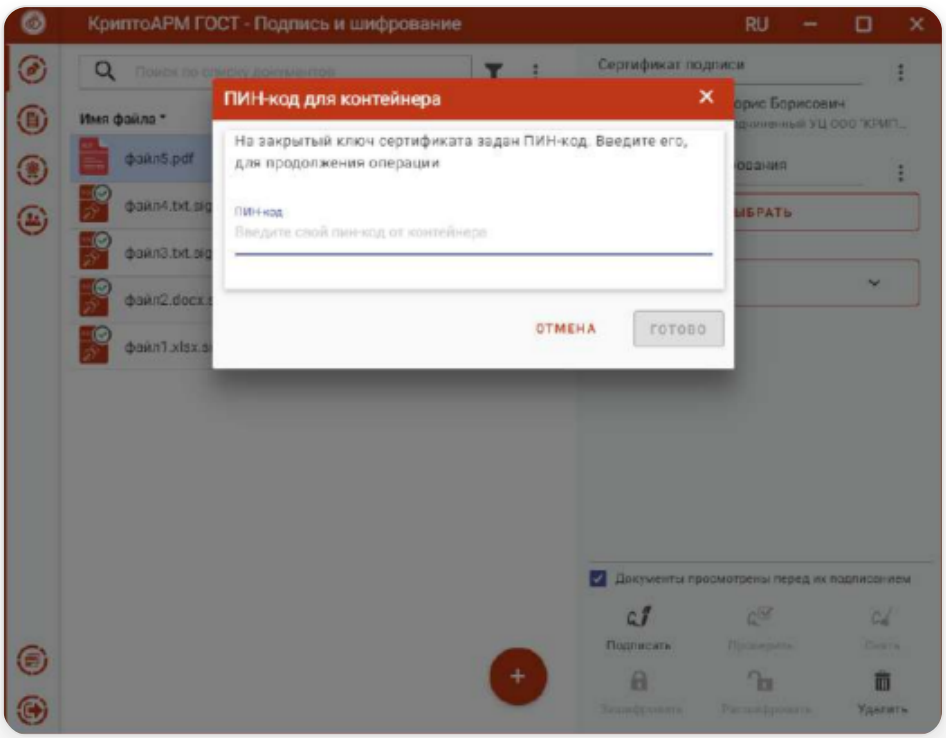
Подпись сертификатом DSS ничем не отличается от подписи обычным сертификатом, за исключением некоторых шагов. Также нужно выбрать файлы для подписи, выбрать сертификат DSS подписчика и установить флаг, что документы просмотрены перед подписанием.



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

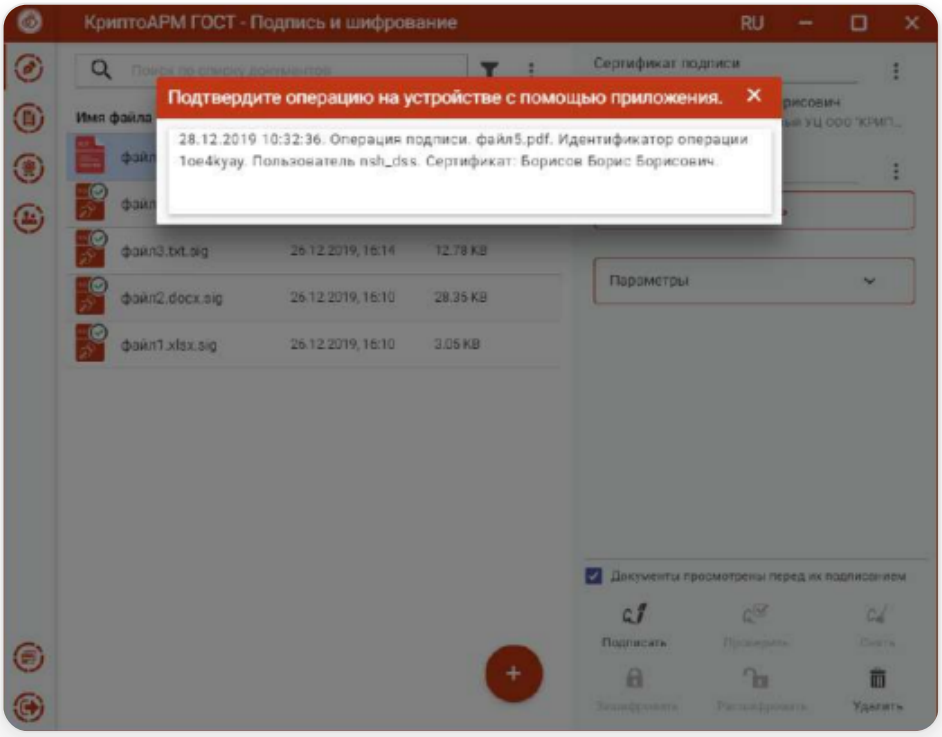


При нажатии на кнопку **Готово** открывается окно для ввода пароля к ключевому контейнеру. Если пароль не задан, то данный шаг пропускается.

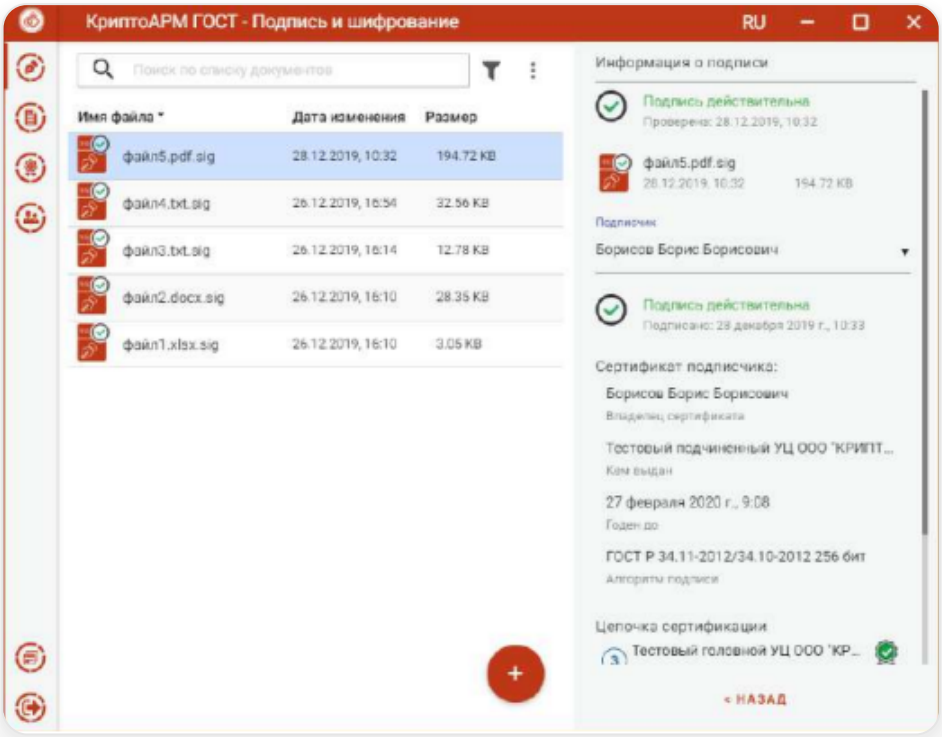


Если у пользователя в личном кабинете DSS в настройках аутентификации стоит подтверждение операции подписи по SMS, по электронной почте или с помощью мобильного

приложения, то на следующем шаге появляется сообщение, что операцию нужно подтвердить.



После подтверждения операции на устройстве происходит подпись файла.



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

Открыть статью на сайте

Включение режима логирования и консоль управления

Архив. КриптоАРМ ГОСТ.

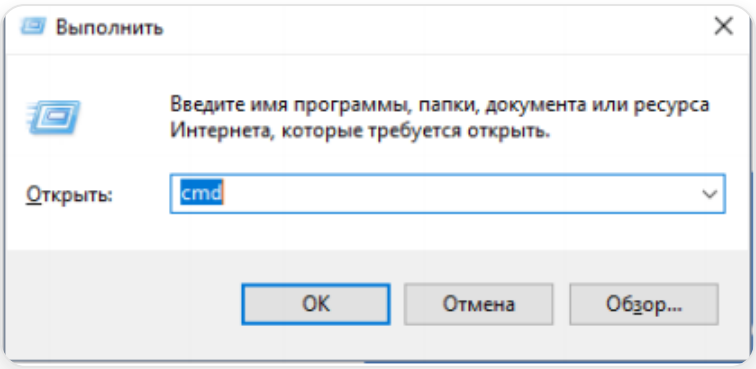
- Отслеживание ошибок на платформе MS Windows
- Отслеживание ошибок на платформе Linux
- Отслеживание ошибок на платформе OS X

Открыть статью на сайте

Отслеживание ошибок на платформе MS Windows

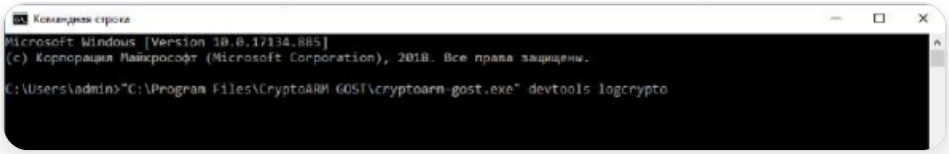
Архив. КриптоАРМ ГОСТ.

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

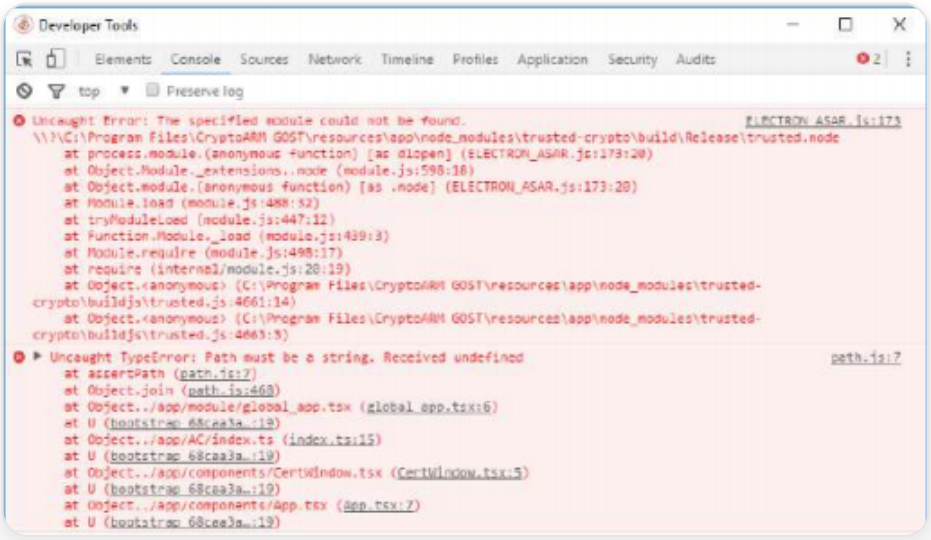


В открывшемся окне ввести команду запуска приложения КриптоАРМ ГОСТ:

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



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



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**.

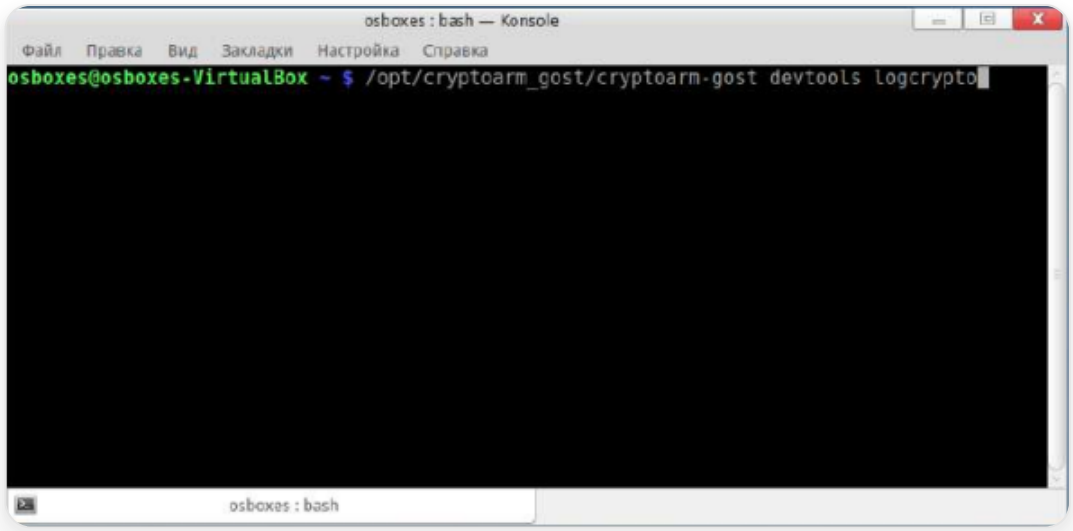
Открыть статью на сайте

Отслеживание ошибок на платформе Linux

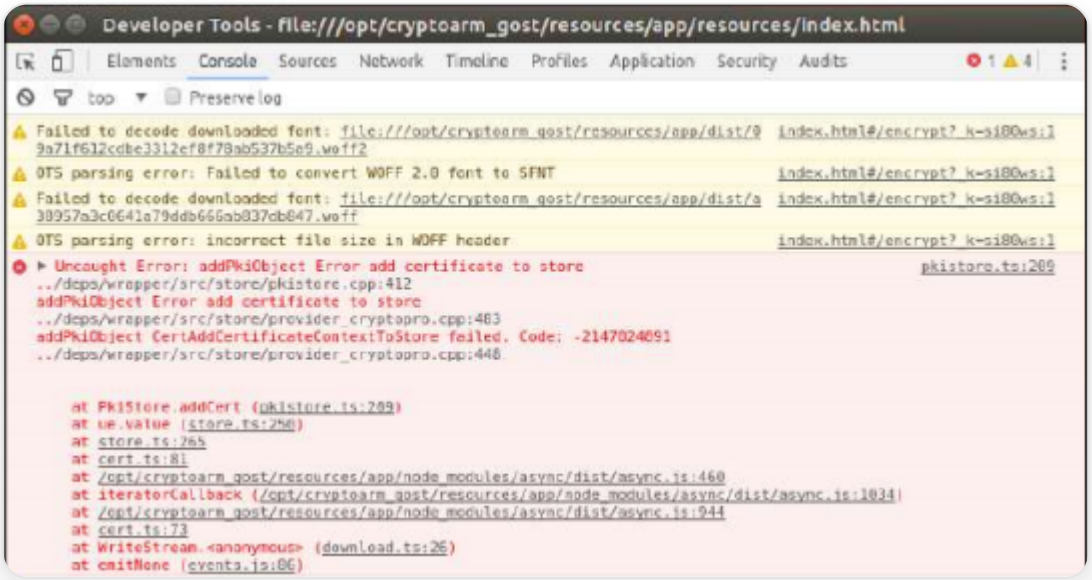
Архив. КриптоАРМ ГОСТ.

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

/opt/cryptoarm_gost/cryptoarm-gost devtools logcrypto



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



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**.

Открыть статью на сайте

Отслеживание ошибок на платформе OS X

Архив. КриптоАРМ ГОСТ.

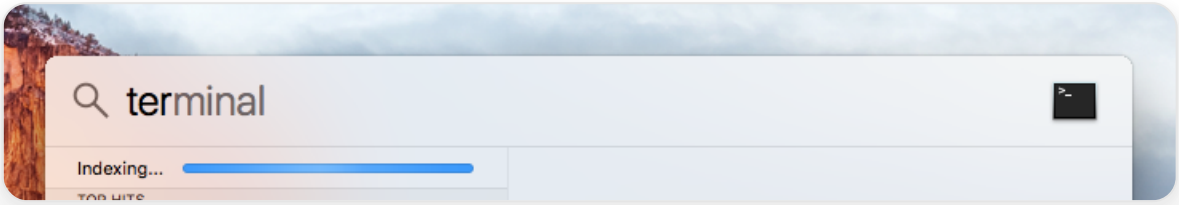
Для получения доступа к дополнительной панели управления приложением и включением режима логирования, в терминале ОС OS X ввести команду:

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

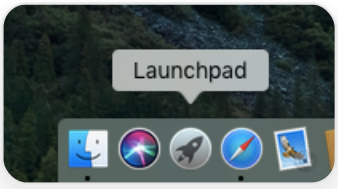
Где найти командную строку

Есть несколько способов:

- Вызовите окно поиска (Cmd + Пробел, на Вашем устройстве может быть установлена другая комбинация), и напишите "Терминал" или "Terminal":

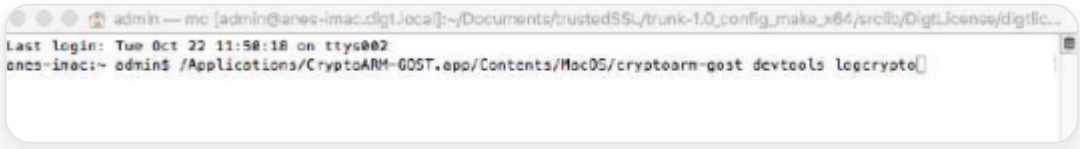


- Другой вариант - найти Терминал в Launchpad:



Там, в папке "Другие", можно найти значок Терминала:





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



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

Открыть статью на сайте

Как подписать и подать проектную документацию в Главгосэкспертизу

Архив. КриптоАРМ ГОСТ.

Главгосэкспертиза консультирует по вопросам проведения экспертизы проектной деятельности, инженерных взысканий, определяет достоверность сметной стоимости объектов строительства, оказывает услуги в сфере ценообразования и сметного нормирования. Экспертные заключения от Главгосэкспертизы также выдаются только в электронном варианте.

Подать документацию можно на сайте Госуслуг и на сайте Главгосэкспертизы. Все документы должны быть подписаны усиленной квалифицированной электронной подписью.

В соответствии с приказом Минстроя России от 21 ноября 2014 г. № 728/пр сметная документация предоставляется в Главгосэкспертизу в формате XML-файла. В случае отсутствия на официальном сайте Минстроя России xml-схемы подлежащей использованию, электронные документы представляются в следующих форматах:

- doc, docx, odt – для документов с текстовым содержанием, не включающим формулы;
- pdf – для документов с текстовым содержанием, в том числе включающих формулы и (или) графические, а также документов с графическим содержанием;
- xls, xlsx, ods – для сводки затрат, сводного сметного расчета стоимости строительства, объектных сметных расчетов (смет), локальных сметных расчетов (смет), сметных расчетов на отдельные виды затрат.

При этом к формированию таких документов установлен ряд требований, в соответствии с которыми они должны:

- формироваться способом, не предусматривающим сканирование документа на бумажном носителе;
- состоять из одного или нескольких файлов, каждый из которых содержит текстовую и (или) графическую информацию;
- обеспечивать возможность поиска по текстовому содержанию документа и возможность копирования текста;
- содержать оглавление и закладки, обеспечивающие переходы по оглавлению и (или) к содержащимся в тексте рисункам и таблицам;
- формироваться для каждого раздела (подраздела) проектной документации и содержать в названии слова “Раздел ПД №”, а также “подраздел ПД №”;
- не превышать предельного размера в 80 мегабайт (в случае превышения предельного размера, документ делится на несколько, название каждого файла дополняется словом “Фрагмент” и порядковым номером файла, полученного в результате деления).

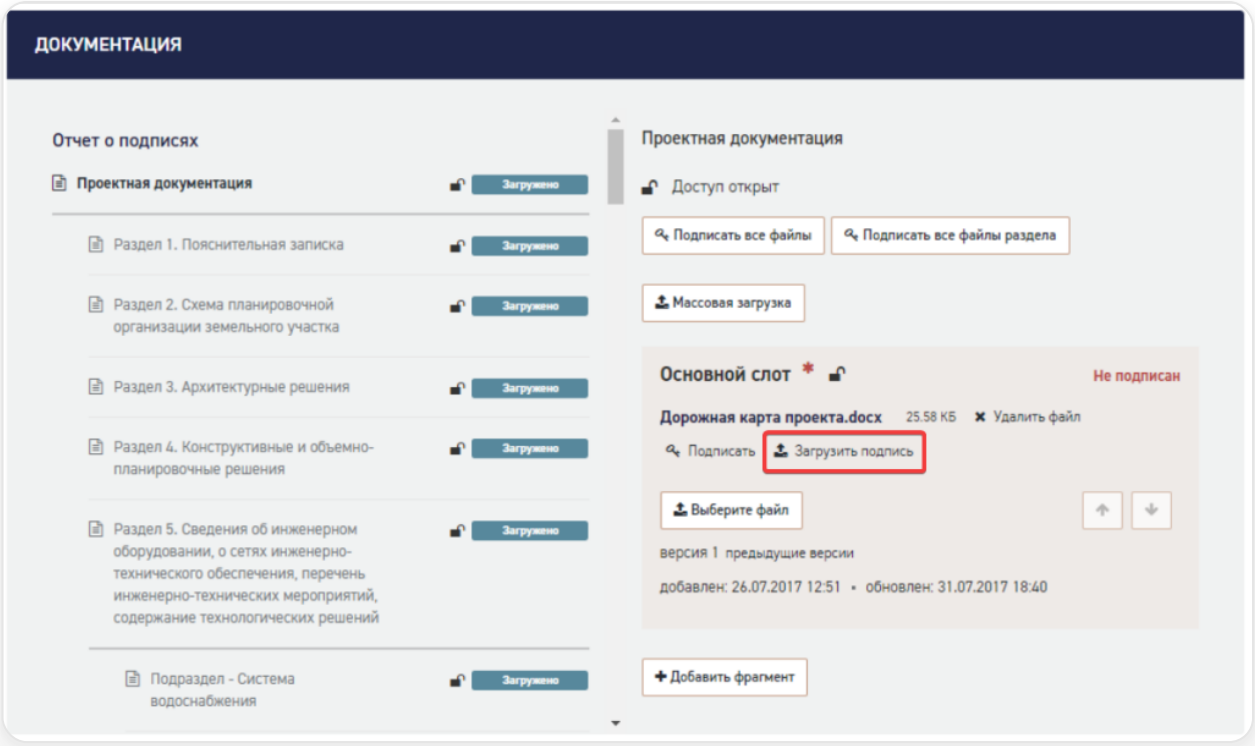
Пошаговая инструкция для подписания проектно-сметной декларации при помощи КриптоАРМ ГОСТ

1. Установите программу КриптоАРМ ГОСТ на свой компьютер, если ее еще нет.
2. Добавьте файлы, нажав на кнопку “+”.
3. В правой боковой панели в разделе “Операции” выберите “Подпись”
4. В разделе “Сертификат подписи” нажмите на кнопу “Выбрать”
5. В разделе “Настройки подписи “ укажите: CMS, Отсоединенная, Base-64
6. Добавьте галочку “Документы просмотрены” и нажмите на “Выполнить”
7. Документы подписаны и доступны для загрузки на сайт Главгосэкспертизы.
8. Готово! Вы успешно подписали проектную декларацию для Главгосэкспертизы с помощью КриптоАРМ ГОСТ.

Как подписать и проверить подпись в КриптоАРМ ГОСТ 2.5

На портале Главгосэкспертизы в целом существуют три способа для подписания и отправки проектно-сметной документации:

- загрузить подписанный файл;
- подписать файл в браузере (кнопка [Подписать]);
- загрузить файл подписи (кнопка [Загрузить подпись]).



Можно загрузить документ одним файлом с присоединенной подписью, можно загрузить неподписанные файлы и подписать их в браузере при помощи специального плагина, а можно как в данной инструкции прикрепить документ и файл подписи.

Открыть статью на сайте

Как подписать документы в МоемСкладе мобильной электронной подписью

Архив. КриптоАРМ ГОСТ.

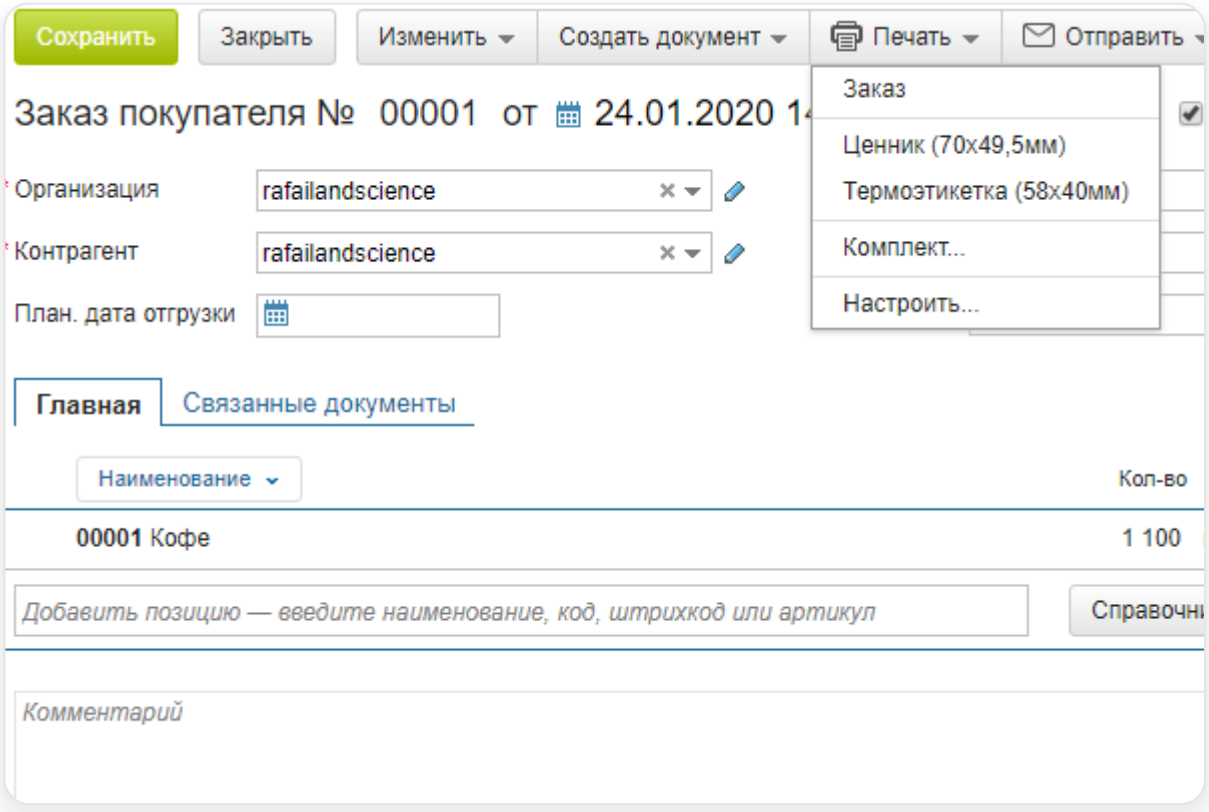
МойСклад - это облачный сервис для управления торговлей. Это товароучётная база и планировщик задач. В системе МойСклад также можно составлять и вести торговую документацию на предприятии.

Иногда для обмена документацией с контрагентами необходим только электронный вариант документа, а для его подписи недостаточно факсимиле, и нужна квалифицированная электронная подпись (КЭП). Подписывать документы КЭП можно, используя мобильную подпись от Билайн и программу для подписи и шифрования документов КриптоАРМ ГОСТ.

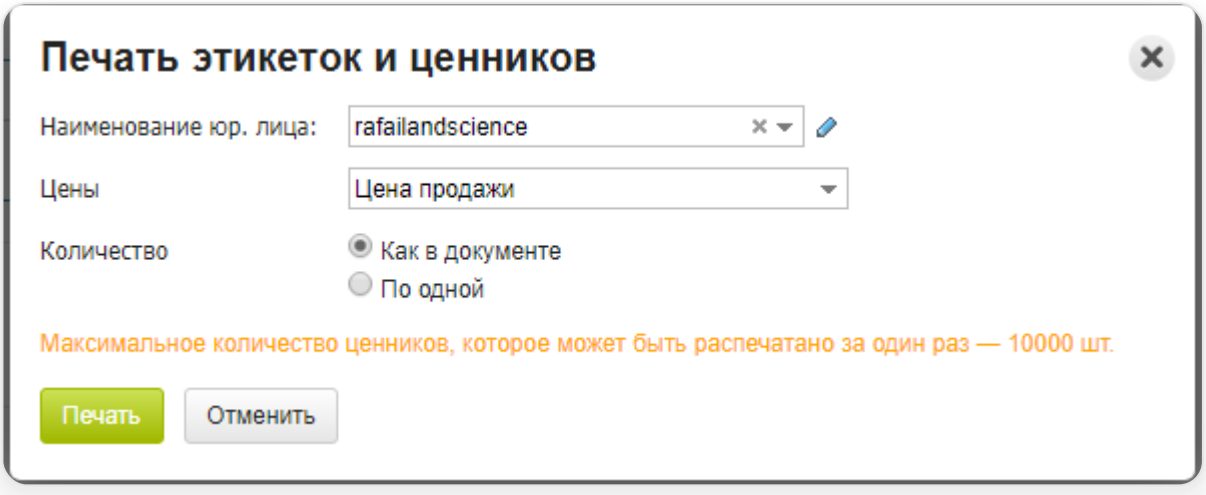
Рассмотрим пошагово, как подписать ЭП любой документ из МоегоСклада мобильной подписью:

1. Откройте документ на МоемСкладе и нажмите кнопку **“Печать”**.

2. В выпадающем списке выберите пункт **“Создание печатной формы”** или тип документа, который нужно составить.



3. Откроется окно подтверждения печати. Нажмите **“Печать”**.

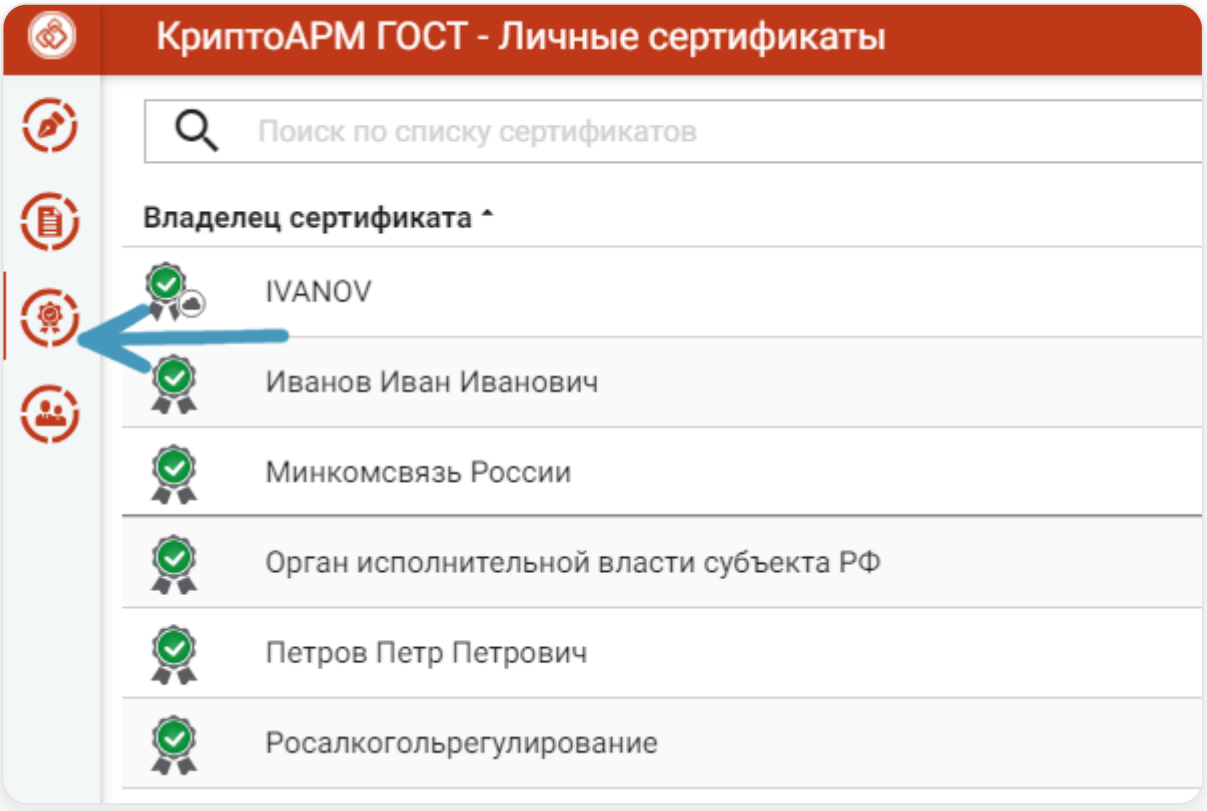


4. Документ загрузится в формате PDF. Загрузка должна произойти автоматически.

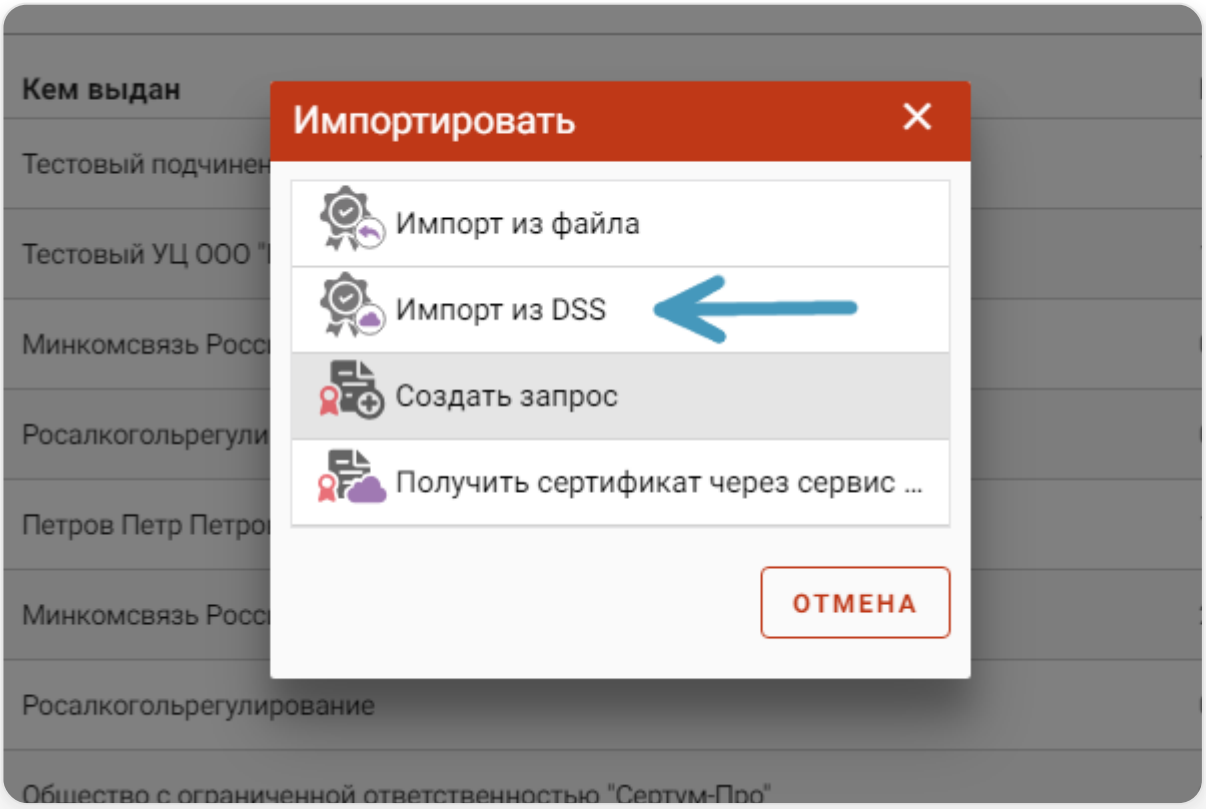
Чтобы установить облачную подпись Билайн в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.

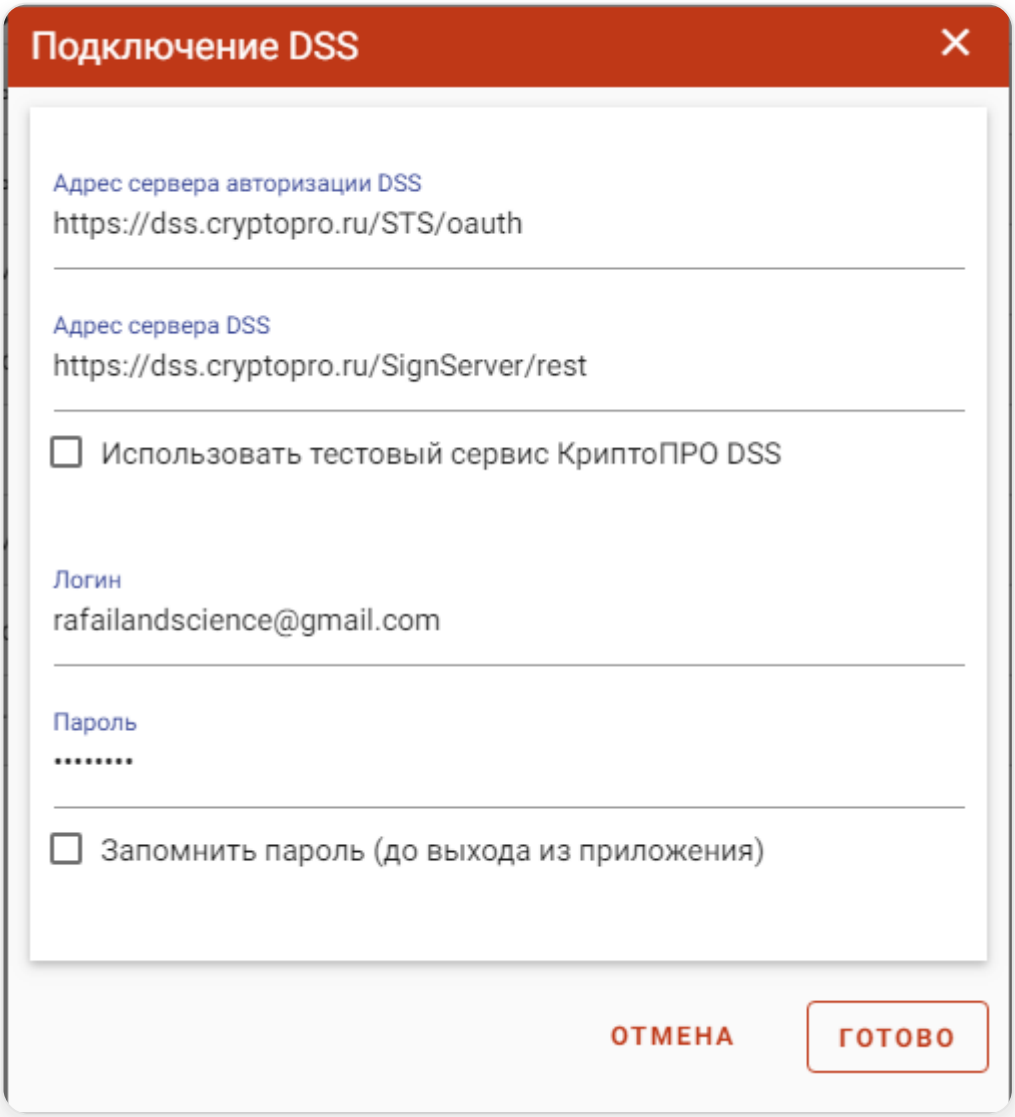
2. В контекстном меню программы зайдите на вкладку **“Сертификаты”**.



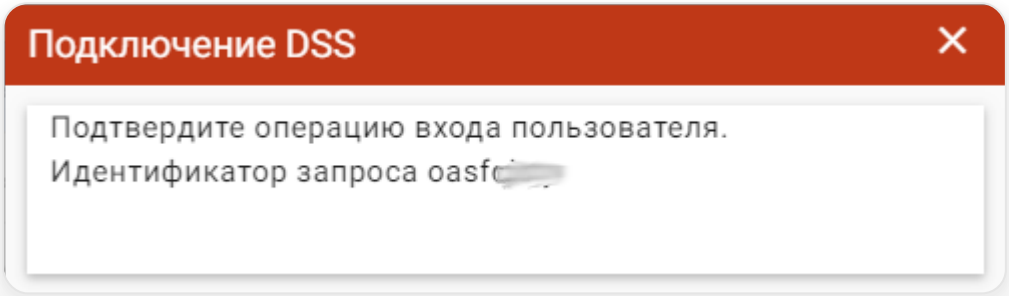
3. Нажмите на кнопку **“+”**, чтобы добавить сертификат, и выберите пункт **“Импорт из DSS”**.

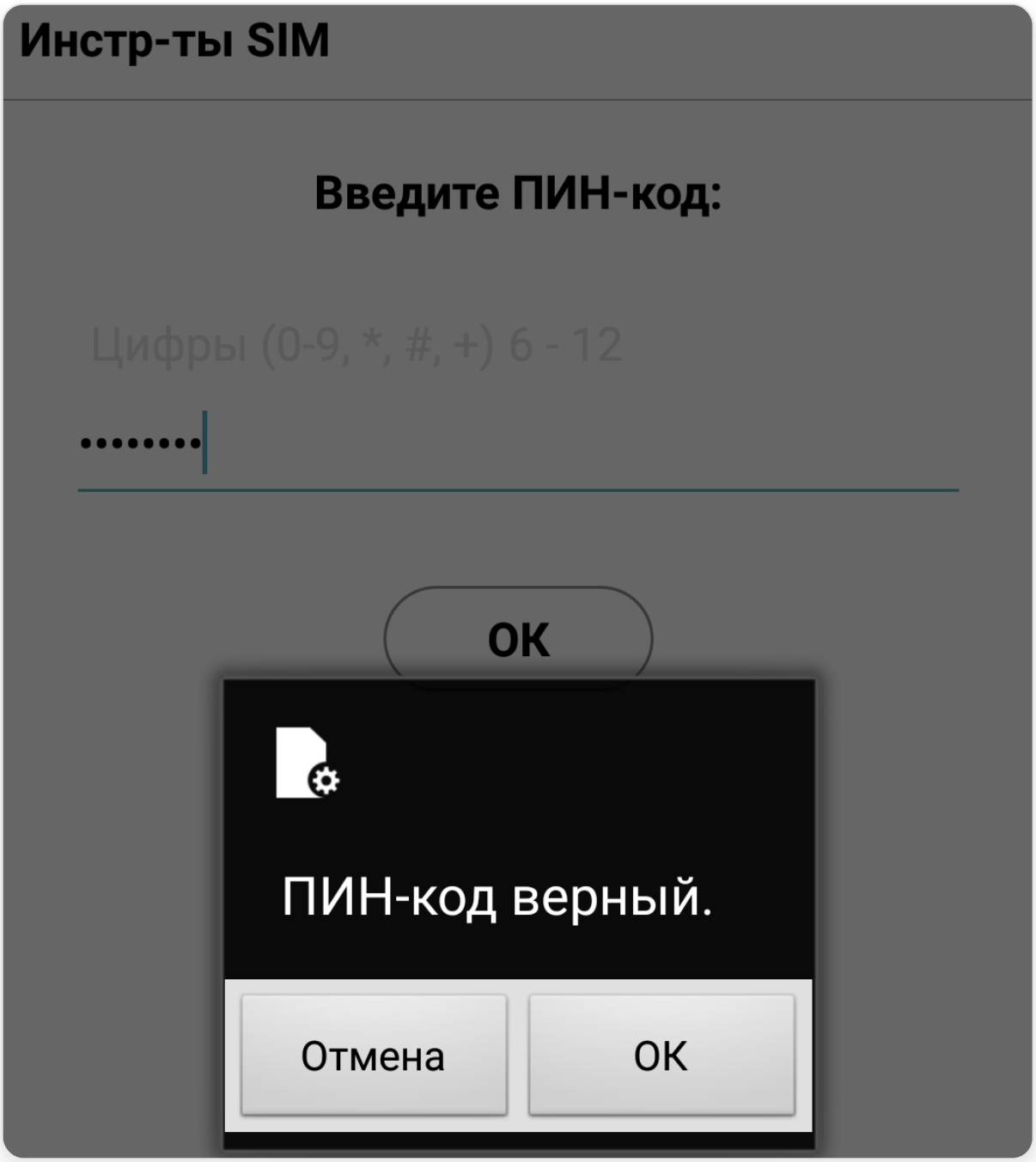


4. Введите адреса **“Сервера авторизации” и “Сервера DSS”**, а затем **логин и пароль** для авторизации на сервере.



5. Подтвердите добавление подписи в КриптоАРМ ГОСТ. **Сверьте идентификаторы и введите ПИН-код** на телефоне, когда придёт всплывающее уведомление.



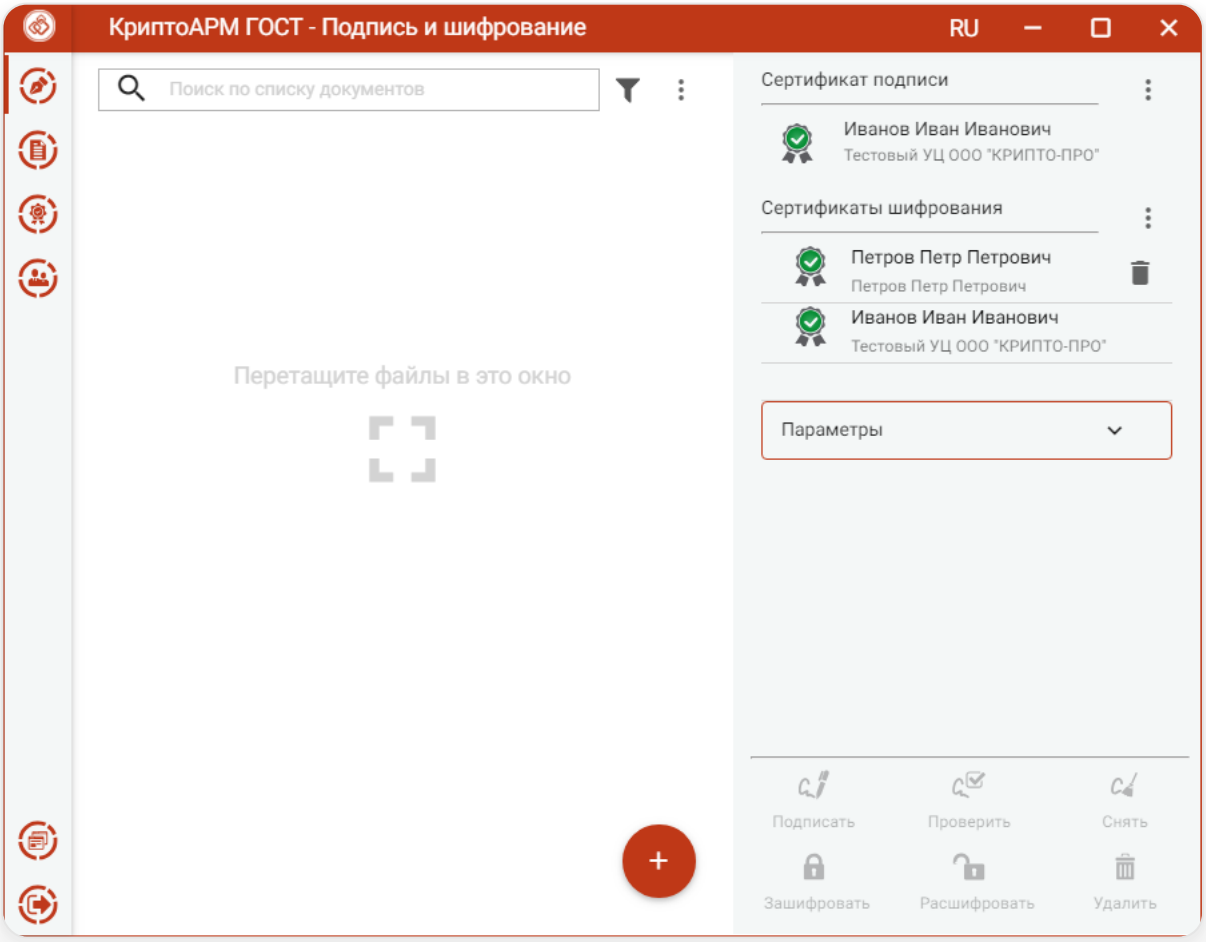


6. Нажмите на кнопку **“Готово”**. Сертификат импортируется в Ваше личное хранилище сертификатов и будет помечен иконкой с облаком. Издатель: ПАО “Вымпелком”.

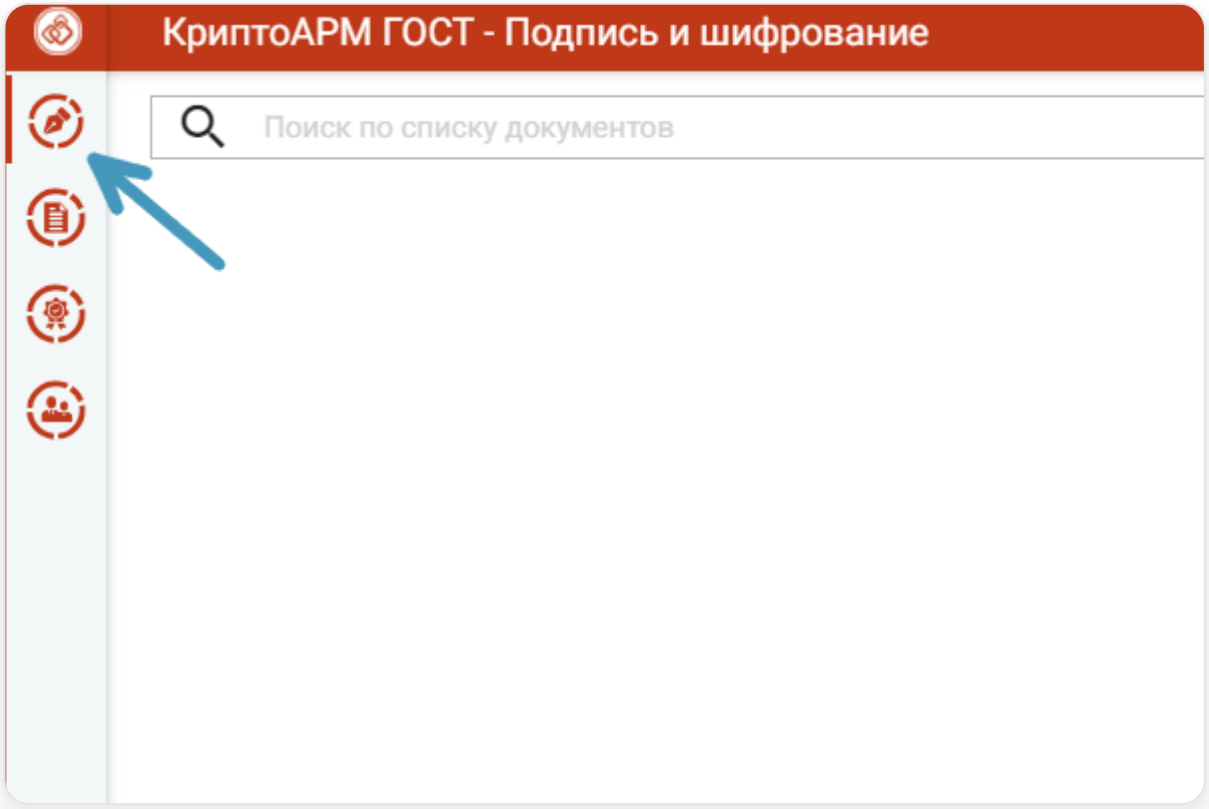
   После успешного импорта сертификата им можно подписывать файлы так же, как и остальными.

Чтобы подписать загруженный из МоегоСклада документ в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.


КриптоАРМ ГОСТ - Подпись и шифрование
RU
Поиск по списку документов
Перетащите файлы в это окно
Сертификат подписи
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
Сертификаты шифрования
Петров Петр Петрович
Петров Петр Петрович
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
Параметры
Подписать
Проверить
Снять
Зашифровать
Расшифровать
Удалить

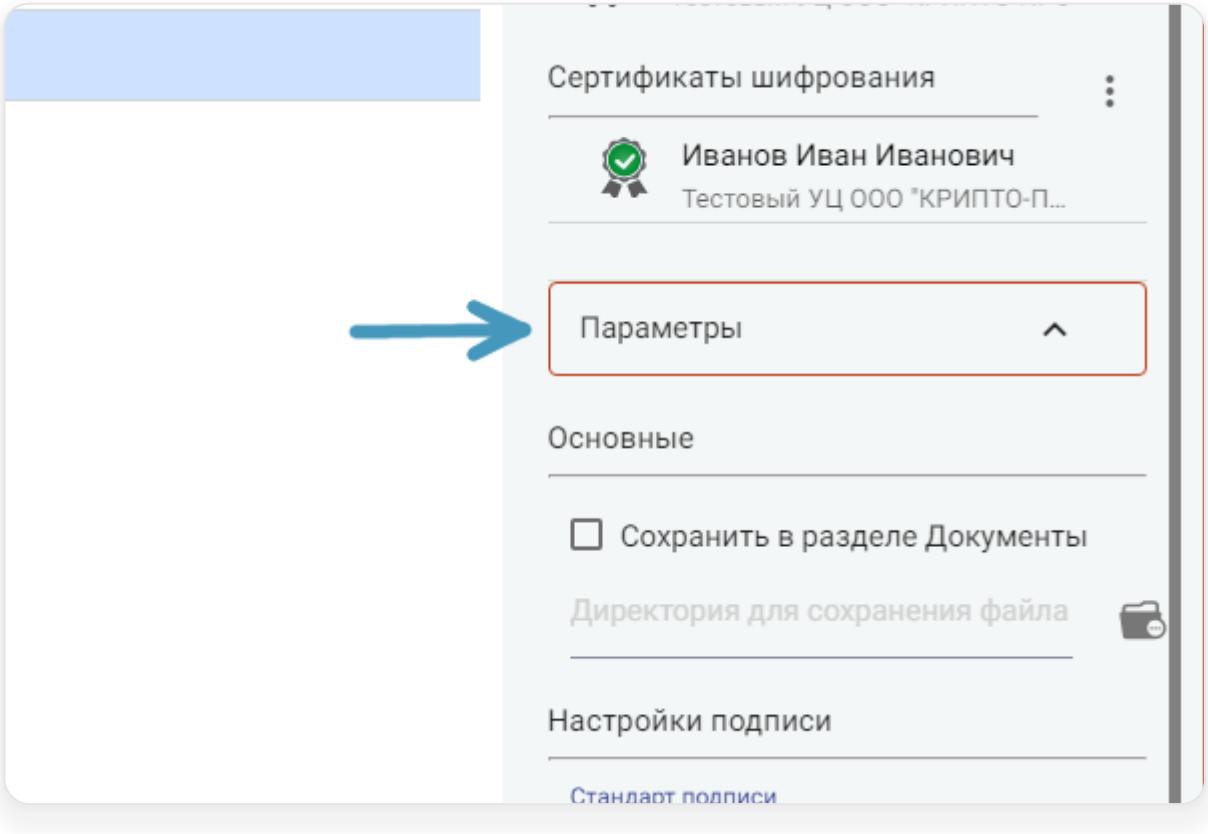
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

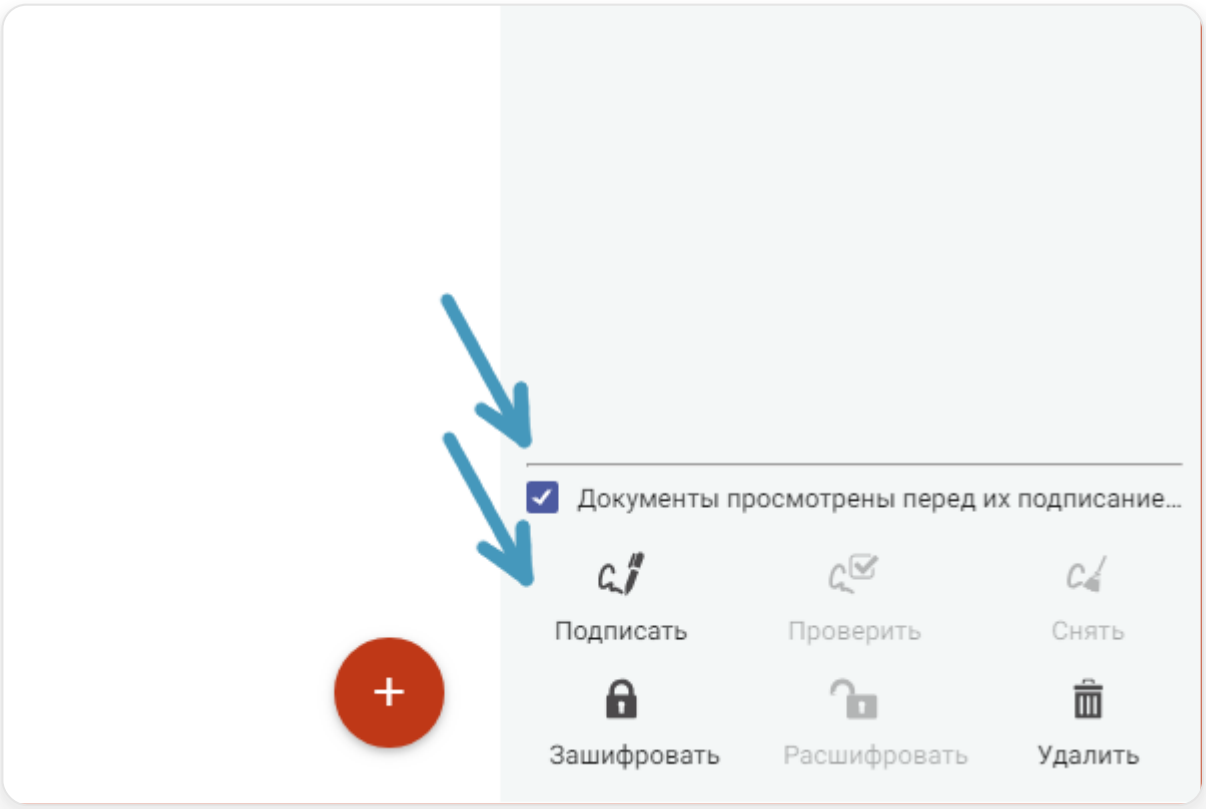
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.



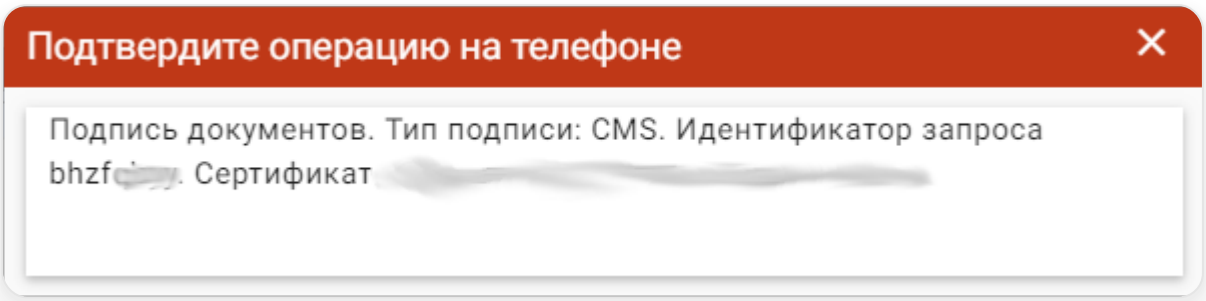
6. Нажмите кнопку **“Заменить”** в контекстном меню настроек подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

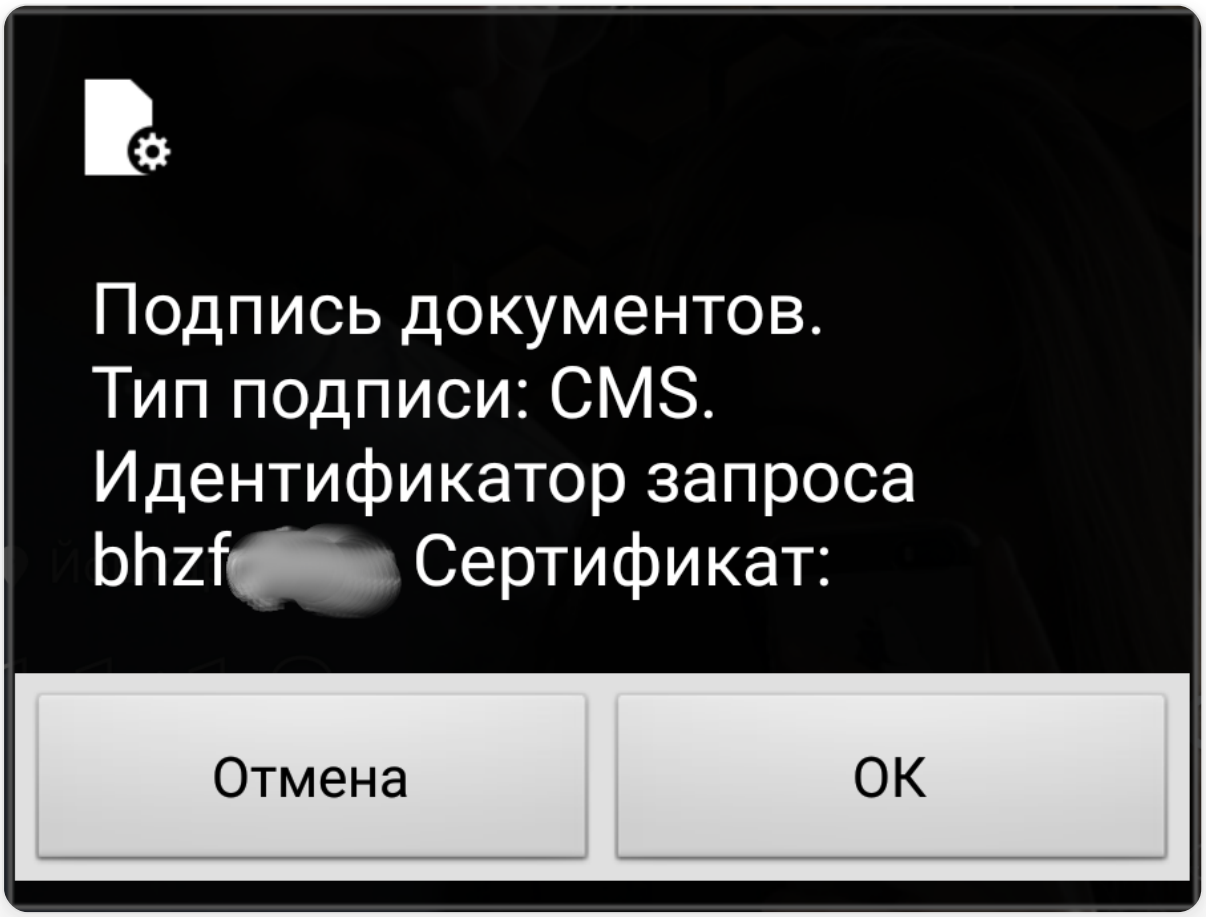
7. Выберите облачный сертификат Билайн DSS и нажмите кнопку **“Выбрать”**.

8. Выберите флаг **“Документы просмотрены перед их подписанием”**.

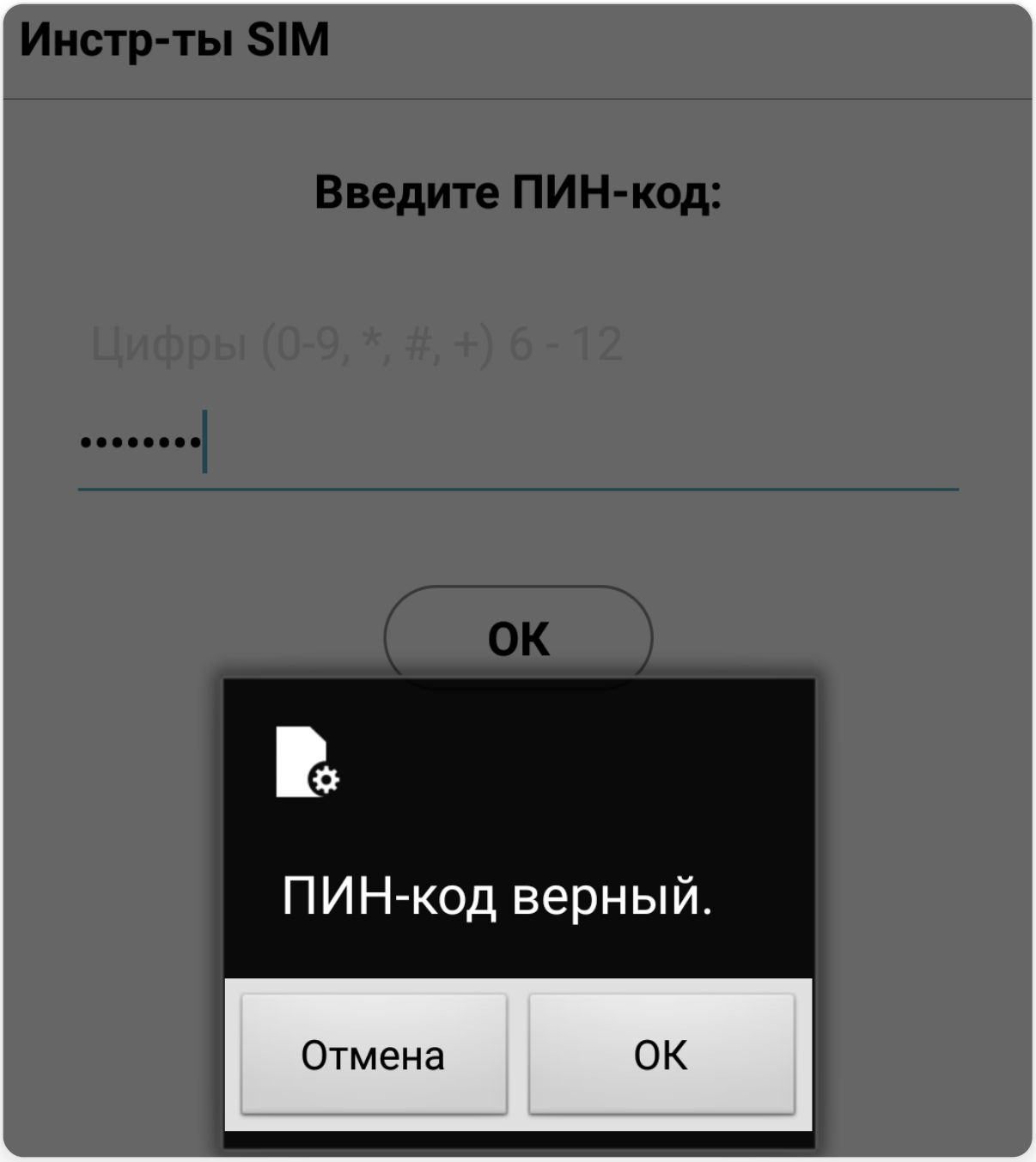


9. Нажмите на кнопку **“Подписать”**. Появится уведомление о том, что нужно подтвердить операцию на телефоне. На телефоне появится всплывающее уведомление о подтверждении операции подписи. **Сверьте идентификаторы и нажмите “ОК”.**




Подпись документов.
Тип подписи: CMS.
Идентификатор запроса
bhzf
Сертификат:
Отмена
OK

10. **Введите ПИН-код**, подтверждающий подпись. Если ПИН-код не был задан, этот шаг пропускается. Нажмите “ОК”.



11. Документ будет подписан. В приложении КриптоАРМ ГОСТ сменятся статус и иконка документа.

    Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.

Открыть статью на сайте

Как обмениваться документами с электронной подписью

Архив. КриптоАРМ ГОСТ.

Электронный документооборот (ЭДО) - это обмен документацией в электронном виде, без использования бумажных носителей. Для организации ЭДО используются электронные подписи и шифрование документов.

Корпоративный электронный документооборот включает в себя внутренний и внешний ЭДО. Внутренний ЭДО используется для обмена документацией и контроля выполнения задач внутри компании, а внешний ЭДО используется для обмена документацией с контрагентами. Чтобы придать ему юридическую значимость, нужно выполнить несколько шагов.

Чтобы самостоятельно юридически организовать ЭДО, нужно:

1. Подписать соглашение об ЭДО с контрагентами согласно Федеральному закону от 06.04.11 г. №63-ФЗ “Об электронной подписи”;
2. Определить лицо, ответственное за подпись электронных документов, и составить приказ о его назначении на эту должность;
3. Получить квалифицированную электронную подпись (КЭП) согласно Федеральному закону от 06.04.11 г. №63-ФЗ “Об электронной подписи”;
4. Получить сертификат ключа проверки электронной подписи юридического лица в аккредитованном удостоверяющем центре;
5. Приобрести средство электронной подписи (например, КриптоАРМ ГОСТ) которое должно быть сертифицировано ФСБ России и должно уметь подписывать пакеты файлов (например, архивы .rar и .zip), автоматически создавать и проверять электронные подписи;
6. Определить сроки хранения электронных документов, идентичные срокам хранения бумажных аналогов.

При этом в ЭДО должны использоваться квалифицированные электронные подписи (КЭП) - это подписи, которые выдаются Удостоверяющими центрами, прошедшими аккредитацию Минкомсвязи РФ. Такие подписи используются в работе с госорганами и в ведении внешнего и внутреннего ЭДО.

При использовании КЭП не нужно заключать договор, удостоверяющий её подлинность, как при использовании простой или неквалифицированной электронной подписи, она имеет юридическую силу без дополнительных условий. Квалифицированная подпись гарантирует юридическую значимость документооборота.

Чтобы подписывать электронные документы с помощью КЭП, понадобятся установленные средство подписи и шифрования КриптоАРМ ГОСТ и криптопровайдер КриптоПро.

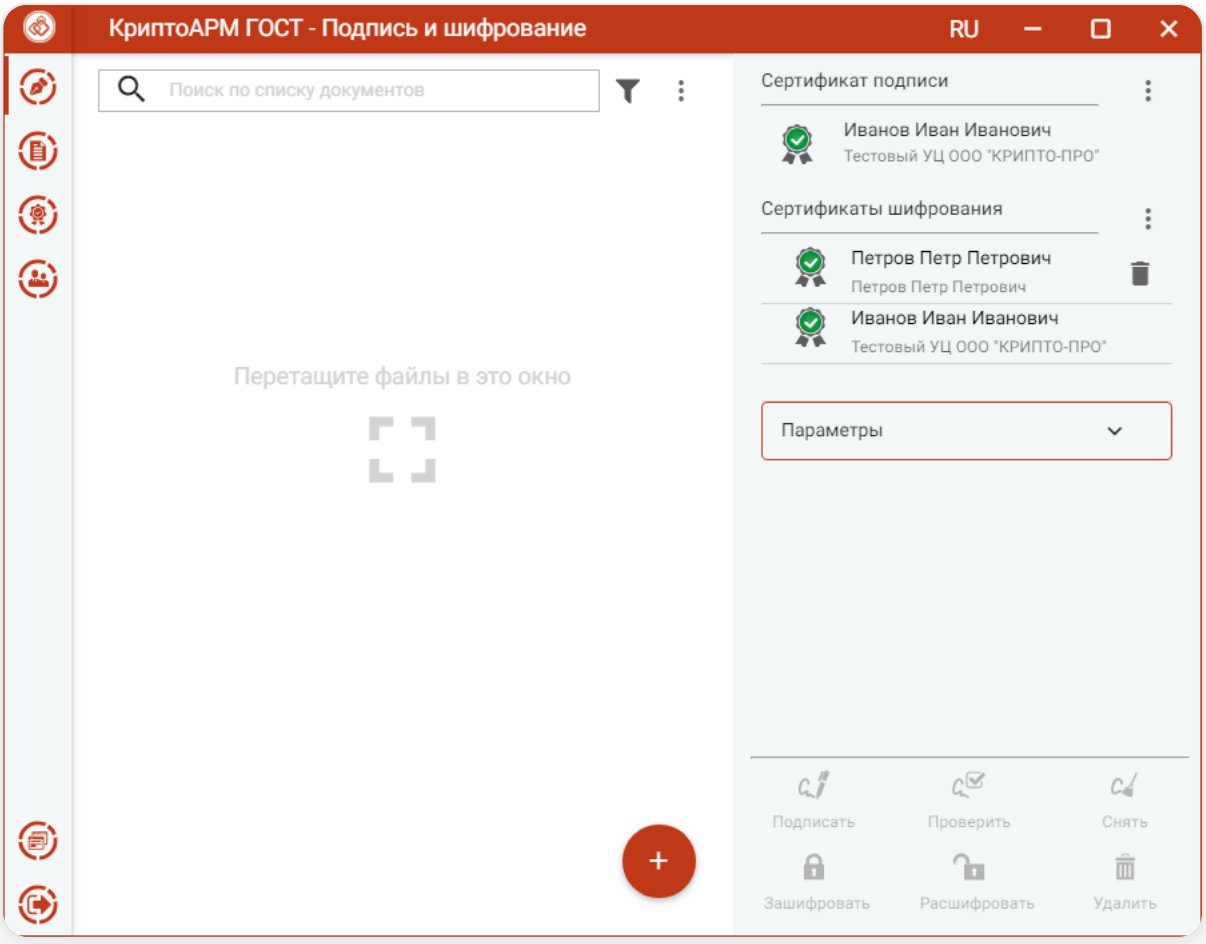
В КриптоАРМ ГОСТ можно подписывать документы электронной подписью и шифровать файлы. Шифрование файлов необходимо, чтобы исключить вмешательство нежелательных лиц в документооборот. Зашифровать документ можно с помощью сертификата открытого ключа КЭП.

Что нужно для подписи файлов:

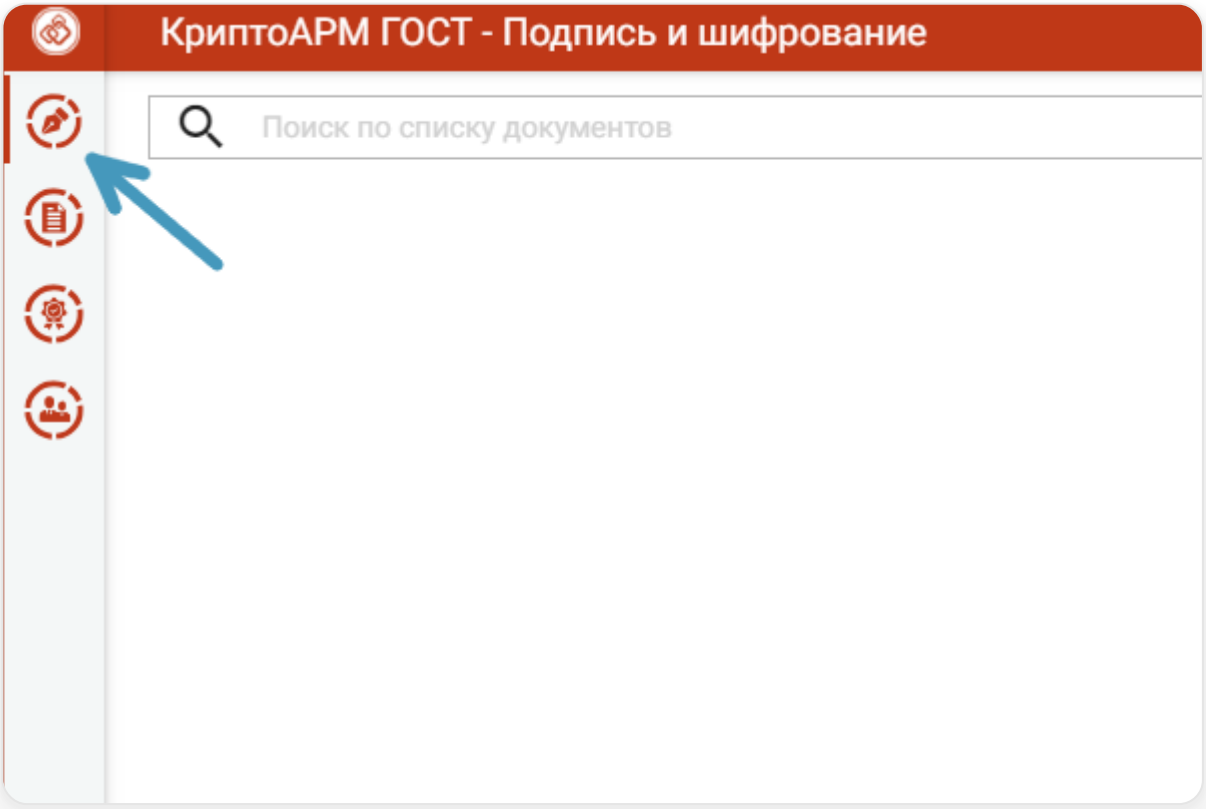
1. КриптоАРМ ГОСТ;
2. КриптоПро CSP;
3. Сертификат электронной подписи.

Чтобы подписать документ в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.



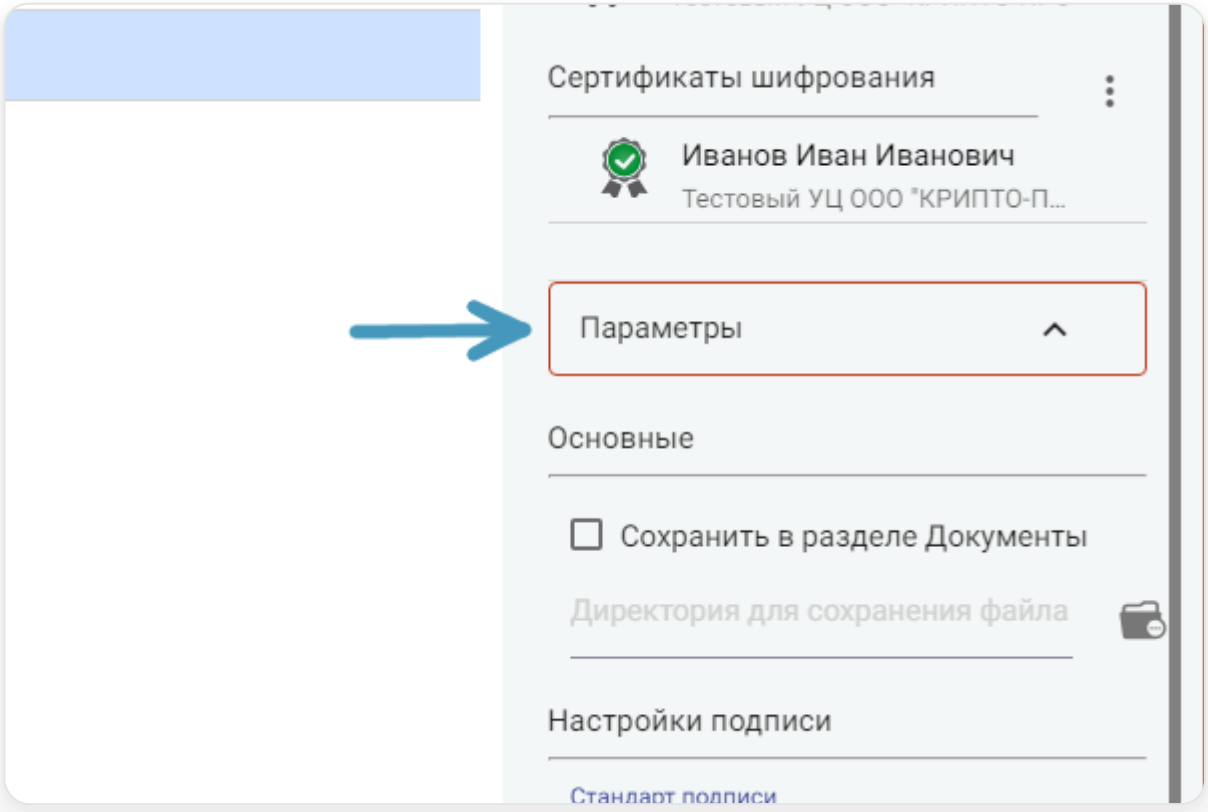
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



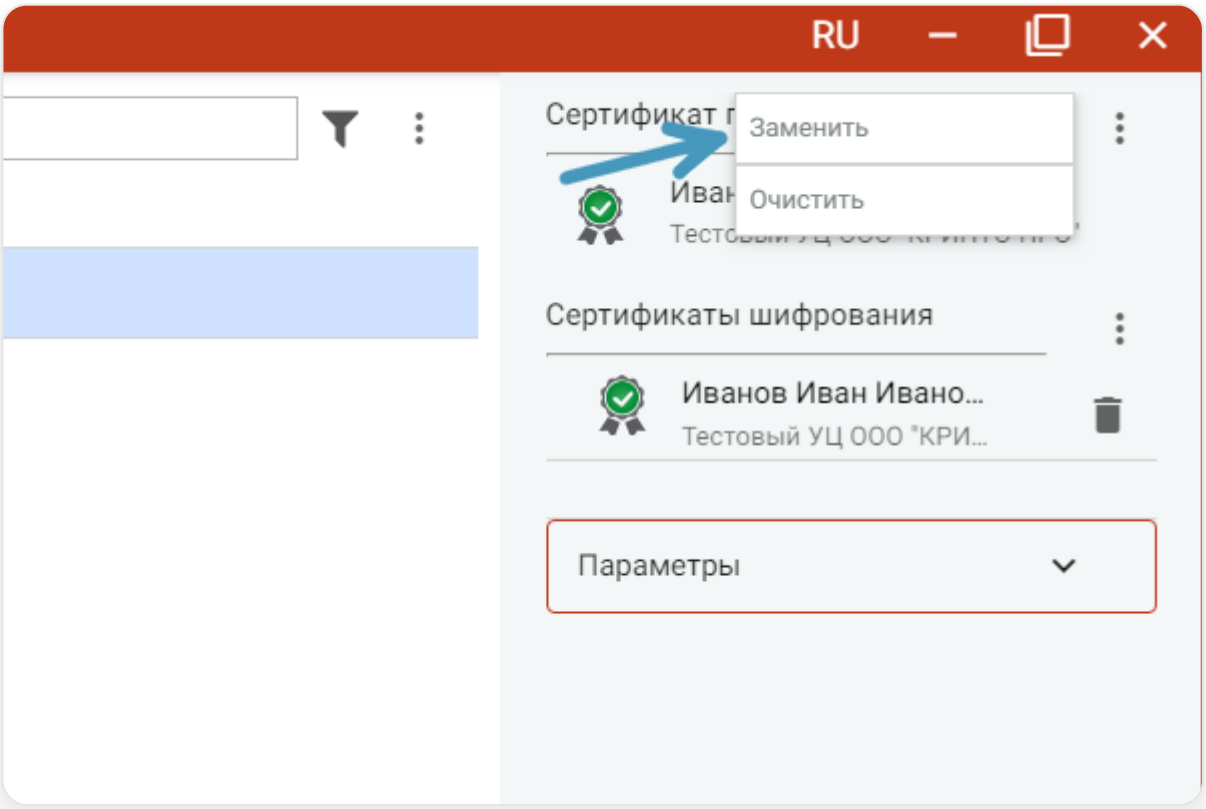
3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

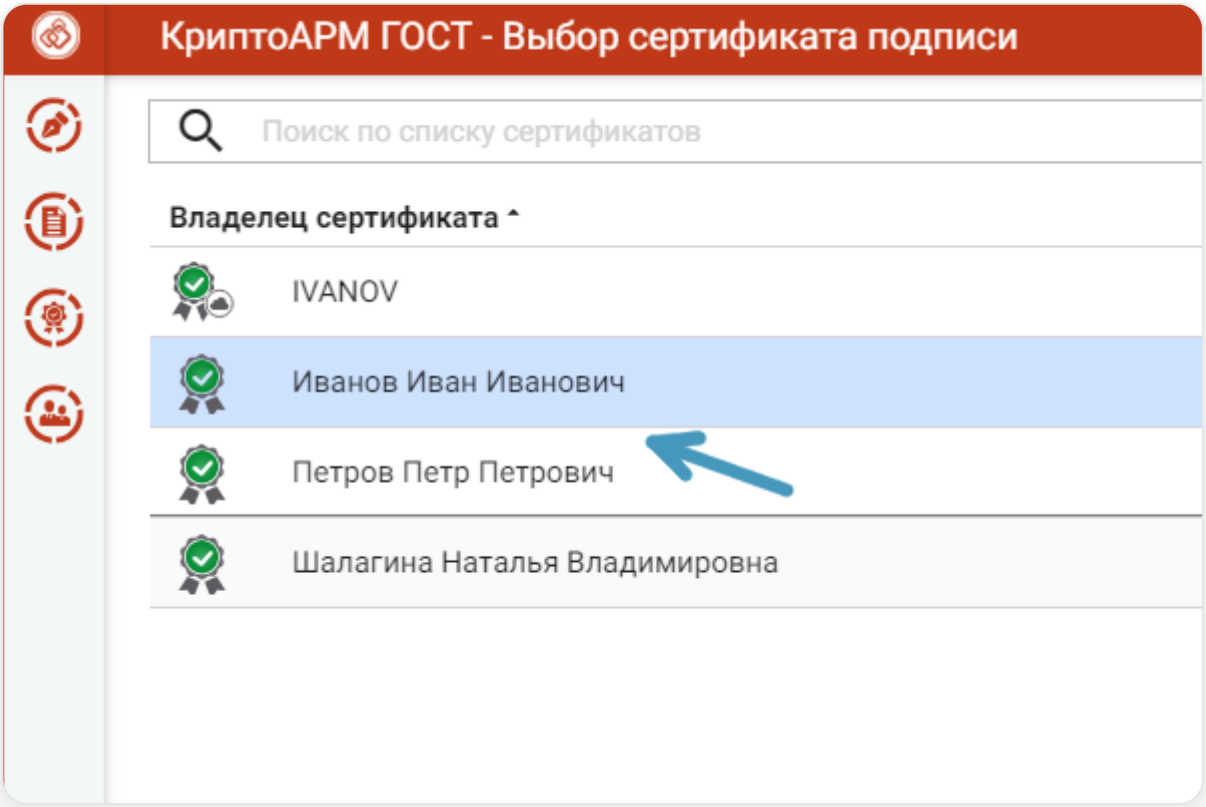
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.

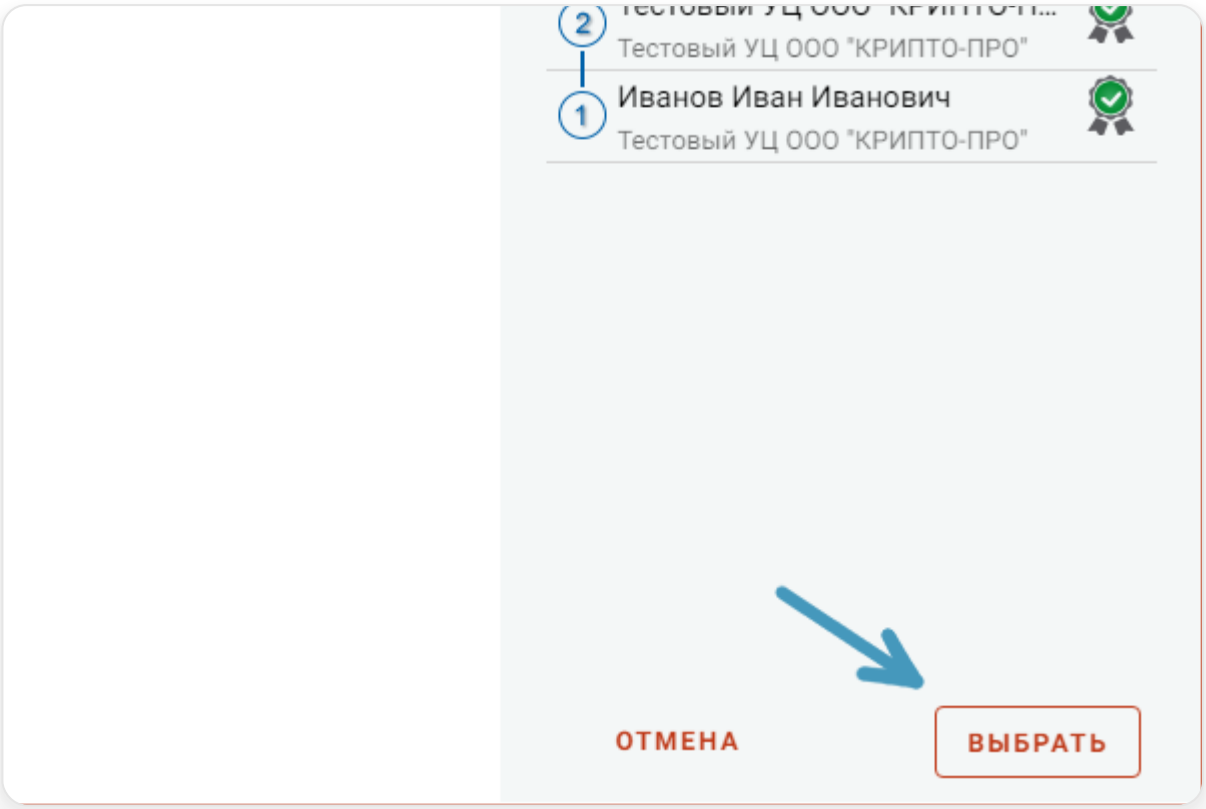


6. Выберите сертификат подписи. Если Вы не хотите использовать сертификат по умолчанию, нажмите кнопку **“Заменить”** в контекстном меню подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

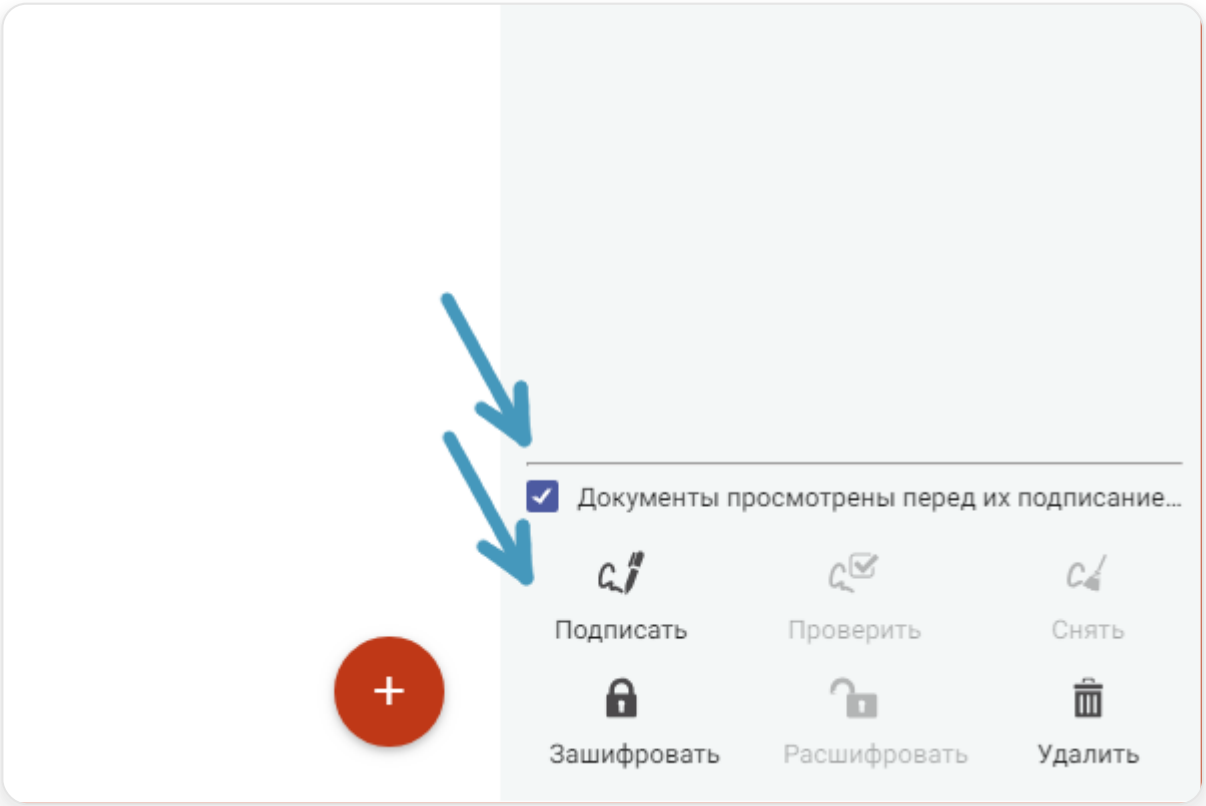


7. Выберите нужный сертификат и нажмите кнопку **“Выбрать”**.


КриптоАРМ ГОСТ - Выбор сертификата подписи
Поиск по списку сертификатов
Владелец сертификата
IVANOV
Иванов Иван Иванович
Петров Петр Петрович
Шалагина Наталья Владимировна

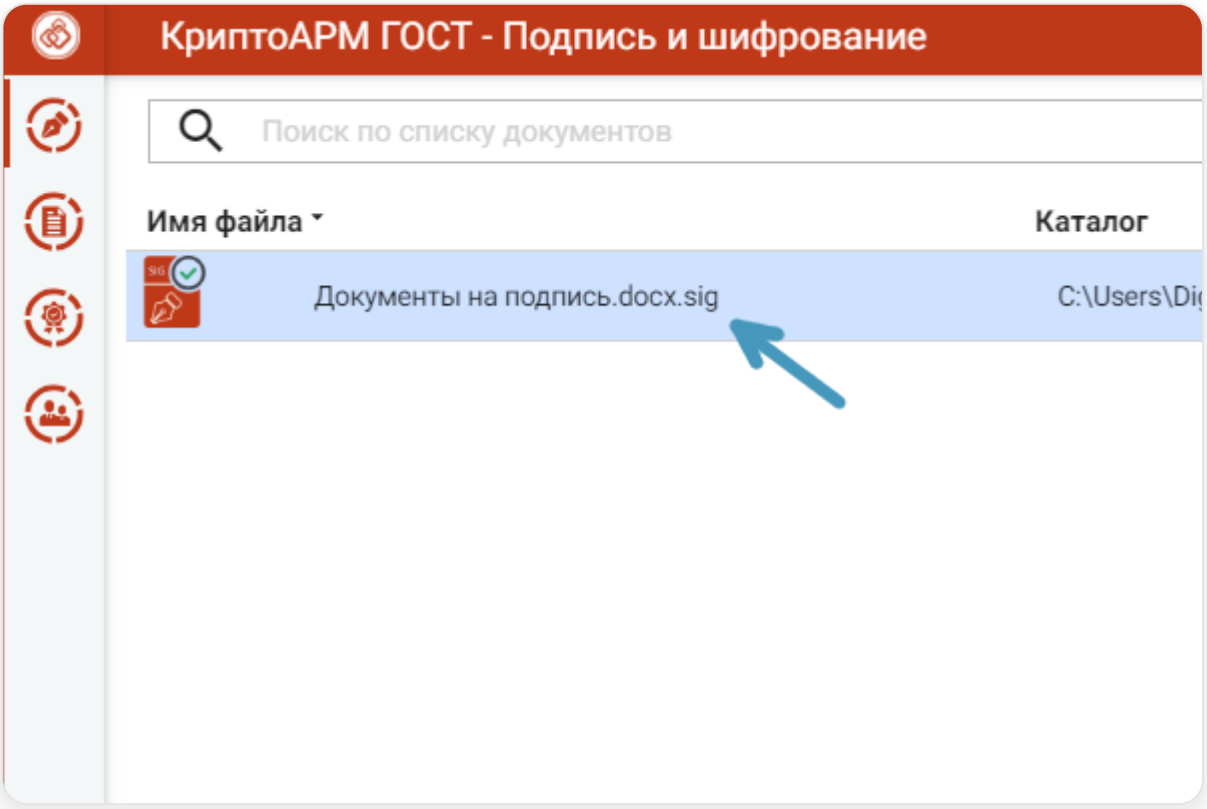

2
Тестовый УЦ ООО "КРИПТО-ПРО"
1
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
ОТМЕНА
ВЫБРАТЬ

8. Выберите флаг **“Документы просмотрены перед их подписанием”.**



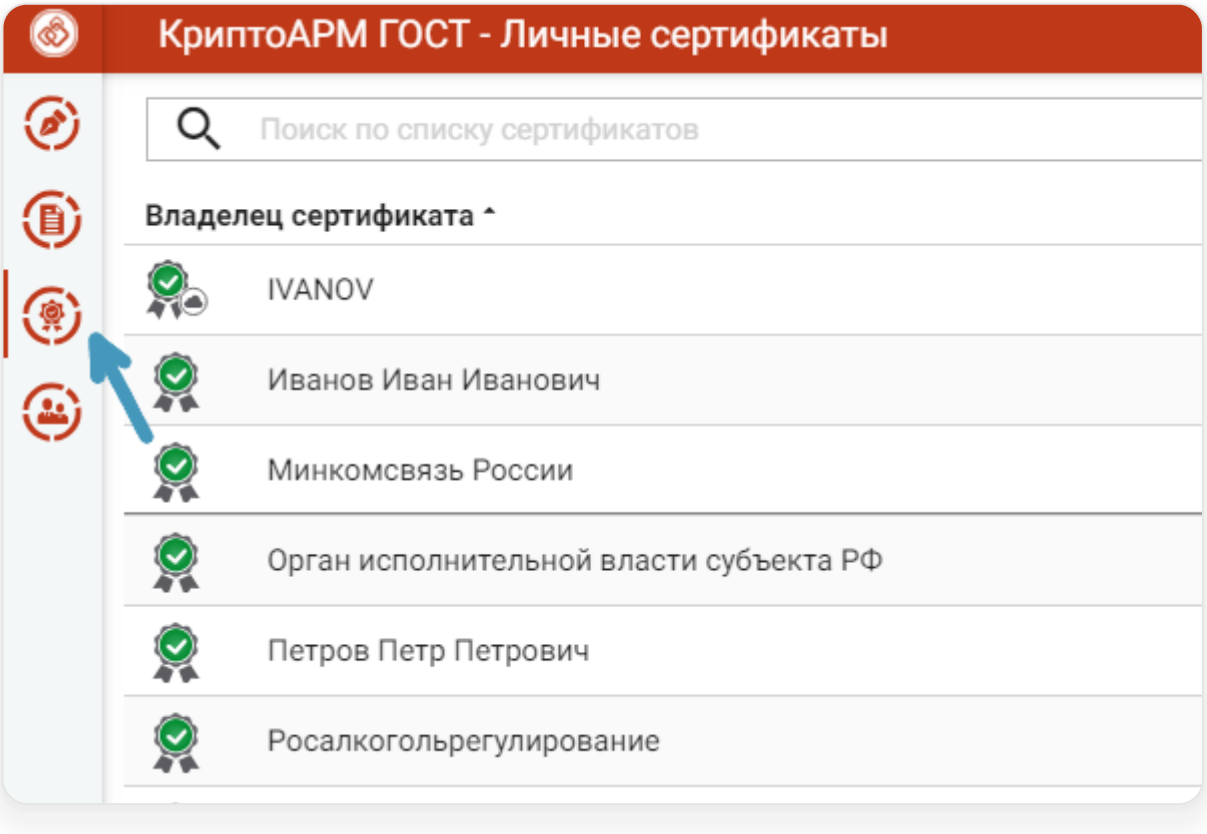
9. Нажмите на кнопку **“Подписать”**.

10. Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.

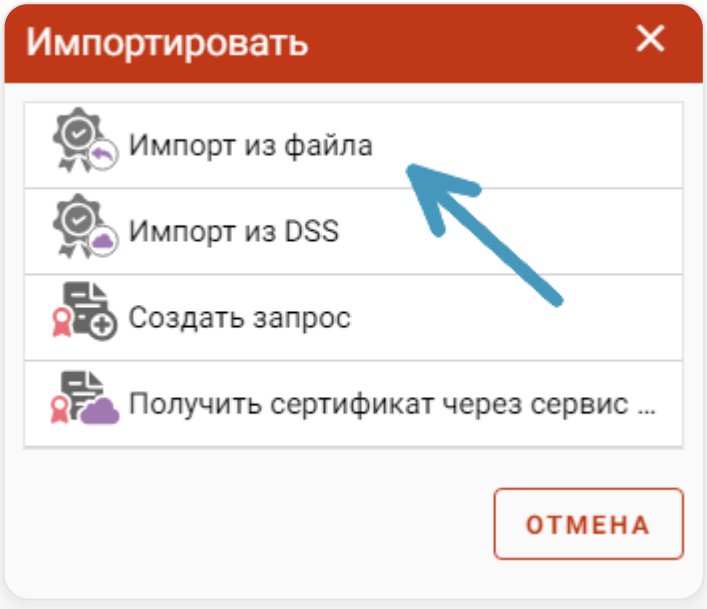


Чтобы зашифровать документ в КриптоАРМ ГОСТ:

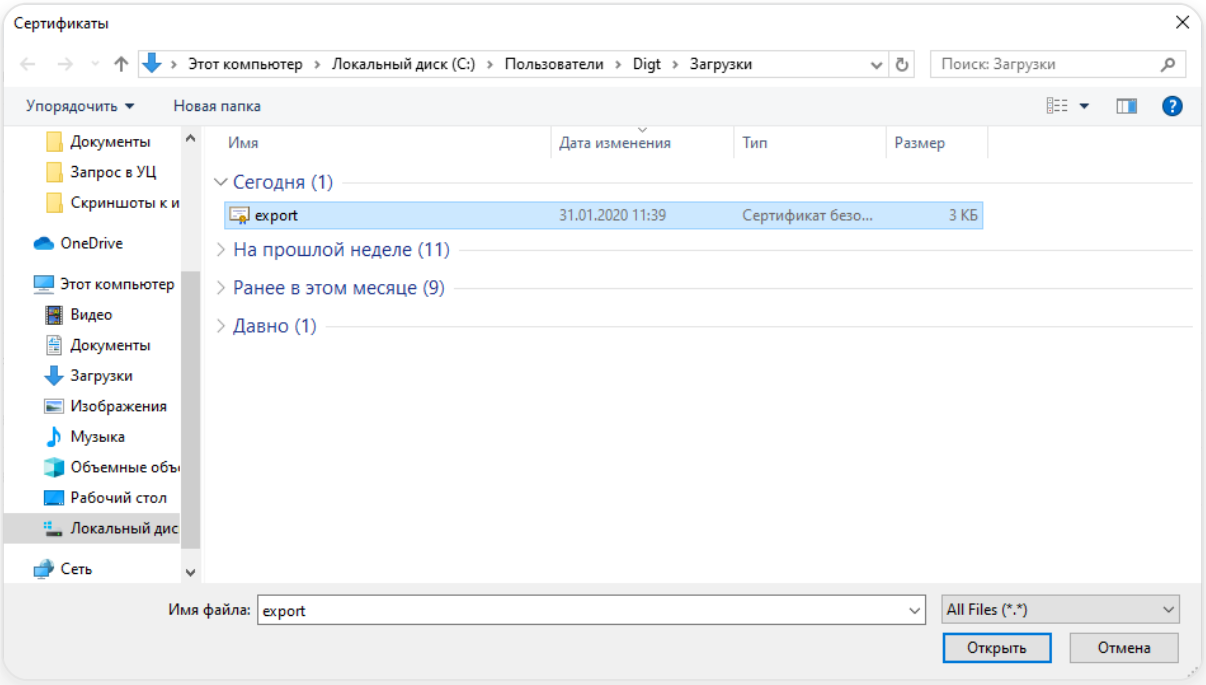
1. Выберите сертификат шифрования. Для этого скачайте сертификат подписи получателя, перейдите в раздел меню **“Сертификаты”**.



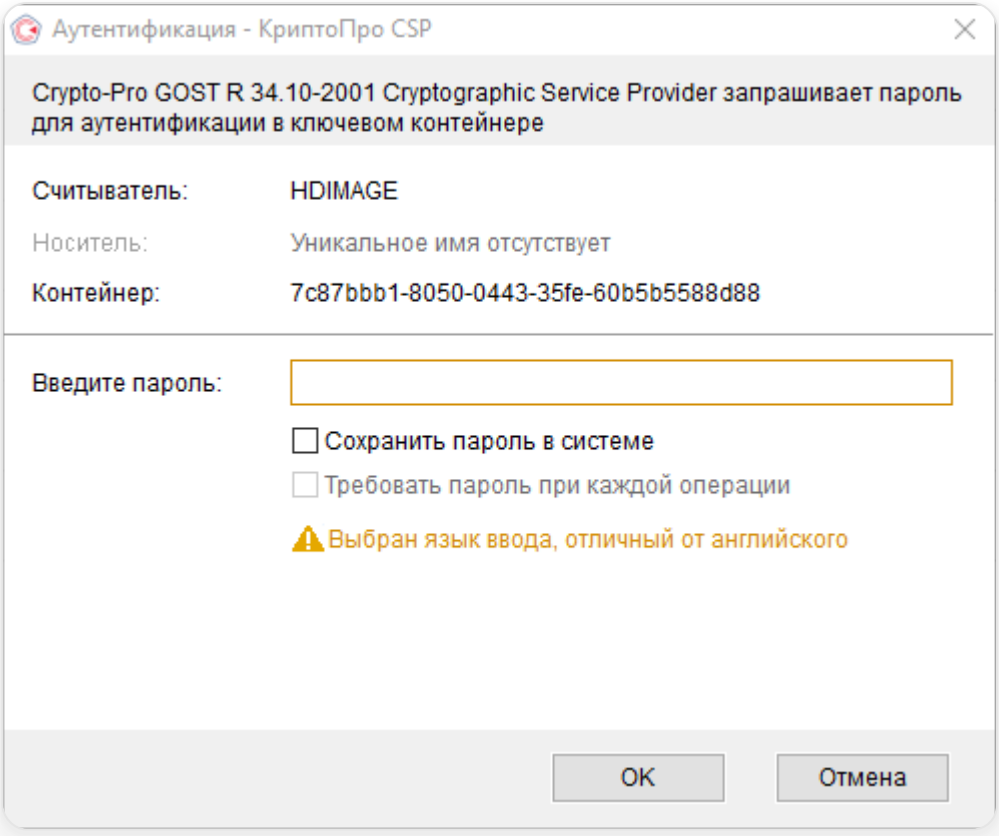
2. Нажмите кнопку **“+”**. В появившемся меню выберите пункт **“Импорт из файла”**.



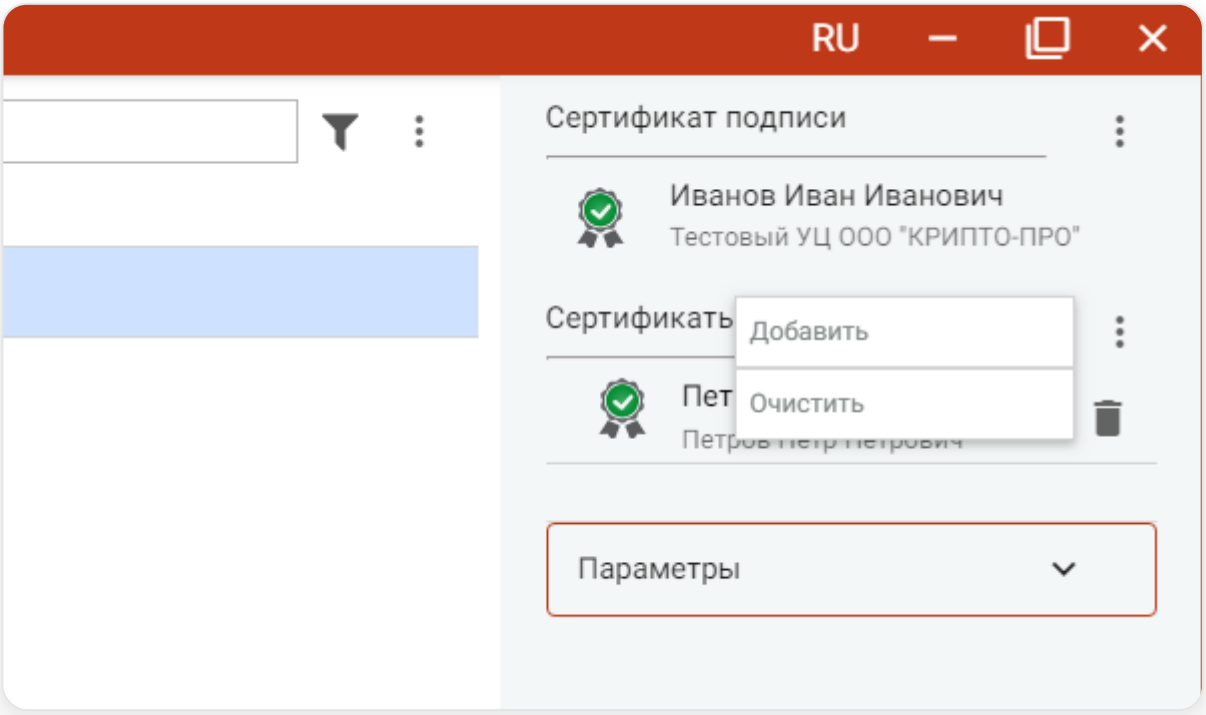
3. Найдите скачанный сертификат получателя и нажмите **“Открыть”**.



4. Введите пароль к контейнеру сертификата и нажмите **“OK”**.



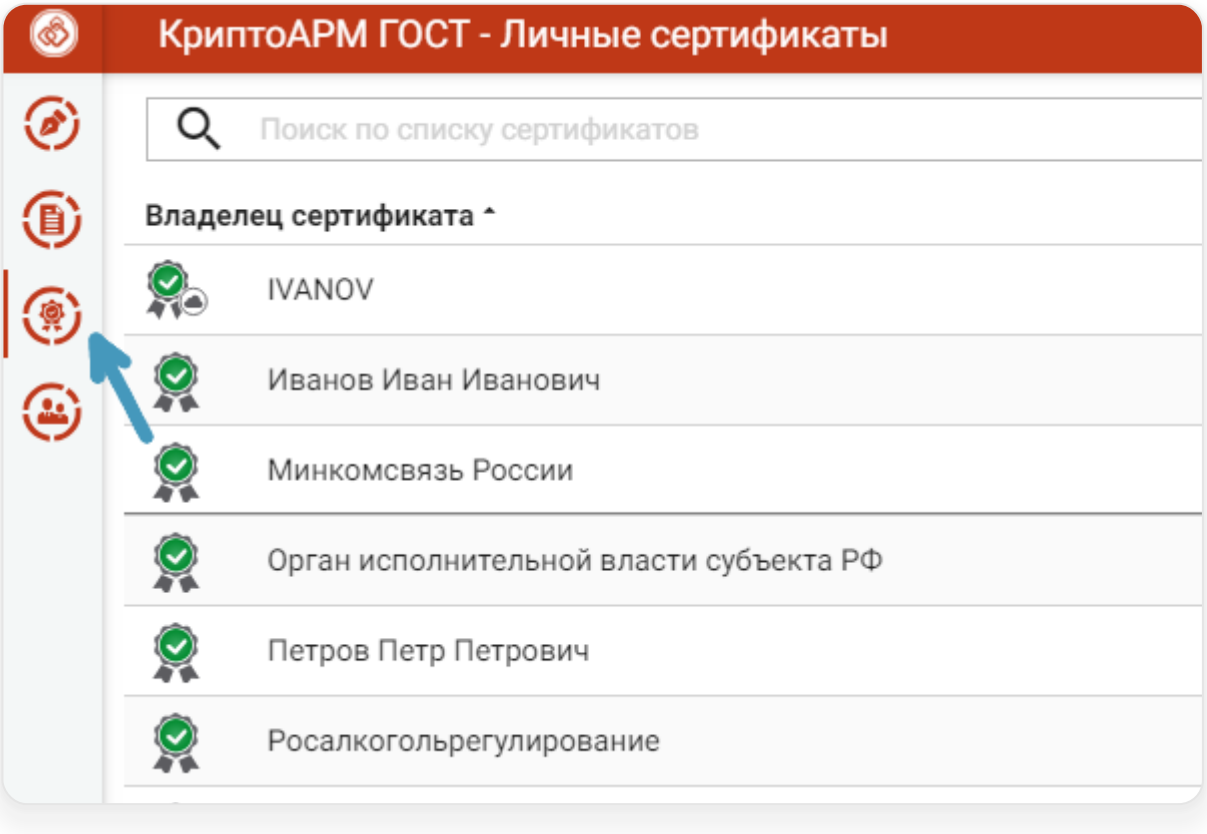
5. Сертификат получателя должен появиться в списке в разделе **“Личные сертификаты”** или **“Сертификаты других пользователей”**.
6. Перейдите на вкладку **“Документы”** и выделите подписанный файл.
7. В правой области окна найдите раздел **“Сертификаты шифрования”**, вызовите контекстное меню и нажмите кнопку **“Добавить”**.



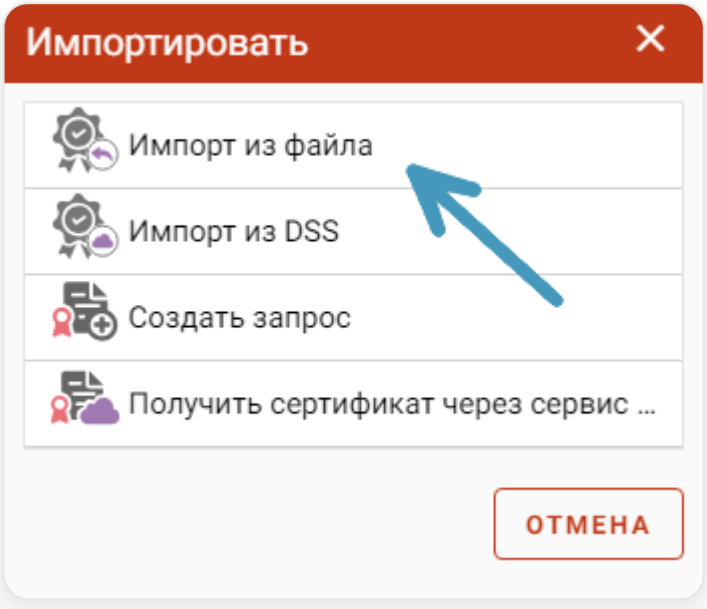
8. Выберите сертификат получателя и нажмите **“Выбрать”**.
9. Нажмите кнопку **“Зашифровать”**. Если операция прошла успешно, программа уведомит об этом.

Чтобы расшифровать полученный документ в КриптоАРМ ГОСТ:

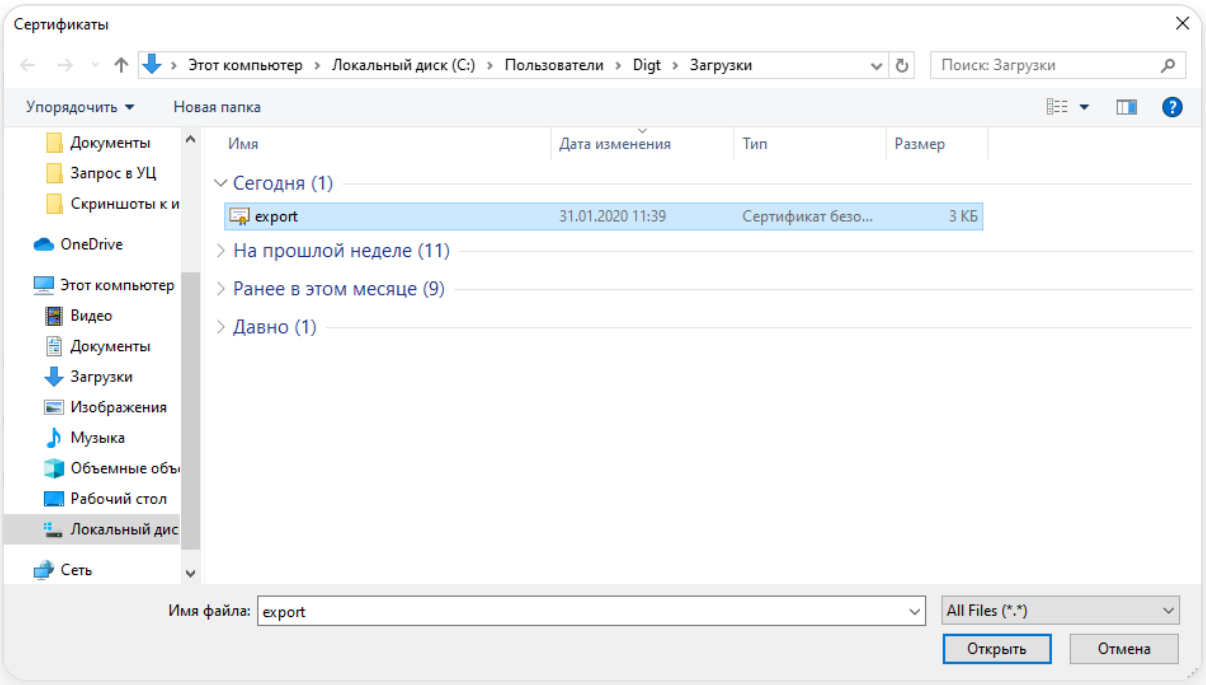
1. Выберите сертификат расшифрования. Для этого скачайте сертификат подписи отправителя, перейдите в раздел меню **“Сертификаты”**.



2. Нажмите кнопку **“+”**. В появившемся меню выберите пункт **“Импорт из файла”**.

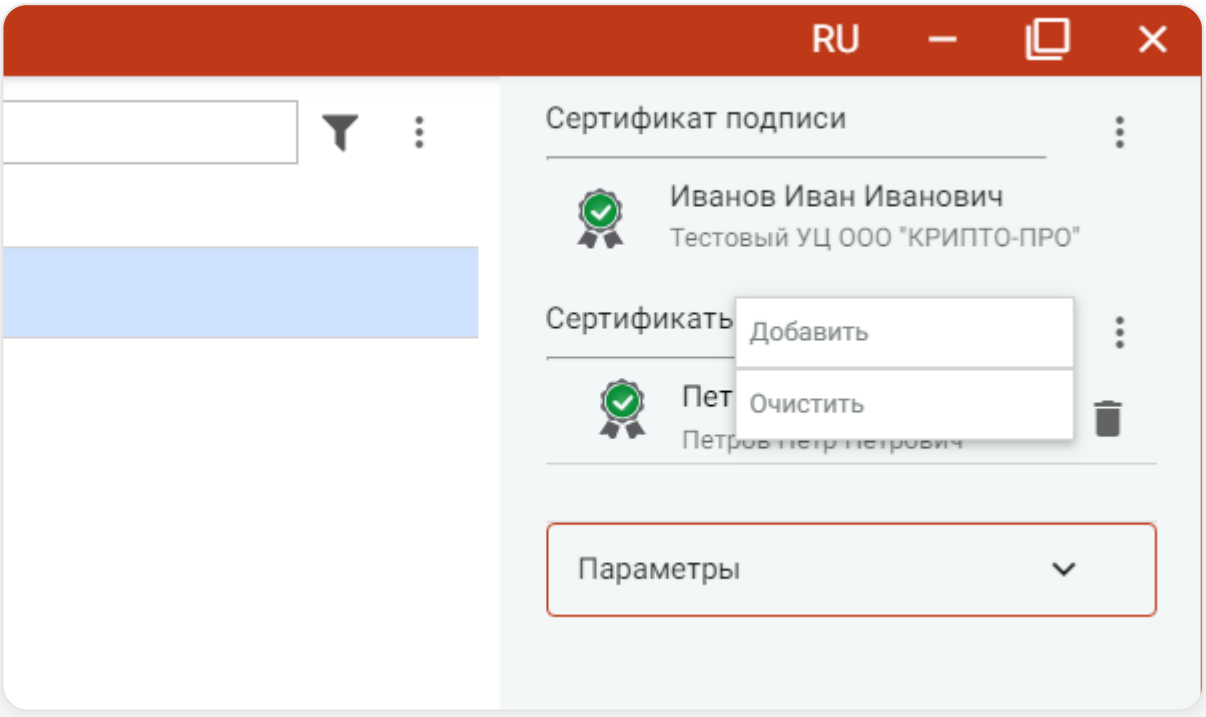


3. Найдите скачанный сертификат отправителя и нажмите **“Открыть”**. Сертификат получателя должен появиться в списке в разделе **“Личные сертификаты”** или **“Сертификаты других пользователей”**.



4. Перейдите на вкладку **“Документы”** и выделите зашифрованный файл.

5. В правой области окна найдите раздел **“Сертификаты шифрования”**, вызовите контекстное меню и нажмите кнопку **“Добавить”**.



6. Выберите сертификат отправителя и нажмите **“Выбрать”**.
7. Нажмите кнопку **“Расшифровать”**. Если операция прошла успешно, программа уведомит об этом.

Открыть статью на сайте

Как отправить запрос в Удостоверяющий центр и получить сертификат электронной подписи

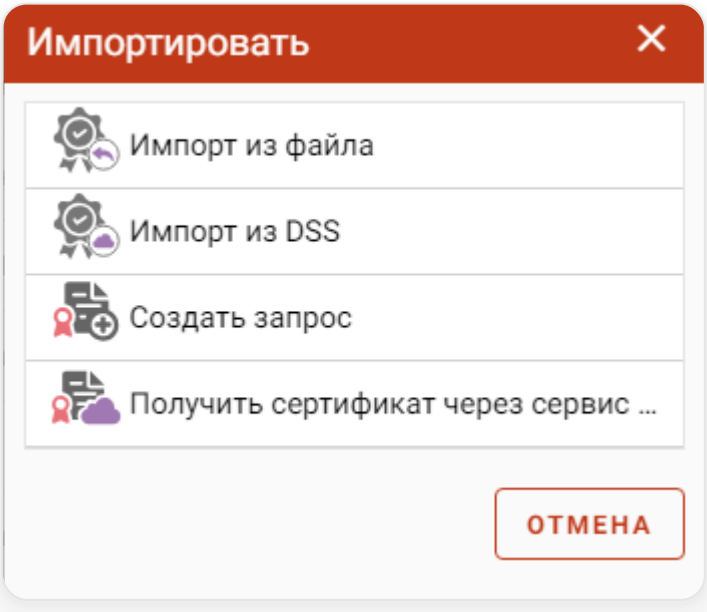
Архив. КриптоАРМ ГОСТ.

Сертификат электронной подписи - это электронный документ или документ на бумажном носителе, выданные удостоверяющим центром либо доверенным лицом удостоверяющего центра и подтверждающие принадлежность ключа проверки электронной подписи владельцу сертификата ключа проверки электронной подписи (**63-ФЗ “Об электронной подписи”**).

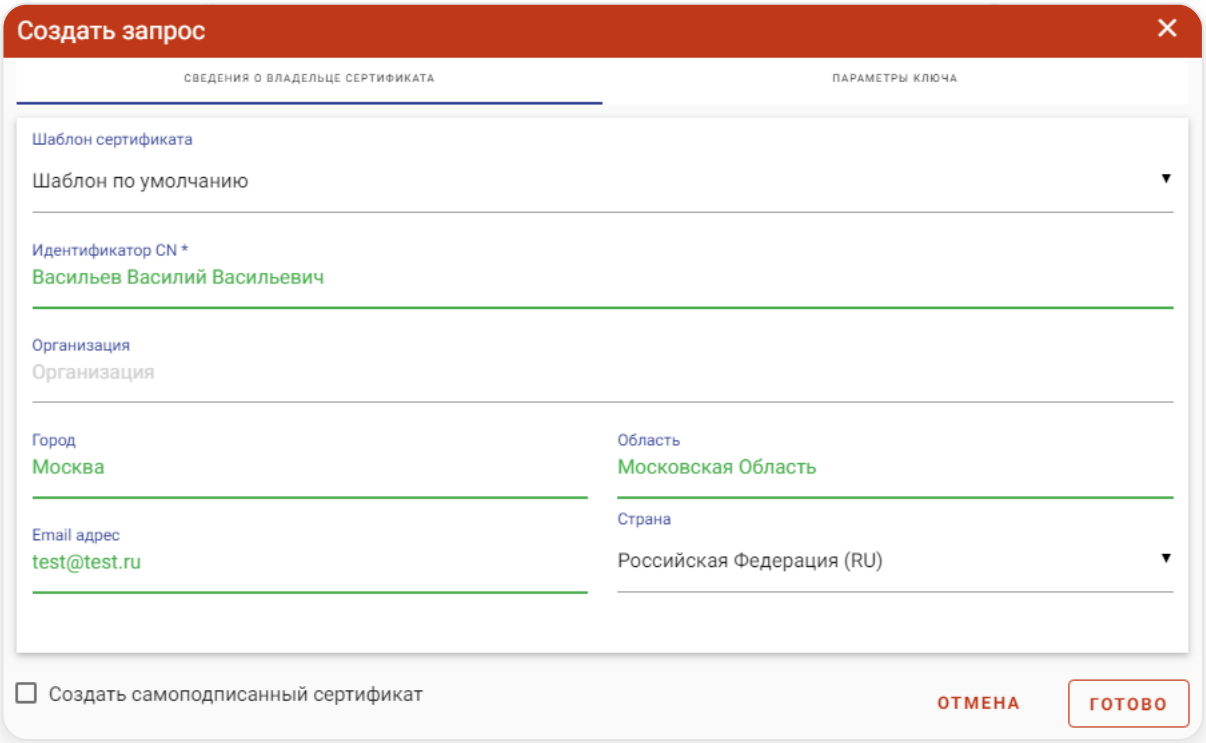
Чтобы получить сертификат подписи из Удостоверяющего центра (УЦ), нужно создать запрос на сертификат в КриптоАРМ ГОСТ и отправить его в Удостоверяющий центр. Запрос можно отправить самостоятельно или автоматически, в КриптоАРМ ГОСТ, если Удостоверяющий центр использует ПАК “КриптоПро УЦ 2.0”.

Чтобы создать запрос на сертификат и отправить его самостоятельно:

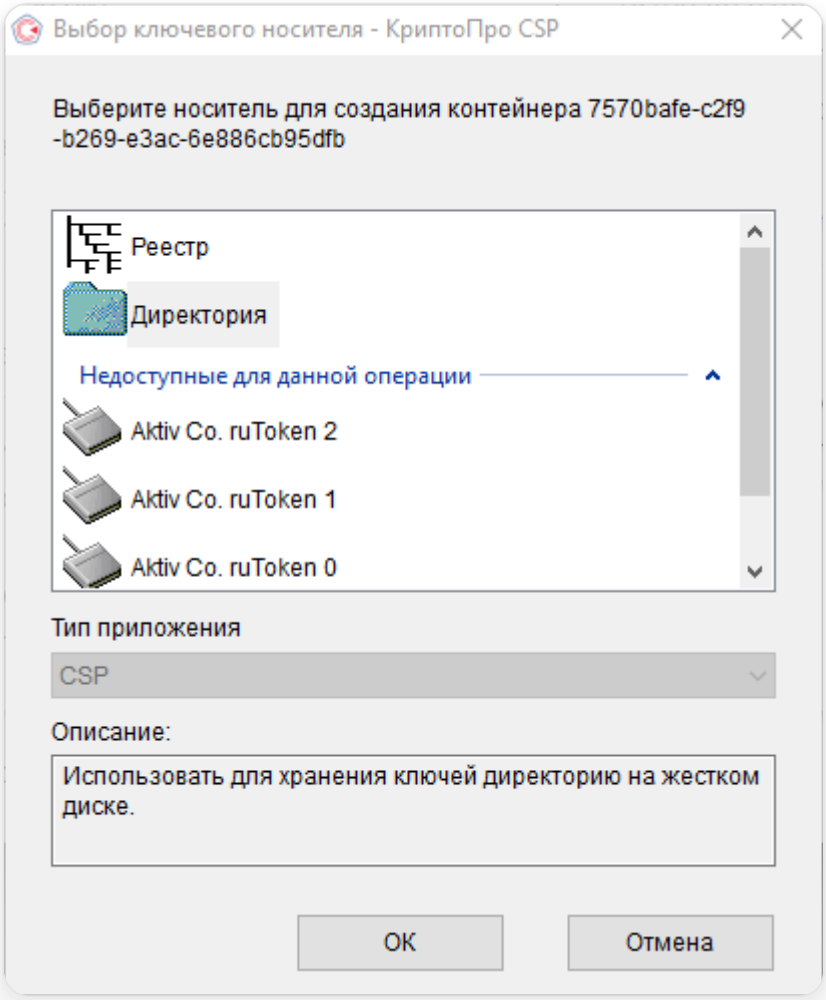
1. Откройте вкладку **“Сертификаты”** и нажмите **“+”**.
2. В появившемся меню нажмите **“Создать запрос”**.



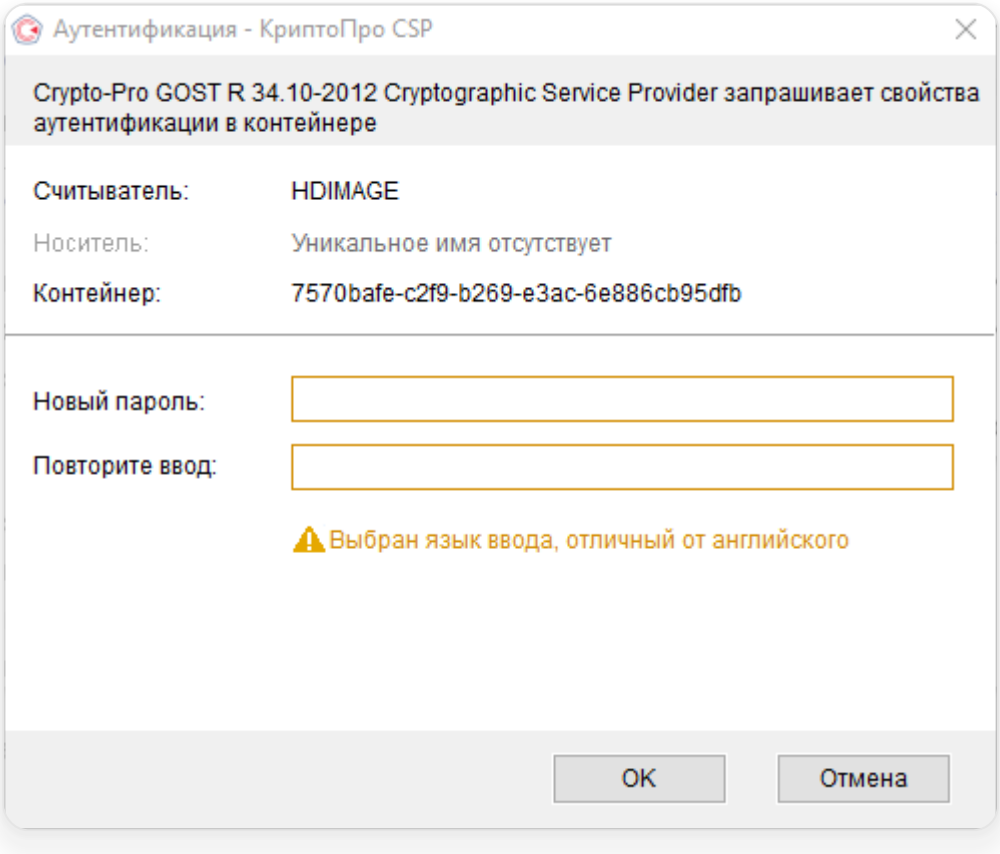
3. На вкладке **“Сведения о владельце сертификата”** введите личные данные.



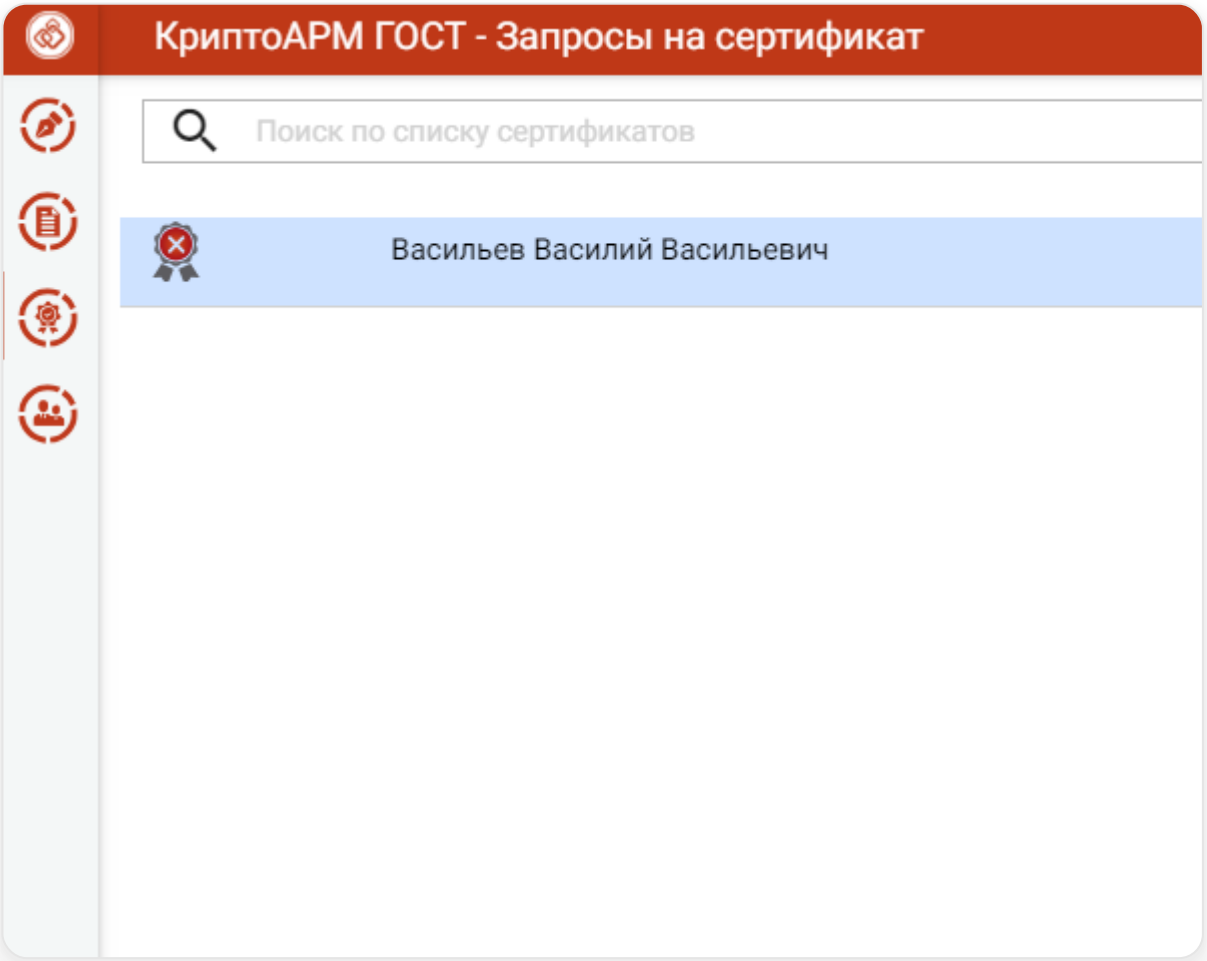
4. Нажмите **“Готово”**. Выберите носитель для создания контейнера с запросом на сертификат.



5. Установите пароль для контейнера с запросом на сертификат и нажмите **“OK”**.

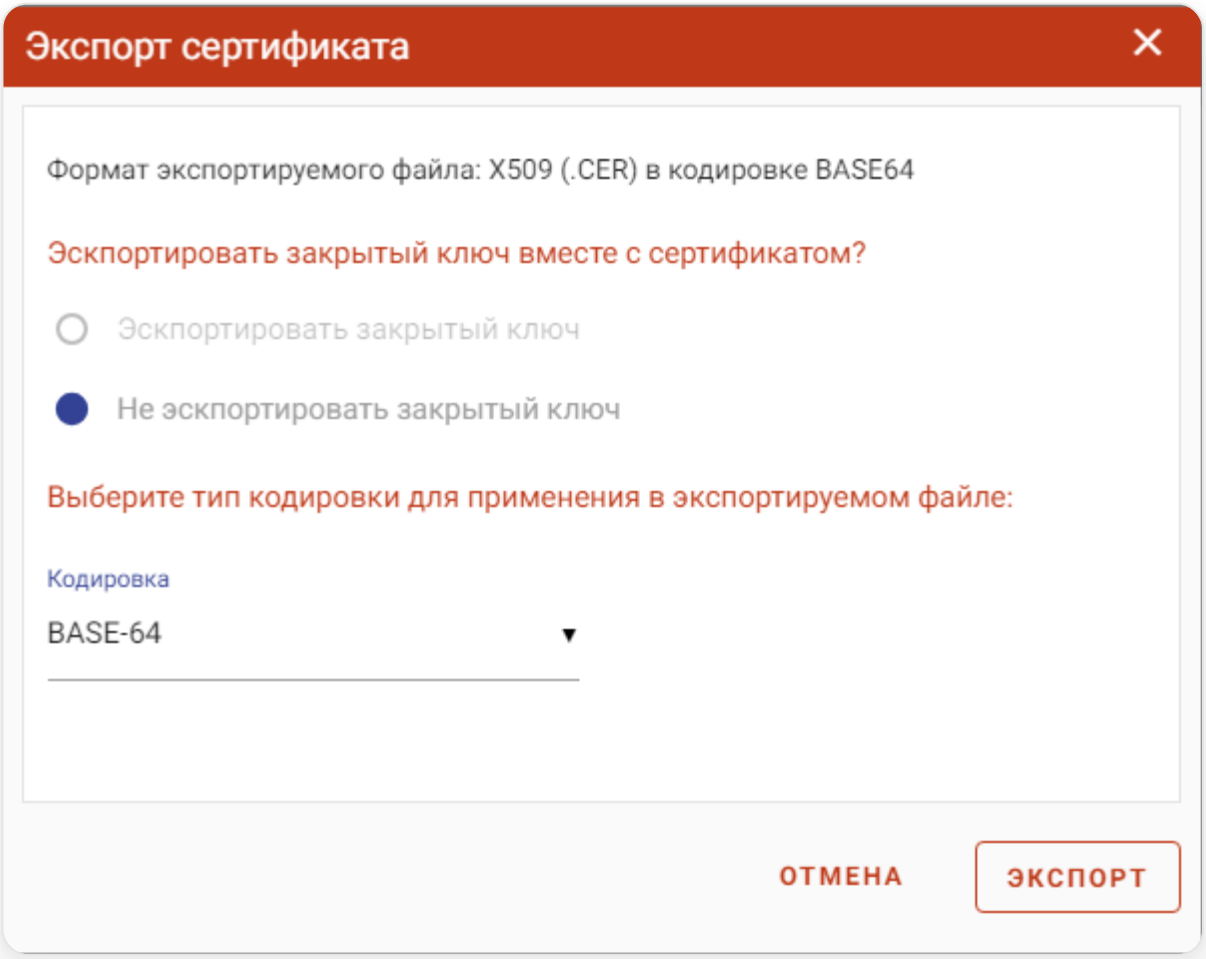


6. Созданный запрос появится во вкладке **“Сертификаты” - “Запросы”**.



7. Чтобы экспортировать запрос, выделите его и в нижнем правом угле нажмите кнопку **“Экспортировать”**.

8. В окне **“Экспорт сертификата”** укажите необходимые настройки и нажмите **“Экспорт”**.

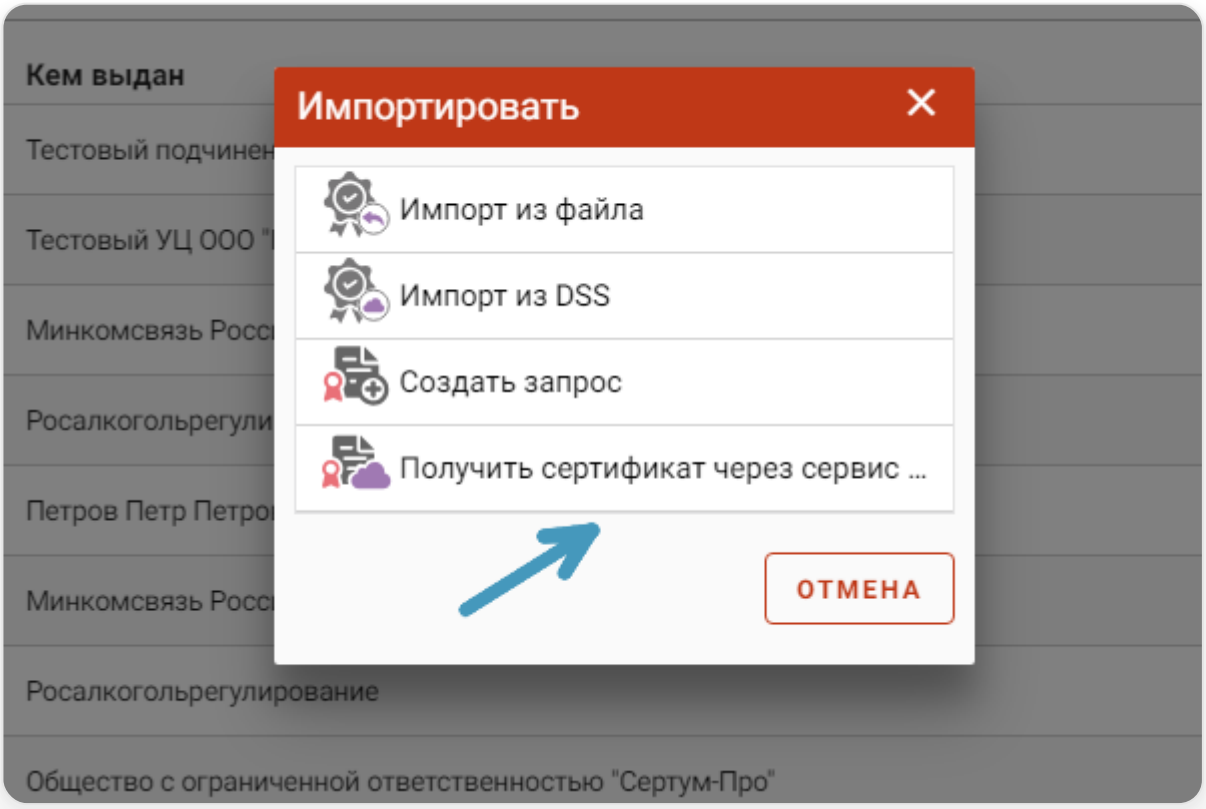


9. Укажите путь экспорта файла запроса.
10. Файл запроса появится в указанной директории с названием “export.cer” по умолчанию. Направьте его в Удостоверяющий центр.

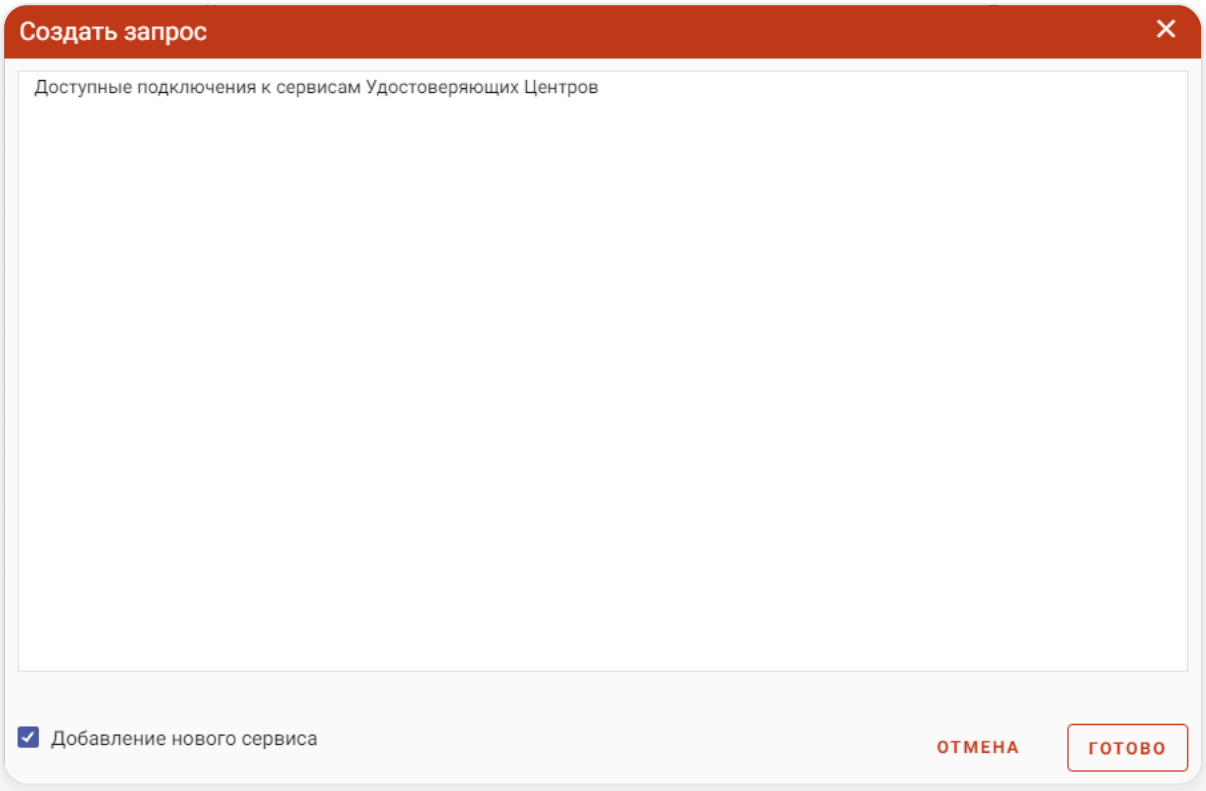
Чтобы создать и отправить запрос на сертификат автоматически через сервис УЦ:

1. В Вашем Удостоверяющем центре узнайте URL, по которому необходимо сформировать запрос.
2. Откройте вкладку **“Сертификаты”** и нажмите **“+”**.

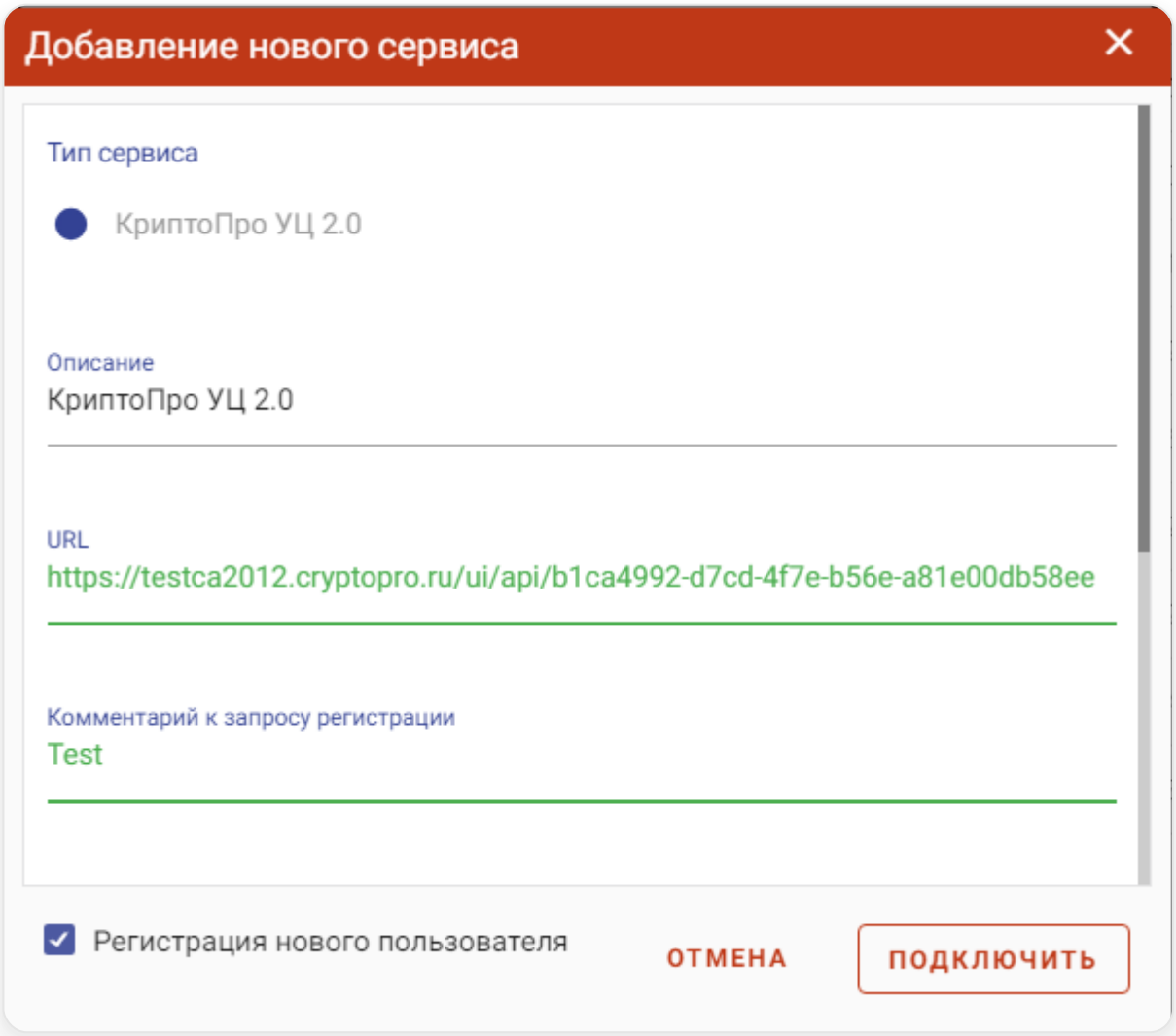
3. В появившемся меню нажмите **“Получить сертификат через сервис УЦ”**.



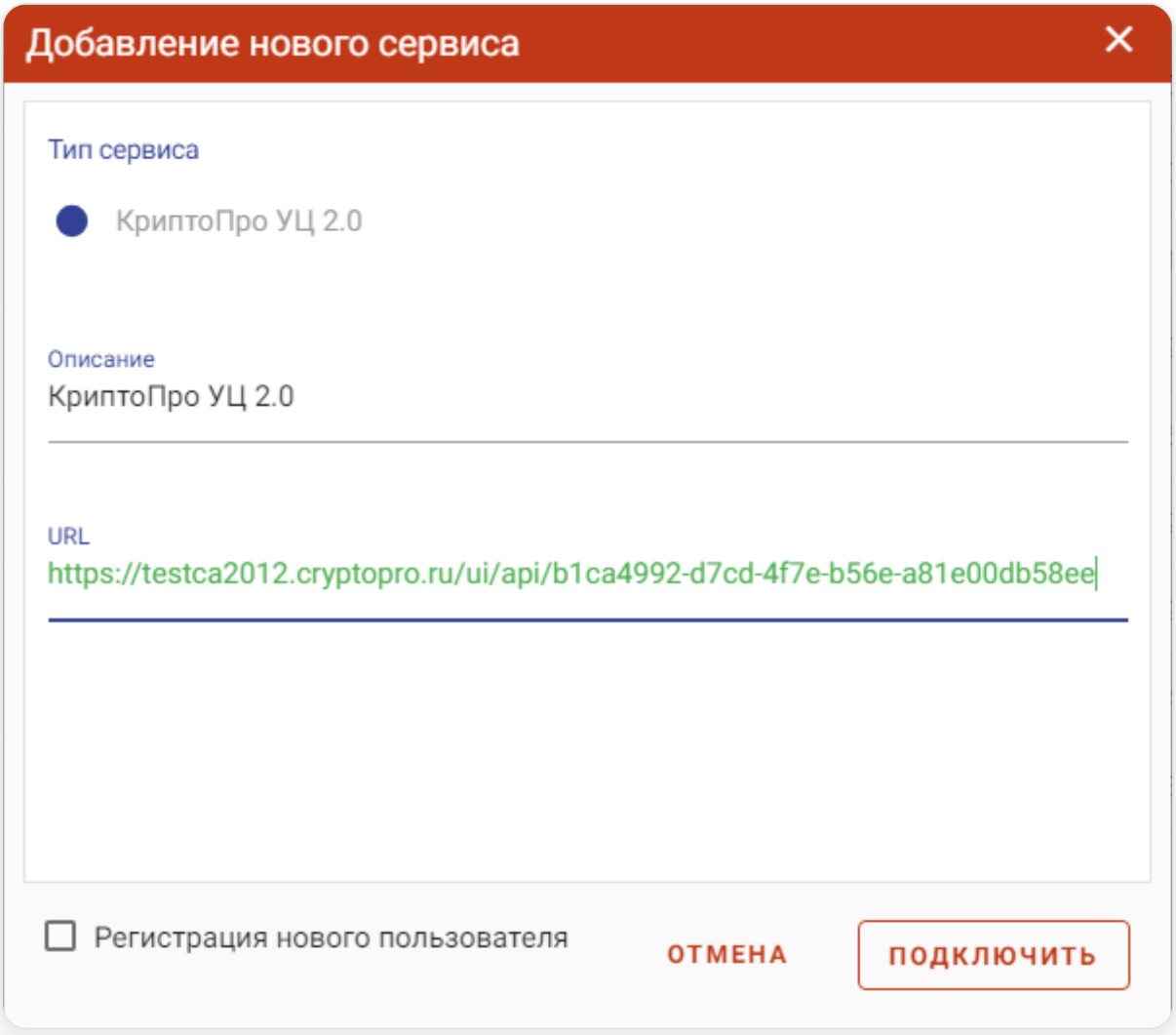
4. Выберите пункт **“Добавление нового сервиса”** и нажмите **“Готово”**.



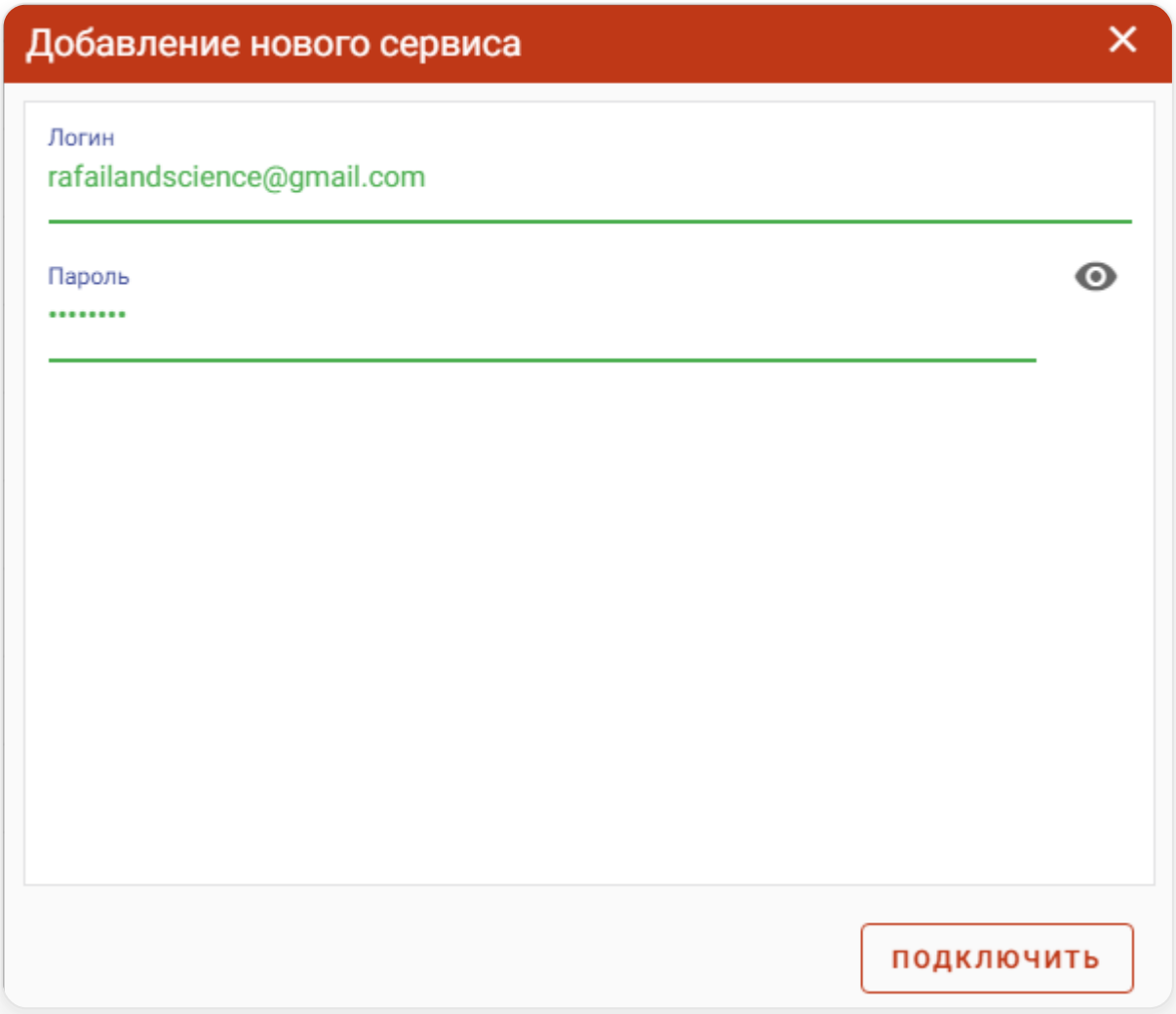
5. Откроется окно ввода параметров подключения с автоматическим выбором функции **“Регистрация нового пользователя”**. Если пользователь ещё не зарегистрирован в УЦ, введите данные для регистрации и нажмите кнопку **“Подключить”**.



6. Если пользователь уже зарегистрирован в УЦ, отключите функцию **“Регистрация нового пользователя”**, введите URL сервера и нажмите **“Подключить”**.



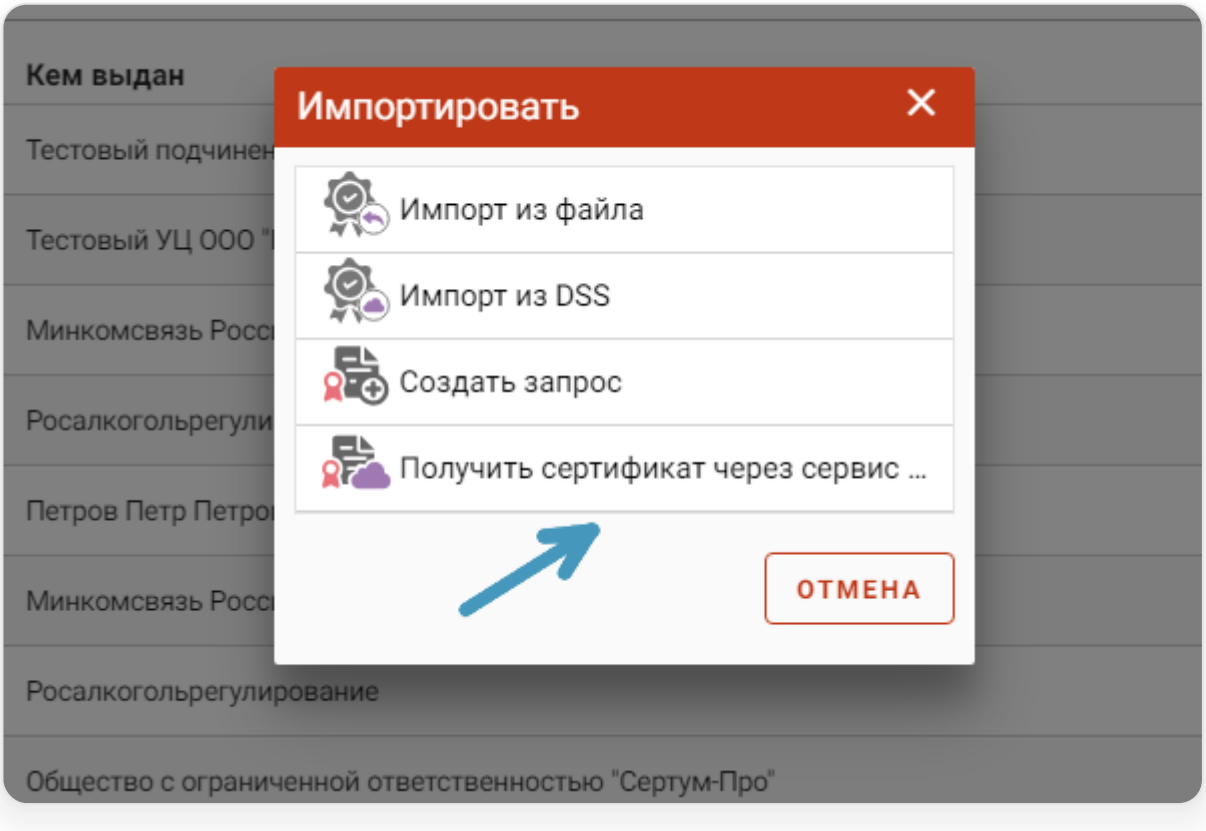
7. Введите данные для авторизации и нажмите **“Подключить”**.



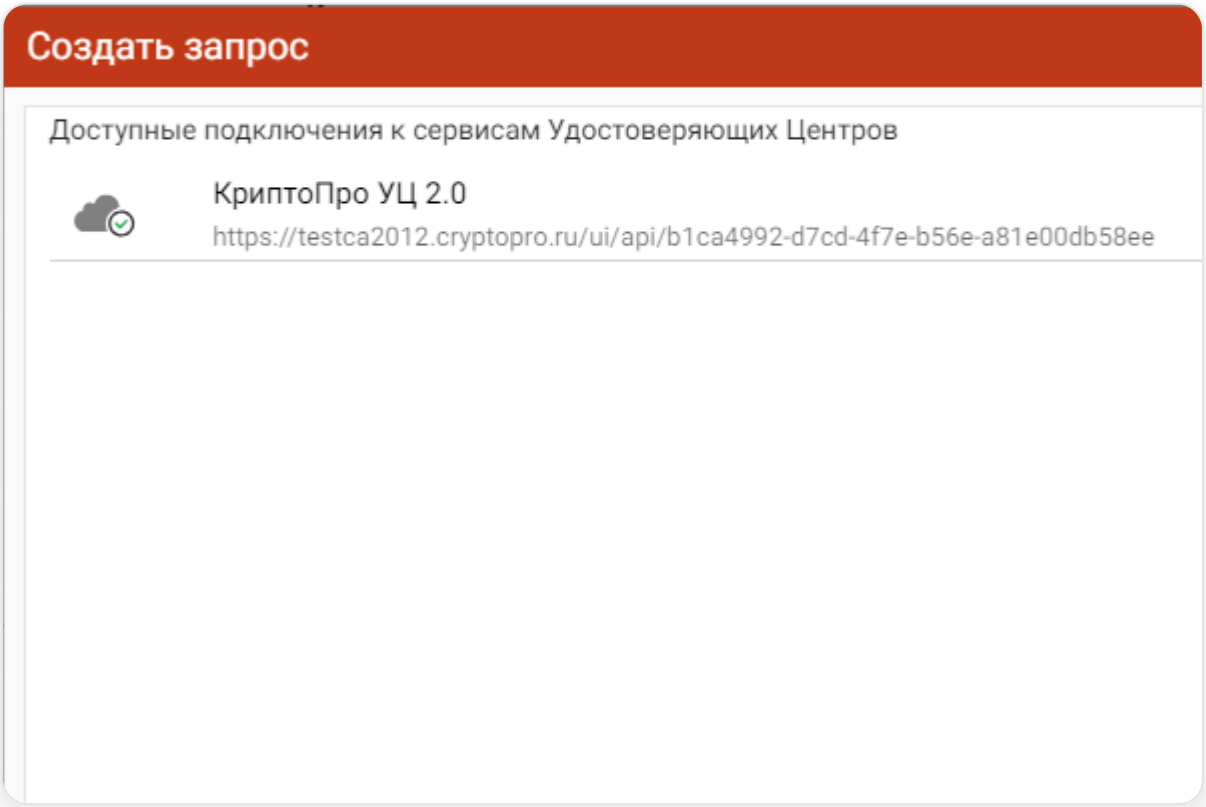
8. Удостоверяющий центр должен появиться в списке в разделе **“Сертификаты”** в списке **“Получить сертификат через сервис УЦ”**. Теперь можно создать запрос на сертификат.

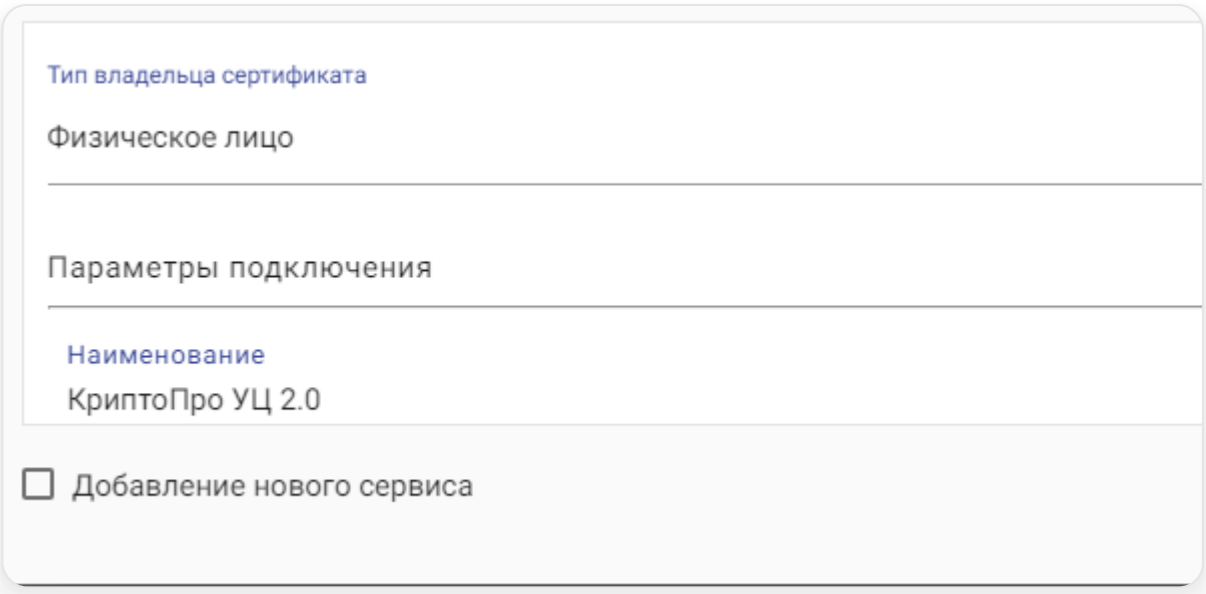
9. Откройте вкладку **“Сертификаты”** в КриптоАРМ ГОСТ и нажмите **“+”**.

10. В появившемся меню нажмите **“Получить сертификат через сервис УЦ”**.

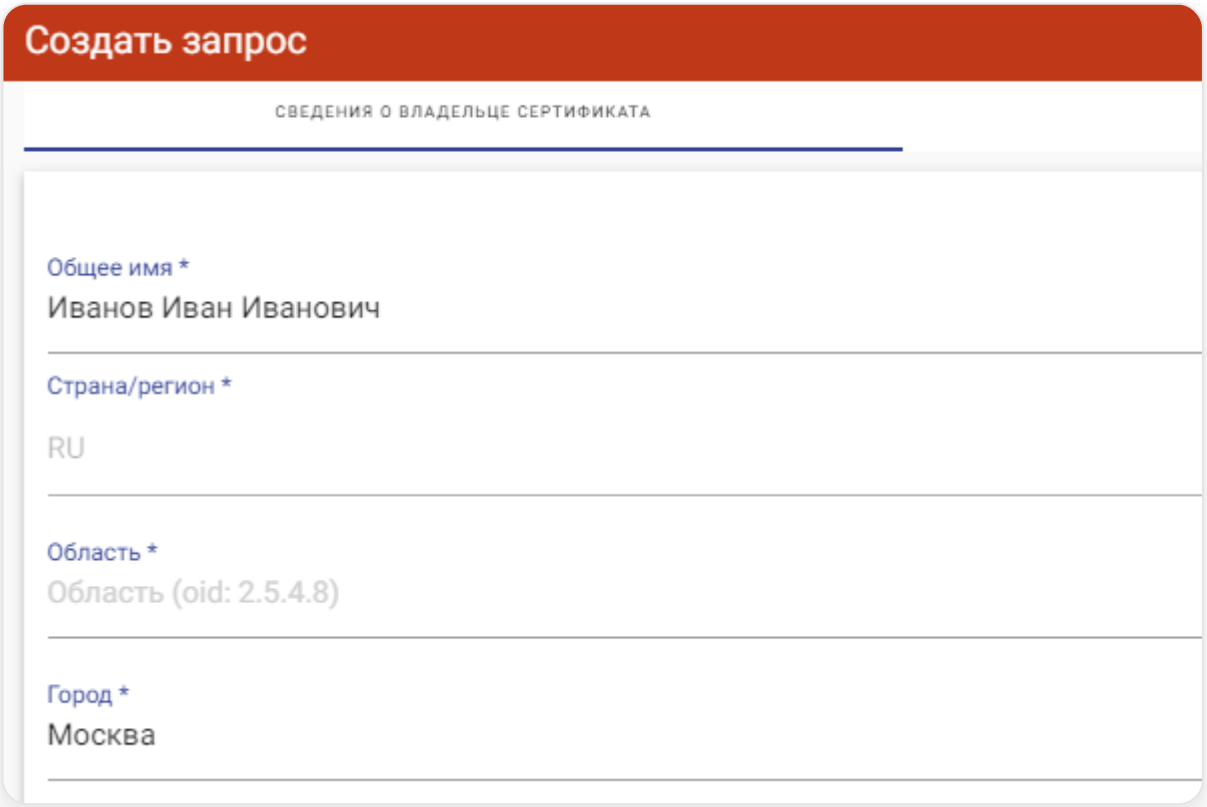


11. Выделите нужный удостоверяющий центр в списке, выберите тип владельца сертификата и нажмите **“Готово”**.

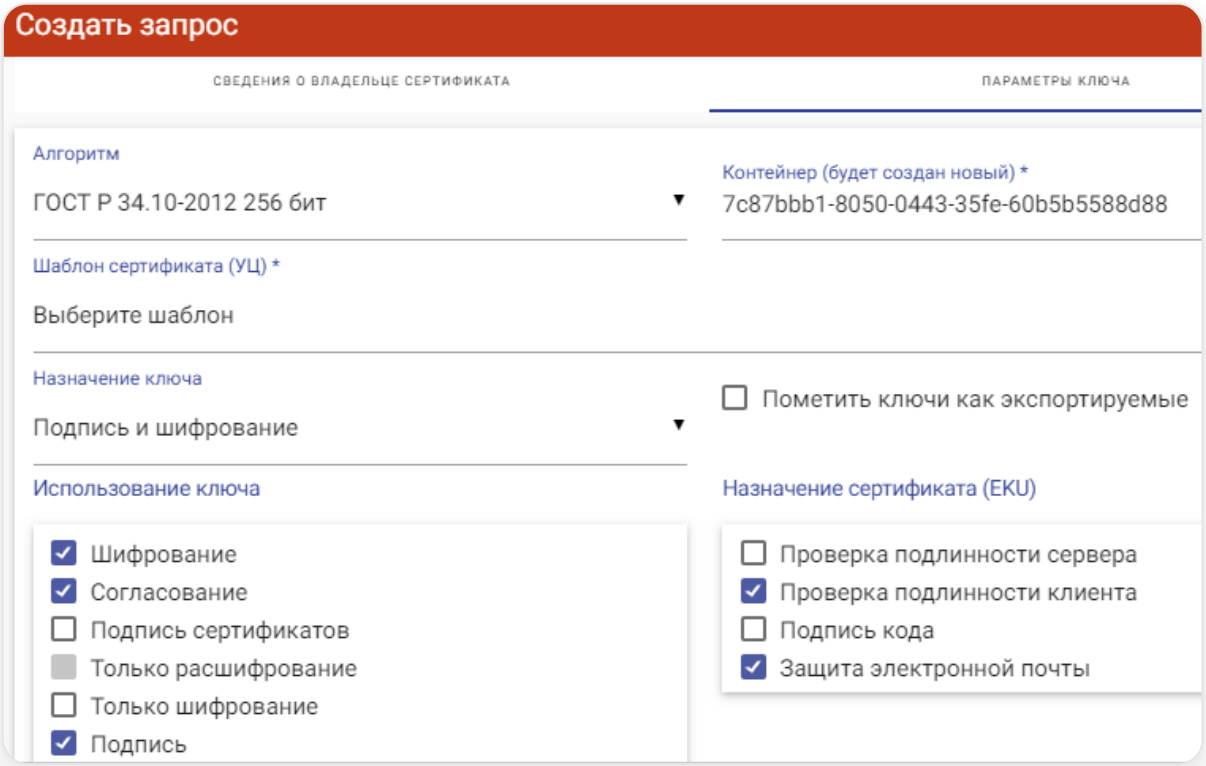

Создать запрос
Доступные подключения к сервисам Удостоверяющих Центров
КриптоПро УЦ 2.0
https://testca2012.cryptopro.ru/ui/api/b1ca4992-d7cd-4f7e-b56e-a81e00db58ee


Тип владельца сертификата
Физическое лицо
Параметры подключения
Наименование
КриптоПро УЦ 2.0
Добавление нового сервиса

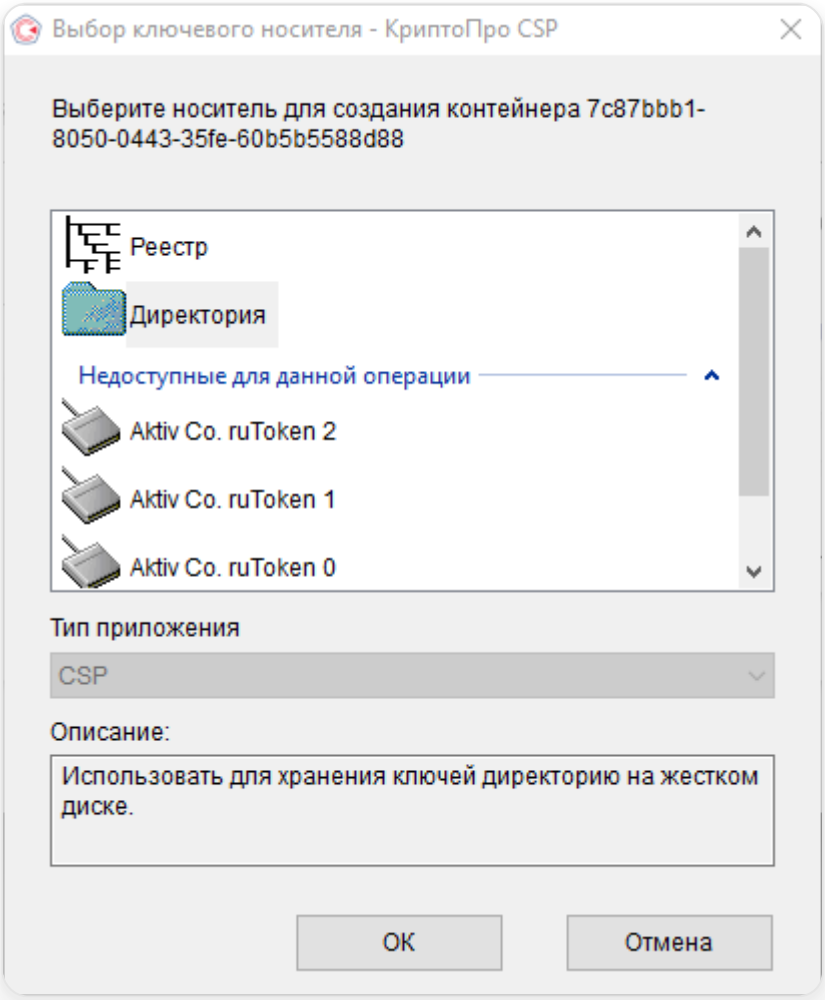
12. В новом окне **“Создать запрос”** заполните сведения о владельце так же, как при добавлении УЦ.



13. Заполните параметры ключа. Нажмите **“Готово”**.



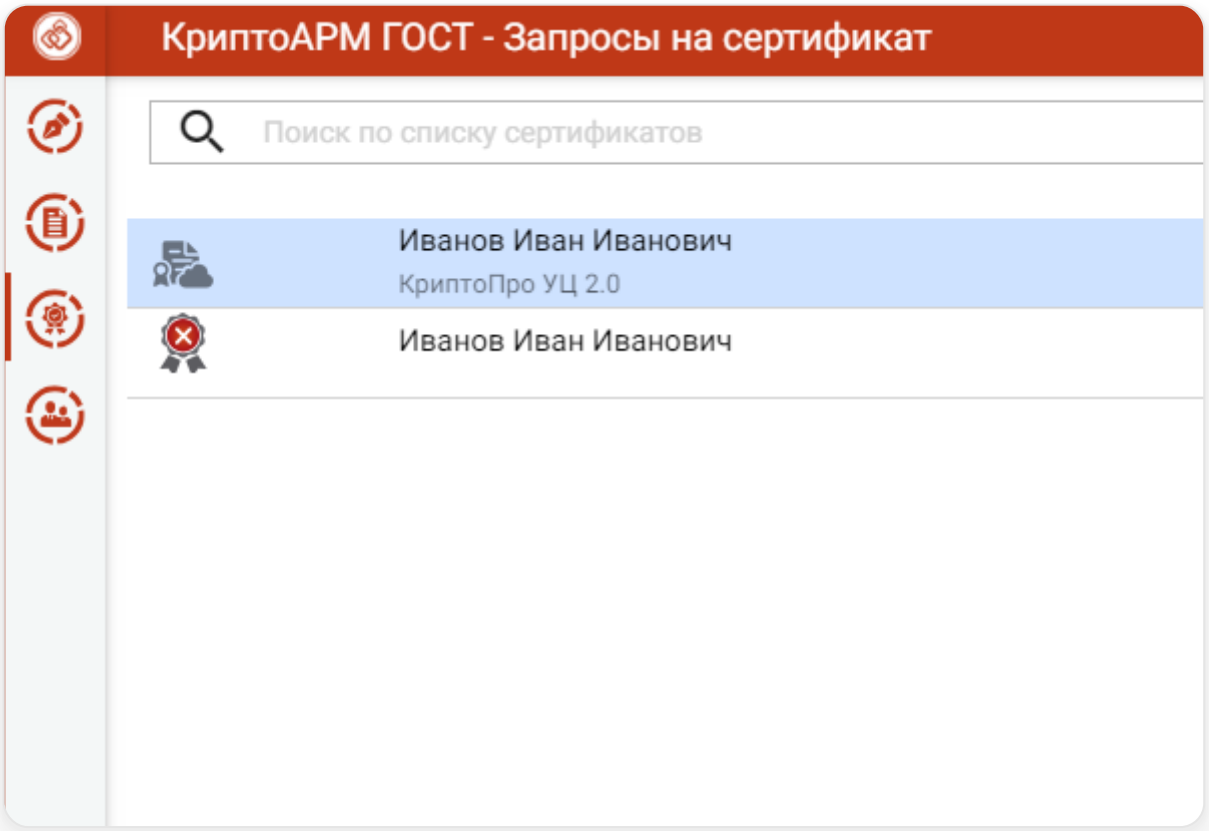
14. Выберите ключевой носитель для хранения контейнера сертификата.



15. Установите пароль для контейнера сертификата.

16. Возникнет окно с информацией о результатах операции.

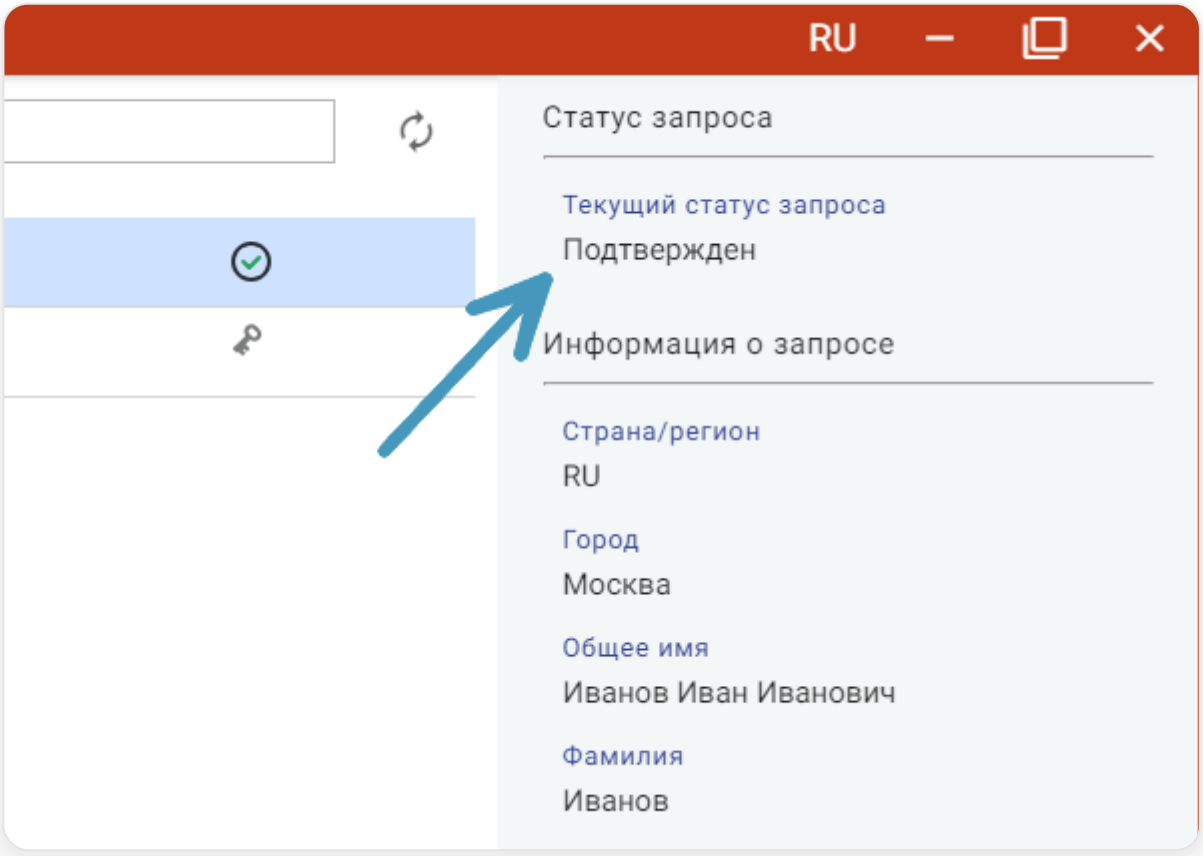
Запрос появится на вкладке **“Запросы”** в разделе меню **“Сертификаты”**. Запросы можно экспортировать, удалить или показать в каталоге, выбрав соответствующие кнопки в правой нижней области окна.



Для запроса сертификата будут отображаться различные статусы:

1. Сертификат подтверждён: выпущен для данного запроса и установлен в Хранилище КриптоПро;
2. Запрос сертификата отклонен удостоверяющим центром;
3. Запрос находится в обработке;

4. Проблемы с соединением, не позволяющим отобразить статус запроса.



Открыть статью на сайте

Как подписать документы мобильной подписью Билайн в КриптоАРМ ГОСТ

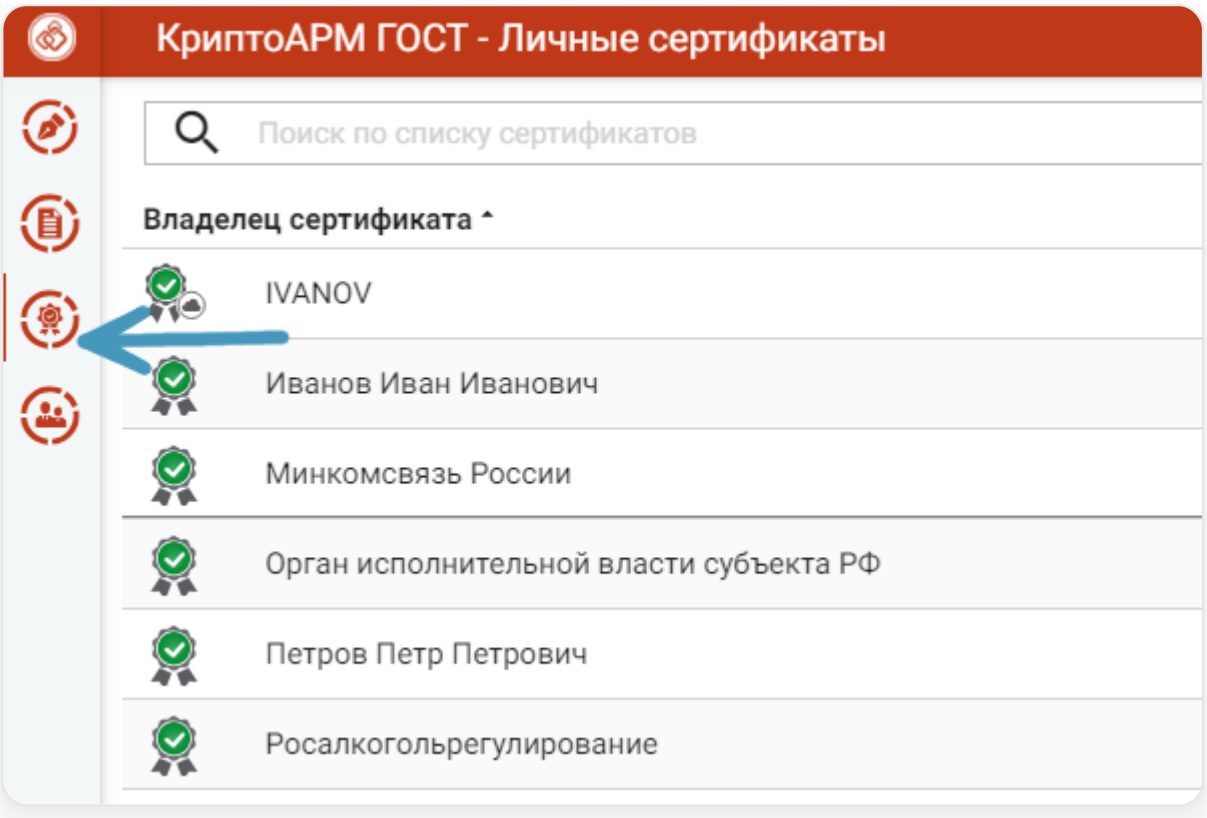
Архив. КриптоАРМ ГОСТ.

Летом 2019 года Билайн запустил услугу мобильной электронной подписи (МЭП). МЭП - это технология создания квалифицированной электронной подписи, для которой используются специальные SIM-карты мобильных операторов, которые выступают в роли удостоверяющих центров. Они создают и хранят в своём облачном хранилище сертификаты электронных подписей, работать с которыми можно посредством push-уведомлений или SMS.

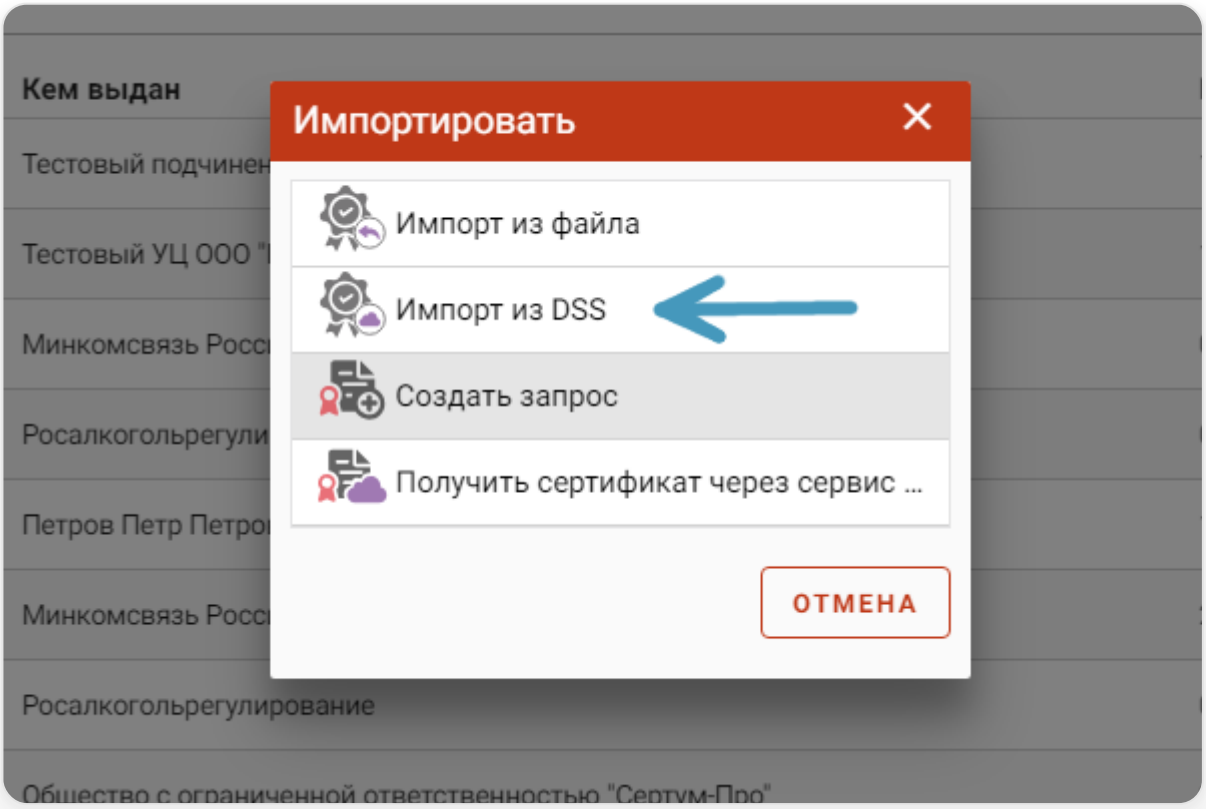
Когда документ подписывается МЭП, на телефон приходит специальный PIN-код, подтверждающий подпись документа. Операция завершится только после того, как он будет введён в программе подписи.

Чтобы установить облачную подпись Билайн в КриптоАРМ ГОСТ:

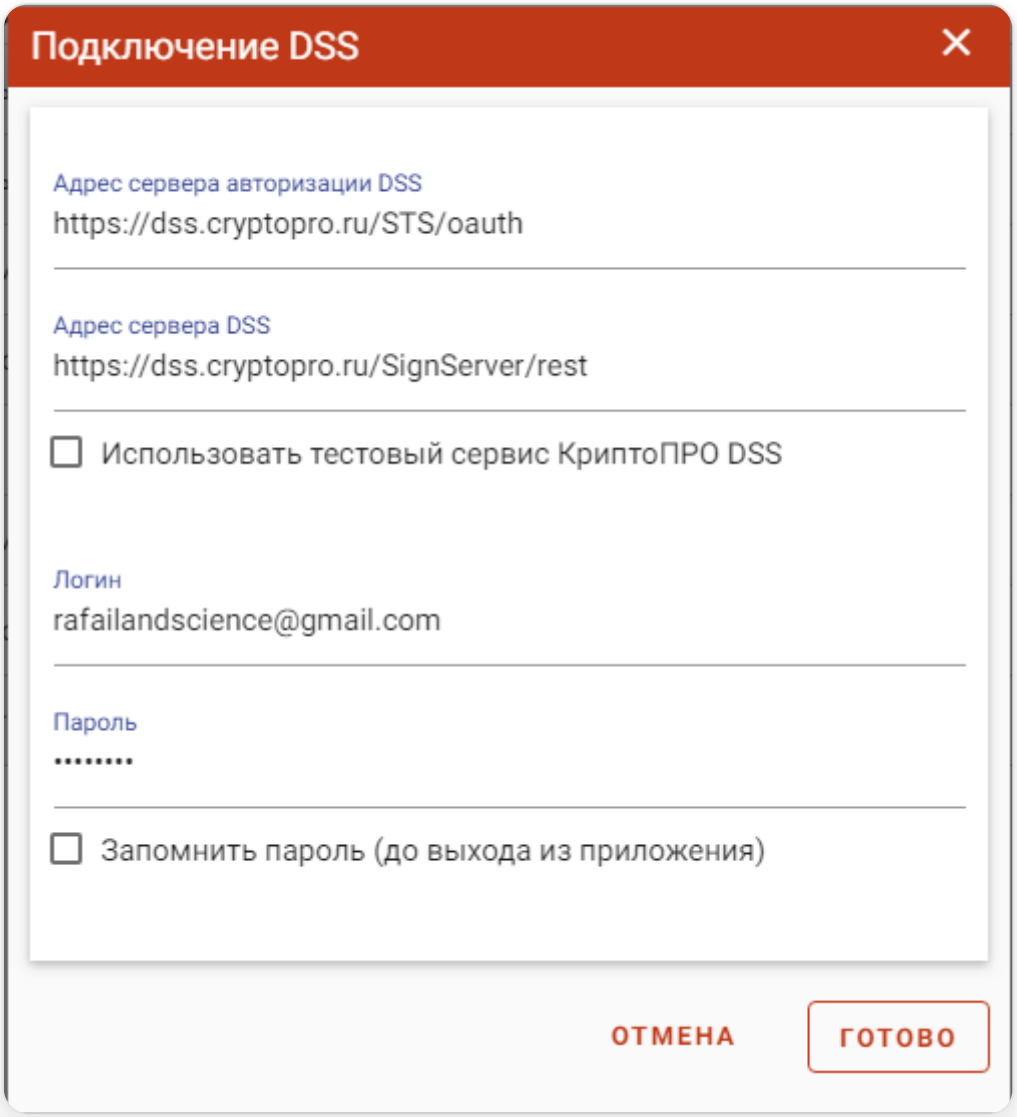
1. Откройте КриптоАРМ ГОСТ.
2. В контекстном меню программы зайдите на вкладку **“Сертификаты”**.



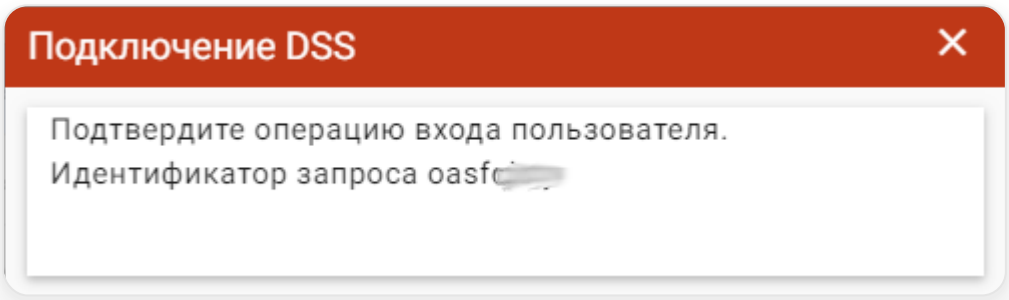
3. Нажмите на кнопку **“+”**, чтобы добавить сертификат, и выберите пункт **“Импорт из DSS”**.

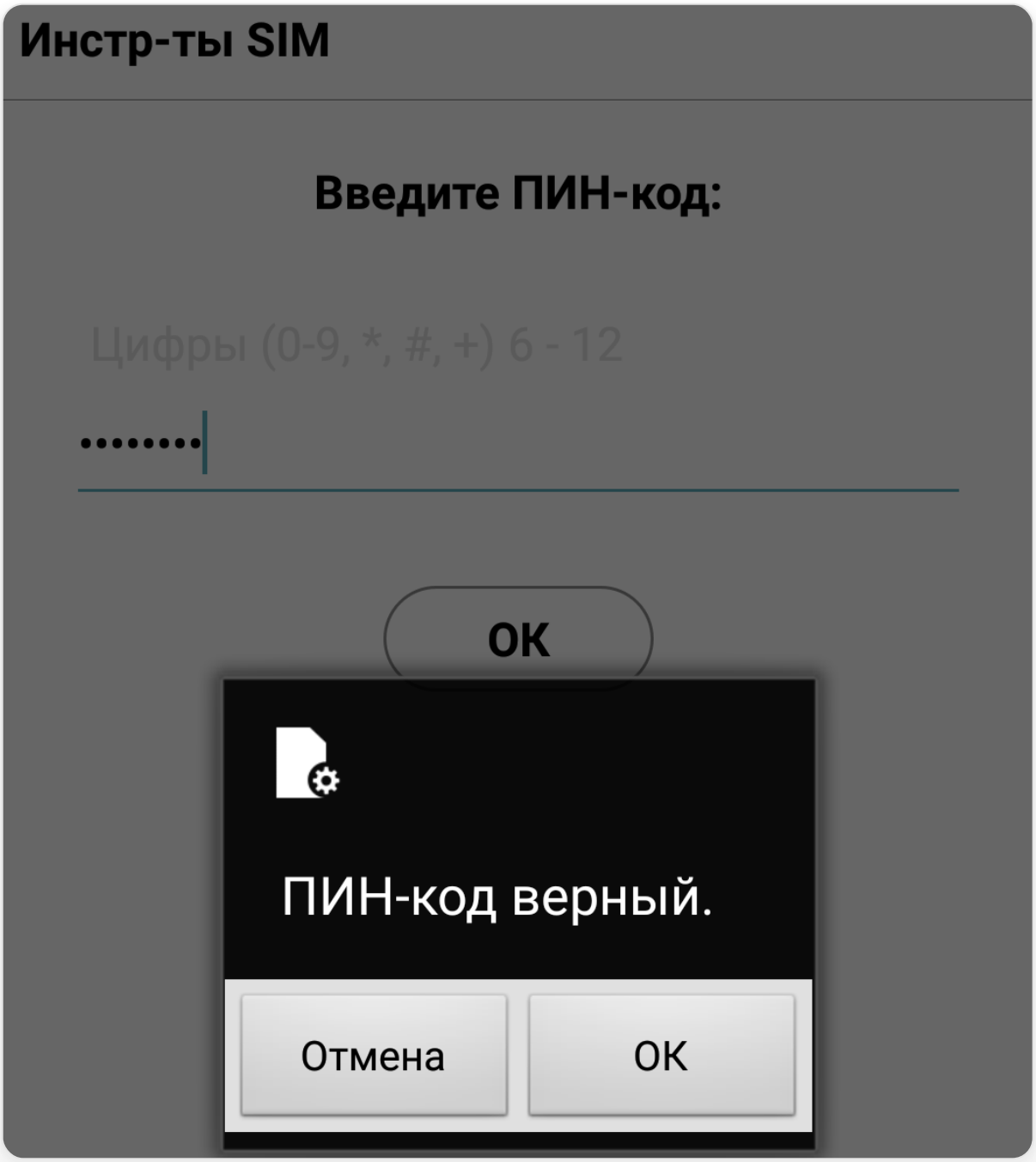


4. Введите адреса **“Сервера авторизации”** и **“Сервера DSS”**, а затем логин и пароль для авторизации на сервере.



5. Подтвердите добавление подписи в КриптоАРМ ГОСТ. **Сверьте идентификаторы и введите ПИН-код** на телефоне, когда придёт всплывающее уведомление.



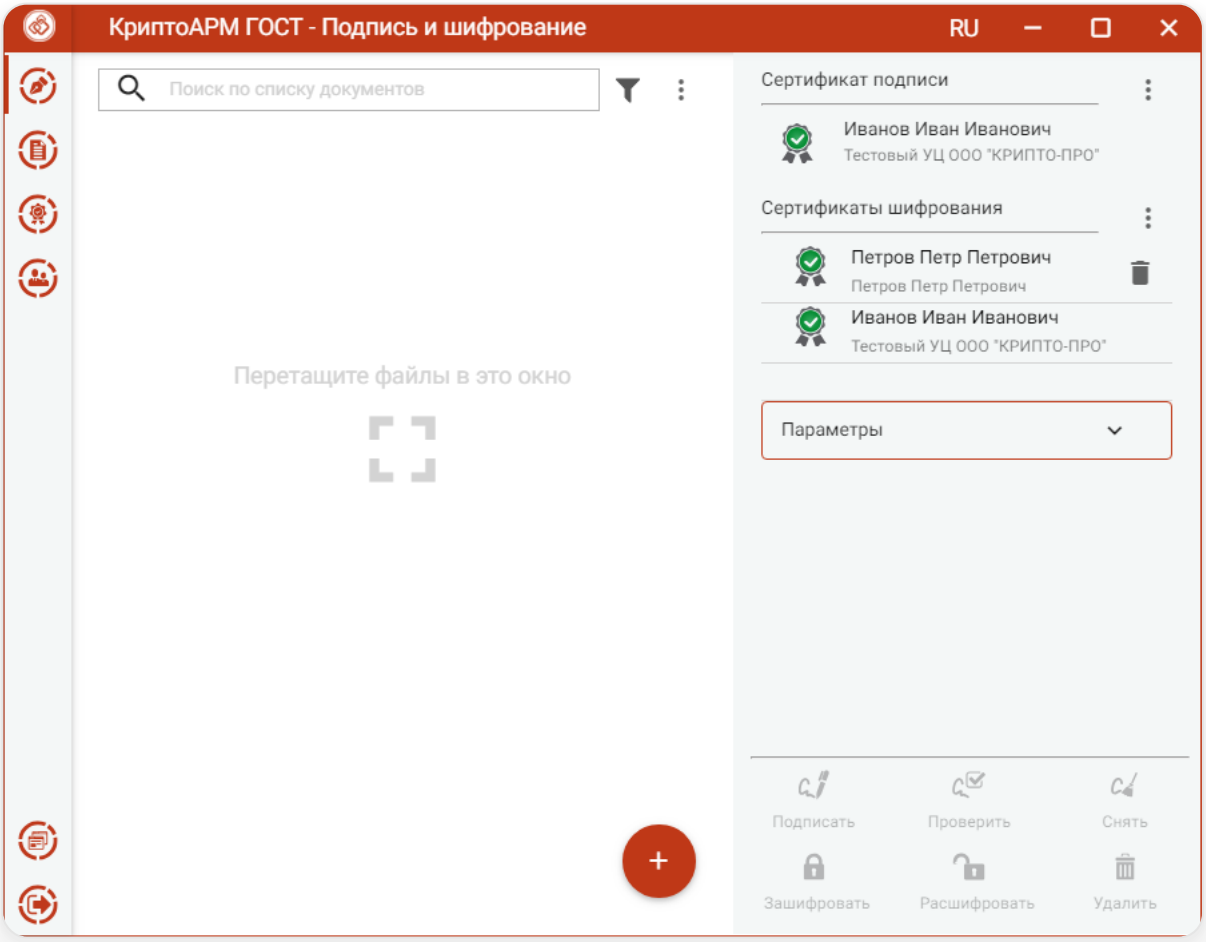


6. Нажмите на кнопку **“Готово”**. Сертификат импортируется в Ваше личное хранилище сертификатов и будет помечен иконкой с облаком. Издатель: ПАО “Вымпелком”.

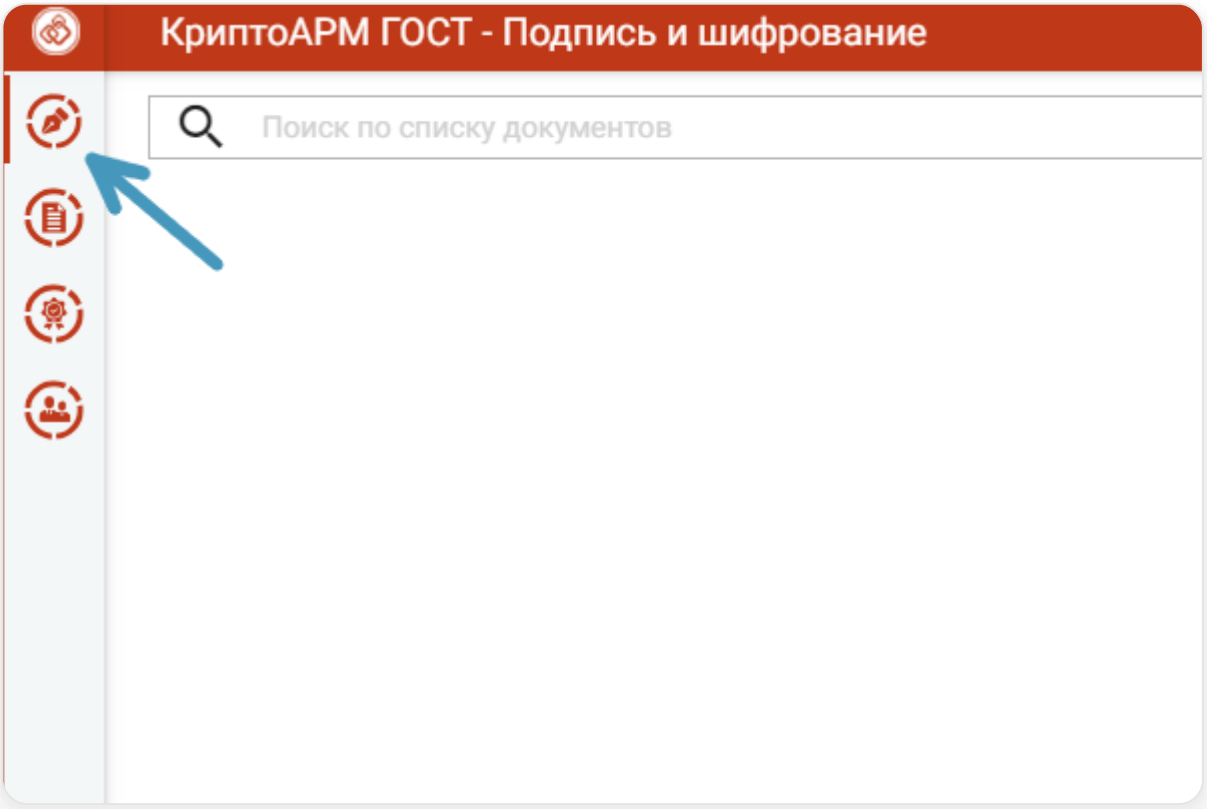
После успешного импорта сертификата, им можно подписывать файлы так же, как и остальными.

Чтобы подписать документ в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.


КриптоАРМ ГОСТ - Подпись и шифрование
RU
Поиск по списку документов
Перетащите файлы в это окно
Сертификат подписи
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
Сертификаты шифрования
Петров Петр Петрович
Петров Петр Петрович
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
Параметры
Подписать
Проверить
Снять
Зашифровать
Расшифровать
Удалить

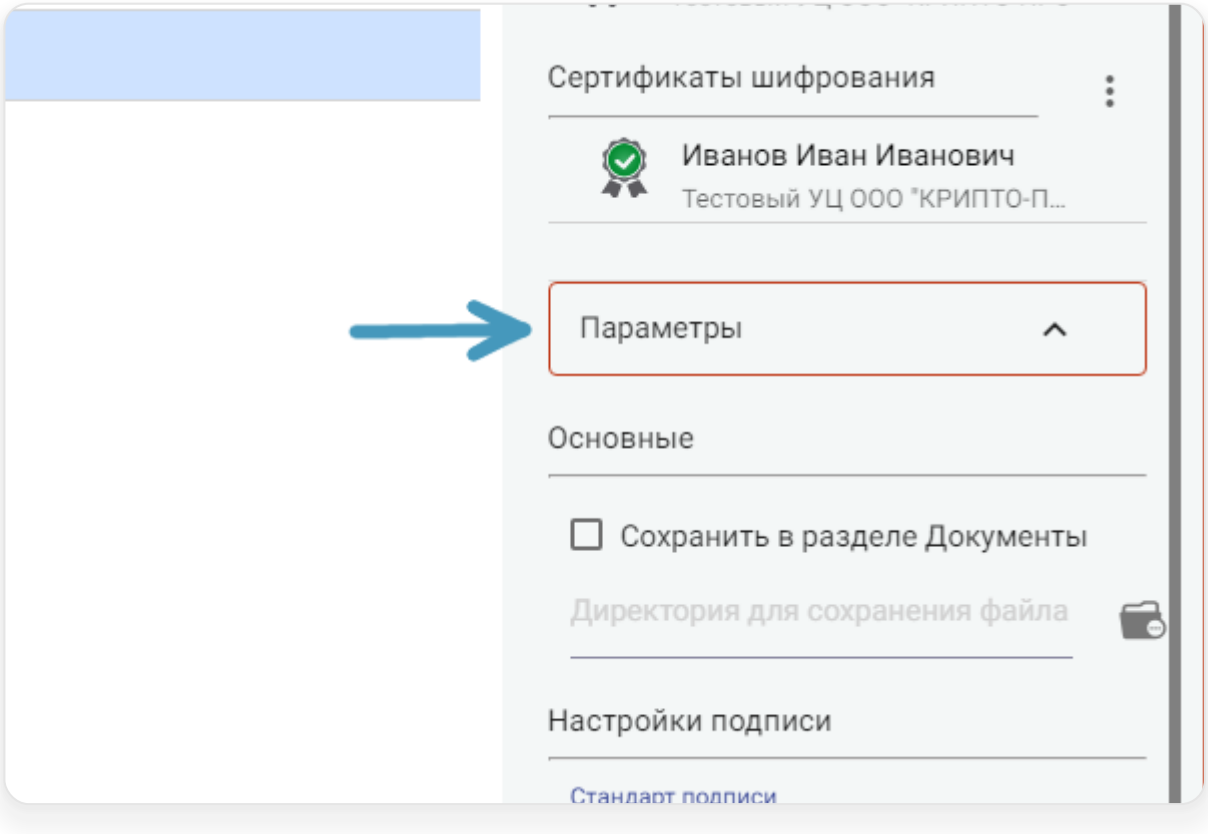
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

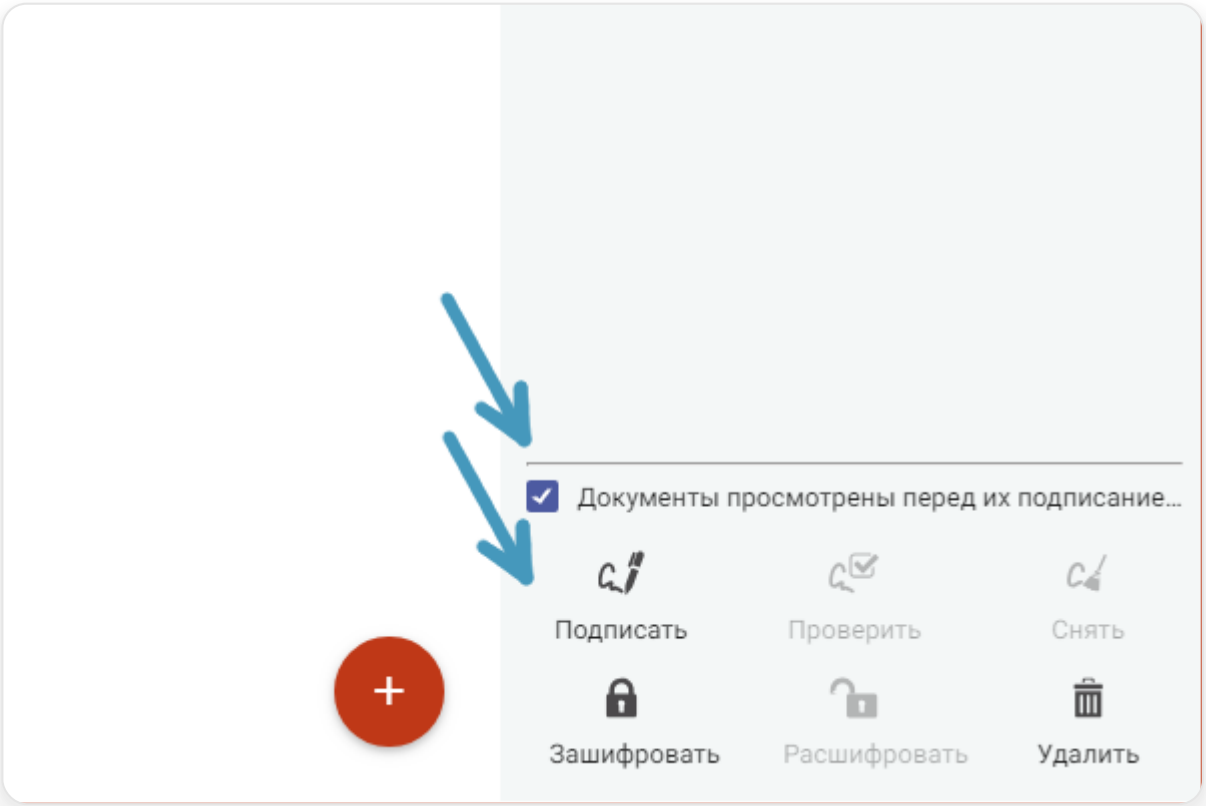
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.



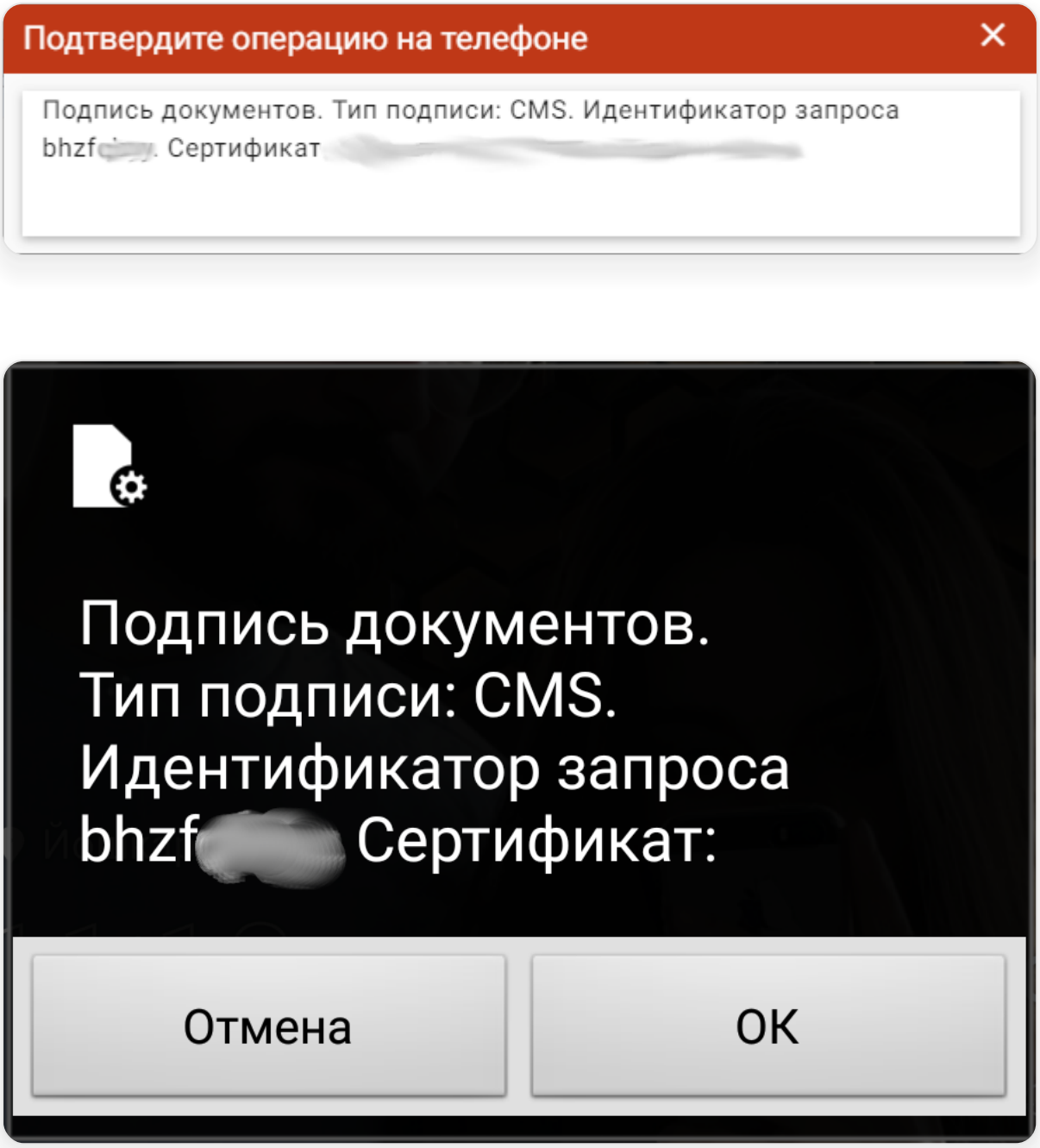
6. Нажмите кнопку **“Заменить”** в контекстном меню настроек подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

7. Выберите облачный сертификат Билайн DSS и нажмите кнопку **“Выбрать”**.

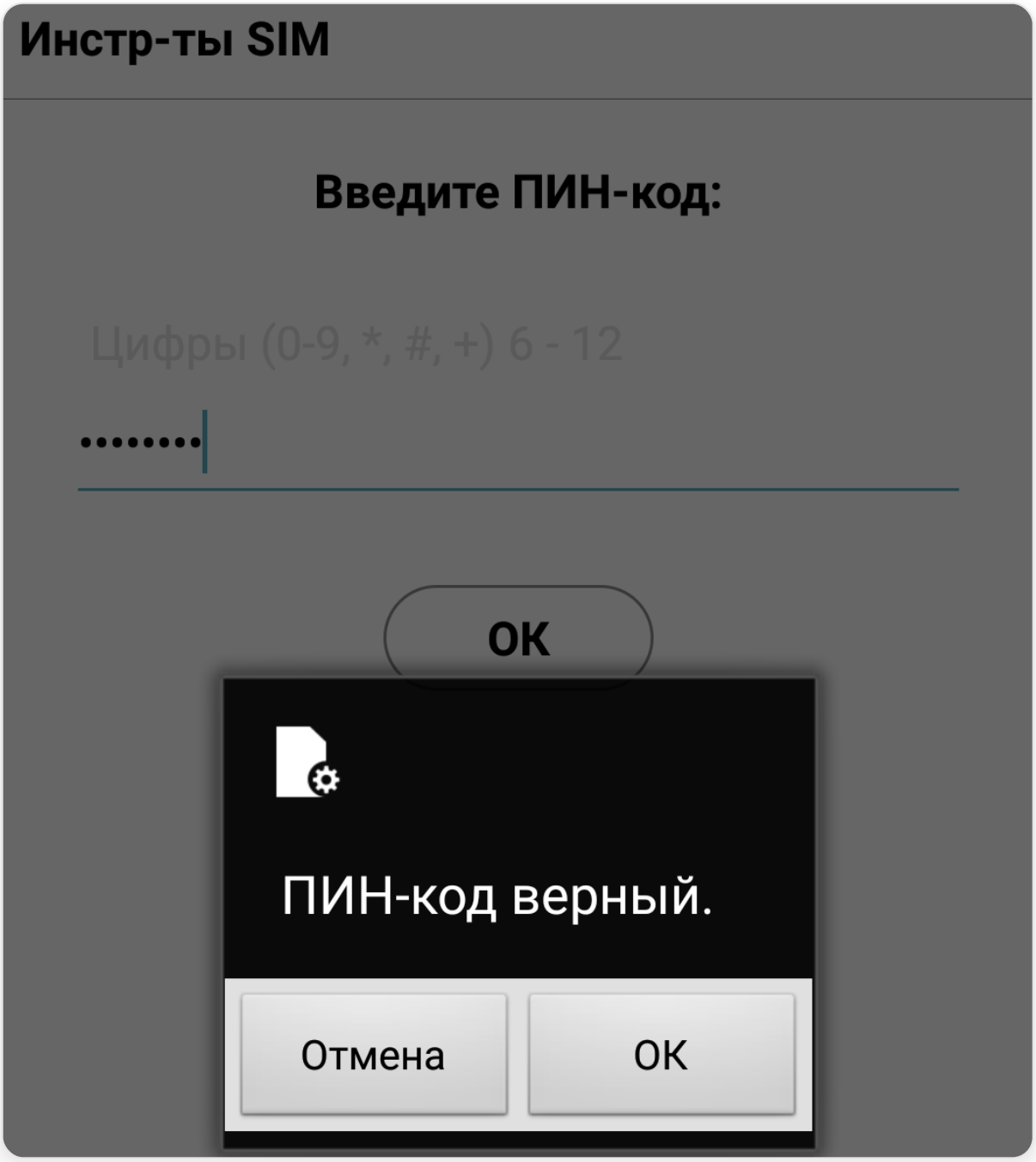
8. Выберите флаг **“Документы просмотрены перед их подписанием”**.



9. Нажмите на кнопку **“Подписать”**. Появится уведомление о том, что нужно подтвердить операцию на телефоне. На телефоне появится всплывающее уведомление о подтверждении операции подписи. **Сверьте идентификаторы и нажмите “ОК”**.


Подтвердите операцию на телефоне
Подпись документов. Тип подписи: CMS. Идентификатор запроса
Сертификат
Подпись документов.
Тип подписи: CMS.
Идентификатор запроса
Сертификат:
Отмена
OK

10. **Введите ПИН-код**, подтверждающий подпись. Если ПИН-код не был задан, этот шаг пропускается. Нажмите **“OK”**.



11. Документ будет подписан. В приложении КриптоАРМ ГОСТ сменятся статус и иконка документа.

Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.

Открыть статью на сайте

Что нужно для юридически значимого ЭДО

Архив. КриптоАРМ ГОСТ.

Электронная подпись – это атрибут электронного документа, позволяющий установить авторство: она может быть равнозначна рукописной подписи, а значит, обеспечивает подписанным электронным документам юридическую силу. На территории РФ в электронном документообороте можно использовать три вида подписей: простую, усиленную неквалифицированную и усиленную квалифицированную. Такая классификация установлена **статьей 5 63-ФЗ “Виды электронных подписей”**.

Классификация электронных подписей:

1. Простая электронная подпись - это подпись, которая подтверждает подпись документа владельцем. Она не может подтвердить неизменность документа. При организации документооборота необходимо заключать договор, который подтверждает её подлинность.

2. Неквалифицированная электронная подпись (НЭП) - это подпись, которая подтверждает авторство и неизменность документа. Для неквалифицированной электронной подписи используются ключи шифрования: закрытый и открытый. При организации документооборота также необходимо заключать договор, который подтверждает её подлинность. НЭП может подтверждаться сертификатом, но это не обязательное условие её получения.

3. Усиленная квалифицированная электронная подпись (УКЭП) - это НЭП, которая выдаётся только теми Удостоверяющими центрами, которые прошли аккредитацию Минкомсвязи РФ. Такие подписи используются в работе с госорганами и в ведении внешнего ЭДО. При использовании УКЭП не нужно заключать договор, удостоверяющий её подлинность, она имеет юридическую силу без дополнительных условий.

Чтобы самостоятельно организовать юридически значимый ЭДО, нужно:

1. **Подписать соглашение об ЭДО** с контрагентами согласно №63-ФЗ “Об электронной подписи”;

2. **Определить лицо, ответственное за подпись электронных документов**, и составить доверенность с его полномочиями;

3. **Получить квалифицированную электронную подпись** согласно №63-ФЗ “Об электронной подписи”;

4. **Приобрести КриптоАРМ ГОСТ** - программу для подписи и шифрования документов: она сертифицирована ФСБ России и подписывает пакеты файлов (например, архивы .rar и .zip), автоматически создаёт и проверяет электронные подписи;

5. **Определить сроки хранения электронных документов**, идентичные срокам хранения бумажных аналогов.

Открыть статью на сайте

Как проверить подлинность электронной подписи на документе

Архив. КриптоАРМ ГОСТ.

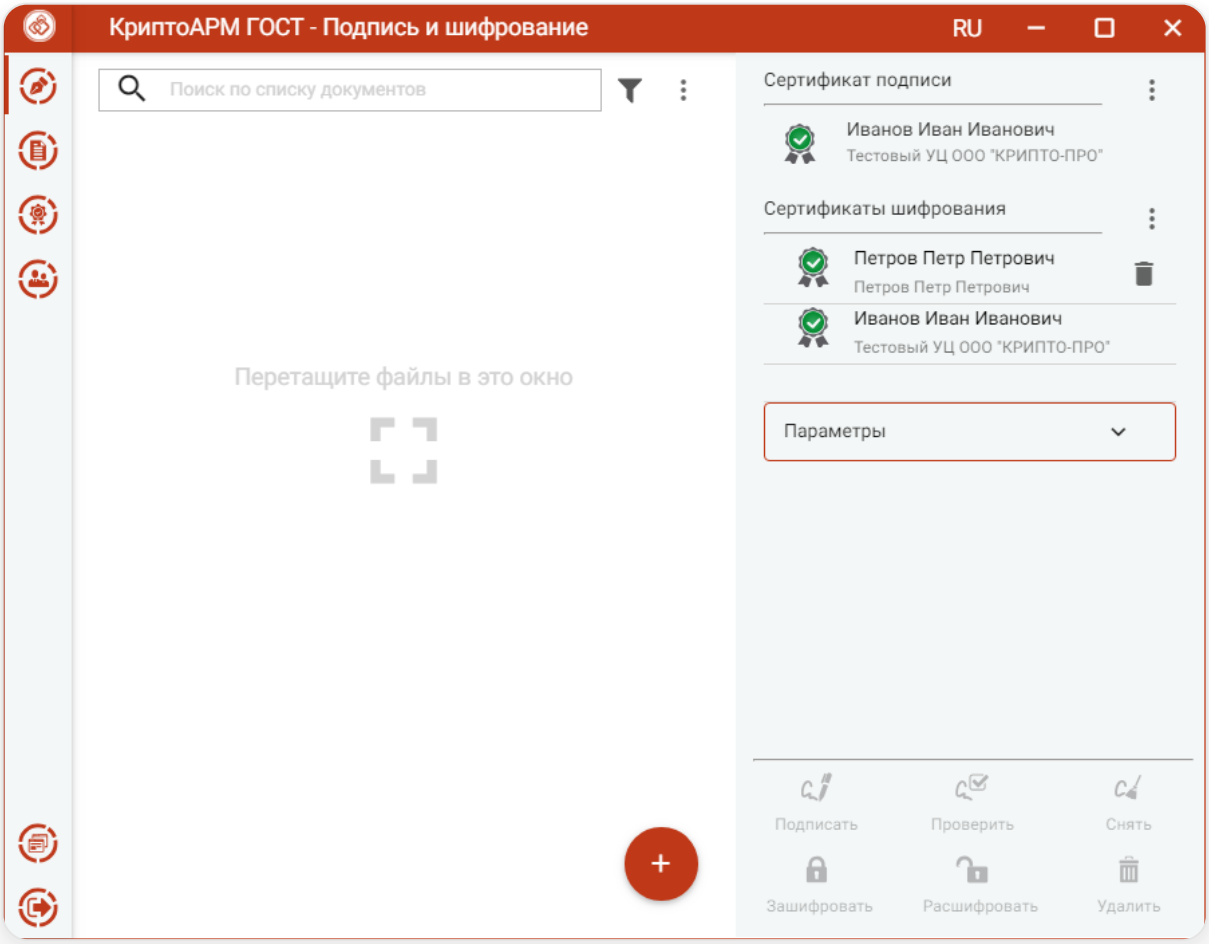
Для того, чтобы убедиться в юридической силе электронного документа, необходимо проверить действительность электронной подписи (ЭП). Проверка позволяет убедиться в том, что ЭП выдана аккредитованным удостоверяющим центром, а срок её действия ещё не истек.

Подлинность ЭП нужно проверять, чтобы:

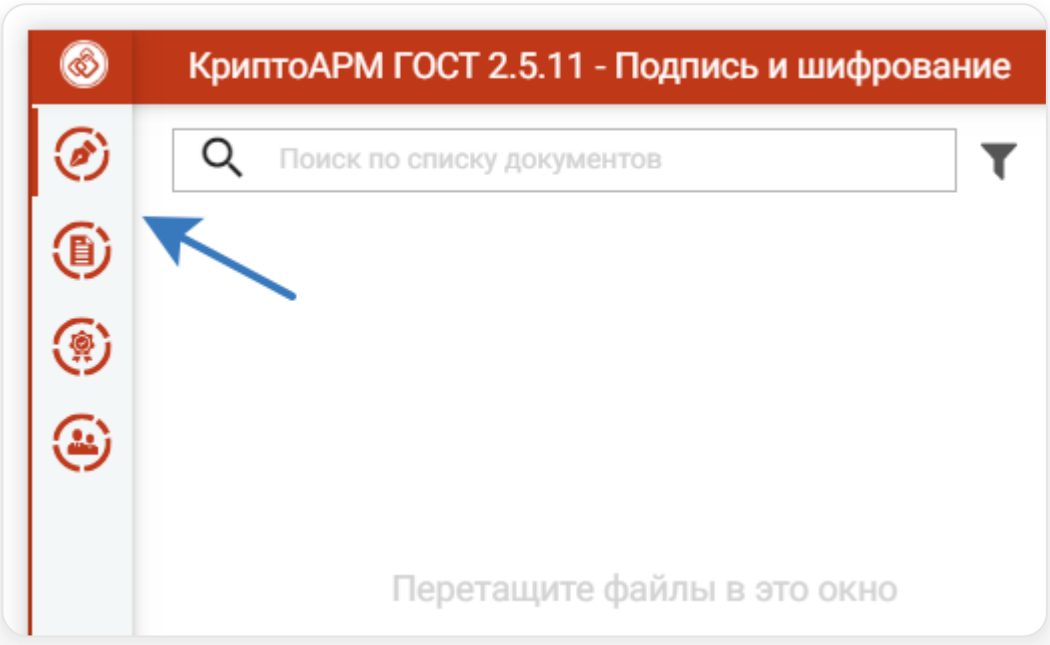
1. Удостовериться, что документ подписало правомерное подписывающее лицо;
2. Убедиться в подлинности документа;
3. Удостовериться, что лицо поставило ЭП не случайно;
4. Убедиться в достоверности ЭП в случае отказа лица от подписи;
5. Убедиться в том, что у ЭП не закончился срок действия.

Как проверить подлинность ЭП:

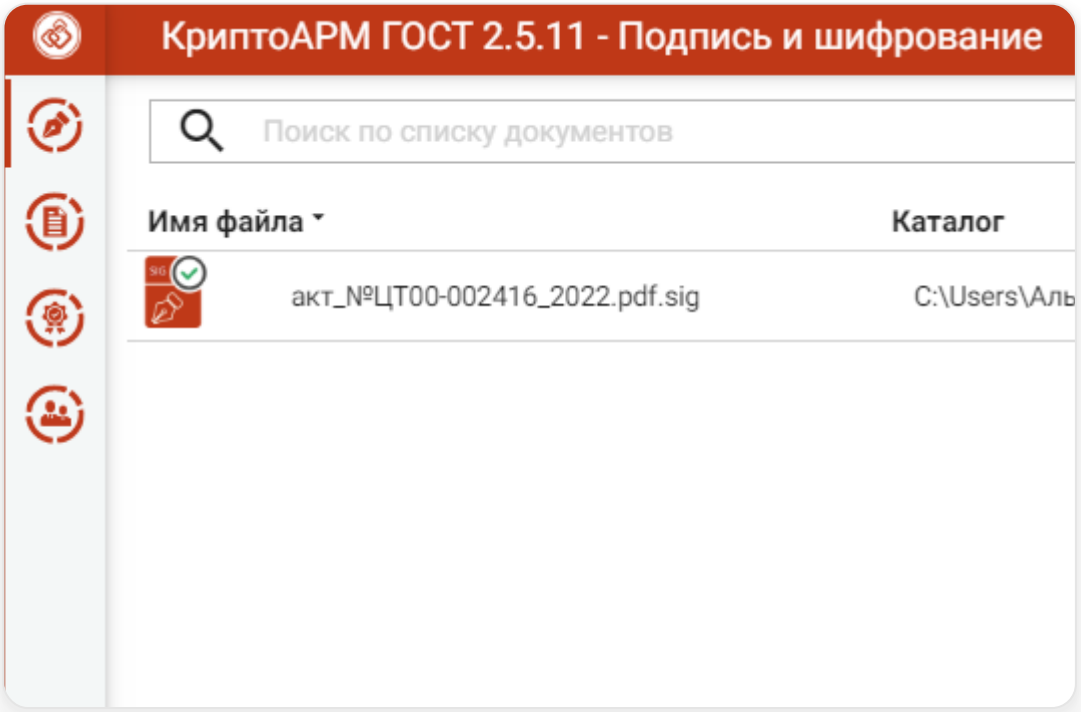
1. Откройте КриптоАРМ ГОСТ.



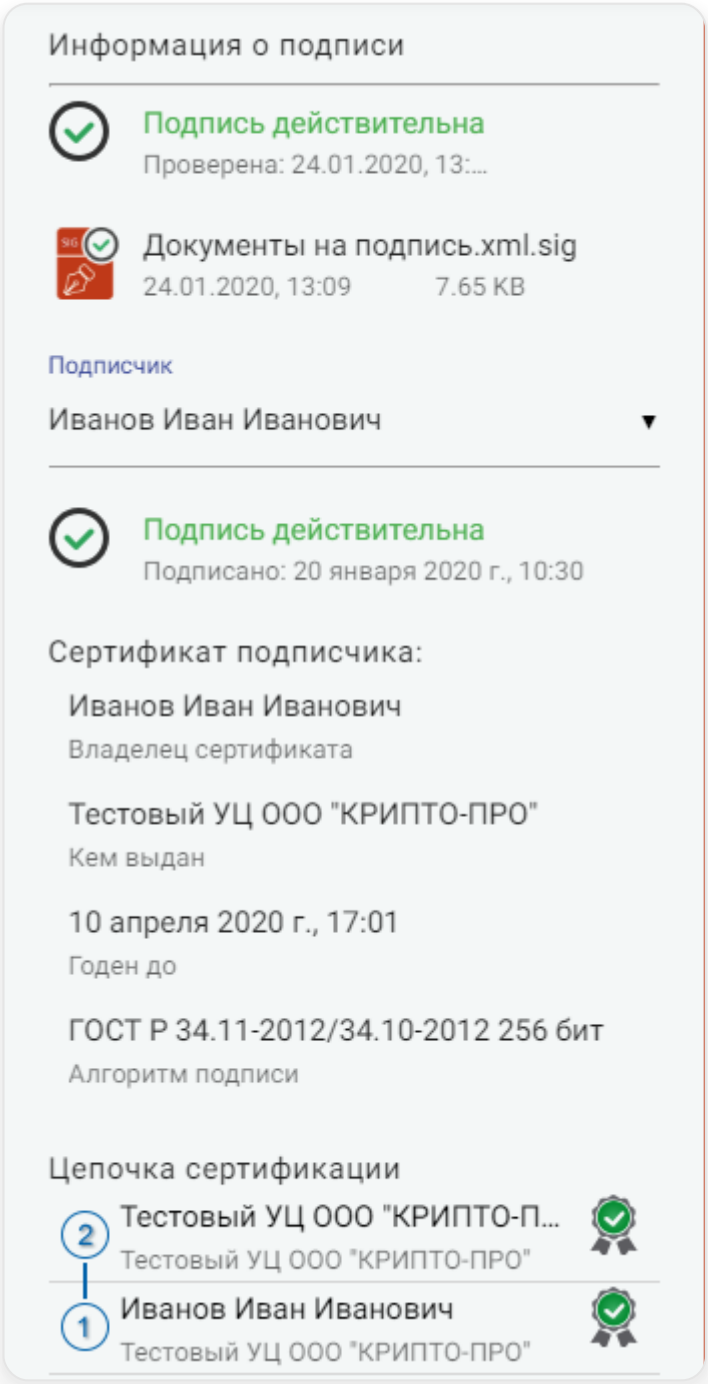
2. Перейдите во вкладку **“Подпись и шифрование”**.



3. Нажмите на **“+”** или перетащите подписанный файл мышью в список документов.



4. Программа автоматически проверит подпись файла. Информация о подписи появится в правой области экрана.



Открыть статью на сайте

Как установить сертификат из DSS (облачную подпись) в КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ.

Облачная электронная подпись – это электронная подпись (ЭП), основные сведения которой хранятся не на токенах или смарт-картах, а в облачном хранилище – в “DSS”. Все вычисления в процессе операций с облачной ЭП происходят на внешнем сервере, а пользователю нужно лишь подтвердить свою личность с помощью ввода пароля.

Плюсы облачного хранения ключей:

1. Нет физического носителя, который можно потерять или сломать;
2. Доступна в любое время;
3. Простота в использовании: нужны Интернет, браузер и наше приложение КриптоАРМ на любом устройстве.

Минусы:

1. Нужен подключенный Интернет;
2. Иногда нужен телефон для подтверждения операций через SMS-сообщения;

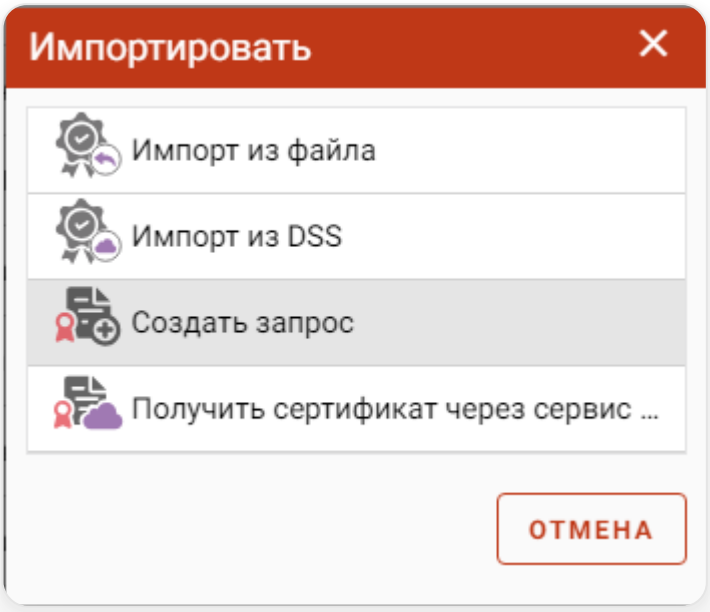
Чтобы установить облачную подпись в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.

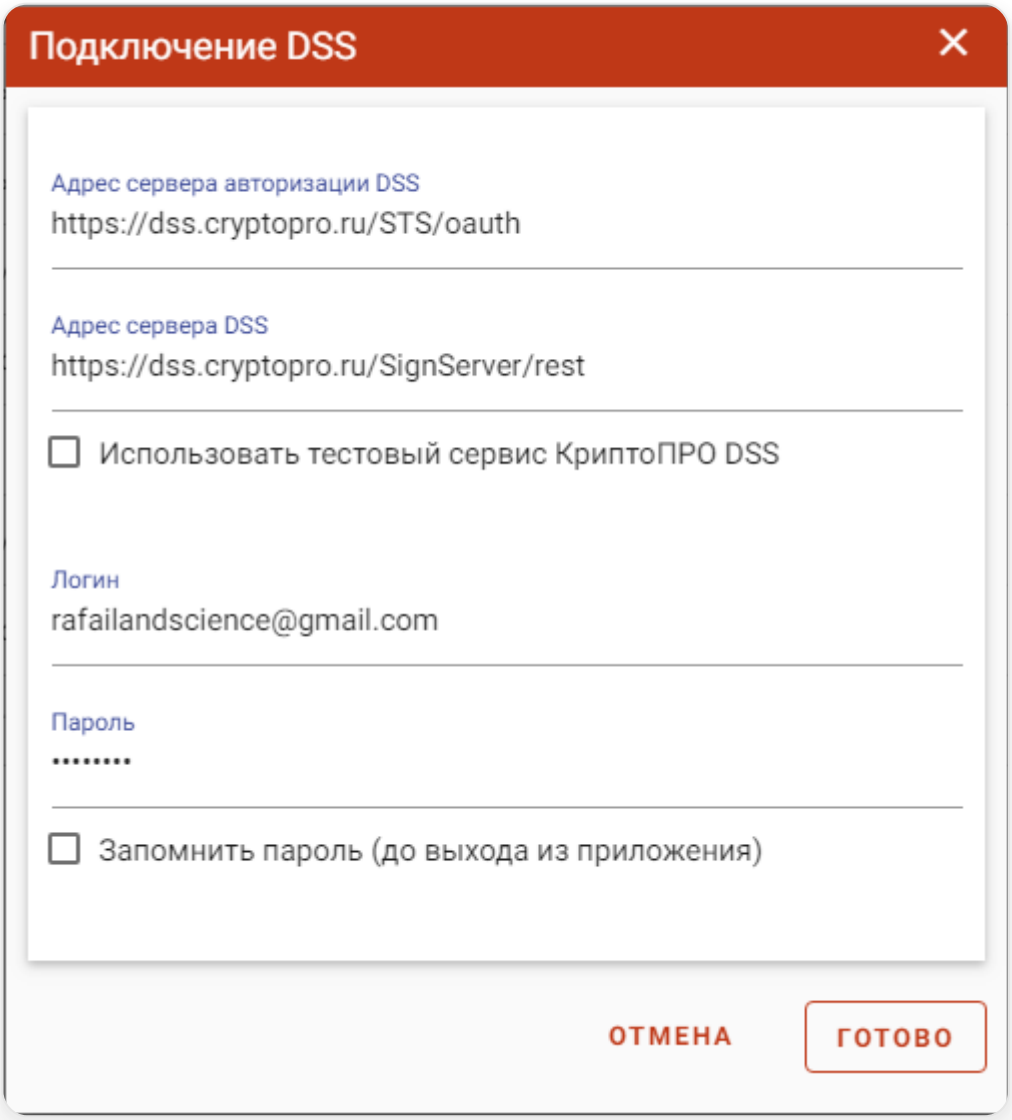
2. В контекстном меню программы зайдите на вкладку **“Сертификаты”**.



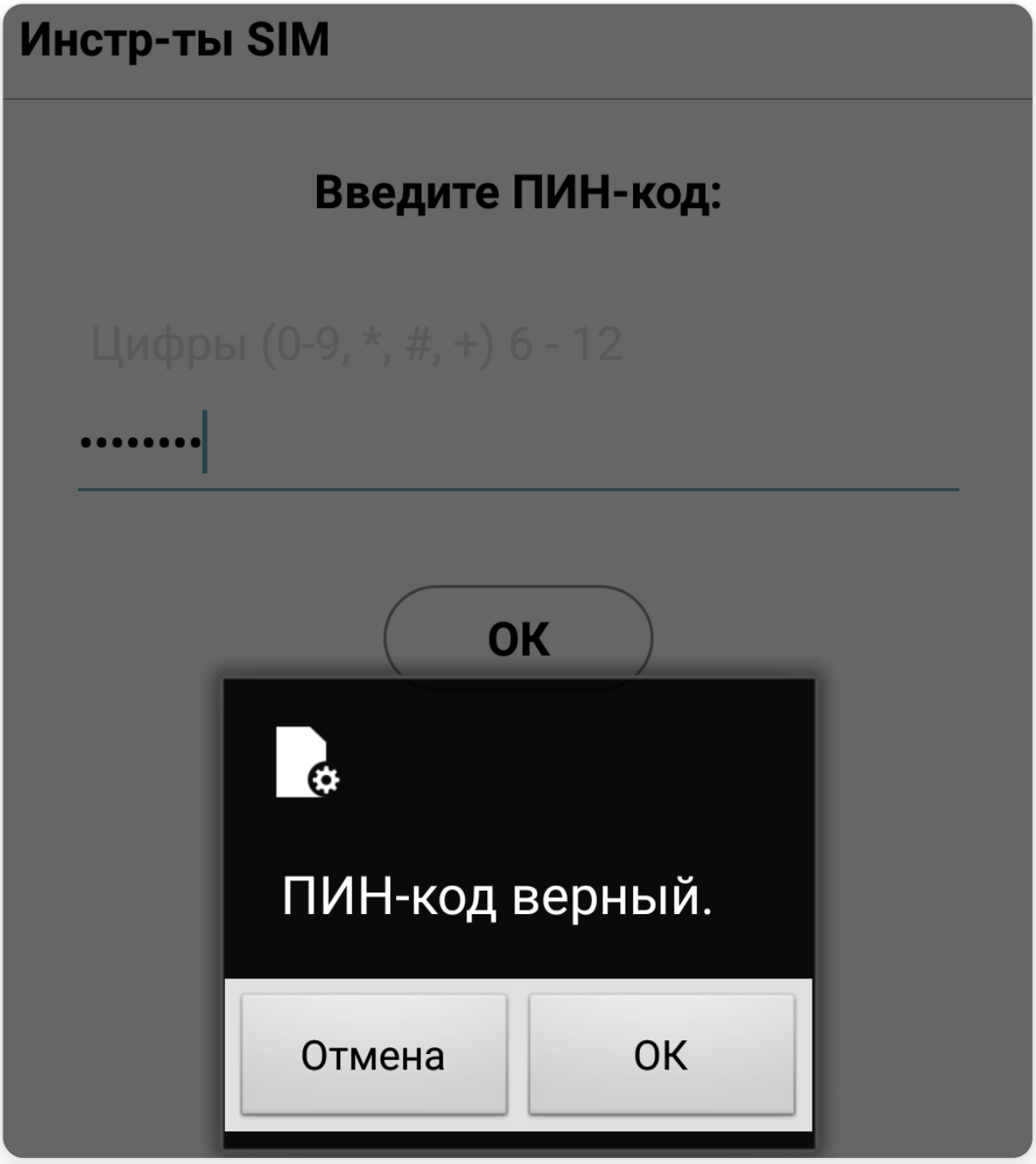
3. Нажмите на кнопку **“+”**, чтобы добавить сертификат, и выберите пункт **“Импорт из DSS”**.



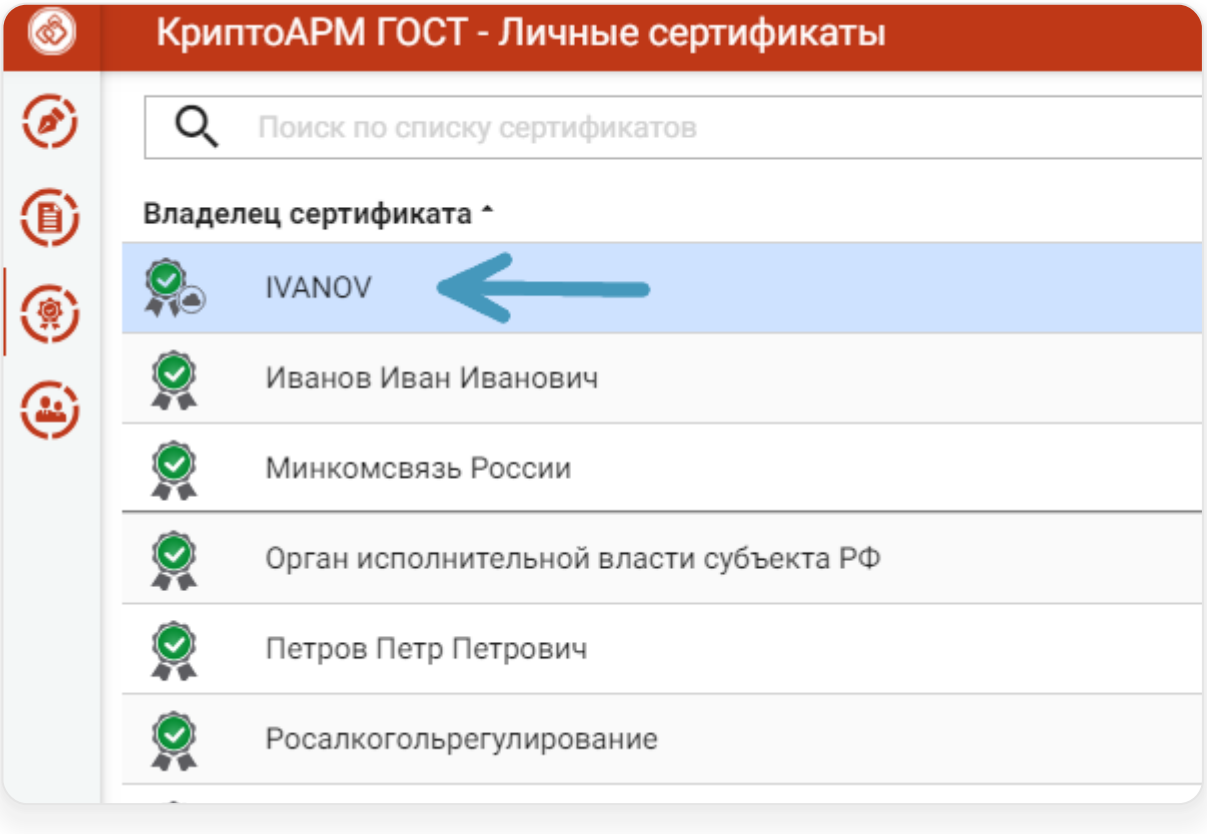
4. Введите адреса **“Сервера авторизации”** и **“Сервера DSS”**, а затем **логин и пароль** для авторизации на сервере.



5. Нажмите на кнопку **“Готово”**. На телефоне нужно будет **ввести пин-код**, подтверждающий добавление облачной подписи.



6. Сертификат импортируется в Ваше личное хранилище сертификатов и будет помечен иконкой с облаком.



Облачный сертификат успешно установлен. В программе КриптоАРМ ГОСТ его можно найти во вкладке **“Сертификаты”**, **в разделе “Личное хранилище сертификатов”**. Теперь можно подписывать файлы облачной подписью для любых сервисов.

Открыть статью на сайте

Как подписать исковое заявление через ГАС “Правосудие” и “Мой арбитр”

Архив. КриптоАРМ ГОСТ.

С 1 января 2017 года исковые заявления в Верховный Суд РФ, арбитражные суды и суды общей юрисдикции можно подавать в виде электронных документов. Приём обращений ведётся через системы ГАС “Правосудие” и “Мой Арбитр”. Войти в системы можно с помощью подтвержденной учётной записи ЕСИА: для этого зарегистрируйтесь на портале “Госуслуги” и подтвердите свою учётную запись. Также войти в системы ГАС “Правосудие” и “Мой Арбитр” можно с помощью усиленной квалифицированной электронной подписи.

В ГАС “Правосудие” принимаются исковые заявления физических лиц против физических или юридических лиц в городские, районные и мировые суды. Юридические лица для подачи документов в арбитражные суды могут воспользоваться похожим сервисом “Мой Арбитр”. Сервис используется только для арбитражных судов, в нём рассматриваются исковые заявления с участием только юридических лиц.

Электронные документы должны быть подписаны усиленной квалифицированной электронной подписью в соответствии с **№ 220-ФЗ “О внесении изменений в отдельные законодательные акты Российской Федерации в части применения электронных документов в деятельности органов судебной власти”**.

Требования к электронному документу, направляемому в ГАС “Правосудие” и “Мой Арбитр”:

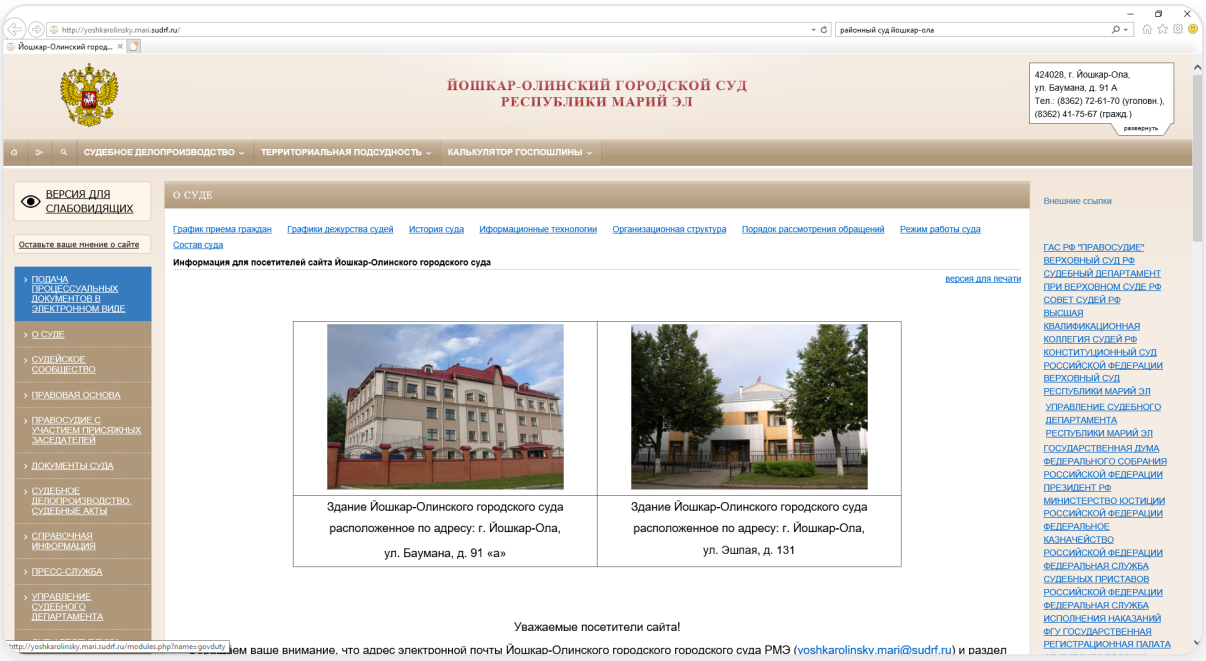
1. Файл обращения в суд должен быть создан в формате PDF с возможностью копирования текста;
2. Файлы документов, прилагаемых к обращению, должны быть представлены в форматах PDF, RTF, DOC, DOCX, XLS, XLSX, ODT – для документов с текстовым содержанием, PDF, JPEG (JPG), PNG, TIFF – для документов с графическим содержанием;
3. Размер каждого файла не должен превышать 30 Мб;
4. Имя файла должно ясно отображать назначение документа и количество листов в нём (например, Доверенность 65 от 10012020 1л.pdf);
5. При подписи файла должна использоваться отсоединенная электронная подпись (должна содержаться в отдельном файле);
6. Электронный документ должен быть подписан лицом, которое указано в тексте электронного документа как подписант.

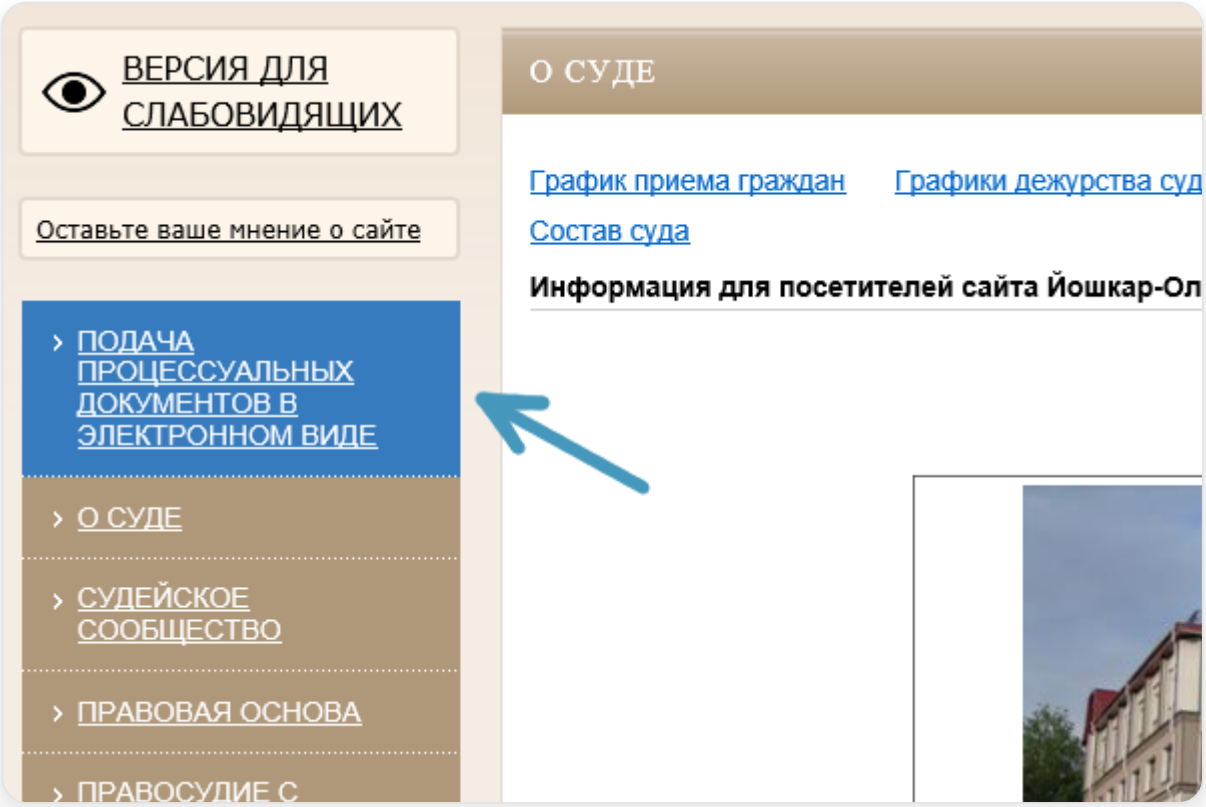
Требования к скану документа (электронному образу), направляемому в ГАС “Правосудие” и “Мой Арбитр”:

1. Документ должен быть отсканирован в масштабе 1:1 в черно-белом или сером цвете в качестве 200-300 точек на дюйм с сохранением всех реквизитов и аутентичных знаков подлинности;
2. Сканирование в режиме цветной печати выполняется только в том случае, если в документе содержатся цветные графические изображения или цветной текст, и передача цвета имеет значение для рассмотрения дела;
3. Файл скана документа должен быть представлен в формате PDF с возможностью копирования текста;
4. Размер каждого файла не должен превышать 30 Мб;
5. Имя файла должно ясно отображать назначение документа и количество листов в нём (например, Доверенность 65 от 10012020 1л.pdf).

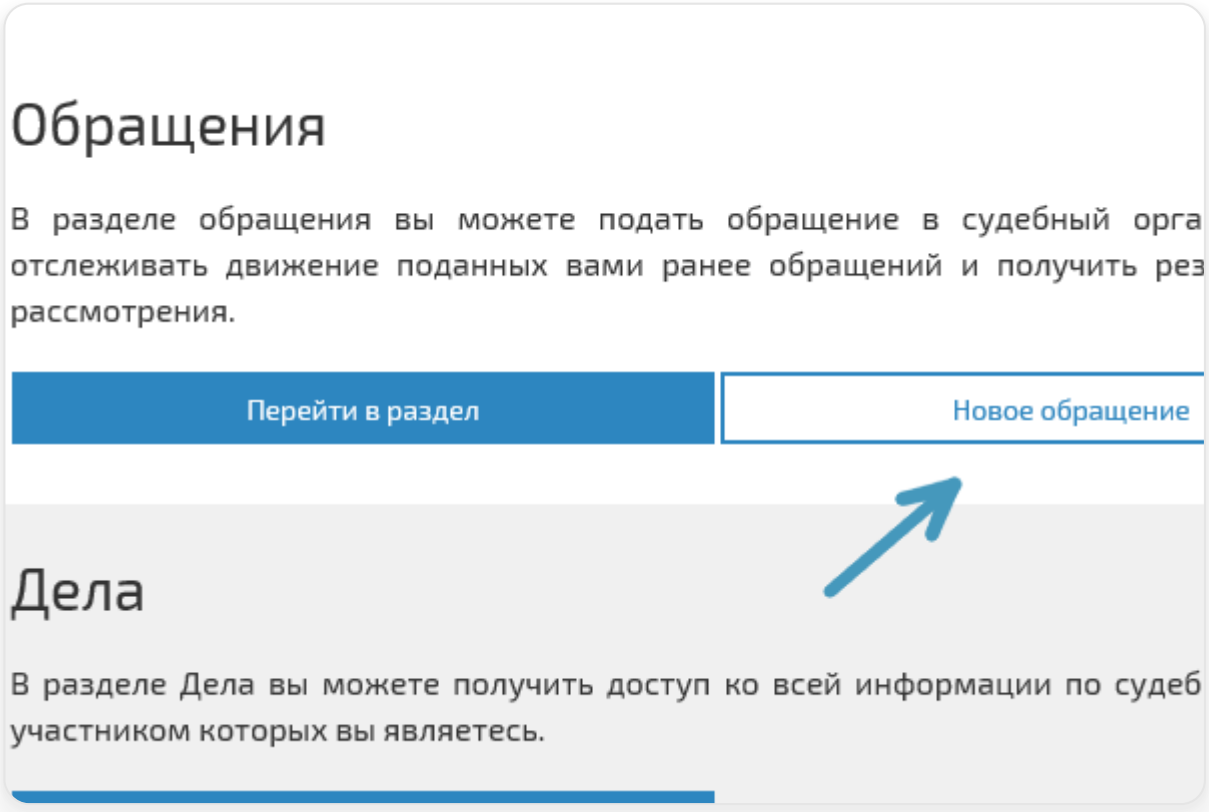
Чтобы подать исковое заявление в электронном виде для ГАС “Правосудие”:

1. На сайте нужного Вам суда выберите **пункт “Подача процессуальных документов в электронном виде”** в меню слева.

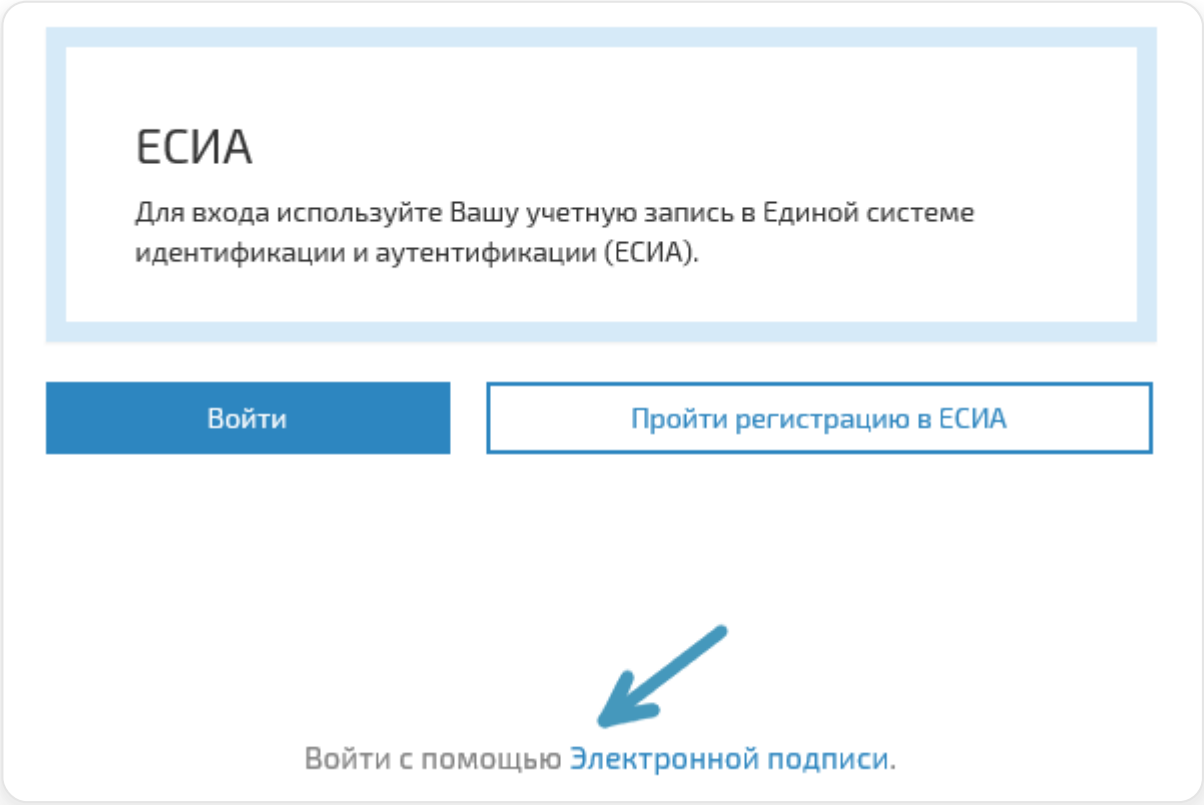



ВЕРСИЯ ДЛЯ СЛАБОВИДЯЩИХ
Оставьте ваше мнение о сайте
ПОДАЧА ПРОЦЕССУАЛЬНЫХ ДОКУМЕНТОВ В ЭЛЕКТРОННОМ ВИДЕ
О СУДЕ
СУДЕЙСКОЕ СООБЩЕСТВО
ПРАВОВАЯ ОСНОВА
ПРАВОСУДИЕ С
О СУДЕ
График приема граждан
Графики дежурства суд
Состав суда
Информация для посетителей сайта Йошкар-Ол

2. Откроется ГАС “Правосудие”. В **разделе “Обращения”** нажмите на кнопку **“Новое обращение”**.



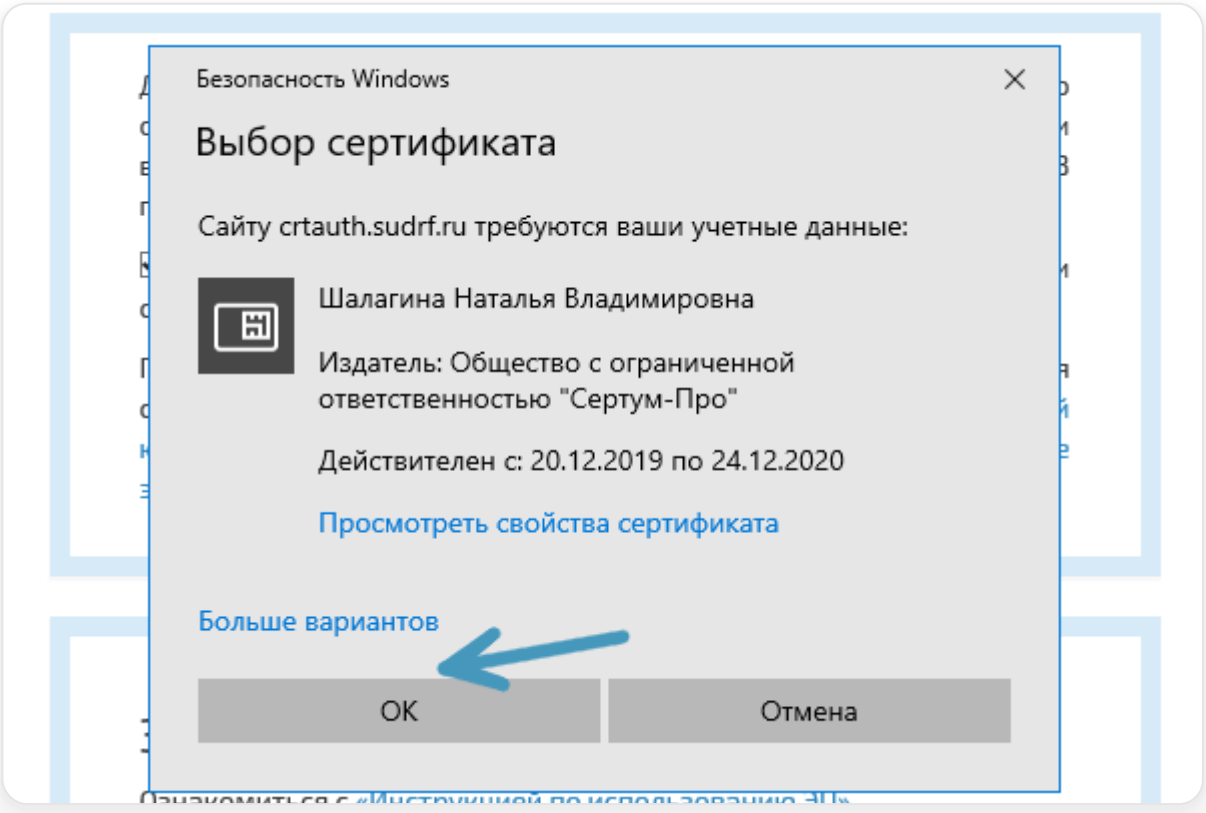
3. На **странице “Авторизация пользователя”** выберите **пункт “Войти с помощью Электронной подписи”**.

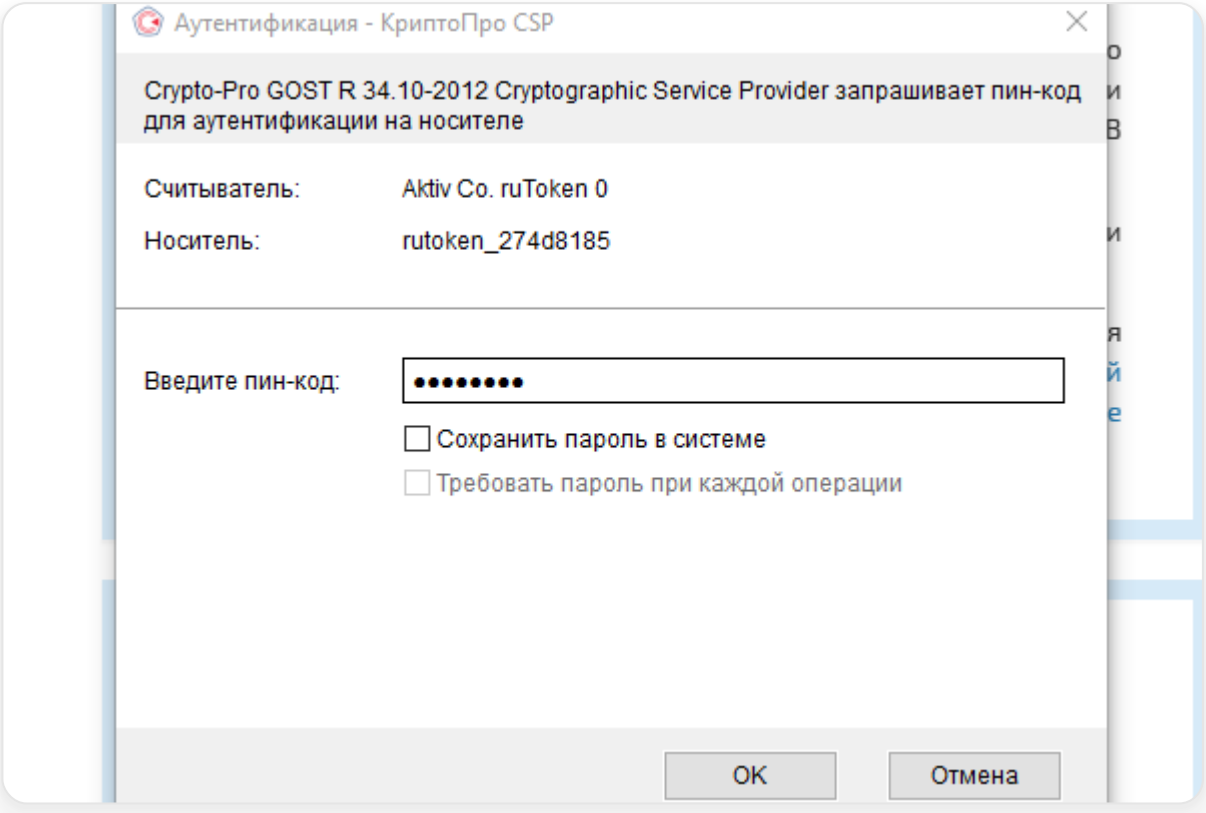


4. Убедитесь, что вы пользуетесь **браузером Internet Explorer 10 и выше**, что на рабочем месте установлен **криптопровайдер КриптоПро CSP 5.0**.

5. Прочитайте пользовательское соглашение и подтвердите согласие с ним.

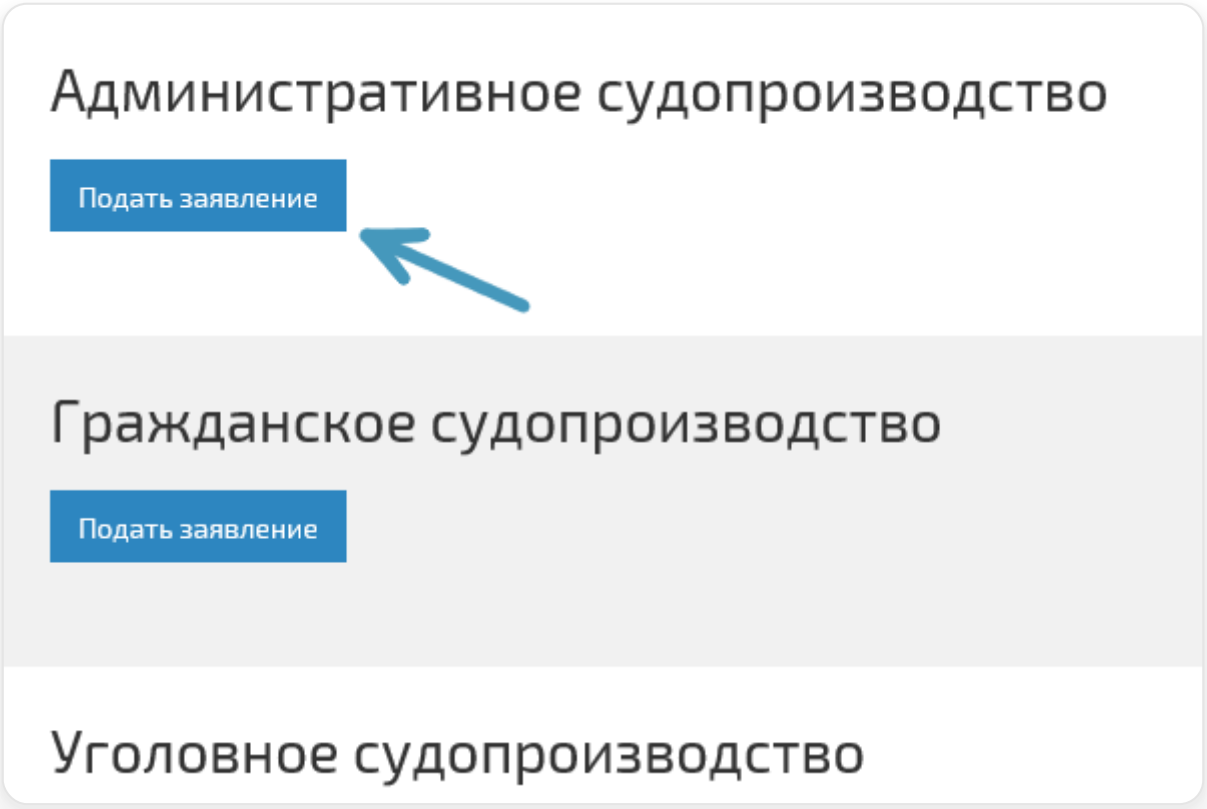
6. Выберите сертификат электронной подписи в открывшемся окне подтверждения доступа.



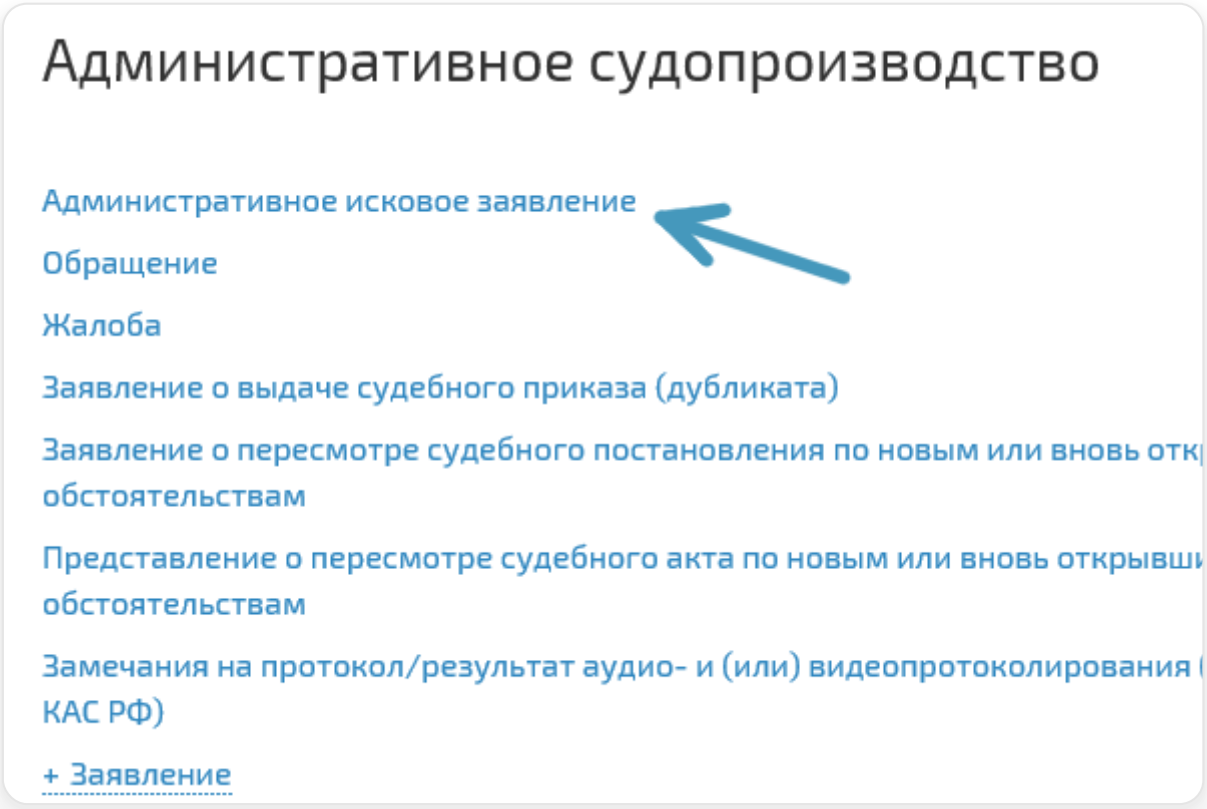


7. Нажмите на кнопку **“ОК”**, затем кнопку **“Войти”**.

8. Откроется страница **“Подать заявление”**, но уже с авторизованным пользователем.

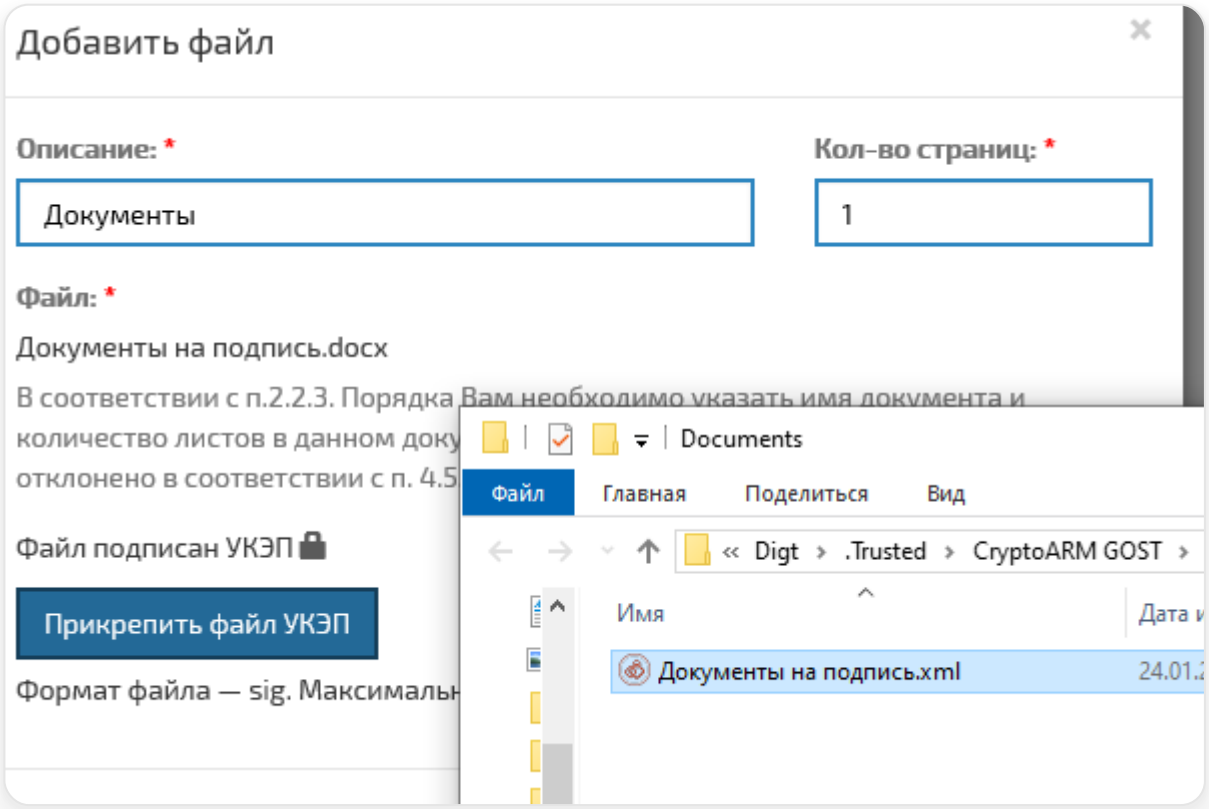


9. Выберите судопроизводство, согласно которому Вы хотите подать иск. Нажмите на кнопку **“Подать заявление”**, в открывшемся меню нажмите **“Исковое заявление”**.



10. Заполните реквизиты заявителя и прикрепите все необходимые документы.

11. При заполнении разделов “Приложения к заявлению”, “Суть заявления”, “Уплата госпошлины” и документа, подтверждающего полномочия, **в разделе “Представитель”** помимо неподписанных документов нужно прикрепить копии этих документов, подписанных электронной подписью в формате ***.sig**.



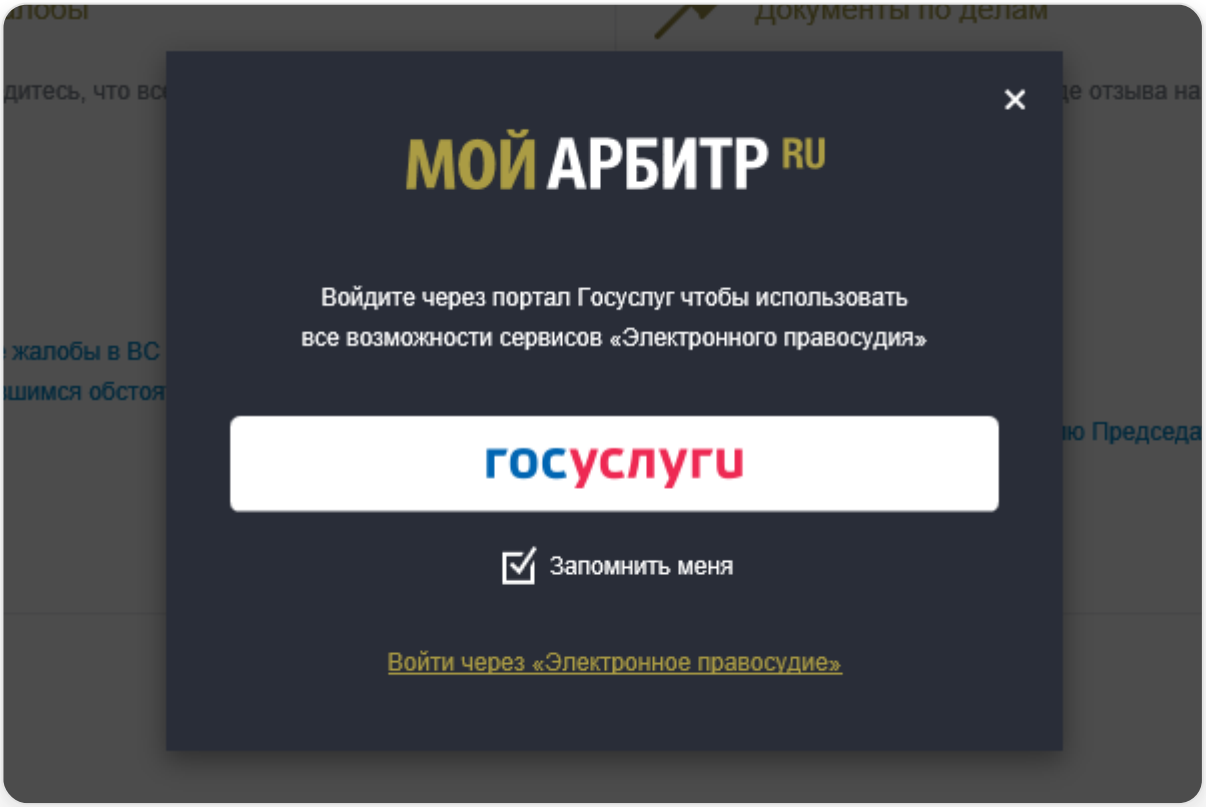
12. Нажмите на кнопку **“Сформировать заявление”**.

13. На форме просмотра черновика заявления нажмите на кнопку **“Отправить заявление”**.

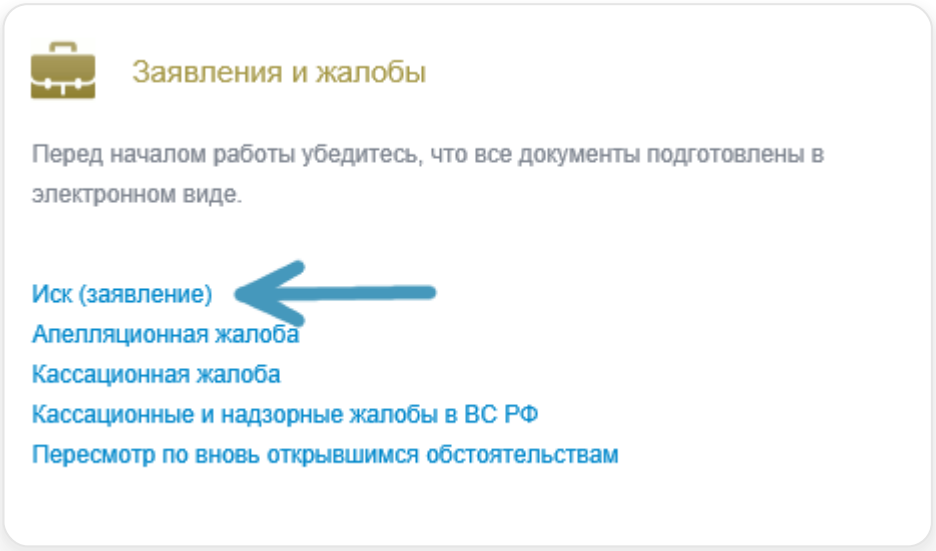
Чтобы подать исковое заявление в электронном виде для “Мой Арбитр”:

1. Откройте сайт “Мой Арбитр”.

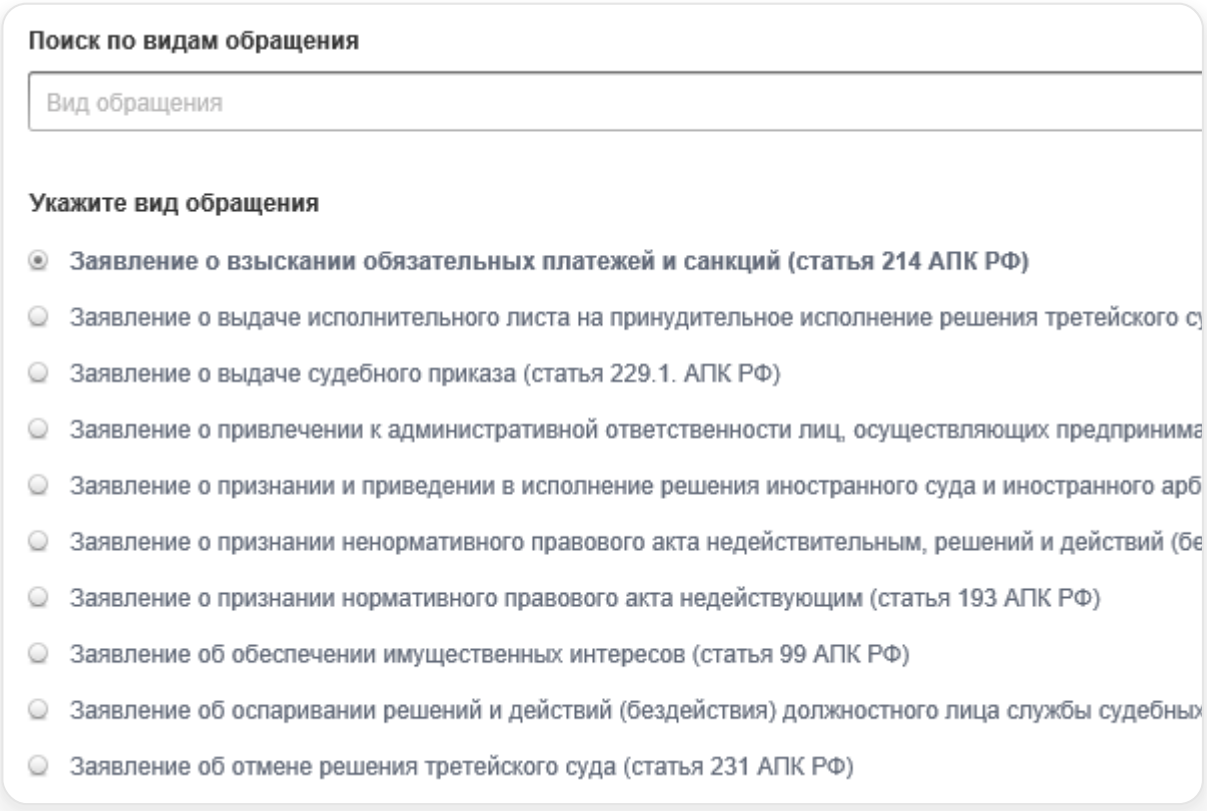
2. Зарегистрируйтесь в личном кабинете системы через **портал “Госуслуги”**.



3. В разделе **“Заявления и жалобы”** выберите **“Иск (заявление)”**.



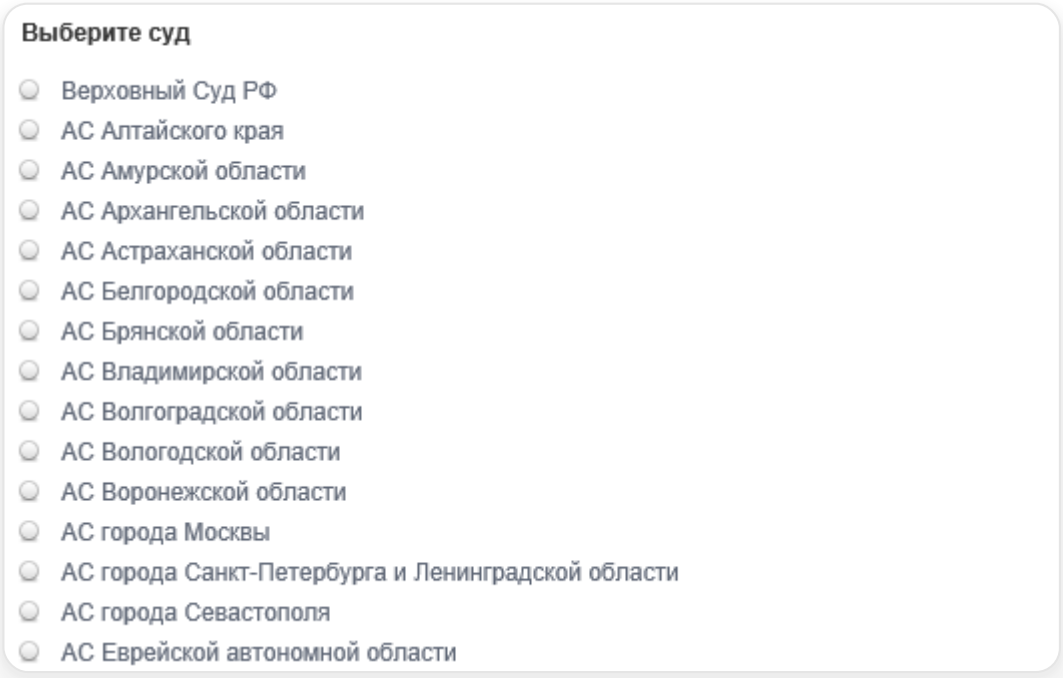
4. Укажите вид обращения. Можно воспользоваться поиском по списку. Нажмите **“Далее”**.



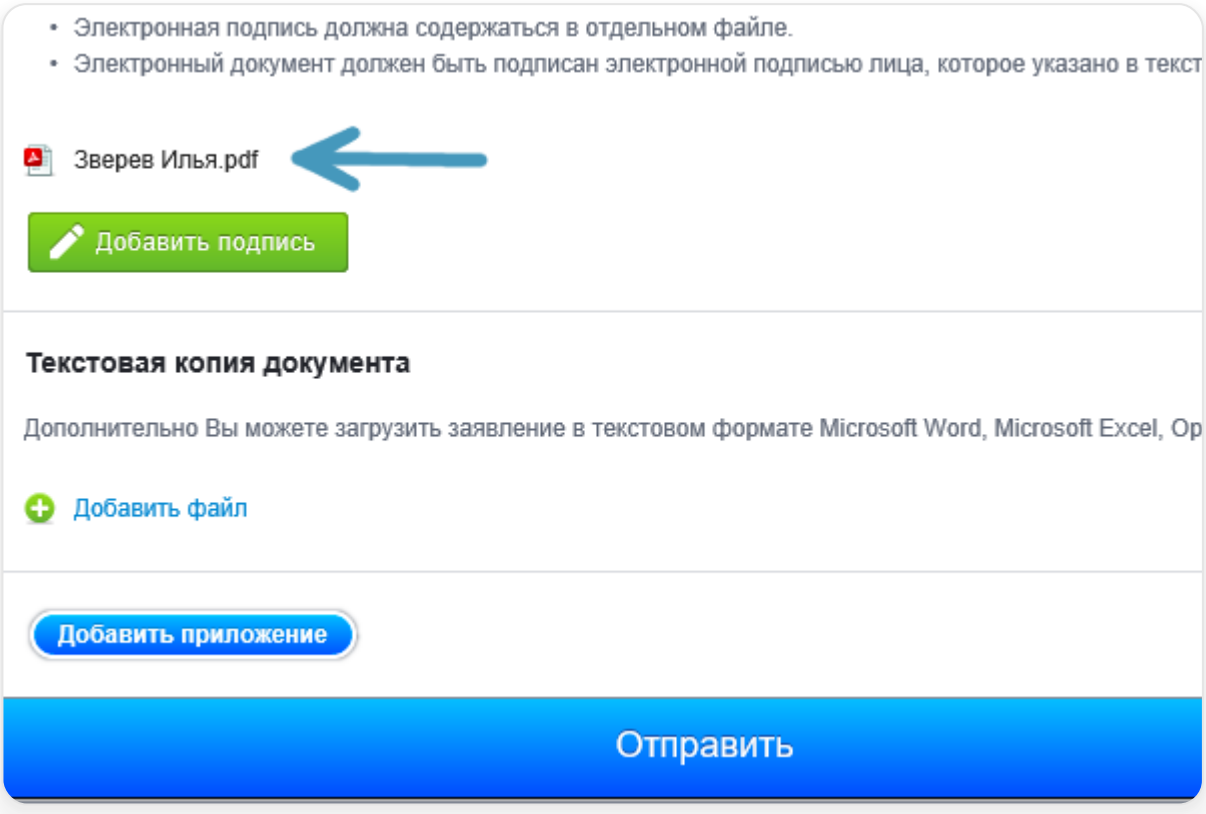
5. Выберите **“Тип участника”** на вкладке **“Истец”**. Укажите необходимые данные. Нажмите **“Далее”**.

6. Выберите **“Тип участника”** на вкладке **“Ответчик”**. Укажите необходимые данные. Нажмите **“Далее”**.

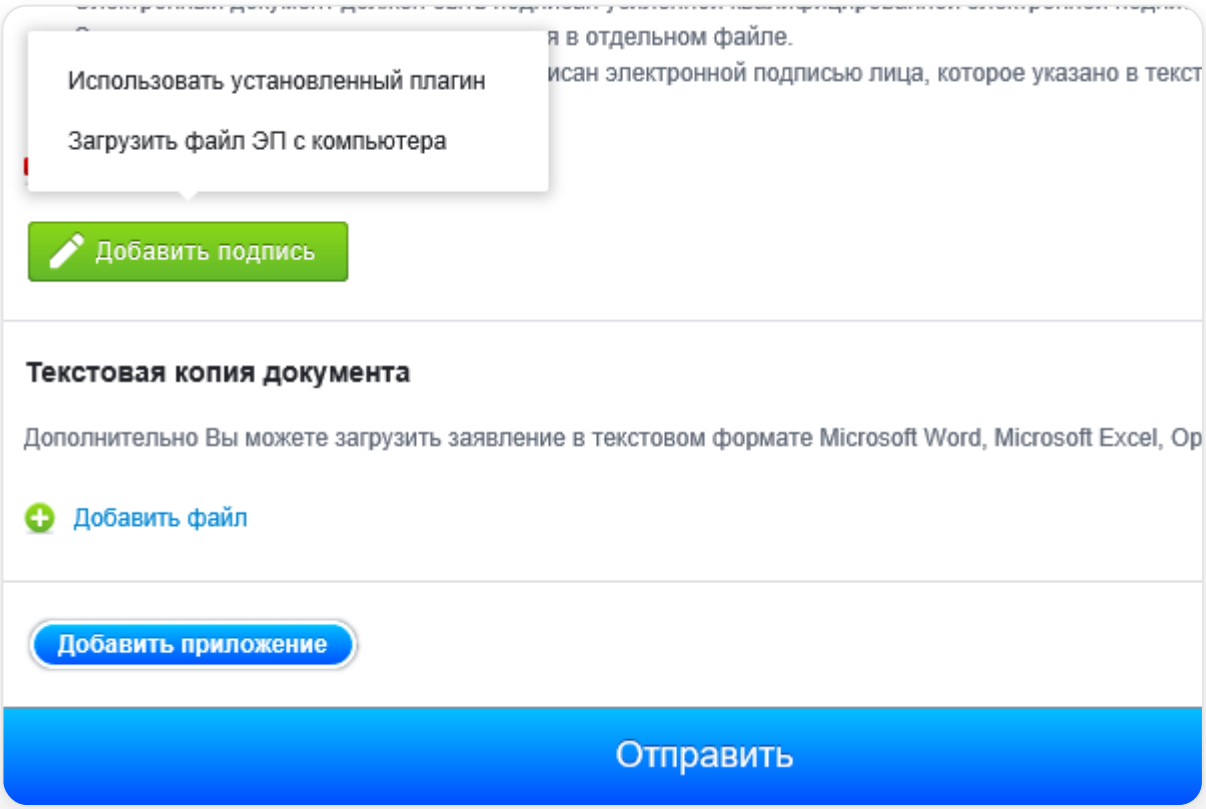
7. Выберите нужный областной Арбитражный суд. Нажмите **“Далее”**.

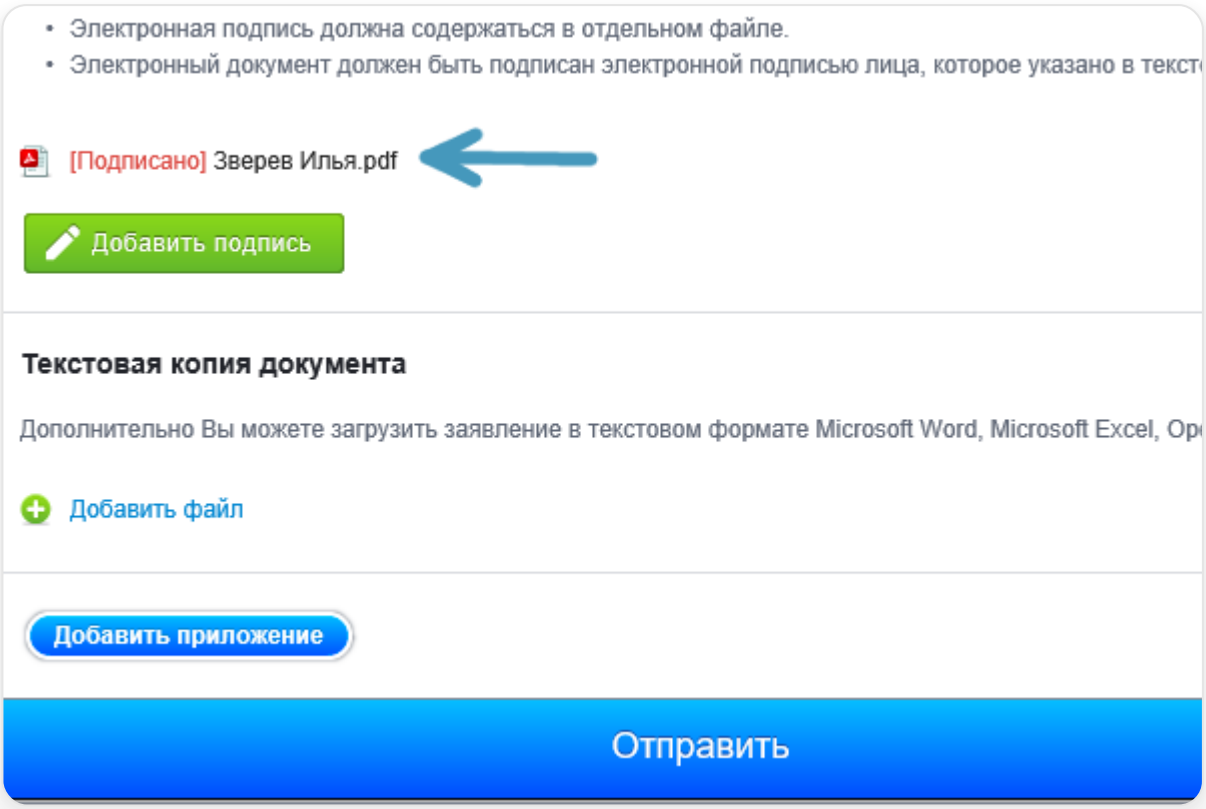


8. На вкладке **“Документы”** в разделе **“Обращение в суд”** прикрепите скан-копию обращения.



9. Появится кнопка **“Добавить подпись”**. Прикрепите версию загруженного файла, подписанную электронной подписью (ЭП). Она должна быть усиленной квалифицированной ЭП. Можете вручную загрузить файл ЭП с компьютера или использовать плагин.





10. Прикрепите текстовую версию обращения.

11. Нажмите кнопку **“Отправить”**.

Открыть статью на сайте

Как подписать документ электронной подписью в КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ.

КриптоАРМ ГОСТ - это программа для электронной подписи и шифрования документов, которая используется при организации электронного документооборота. Электронная подпись (ЭП) является аналогом личной подписи и позволяет обмениваться документами на предприятии и подавать документы в государственные органы удалённо, в электронном варианте, без бумажной волокиты.

Организация электронного документооборота удобнее по сравнению с бумажным и исключает подделку подписей или подпись документов “задним числом”. Использование электронной подписи упрощает взаимодействие с государственными органами. Электронные версии документов, подписанные ЭП, принимают такие государственные органы и инстанции, как Росреестр, ФСРАР, Банк России, РосАккредитация и др.

Чтобы электронная подпись имела юридическую силу, она должна быть квалифицированной, то есть должна быть выдана Удостоверяющим центром, который аккредитован государством.

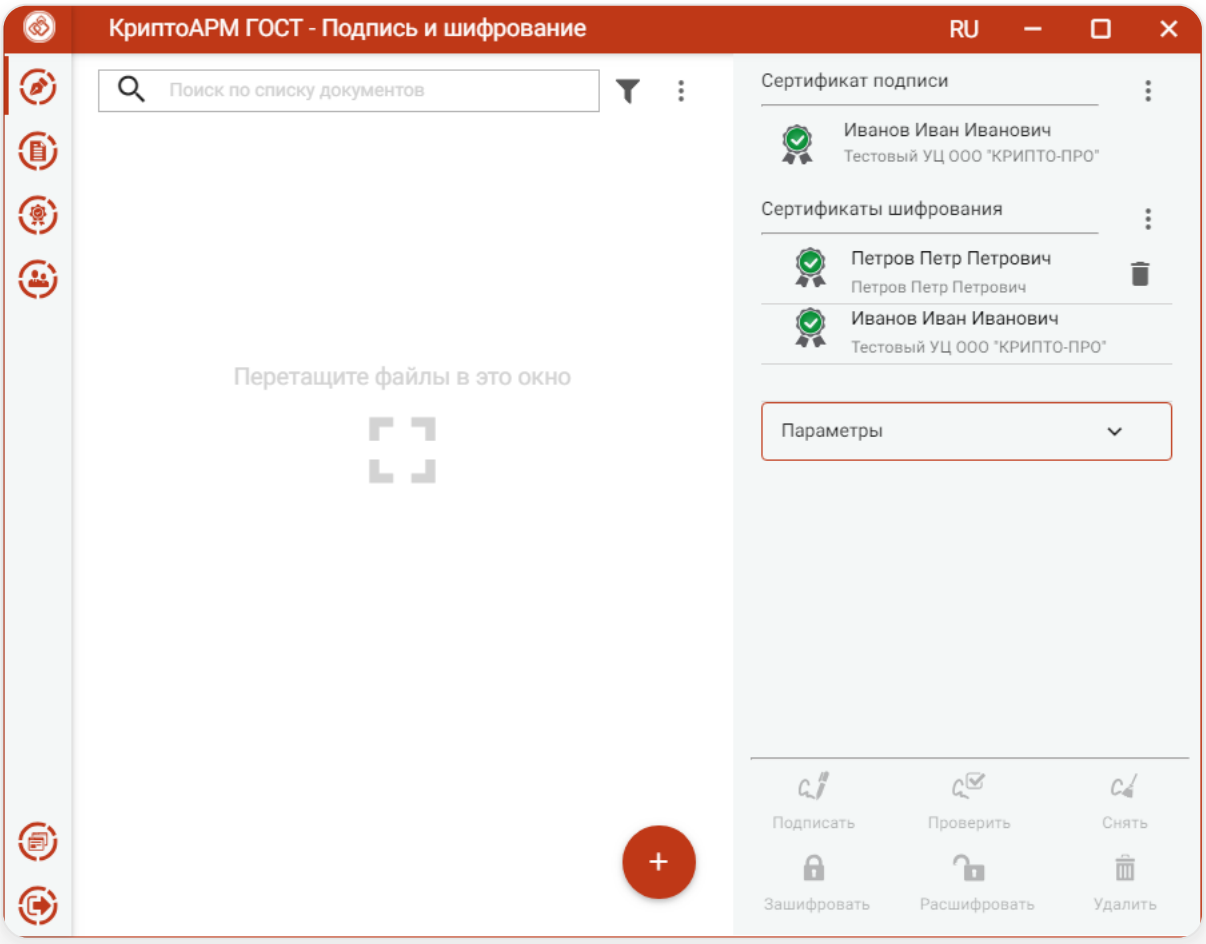
С помощью программы подписи и шифрования документов КриптоАРМ ГОСТ можно подписать и заверить любые виды электронным документов в любом расширении.

Что нужно для подписи файлов:

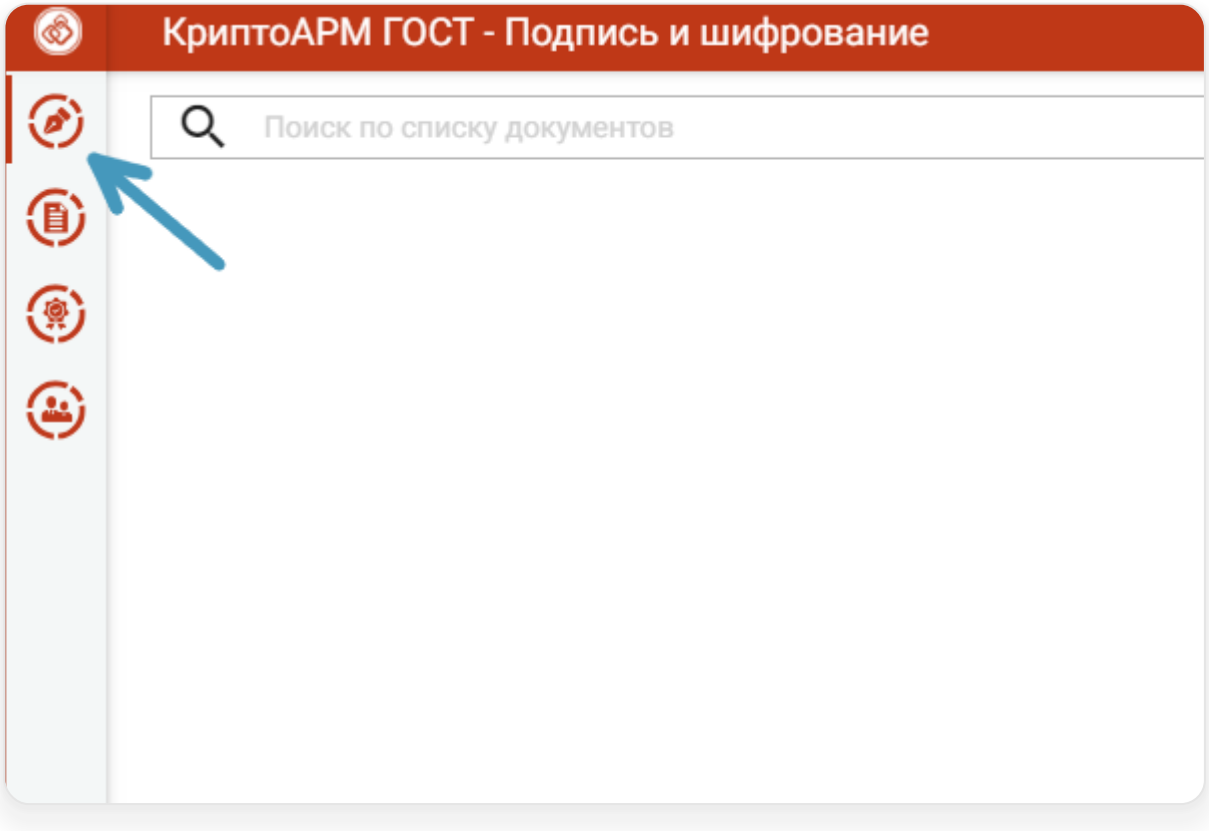
1. КриптоАРМ ГОСТ;
2. КриптоПро CSP;
3. Сертификат электронной подписи.

Чтобы подписать документ в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.



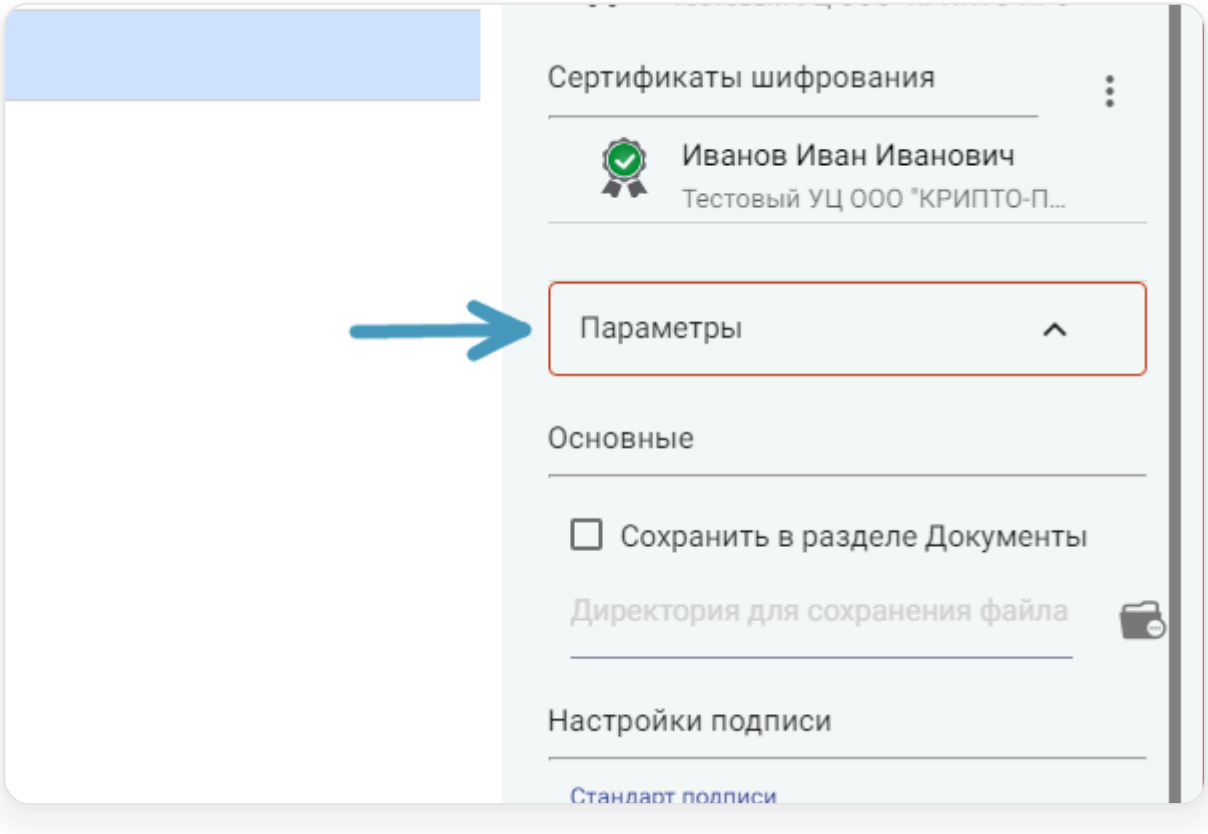
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



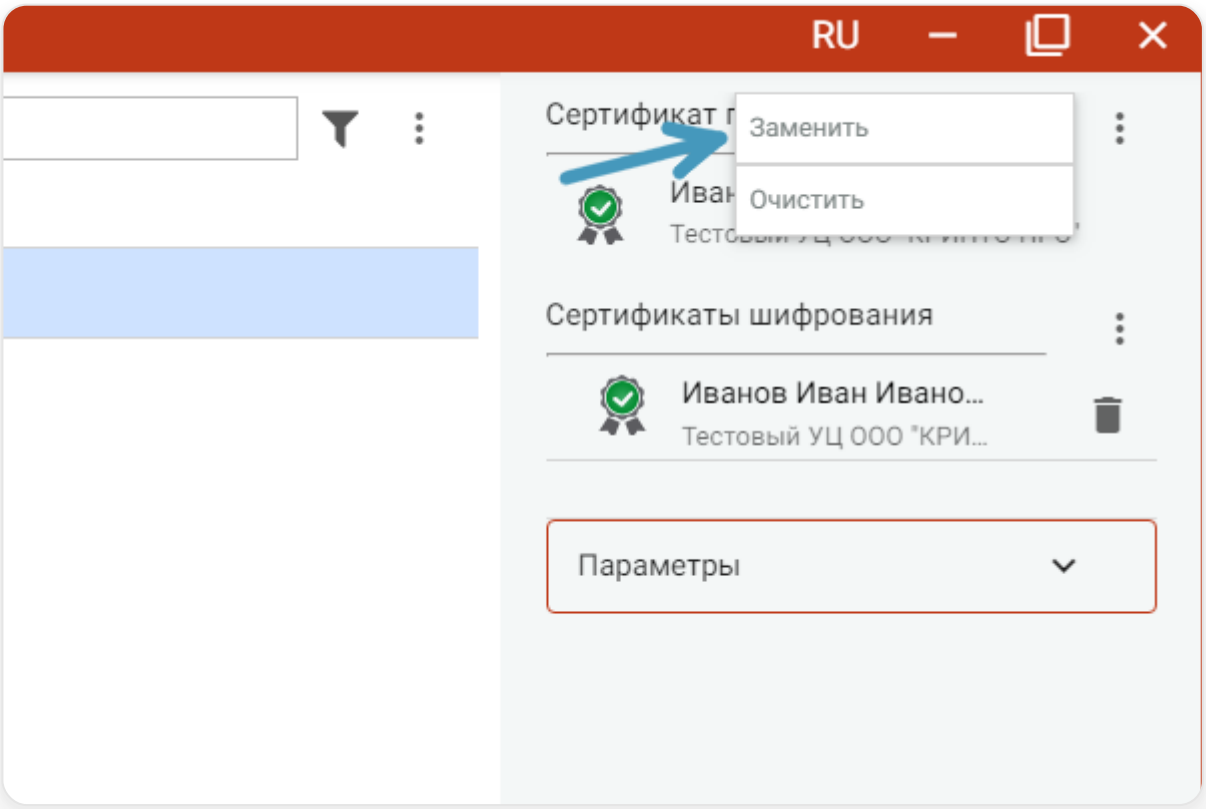
3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

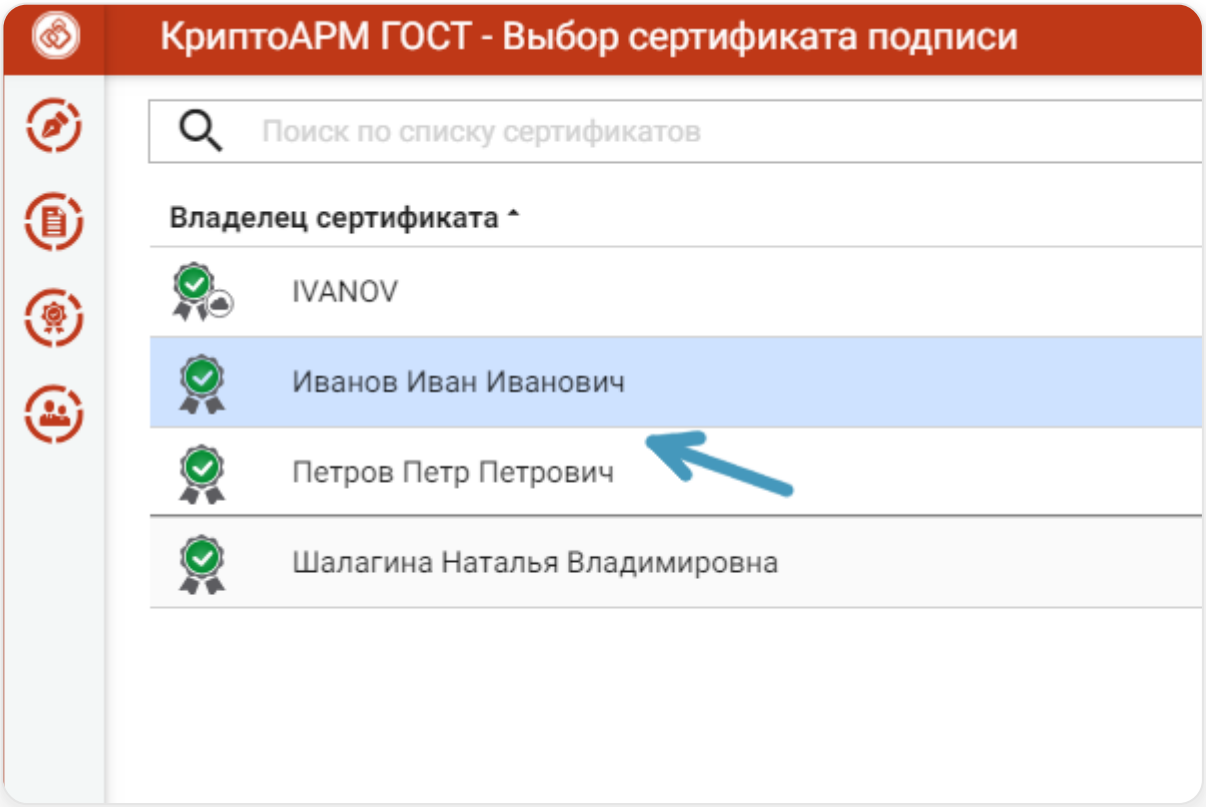
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.

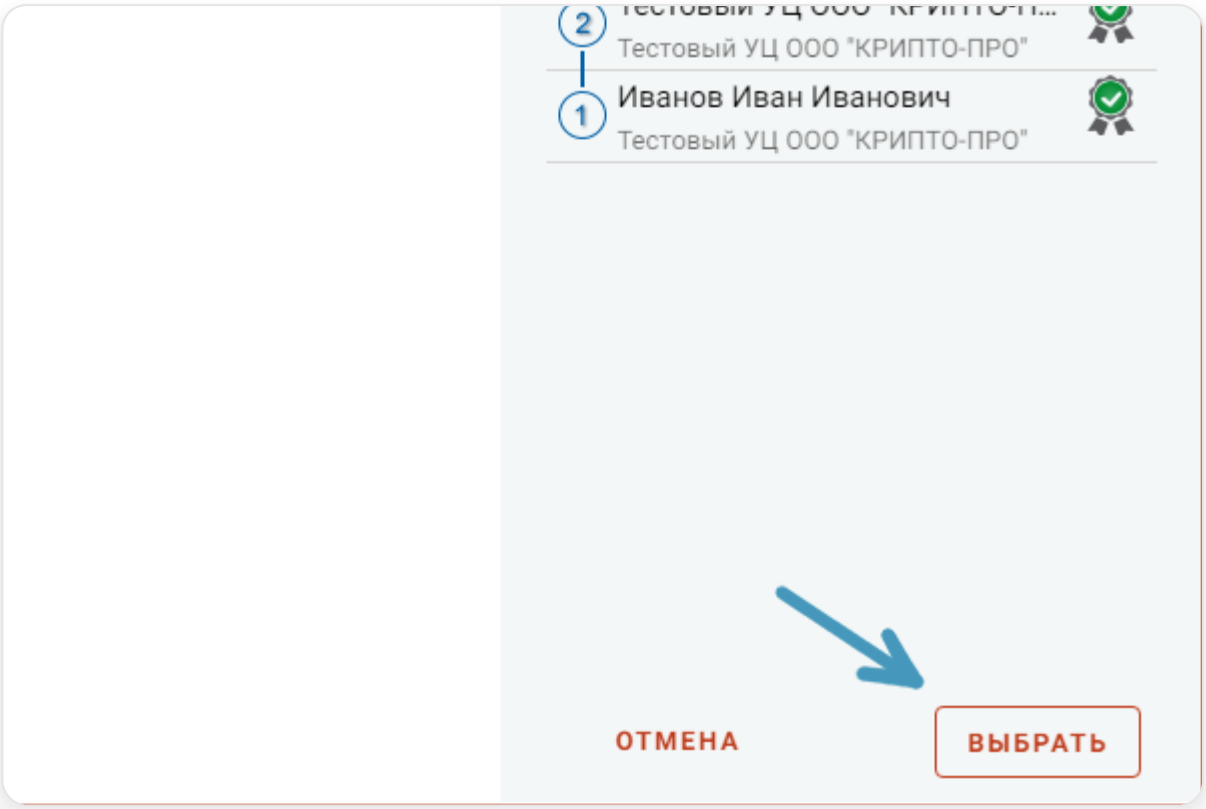


6. Выберите сертификат подписи. Если Вы не хотите использовать сертификат по умолчанию, нажмите кнопку **“Заменить”** в контекстном меню подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

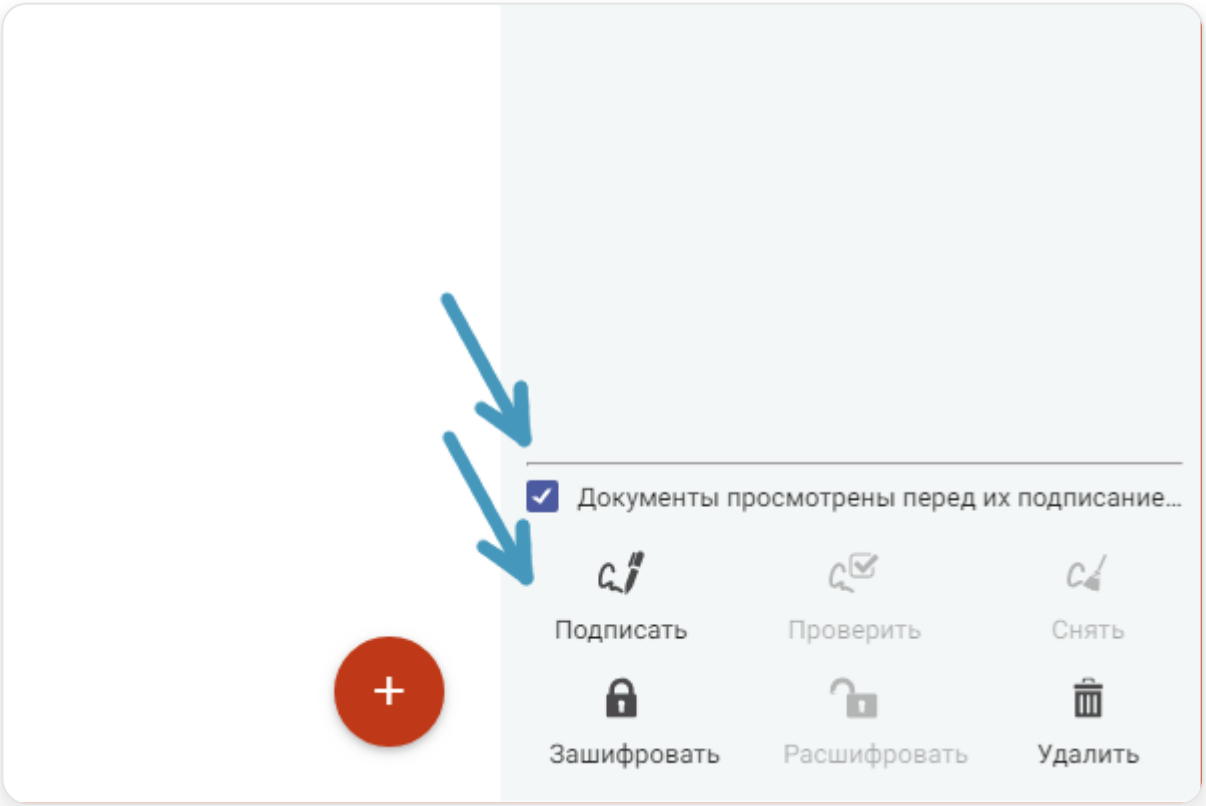


7. Выберите нужный сертификат и нажмите кнопку **“Выбрать”**.


КриптоАРМ ГОСТ - Выбор сертификата подписи
Поиск по списку сертификатов
Владелец сертификата
IVANOV
Иванов Иван Иванович
Петров Петр Петрович
Шалагина Наталья Владимировна

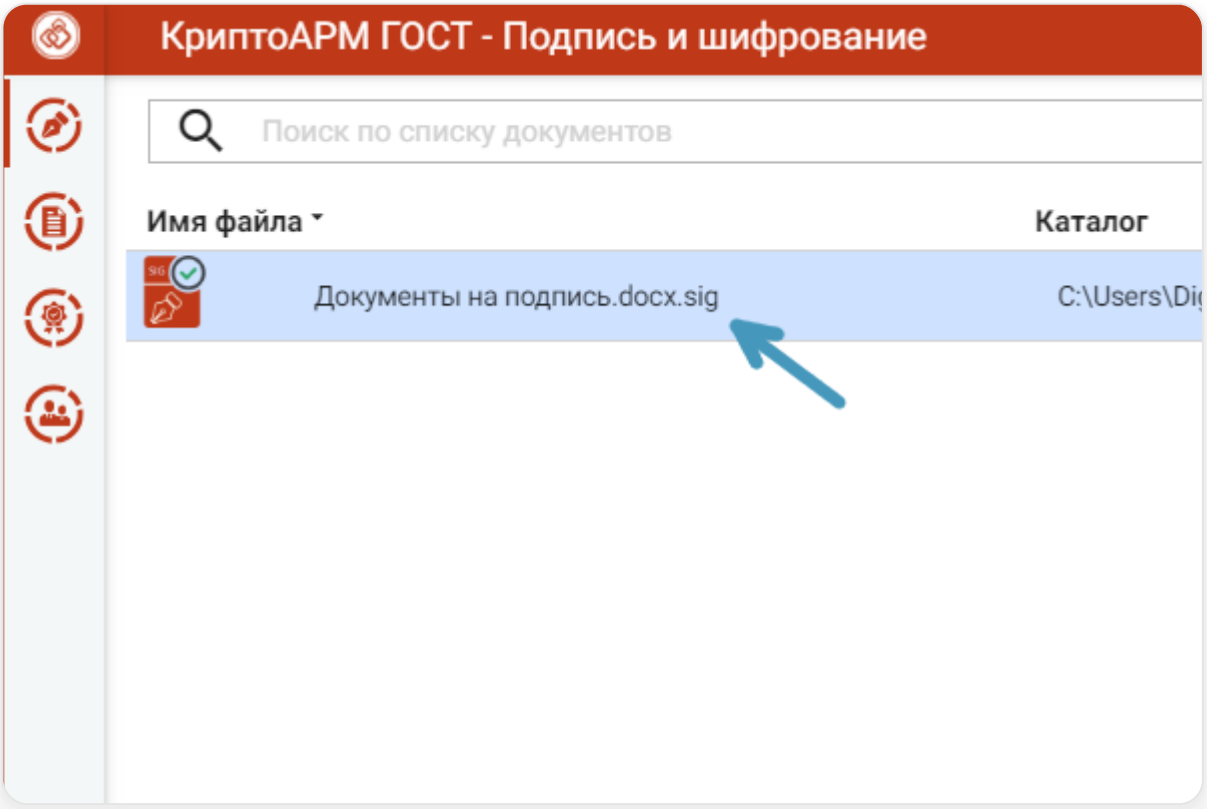

2
Тестовый УЦ ООО "КРИПТО-ПРО"
1
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
ОТМЕНА
ВЫБРАТЬ

8. Выберите флаг **“Документы просмотрены перед их подписанием”**.



9. Нажмите на кнопку **“Подписать”**.

10. Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.



Открыть статью на сайте

Как подписать межевой план электронной подписью и загрузить его на сайт Росреестра

Архив. КриптоАРМ ГОСТ.

Межевой план - это документ о земельном участке, который включает в себя информацию о постановке участка на учёт, о его размерах и границах, изменении его характеристик. Чтобы составить межевой план, нужно обратиться к кадастровому инженеру.

Подать межевой план для проверки в Росреестр можно двумя способами: в электронном виде и в печатном. С введением онлайн-системы Росреестра межевой план составляют и подают на учёт в электронном виде в XML-формате.

Электронная форма межевого плана, согласно Приложению N 1 к Приказу Минэкономразвития России от 08.12.2015 N 921, состоит из двух частей:

1. графической. В этой части отображаются сведения кадастрового плана соответствующей территории или выписки из ЕГРН о земельном участке. Указываются границы образуемого участка (участков) или границы части (частей) участка, либо уточняемые границы, а также проходы или проезды от участков общего пользования, включая установление сервитута;

2. текстовой. Эта часть содержит сведения о земельном участке (участках), которые необходимы для внесения в ЕГРН, в том числе пункты геодезических сетей или опорных межевых сетей, а также, в установленном случае, акт согласования местоположения границ.

Графическая часть, Акт согласования и бумажные документы оформляются в форме сканов бумажных документов в формате PDF. Скан документа должен быть представлен в масштабе 1:1 по сравнению с оригиналом. Качество должно позволять прочитать текст документа и его реквизиты. Для сканирования документов нужно использовать полноцветный режим с разрешением 300 dpi.

Если бумажный документ состоит из двух и более листов, электронный образ такого бумажного документа формируется в виде одного файла.

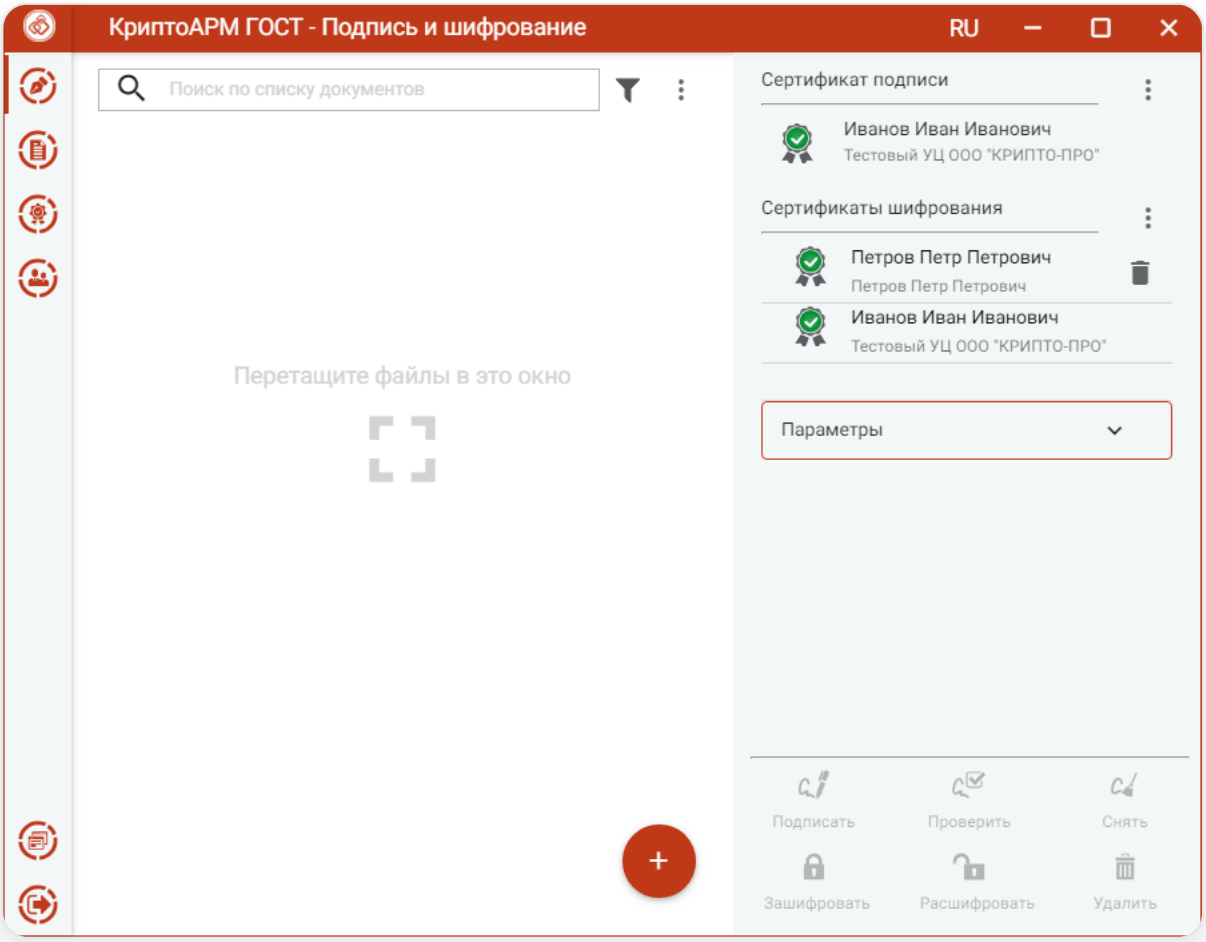
Для подачи межевого плана XML-документ должен быть подписан кадастровым инженером с использованием усиленной квалифицированной электронной подписи. **Федеральный закон N 218-ФЗ “О государственной регистрации недвижимости”, статья 22, пункт 12**: “Межевой план подготавливается в форме электронного документа и подписывается усиленной квалифицированной электронной подписью кадастрового инженера, подготовившего такой план. Межевой план, если это предусмотрено договором подряда, также подготавливается в форме документа на бумажном носителе, заверенного подписью и печатью подготовившего такой план кадастрового инженера, для передачи его заказчику по договору подряда.”

Получить такую электронную подпись можно в любом аккредитованном Удостоверяющем центре.

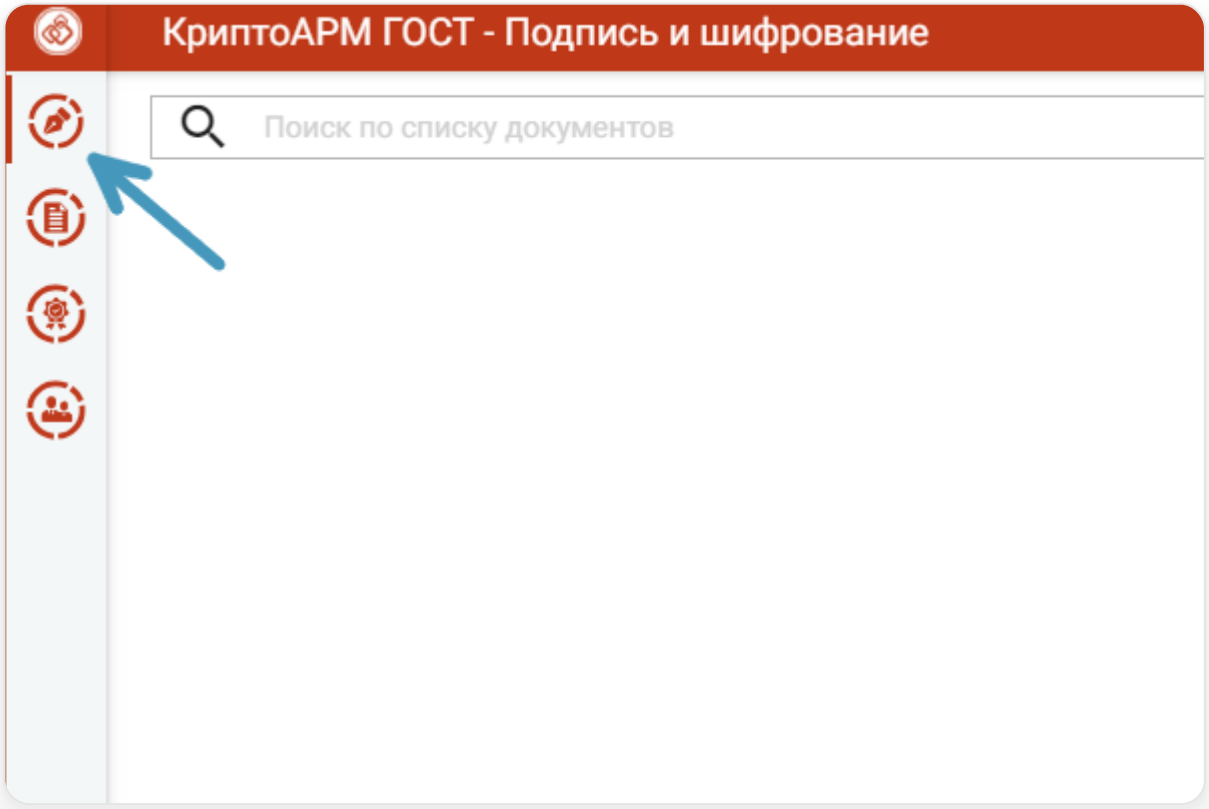
На рабочем месте для подписи межевого плана должны быть установлены программа подписи и шифрования КриптоАРМ ГОСТ и криптопровайдер КриптоПро CSP последней версии.

Как подписать межевой план ЭП в КриптоАРМ ГОСТ и загрузить на сайт Росреестра:

1. Откройте КриптоАРМ ГОСТ.



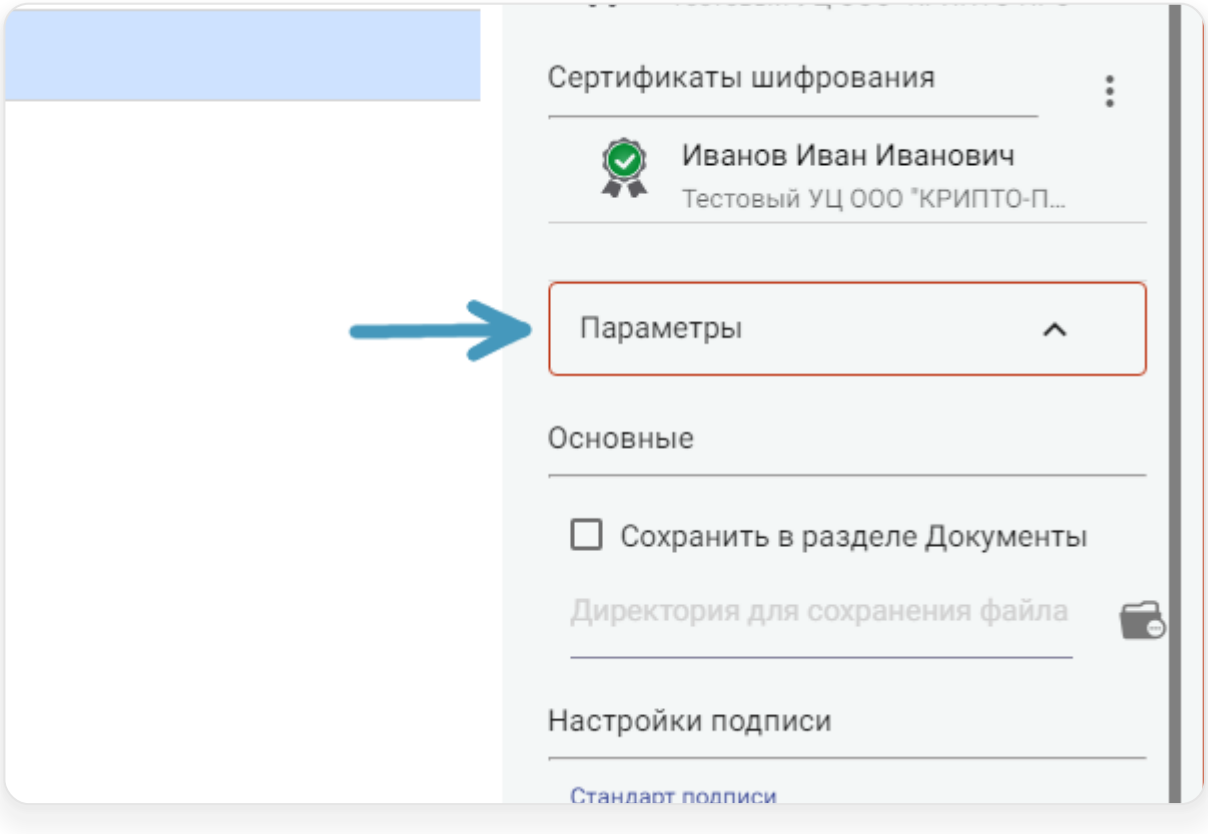
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



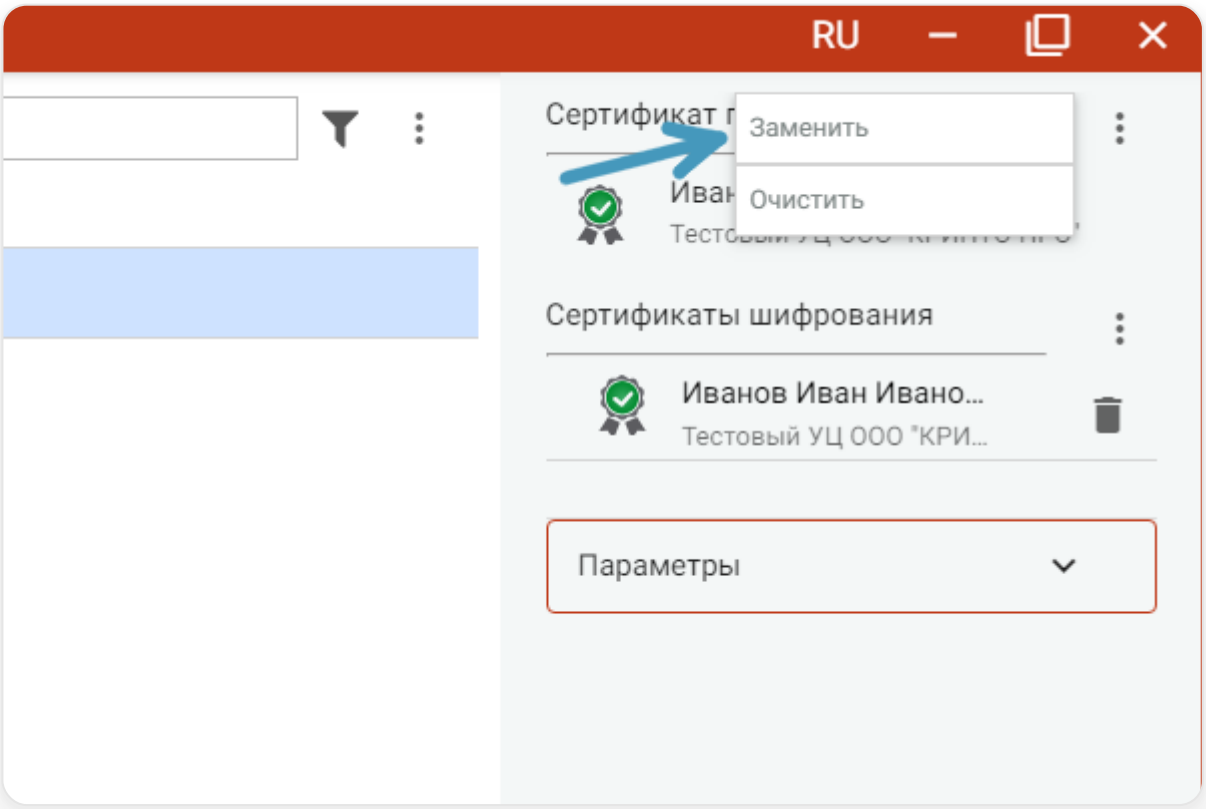
3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

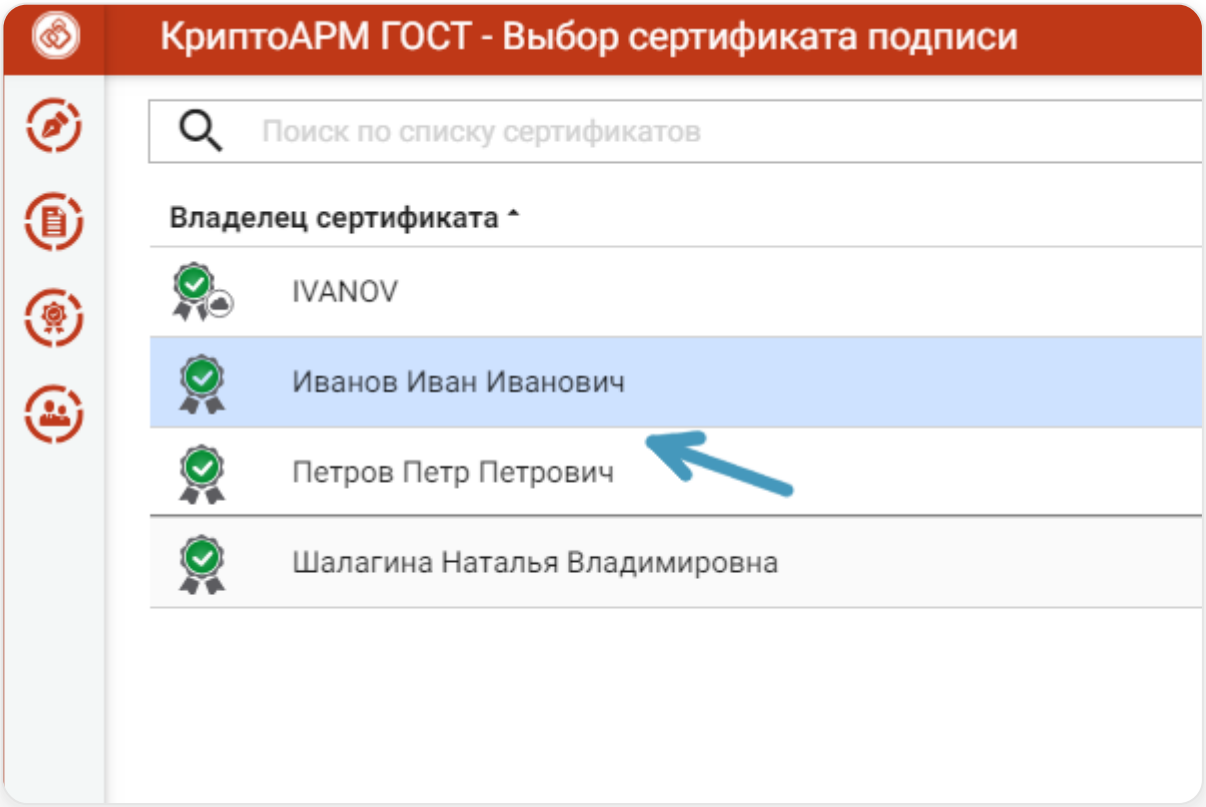
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.

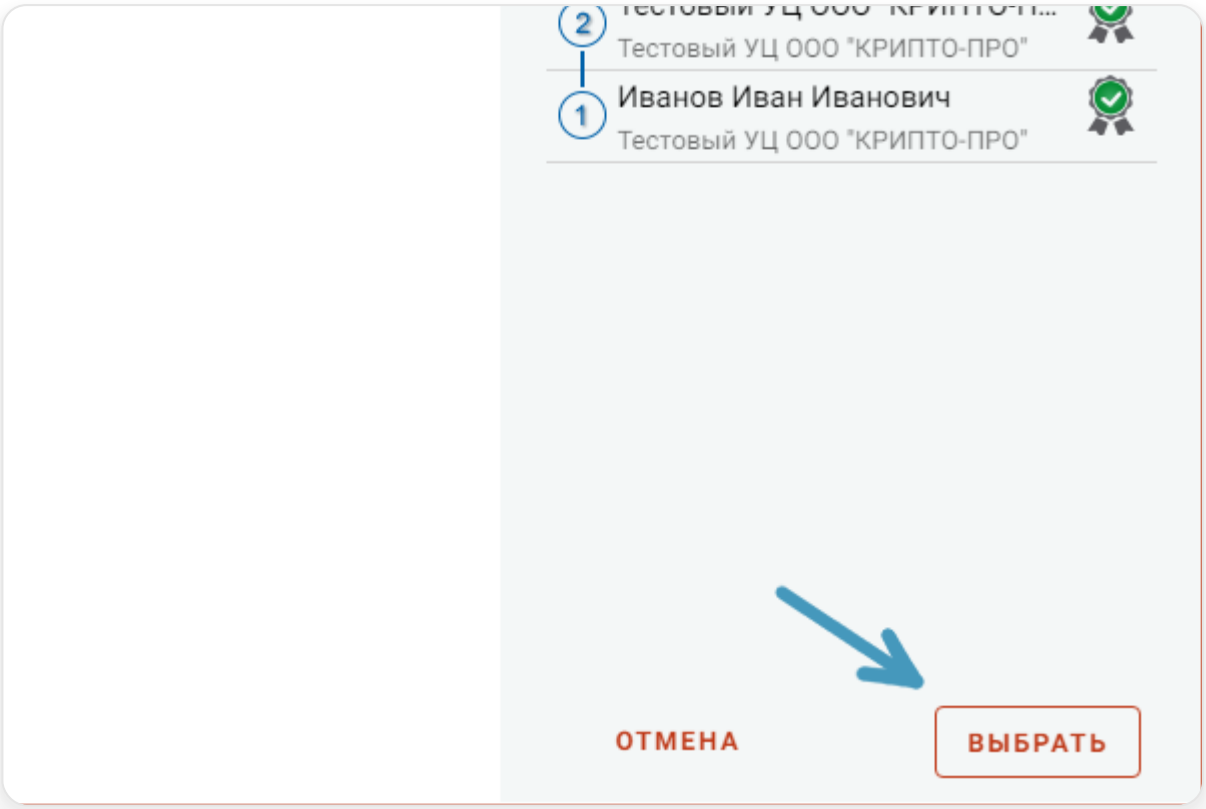


6. Выберите сертификат подписи. Если Вы не хотите использовать сертификат по умолчанию, нажмите кнопку **“Заменить”** в контекстном меню подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

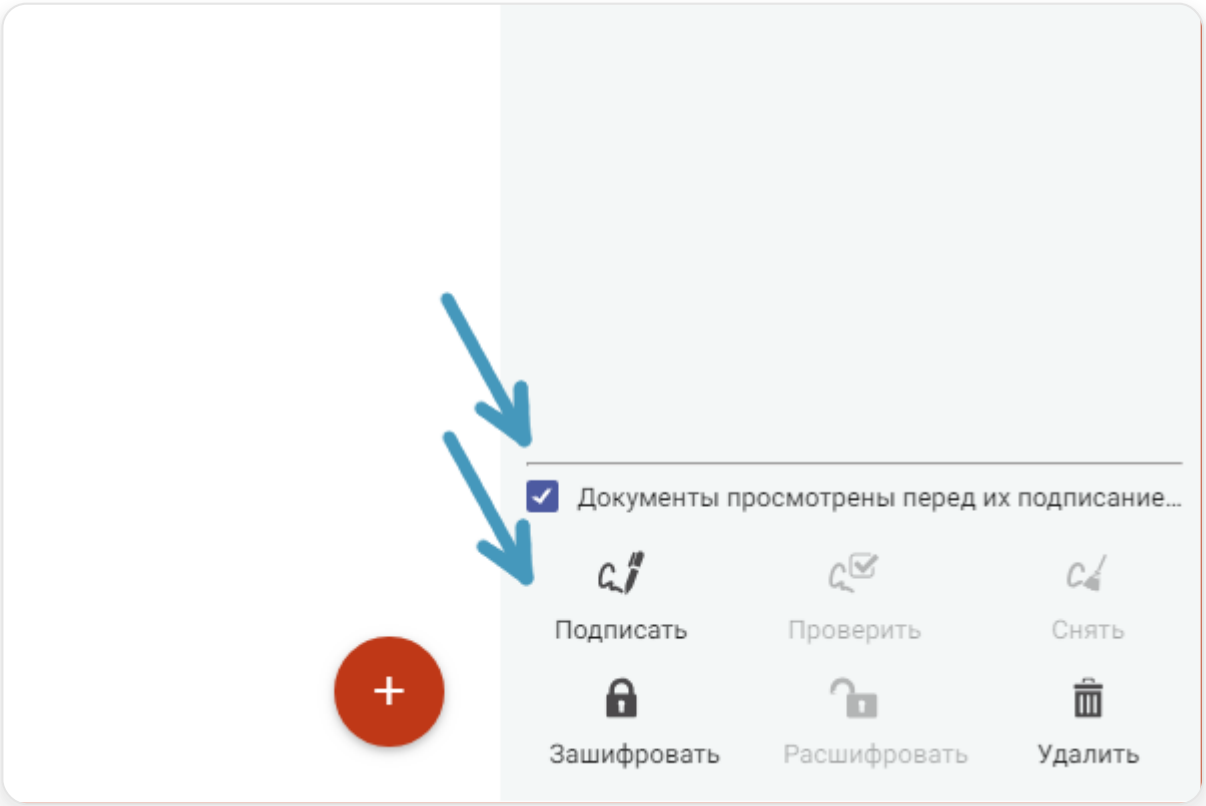


7. Выберите нужный сертификат и нажмите кнопку **“Выбрать”**.


КриптоАРМ ГОСТ - Выбор сертификата подписи
Поиск по списку сертификатов
Владелец сертификата
IVANOV
Иванов Иван Иванович
Петров Петр Петрович
Шалагина Наталья Владимировна

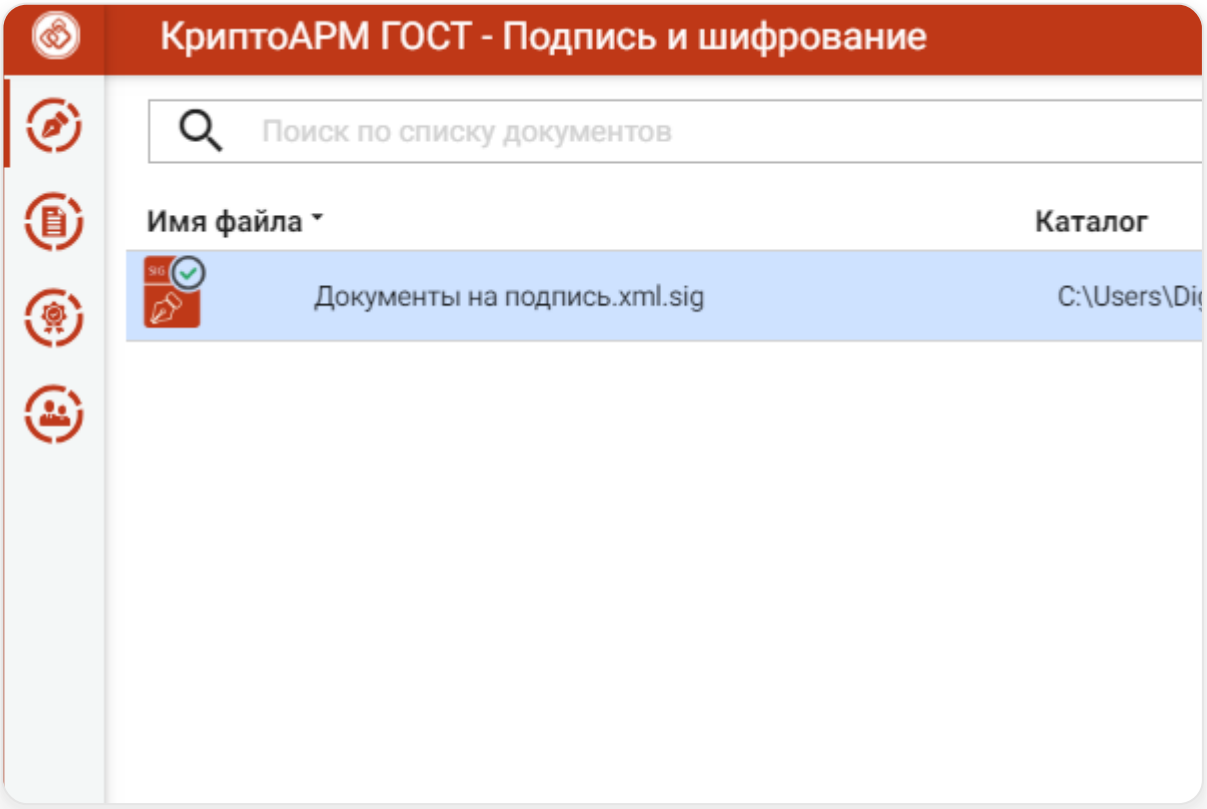

2
Тестовый УЦ ООО "КРИПТО-ПРО"
1
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
ОТМЕНА
ВЫБРАТЬ

8. Выберите флаг **“Документы просмотрены перед их подписанием”**.



9. Нажмите на кнопку **“Подписать”**.

10. Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.



11. Зайдите на **сайт Росреестра**.
12. Войдите в личный кабинет с помощью электронной подписи.
13. В меню сайта найдите вкладку **“Мои задачи”**. Если она недоступна, необходимо пополнить баланс в Личном кабинете: 500 рублей за 20 услуг Росреестра, 1250 рублей за 50 услуг и 2500 рублей за 100 услуг.
14. Чтобы загрузить на проверку межевой план, нажмите кнопку **“Добавить документ”**.
15. В открывшемся окне нажмите на ссылку **“Загрузить .xml или .zip файл”**.
16. Выберите нужный файл и нажмите кнопку **“Открыть”**.
17. Далее нажмите кнопку **“Начать проверку”**. Запустится автоматизированная проверка загруженного документа. Система проверит оформление межевого плана и действительность электронной подписи.

Открыть статью на сайте

Как нотариально заверить документы в КриптоАРМ ГОСТ

Архив. КриптоАРМ ГОСТ.

С 2014 года нотариусы могут заверять электронные версии документов с помощью электронной подписи (ЭП), которая является цифровым аналогом обычной подписи и аналогом печати. С помощью ЭП можно заверять оригиналы документов и подтверждать подлинность электронных копий.

Чтобы подписанные электронные документы были приняты во всех госорганах, электронная подпись нотариуса должна быть усиленной и квалифицированной. Такую ЭП можно получить в аккредитованном Удостоверяющем центре. Электронный нотариальный документ должен быть представлен в виде XML-файла и соответствовать стандартам Федеральной нотариальной палаты, www.notariat.ru.

Электронный образ документа на бумажном носителе формируется в виде одного файла изображения в формате PDF. Сканирование нотариально оформленного документа должно производиться с разрешением 200 dpi (точек на дюйм) в оттенках серого, глубина цвета 8 бит на пиксель.

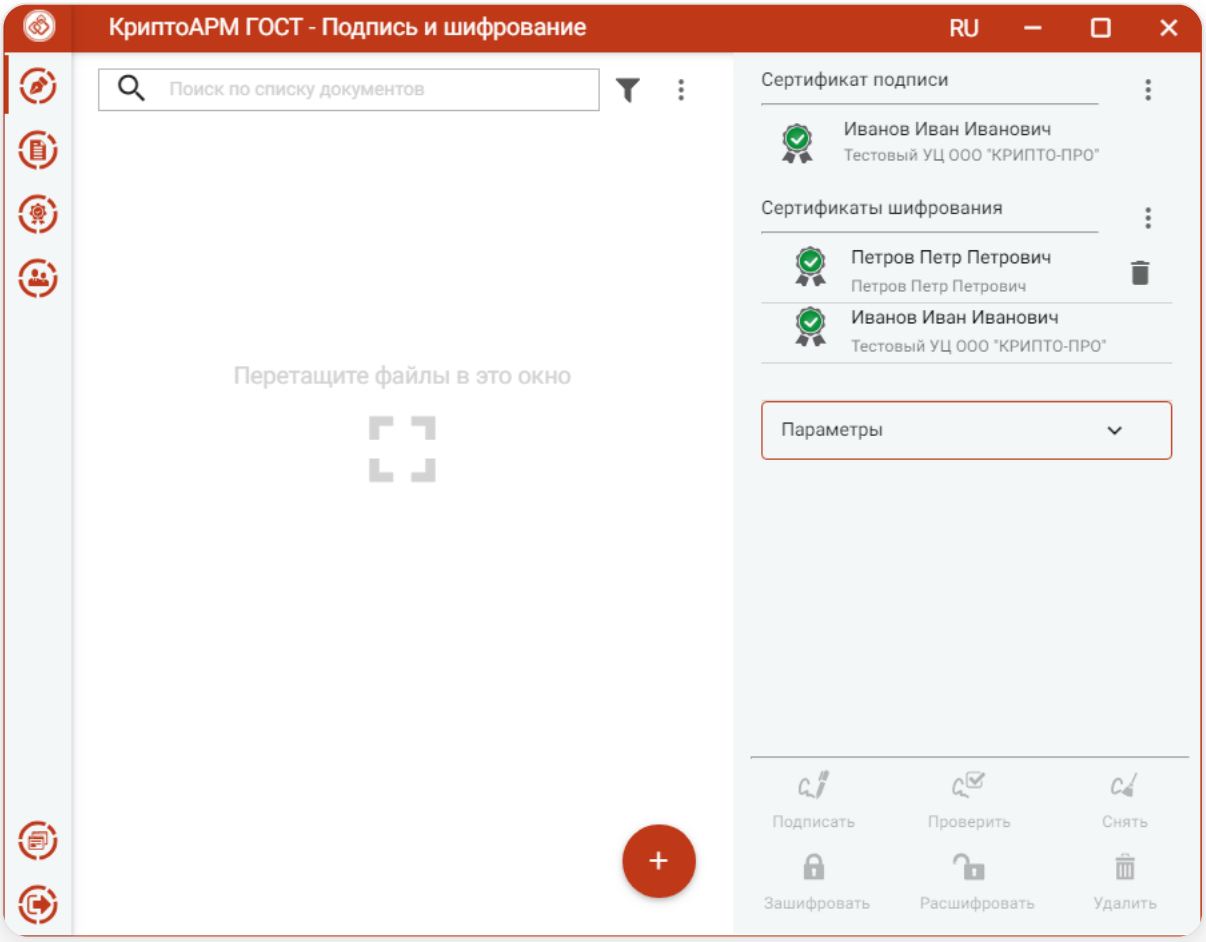
Электронной подписью можно заверить все документы и операции, предусмотренные **ст. 35 “Основ законодательства Российской Федерации о нотариате”**, о чём свидетельствует **ст. 44.2 - “Совершение нотариальный действий в электронной форме”**.

Требования к электронной подписи для нотариусов:

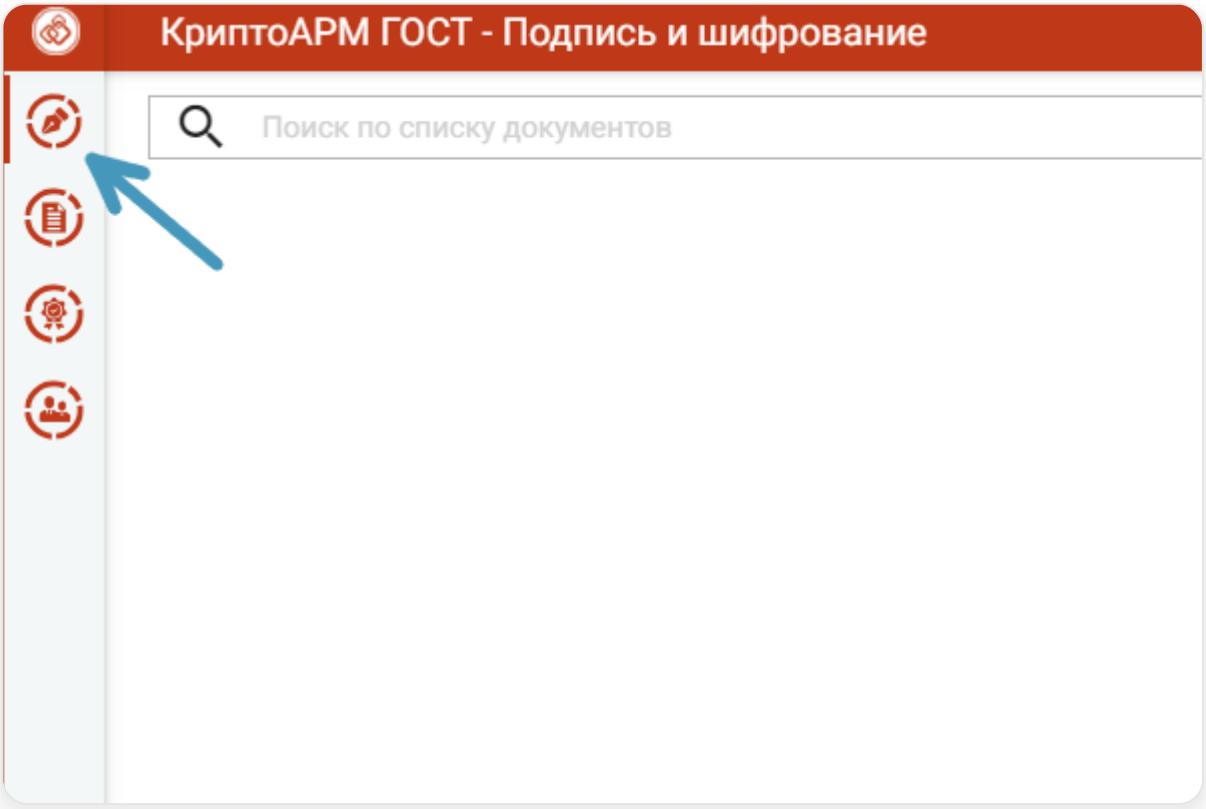
1. ЭП нотариуса должна быть действительна на момент подписи;
2. ЭП должна быть усиленной и квалифицированной;
3. При подписи нужно использовать формат PKCS#7 - кодировку DER;
4. Подпись должна быть отсоединённой.

Чтобы подписать XML-документ в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.


КриптоАРМ ГОСТ - Подпись и шифрование
RU
Поиск по списку документов
Перетащите файлы в это окно
Сертификат подписи
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
Сертификаты шифрования
Петров Петр Петрович
Петров Петр Петрович
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
Параметры
Подписать
Проверить
Снять
Зашифровать
Расшифровать
Удалить

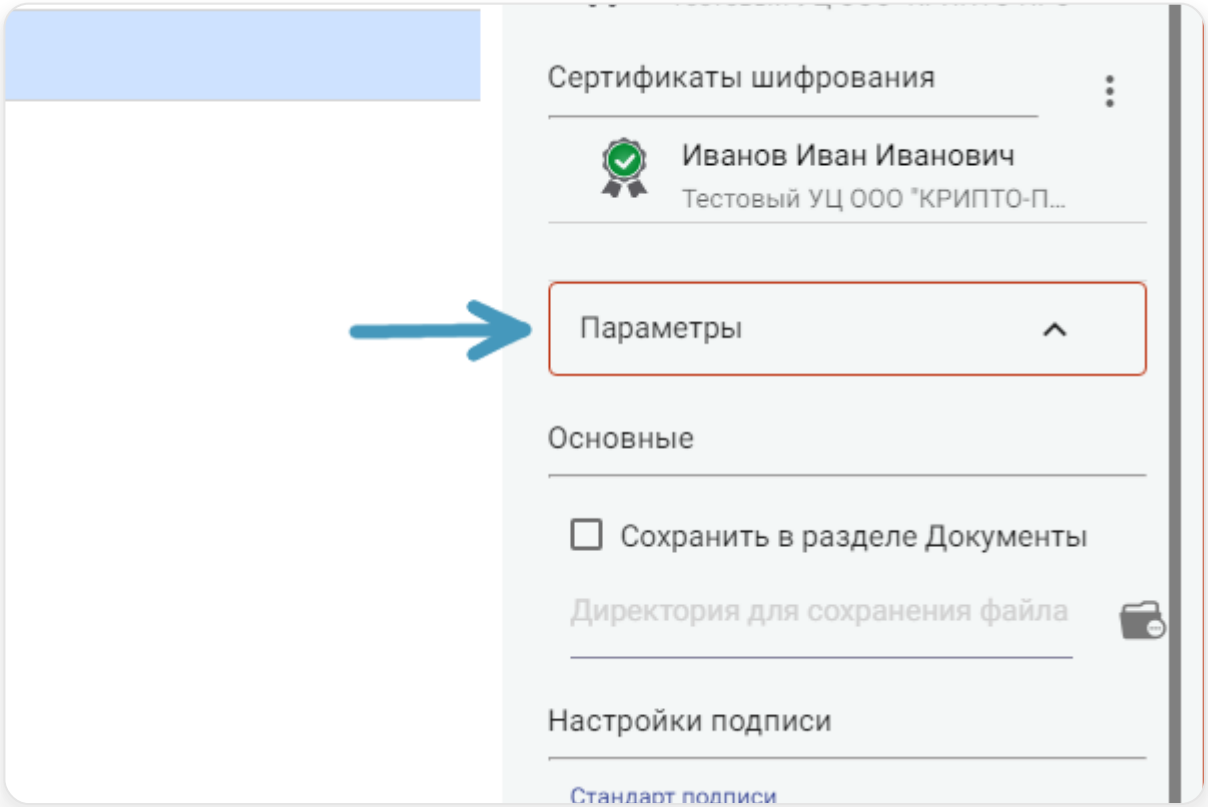
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



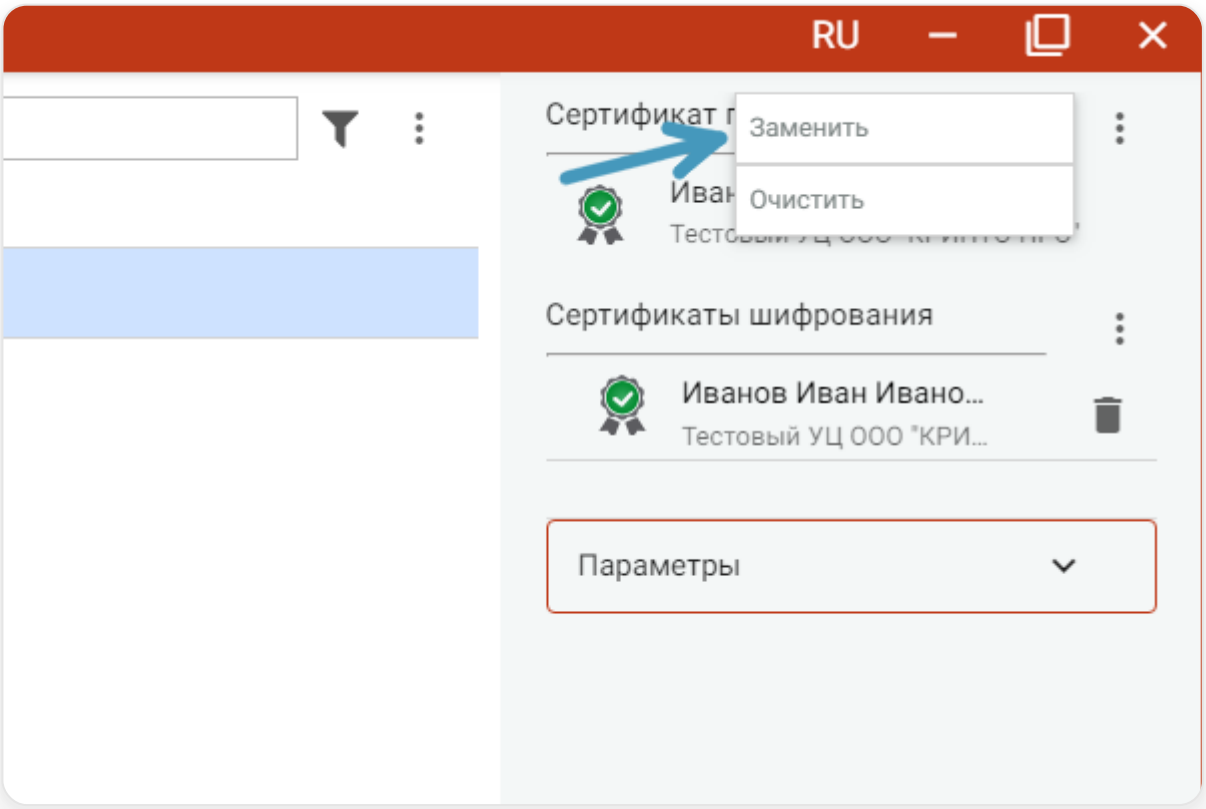
3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

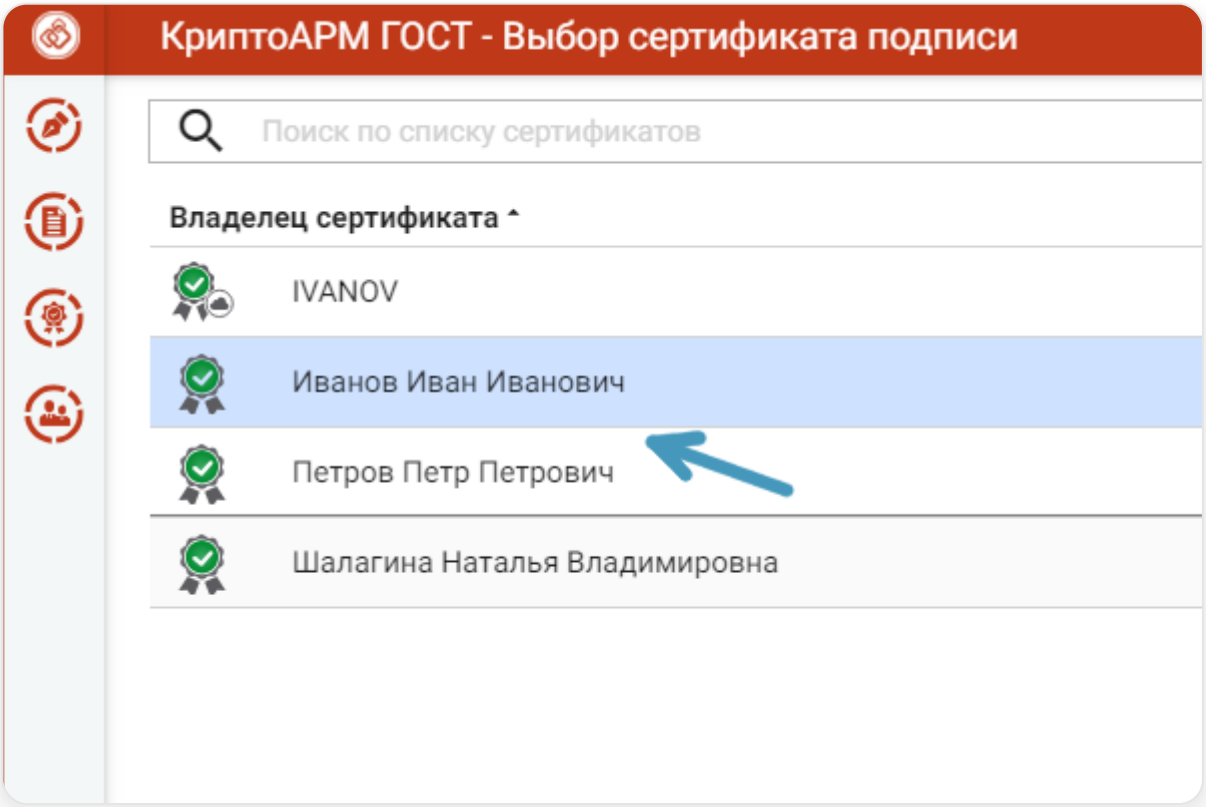
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.

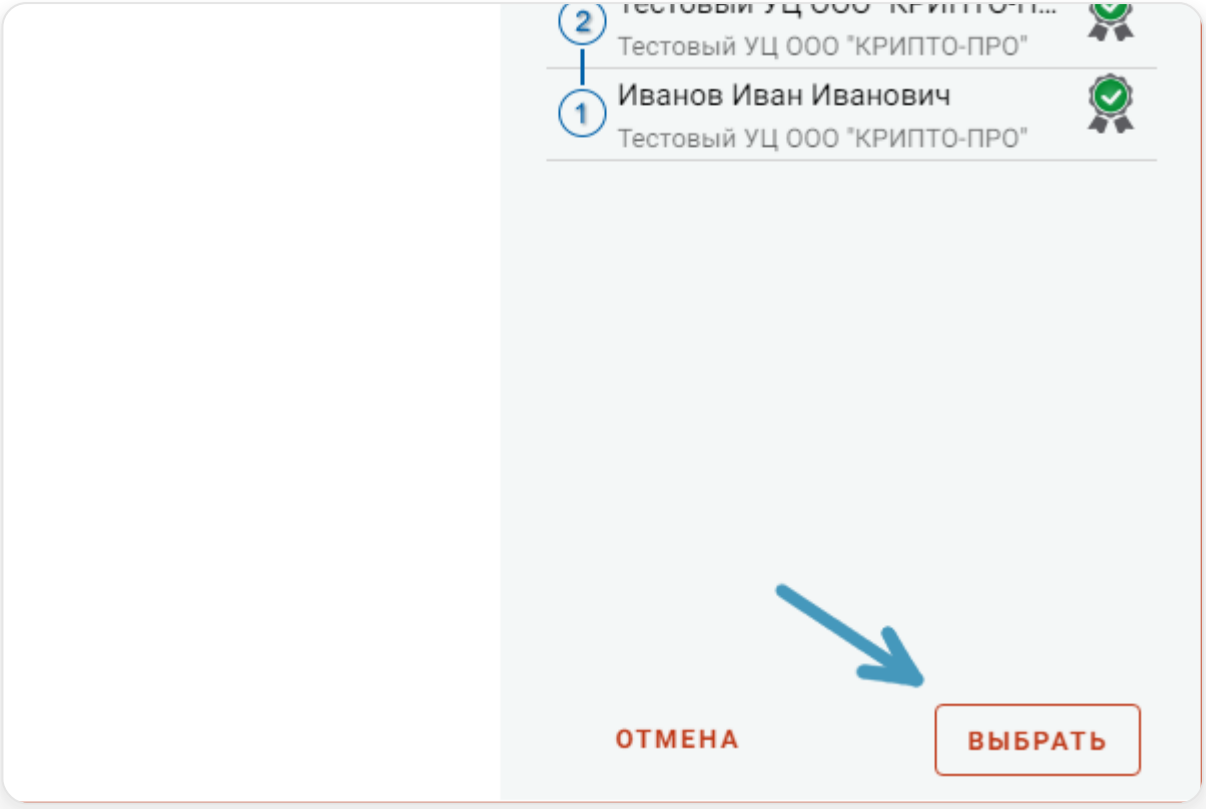


6. Выберите сертификат подписи. Если Вы не хотите использовать сертификат по умолчанию, нажмите кнопку **“Заменить”** в контекстном меню подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

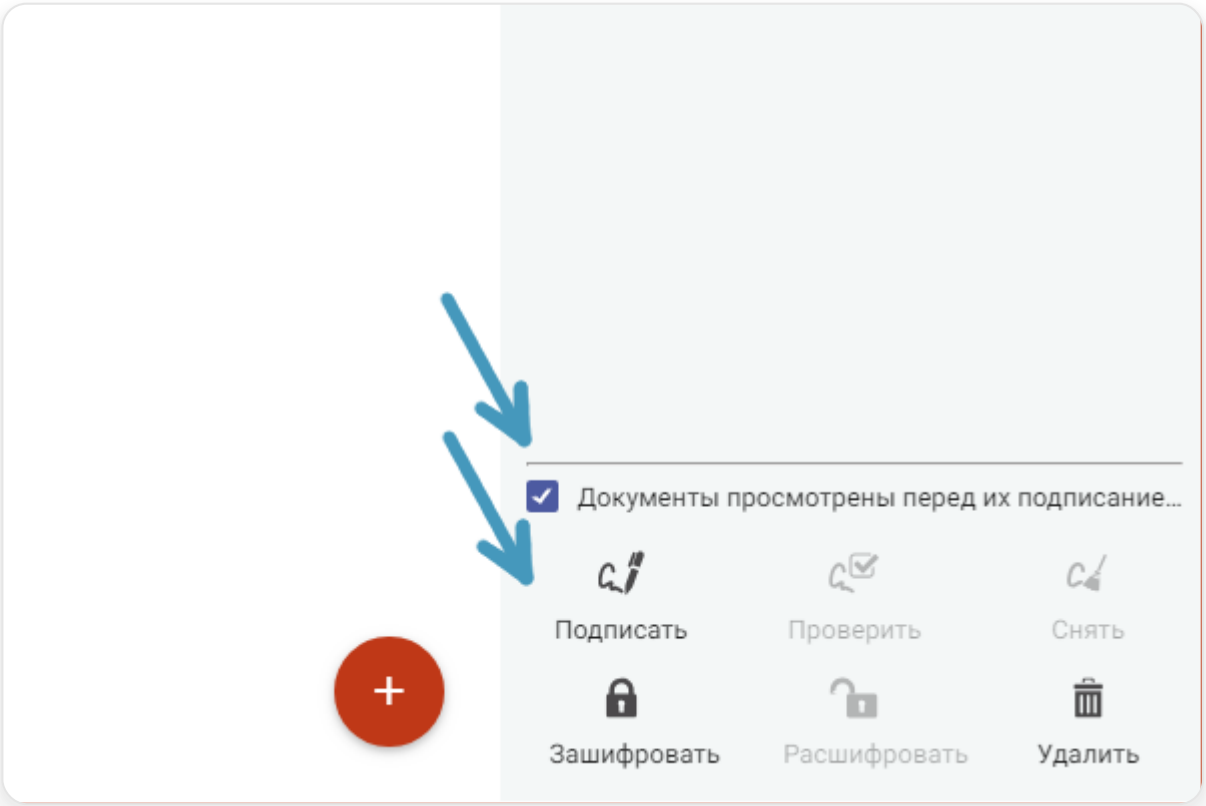


7. Выберите нужный сертификат и нажмите кнопку **“Выбрать”**.


КриптоАРМ ГОСТ - Выбор сертификата подписи
Поиск по списку сертификатов
Владелец сертификата
IVANOV
Иванов Иван Иванович
Петров Петр Петрович
Шалагина Наталья Владимировна

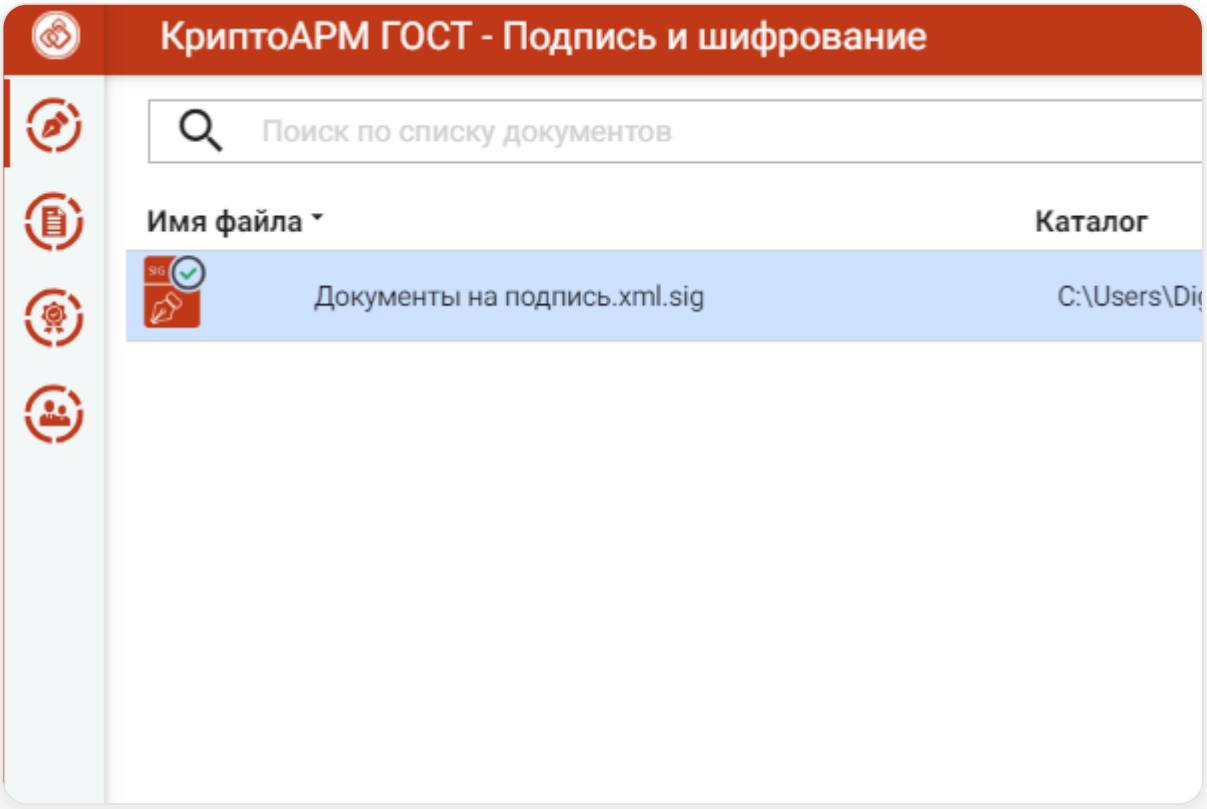

2
Тестовый УЦ ООО "КРИПТО-ПРО"
1
Иванов Иван Иванович
Тестовый УЦ ООО "КРИПТО-ПРО"
ОТМЕНА
ВЫБРАТЬ

8. Выберите флаг **“Документы просмотрены перед их подписанием”**.



9. Нажмите на кнопку **“Подписать”**.

10. Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.



Открыть статью на сайте

Как подписать госконтракт электронной подписью

Архив. КриптоАРМ ГОСТ.

Согласно ФЗ-44, государственный контракт – это договор предоставления товаров и услуг, заказчиком которых выступают являться муниципальный или государственный орган. Исполнитель госконтракта выбирается на конкурсной основе.

Государственный заказчик размещает на сайте конкурсную документацию, в которой указываются сроки исполнения договора, максимальные цены, определение качества товаров и прочие условия выполнения контракта.

После этого участники конкурса направляют заказчику свои заявки, которые должны пройти регистрацию. После заседания конкурсной комиссии участникам приходит рассылка уведомлений об участии в торгах, после чего окончательное заседание конкурсной комиссии по рассмотрению заявок и цен. На сайте оформляется договор, и победитель получает свой экземпляр протокола и проекта госзаказа.

Требования к участникам конкурса по ст. 31 ФЗ-44:

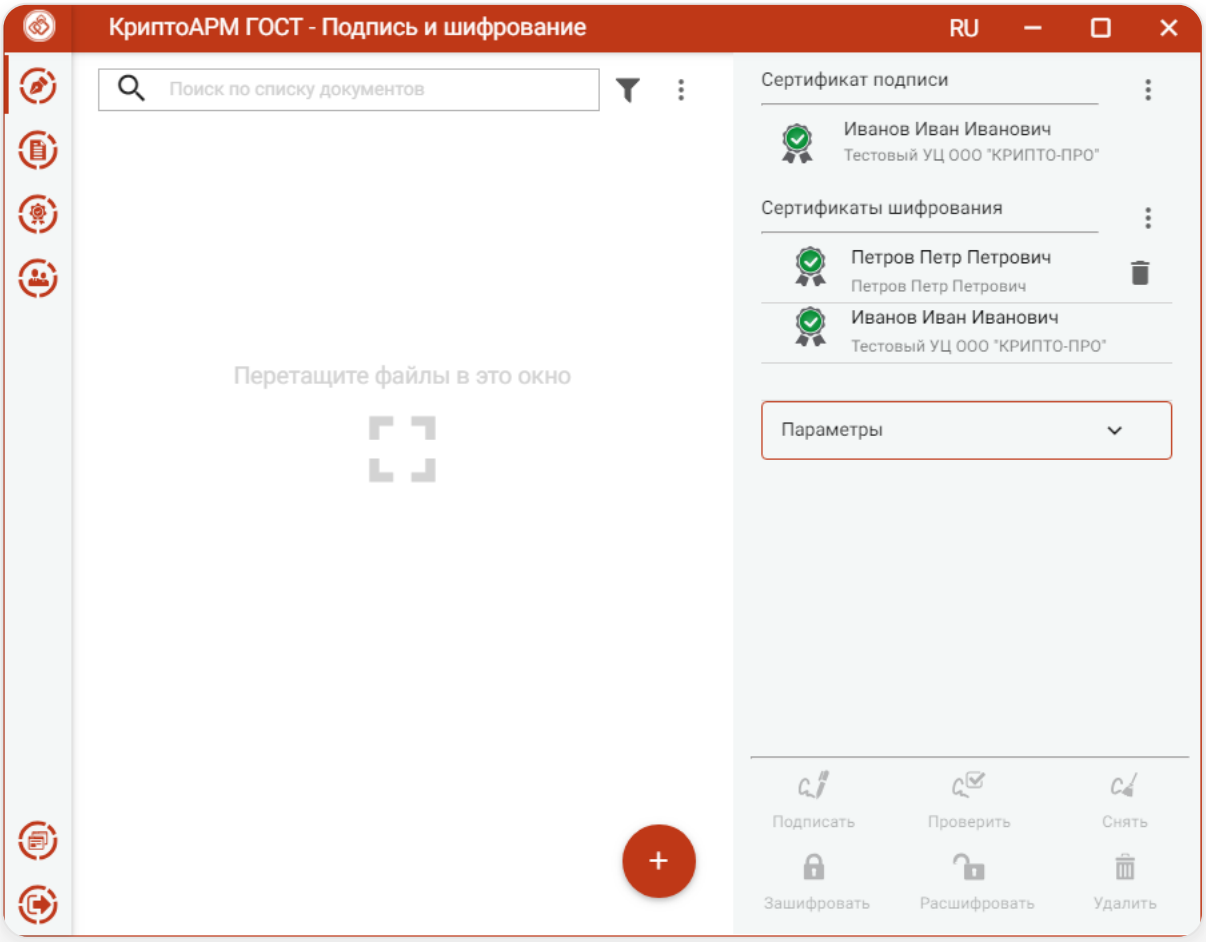
1. Разрешение на выполнение определенных услуг юридическим лицом;
2. Организация не должна быть признана банкротом;
3. Деятельность организации не должна быть приостановлена на дату подачи заявки;
4. Отсутствие задолженности перед бюджетной системой РФ;
5. Отсутствие у участника закупки или главного бухгалтера юр. лица судимости по статьям 289, 290, 291, 291.1 УК РФ;
6. Отсутствие у участника закупки или главного бухгалтера запрета на исполнение определенных видов деятельности;
7. Непривлечение юр. лица к административной ответственности по статье 19.28 КоАП РФ;
8. Отсутствие конфликта интересов;
9. Организация не являются офшорной компанией;
10. Отсутствие запрета на участие в закупках;
11. Обладание исключительными правами на результаты интеллектуальной деятельности, если они используются при исполнении контракта.

Что нужно для подписи:

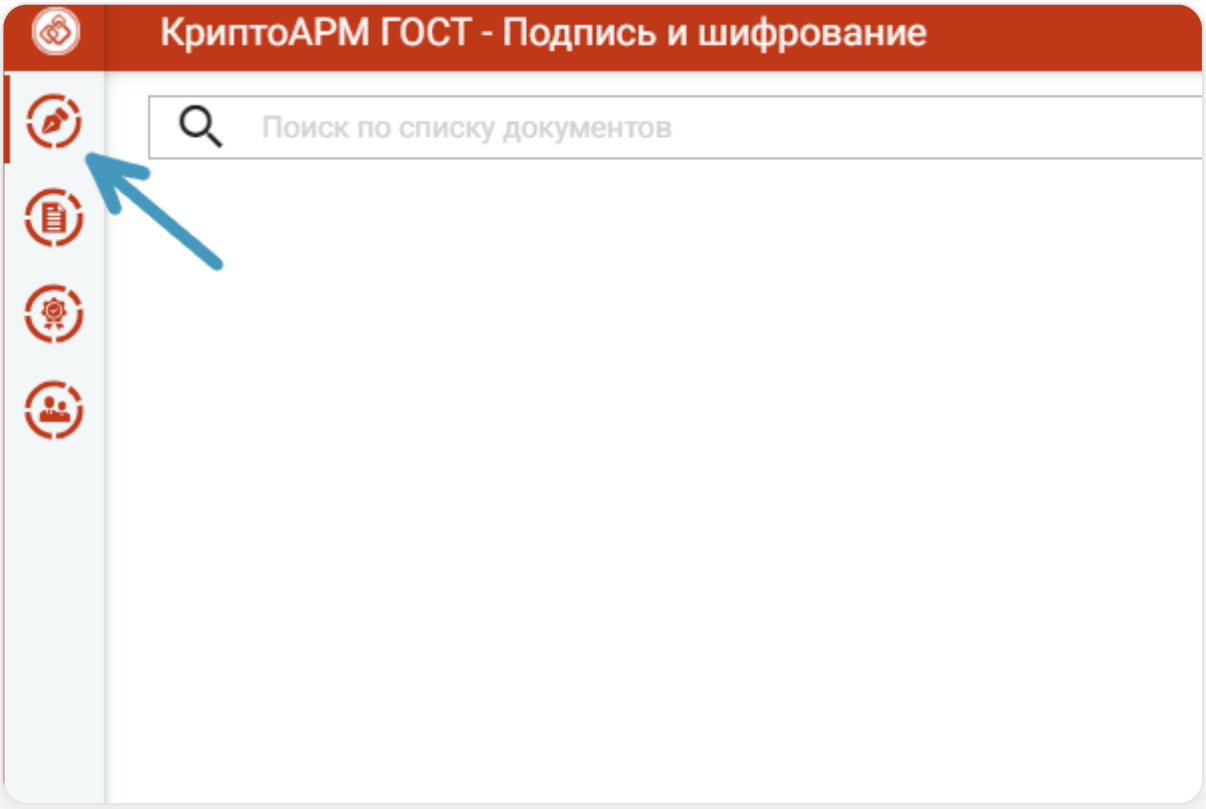
1. Установленная программа КриптоАРМ ГОСТ.
2. Установленный криптопровайдер КриптоПро CSP.
3. Усиленная квалифицированная электронная подпись.

Чтобы подписать госконтракт в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.



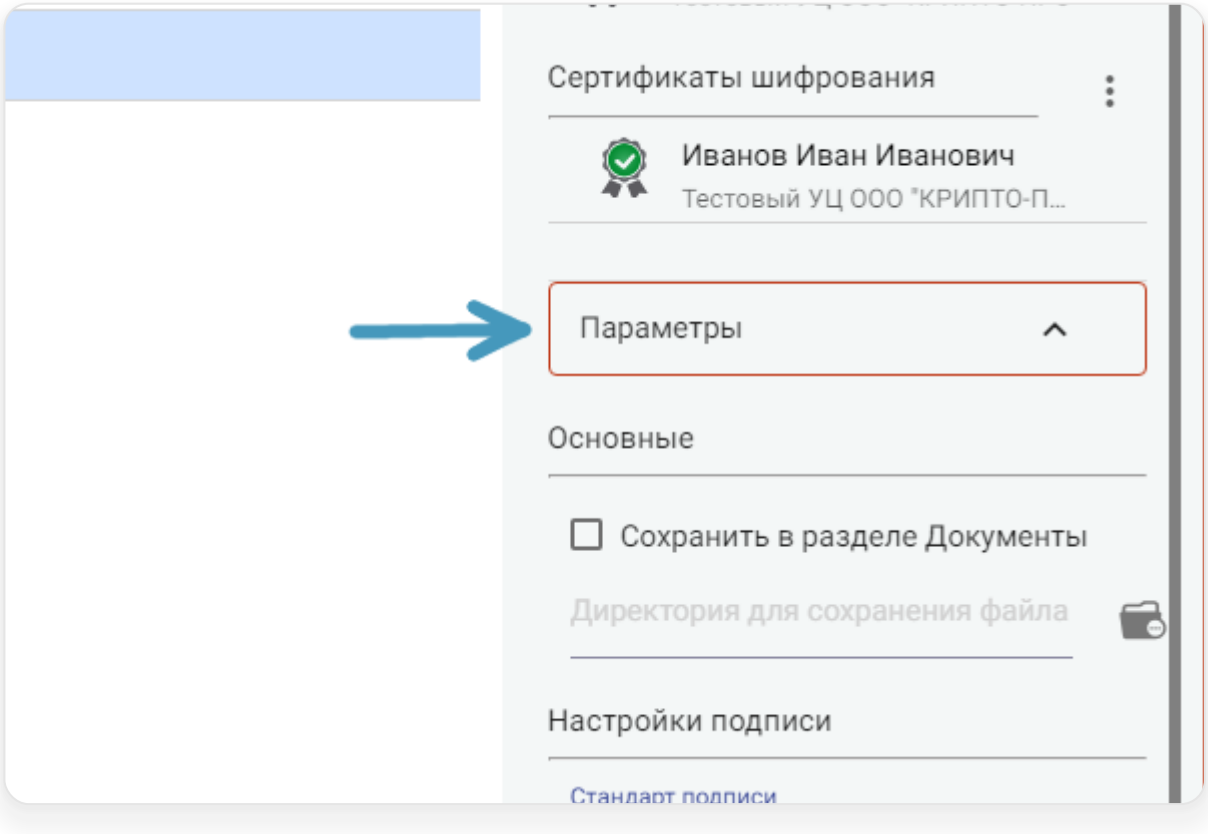
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



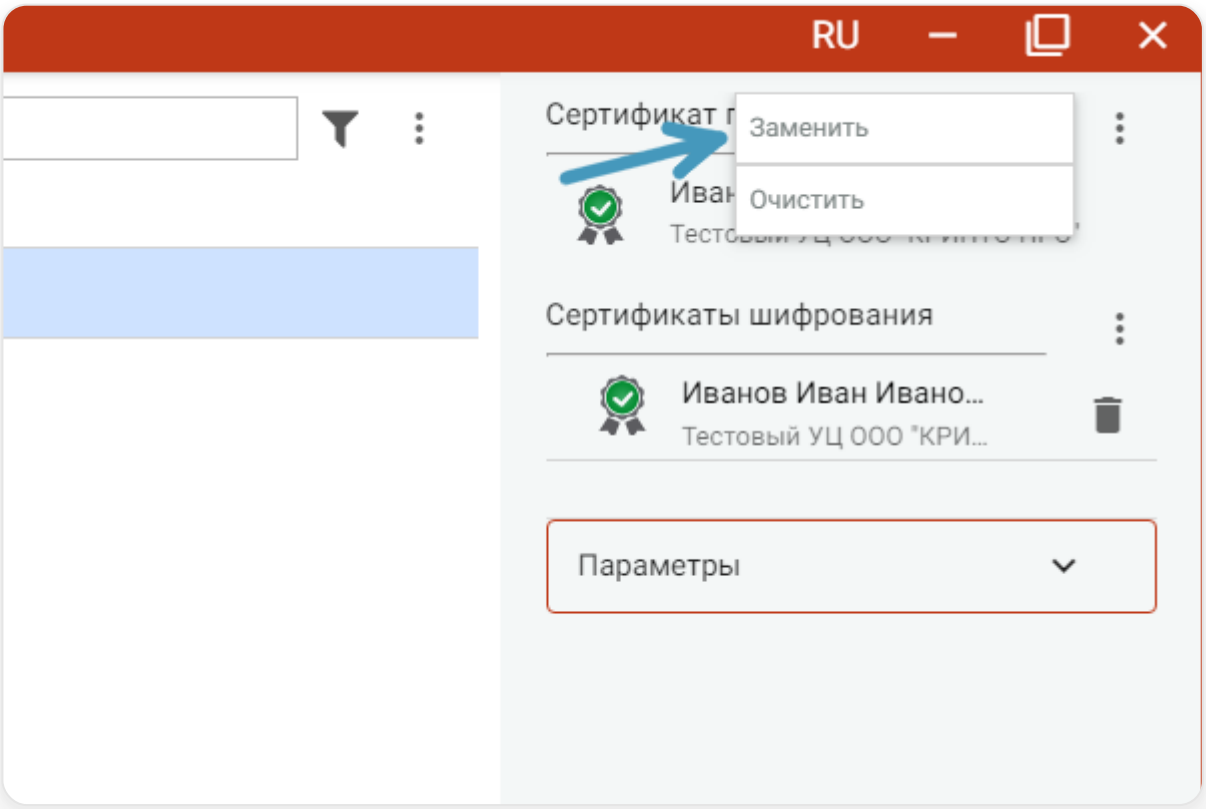
3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

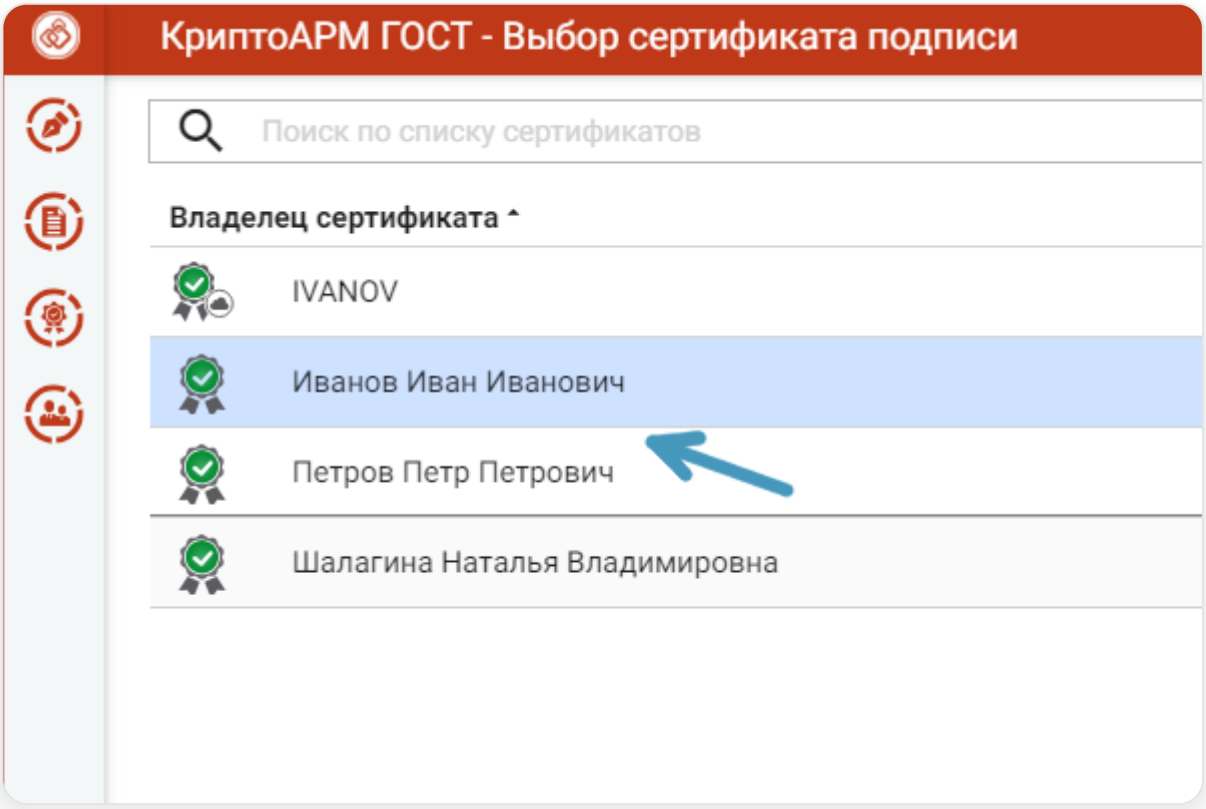
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.

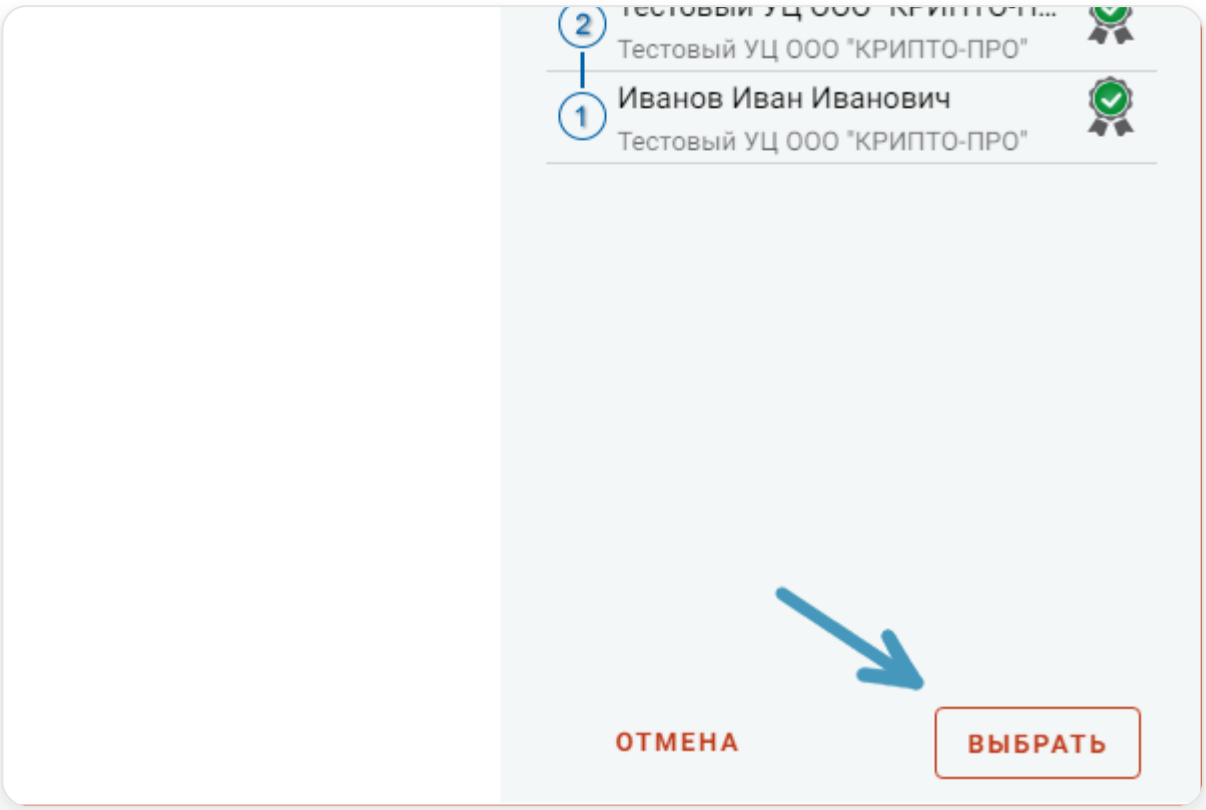


6. Выберите сертификат подписи. Если Вы не хотите использовать сертификат по умолчанию, нажмите кнопку **“Заменить”** в контекстном меню подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

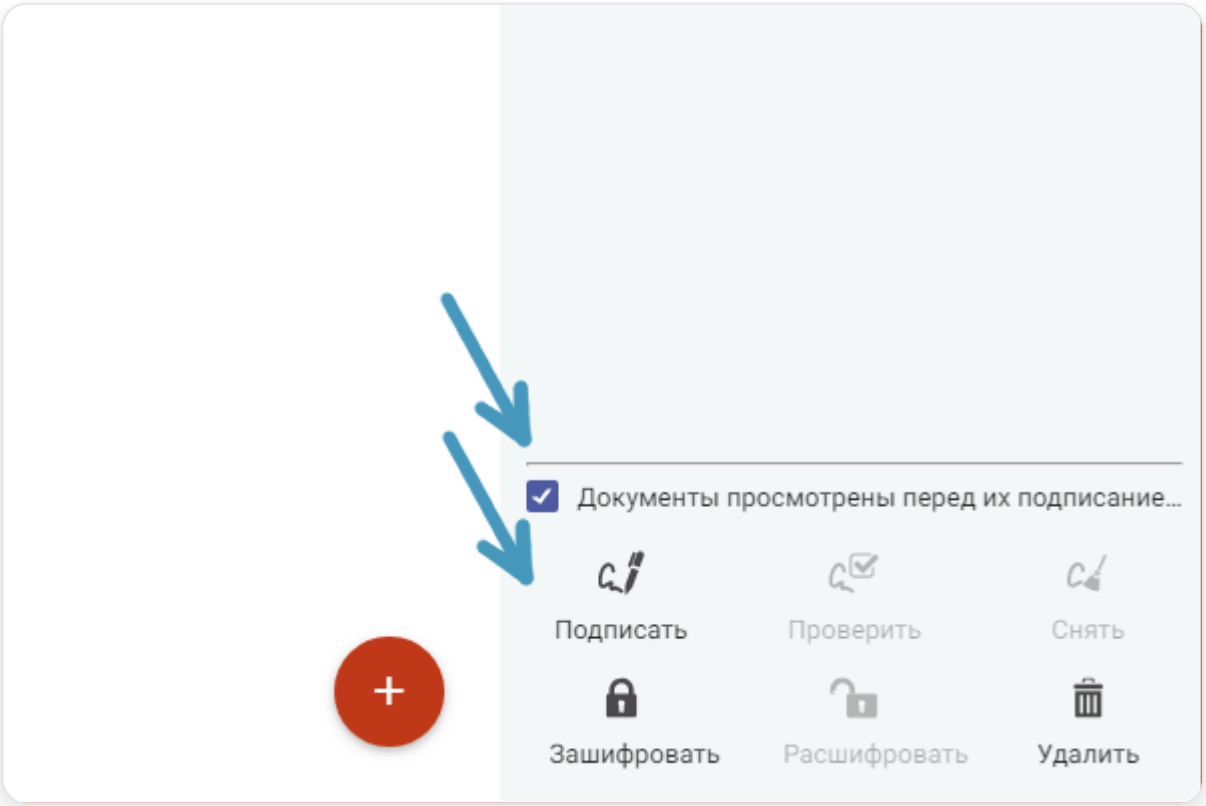

RU
Заменить
Очистить
Сертификаты шифрования
Иванов Иван Ивано...
Тестовый УЦ ООО "КРИ...
Параметры

7. Выберите нужный сертификат и нажмите кнопку **“Выбрать”**.



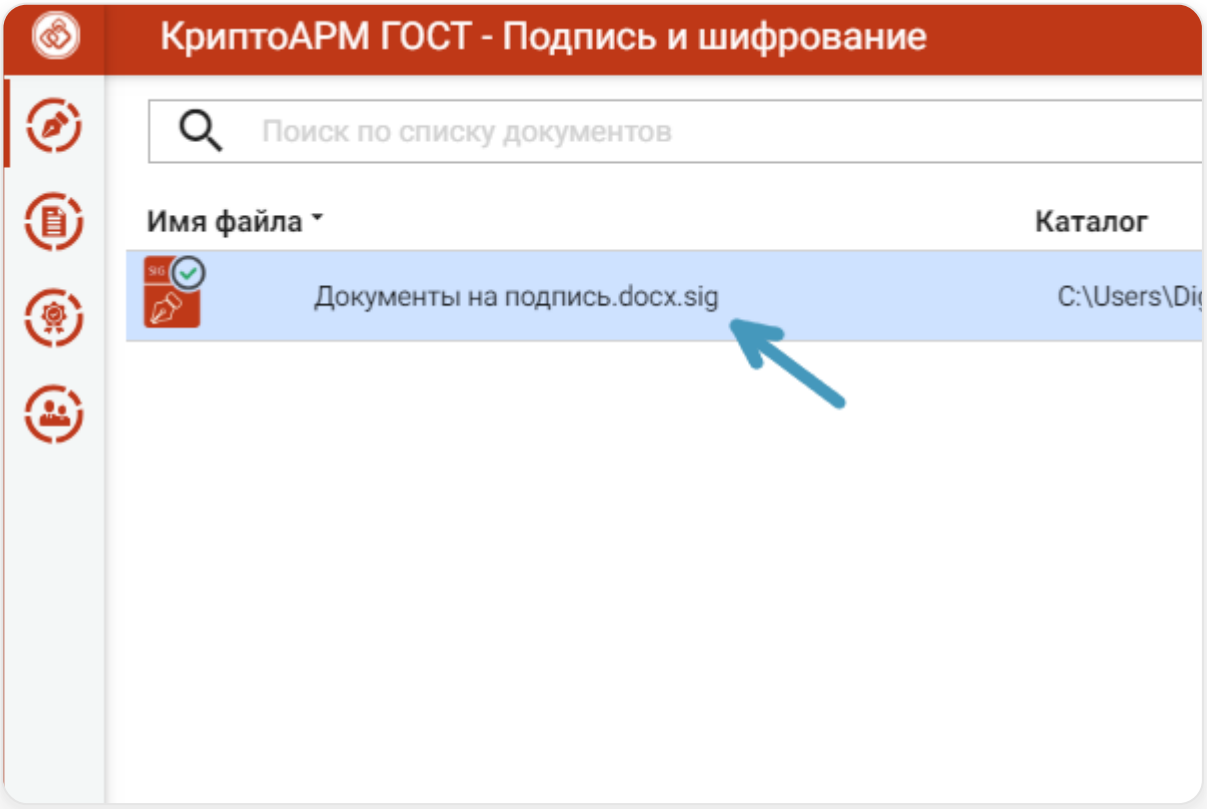


8. Выберите флаг **“Документы просмотрены перед их подписанием”**.



9. Нажмите на кнопку **“Подписать”**.

10. Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.



Открыть статью на сайте

Как подписать запрос предложения электронной подписью

Архив. КриптоАРМ ГОСТ.

Запрос предложений - это способ выбора исполнителя госзаказа, при котором участник конкурса в открытом виде размещает информацию о закупках. Проведение запросов в электронной форме регулирует **44-ФЗ "О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд", статья 83.1**.

Запрос предложений в электронной форме проводится в случаях:

1. Закупки спортинвентаря и оборудования, которые необходимы для подготовки спортивных команд РФ;
2. Расторжения контракта с предыдущим исполнителем;
3. Закупки лекарств по решению врачебной комиссии;
4. Закупок в иностранные и международные суды, арбитражи исков к РФ для защиты интересов РФ;
5. Признания недействительным открытого конкурса или аукциона;
6. Закупки изделий народных художественных промыслов, когда их ценность подтверждена комиссией при Правительстве РФ;
7. Закупок жилья для детей-сирот у физических лиц.

Заявка на участие в запросе предложений в электронной форме в электронной форме должна включать в себя:

1. Наименование организации и место нахождения - для юридического лица;
2. ФИО, паспортные данные, место жительства - для физического лица;
3. Почтовый адрес, адрес электронной почты, номер контактного телефона, ИНН или аналог ИНН для иностранного лица;
4. ИНН учредителей и членов исполнительного органа юр. лица;
5. Документы, подтверждающие соответствие товара, работы или услуги требованиям законодательства, если эти документы не передаются вместе с товаром;
6. Документы, подтверждающие соответствие участника запроса требованиям, установленным ст.31 44-ФЗ, или копии таких документов;

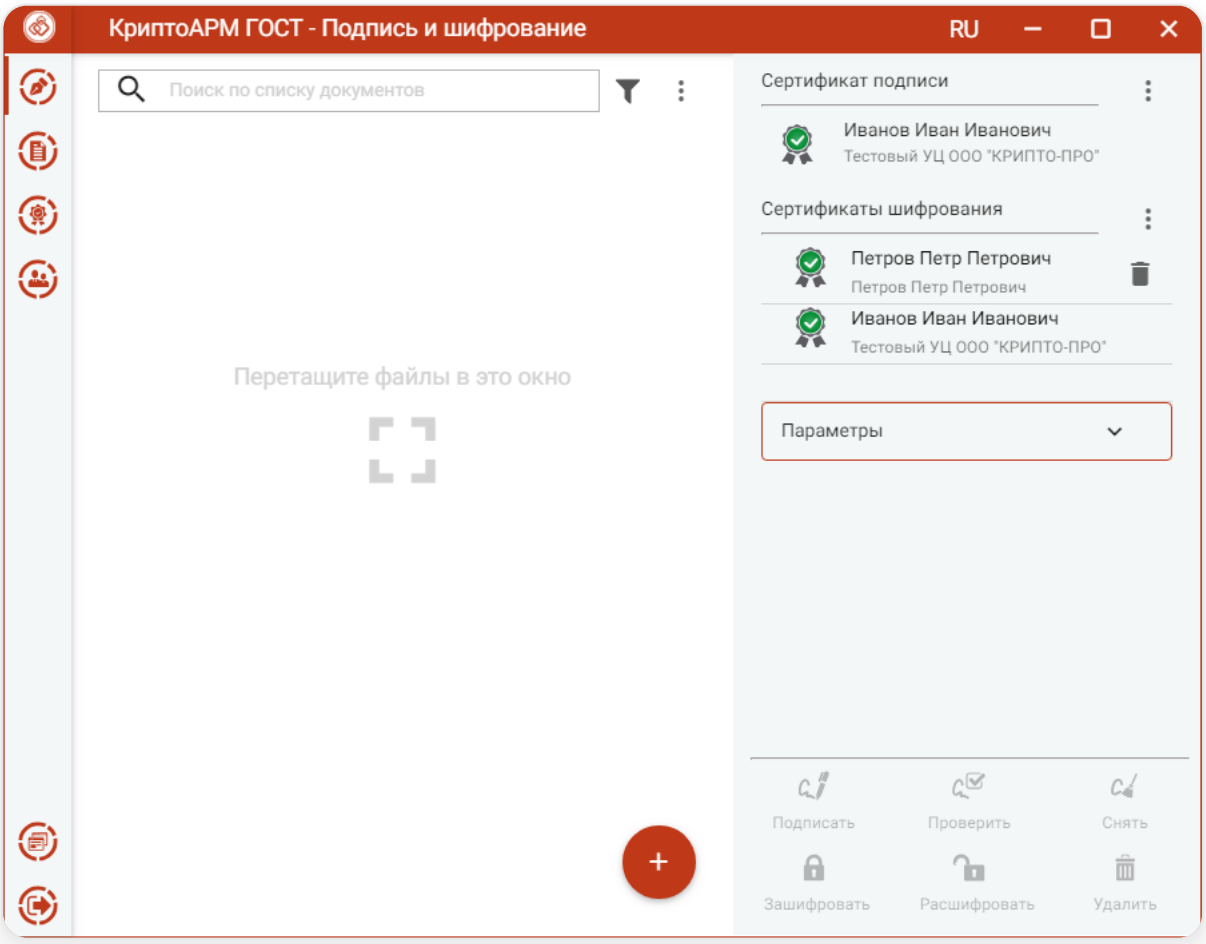
7. Документы, подтверждающие право участника на получение преимуществ в соответствии со ст. 28 и 29 44-ФЗ;
8. Документы о предоставлении товаров и услуг иностранного государства или иностранными лицами;
9. Документы, подтверждающие квалификацию участника или копии таких документов;
10. Предложение участника об условиях исполнения контракта;
11. Декларацию о принадлежности участника к субъектам малого предпринимательства или социально ориентированным НКО в соответствии с ч.3 ст.30 44-ФЗ.

Для электронной подписи Вам понадобится:

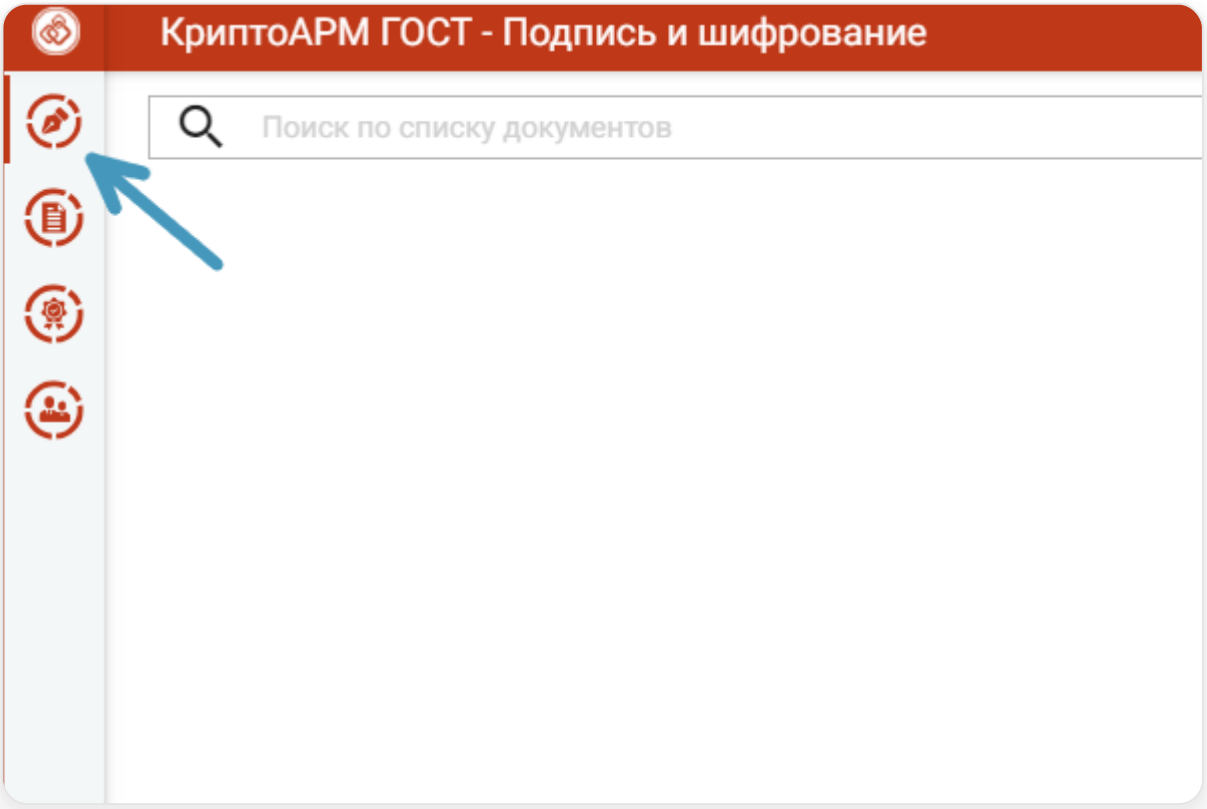
1. Сертификат квалифицированной подписи, который можно получить в аккредитованном Удостоверяющем центре.
2. Программа для подписи и шифрования документов КриптоАРМ ГОСТ.
3. Средство криптографической защиты информации КриптоПро CSP, установленное на рабочем месте.

Чтобы подписать запрос предложений в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.



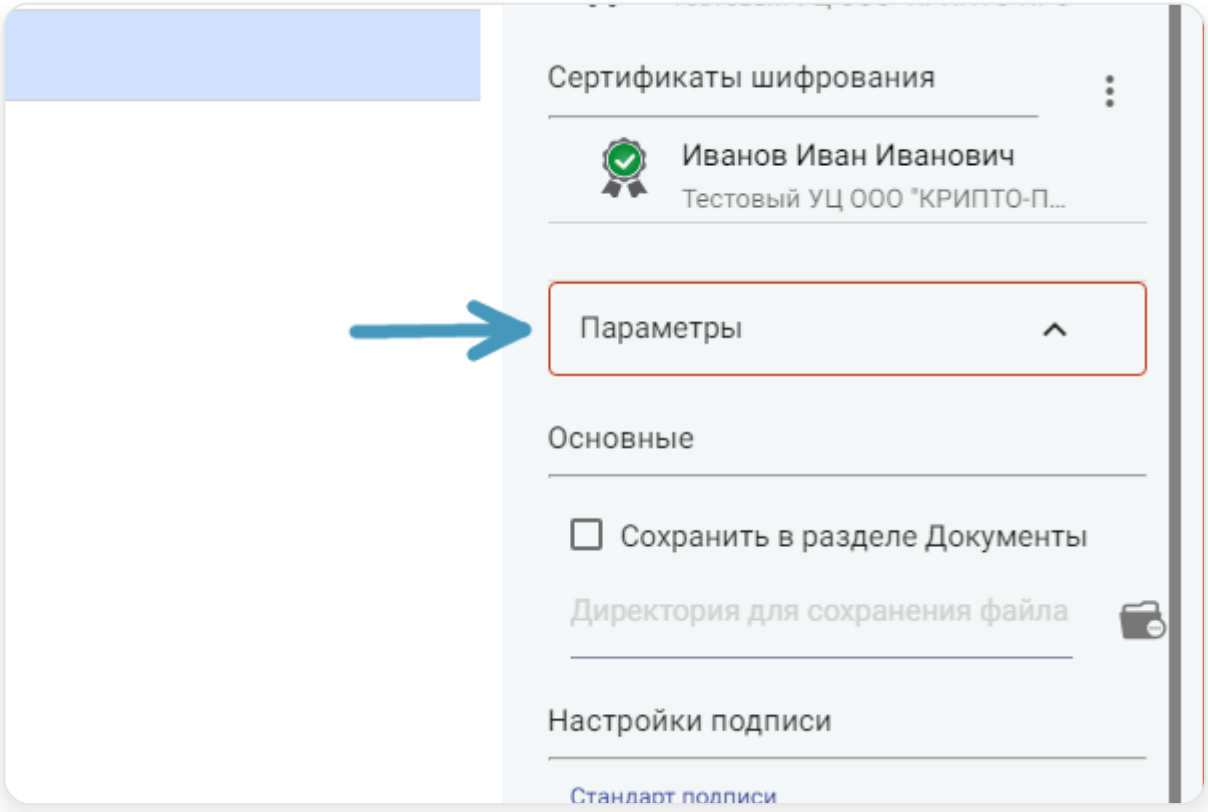
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



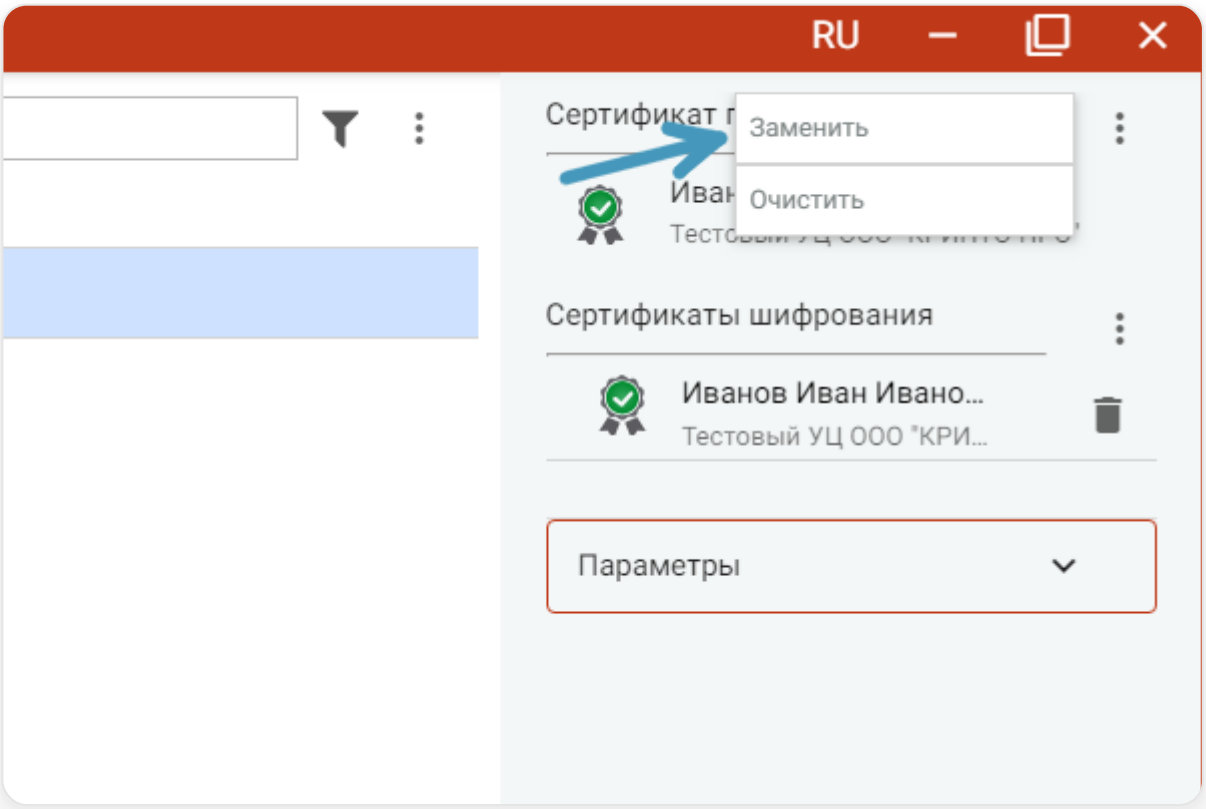
3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

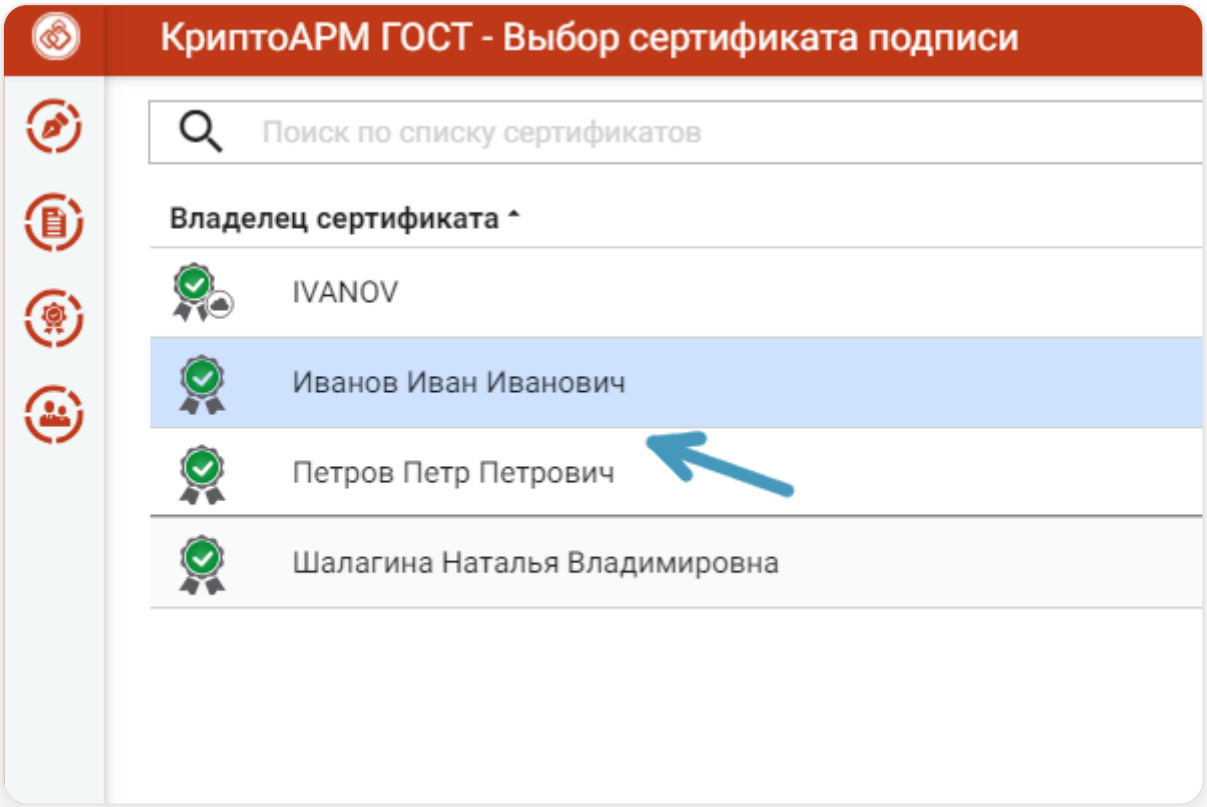
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.

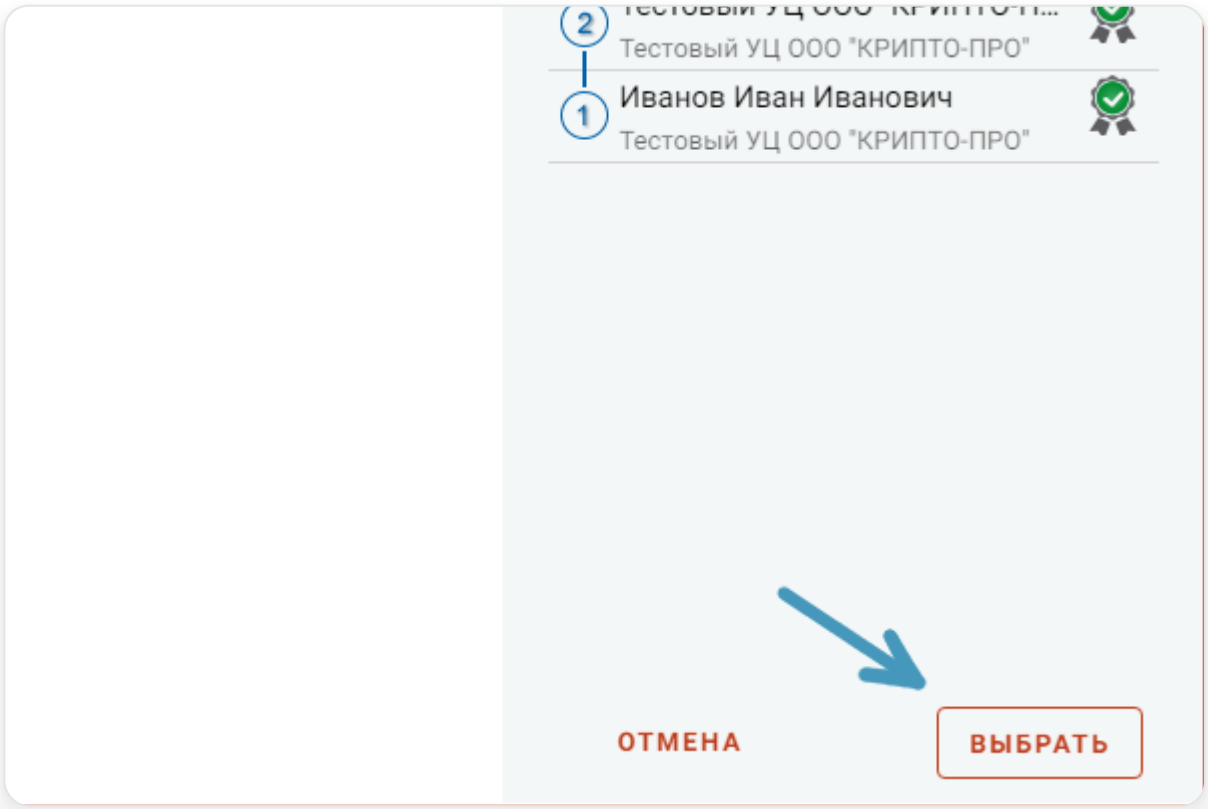


6. Выберите сертификат подписи. Если Вы не хотите использовать сертификат по умолчанию, нажмите кнопку **“Заменить”** в контекстном меню подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

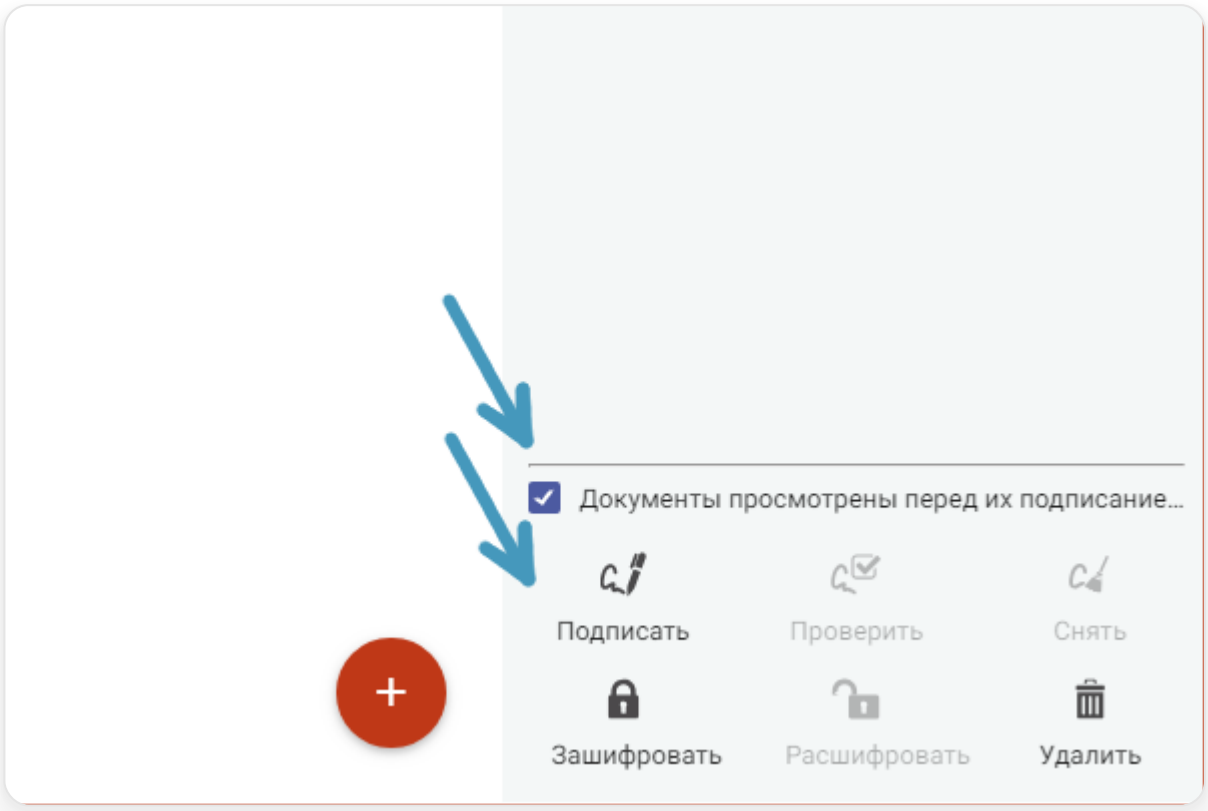


7. Выберите нужный сертификат и нажмите кнопку **“Выбрать”**.



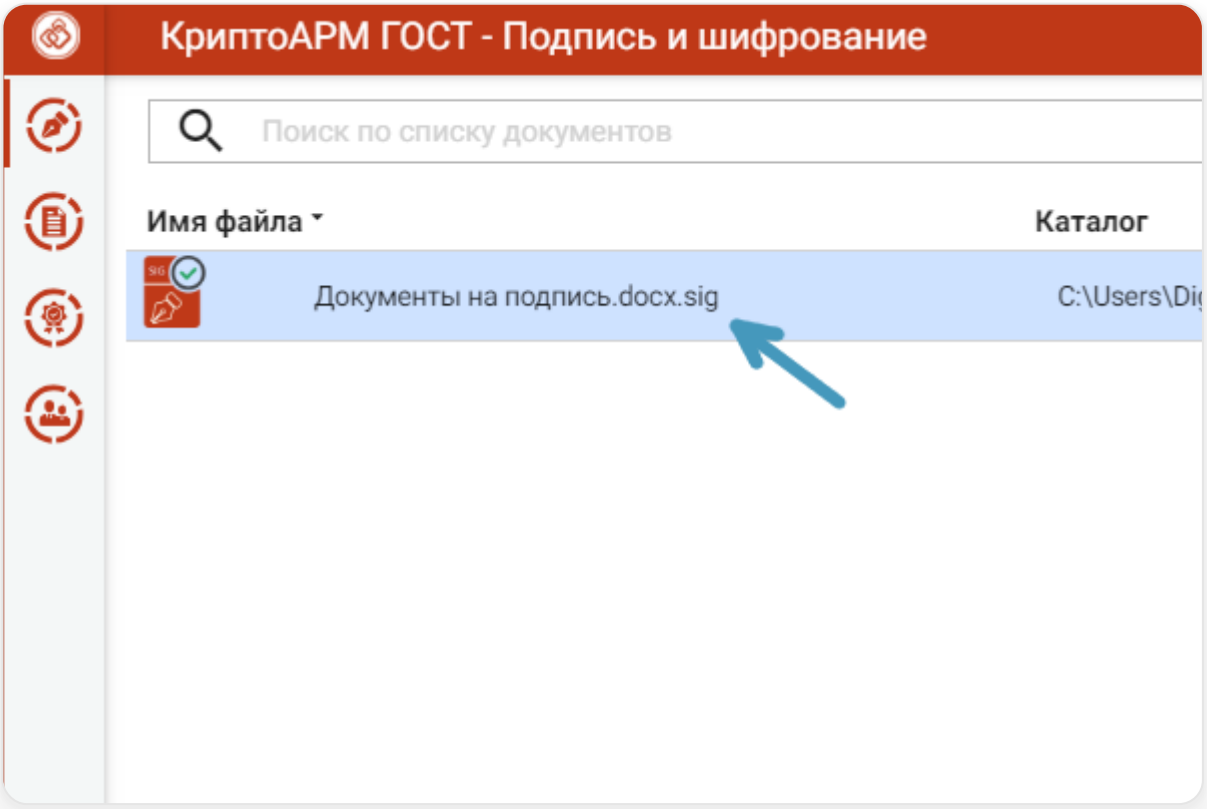


8. Выберите флаг **“Документы просмотрены перед их подписанием”**.



9. Нажмите на кнопку**“Подписать”**.

10. Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.



Открыть статью на сайте

Как подписать котировочную заявку электронной подписью

Архив. КриптоАРМ ГОСТ.

Котировочная заявка - это документ, который составляется участником конкурса на исполнение госзаказа. Государство объявляет конкурс, участники которого предлагают свои условия исполнения заказа с помощью подачи котировочных заявок. Порядок запроса котировок регулирует федеральный закон **"О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд" № 44-ФЗ**.

Котировочная заявка должна включать в себя следующие сведения:

1. Для юридических лиц - наименование, место нахождения, для физических лиц - ФИО, место жительства;
2. Почтовый адрес участника котировок, банковские реквизиты;
3. Согласие участника на исполнение контракта;
4. Предложение о цене товаров и услуг;
5. Документы, подтверждающие право участника на получение преимуществ, или их копии;
6. ИНН налогоплательщика;
7. Декларацию о принадлежности участника к субъектам малого строительства или социально ориентированной НКО;
8. Документы, подтверждающие закупку товаров и услуг для исполнения контракта;
9. Декларация о соответствии участника требованиям к исполнению контракта (по критериям п.3-9, ст. 31 44-ФЗ);
10. Указание страны товара, закупаемого при исполнении контракта.

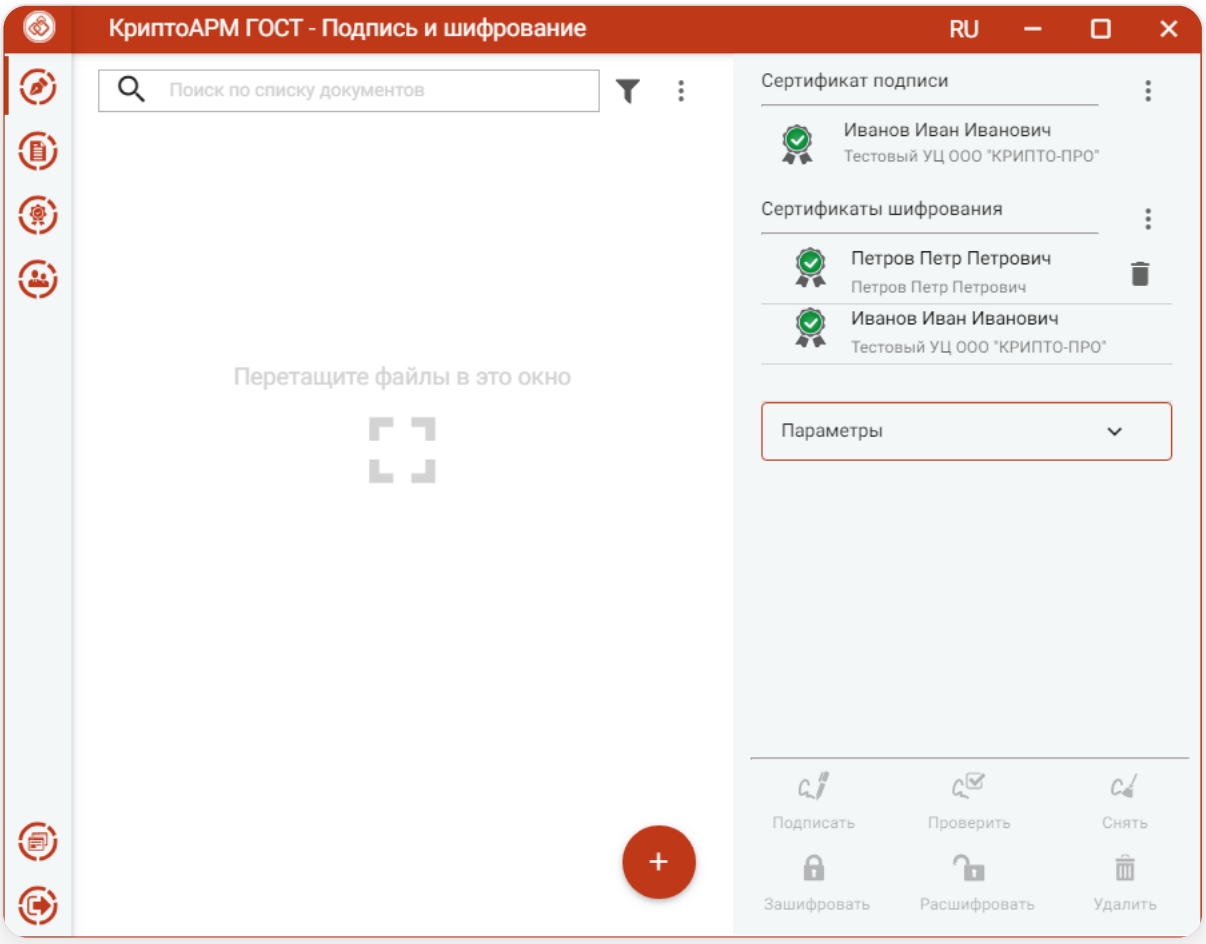
С 1 января 2019 года запрос котировочных заявок принимается в электронной форме. Котировочная заявка должна быть подписана усиленной квалифицированной электронной подписью.

Что нужно для подписи:

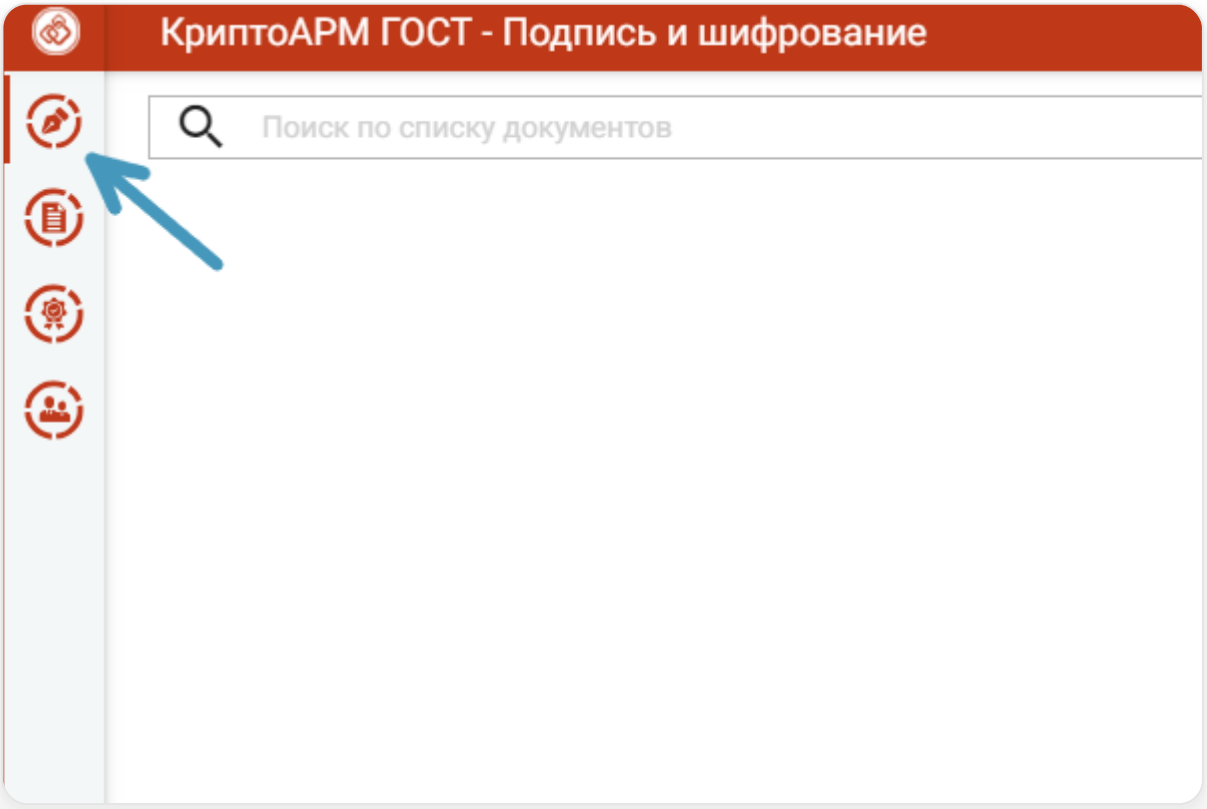
1. Установленная программа КриптоАРМ ГОСТ.
2. Установленный криптопровайдер КриптоПро CSP.
3. Усиленная квалифицированная электронная подпись.

Чтобы подписать котировочную заявку в КриптоАРМ ГОСТ:

1. Откройте КриптоАРМ ГОСТ.



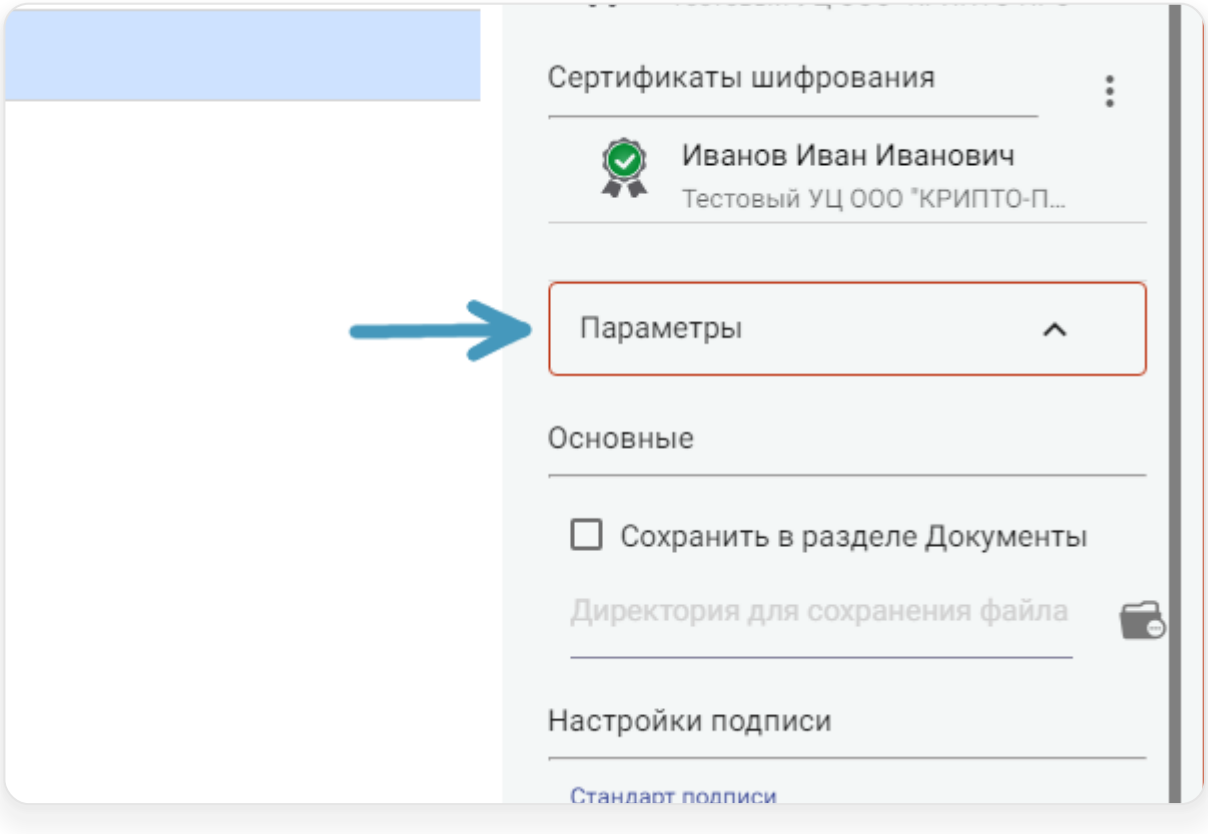
2. Откройте страницу **“Подпись и шифрование”** или **“Документы”** в левом меню программы.



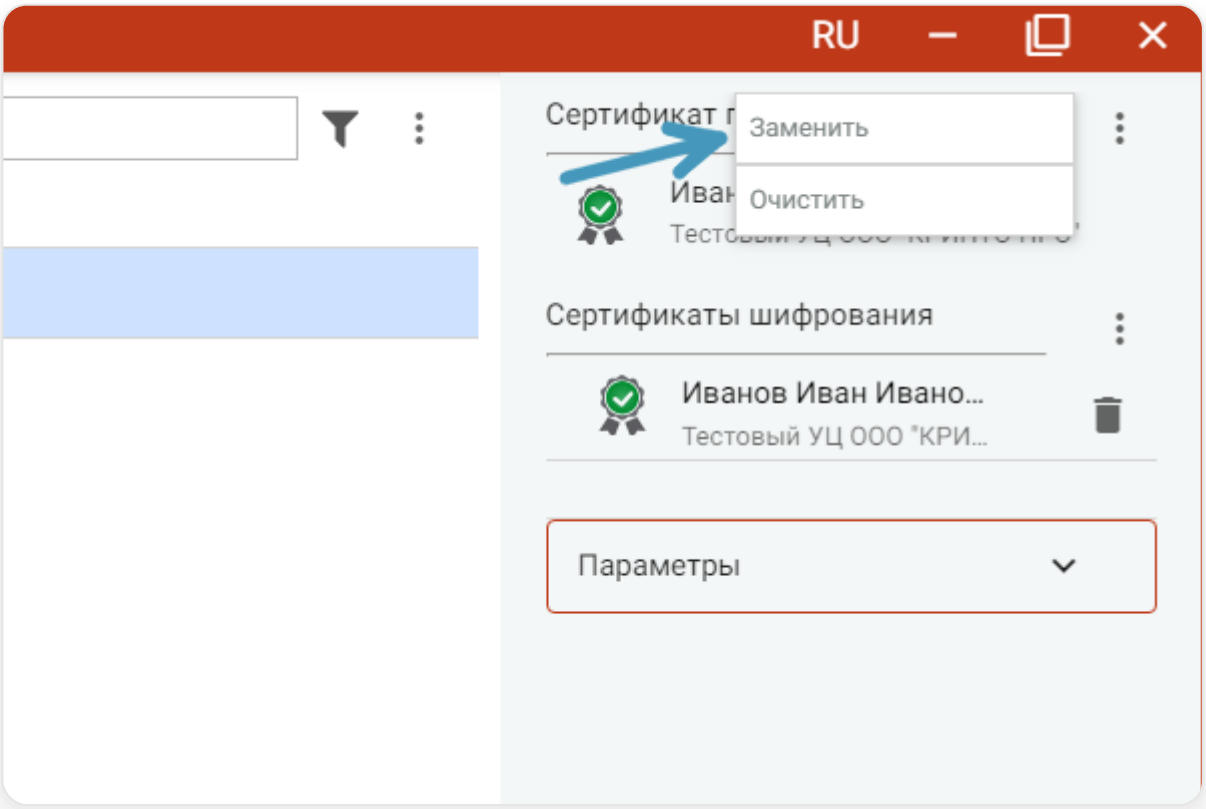
3. Выберите файлы, нажав на кнопку **“+”**, или перетащите их мышкой в область списка файлов.

4. Настройте подпись. При первом запуске приложения создается настройка по умолчанию **“Настройка #1”**, в которой задается кодировка подписи base64, вид подписи – присоединенная. В подпись будет добавлено время подписи.

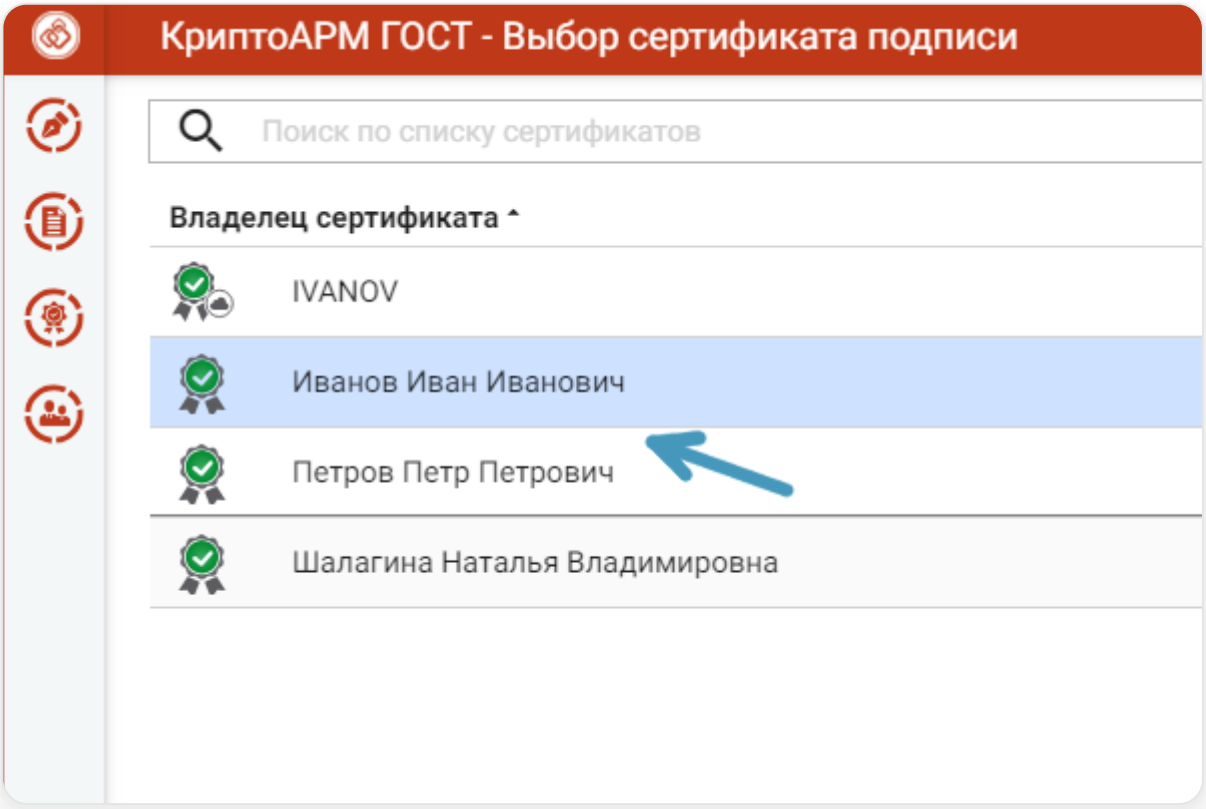
5. Если Вы хотите изменить настройки подписи, нажмите на кнопку **“Параметры”** в контекстном меню.

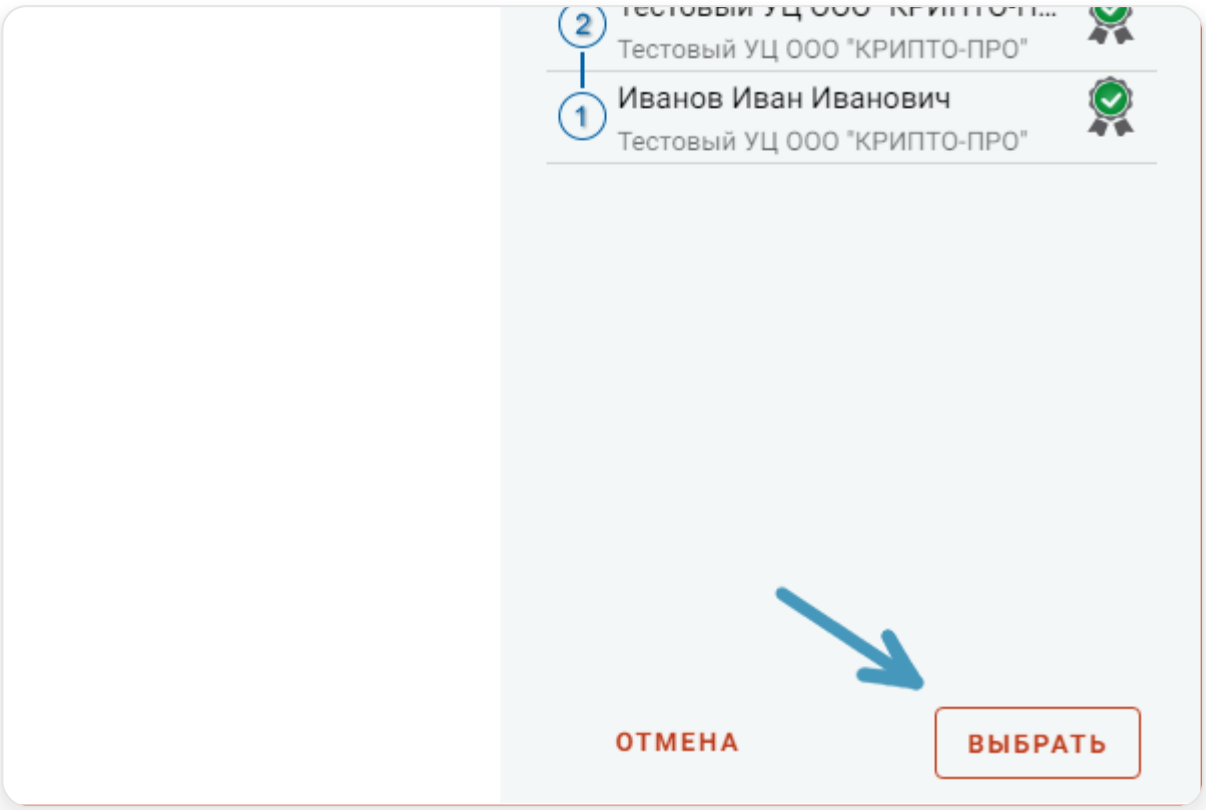


6. Выберите сертификат подписи. Если Вы не хотите использовать сертификат по умолчанию, нажмите кнопку **“Заменить”** в контекстном меню подписи. В появившемся окне появятся сертификаты, которые могут использоваться для подписи документа.

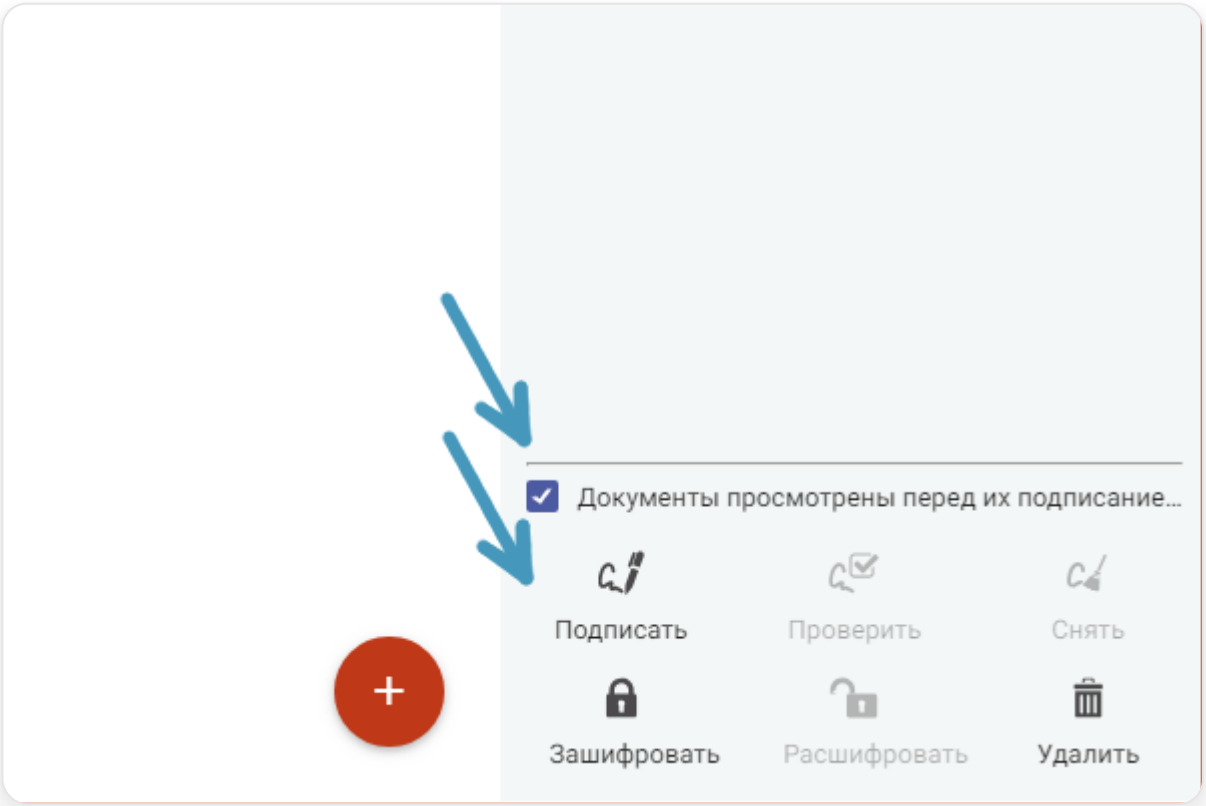

RU
Заменить
Очистить
Сертификаты шифрования
Иванов Иван Ивано...
Тестовый УЦ ООО "КРИ...
Параметры

7. Выберите нужный сертификат и нажмите кнопку **“Выбрать”**.



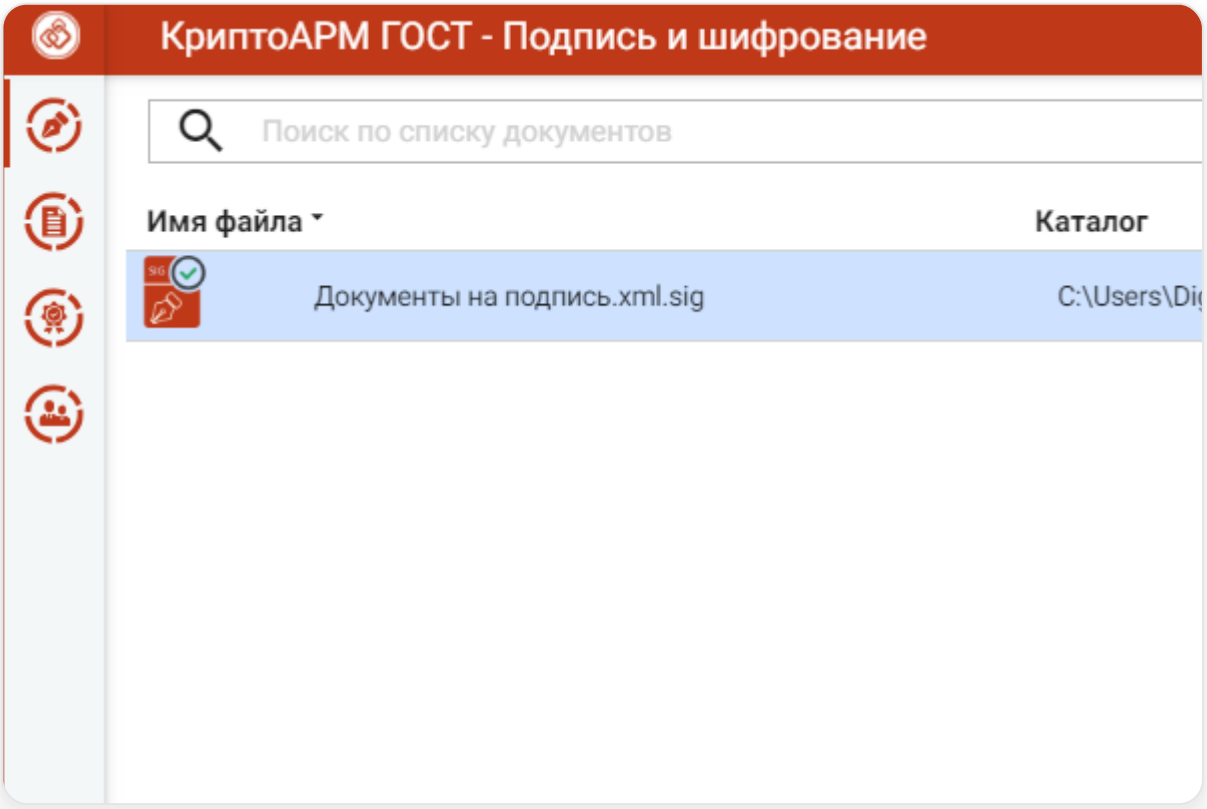


8. Выберите флаг **“Документы просмотрены перед их подписанием”**.



9. Нажмите на кнопку **“Подписать”**.

10. Если подпись файла прошла успешно, приложение уведомит Вас об этом. Расширение файла сменится на ***.sig**. Теперь документ заверен электронной подписью.



Открыть статью на сайте

Как подписать декларацию в ФСРАР

Архив. КриптоАРМ ГОСТ.

Если организация или индивидуальный предприниматель осуществляют оборот алкогольной продукции, им нужно предоставлять отчёты в Росалкогольрегулирование. Декларации включают в себя информацию об объемах производства, оборота и (или) использования этилового спирта, алкогольной и спиртосодержащей продукции.

В число подотчётных организаций входят:

1. Организации, осуществляющие производство и продажу продукции с содержанием этилового спирта, алкогольной и спиртосодержащей продукции с содержанием этилового спирта более 25% объема общей продукции;
2. ИП, осуществляющие торговлю пивом и пивными напитками;
3. Организации, осуществляющие закупку этилового спирта в объемах больше 200 декалитров в год по фармакопейным статьям для производства этилового спирта или лекарственной продукции;
4. Организации, осуществляющие производство этилового спирта или спиртосодержащей продукции.

Более подробно о требованиях к предоставлению деклараций читайте в постановлении Правительства Российской Федерации от 09.08.2012 № 815 «О представлении деклараций об объеме производства, оборота и (или) использования этилового спирта, алкогольной и спиртосодержащей продукции, об использовании производственных мощностей».

Порядок заполнения деклараций и Классификатор видов продукции утверждены Приказом Росалкогольрегулирования от 17.12.2020 № 396.

Сроки предоставления деклараций:

Декларации для Росалкогольрегулирования должны подаваться ежеквартально, не позднее 20 числа месяца, следующего за отчётным кварталом. Так, если Вы предоставляете отчётность за квартал с января по март, декларация должна быть подана не позднее 20 апреля.

В том случае, если 20 число месяца выпадает на нерабочий день, декларация должна быть подана не позднее следующего рабочего дня.

Предоставление электронной декларации:

Декларации в ФСРАР можно подать не только в бумажном, но и в электронном виде в формате XML-таблицы. Декларации предоставляются в Личном кабинете на сайте ФСРАР.

Зарегистрироваться в Личном кабинете можно с помощью учётной записи ЕСИА «Госуслуги» (важно, чтобы учётная запись была подтвержденной) или с помощью усиленной квалифицированной электронной подписи, получить которую можно в аккредитованном Удостоверяющем Центре.

К загружаемой электронной декларации есть определённые требования оформления. Имя файла перед подписью должно иметь следующий вид:

D1_номер-ИНН-организации_Z_ddmmgggg_N.xml, где:

1. Z — двузначный номер квартала, за который подаётся декларация: для I квартала — 03, для II квартала — 06, для III квартала — 09, для IV квартала — 00 и последней цифры года, за который передается информация. Например, Z для декларации за первый квартал 2020 года будет иметь значение 030.

2. gggg — год, mm — месяц, dd — день формирования передаваемого файла. Например, 20052020 — если декларация сформирована на момент 20 мая 2020 года;

3. N — 36-символьный номер передаваемого файла, который формируется с использованием глобально уникального идентификатора GUID.

Файл обмена должен быть подписан усиленной квалифицированной электронной подписью (ЭП) организации-декларанта, представляющего декларацию. Шифрование и архивирование файла обмена должно осуществляться сертификатом Росалкогольрегулирования.

При начальном имени файла **D1_номер-ИНН-организации_Z_ddmmgggg_N.xml** конечный файл получился — **D1_номер-ИНН-организации_Z_ddmmgggg_N.xml.sig.zip.enc** (расширение enc может не отображаться в проводнике Windows, при этом «Тип» должен быть «Шифрованные данные»).

Первая строка XML-файла электронной декларации должна иметь следующий вид:

<?xml version="1.0" encoding ="windows-1251"?>

Что нужно для подписи:

1. Установленная программа КриптоАРМ ГОСТ.

2. Установленный криптопровайдер КриптоПро CSP.

3. Установленный КриптоПро ЭЦП Browser plug-in — расширение для браузера.

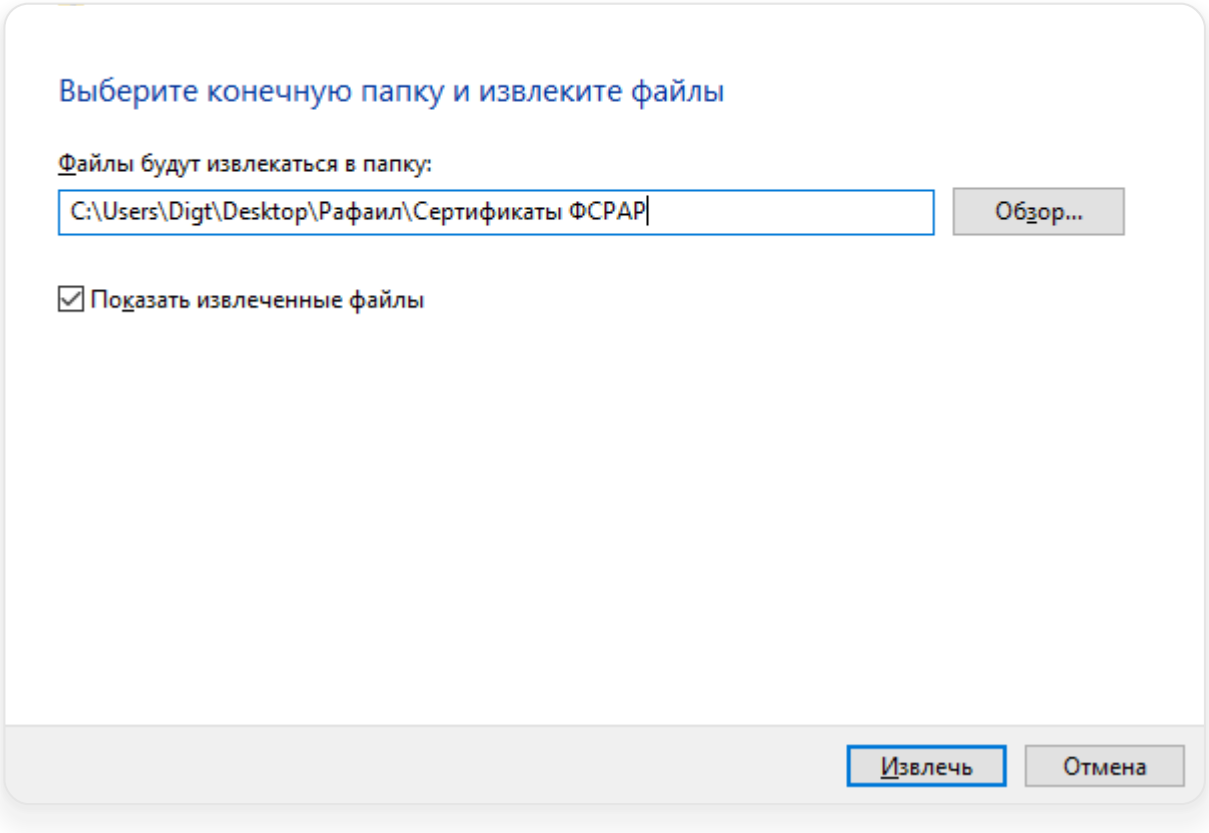
4. Усиленная квалифицированная электронная подпись.

Как подписать электронную декларацию в ФСРАР и подать её в электронном виде:

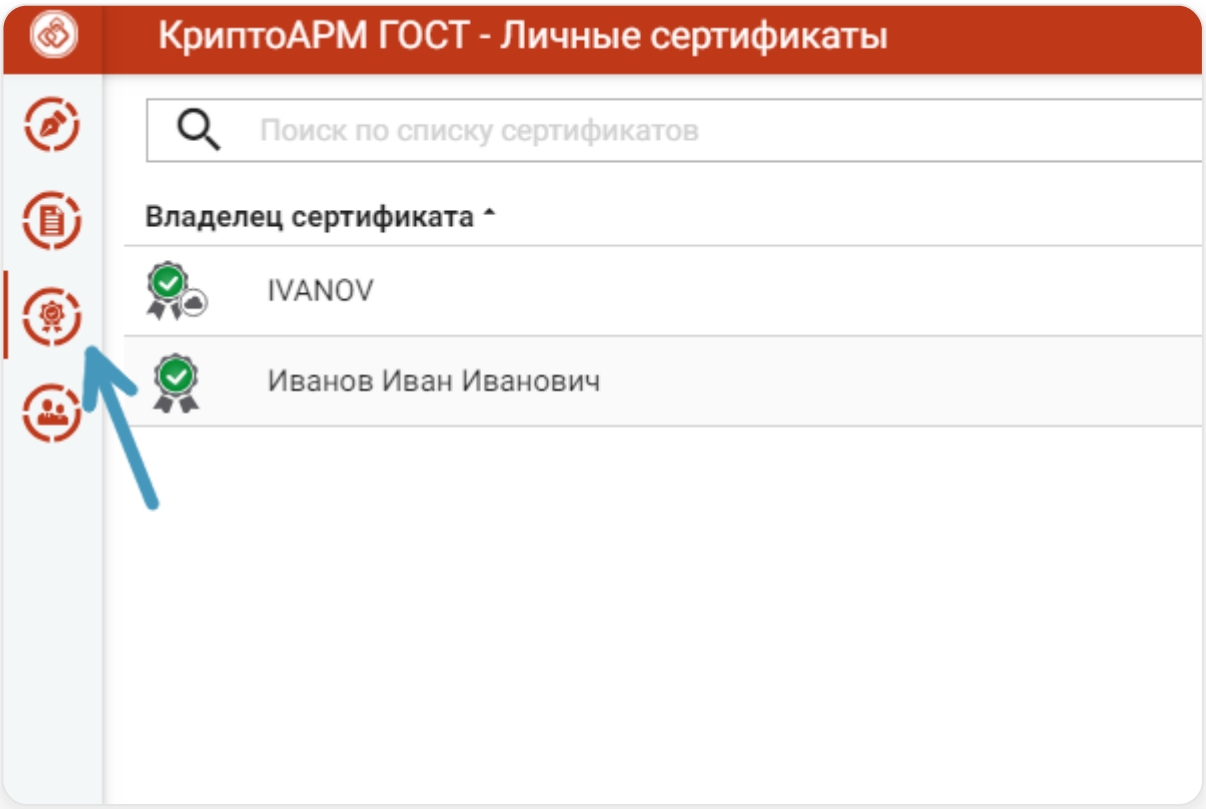
1. Получите личный сертификат электронной подписи для отчетности в ФСРАР в одном из аккредитованных Удостоверяющих Центров (УЦ).

2. Скачайте архив с сертификатами Росалкогольрегулирования.

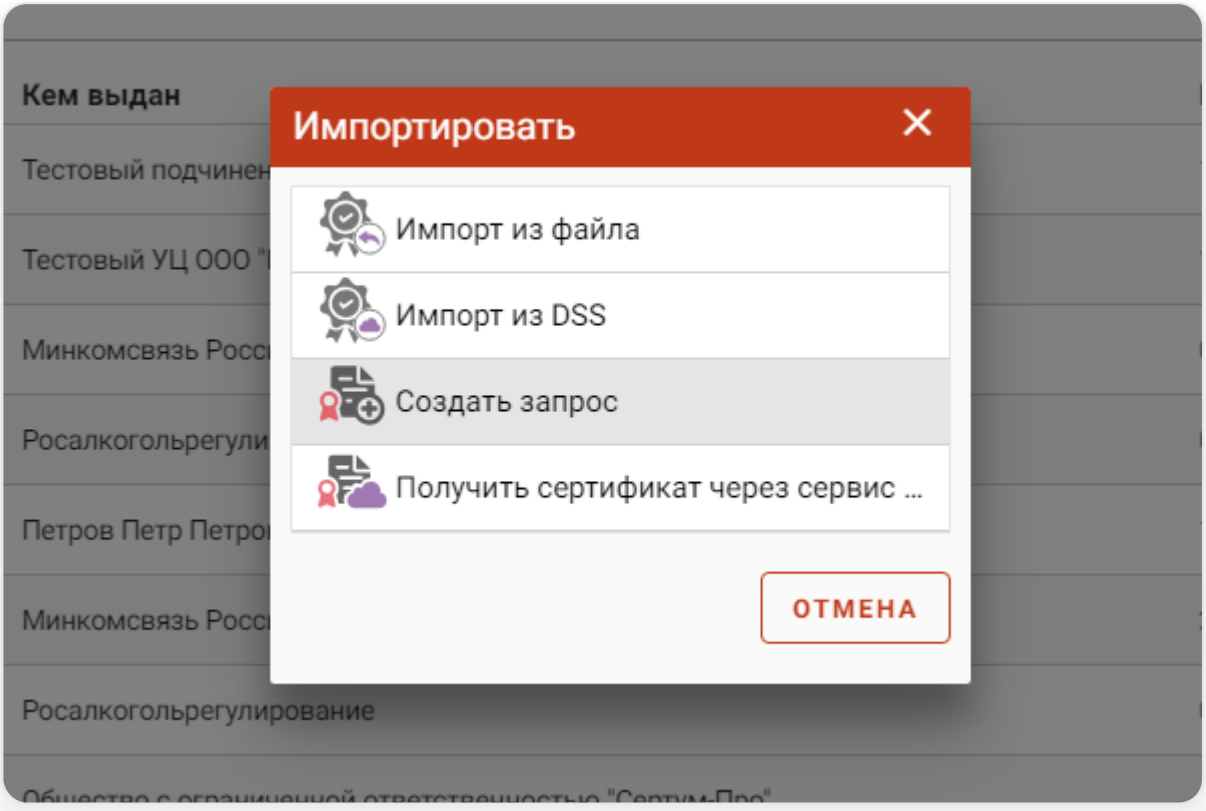
3. Распакуйте сертификаты ФСРАР из загруженного архива.



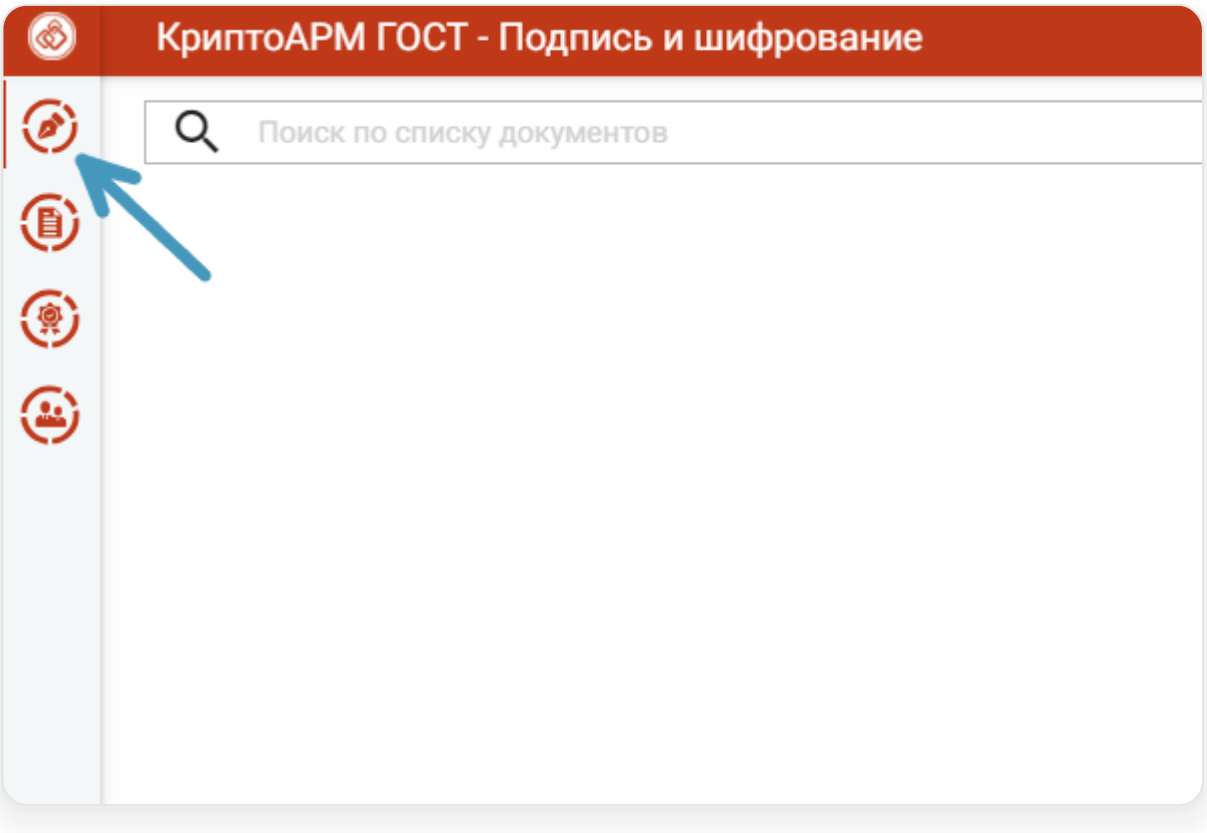
4. Поочерёдно установите скачанные сертификаты: **Орган исполнительной власти субъекта РФ.cer** и **Федеральная служба по регулированию алкогольного рынка.cer**. Для этого в КриптоАРМ ГОСТ зайдите во вкладку **Сертификаты** в контекстном меню программы.



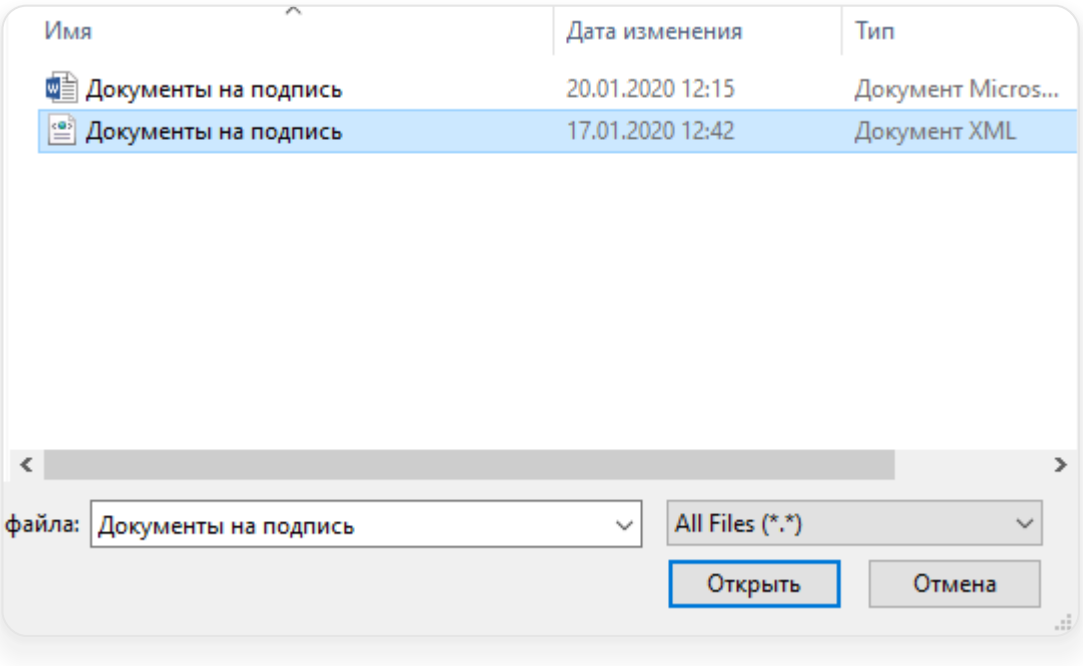
5. В меню окна **Сертификаты** нажмите на значок **+ — Импорт из файла**.



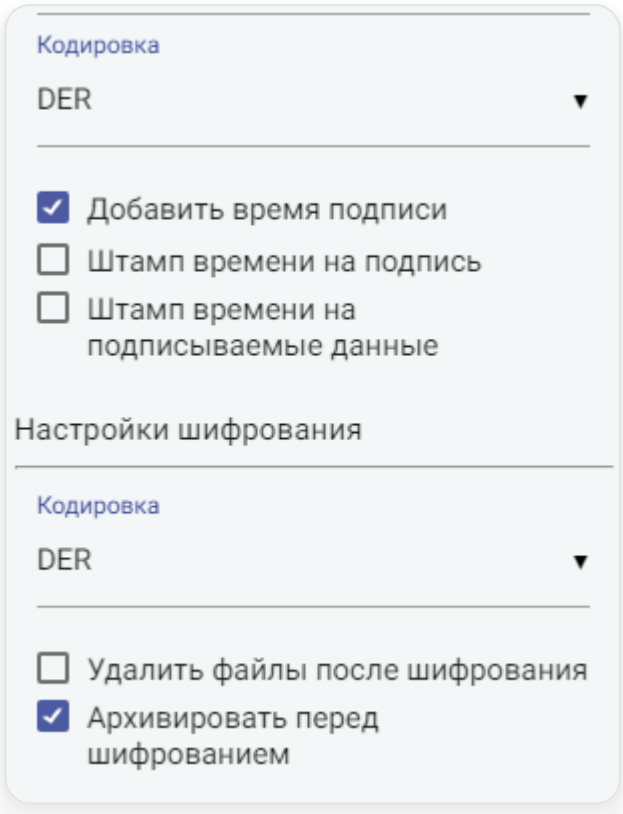
6. Найдите нужные сертификаты и нажмите **Открыть**.
7. Поочередно добавьте все нужные сертификаты ФСРАР. Они должны появиться в списке сертификатов в КриптоАРМ ГОСТ.
8. Сформируйте файл декларации в электронном виде на основе XML-таблицы (Excel).
9. Откройте документ с декларацией в КриптоАРМ ГОСТ. Для этого откройте страницу **Подпись и шифрование** или **Документы** в КриптоАРМ ГОСТ.



10. Выберите файл декларации, нажав на кнопку **+**, или перетащите их мышкой в область списка файлов.



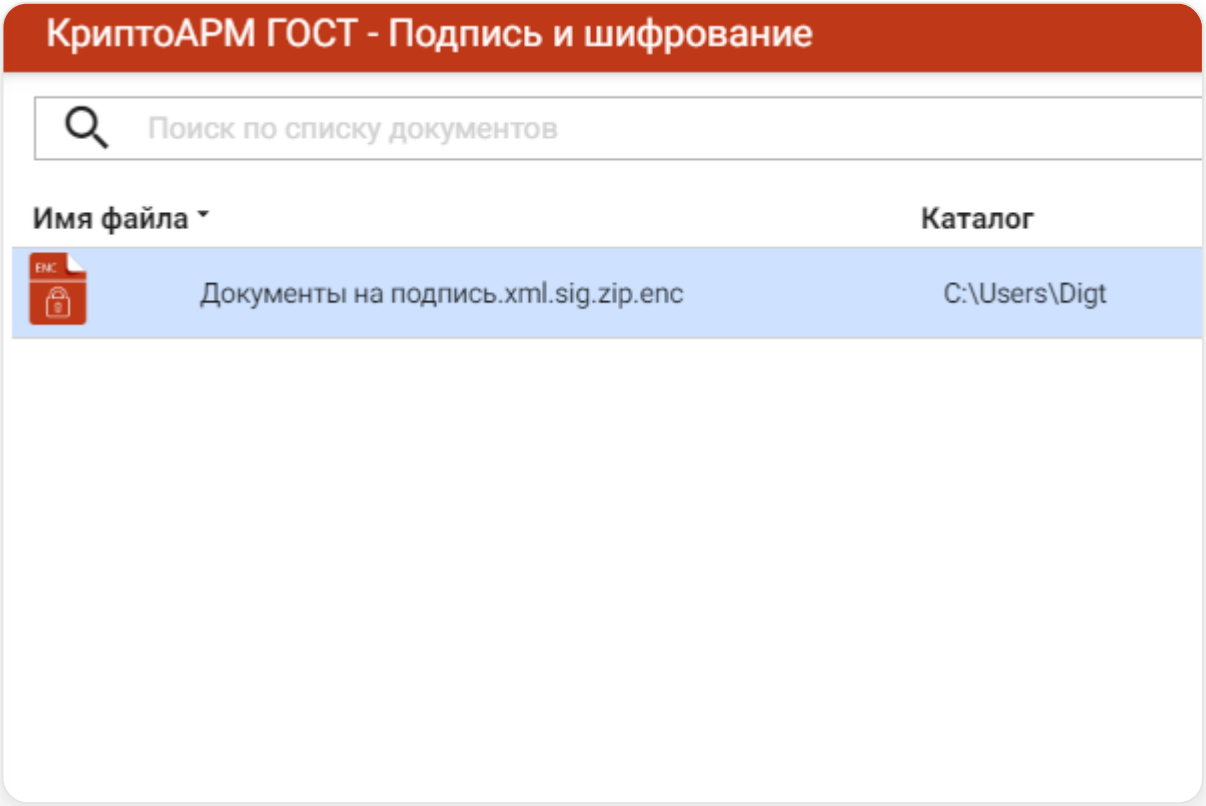
11. В правой области окна выберите сертификат подписи — сертификат вашей организации. В качестве сертификата шифрования выберите установленные сертификаты ФСРАР и Органа исполнительной власти, далее нажмите на кнопку **Параметры** и для подписываемого документа выберите **кодировку DER** и опцию **Архивировать файлы перед шифрованием**.



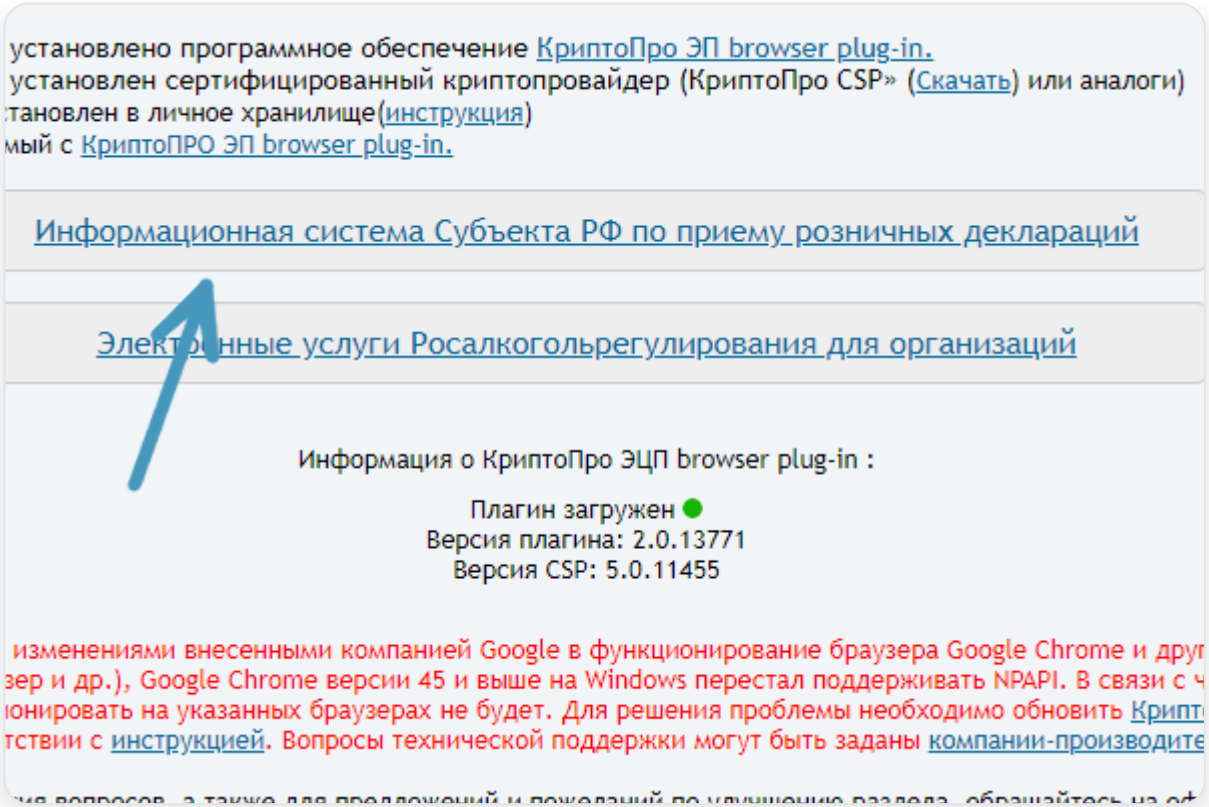
12. Поставьте галочку напротив опции **Добавить время подписи**.

13. Проверьте содержимое файла перед подписью. Установите флаг о том, что Вы просмотрели документ перед его подписанием.

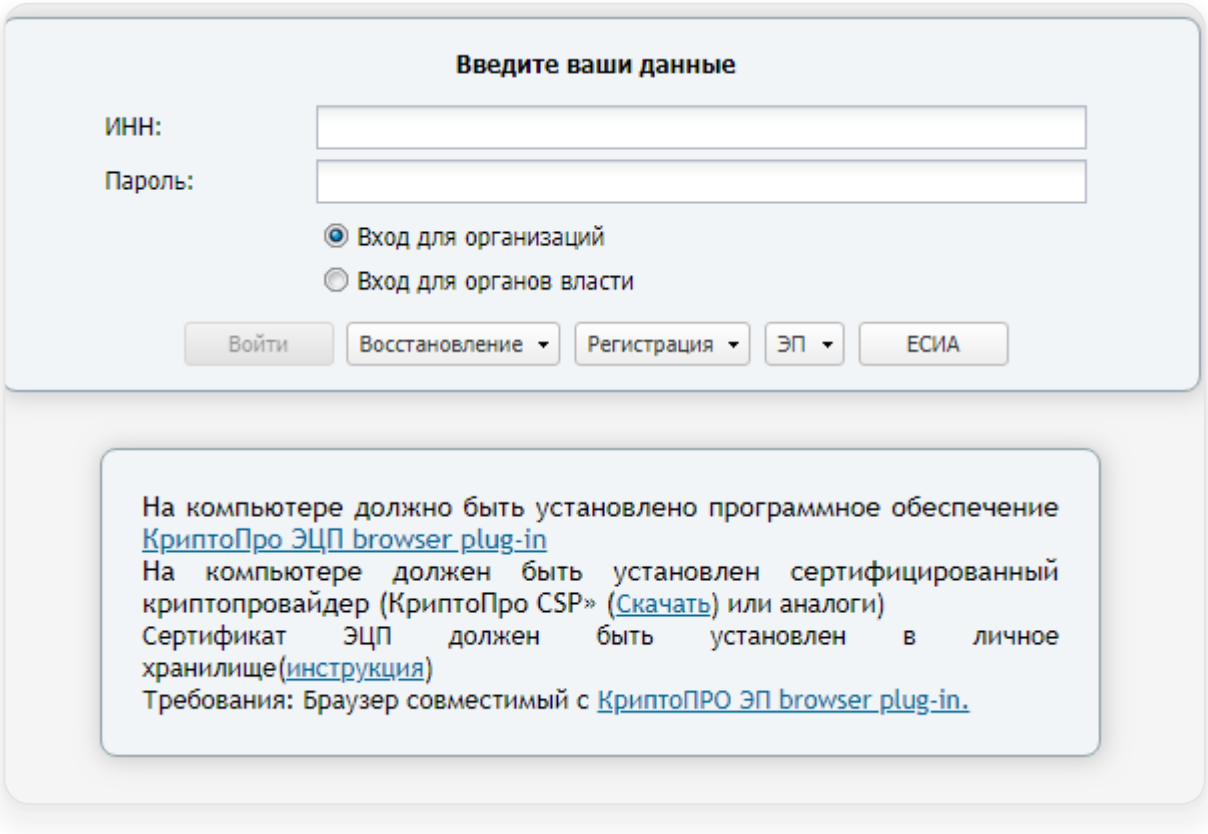
14. Нажмите на кнопку **Подписать**, затем нажмите кнопку **Зашифровать**. В результате Вы получите **файл с расширением .xml.sig.zip.enc**.



15. Зайдите в Личный кабинет ФСРАР. Убедитесь, что на компьютере установлен КриптоПро ЭЦП Browser plug-in.

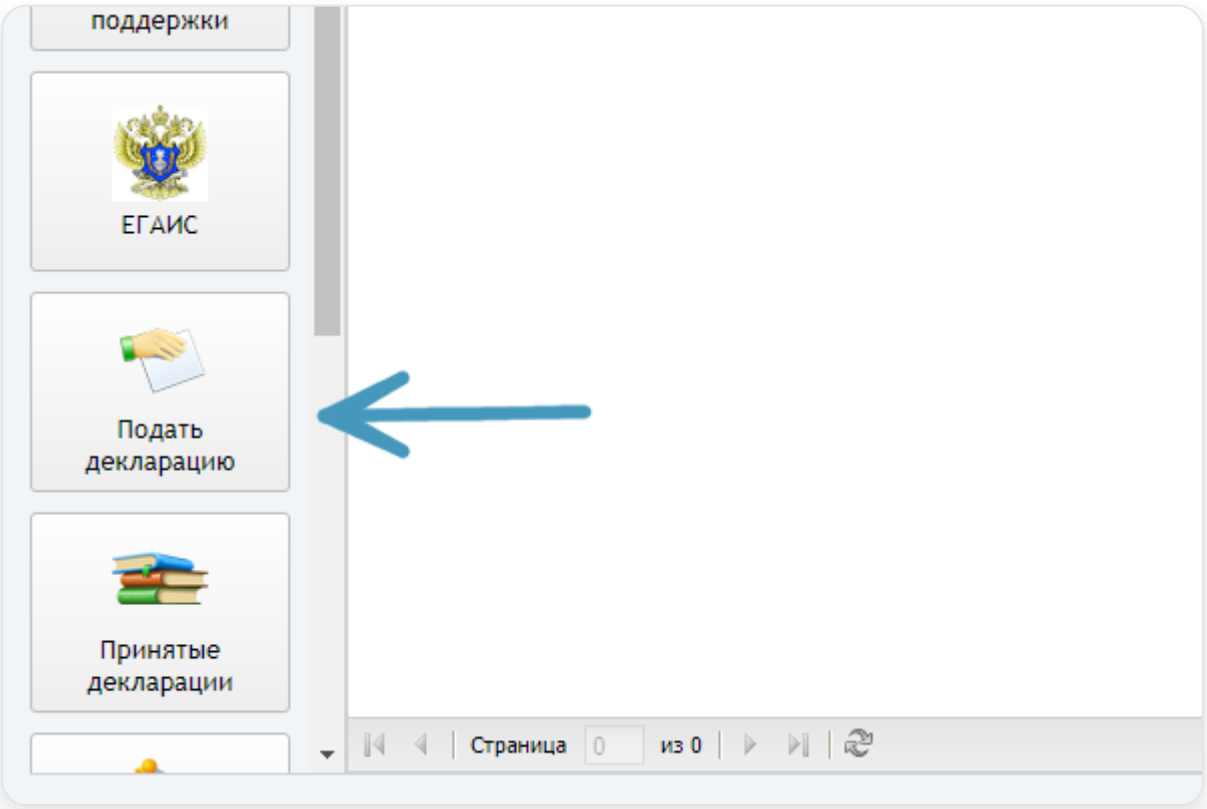


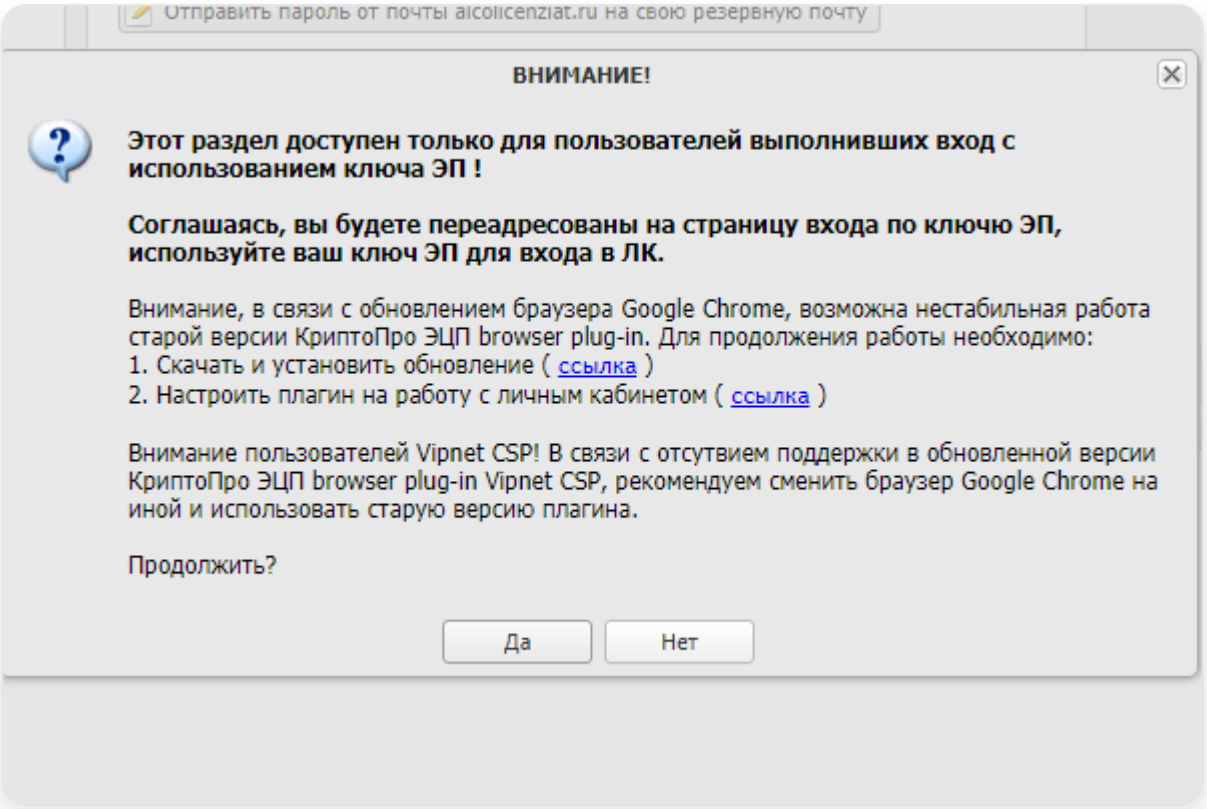
16. Выберите пункт **Информационная система Субъекта РФ по приёму розничных деклараций**. Откроется страница авторизации.



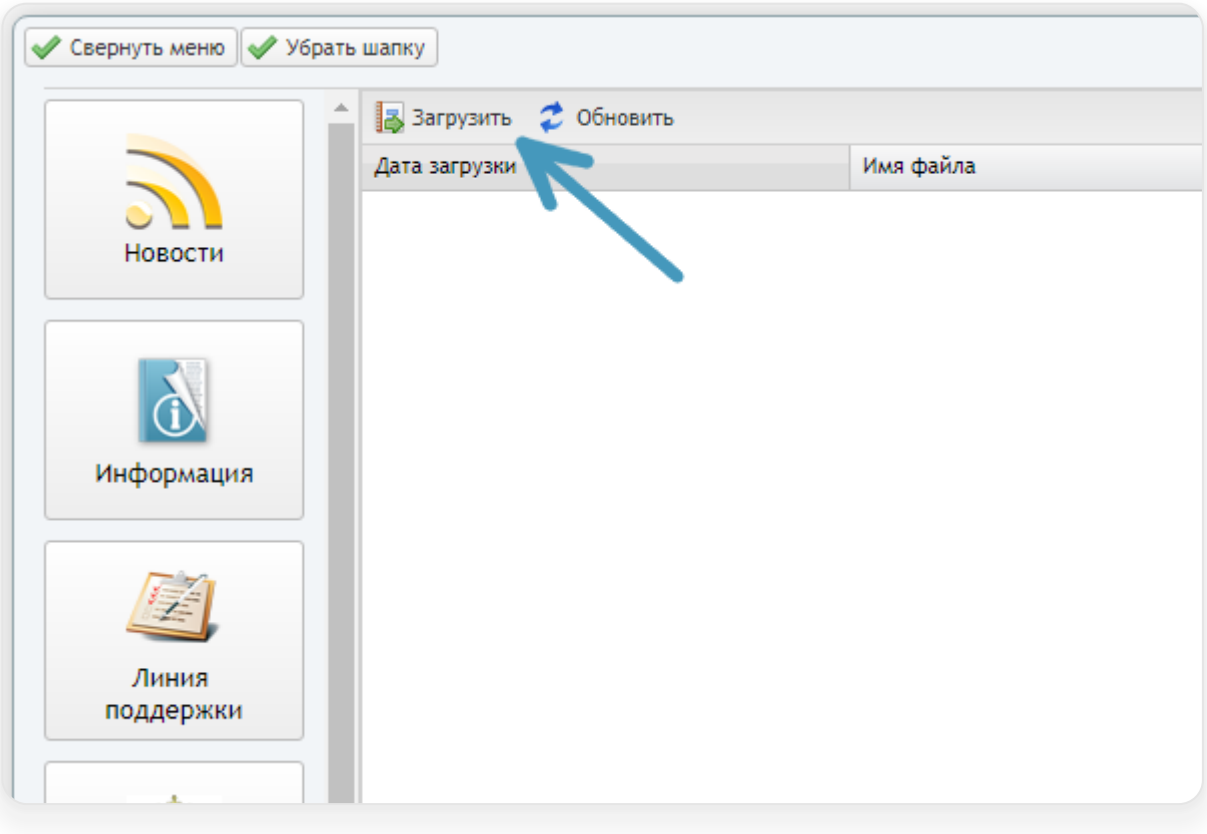
17. Заполните поля **“ИНН и пароль”** и нажмите кнопку **“Войти”**.

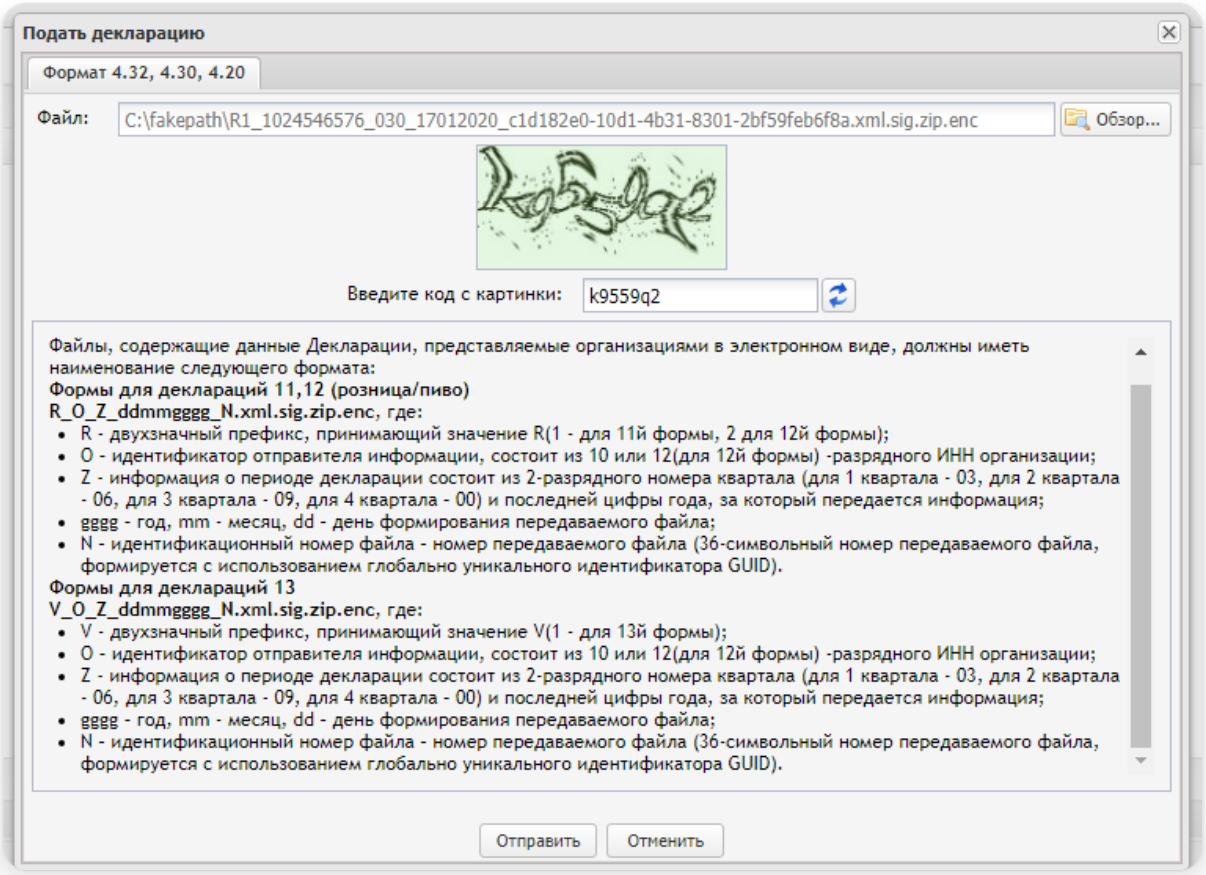
18. Откроется страница **Портал сервисов** ФСРАР. В левой области окна найдите кнопку **Подать декларацию** и нажмите её. Подтвердите переход к подаче декларации.


поддержки
ЕГАИС
Подать декларацию
Принятые декларации
Страница
0
из 0


Отправить пароль от почты alcolicenziat.ru на свою резервную почту
ВНИМАНИЕ!
Этот раздел доступен только для пользователей выполнивших вход с использованием ключа ЭП !
Соглашаясь, вы будете переадресованы на страницу входа по ключю ЭП, используйте ваш ключ ЭП для входа в ЛК.
Внимание, в связи с обновлением браузера Google Chrome, возможна нестабильная работа старой версии КриптоПро ЭЦП browser plug-in. Для продолжения работы необходимо:
1. Скачать и установить обновление (ссылка)
2. Настроить плагин на работу с личным кабинетом (ссылка)
Внимание пользователей Vipnet CSP! В связи с отсутвием поддержки в обновленной версии КриптоПро ЭЦП browser plug-in Vipnet CSP, рекомендуем сменить браузер Google Chrome на иной и использовать старую версию плагина.
Продолжить?
Да
Нет

19. На вкладке **Подать декларацию** нажмите кнопку **Загрузить**. Откроется окно загрузки: внимательно ознакомьтесь с требованиями к файлу.





20. Нажмите кнопку **Отправить**. Декларация будет успешно подана.

Открыть статью на сайте

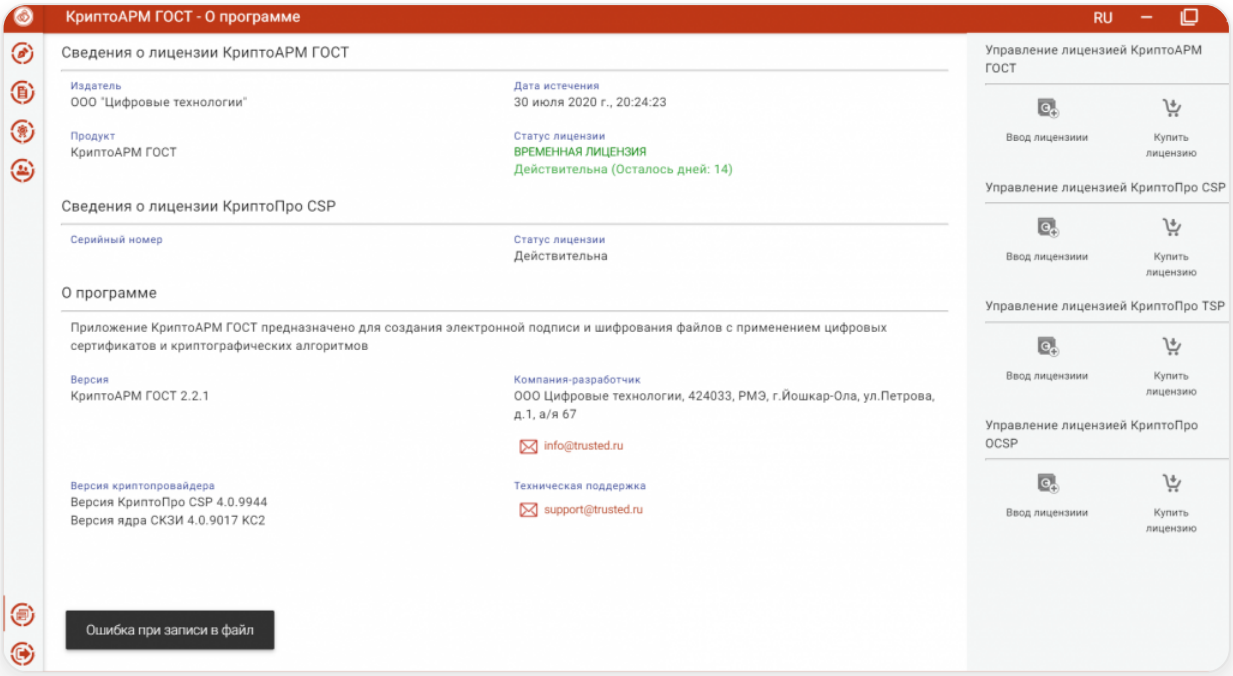
Ошибка при записи в файл во время установки лицензии

Архив. КриптоАРМ ГОСТ.

Текст ошибки:

Ошибка при записи в файл

Как выглядит ошибка:

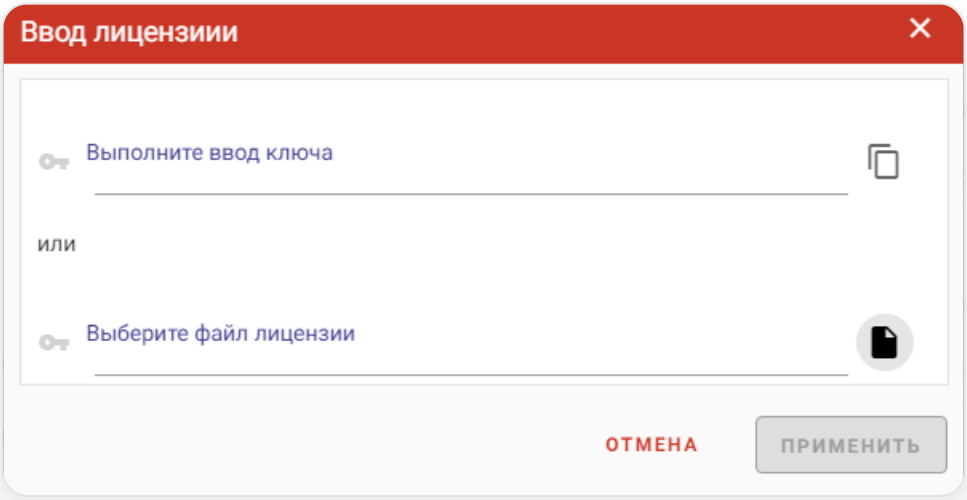


Решение

1. Выполните запуск программы от имени администратора и повторите попытку ввода ключа.

2. Создайте файл в блокноте, впишите туда символы лицензионного ключа без пробелов в начале и конце. Далее переименуйте этот файл в **license.lic** и повторите попытку ввода лицензии через меню **О программе** - **Ввод лицензии**. Также выполните запуск программы от имени администратора.

В окне выберите второй способ установки - **Выберите файл лицензии** и установите из файла.



Если этим способом лицензия также не установилась, то данный файл лицензии **КриптоАРМ ГОСТ 2.5** сохраните в папку пользователя в каталоге:

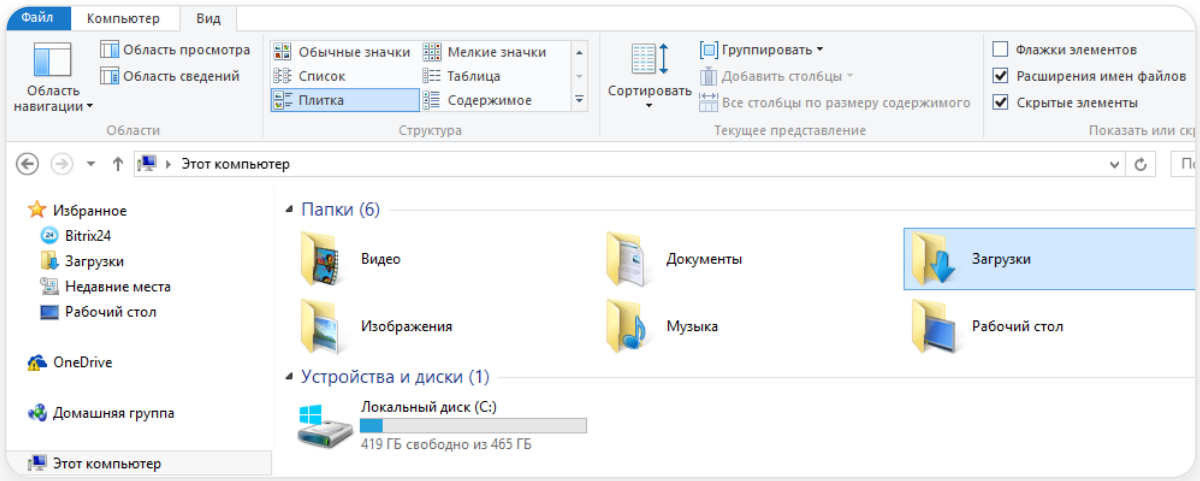
C:\Users\<имя пользователя>\AppData\Local\Trusted\CryptoARM GOST (в наименовании пути не должно быть русских букв). Для Linux каталог **/etc/opt/Trusted/CryptoARM GOST**. После сохранения файла лицензии перезапустите программу нажав кнопку **Выход**.

Для установки лицензии **КриптоАРМ ГОСТ 3 на Windows** путь будет такой:

C:\Users\<имя пользователя>**AppData** (скрытая, надо включить отображение папок в проводнике)**\Local\Trusted\CryptoARM GOST 3** для случая, если используется сертифицированная сборка **3.7.37**.

Для **Linux** каталог /etc/opt/Trusted/CryptoARM GOST 3 (или папка CryptoARM, в зависимости от сборки).

На операционных системах Windows может быть выключено отображение расширений файлов. Переименование файла в этом случае результата не даст, ошибка при записи в файл снова возникнет. Поэтому в проводнике выберите **Компьютер** - **Вид** и включите настройку **Расширения имен файлов**.



Тогда при переименовании файла лицензии у вас не возникнет ошибок и лицензия установится из этого файла.

Если файлом установить также не получается, можно записать лицензию в реестре компьютера, создав строковый параметр с именем license. Путь в реестре такой:

HKeyLocalMachine\SOFTWARE\Trusted\CryptoARM GOST

Ветка реестра для записи ключа КриптоАРМ ГОСТ 3:

HKeyLocalMachine\SOFTWARE\Trusted\CryptoARM GOST 3

Открыть статью на сайте

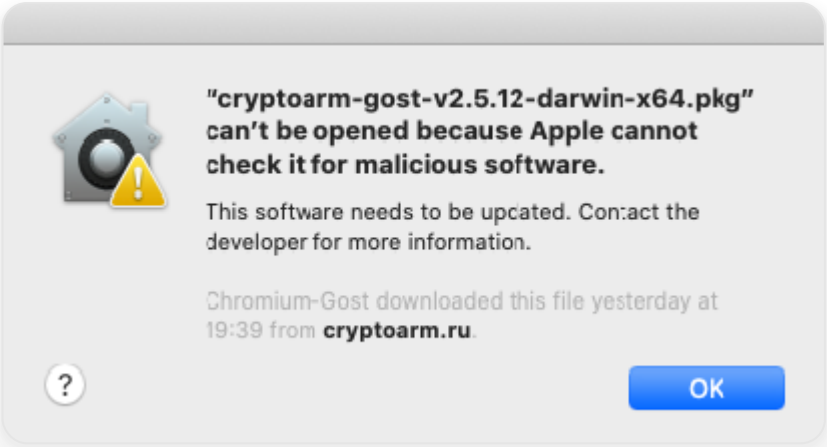
Не устанавливается КриптоАРМ ГОСТ на MacOS

Архив. КриптоАРМ ГОСТ.

Текст ошибки:

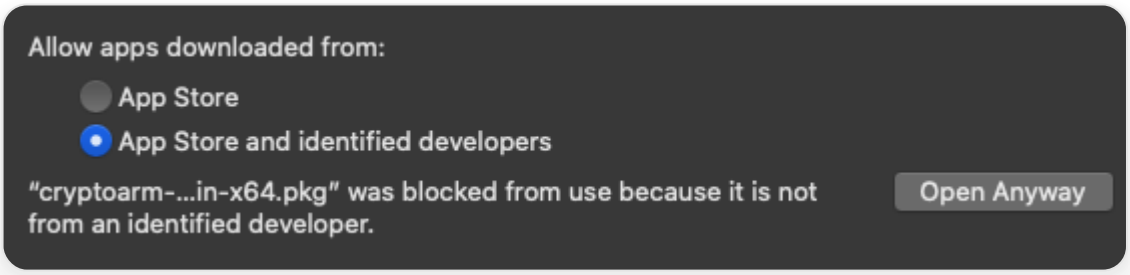
Не устанавливается КриптоАРМ ГОСТ на MacOS или Файл «cryptoarm-gost-v2.5.12-darwin-x64.pkg» невозможно открыть, так как Apple не может проверить его на наличие вредоносного ПО.

Как выглядит ошибка:

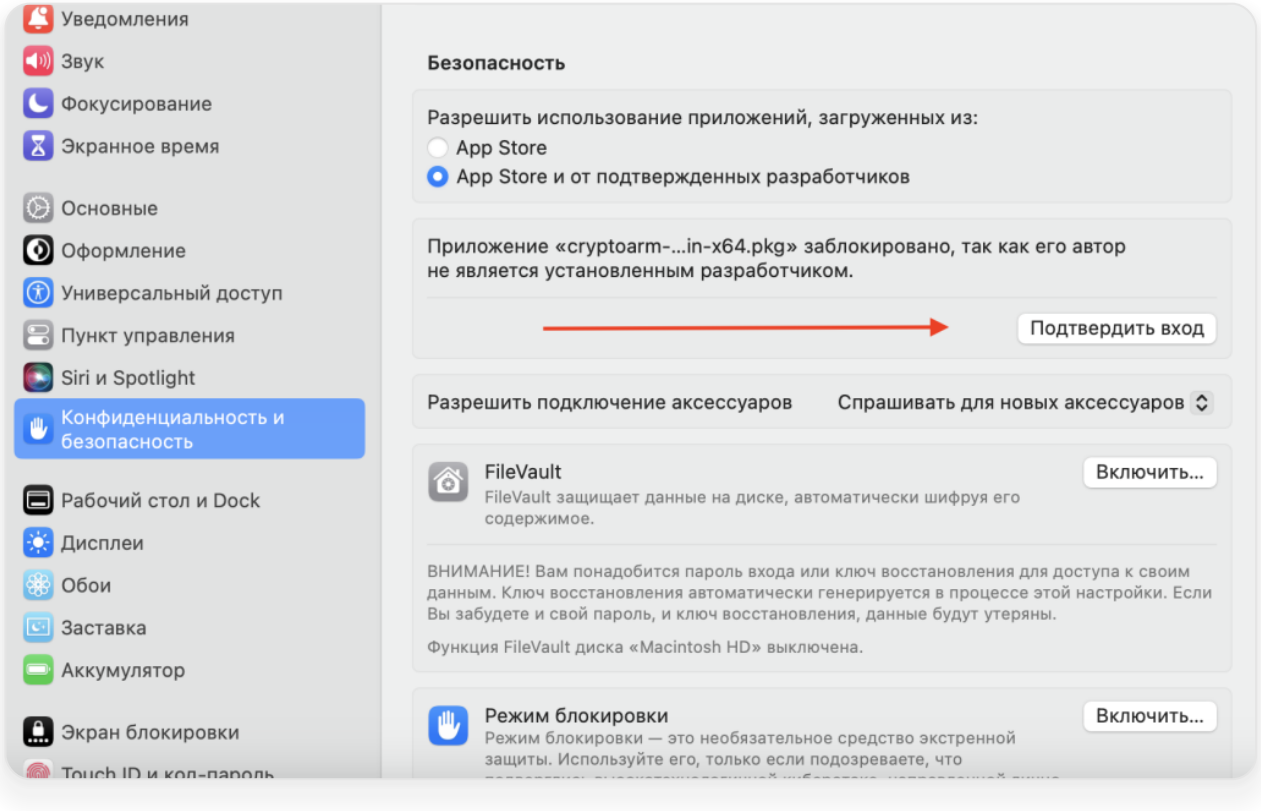


Решение:

- В меню **Системные настройки** щелкните **Защита и безопасность** и выберите **Основные**
- Щелкните значок замка (нужно чтобы он был открыт) и введите пароль, чтобы внести изменения.
- Выберите App Store в разделе Разрешить использование приложений, загруженных из.



На новых системах это может выглядеть таким образом, нажмите **Подтвердить вход**:



Открыть статью на сайте

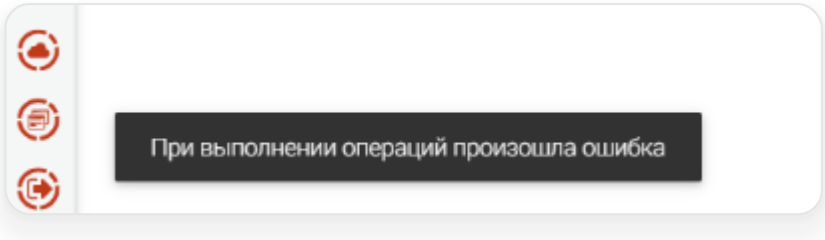
При выполнении операции произошла ошибка

Архив. КриптоАРМ ГОСТ.

Текст ошибки:

При выполнении операции возникла ошибка

Как выглядит ошибка:

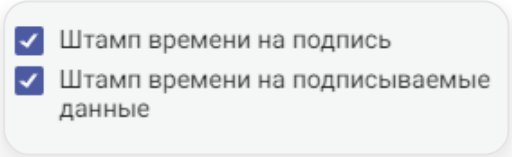


Решение:

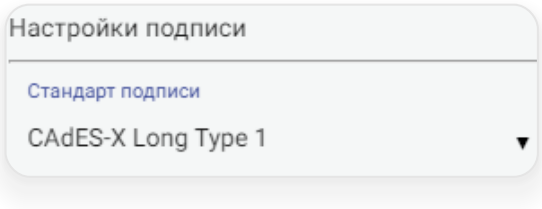
1. Проверьте, действительны ли лицензии на КриптоАРМ ГОСТ и КриптоПро CSP. В меню КриптоАРМ ГОСТ кнопка **О программе**. В меню КриптоПро CSP вкладка **Общие**. Если не действительна лицензия на КриптоАРМ ГОСТ, можно оформить заказ на нее здесь. Если у КриптоПро CSP истек срок действия лицензии, то приобрести ее можно по ссылке. Если обе лицензии действительны, перейдите к следующему пункту.

2. Зайдите в раздел **Подпись и шифрование**. Посмотрите на параметры подписи.

Если вы включили **Штамп времени на подпись** или **Штамп времени на подписываемые данные**, то это потребует покупки дополнительной лицензии на модуль штампа времени КриптоПро TSP client.



Если вы изменили стандарт подписи и выбрали **Cades-X Long Type 1**, то это потребует покупки еще одной дополнительной лицензии на модуль проверки статуса сертификата КриптоПро OCSP client.



Проверить наличие таких лицензии можно открыв на компьютере **Управление лицензиями КриптоПро PKI**. Без этих лицензий подписание с такими параметрами завершится ошибкой. Если стандарт подписи вы не меняли и не включали штампы времени, то понадобится переустановить сертификат подписи.

3. Переустановка сертификата описана в соответствующем разделе инструкции по ссылке.

4. Если вышеуказанные действия не помогли, пришлите лог нам на почту support@trusted.ru, который представляет собой текстовый файл **cryptoarm_gost_operations.log**, который располагается в каталоге пользователя в папке **.Trusted**.
Или пришлите скриншот вкладки Console после включения режима логирования на Linux и MacOS.

Открыть статью на сайте

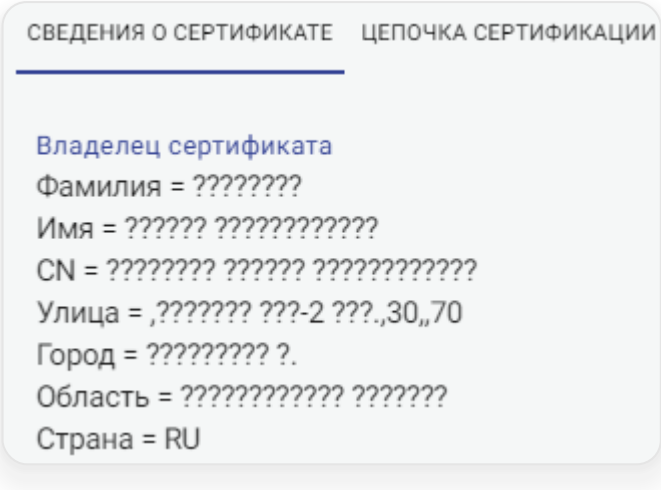
В полях сертификата вместо букв знаки вопроса

Архив. КриптоАРМ ГОСТ.

Текст ошибки:

В полях сертификата вместо букв знаки вопроса

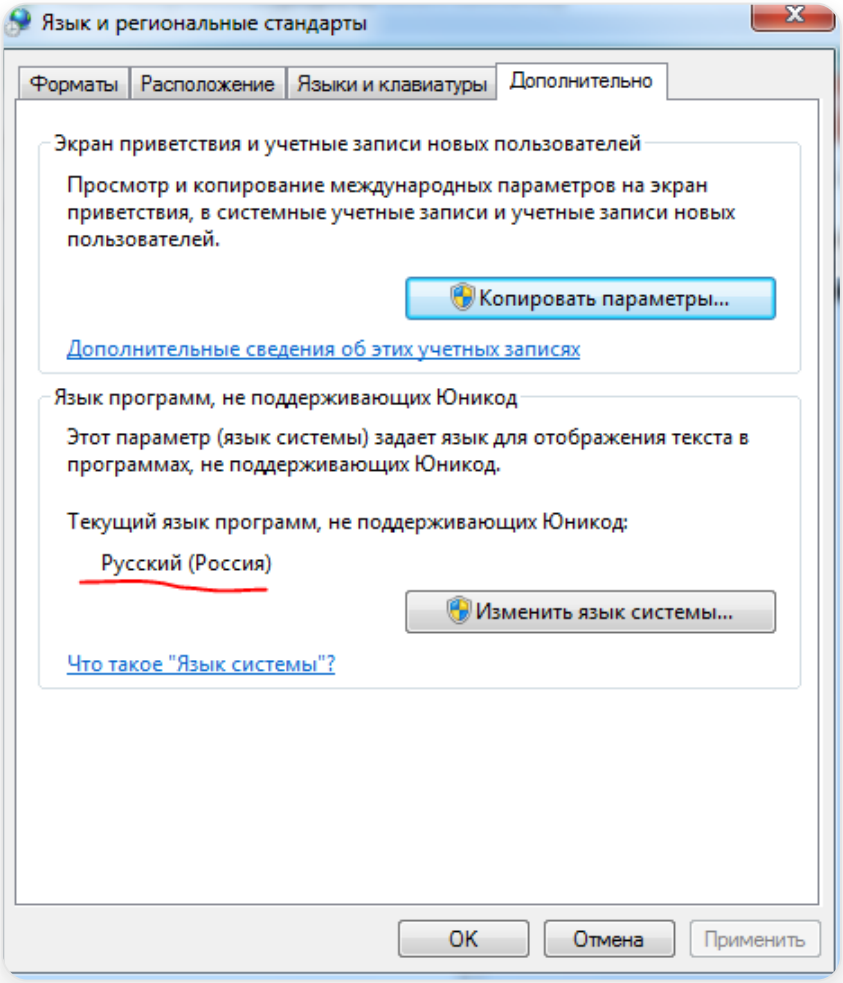
Как выглядит ошибка:



Решение:

1. Нужно установить русский языковой пакет. Скачать можно по ссылке.

2. В настройках операционной системы в языковых параметрах на вкладке **Дополнительно** выставить **Язык программ, не поддерживающих юникод** - **русски**й.


Язык и региональные стандарты
Форматы
Расположение
Языки и клавиатуры
Дополнительно
Экран приветствия и учетные записи новых пользователей
Просмотр и копирование международных параметров на экран приветствия, в системные учетные записи и учетные записи новых пользователей.
Копировать параметры...
Дополнительные сведения об этих учетных записях
Язык программ, не поддерживающих Юникод
Этот параметр (язык системы) задает язык для отображения текста в программах, не поддерживающих Юникод.
Текущий язык программ, не поддерживающих Юникод:
Русский (Россия)
Изменить язык системы...
Что такое "Язык системы"?
OK
Отмена
Применить

Открыть статью на сайте

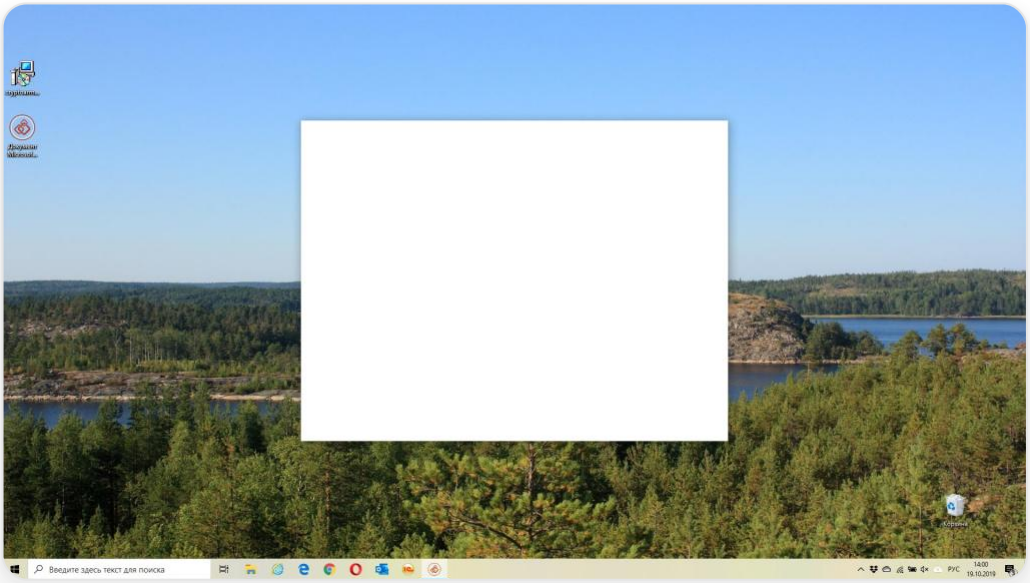
Не запускается КриптоАРМ ГОСТ на Windows или запускается, но висит белым окном

Архив. КриптоАРМ ГОСТ.

Текст ошибки:

КриптоАРМ ГОСТ не запускается, КриптоАРМ ГОСТ завис белым окном

Как выглядит ошибка:



Решение:

1. Причиной может быть конфликт криптопровайдеров. Проверьте, установлены ли у вас другие криптопровайдеры, если установлен еще и VipNet CSP, помимо КриптоПро CSP, то в настройках VipNet CSP на вкладке **Дополнительно** необходимо выключить настройку **Поддержка работы ViPNet CSP через Microsoft CryptoAP**I.

2. Переустановите КриптоПро CSP, если он устаревший, то обновите его сборку. В рамках версии обновление позволительно, лицензия остается действующей. При переходе с версии КриптоПро CSP 4 до КриптоПро CSP 5 понадобится обновление лицензии за доплату.

3. Удалите КриптоАРМ ГОСТ, удалите папку .Trusted в каталоге пользователя, установите снова. Скачать актуальную сборку можно здесь.

4. Включите консольный режим, выполните запуск программы и пришлите в техподдержку на support@trusted.ru скриншот вкладки **Console**.

Открыть статью на сайте

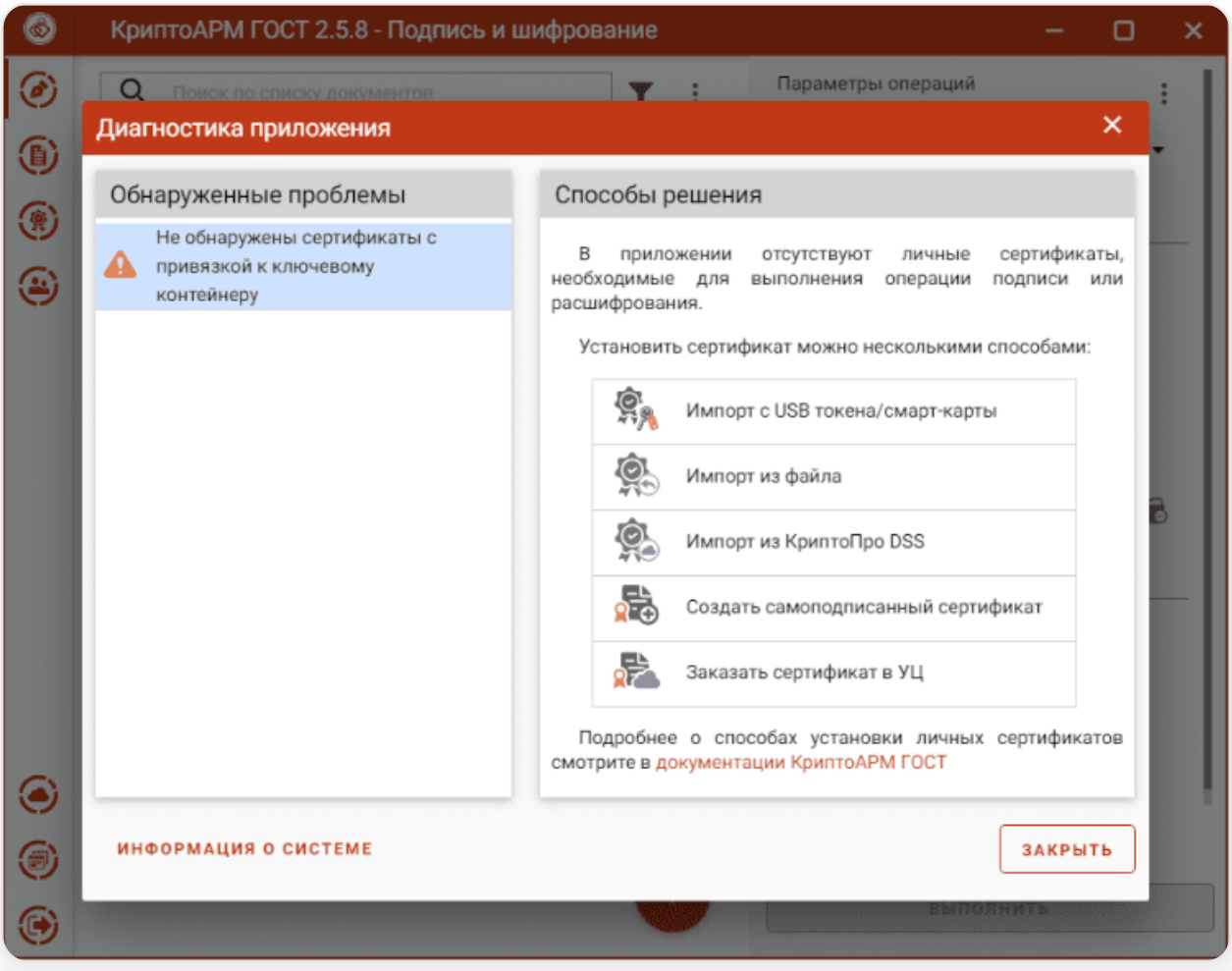
Не обнаружены сертификаты с привязкой к ключевому контейнеру

Архив. КриптоАРМ ГОСТ.

Текст ошибки:

Не обнаружены сертификаты с привязкой к ключевому контейнеру

Как выглядит ошибка:



Решение:

Добавить личный сертификат можно несколькими способами:

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

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

Открыть статью на сайте

Не удалось получить сертификат сервиса при открытии КриптоАРМ ГОСТ по ссылке с внешнего сервиса

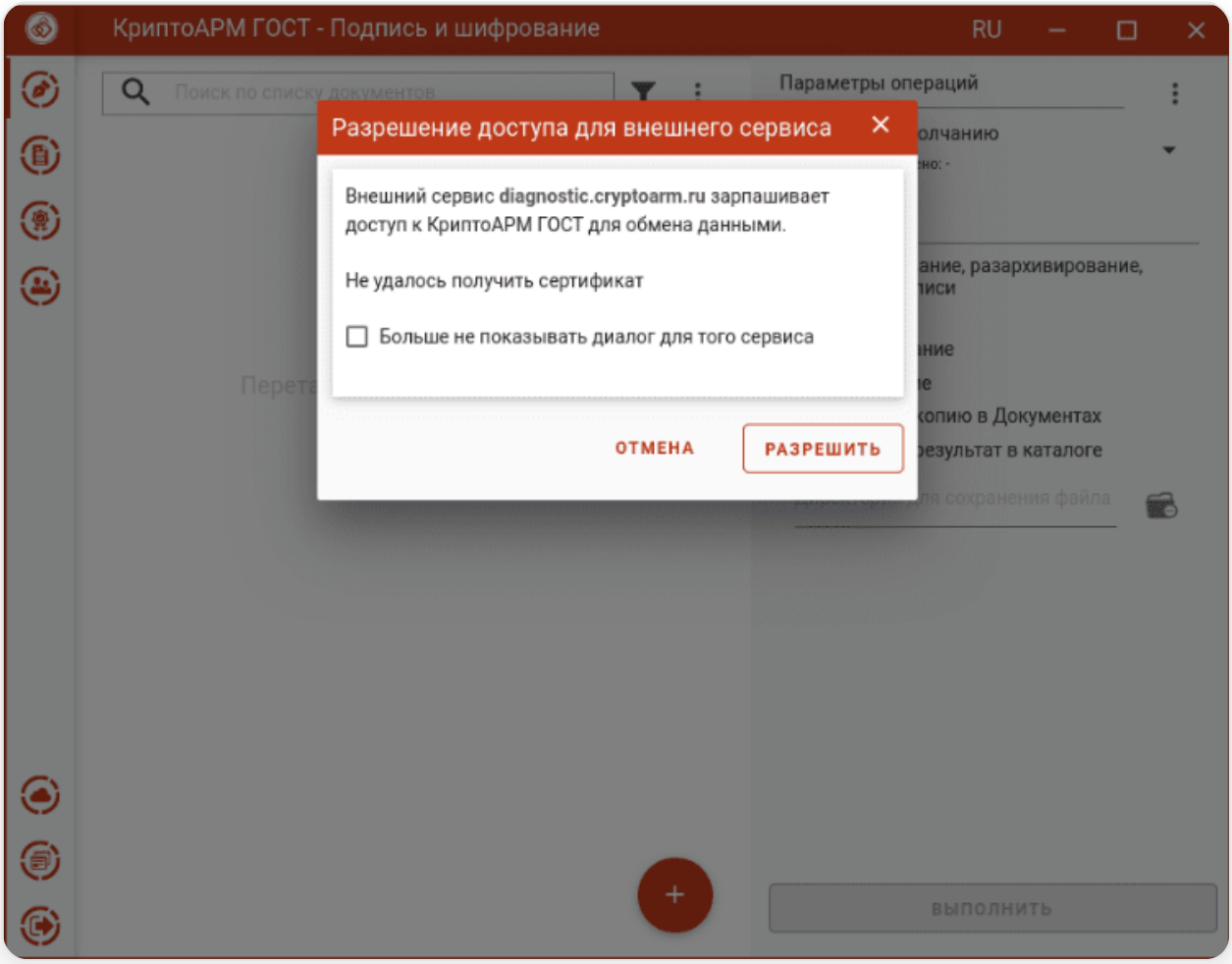
Архив. КриптоАРМ ГОСТ.

Текст ошибки:

Внешний сервис diagnostic.cryptoarm.ru запрашивает доступ к КриптоАРМ ГОСТ для обмена данными
Не удалось получить сертификат

Как выглядит ошибка:

Для КриптоПРМ ГОСТ 2.5



Решение:

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

Открыть статью на сайте

Сертификат недействительный

Архив. КриптоАРМ ГОСТ.

Текст ошибки:

Сертификат недействителен. Статус сертификата недействителен. Цепочка недействительна. Красный статус у сертификата в КриптоАРМ ГОСТ.

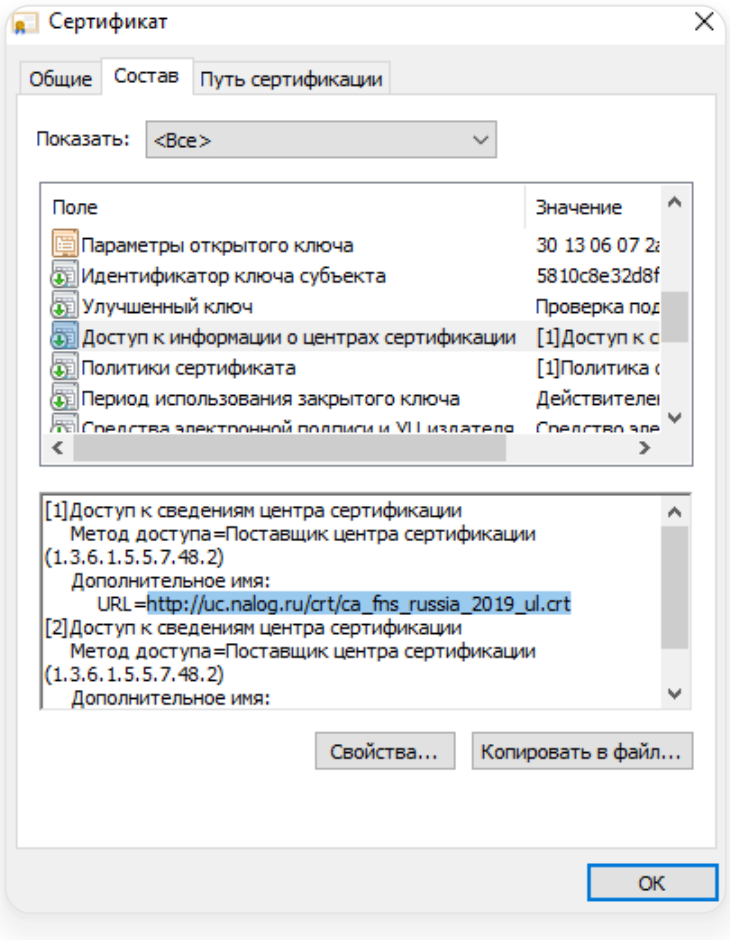
Решение:

1. Сертификат может считаться не действительным, если **не построена цепочка сертификации**.

Нужно установить в хранилище сертификатов корневой сертификат. Если статус сертификата не изменился, то нужно импортировать все промежуточные сертификаты. Если после установки корневого и промежуточных сертификатов статус сертификата не изменился, то нужно импортировать еще список отзыва.

Примечание: Для получения корневого и промежуточного сертификата обратитесь в Удостоверяющий центр, который выпустил сертификат.

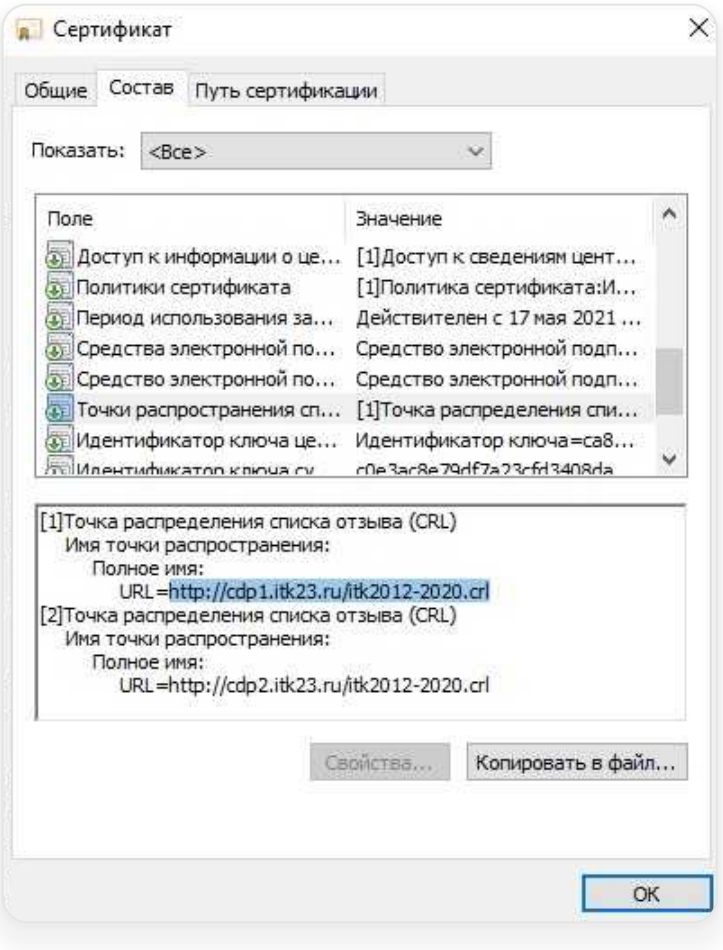
На операционной системе Windows открыть сертификат в хранилище **Сертификаты** - **Личные**. На вкладке **Состав** выберите строку **Доступ к информации о центрах сертификации**. Скопируйте ссылку для скачивания сертификата (это ссылка с окончанием **crt** или **cer**). Скачайте сертификат УЦ через любой браузер. Установите сертификат в хранилище корневых или промежуточных сертификатов, в зависимости от того, какой сертификат был скачан.



2. Цепочка сертификации построена, но **не загружен список отозванных сертификатов**.

Примечание: Для получения списка отозванных сертификатов обратитесь в Удостоверяющий центр, который выпустил сертификат.

На операционной системе Windows открыть сертификат в хранилище **Сертификаты** - **Личные** на вкладке **Состав**. Выберите в составе строку **Точка распределения списка отзыва** (CRL). Скопируйте ссылку для скачивания списка отзыва (это ссылка с окончанием **crl**).



Установка промежуточных, корневых сертификатов и списков отзыва описана в статье.