

424000, РМЭ, г. Йошкар-Ола, ул. Карла Маркса, д. 109Б

Телефоны: 8 (495) 532-11-08

8 (800) 222-11-08

8 (8362) 33-70-50

<https://trusted.ru>

E-mail: info@trusted.ru



127018, Москва, Сущёвский Вал, 18

Телефон: 8 (495) 995-48-20

<https://CryptoPro.ru>

E-mail: info@CryptoPro.ru



Средство

КриптоПро CSP версии 5.0 R2 КС1

Криптографической

Исполнение 1-КриптоАРМ

Защиты

Информации

Руководство пользователя

ЖТЯИ.00101-12 92 01

Листов 120

2021 г

Содержание

1	Общие сведения о программном продукте	4
1.1	Функциональность версии.....	4
1.2	Поддерживаемые криптопровайдеры	5
1.3	Лицензия на программный продукт	5
2	Установка и настройка приложения КриптоАРМ ГОСТ.....	6
2.1	Установка программного продукта.....	6
2.1.1	Установка на платформу Microsoft Windows.....	6
2.1.2	Установка на платформу Linux	6
2.1.3	Установка на платформу OS X	6
2.2	Установка лицензии на программный продукт	6
2.3	Установка лицензий на модули КриптоПро TSP Client 2.0 или КриптоПро OCSP Client 2.0	8
2.3.1	Установка лицензии на модуль TSP	8
2.3.2	Установка лицензии на модуль OCSP.....	10
3	Графический пользовательский интерфейс приложения	12
3.1	Начало работы с приложением.....	12
3.2	Создание подписи	13
3.3	Создание подписи со штампом времени (TSP).....	20
3.4	Создание усовершенствованной подписи	23
3.5	Проверка электронной подписи	26
3.6	Добавление подписи	30
3.7	Архивирование файлов.....	33
3.8	Шифрование файлов	36
3.9	Снятие электронной подписи.....	42
3.10	Расшифрование файлов	44
3.11	Прямые групповые операции (подпись, архивирование, шифрование)	46
3.11.1	Подпись и архивирование.....	46
3.11.2	Подпись и шифрование	53
3.11.3	Архивирование и шифрование	59
3.11.4	Подпись, архивирование и шифрование	64
3.12	Обратные групповые операции (расшифрование, разархивирование, снятие подписи)	70
3.12.1	Расшифрование и разархивирование файлов	70
3.12.2	Расшифрование и снятие подписи с файлов	72
3.12.3	Разархивирование и снятие подписи	73
3.12.4	Расшифрование, разархивирование и снятие подписи	75
3.13	Управление списком файлов для выполнения операций	76
3.14	Управление параметрами операции.....	81
3.15	Документы	85
3.16	Сертификаты	90

3.16.1	Импорт сертификата из файла	92
3.16.2	Экспорт сертификата в файл.....	96
3.16.3	Удаление сертификата	98
3.16.4	Создание запроса на сертификат.....	99
3.16.5	Создание самоподписанного сертификата	103
3.16.6	Списки отзыва сертификатов (СОС)	105
3.16.7	Ключевые контейнеры.....	107
3.16.8	Поиск сертификата	109
3.17	Контакты	110
3.18	О программе.....	115
3.18.1	О программе	116
3.18.2	Журнал операций.....	116

Аннотация

Настоящее руководство содержит инструкцию по использованию СКЗИ КристоПро CSP версия 5.0 R2 KC1 исполнение 1-КристоАРМ (далее по тексту — КристоАРМ ГОСТ).

Инструкции администратора безопасности и пользователя различных автоматизированных систем, использующих СКЗИ, должны разрабатываться с учетом требований настоящего документа.

Установка, настройка и использование СКЗИ КристоПро CSP версия 5.0 R2 KC1 исполнение 1-Base, входящего в комплект поставки, должна осуществляться в соответствии с требованиями и рекомендациями эксплуатационной документации на СКЗИ (ЖТЯИ.00101-02).

1 Общие сведения о программном продукте

КристоАРМ ГОСТ - это универсальное приложение с графическим пользовательским интерфейсом для выполнения операций по созданию и проверке электронной подписи файлов, шифрования и расшифрования, управления сертификатами, размещенных в хранилищах криптопровайдера КристоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

Приложение КристоАРМ ГОСТ является кроссплатформенным, и представлено различными установочными дистрибутивами под платформы: Microsoft Windows, Linux, OSX. На каждой из платформ реализована поддержка российских криптографических стандартов посредством использования криптопровайдера КристоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

В приложении поддерживается работа с ключевыми носителями Рутокен и JaCarta через криптопровайдер КристоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

1.1 Функциональность версии

Приложение текущей версии рассчитано на выполнение операций:

Электронная подпись	<ul style="list-style-type: none">— электронная подпись файлов размером до 2 Гб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память;— Проверка ЭП размером до 2 Гб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память;— добавление электронной подписи к уже существующим (функция создания соподписи) размером до 2 Гб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память;— создание как присоединенной, так и отдельной электронной подписи;— создание подписи со штампом времени на подпись и подписываемые данные;— создание усовершенствованной подписи.
Шифрование	<ul style="list-style-type: none">— шифрование и расшифрование файлов размером до 2 Гб на

		поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память;
		– удаление исходного файла после шифрования;
		– шифрование данных по стандарту PKCS#7/CMS.
Управление сертификатами и ключами		– отображение сертификатов и привязанных к ним ключей ЭП относительно хранилищ криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base;
		– проверка корректности выбранного сертификата с построением цепочки доверия и скачиванием актуального списка отзыва;
		– хранение ключей ЭП на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.) при условии использования криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base;
		– создание запросов на сертификат;
		– импорт сертификатов с привязкой к ключу ЭП;
		– экспорт сертификатов;
		– удаление сертификатов.
Просмотр и управление журналом операций	–	отображение результатов операций, которые производились в приложении.
Работа с файлами в каталоге Документы	–	сохранение всех результатов выполнения операций с файлами в централизованном каталоге Документы

1.2 Поддерживаемые криптопровайдеры

В приложении осуществляется поддержка криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

1.3 Лицензия на программный продукт

При первой установке приложения активируется временная лицензия сроком на 14 дней. После истечения ознакомительного периода для полноценной работы приложения требуется приобретение и установка лицензии. Без установки лицензии на операции доступа к ключу ЭП при операциях подписи и расшифрования будут наложены ограничения.

Для приобретения лицензии на программный продукт КриптоАРМ ГОСТ можно обратиться в компанию ООО «Цифровые технологии» или ООО «КРИПТО-ПРО».

2 Установка и настройка приложения КриптоАРМ ГОСТ

2.1 УСТАНОВКА ПРОГРАММНОГО ПРОДУКТА

2.1.1 УСТАНОВКА НА ПЛАТФОРМУ MICROSOFT WINDOWS

Установка приложения КриптоАРМ ГОСТ на платформу Microsoft Windows описана в «ЖТЯИ.00101-12 91 01. Руководство администратора. Windows».

Для функционирования КриптоАРМ необходим установленный версия 5.0 R2 KC1 исполнение 1-Base. Установка описана в документе ЖТЯИ.00101-02 91 02. КриптоПро CSP. Руководство администратора безопасности. Windows.

2.1.2 УСТАНОВКА НА ПЛАТФОРМУ LINUX

Установка приложения КриптоАРМ ГОСТ на операционную систему Linux описана в «ЖТЯИ.00101-12 91 02. Руководство администратора. Linux».

Для функционирования КриптоАРМ необходим установленный КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base. Установка описана в документе ЖТЯИ.00101-02 91 03. КриптоПро CSP. Руководство администратора безопасности. Linux.

2.1.3 УСТАНОВКА НА ПЛАТФОРМУ OS X

Установка приложения на платформу MacOS описана в «ЖТЯИ.00101-12 91 03. Руководство администратора. Mac OS»

Для функционирования КриптоАРМ необходим установленный КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base. Установка описана в документе ЖТЯИ.00101-02 91 07. КриптоПро CSP. Руководство администратора безопасности. Mac OS.

2.2 УСТАНОВКА ЛИЦЕНЗИИ НА ПРОГРАММНЫЙ ПРОДУКТ

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения. На открывшейся странице (Рисунок 1) нажать на кнопку **Ввод лицензии** в разделе управления лицензией КриптоАРМ ГОСТ. В результате должно появиться всплывающее окно ввода лицензии, предполагающее выполнение действия одним из двух способов (Рисунок 2): выполнение ввода копированием содержимого файла лицензии в текстовое поле и выполнение ввода с указанием файла лицензии.

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

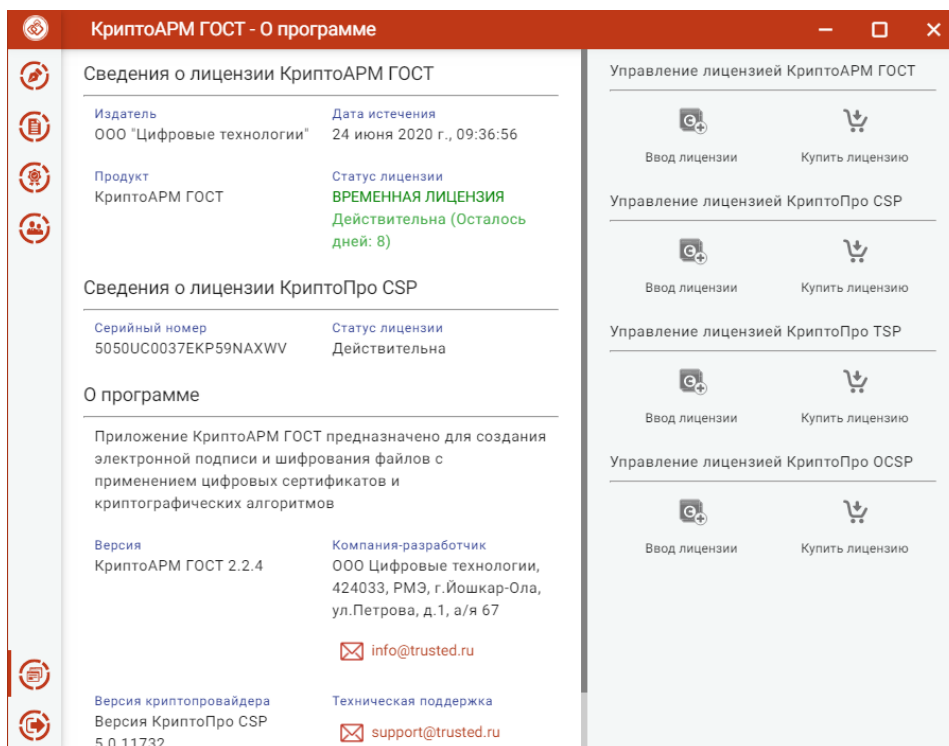


Рисунок 1. Страница ввода лицензионного ключа на программный продукт

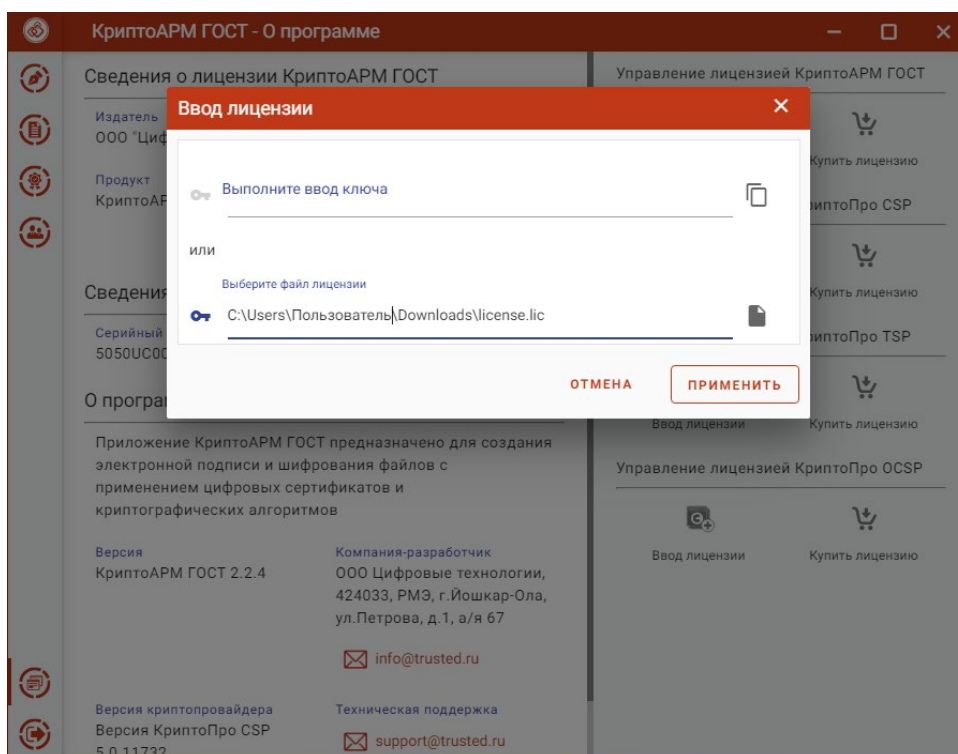


Рисунок 2. Диалоговое окно с выбором варианта ввода лицензионного ключа

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

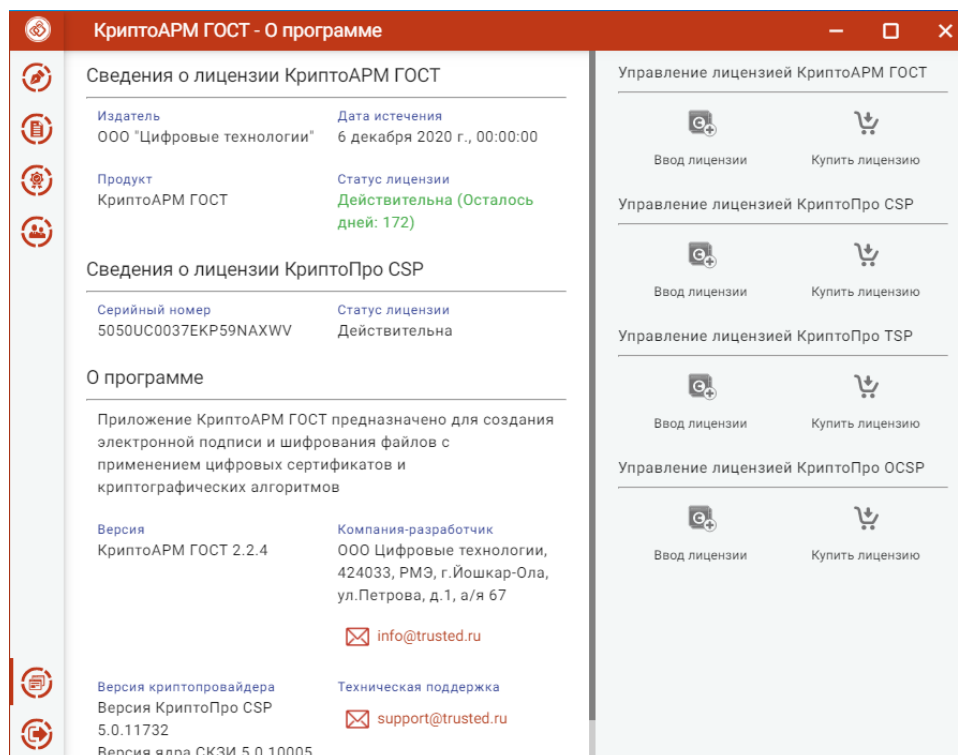


Рисунок 3. Сведения о лицензии

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

2.3 Установка лицензий на модули КриптоПро TSP Client 2.0 или КриптоПро OCSP Client 2.0

Для создания подписи со штампом времени или усовершенствованной подписи требуется установка модулей КриптоПро TSP Client 2.0 или КриптоПро OCSP Client 2.0.

2.3.1 Установка лицензии на модуль TSP

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

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения. На открывшейся странице (Рисунок 4) нажать на кнопку **Установить лицензию** в разделе управления лицензией модуля штампов времени (TSP).

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

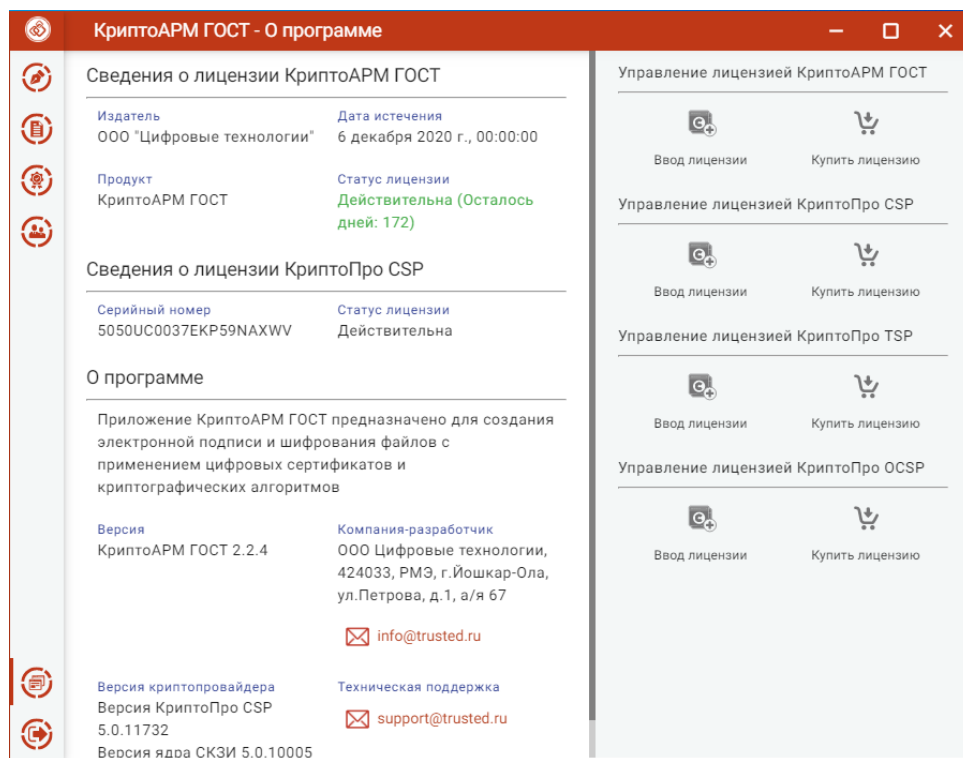


Рисунок 4. Страница ввода лицензионного ключа на модуль TSP

В результате должно появиться всплывающее окно ввода лицензии копированием содержимого файла лицензии в текстовое поле (Рисунок 5).

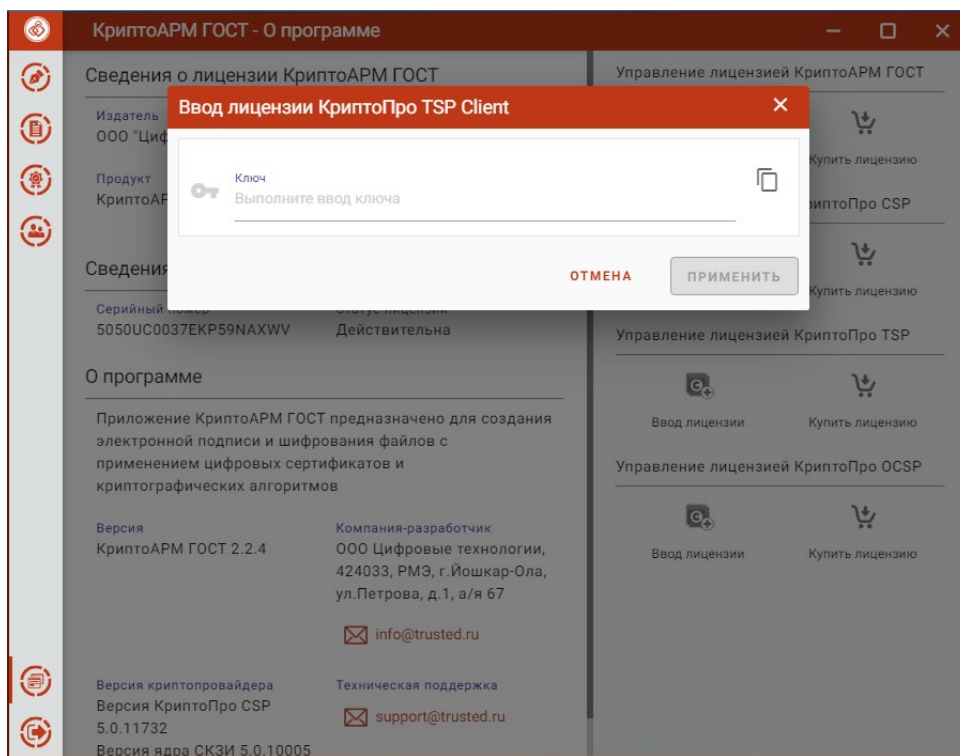


Рисунок 5. Окно ввода лицензионного ключа на модуль TSP

При успешной операции должно появиться информационное сообщение.

2.3.2 Установка лицензии на модуль OCSP

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

Для установки лицензии через пользовательский интерфейс нужно перейти на страницу **Лицензии** через пункт **О программе** главного меню приложения. На открывшейся странице (Рисунок 6) нажать на кнопку **Установить лицензию** в разделе управления лицензией модуля (OCSP).

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

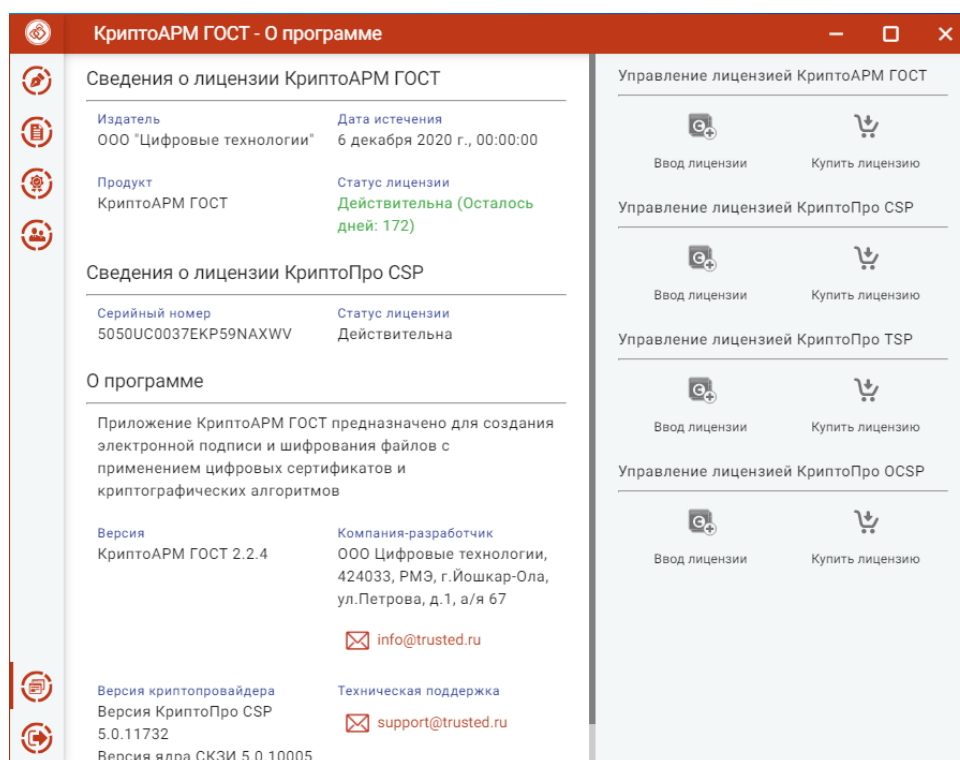


Рисунок 6. Страница ввода лицензионного ключа на модуль OCSP

В результате должно появиться всплывающее окно ввода лицензии копированием содержимого файла лицензии в текстовое поле (Рисунок 7).

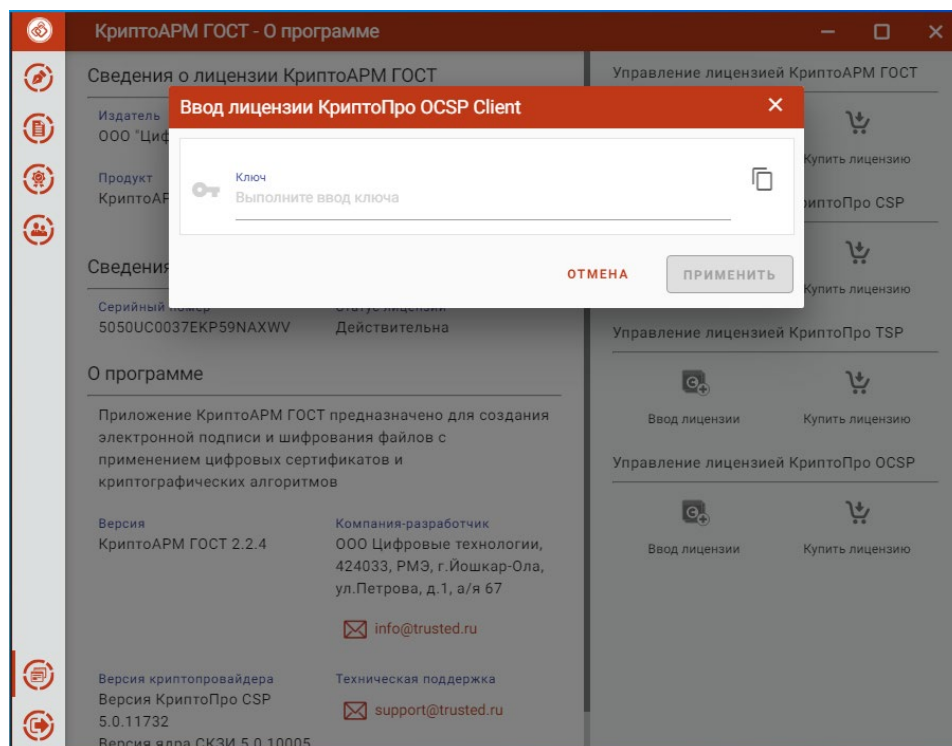


Рисунок 7. Окно ввода лицензионного ключа на модуль OSCP

При успешной операции должно появиться информационное сообщение.

3 Графический пользовательский интерфейс приложения

3.1 НАЧАЛО РАБОТЫ С ПРИЛОЖЕНИЕМ

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

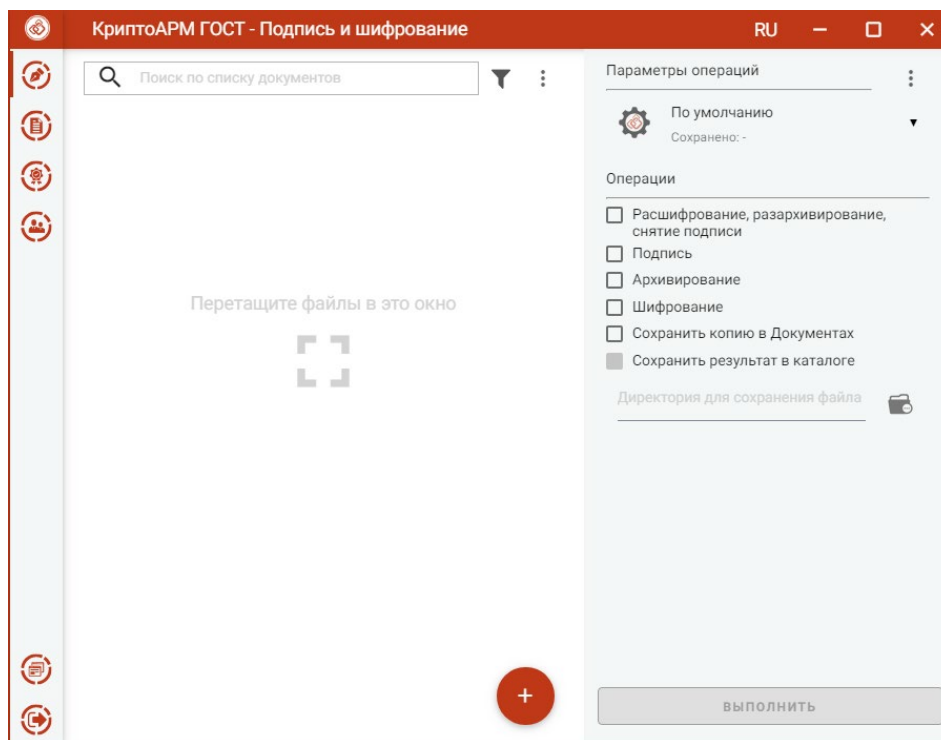


Рисунок 8. Стартовое окно приложения

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

- **Расшифрование, разархивирование, снятие подписи** – опция для выполнения обратных операций (расшифрование, разархивирование, снятие подписи). Для выполнения обратных операций не требуется установка дополнительных параметров.
- **Подпись, архивирование, шифрование** – для выполнения прямых операций (подпись, шифрование, архивирование). 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 заданных каталога.

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

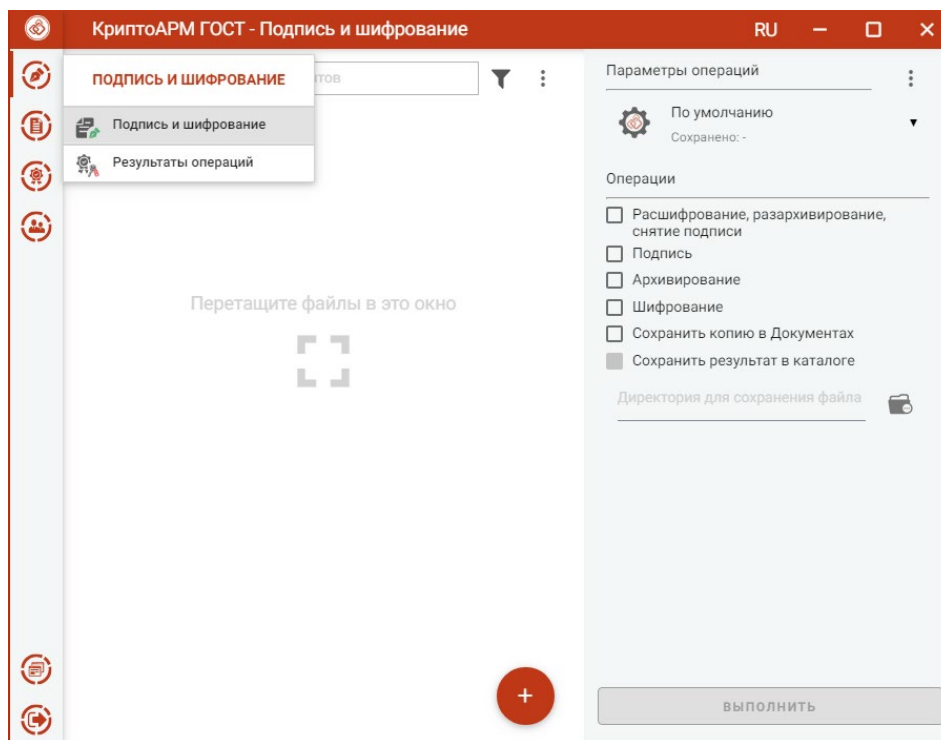


Рисунок 9. Пункт меню Подпись и шифрование с подменю

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

3.2 Создание подписи

Для подписи файлов нужно в мастере **Подписи и шифрование** выбрать подписываемые файлы, выбрать опцию **Подпись** в разделе операций, задать сертификат подписи и параметры подписи.

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

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (Рисунок 10).

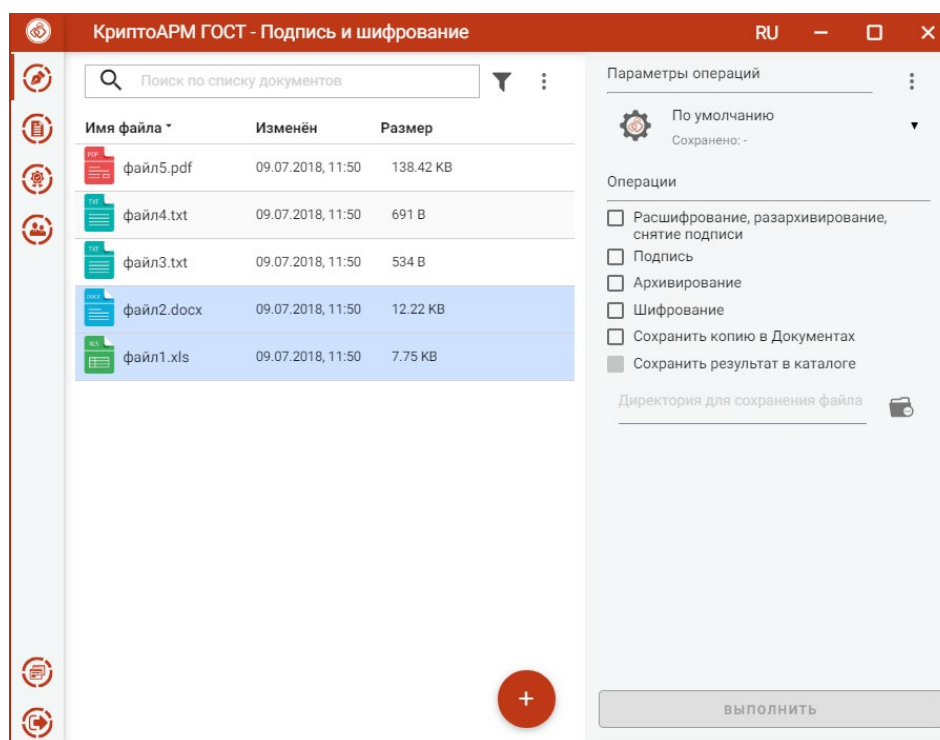


Рисунок 10. Список подписываемых файлов

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (Рисунок 11).

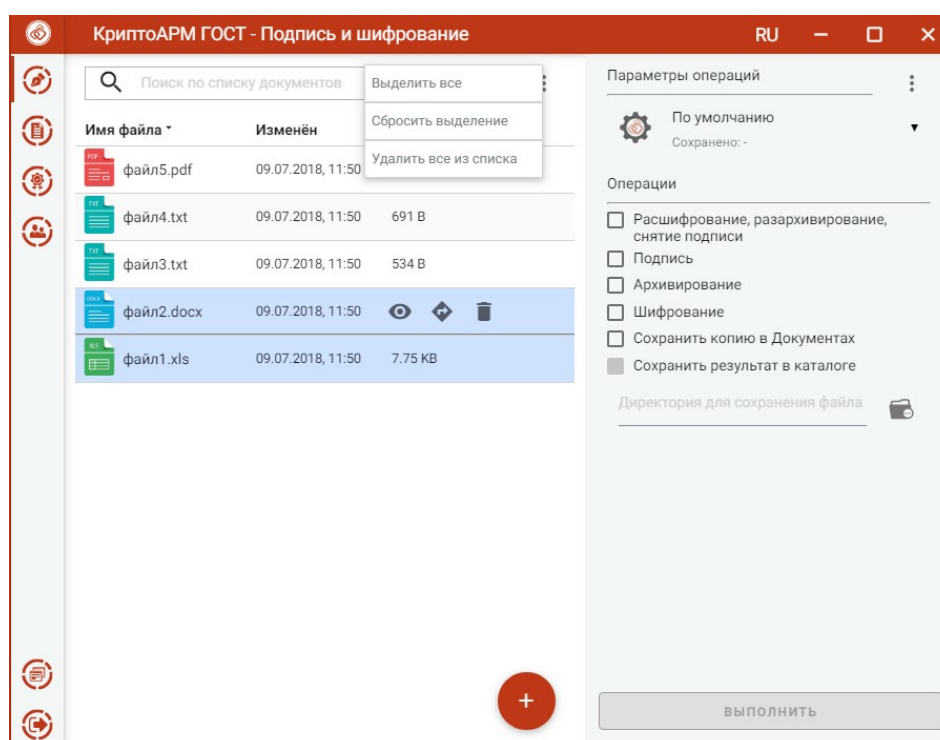


Рисунок 11. Контекстное меню управления списком файлов

УСТАНОВКА ПАРАМЕТРОВ ПОДПИСИ. Для подписи файлов в разделе **Операции** необходимо выбрать опцию **Подпись**, становятся доступны параметры подписи (Рисунок 12).

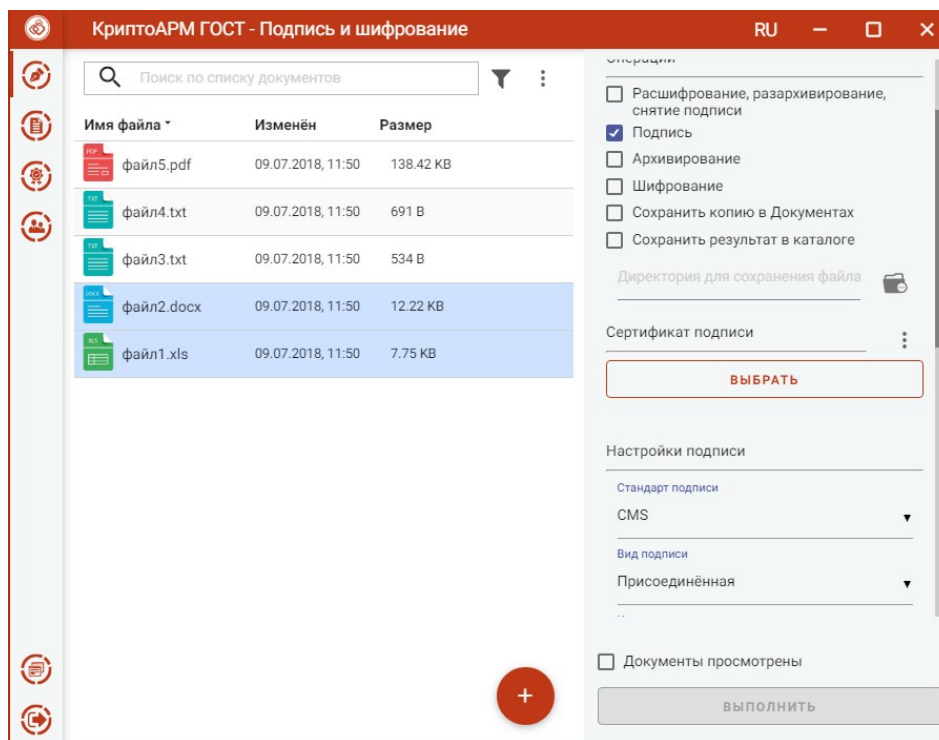


Рисунок 12. Настройка параметров подписи

В параметрах можно настроить:

- **Сертификат подписи** – сертификат с ключом ЭП.
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее о создании усовершенствованной подписи в пункте «[Создание усовершенствованной подписи](#)»). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client 2.0 и КриптоПро OCSP Client 2.0.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Добавить время подписи** - при установленном флажке в подпись сохраняется время (системное) подписи.
- **Добавлять штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.
- **Добавлять штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.

Можно задать каталог для сохранения подписанных документов, выбрав в операциях опцию **Сохранить результат в каталоге**. При установке флага становится доступно поле выбора каталога (Рисунок 13).

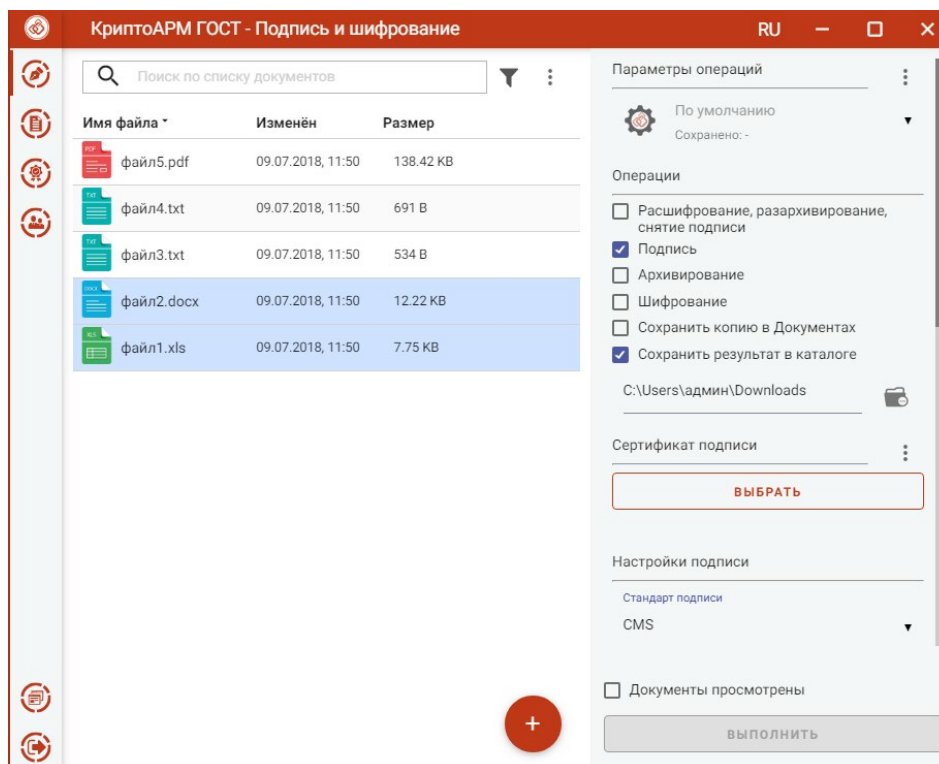


Рисунок 13. Выбор каталога для сохранения результата операции подписи

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

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге `./Trusted/CryptoARM GOST/`. 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](#)

ВЫБОР СЕРТИФИКАТА ПОДПИСИ. Для того, чтобы выполнить подпись необходимо выбрать сертификат, к которому привязан ключ ЭП. Эта операция производится нажатием кнопки **Выбрать** сертификат подписи. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи (Рисунок 14).

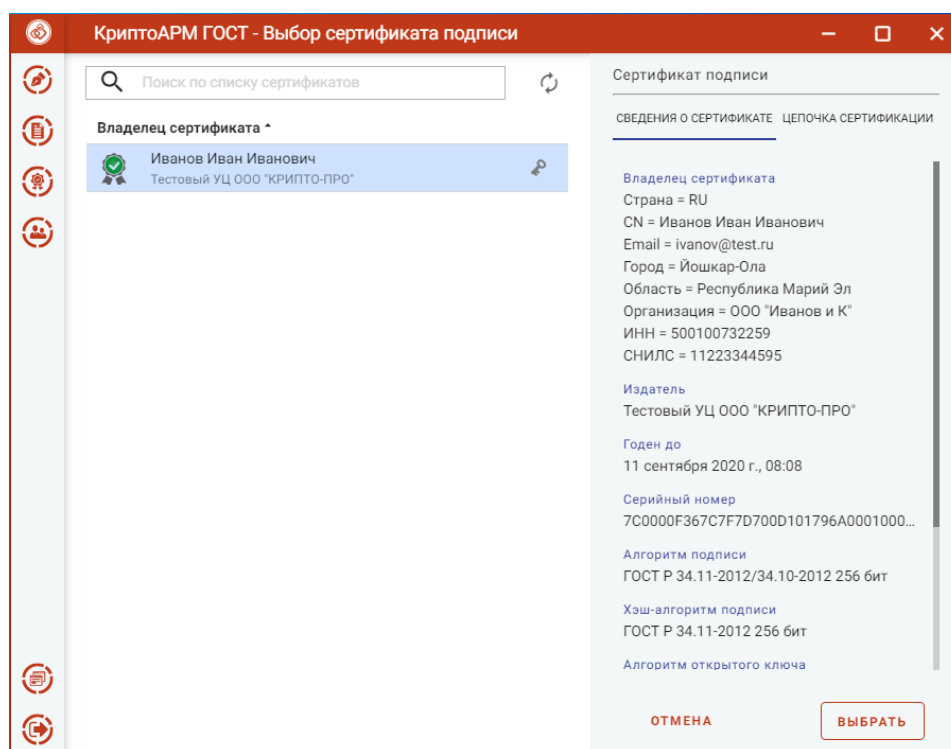


Рисунок 14. Выбор сертификата подписи

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

Сертификат подписи можно изменить с помощью контекстного меню (Рисунок 15).

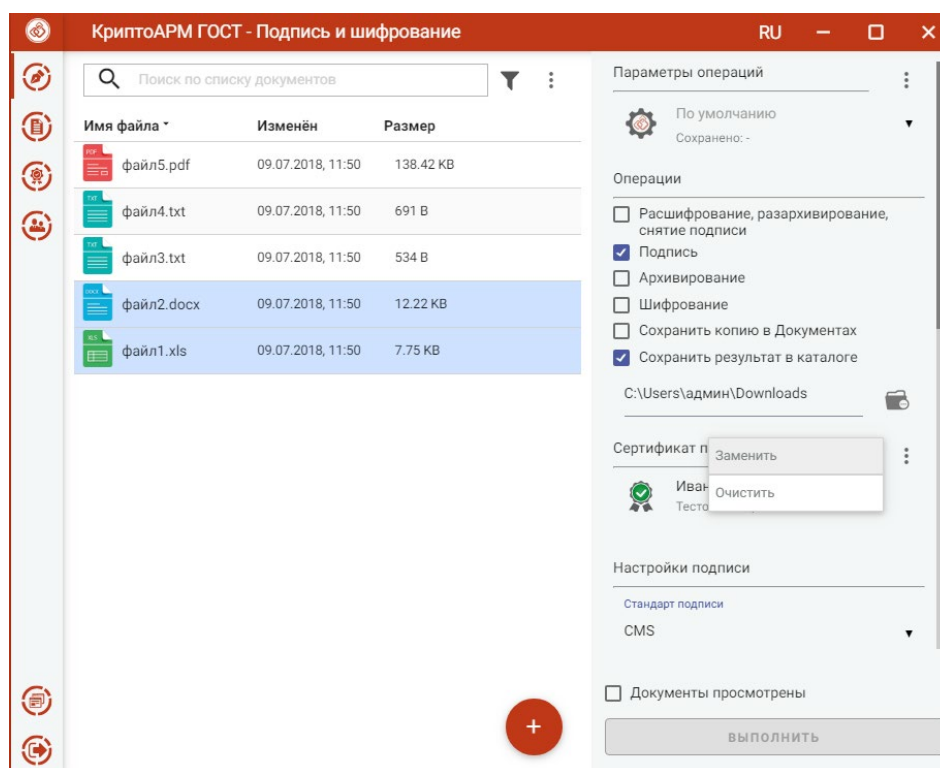


Рисунок 15. Изменение сертификата подписи

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

Подпись файлов. При условии выбора сертификата подписи, файлов для подписи и установленного флага, что документы просмотрены, в мастере становится доступной кнопка **Выполнить** (Рисунок 16). Подписать можно любые файлы, кроме зашифрованных.

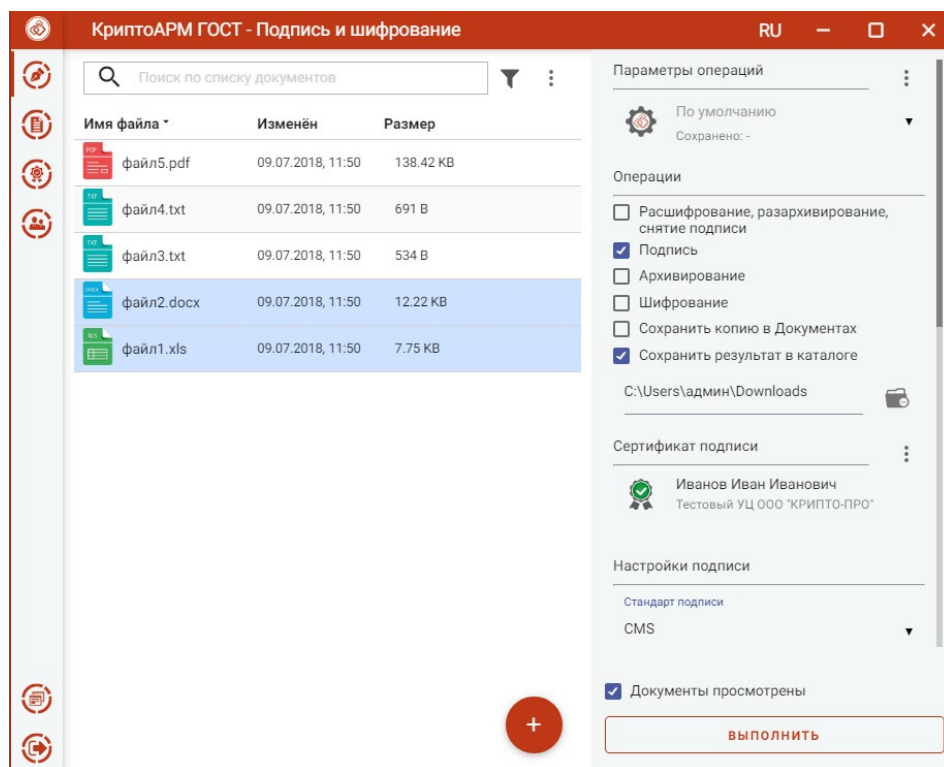


Рисунок 16. Подпись файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи. Исходные документы (оригиналы) и результаты операции подписи отображаются в отдельном мастере **Результаты операций** (Рисунок 17).

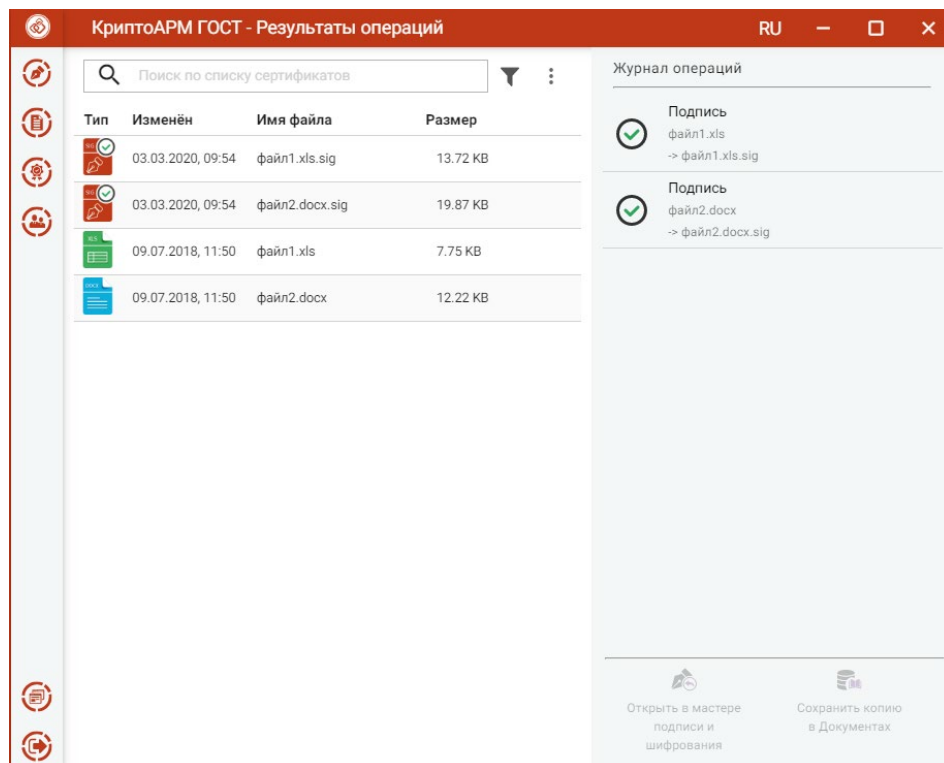


Рисунок 17. Результаты операций

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/`. Документы из данного каталога доступны в пункте меню **Документы**.

Для подписанных документов подпись проверяется автоматически.

Для просмотра информации о подписи нужно выделить один подписанный файл в списке (Рисунок 18).

Для каждого документа доступны операции (Рисунок 18):

- **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.

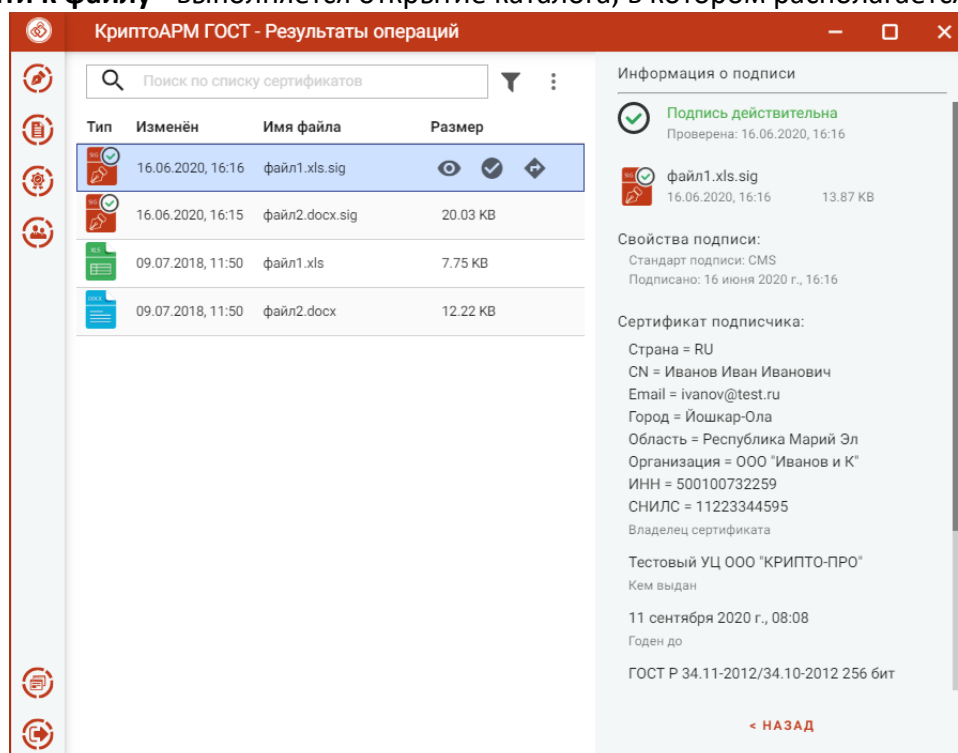


Рисунок 18. Операции для документа

Для списка документов доступно контекстное меню, позволяющее выделить файлы по типу операции (Рисунок 19).

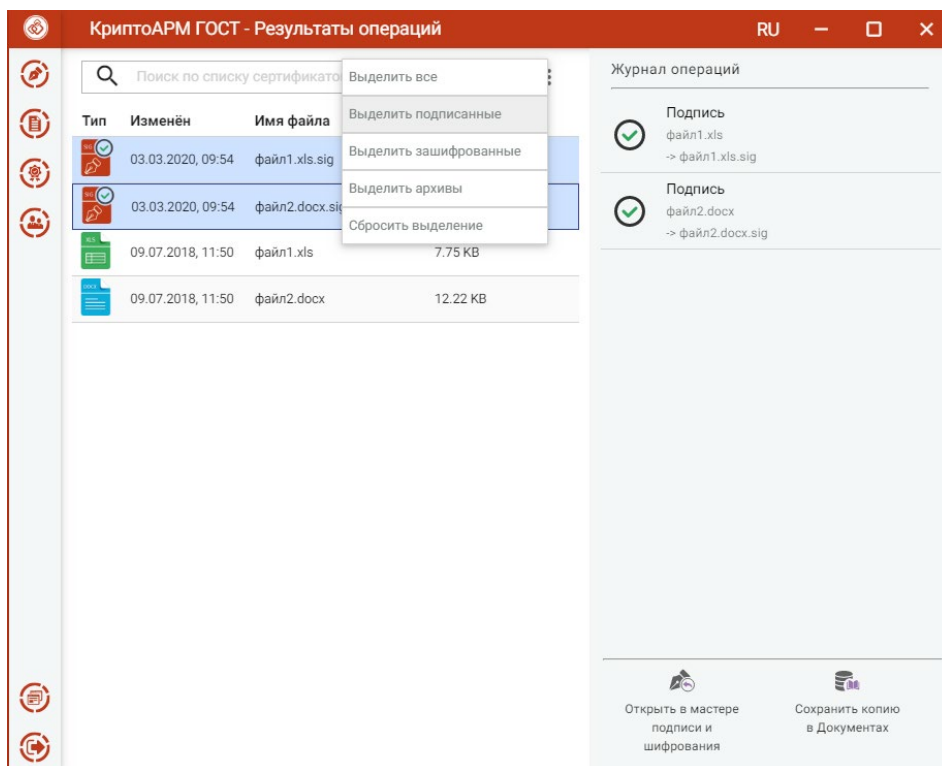


Рисунок 19. Выделение группы файлов по типу файла

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 19). 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**.

3.3 Создание подписи со штампом времени (TSP)

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

Создание подписи со штампом времени возможно только при установленном модуле КриптоПро TSP Client 2.0 и лицензии на модуль TSP.

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 (рис. 4.3.1);

- установить флаг **Добавлять штамп времени на подписываемые данные**, если требуется поставить штамп на данные (Рисунок 20);

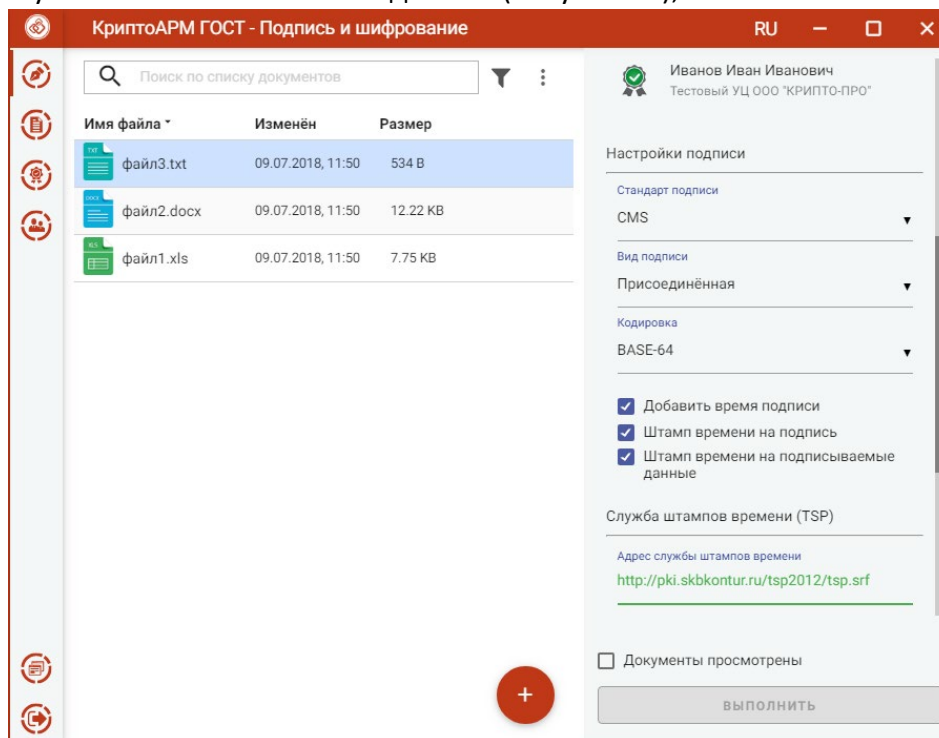


Рисунок 20. Установка флага для добавления штампа времени в подпись

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

- **Адрес службы штампов времени** - адрес службы штампов времени можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: <протокол>://<сервер>[:порт]/[путь]. В качестве протокола вы может быть указан "http" и "https".

- **Использовать настройки прокси-сервера** – если при подключении к службе TSP используется прокси-сервер, то установка флага активирует настройки прокси-сервера: **Адрес прокси-сервера, Порт, Логин, Пароль**, которые можно узнать у системного администратора.

После заполнения параметров подписи и установки флага, что файлы просмотрены перед их подписанием, становится доступна кнопка **Выполнить** (Рисунок 21).

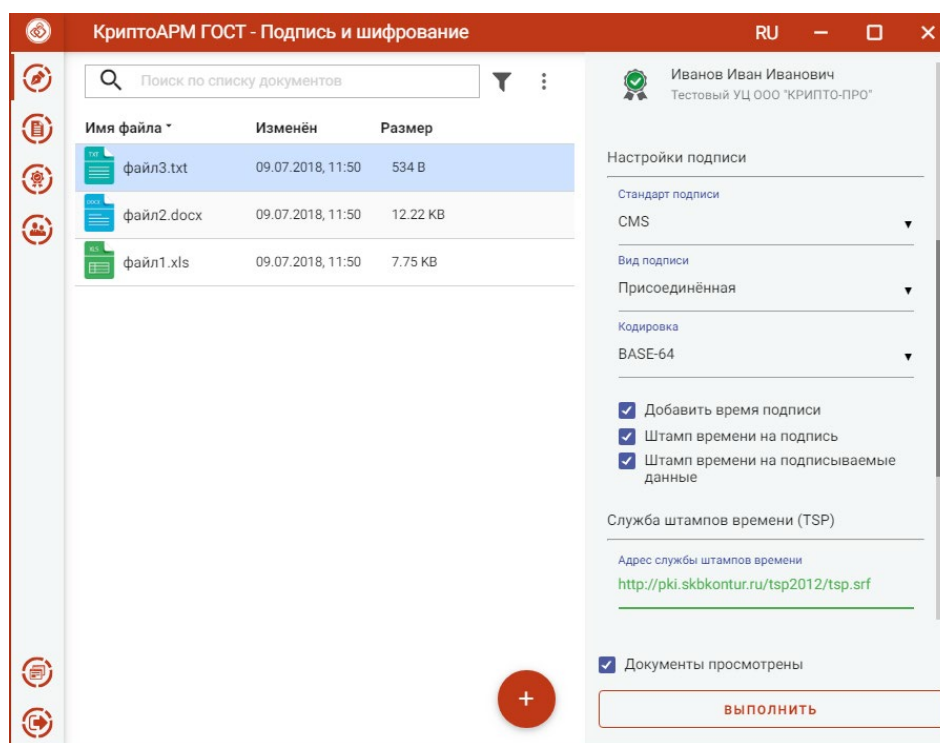


Рисунок 21. Подпись документов со штампом времени

Нажатие на кнопку **Выполнить** запускает процесс подписи. Исходные документы (оригиналы) и результаты операции подписи отображаются в отдельном мастере **Результаты операций** (Рисунок 22). Причем, после выполнения операции мастер подписи и шифрования очищается от добавленных в него файлов.

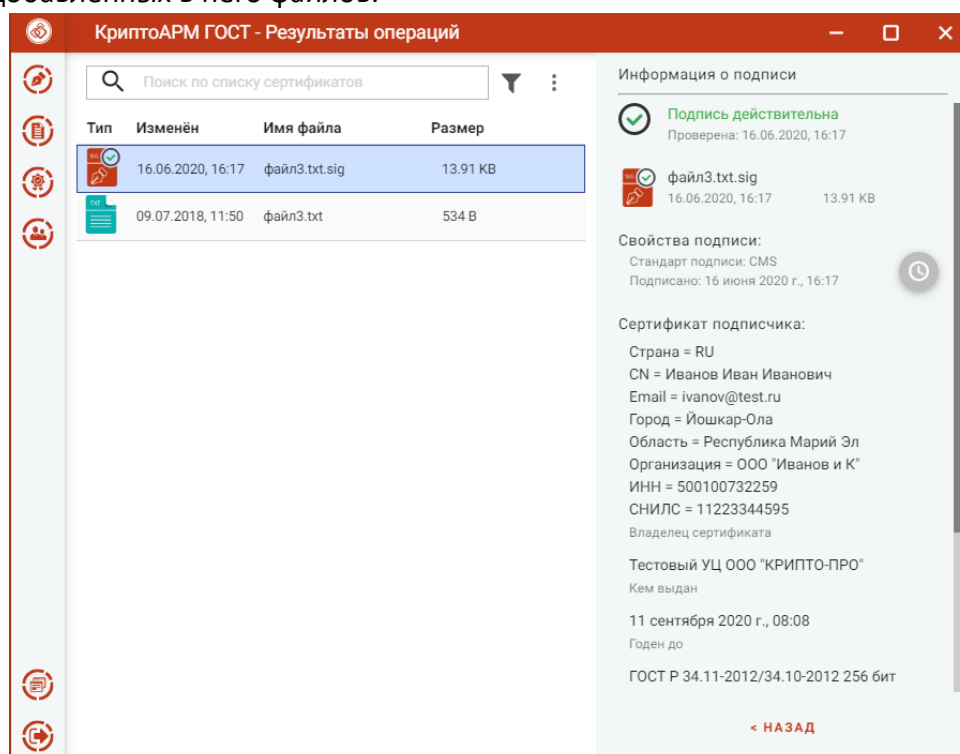


Рисунок 22. Результаты операции подписи

При просмотре информации о подписи отображается информация о штампе времени (Рисунок 23)

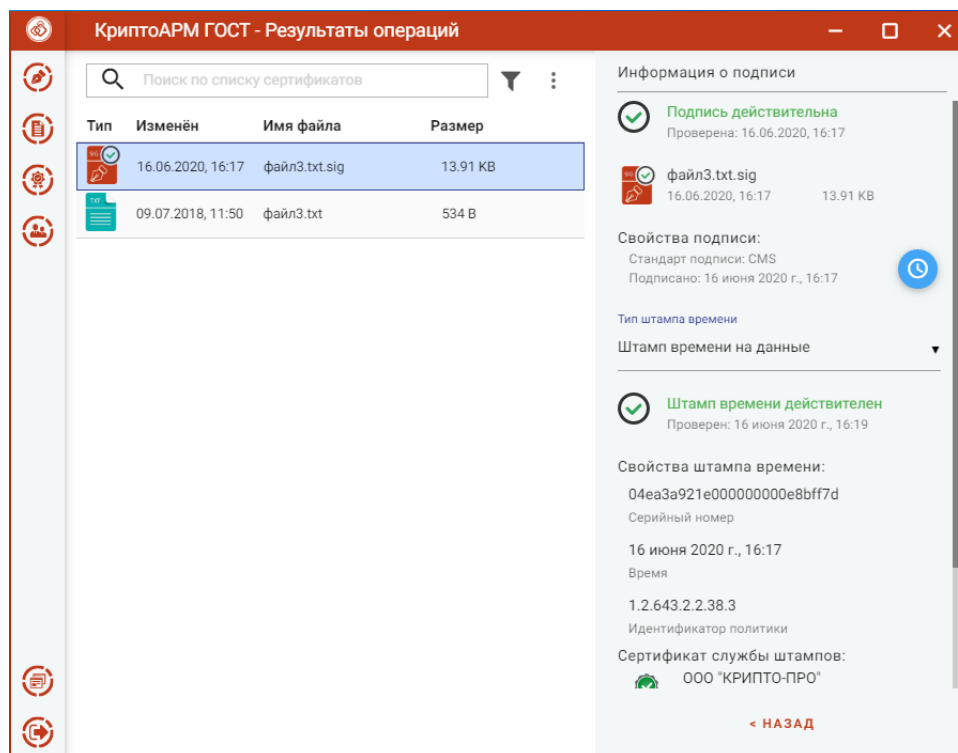


Рисунок 23. Информация о штампе времени при просмотре подписи

3.4 СОЗДАНИЕ УСОВЕРШЕНСТВОВАННОЙ ПОДПИСИ

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

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

Создание усовершенствованной подписи возможно только при установленных модулях TSP Client 2.0 и OCSP Client 2.0 и лицензий на них.

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

- Выбрать стандарт подписи **CAdES-X Type 1** (Рисунок 24);

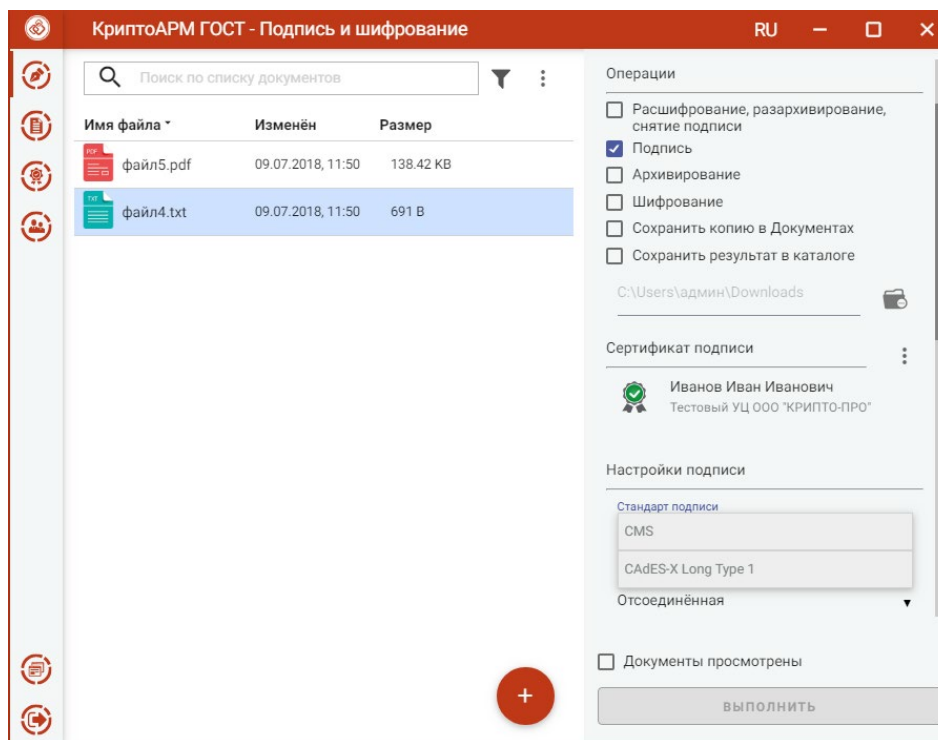


Рисунок 24. Стандарт подписи CAdES-X Type 1

- Заполнить параметры раздела **Служба штампов времени (TSP)** (Рисунок 25): **Адрес службы штампов времени**, **Использовать настройки прокси-сервера** (если при подключении к службе TSP используется прокси-сервер)

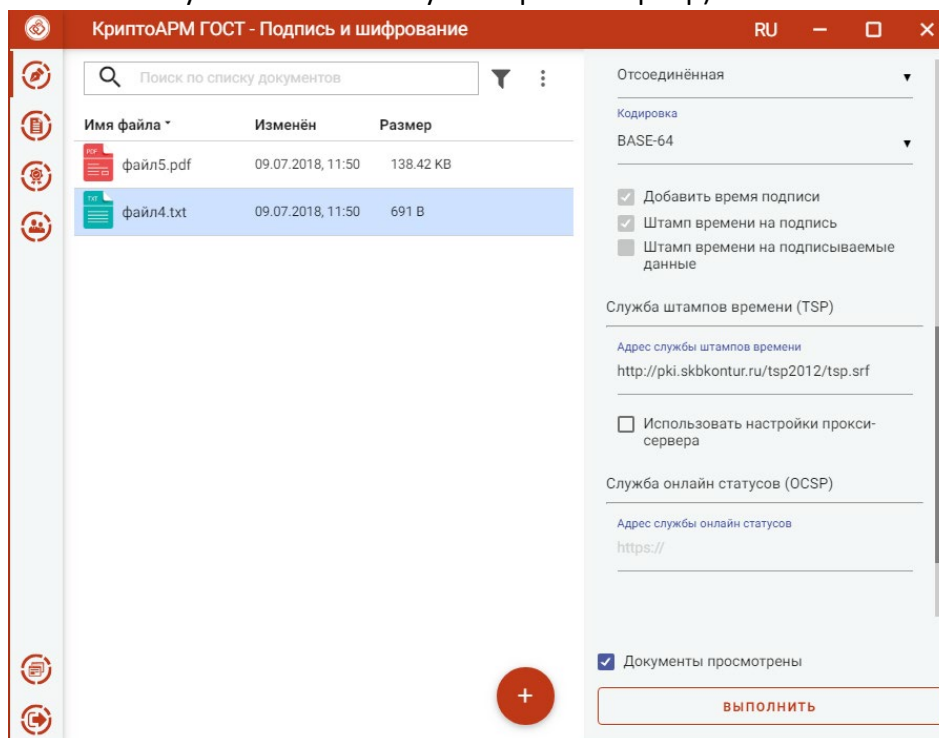


Рисунок 25. Параметры службы штампов времени

- Заполнить параметры раздела **Службы online статусов (OCSP)** (Рисунок 25): **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** (Рисунок 26).

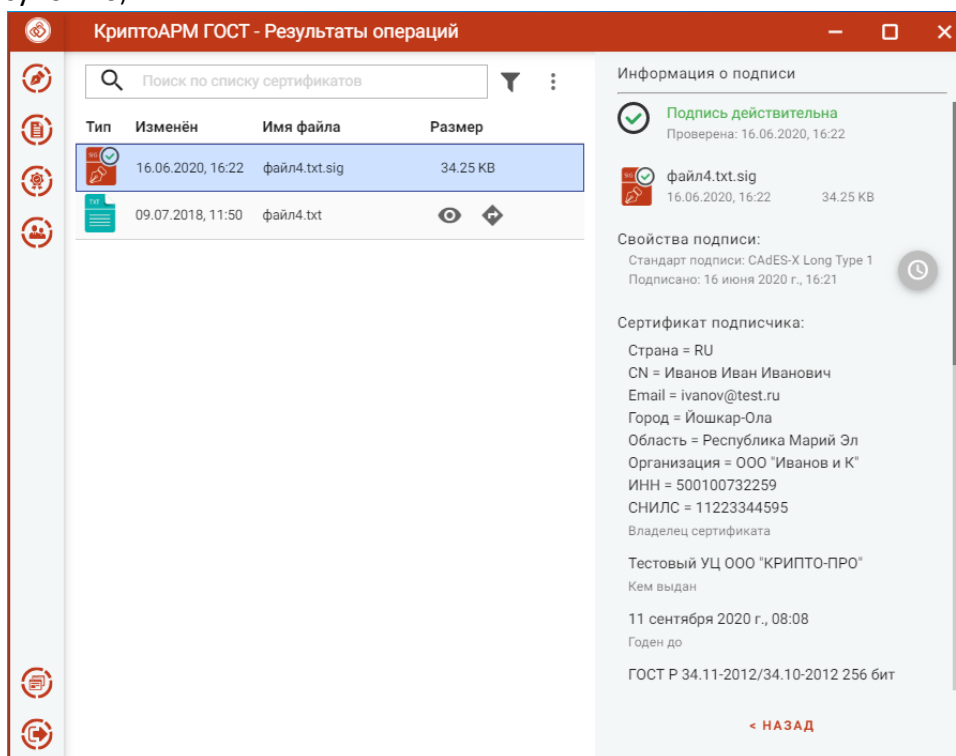


Рисунок 26. Результаты операций подписи

При просмотре информации о подписи отображается информация о OCSP ответе (Рисунок 27)

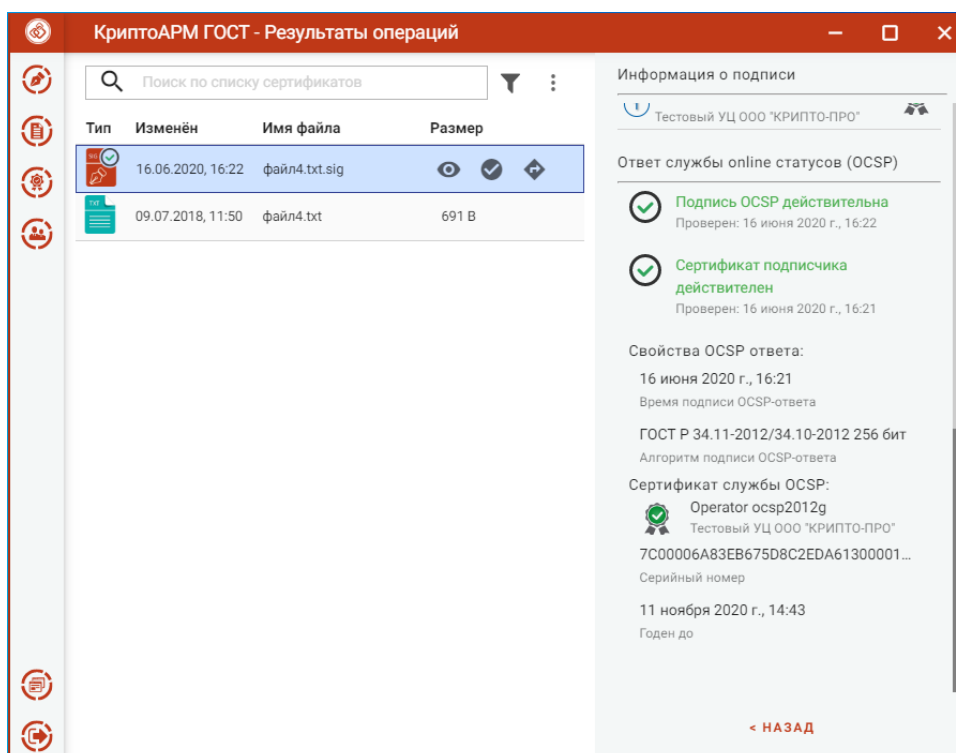


Рисунок 27. Информация об OCSP ответе при просмотре подписи

Информация о штампе времени на подпись (Рисунок 28).

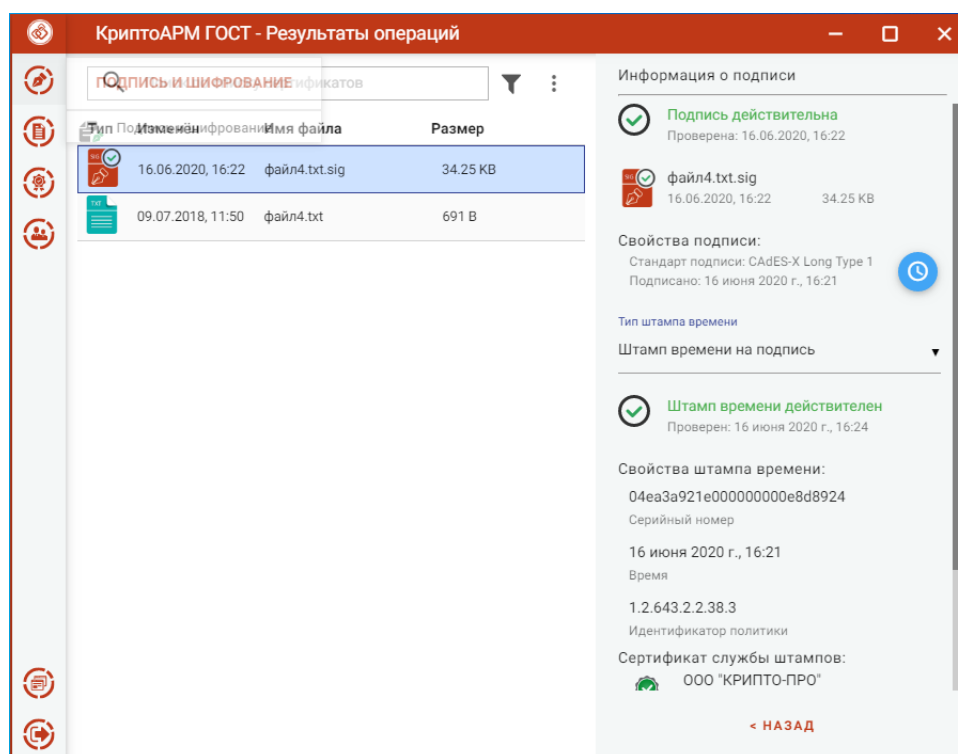


Рисунок 28. Информация об штампе времени на подпись

И информация о доказательствах подлинности (Рисунок 29).

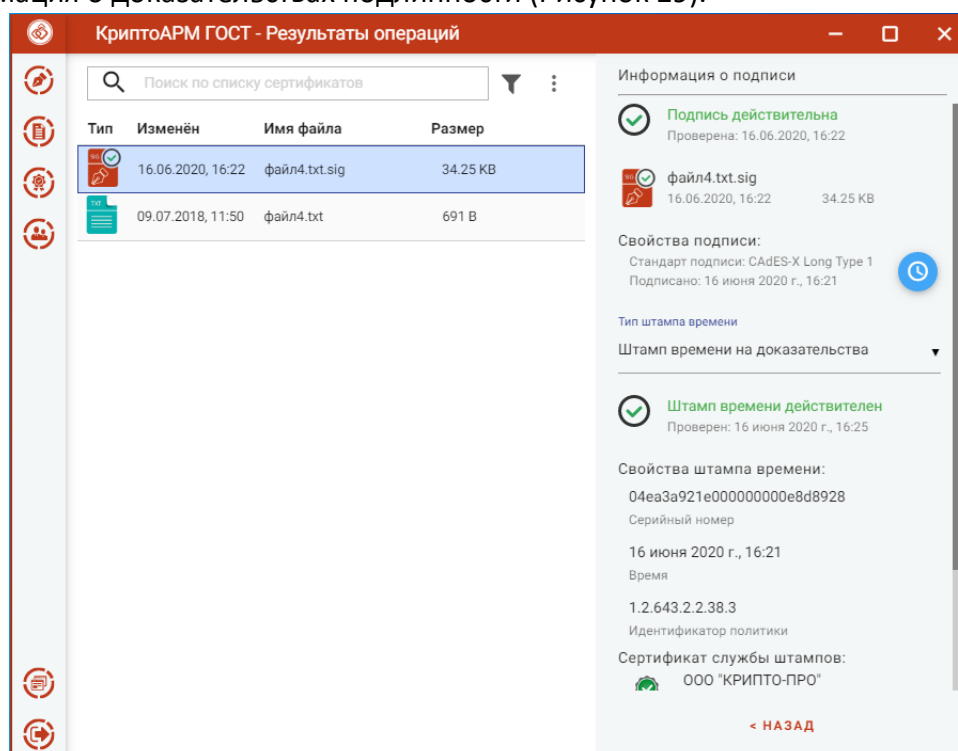


Рисунок 29. Информация о доказательствах подлинности

3.5 ПРОВЕРКА ЭЛЕКТРОННОЙ ПОДПИСИ

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 (Рисунок 30): зеленый - подпись действительна; красный - подпись недействительна.

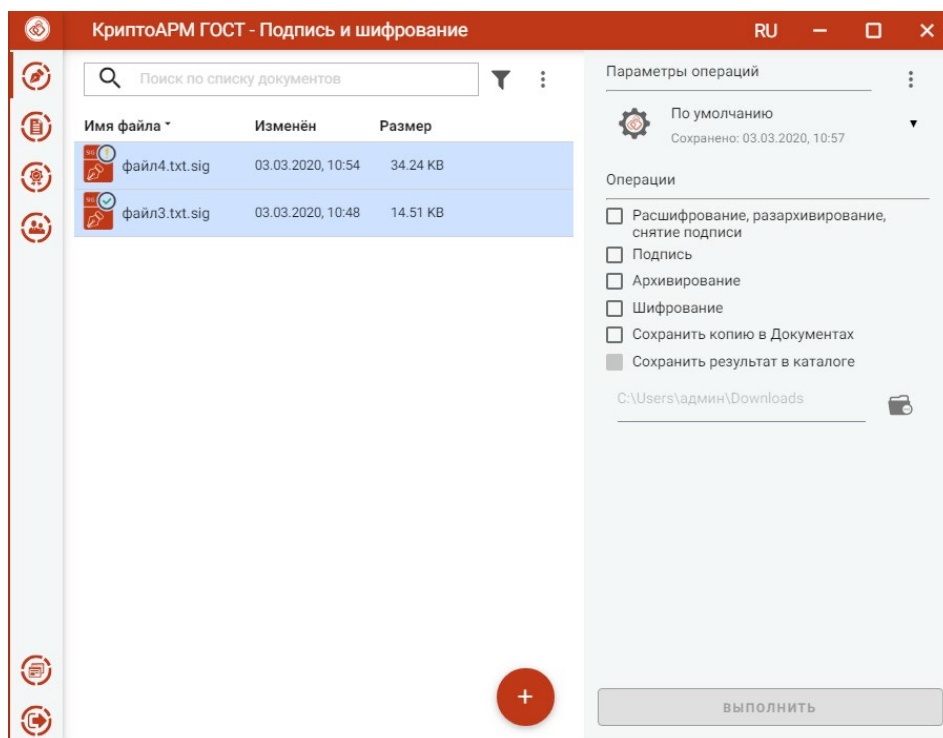


Рисунок 30. Результат проверки подписи файлов

Если при проверке отдельной 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 (Рисунок 31). Откроется окно для его выбора.

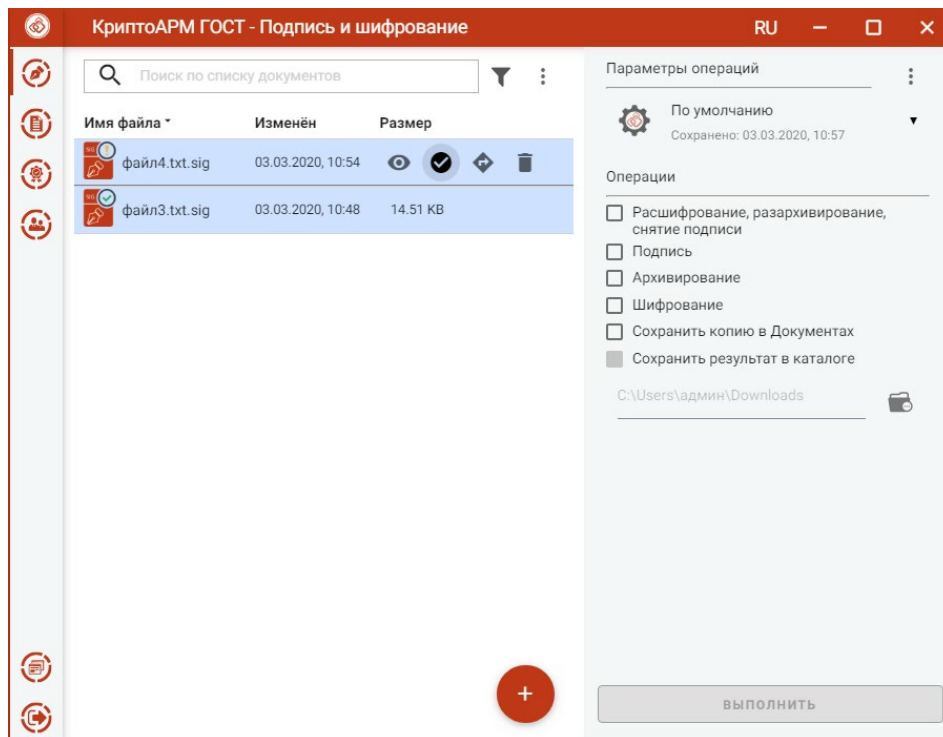


Рисунок 31. Иконка вызова проверки подписи файла

При выделении одного подписанного файла в правой области отображается информация о подписи (Рисунок 32).

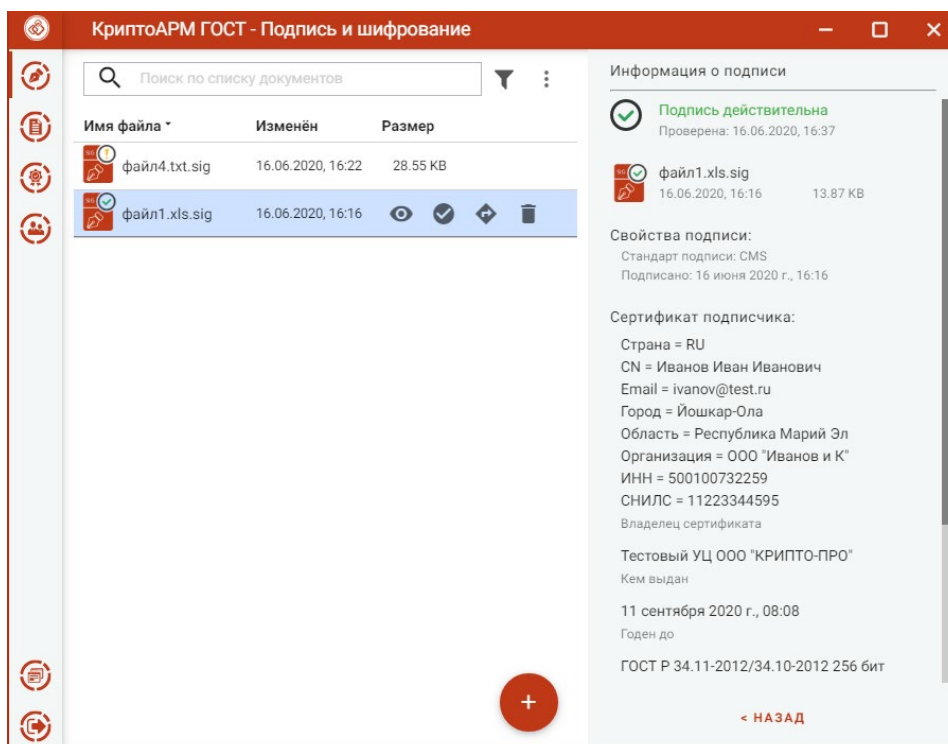


Рисунок 32. Отображение информации о подписи

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

Если документ подписан несколькими подписями (имеет соподписи), то для просмотра информации о подписи нужно в списке выбрать сертификат подписи (Рисунок 33).

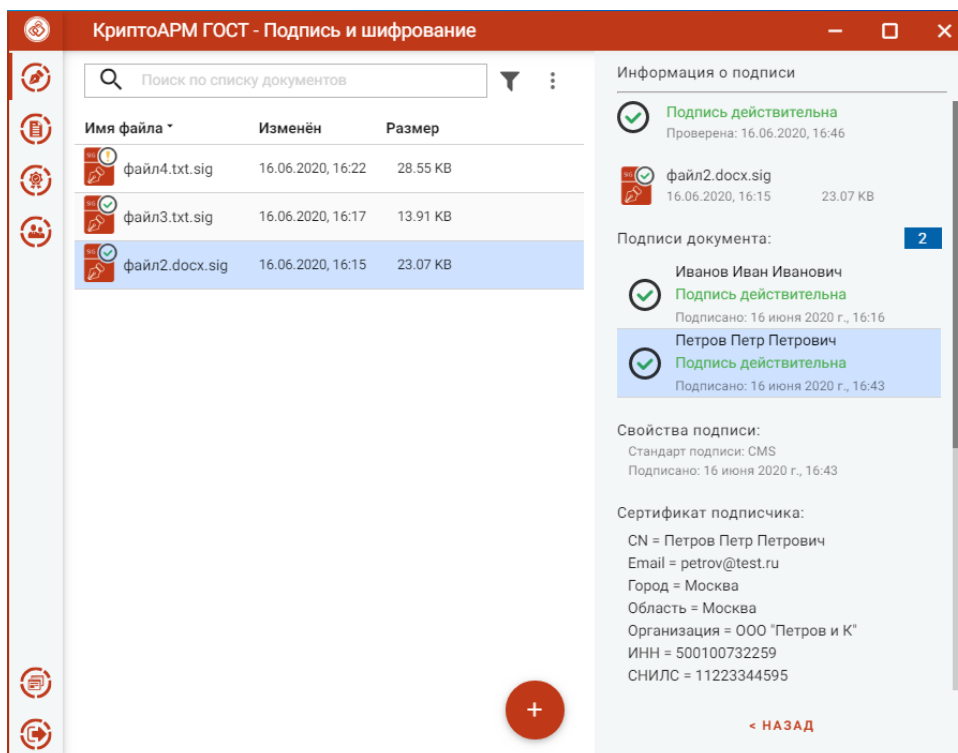


Рисунок 33. Выбор сертификата для просмотра информации о подписи

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 (Рисунок 34).

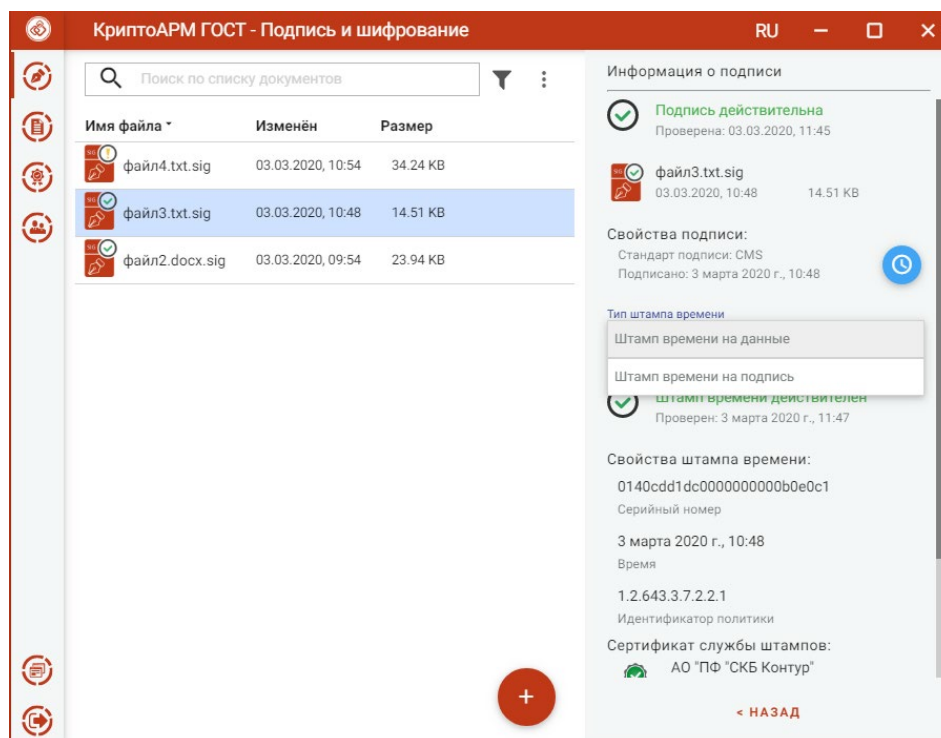


Рисунок 34. Отображение информации о подписи со штампом времени

Если документ подписан усовершенствованной подписью, то для просмотра сведений о штампах времени в усовершенствованной подписи, нужно нажатием на иконку развернуть информацию и выбрать в выпадающем списке тип штампа времени (Рисунок 35).

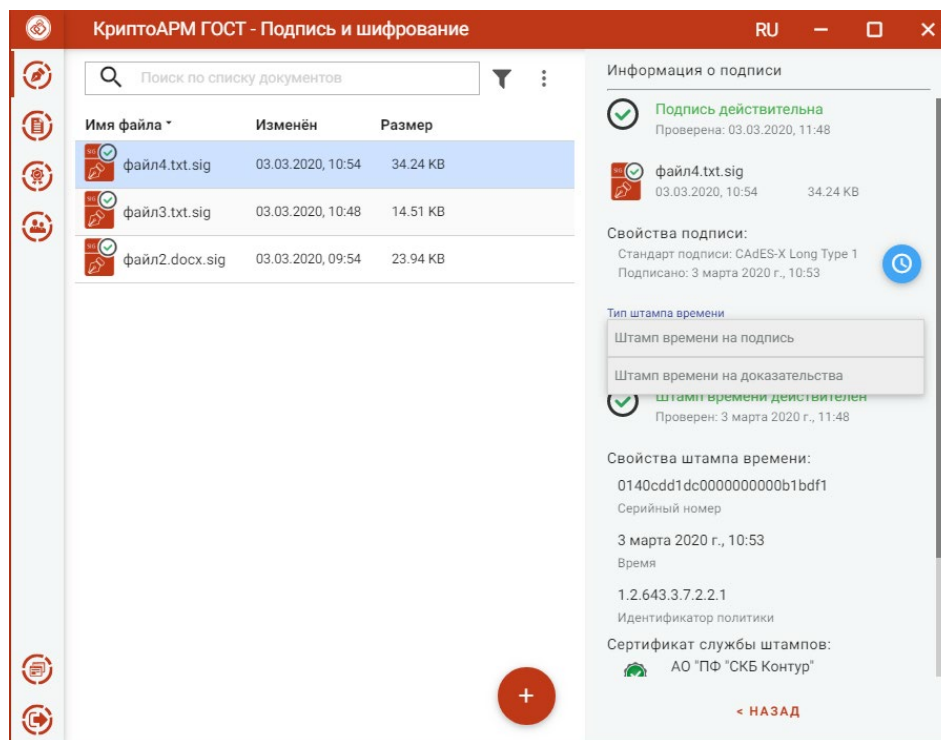


Рисунок 35. Отображение информации о штампах времени усовершенствованной подписи

Информация о OCSP ответе усовершенствованной подписи представлена на рисунке Рисунок 36.

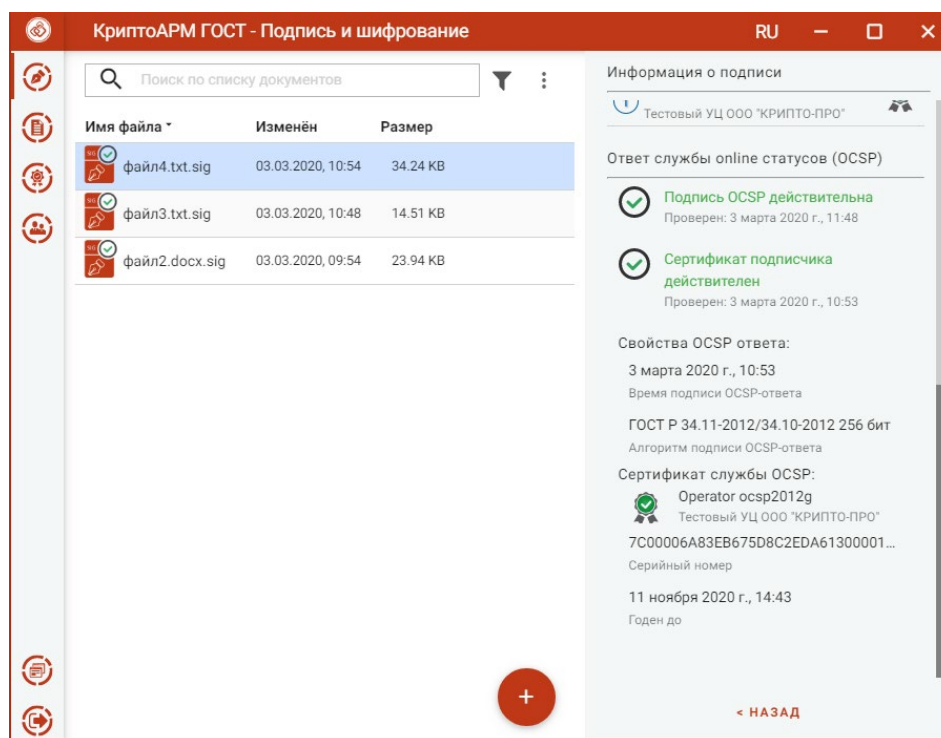


Рисунок 36. Отображение информации о OCSP ответе усовершенствованной подписи

3.6 ДОБАВЛЕНИЕ ПОДПИСИ

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 (Рисунок 37).

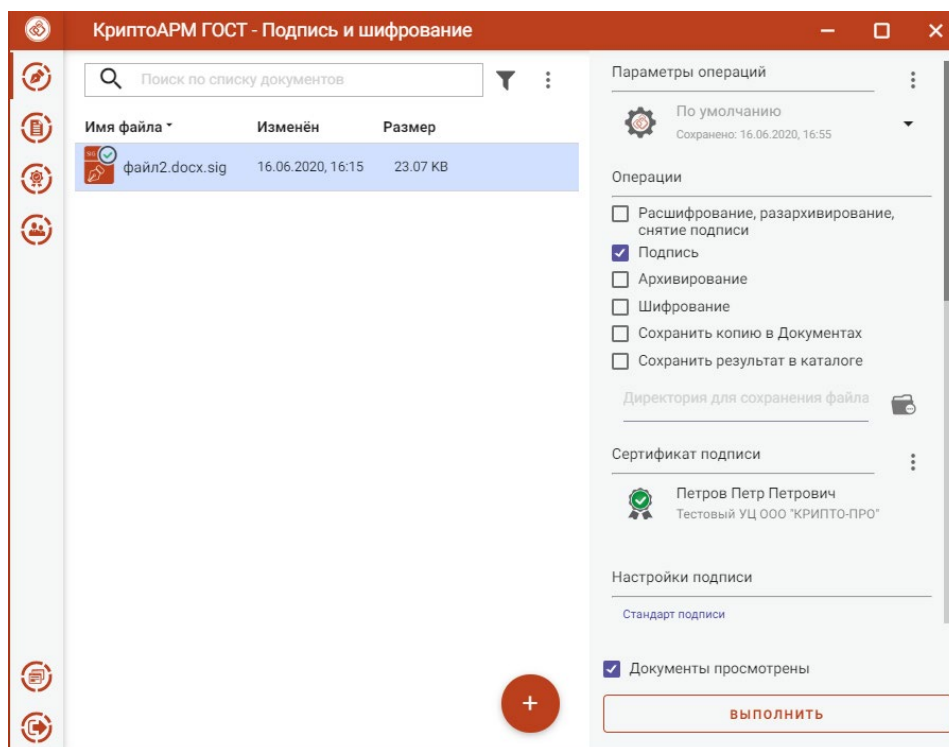


Рисунок 37. Добавление подписи к уже подписанным файлам

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

Тип подписи и использование штампов времени можно настроить.

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** (Рисунок 38).

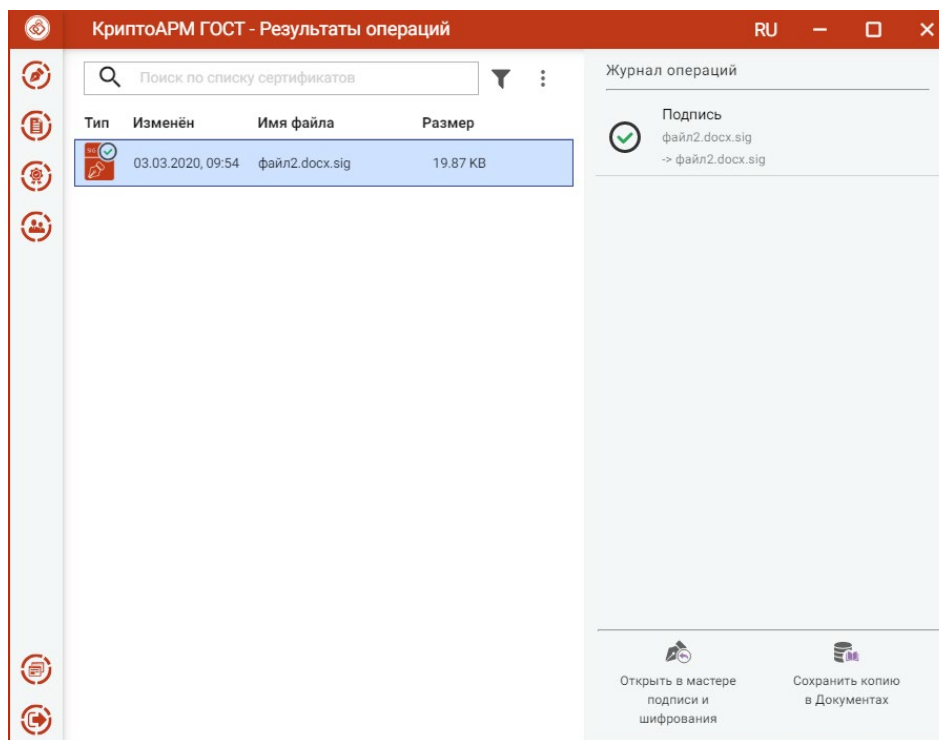


Рисунок 38. Результаты операции добавления подписи

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 конкретной подписи, нужно выбрать подпись из списка (Рисунок 39).

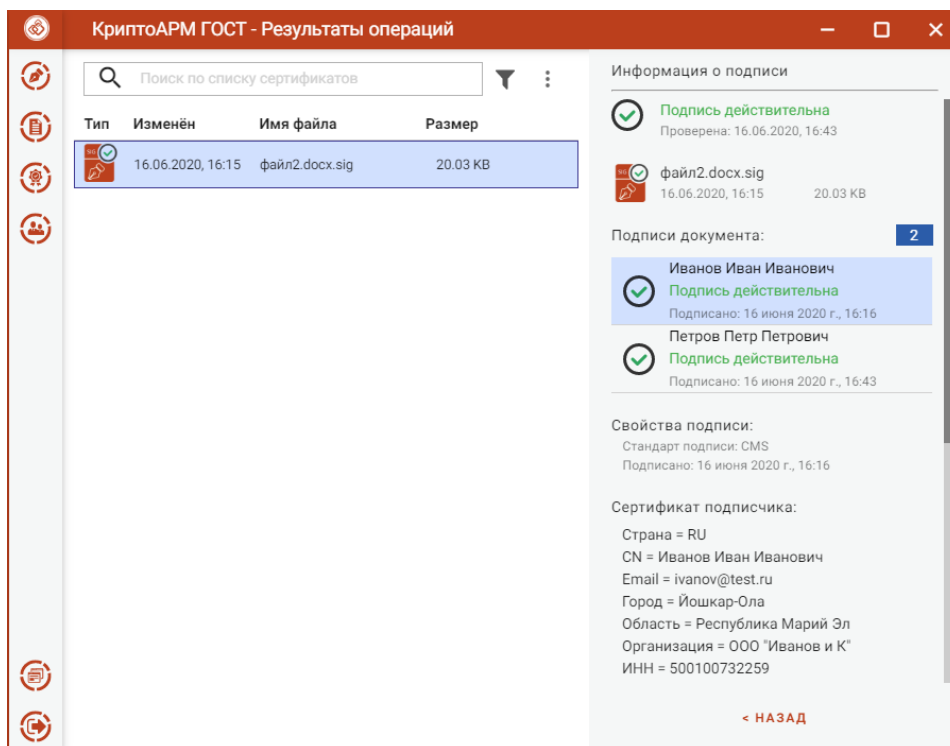


Рисунок 39. Выбор сертификата при просмотре информации о подписи

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 38). 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**.

3.7 АРХИВИРОВАНИЕ ФАЙЛОВ

Для архивирования файлов нужно выбрать файлы и опцию **Архивирование** (Рисунок 40)

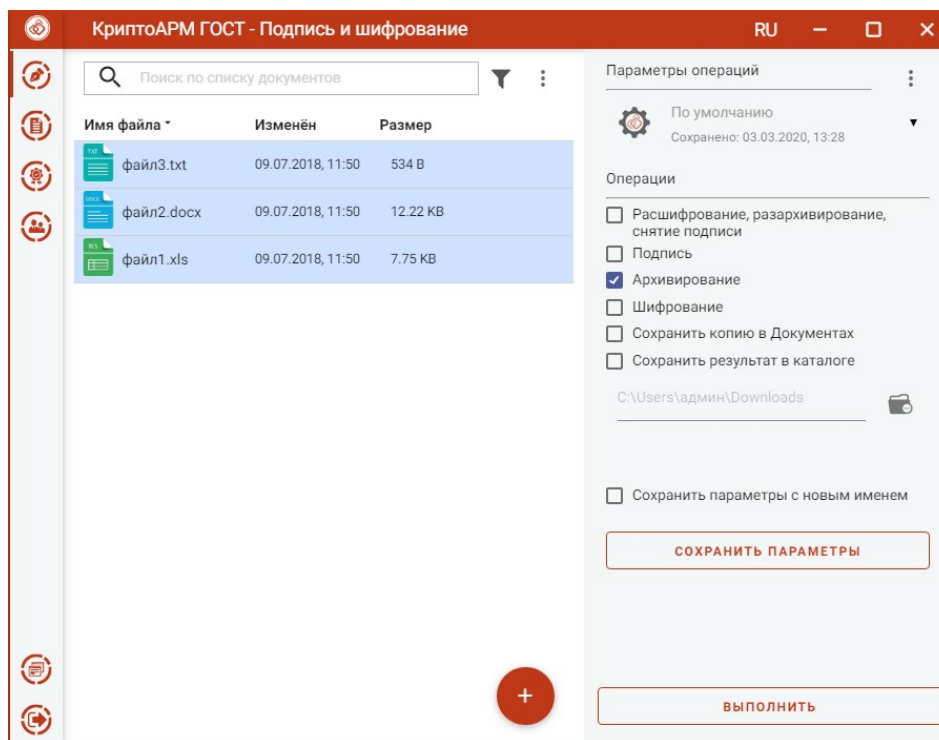


Рисунок 40. Архивирование файлов

Можно задать каталог для сохранения архива документов, выбрав в операциях опцию **Сохранить результат в каталоге**. При установке флага становится доступно поле выбора каталога (Рисунок 41).

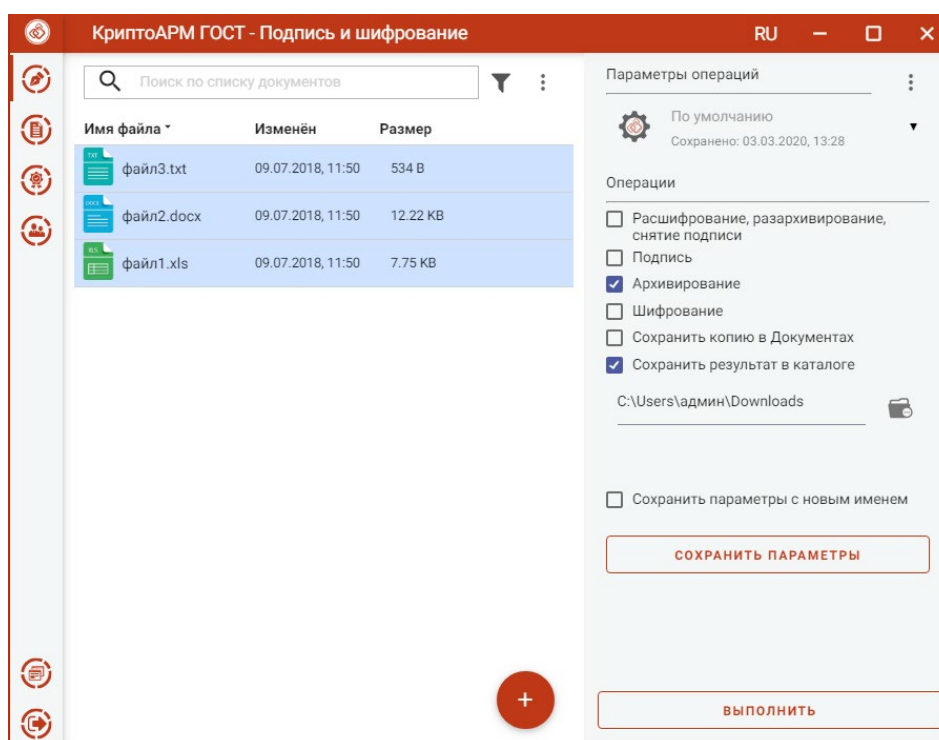


Рисунок 41. Выбор папки для сохранения архива

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** (Рисунок 42)

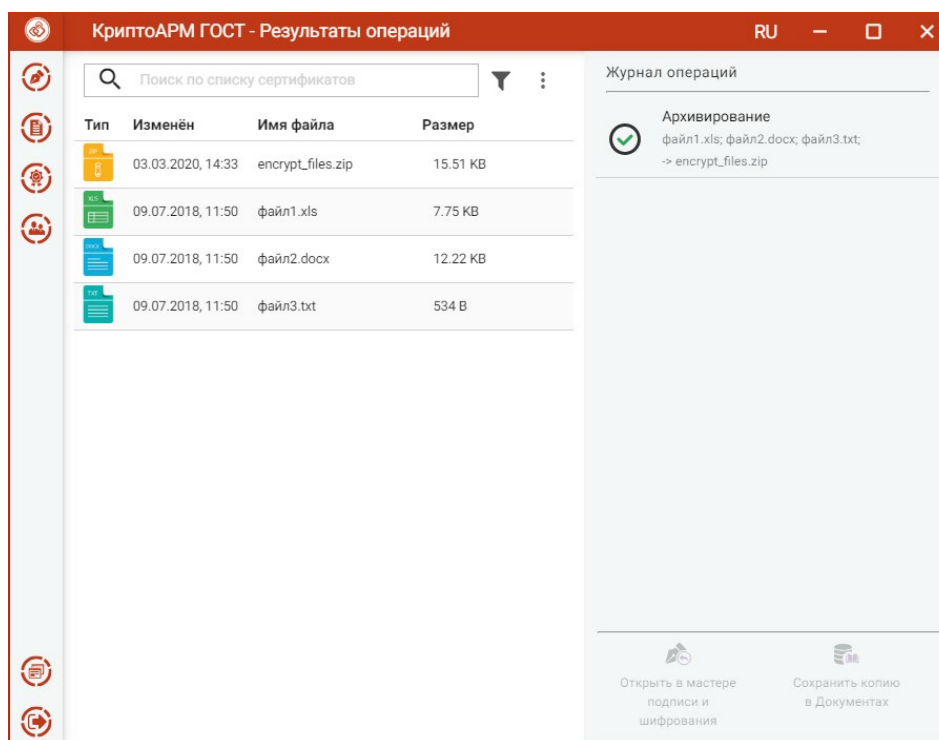


Рисунок 42 Результат операции архивирования

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.

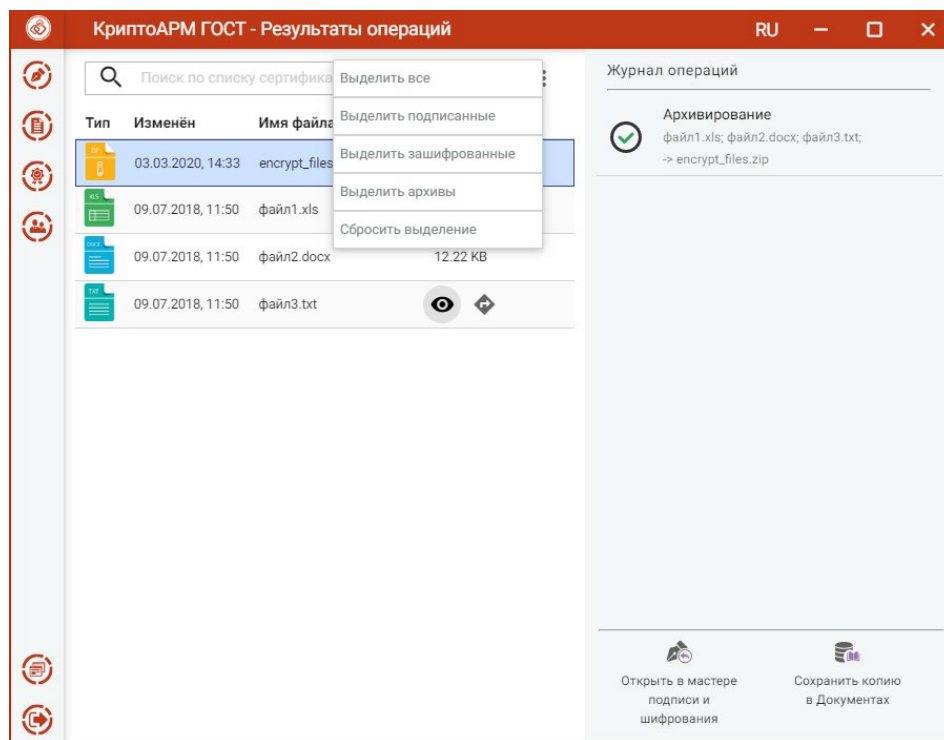


Рисунок 43. Операции для документа

Для списка документов доступно контекстное меню, позволяющее выделить файлы по типу операции (Рисунок 43).

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 43). 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**.

3.8 ШИФРОВАНИЕ ФАЙЛОВ

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

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 перетаскив файлы мышкой в область формирования списка файлов.

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (Рисунок 44).

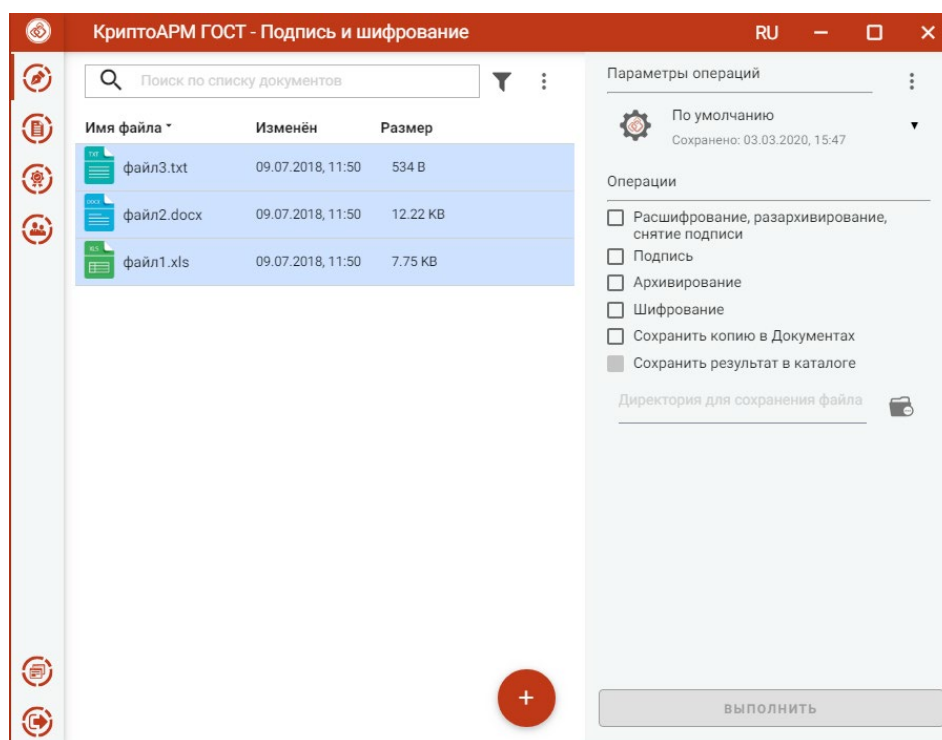


Рисунок 44. Список файлов для шифрования

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (Рисунок 45).

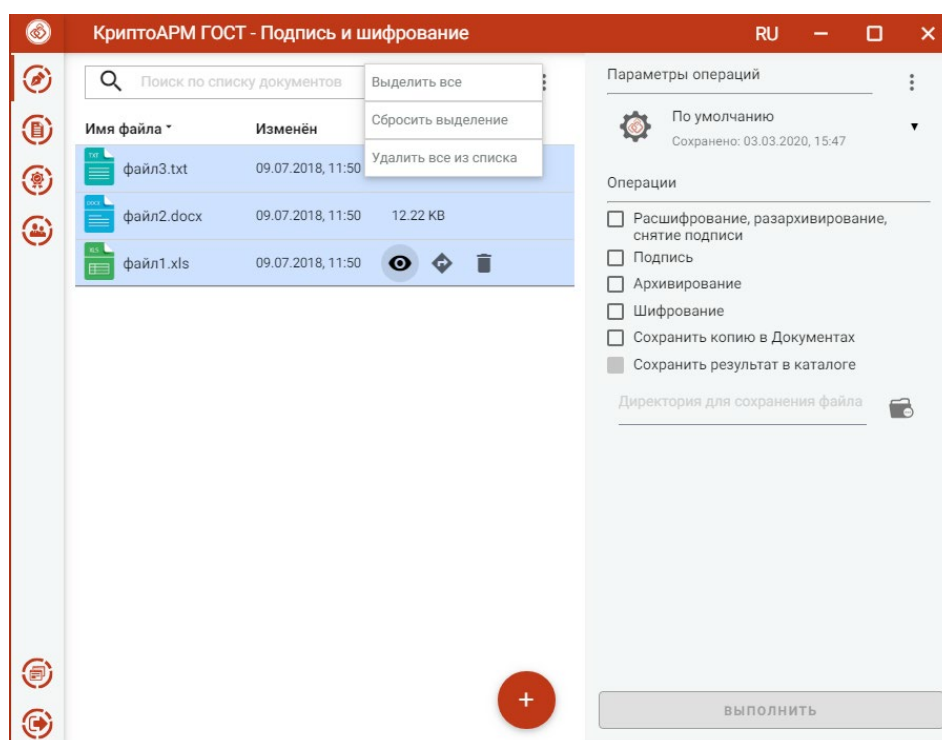


Рисунок 45. Контекстное меню управления списком файлов

НАСТРОЙКА ПАРАМЕТРОВ ШИФРОВАНИЯ. Для доступа к настройке параметров шифрования в разделе Операции необходимо выбрать опцию **Шифрование** (Рисунок 46).

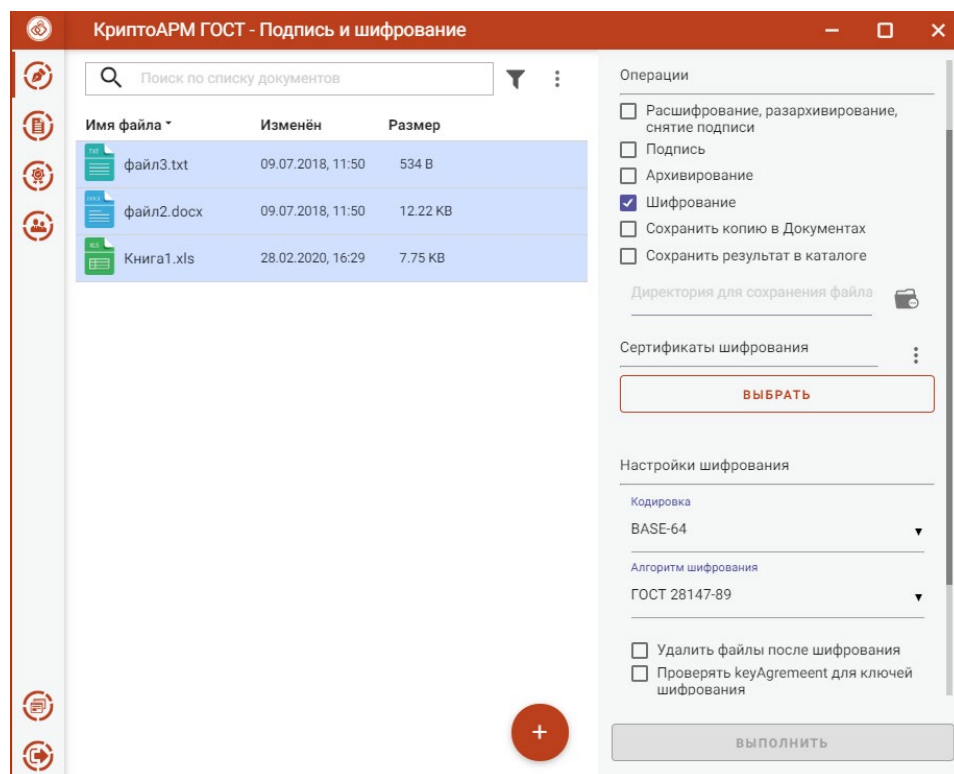


Рисунок 46. Выбор параметров шифрования

В параметрах можно настроить:

- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнечик».
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции.
- **Проверить keyAgreement для ключей шифрования** - при установленном флаге при операции шифрования в сертификатах проверяется наличие в расширении keyUsage использование ключа keyAgreement (согласование ключей). Если в сертификате нет использования ключа «Согласование ключей», то при включенном флаге операция шифрования в адрес такого сертификата производится не будет. При выключенном флаге шифрование будет выполняться в адрес сертификатов без использования ключа «Согласование ключей».

Внимание: шифрование без установленного флага «Проверить keyAgreement для ключей шифрования» возможно только в тестовых целях.

Можно задать каталог для сохранения зашифрованных документов, выбрав в операциях опцию **Сохранить результат в каталоге**. При установке флага становится доступно поле выбора каталога (Рисунок 47).

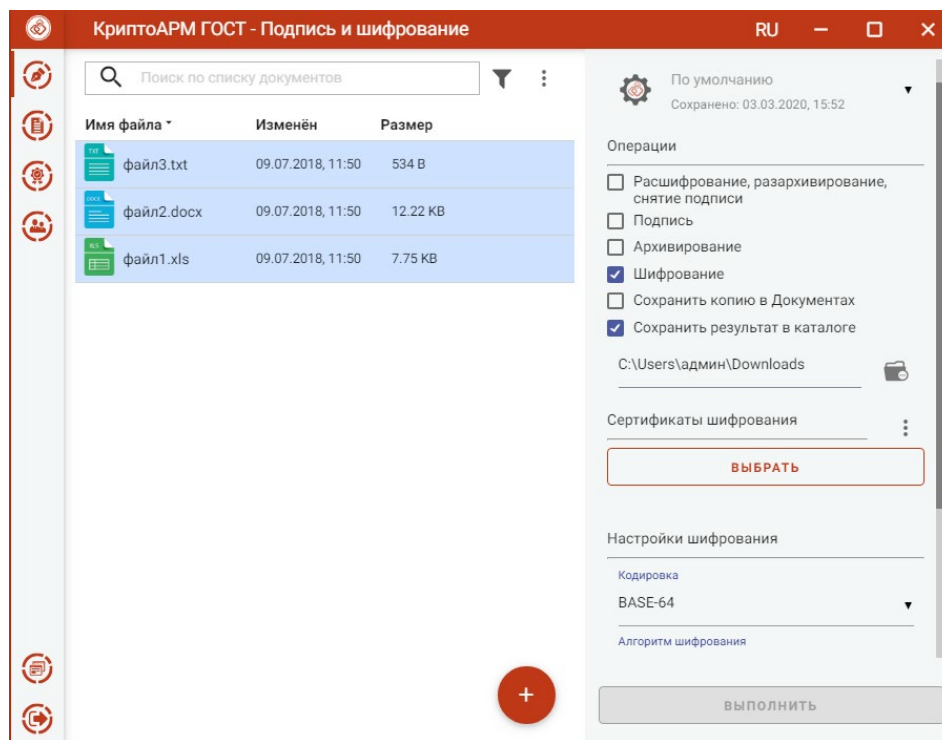


Рисунок 47. Выбор каталога для сохранения зашифрованного файла

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

Опция **Сохранить копию в Документах** служит для сохранения копии полученного после операции файла в специальный каталог Documents, расположенный в папке пользователя в каталоге `./Trusted/CryptoARM GOST/`. 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»](#).

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** (Рисунок 48).

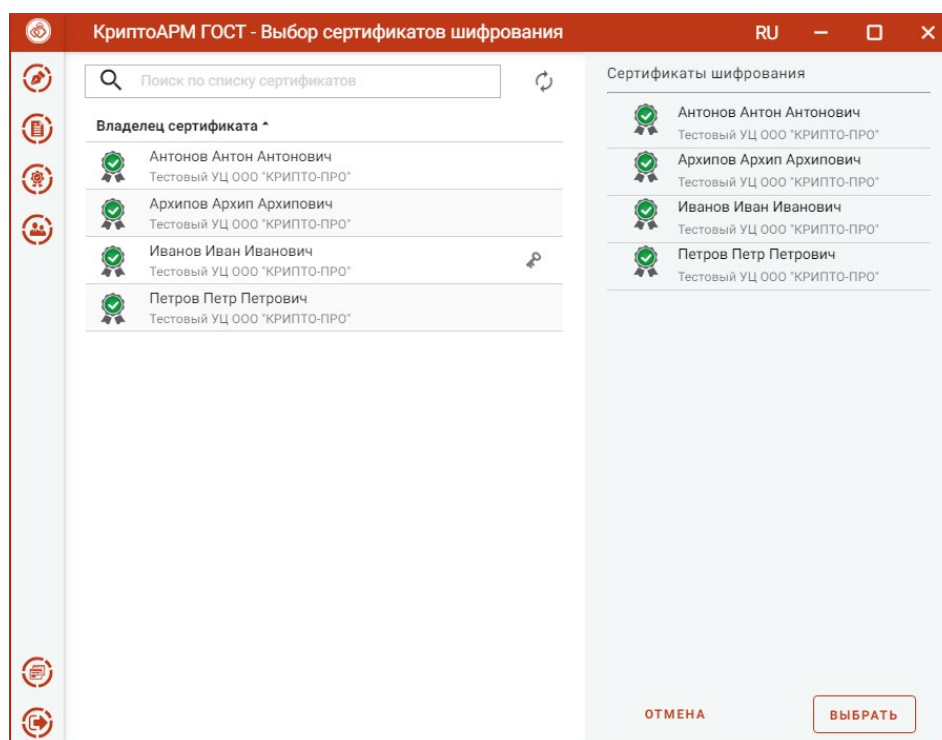


Рисунок 48. Выбор сертификатов шифрования

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

Выбранные сертификаты получателей перемещаются в правый список. Сертификаты в списке можно удалять, по ним можно посмотреть детальную информацию, нажав на интересующий сертификат в правой области (Рисунок 49).

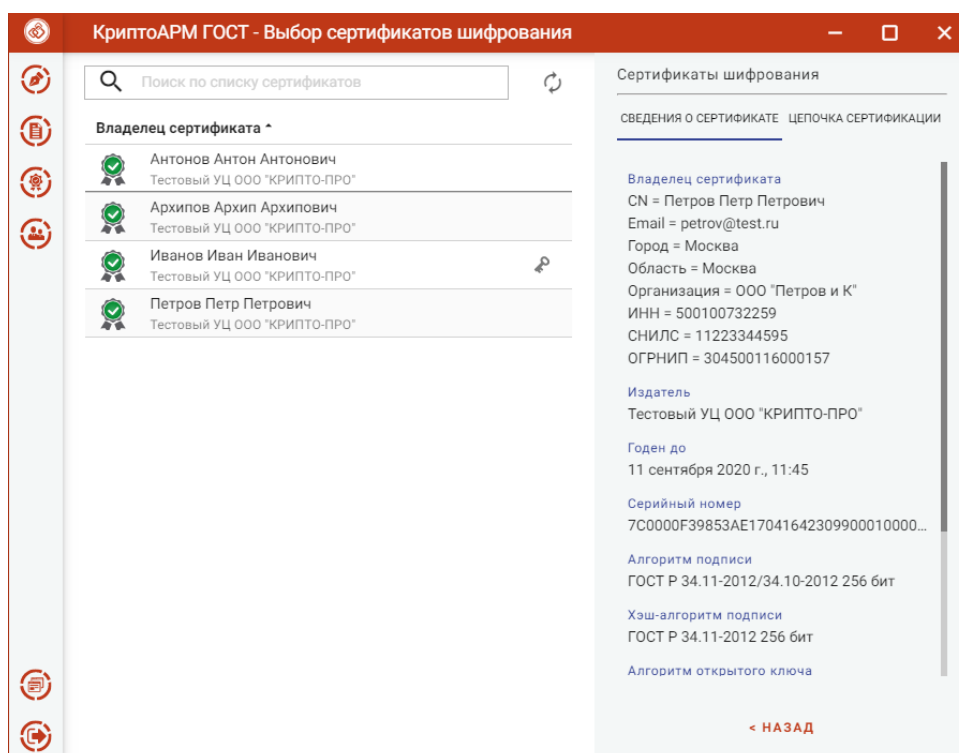


Рисунок 49. Информация о сертификате шифрования

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

Изменить список сертификатов шифрования можно с помощью контекстного меню (Рисунок 50). Удалить сертификаты из сформированного списка можно кнопкой **Удалить**.

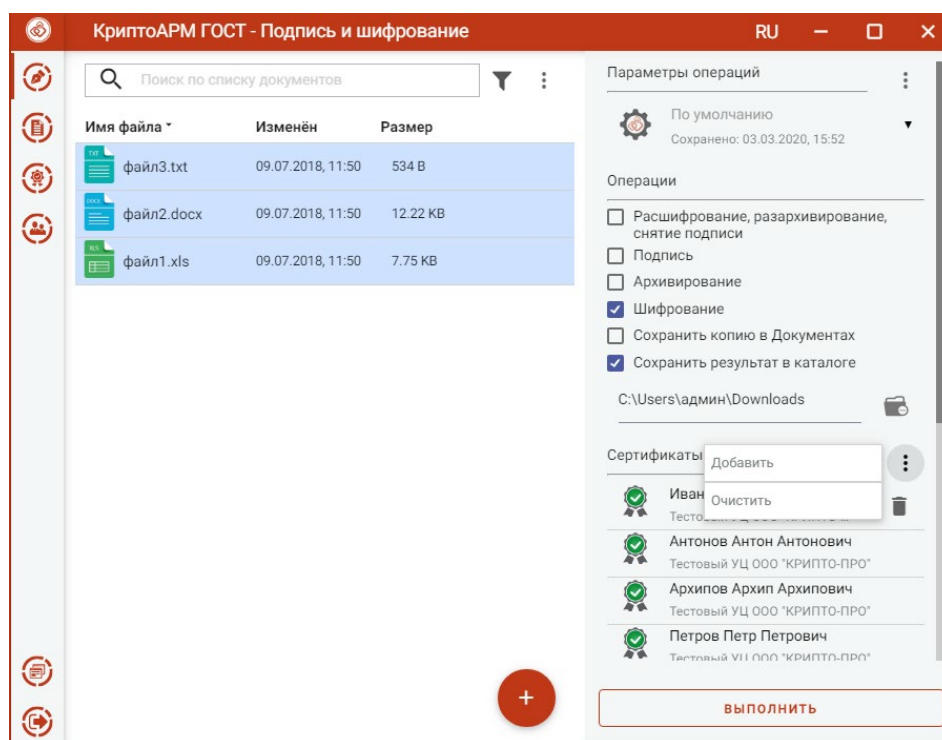


Рисунок 50. Изменение списка сертификатов шифрования

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

ШИФРОВАНИЕ ФАЙЛОВ. При условии выбора файлов, установи опции **Шифрование**, задания сертификатов получателей становится доступной кнопка **Выполнить** (Рисунок 51). Шифровать можно любые файлы, кроме ранее зашифрованных.

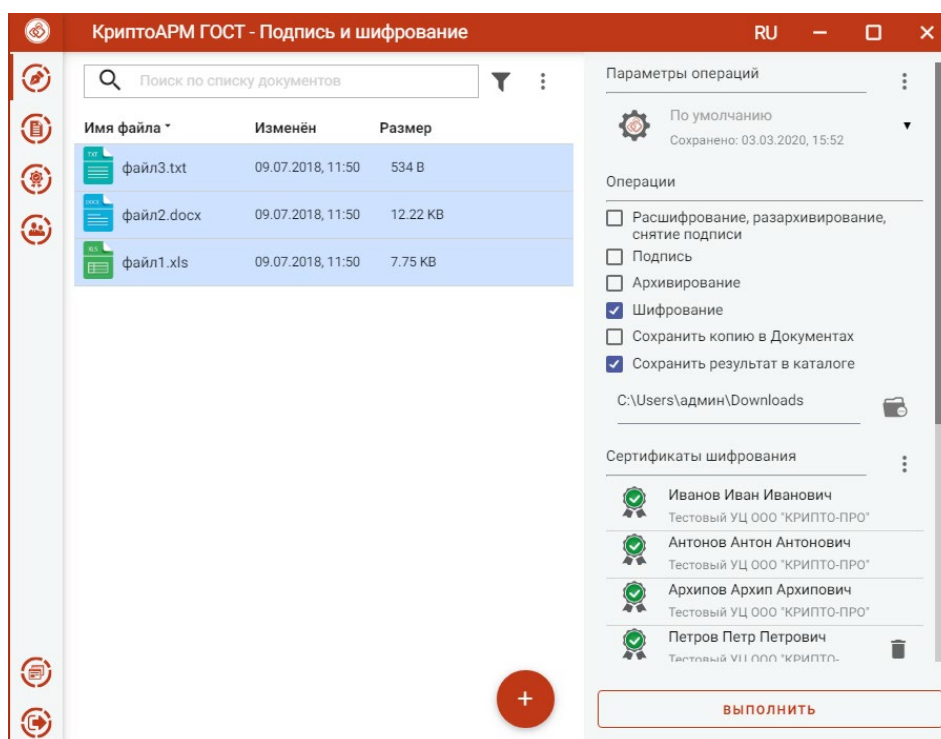


Рисунок 51. Шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс шифрования. Исходные и зашифрованные файлы отображаются в отдельном мастере **Результаты операций** (Рисунок 52).

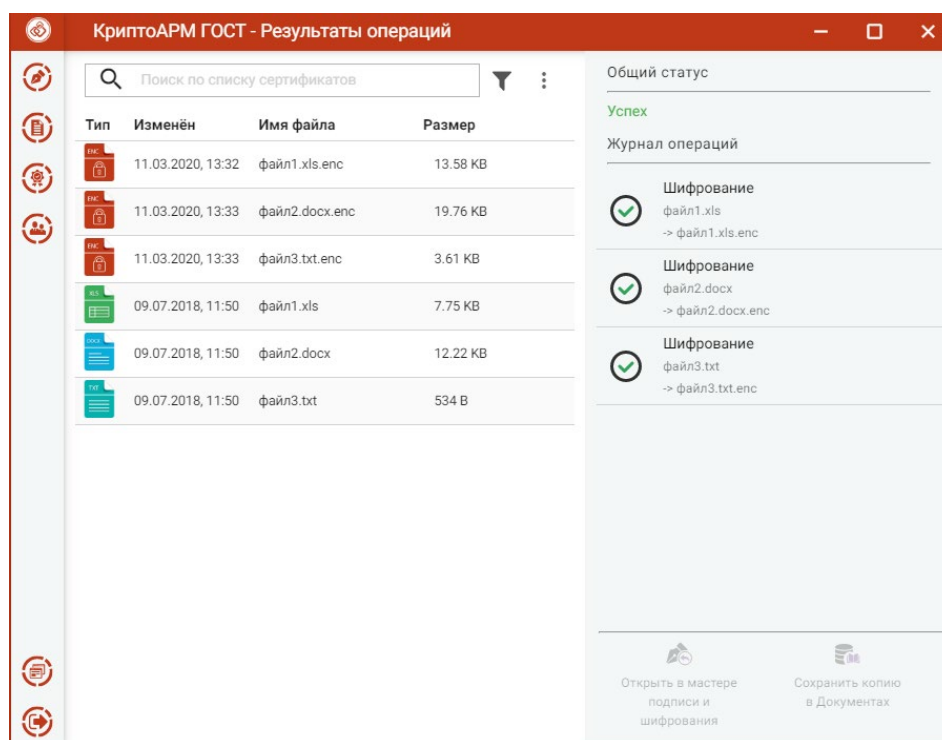


Рисунок 52. Результаты операции шифрования

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 (Рисунок 52). 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**.

3.9 Снятие электронной подписи

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** (Рисунок 53). Дополнительные параметры при снятии подписи выбирать не нужно.

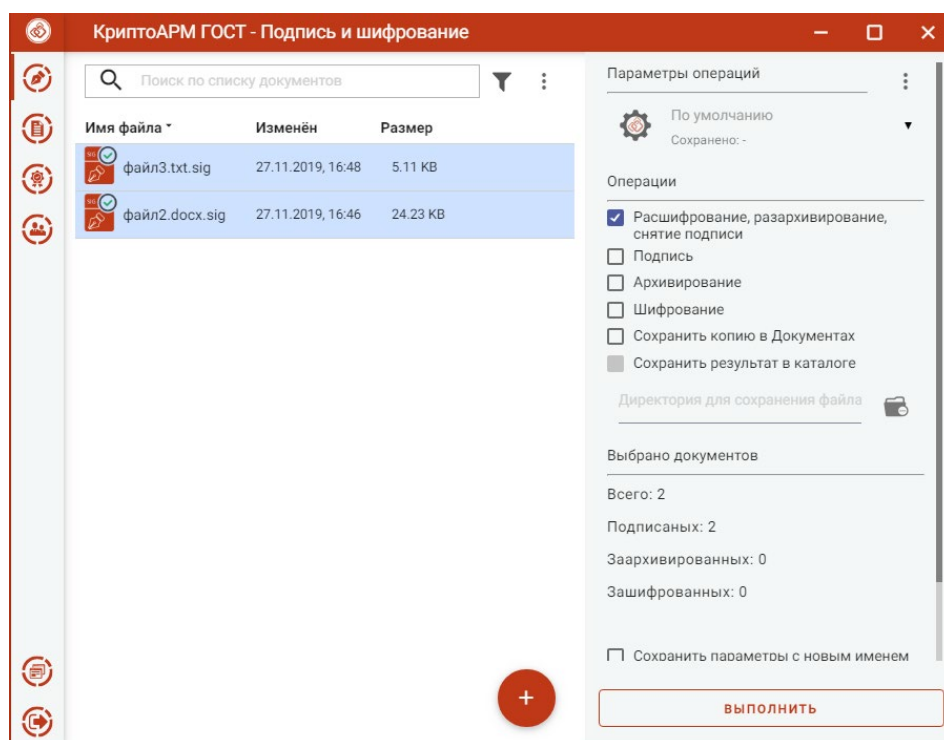


Рисунок 53. Выделенные файлы для снятия подписи

Подписанные и полученные файлы отображаются в отдельном мастере **Результаты операций** (Рисунок 54).

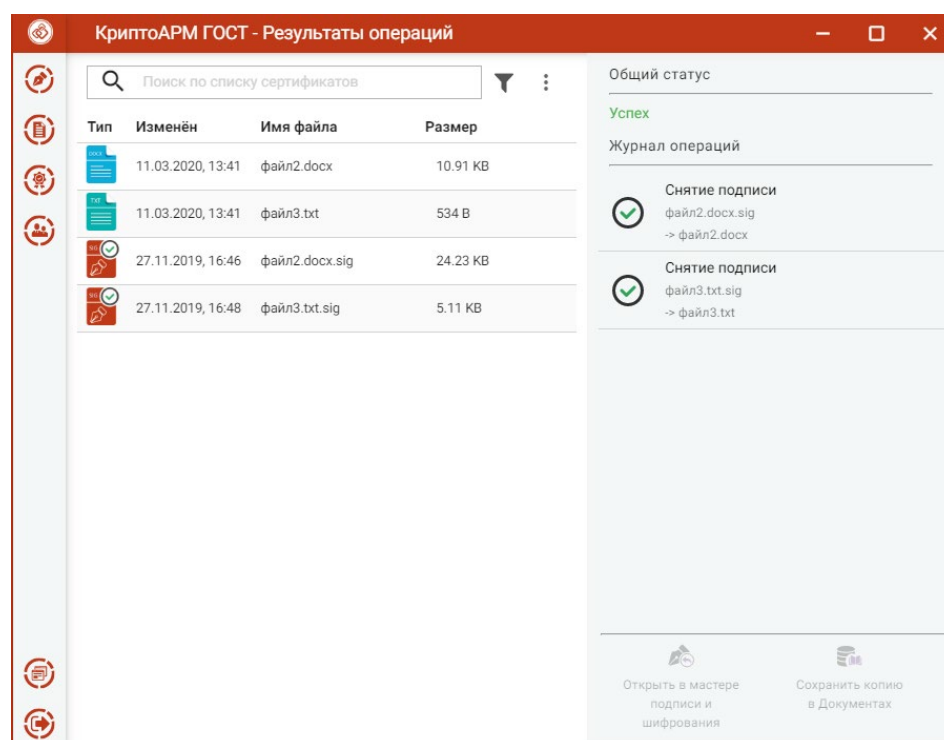


Рисунок 54. Результат снятия подписи с файлов

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 54). 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 отдельной подписи при выполнении операции снятия подписи возникает сообщение об ошибке, в окне **Результаты операций** отображаются только подписанные файлы.

3.10 РАСШИФРОВАНИЕ ФАЙЛОВ

Для расшифрования достаточно выбрать зашифрованные файлы - файлы с расширением **.enc**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить** (Рисунок 55). Настройка дополнительных параметров для операции расшифрования не требуется.

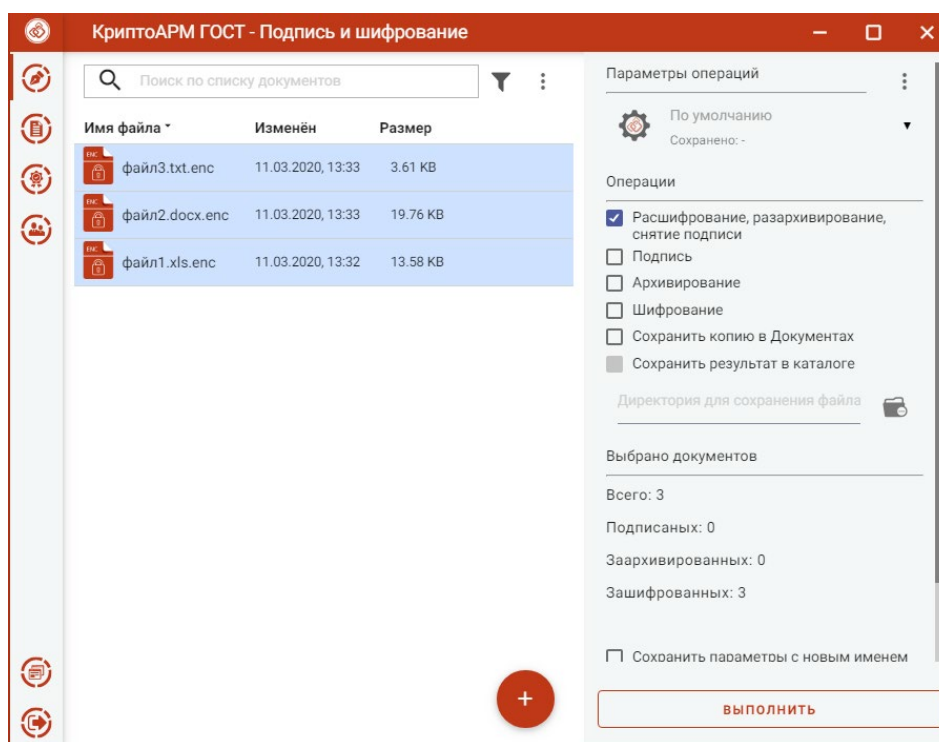


Рисунок 55. Мастер расшифрования файлов

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций** (Рисунок 56).

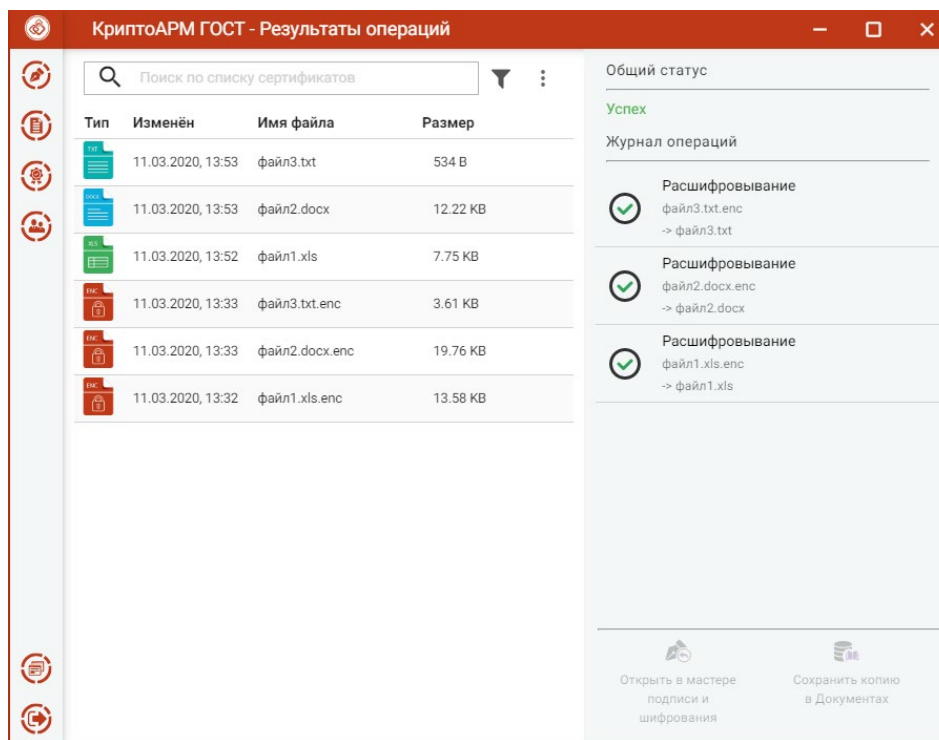


Рисунок 56. Результаты расшифрования файлов

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

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (рис. 4.10.2). 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**.

Если в хранилище сертификатов не окажется сертификата с ключом ЭП, который был выбран в качестве сертификата получателя при шифровании, расшифрование не будет выполнено. В мастере Результаты операций будут только зашифрованные файлы (Рисунок 57).

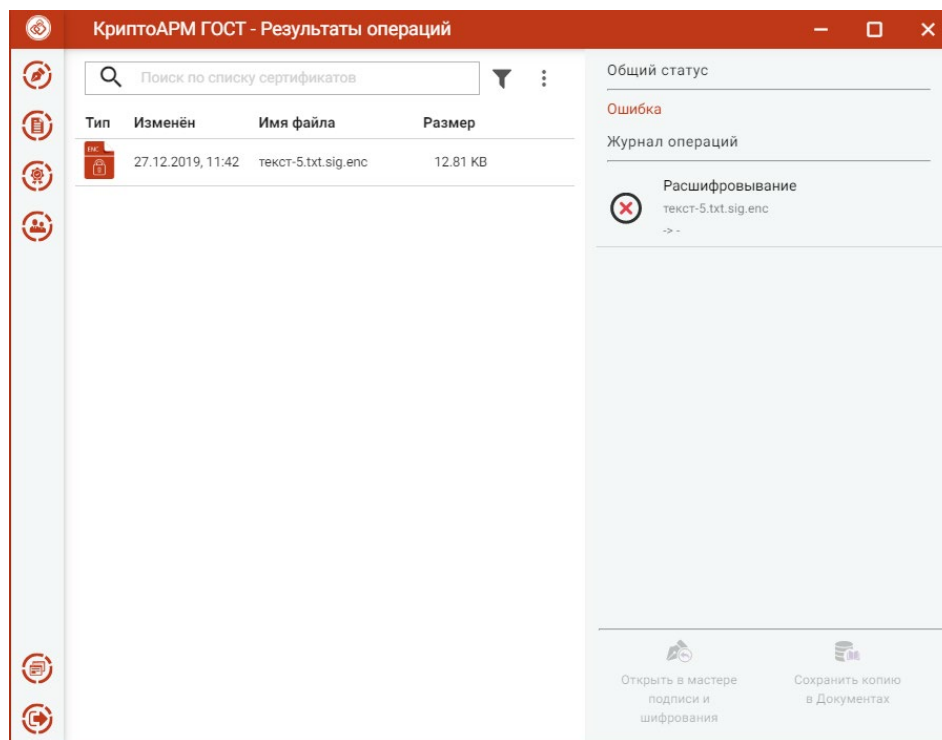


Рисунок 57. Ошибка при расшифровании файлов

3.11 ПРЯМЫЕ ГРУППОВЫЕ ОПЕРАЦИИ (ПОДПИСЬ, АРХИВИРОВАНИЕ, ШИФРОВАНИЕ)

В приложении доступно выполнение следующих групповых операций:

- Подпись и архивирование – документ сначала подписывается, затем архивируется;
- Подпись и шифрование – документ сначала подписывается, затем шифруется.
- Архивирование и шифрование – документы сначала архивируются, затем шифруются.
- Подпись, архивирование и шифрование – документы сначала подписываются, затем архивируются, потом шифруются.

3.11.1 Подпись и архивирование.

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

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

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (Рисунок 58).

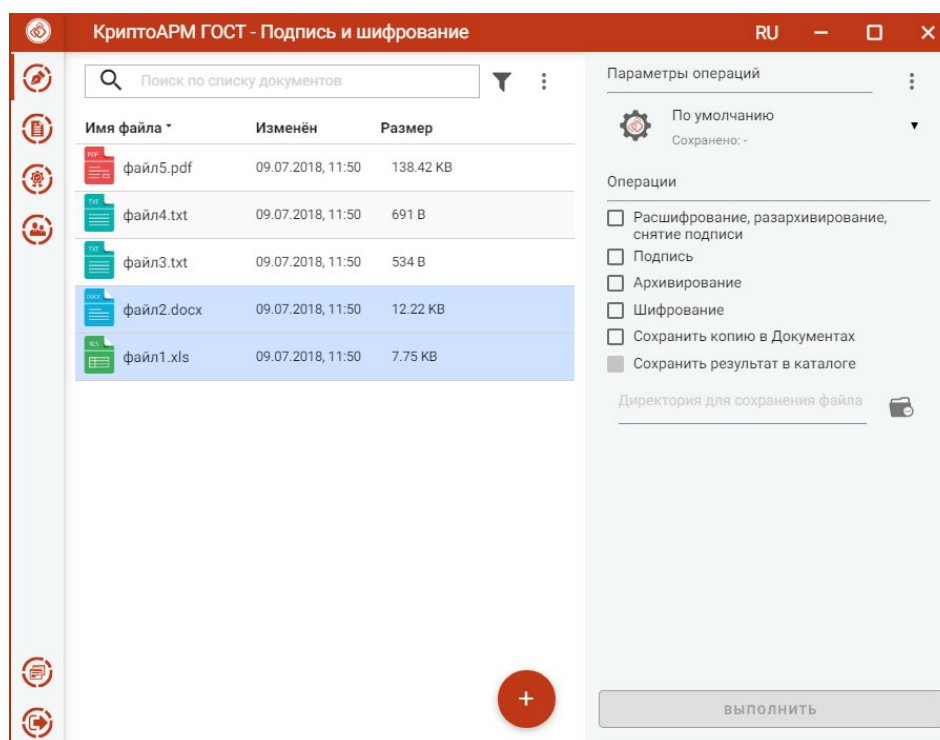


Рисунок 58. Список файлов для операции

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (Рисунок 59).

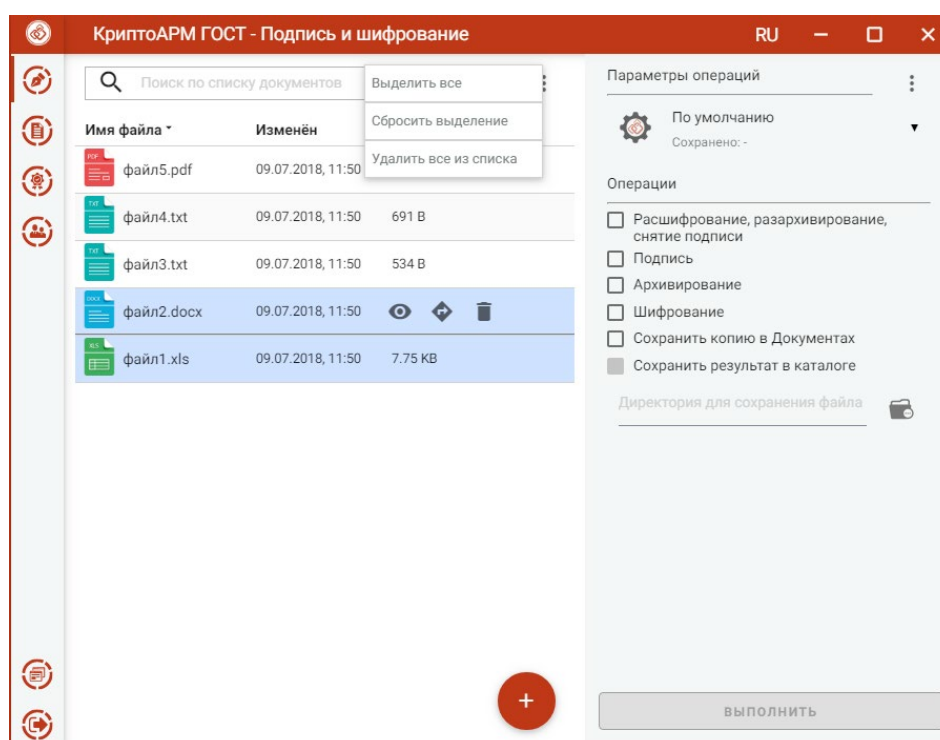


Рисунок 59. Контекстное меню управления списком файлов

УСТАНОВКА ПАРАМЕТРОВ ПОДПИСИ И АРХИВИРОВАНИЯ. Для операций подписи и архивирования файлов в разделе **Операции** необходимо выбрать опции **Подпись** и **Архивирование**, становятся доступны настройки параметров подписи (Рисунок 60).

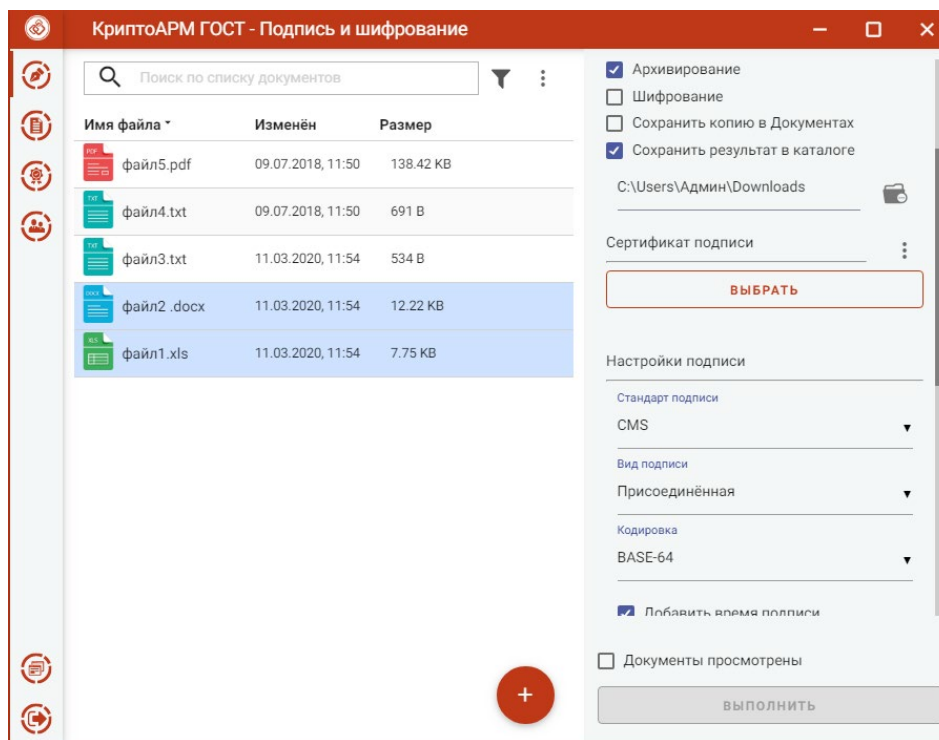


Рисунок 60. Настройка параметров подписи

В параметрах можно настроить:

- **Сертификат подписи.**
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее о создании усовершенствованной подписи в пункте «[Создание усовершенствованной подписи](#)»). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client 2.0 и КриптоПро OCSP Client 2.0.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Добавить время подписи** - при установленном флажке в подпись сохраняется время (системное) подписи.
- **Добавлять штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.
- **Добавлять штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.

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

Если флаг не установлен, то файл сохраняется рядом с исходным 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](#)».

ВЫБОР СЕРТИФИКАТА ПОДПИСИ. Для того, чтобы выполнить подпись необходимо выбрать сертификат, к которому привязан ключ ЭП. Эта операция производится нажатием кнопки **Выбрать** сертификат подписи. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи (Рисунок 61).

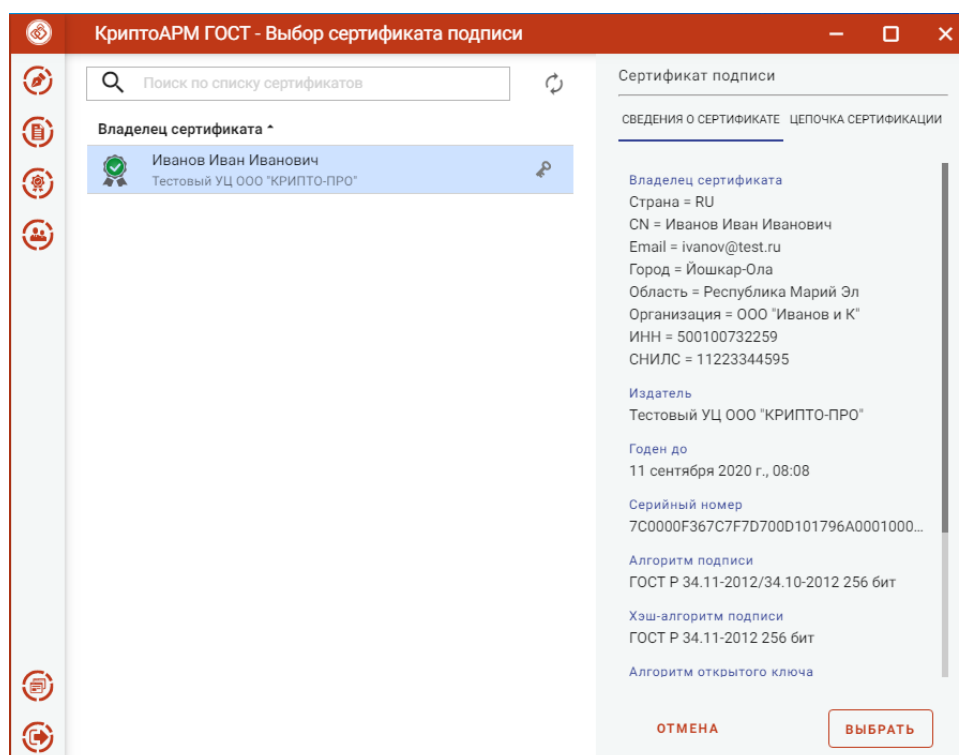


Рисунок 61. Выбор сертификата подписи

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

Сертификат подписи можно изменить с помощью контекстного меню (Рисунок 62).

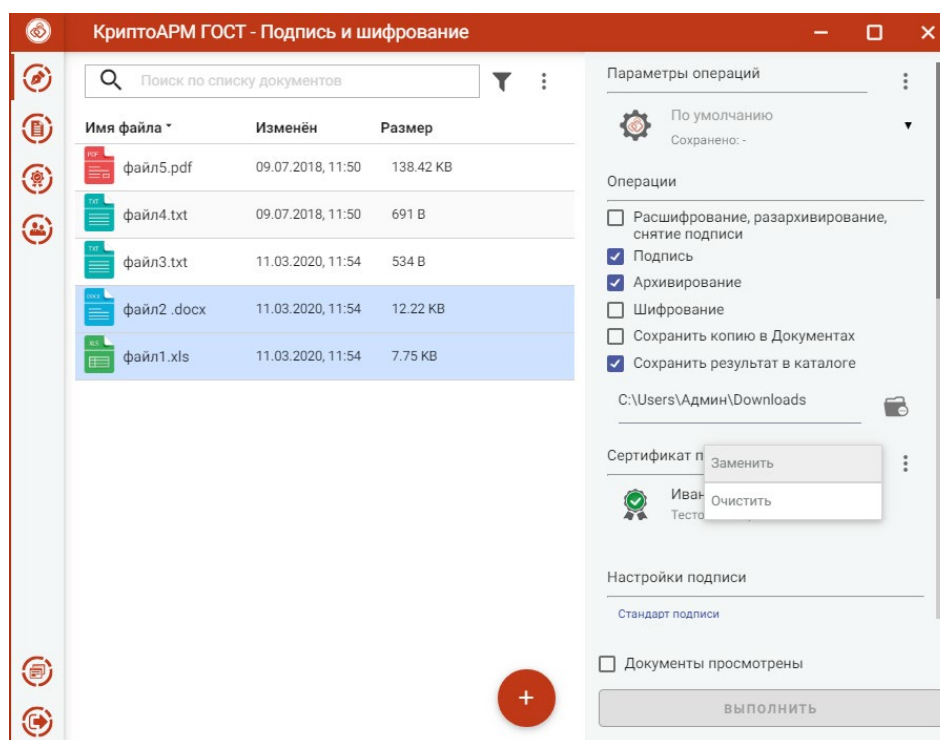


Рисунок 62. Изменение сертификата подписи

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

Подпись и архивирование файлов. При условии выбора сертификата подписи, файлов для подписи и установленного флага, что документы просмотрены, в мастере становится доступной кнопка **Выполнить** (Рисунок 63). Подписать и заархивировать можно любые файлы, кроме зашифрованных.

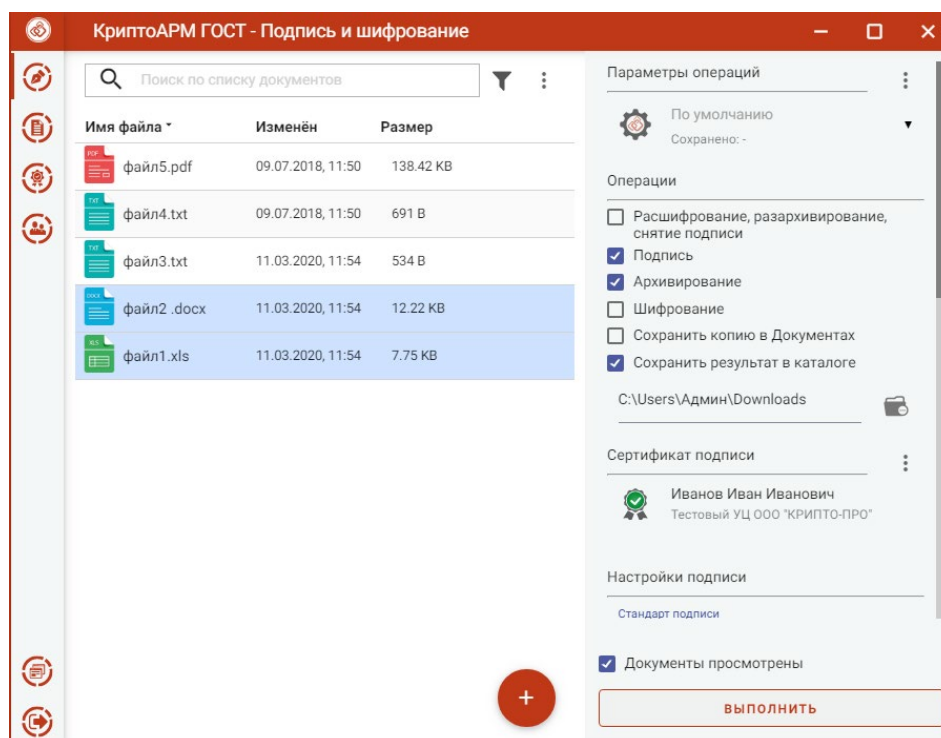


Рисунок 63. Подпись и архивирование файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи, а затем подписанный файл архивируется. Исходные документы (оригиналы), подписанные файлы (промежуточные) и результаты операции архивирования отображаются в отдельном мастере **Результаты операций** (Рисунок 64).

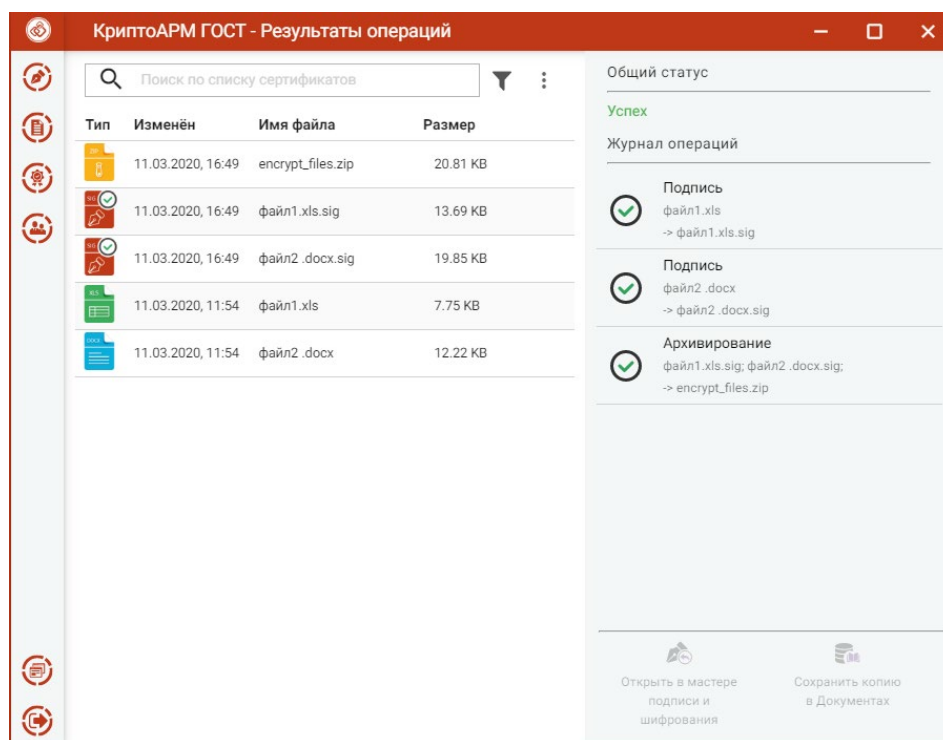


Рисунок 64. Результаты операций

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

Архив подписанных файлов сохраняется в каталоге, если в операциях был выбран каталог для сохранения результатов, или в домашней папке пользователя, если в операциях не был установлен флаг **Сохранить результат в каталоге**. Подписанные файлы сохраняются во временную папку TEMP, расположенную в домашней папке пользователя в каталоге ./Trusted/CryptoARM GOST/, и остаются до выполнения следующей операции.

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

Для подписанных файлов подпись проверяется автоматически.

Для каждого документа доступны операции (Рисунок 65):

- **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.

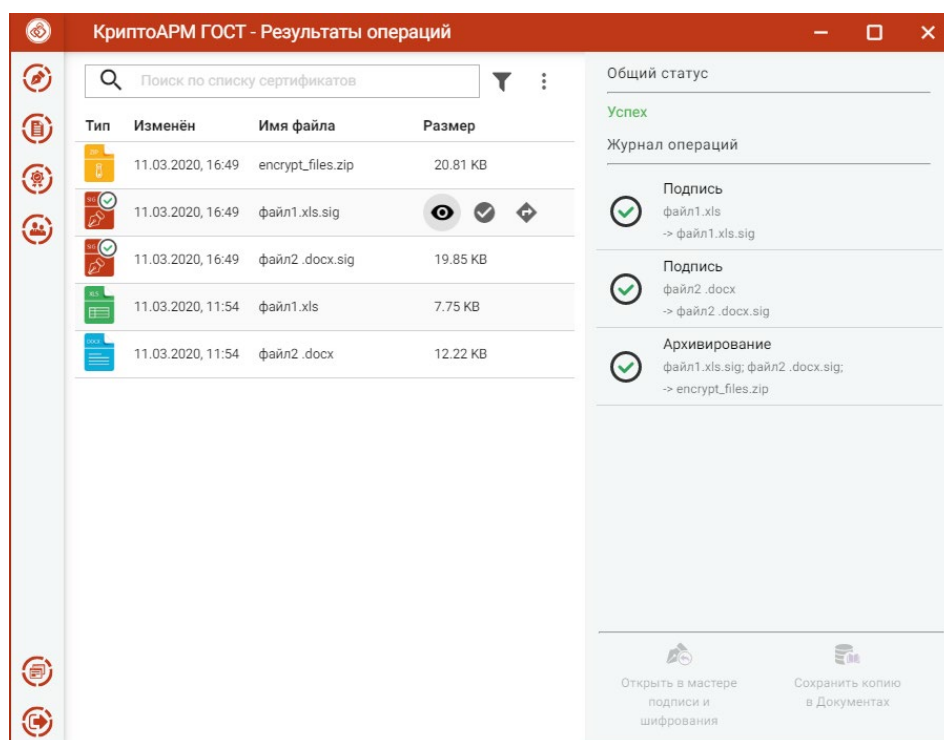


Рисунок 65. Операции для документа

Для списка документов доступно контекстное меню, позволяющее выделить файлы по типу операции (Рисунок 66).

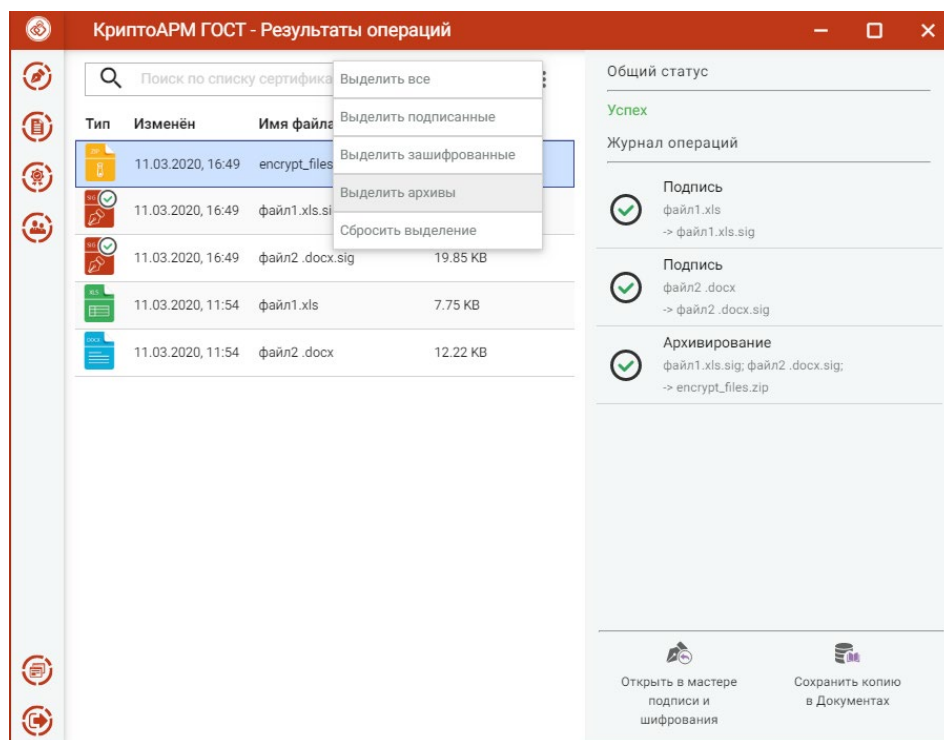


Рисунок 66. Выделение группы файлов по типу файла

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 66). 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**.

3.11.2 Подпись и шифрование

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

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

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (Рисунок 67).

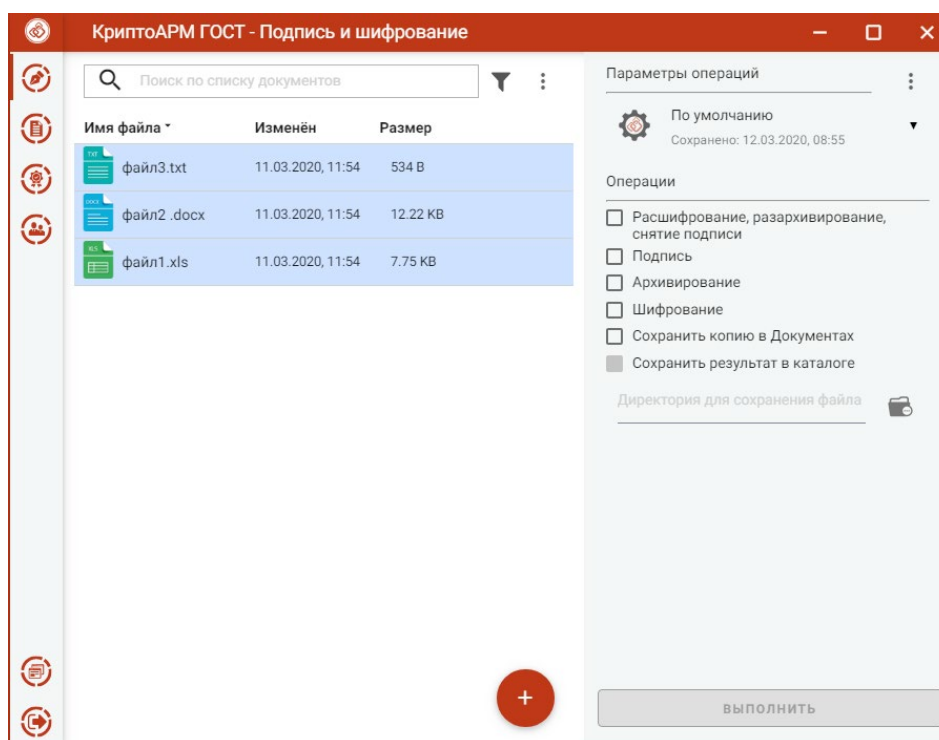


Рисунок 67. Список файлов для операции

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (Рисунок 68).

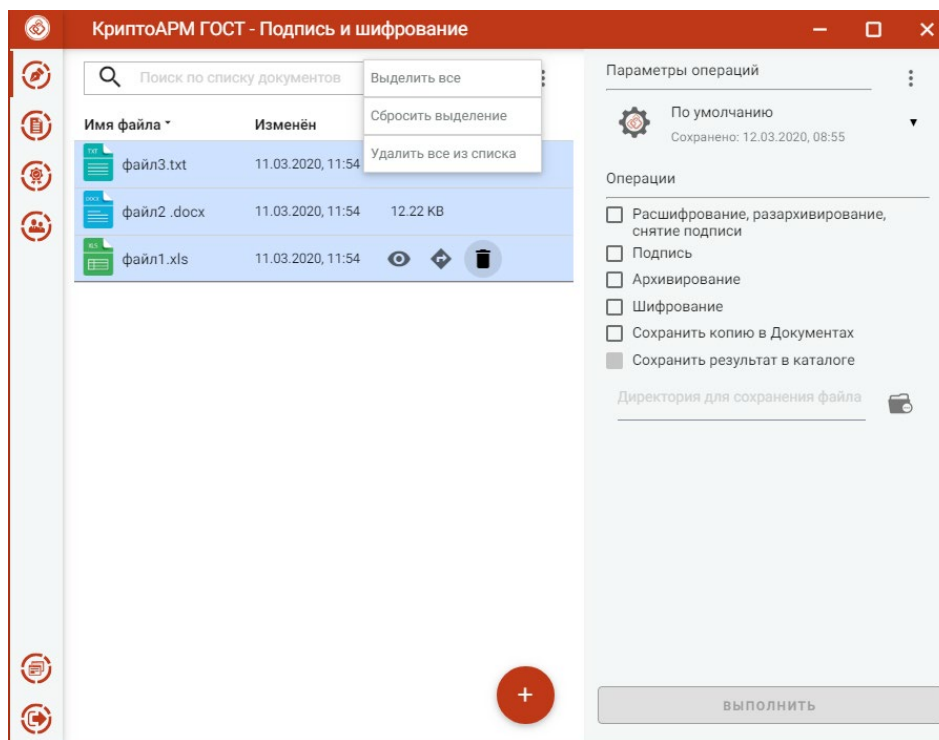


Рисунок 68. Контекстное меню управления списком файлов

УСТАНОВКА ПАРАМЕТРОВ ПОДПИСИ И ШИФРОВАНИЯ. Для операций подписи и шифрования файлов в разделе **Операции** необходимо выбрать опции **Подпись** и **Шифрование**, становятся доступны настройки параметров подписи и шифрования (Рисунок 69).

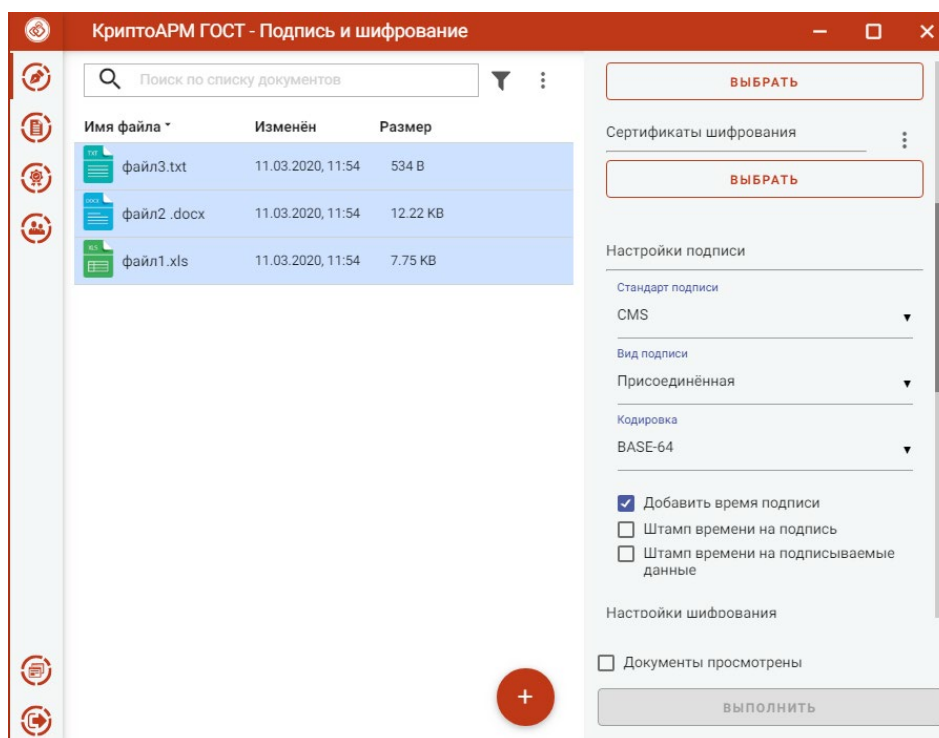


Рисунок 69. Настройка параметров подписи и шифрования

В параметрах подписи можно настроить:

- **Сертификат подписи** - сертификат, к которому привязан ключ ЭП. Выбор сертификата производится нажатием кнопки **Выбрать**. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи.

- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее о создании усовершенствованной подписи в пункте «[Создание усовершенствованной подписи](#)»). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client 2.0 и КриптоПро OCSP Client 2.0.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Добавить время подписи** - при установленном флажке в подпись сохраняется время (системное) подписи.
- **Добавлять штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.
- **Добавлять штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.

В параметрах шифрования можно настроить:

- **Сертификаты шифрования** - сертификаты получателей. Выбор производится нажатием кнопки **Выбрать** сертификаты шифрования. В появившемся диалоговом окне отображаются сертификаты категории **Личные** и категории **Сертификаты других пользователей (Контакты)**. В списке сертификатов допускается выбор нескольких сертификатов, так как число получателей может быть различным.
- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнецик».
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции.
- **Проверить keyAgreement для ключей шифрования** - при установленном флаге при операции шифрования в сертификатах проверяется наличие в расширении keyUsage использование ключа keyAgreement (согласование ключей). Если в сертификате нет использования ключа «Согласование ключей», то при включенном флаге операция шифрования в адрес такого сертификата производится не будет. При выключенном флаге шифрование будет выполняться в адрес сертификатов без использования ключа «Согласование ключей».

Внимание: шифрование без установленного флага “Проверить keyAgreement для ключей шифрования” возможно только в тестовых целях.

Можно задать каталог для сохранения полученных документов, выбрав в операциях опцию **Сохранить результат в каталоге**. При установке флага становится доступно поле выбора каталога. Если флаг не установлен, то файл сохраняется рядом с исходным 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 можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте «[Управление параметрами операции](#)».

Подпись и шифрование файлов. При условии выбора сертификата подписи, сертификатов получателей, файлов для выполнения операции и установленного флага, что документы просмотрены, в мастере становится доступной кнопка **Выполнить** (Рисунок 70). Подписать и зашифровать можно любые файлы, кроме зашифрованных.

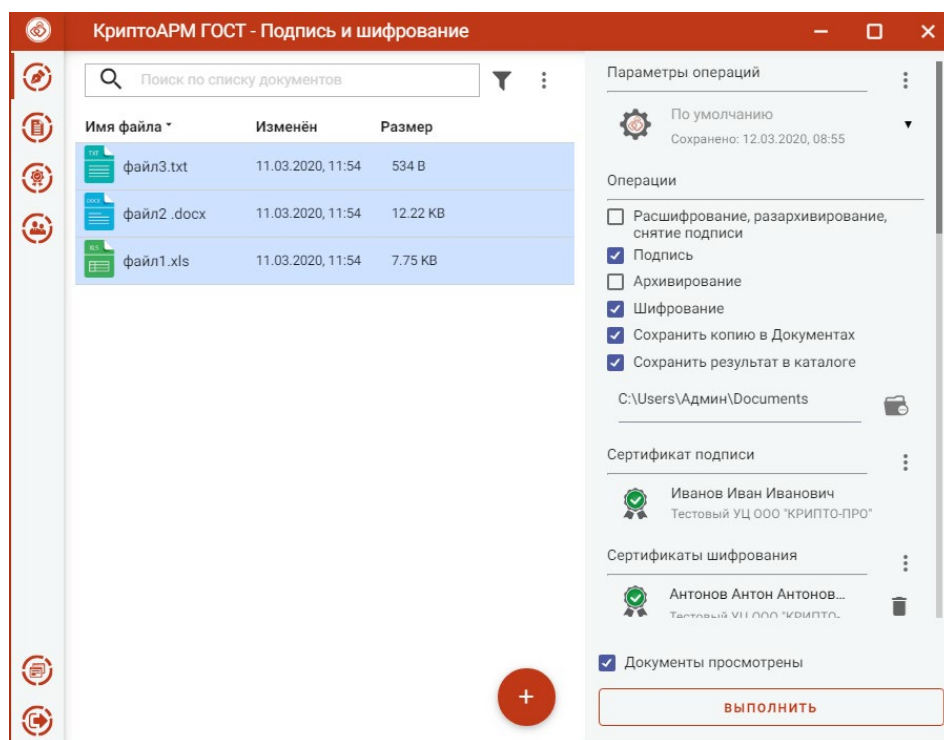


Рисунок 70. Подпись и шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи, а затем подписанный файл шифруется. Исходные документы (оригиналы), подписанные файлы (промежуточные) и результаты операции шифрования отображаются в отдельном мастере **Результаты операций** (Рисунок 71).

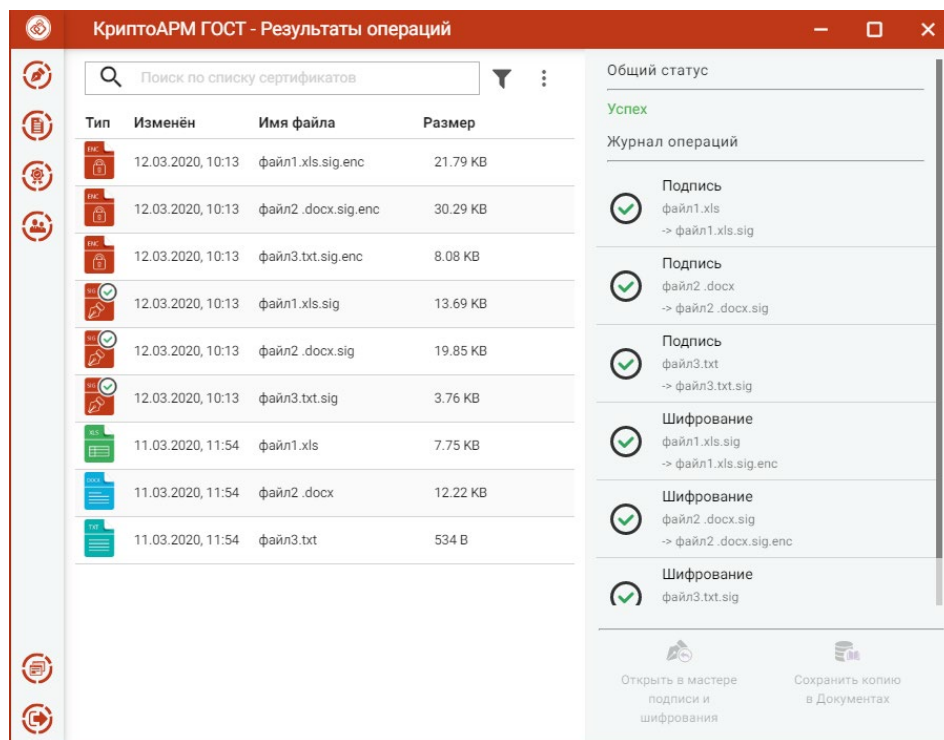


Рисунок 71. Результаты операций

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

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

Если при выборе параметров подписи был указан вид подписи **Отсоединенная**, то перед шифрованием исходные файлы и файлы подписи архивируются, а затем шифруются. В итоге операции подписи и шифрования получится зашифрованный архив.

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

Для подписанных файлов подпись проверяется автоматически.

Для каждого документа доступны операции (Рисунок 72):

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

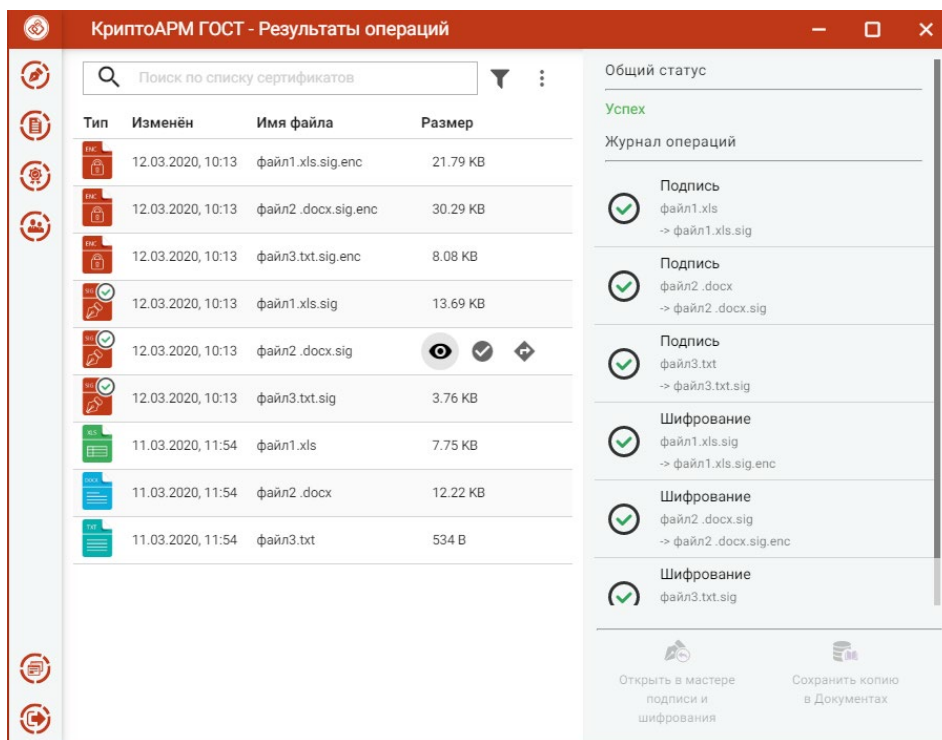


Рисунок 72. Операции для документа

Для списка документов доступно контекстное меню, позволяющее выделить файлы по типу операции (Рисунок 73).

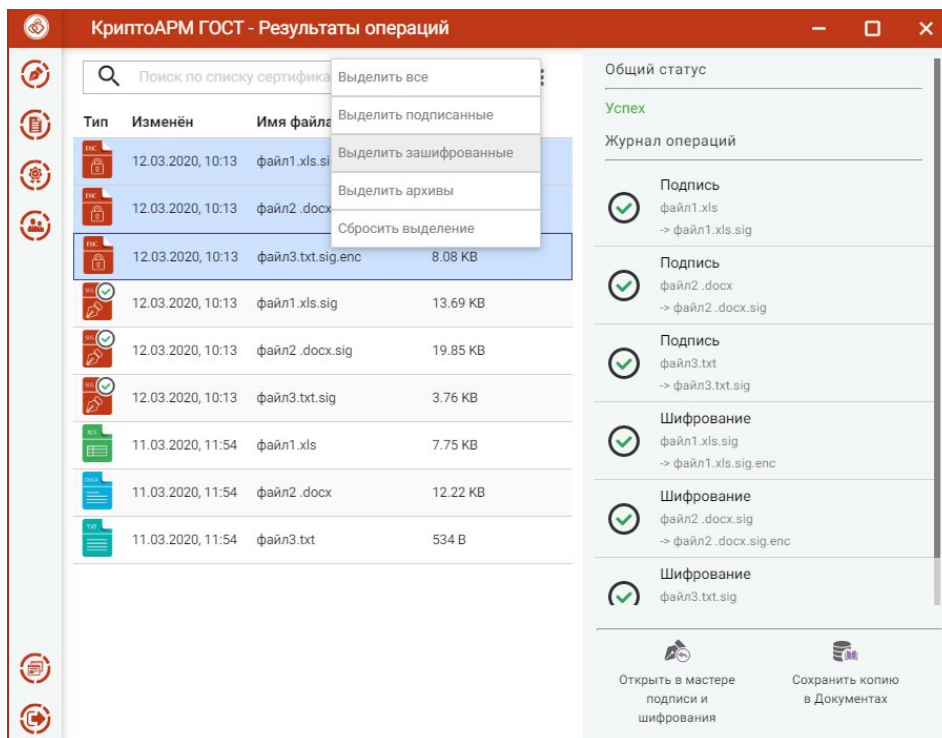


Рисунок 73. Выделение группы файлов по типу файла

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 73). 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**.

3.11.3 Архивирование и шифрование

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

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

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (Рисунок 74).

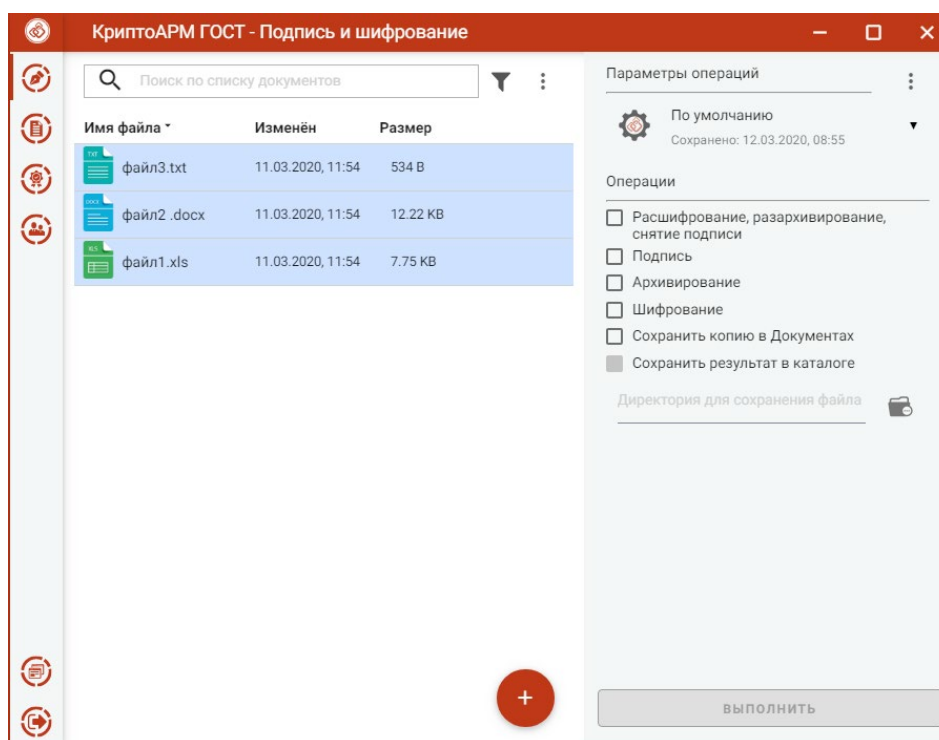


Рисунок 74. Список файлов для операции

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (Рисунок 75).

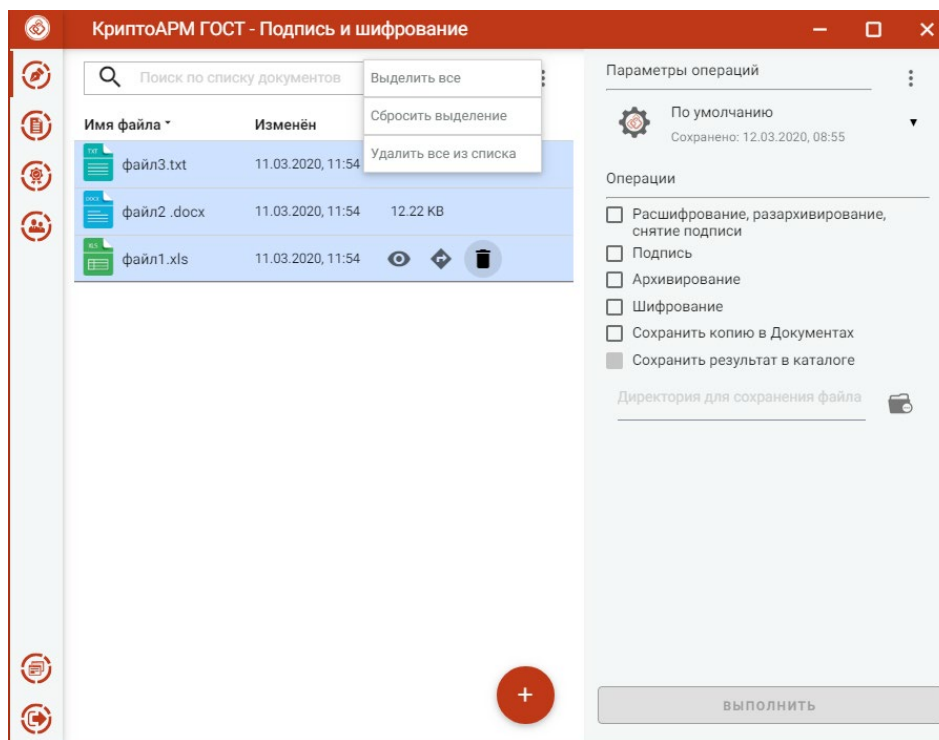


Рисунок 75. Контекстное меню управления списком файлов

УСТАНОВКА ПАРАМЕТРОВ АРХИВИРОВАНИЯ И ШИФРОВАНИЯ. Для операций архивирования и шифрования файлов в разделе **Операции** необходимо выбрать опции **Архивирование** и **Шифрование**, становятся доступны настройки параметров шифрования (Рисунок 76).

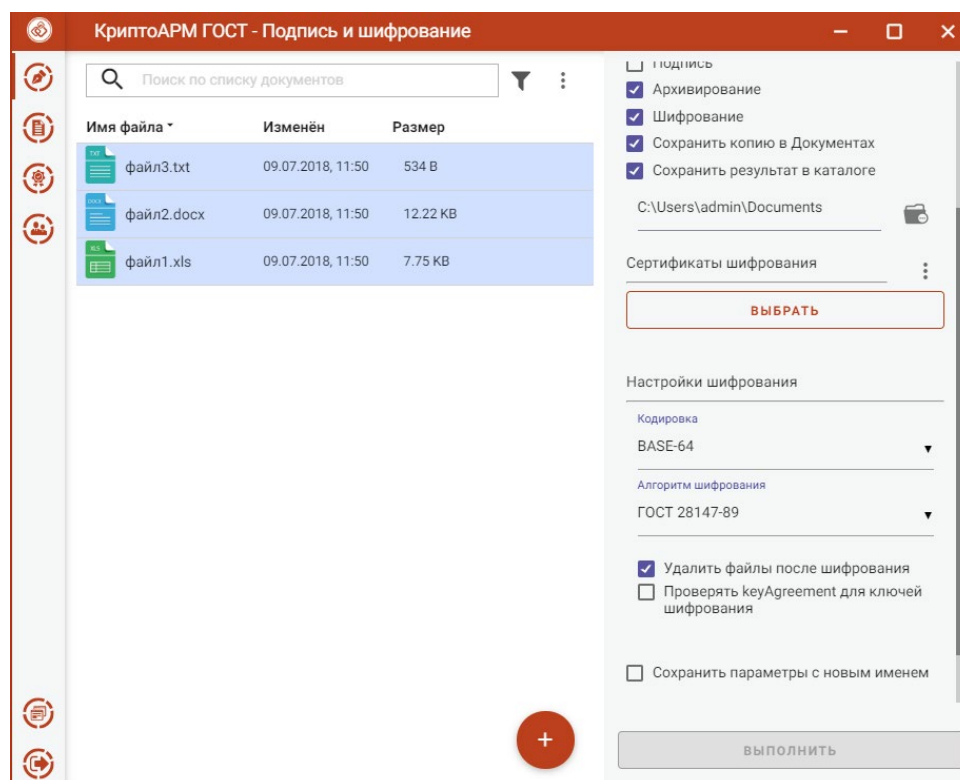


Рисунок 76. Настройка параметров архивирования и шифрования

В параметрах шифрования можно настроить:

- **Сертификаты шифрования** - сертификаты получателей. Выбор производится нажатием кнопки **Выбрать** сертификаты шифрования. В появившемся диалоговом окне отображаются сертификаты категории **Личные** и категории **Сертификаты других пользователей (Контакты)**. В списке сертификатов допускается выбор нескольких сертификатов, так как число получателей может быть различным.
- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнечик».
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции.
- **Проверить keyAgreement для ключей шифрования** - при установленном флаге при операции шифрования в сертификатах проверяется наличие в расширении keyUsage использование ключа keyAgreement (согласование ключей). Если в сертификате нет использования ключа «Согласование ключей», то при включенном флаге операция шифрования в адрес такого сертификата производится не будет. При выключенном флаге шифрование будет выполняться в адрес сертификатов без использования ключа «Согласование ключей».

Внимание: шифрование без установленного флага «Проверить keyAgreement для ключей шифрования» возможно только в тестовых целях.

Можно задать каталог для сохранения полученных документов, выбрав в операциях опцию **Сохранить результат в каталоге**. При установке флага становится доступно поле выбора каталога. Если флаг не установлен, то файл сохраняется рядом с исходным 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 можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте «[Управление параметрами операции](#)».

Архивирование и шифрование файлов. При условии выбора сертификатов получателей, файлов для выполнения операции, в мастере становится доступной кнопка **Выполнить** (Рисунок 77). Подписать и зашифровать можно любые файлы, кроме зашифрованных.

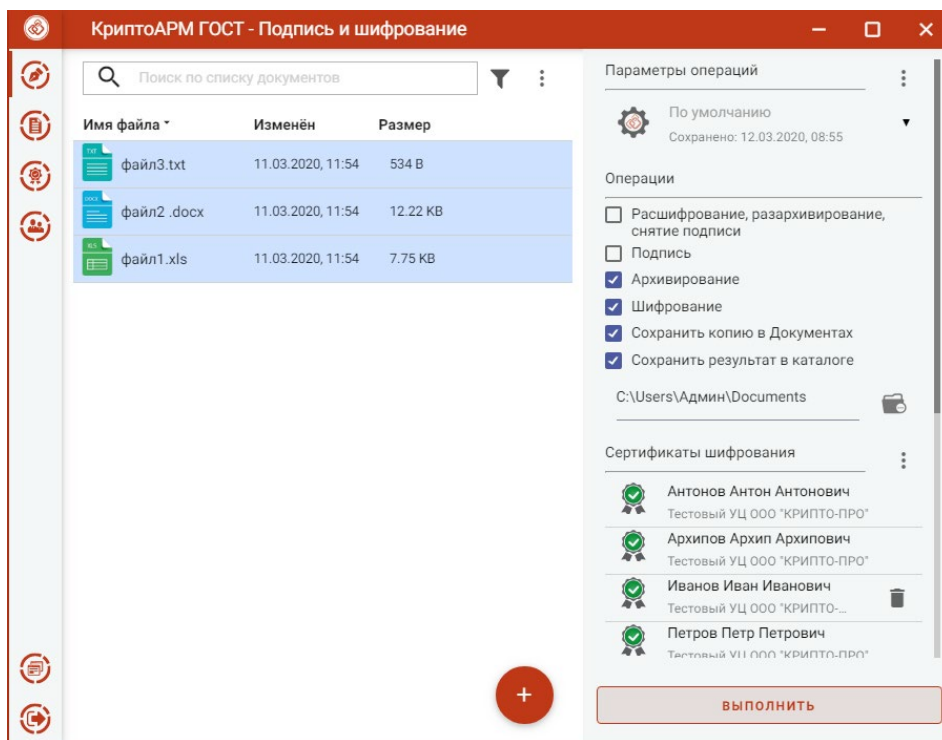


Рисунок 77. Архивирование и шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс архивирования, а затем архив файл шифруется. Исходные документы (оригиналы), архив (промежуточные) и результаты операции шифрования отображаются в отдельном мастере **Результаты операций** (Рисунок 78).

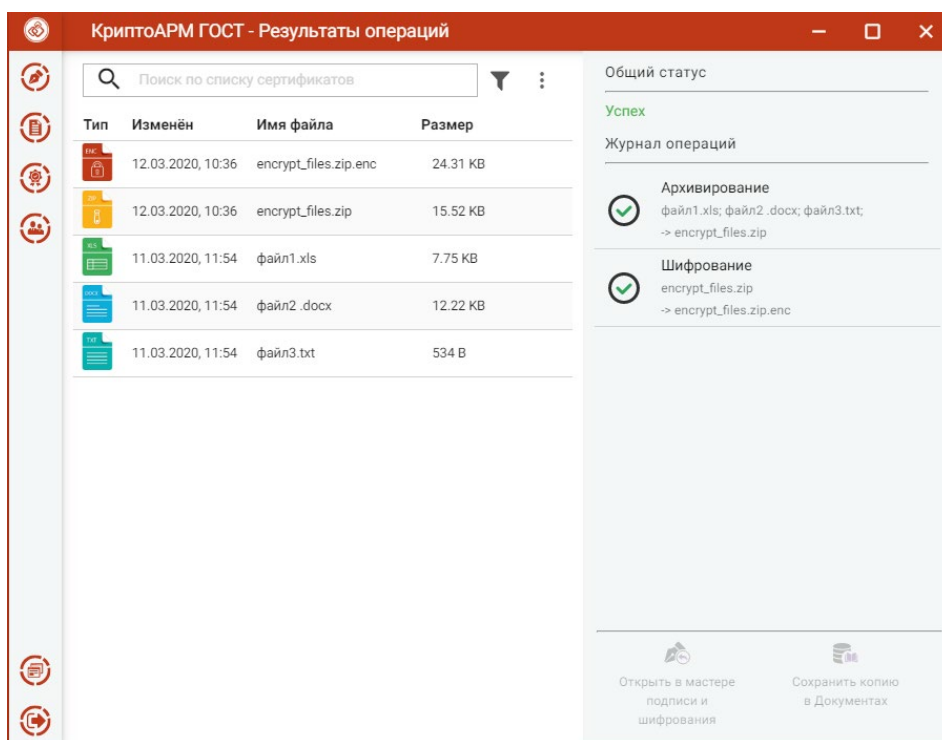


Рисунок 78. Результаты операций

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

Зашифрованный файл сохраняется в каталоге, если в операциях был выбран каталог для сохранения результатов, или рядом с исходными файлами, если в операциях не был

установлен флаг **Сохранить результат в каталоге**. Архив сохраняется во временную папку TEMP, расположенную в домашней папке пользователя в каталоге `./Trusted/CryptoARM GOST/`, и остается до выполнения следующей операции.

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

Если в параметрах шифрования была выбрана опция **Удалить после шифрования**, то в Результатах операции будут только полученный зашифрованный файл.

Для каждого документа доступны операции (Рисунок 79):

- **Просмотр** - выполняется открытие файла через приложение, которое ассоциировано с его расширением. Для зашифрованных файлов данная опция не доступна.
- **Перейти к файлу** - выполняется открытие каталога, в котором располагается файл.

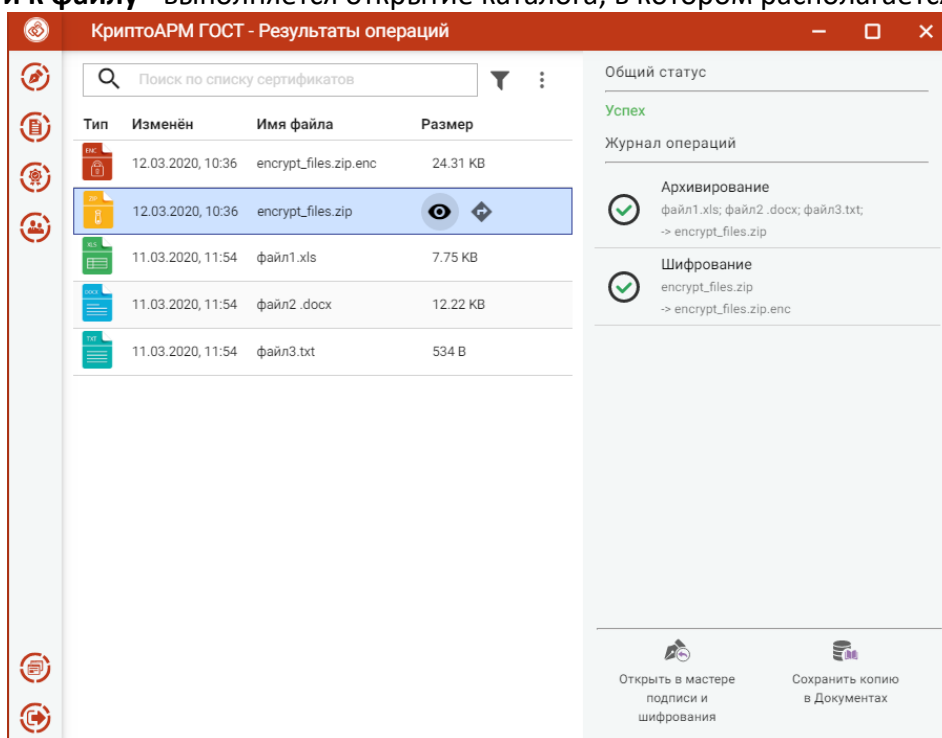


Рисунок 79. Операции для документа

Для списка документов доступно контекстное меню, позволяющее выделить файлы по типу операции (Рисунок 80).

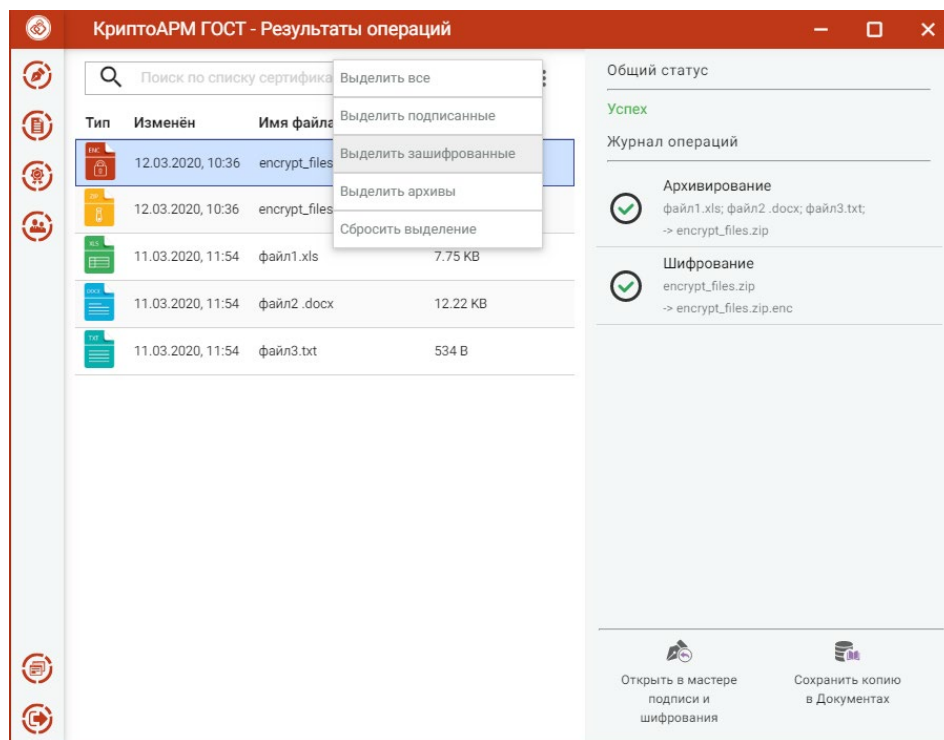


Рисунок 80. Выделение группы файлов по типу файла

Документы из результатов операции можно Открыть в мастере Подписи и шифрования для выполнения других операций или Сохранить копию в Документах (Рисунок 80). 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**.

3.11.4 Подпись, архивирование и шифрование

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

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

Выбранные файлы заносятся в левую область и представляют собой одноуровневый список (Рисунок 81).

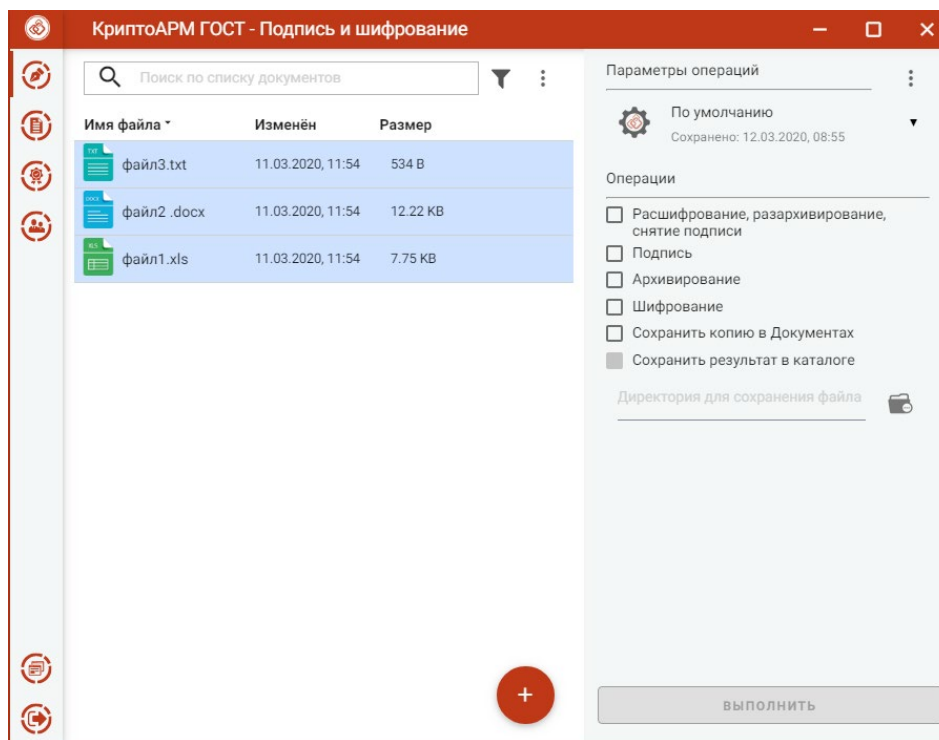


Рисунок 81. Список файлов для операции

Для данного списка доступны поиск, фильтрация, управление файлами в списке через контекстное меню и кнопки для каждого файла (Рисунок 82).

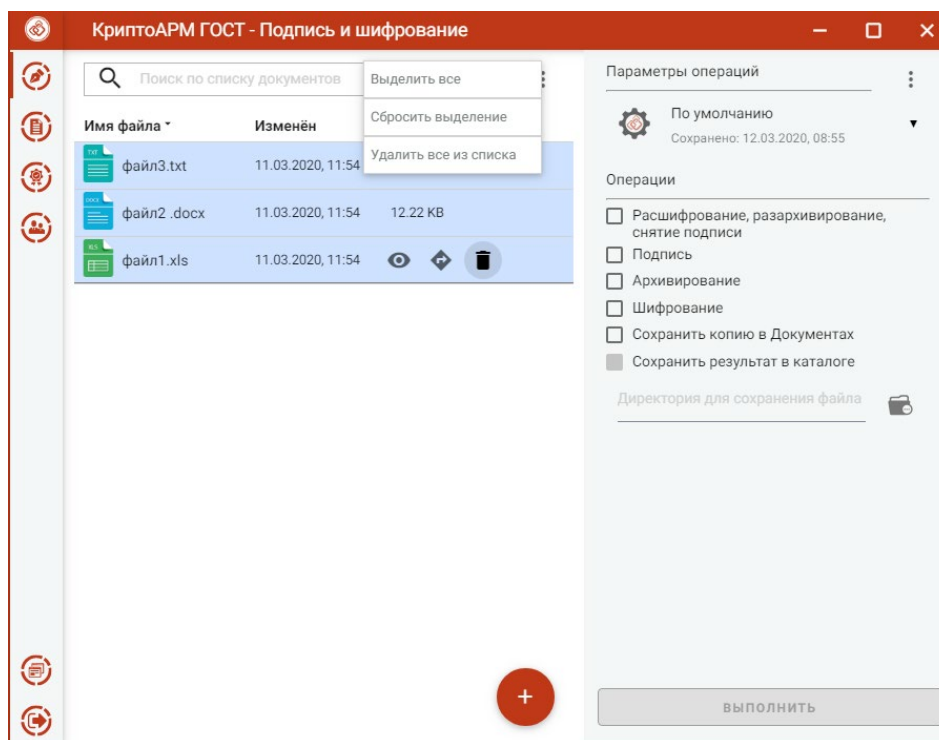


Рисунок 82. Контекстное меню управления списком файлов

УСТАНОВКА ПАРАМЕТРОВ ПОДПИСИ, АРХИВИРОВАНИЯ И ШИФРОВАНИЯ. Для операций подписи, архивирования и шифрования файлов в разделе **Операции** необходимо выбрать опции **Подпись**, **Архивирование** и **Шифрование**, становятся доступны настройки параметров подписи и шифрования (Рисунок 83).

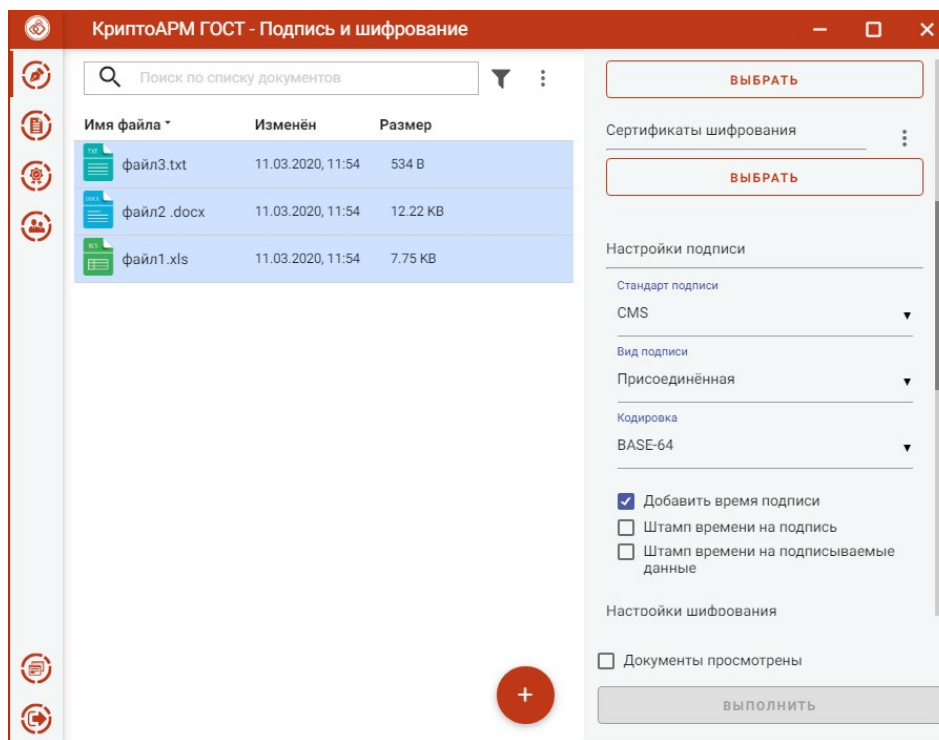


Рисунок 83. Настройка параметров подписи, архивирования и шифрования

В параметрах подписи можно настроить:

- **Сертификат подписи** - сертификат, к которому привязан ключ ЭП. Выбор сертификата производится нажатием кнопки **Выбрать**. В появившемся диалоговом окне отображаются сертификаты категории **Личные**, которые могут использоваться для подписи.
- **Стандарт подписи** – CMS для создания классической подписи или CAdES-X Long Type 1 для создания усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 требуется заполнить поля в разделе **Служба штампов времени (TSP)** (подробнее о создании усовершенствованной подписи в пункте «[Создание усовершенствованной подписи](#)»). Стандарт подписи CAdES-X Long Type 1 доступен только при установленном модуле КриптоПро TSP Client 2.0 и КриптоПро OCSP Client 2.0.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Добавить время подписи** - при установленном флажке в подпись сохраняется время (системное) подписи.
- **Добавлять штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.
- **Добавлять штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При установке флага требуется заполнить поля в разделе **Служба штампов времени** (подробно о создании подписи со штампом описано в пункте «[Создание подписи со штампом времени](#)»). Данная опция доступна только при установленном модуле КриптоПро TSP Client 2.0.

В параметрах шифрования можно настроить:

- **Сертификаты шифрования** - сертификаты получателей. Выбор производится нажатием кнопки **Выбрать** сертификаты шифрования. В появившемся диалоговом окне отображаются сертификаты категории **Личные** и категории **Сертификаты других пользователей (Контакты)**. В списке сертификатов допускается выбор нескольких сертификатов, так как число получателей может быть различным.
- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: «ГОСТ 28147-89», «ГОСТ Р 34.12-2015 Магма», «ГОСТ Р 34.12-2015 Кузнечик».
- **Удалить файлы после шифрования** - исходные файлы, над которыми выполняется операция шифрования, удаляются из файловой системы в случае успешного завершения операции.
- **Проверить keyAgreement для ключей шифрования** - при установленном флаге при операции шифрования в сертификатах проверяется наличие в расширении keyUsage использование ключа keyAgreement (согласование ключей). Если в сертификате нет использования ключа «Согласование ключей», то при включенном флаге операция шифрования в адрес такого сертификата производится не будет. При выключенном флаге шифрование будет выполняться в адрес сертификатов без использования ключа «Согласование ключей».

Внимание: шифрование без установленного флага «Проверить keyAgreement для ключей шифрования» возможно только в тестовых целях.

Можно задать каталог для сохранения полученных документов, выбрав в операциях опцию **Сохранить результат в каталоге**. При установке флага становится доступно поле выбора каталога. Если флаг не установлен, то файл сохраняется рядом с исходным 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 можно сохранить и использовать при последующих запусках приложения. Процесс сохранения и изменения параметров описан в пункте [«Управление параметрами операции»](#).

Подпись, архивирование и шифрование файлов. При условии выбора сертификата подписи, сертификатов получателей, файлов для выполнения операции и установленного флага, что документы просмотрены, в мастере становится доступной кнопка **Выполнить** (Рисунок 84). Подписать, заархивировать и зашифровать можно любые файлы, кроме зашифрованных.

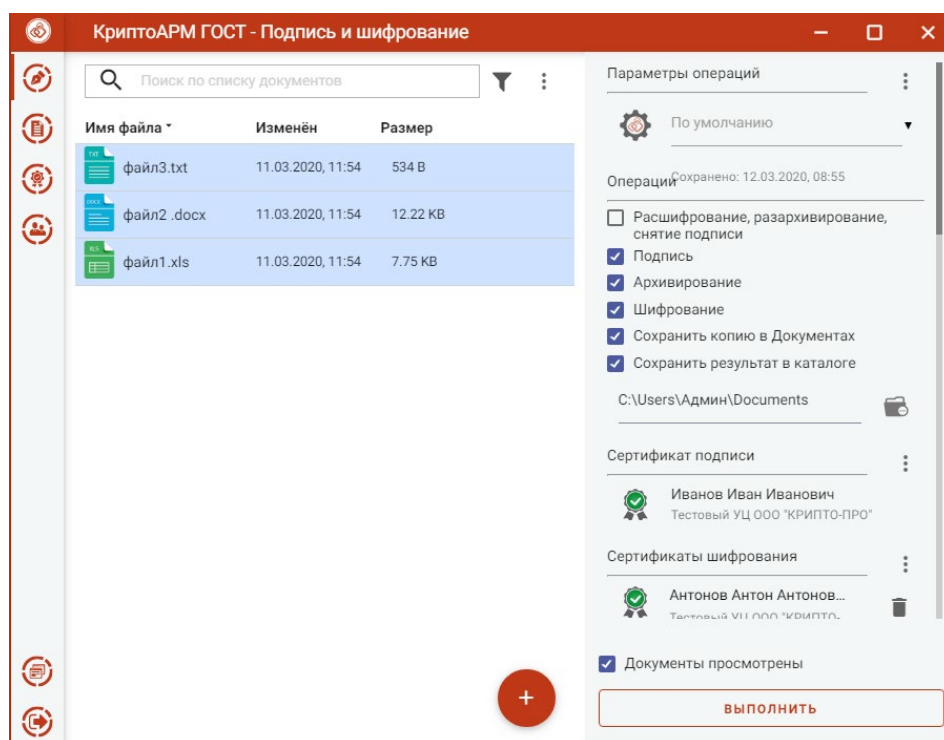


Рисунок 84. Подпись, архивирование и шифрование файлов

Нажатие на кнопку **Выполнить** запускает процесс подписи, затем подписанный файл архивируется, потом архив шифруется. Исходные документы (оригиналы), подписанные файлы и архив (промежуточные) и результаты операции шифрования отображаются в отдельном мастере **Результаты операций** (Рисунок 85).

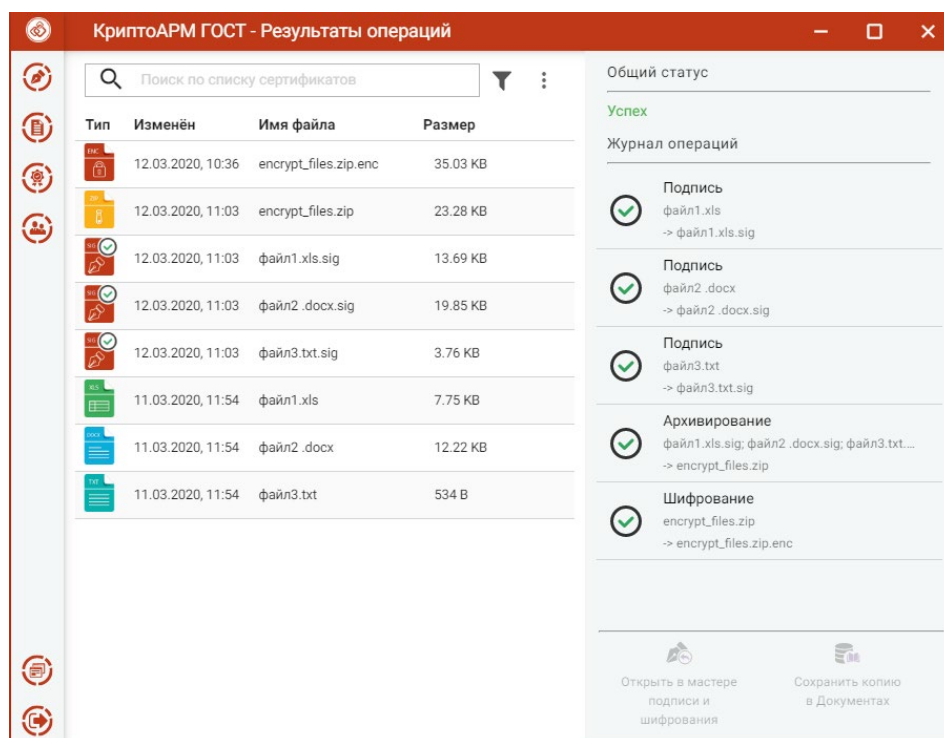


Рисунок 85. Результаты операций

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

Зашифрованные файлы сохраняются в каталоге, если в операциях был выбран каталог для сохранения результатов, или рядом с исходными файлами, если в операциях не был установлен флаг **Сохранить результат в каталоге**.

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

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

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

Для подписанных файлов подпись проверяется автоматически.

Для каждого документа доступны операции (Рисунок 86):

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

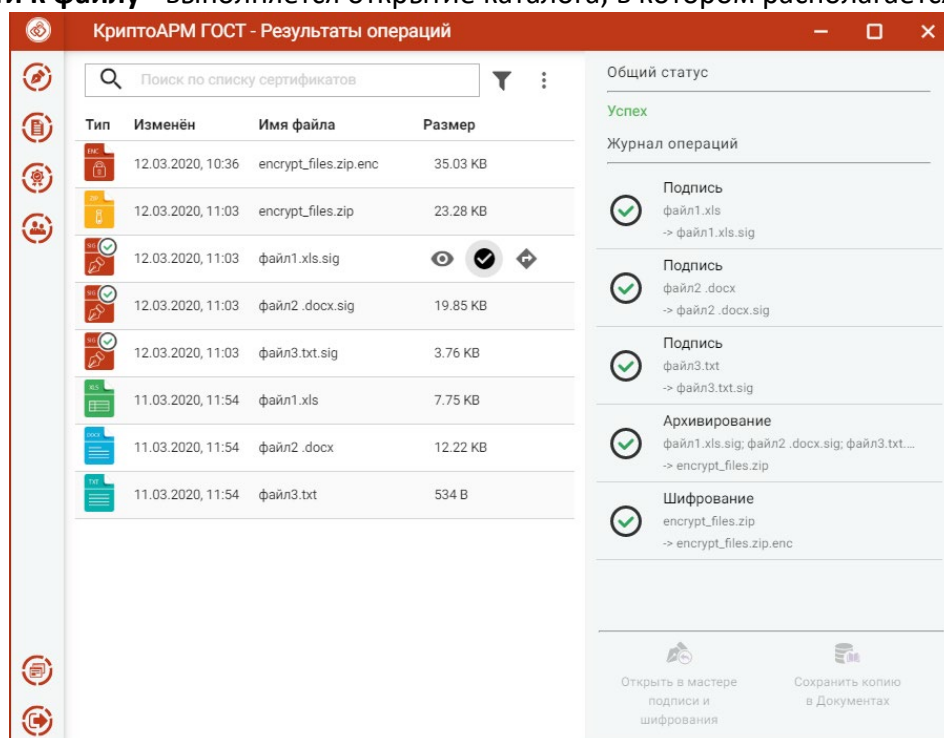


Рисунок 86. Операции для документа

Для списка документов доступно контекстное меню, позволяющее выделить файлы по типу операции (Рисунок 87).

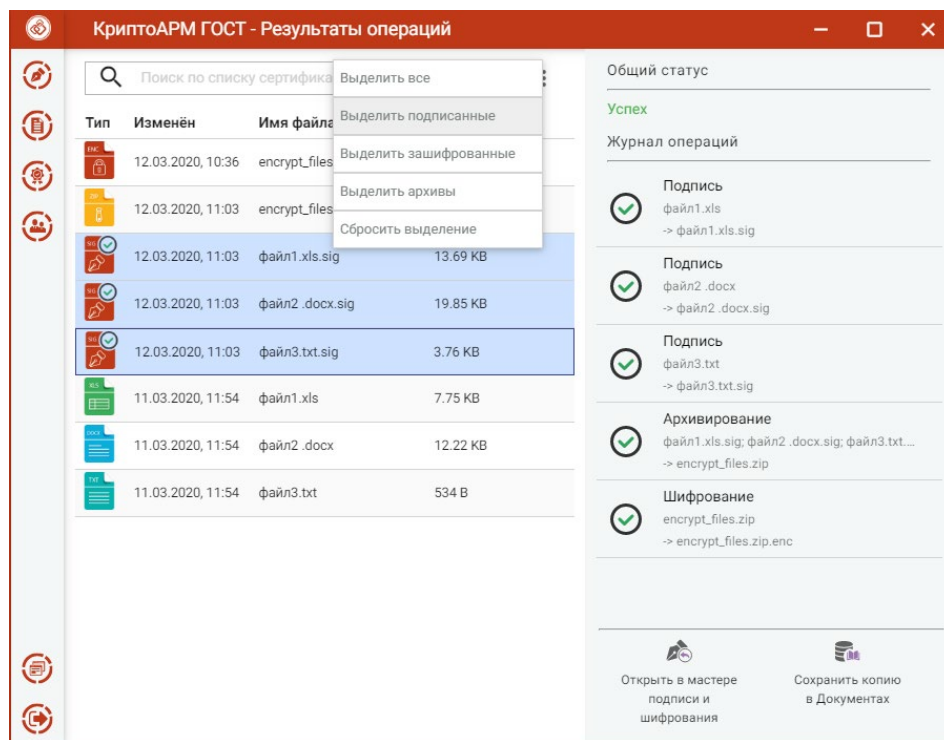


Рисунок 87. Выделение группы файлов по типу файла

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 87). 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**.

3.12 ОБРАТНЫЕ ГРУППОВЫЕ ОПЕРАЦИИ (РАСШИФРОВАНИЕ, РАЗАРХИВИРОВАНИЕ, СНЯТИЕ ПОДПИСИ)

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

3.12.1 РАСШИФРОВАНИЕ И РАЗАРХИВИРОВАНИЕ ФАЙЛОВ

Для расшифрования и разархивирования достаточно выбрать зашифрованные архивы - файлы с расширением `.zip.enc`, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить** (Рисунок 88). Настройка дополнительных параметров для операции не требуется.

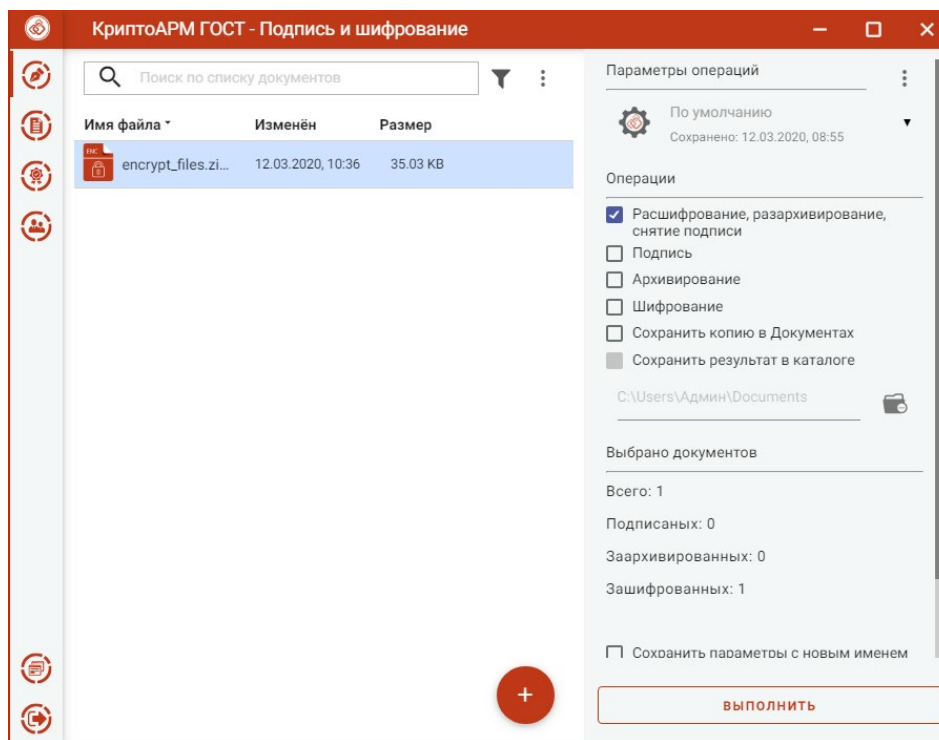


Рисунок 88. Расшифрование и разархивирование файлов

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций** (Рисунок 89).

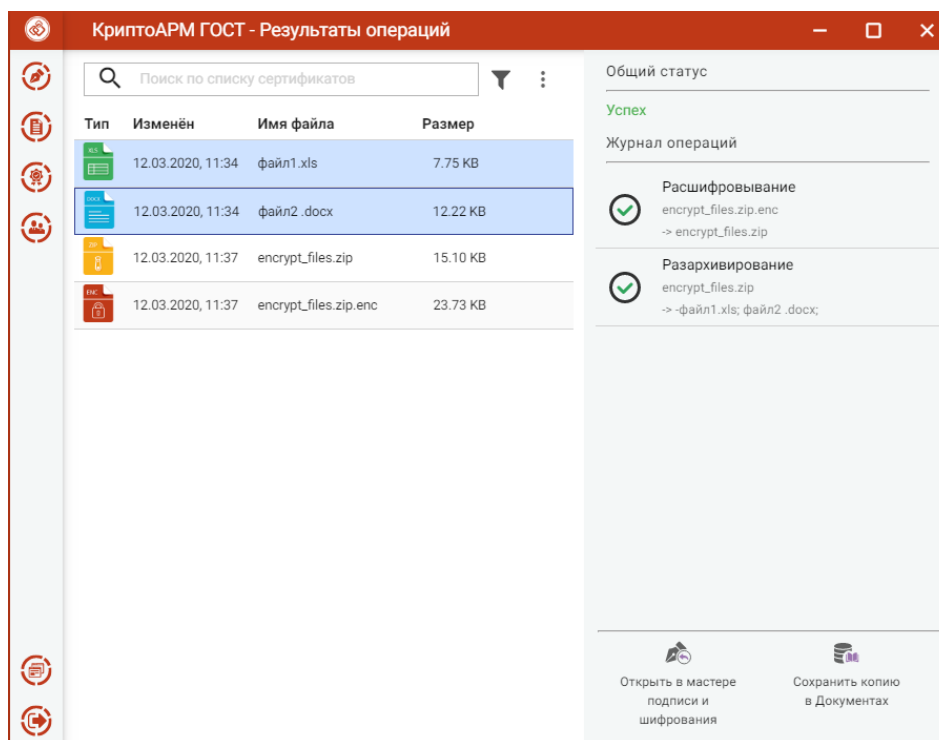


Рисунок 89. Результаты расшифрования и разархивирования файлов

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

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 89). 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**.

3.12.2 РАСШИФРОВАНИЕ И СНЯТИЕ ПОДПИСИ С ФАЙЛОВ

Для расшифрования и снятия подписи достаточно выбрать подписанные и зашифрованные файлы - файлы с расширением **.sig.ens**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить** (Рисунок 90). Настройка дополнительных параметров для операции не требуется.

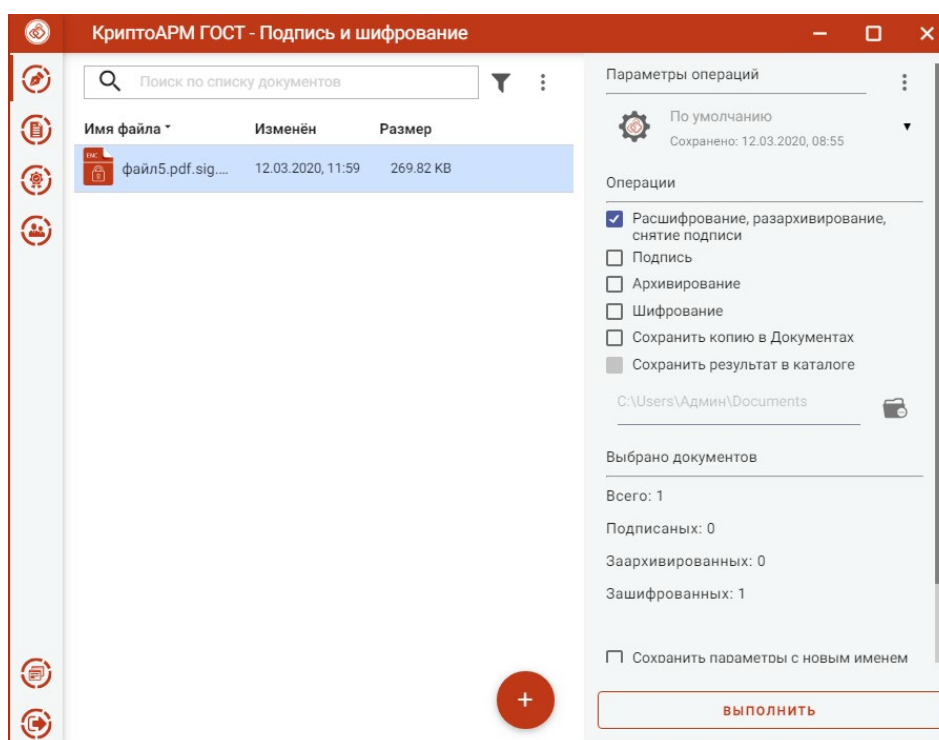


Рисунок 90. Расшифрование и снятие подписи

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере Результаты операций (Рисунок 91).

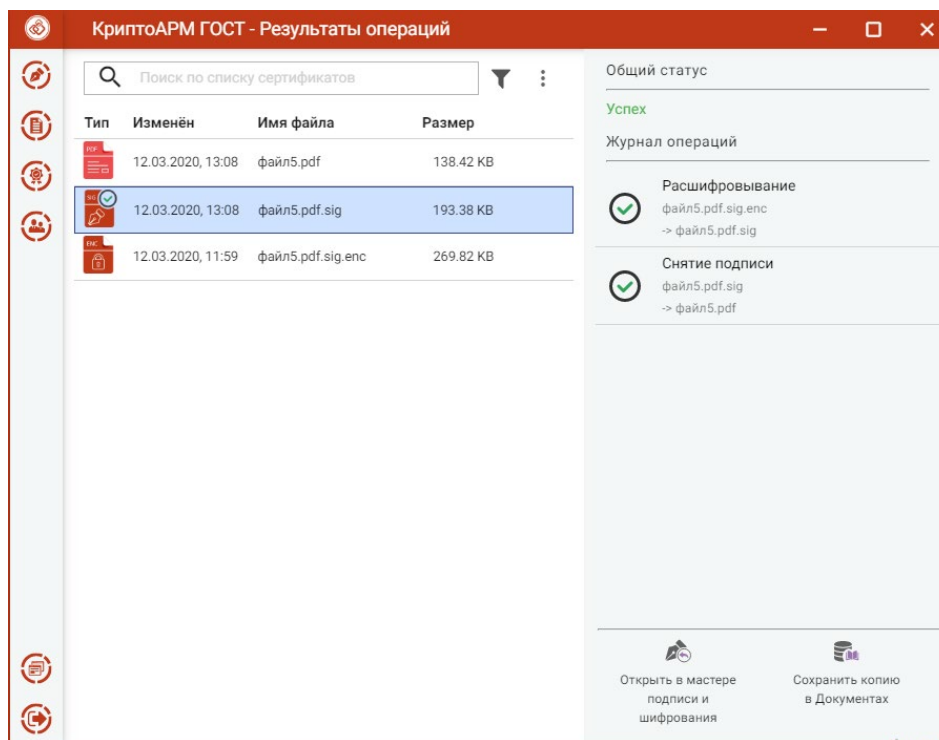


Рисунок 91. Результаты расшифрования и снятия подписи

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

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 91). 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**.

3.12.3 РАЗАРХИВИРОВАНИЕ И СНЯТИЕ ПОДПИСИ

Для разархивирования и снятия подписи достаточно выбрать подписанные и заархивированные файлы - файлы с расширением **.sig.zip**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить** (Рисунок 92). Если несколько подписанных файлов были упакованы в архив, то выбирается архивный файл с расширением **.zip**.

Настройка дополнительных параметров для операции не требуется.

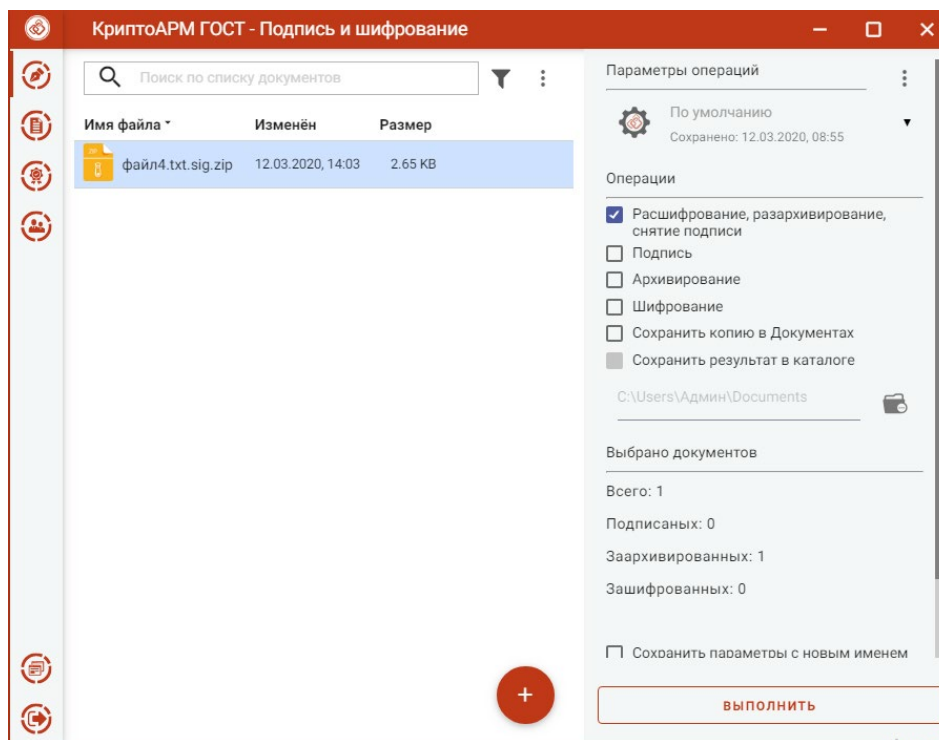


Рисунок 92. Разархивирование и снятие подписи

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций** (Рисунок 93).

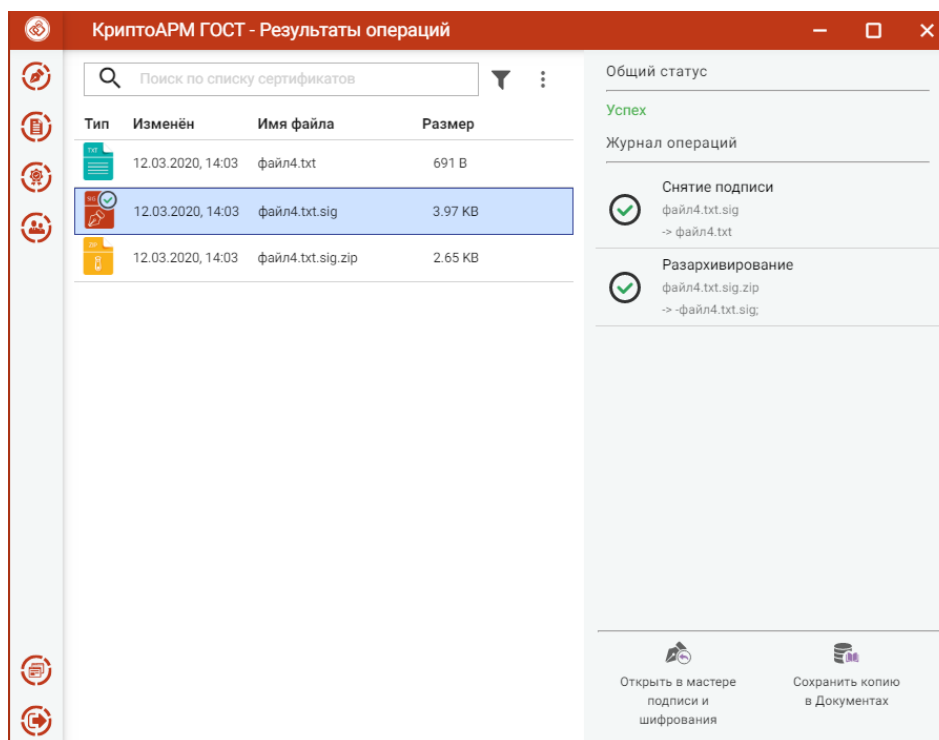


Рисунок 93. Результаты разархивирования и снятия подписи

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

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 93). 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**.

3.12.4 РАСШИФРОВАНИЕ, РАЗАРХИВИРОВАНИЕ И СНЯТИЕ ПОДПИСИ

Для расшифрования, разархивирования и снятия подписи достаточно выбрать зашифрованный архив подписанного файла - файл с расширением **.sig.zip.enc**, выбрать операцию **Расшифрование, разархивирование, снятие подписи** и нажать на кнопку **Выполнить** (Рисунок 94). Если несколько подписанных файлов были упакованы в архив и зашифрованы, то выбирается зашифрованный архив с расширением **.zip.enc**.

Настройка дополнительных параметров для операции не требуется.

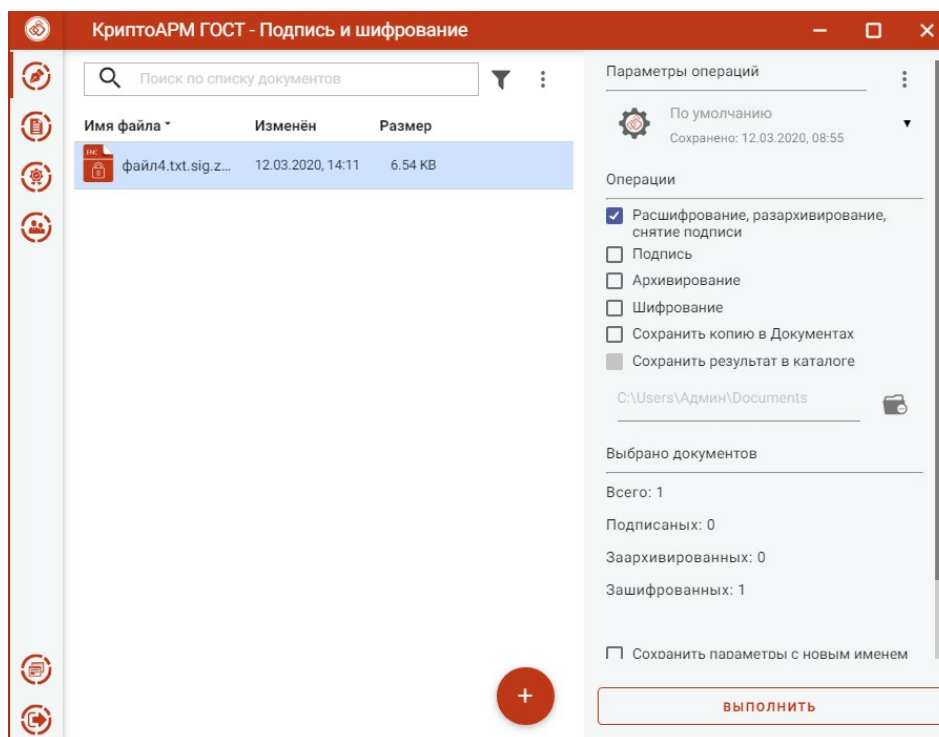


Рисунок 94. Расшифрование, разархивирование и снятие подписи

Исходные зашифрованные и полученные файлы отображаются в отдельном мастере **Результаты операций** (Рисунок 95).

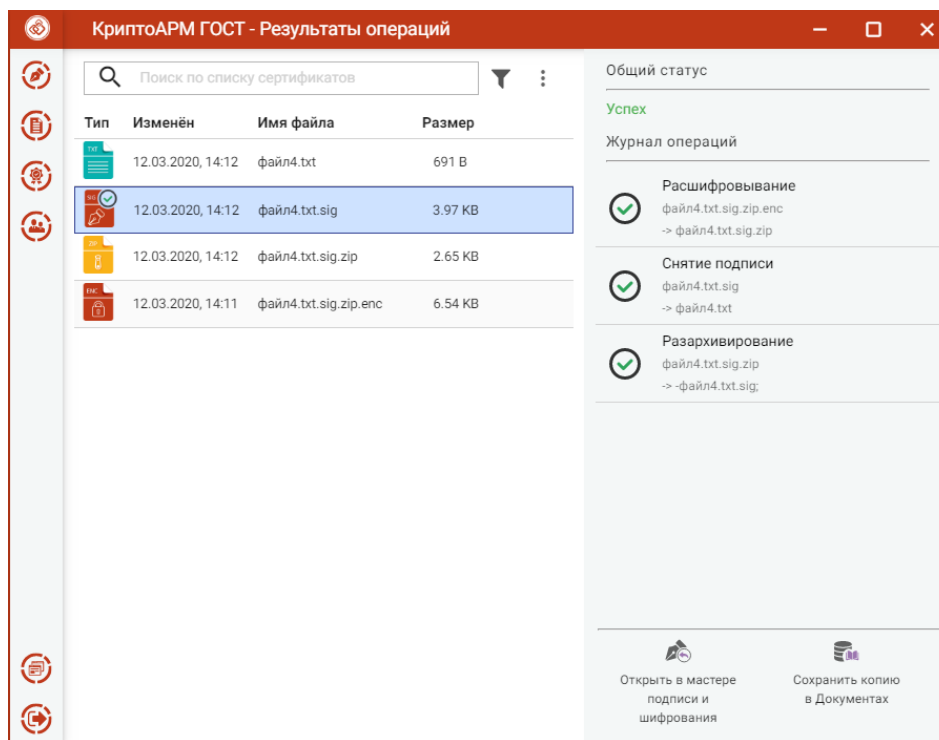


Рисунок 95. Результаты расшифрования, разархивирования и снятия подписи

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

Документы из результатов операции можно **Открыть в мастере Подписи и шифрования** для выполнения других операций или **Сохранить копию в Документах** (Рисунок 95). 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**.

3.13 УПРАВЛЕНИЕ СПИСКОМ ФАЙЛОВ ДЛЯ ВЫПОЛНЕНИЯ ОПЕРАЦИЙ

Список файлов для выполнения операций представляет собой одноуровневый список (Рисунок 96).

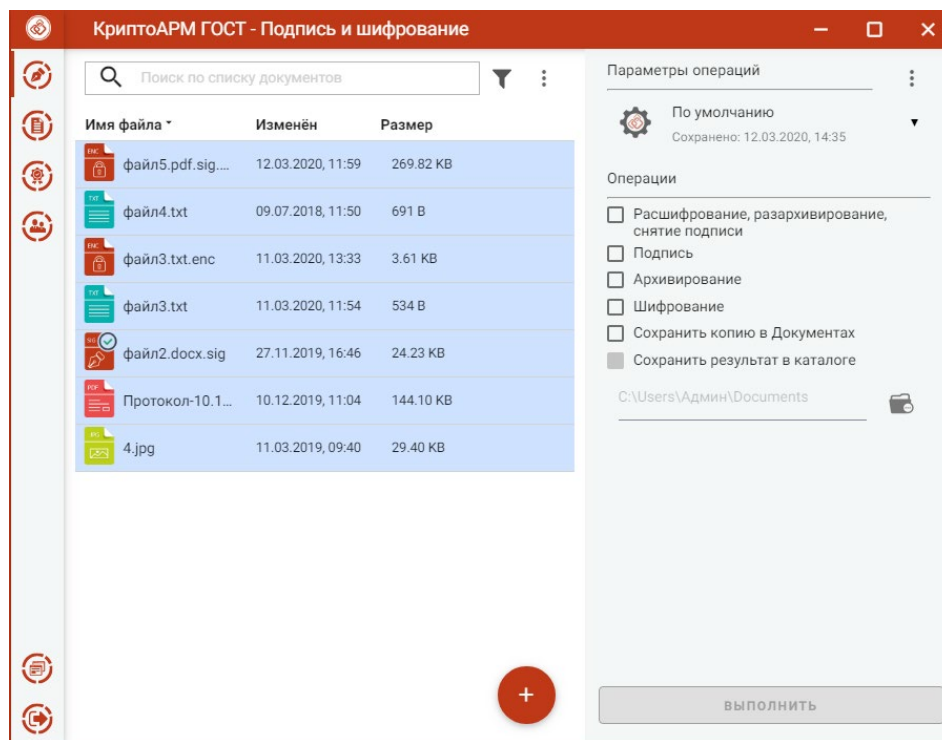


Рисунок 96. Список файлов

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

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

Для списка доступно контекстное меню (Рисунок 97), состоящее из пунктов:

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

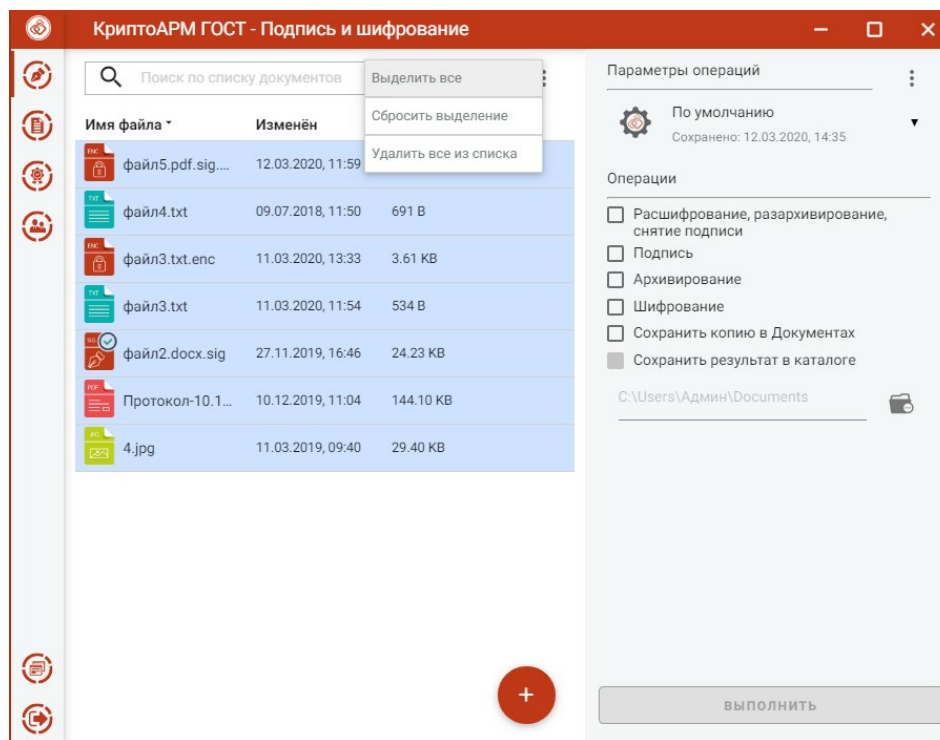


Рисунок 97. Контекстное меню списком файлов

Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши (Рисунок 98):

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

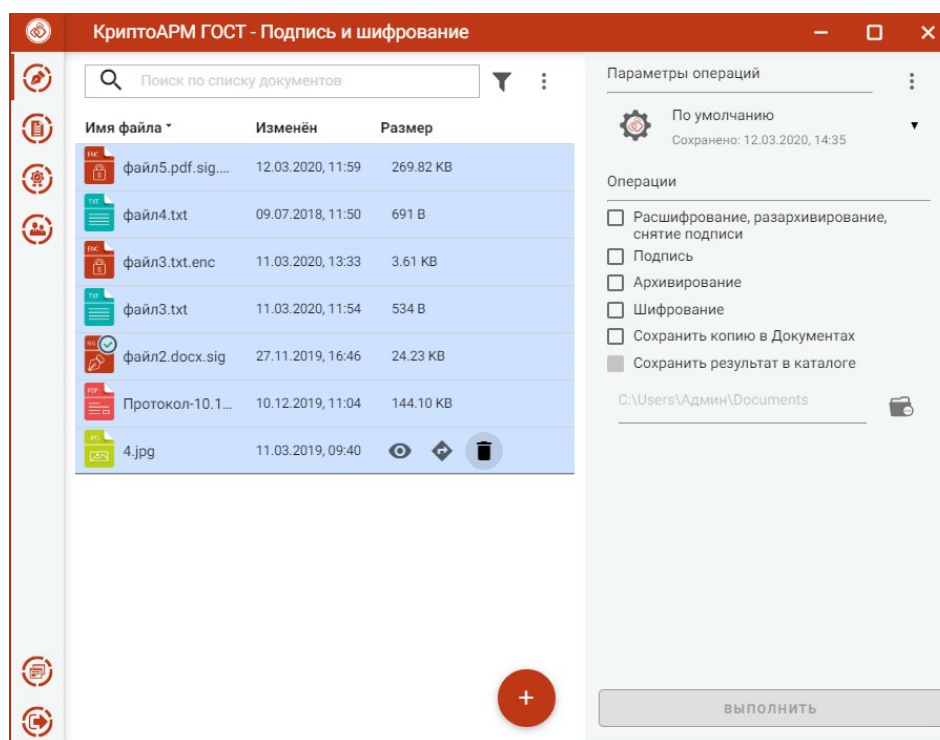


Рисунок 98. Кнопки операций файла

В приложении реализован поиск файлов по символьному совпадению (Рисунок 99)

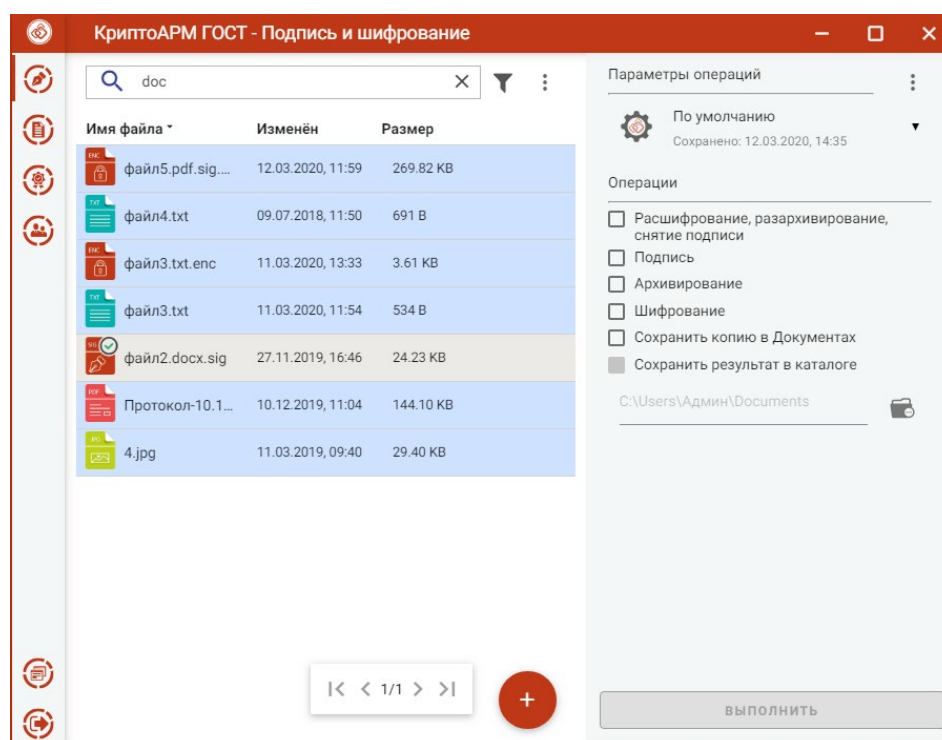


Рисунок 99. Поиск файлов

Список файлов можно отфильтровать, задав настройки фильтрации (Рисунок 100).

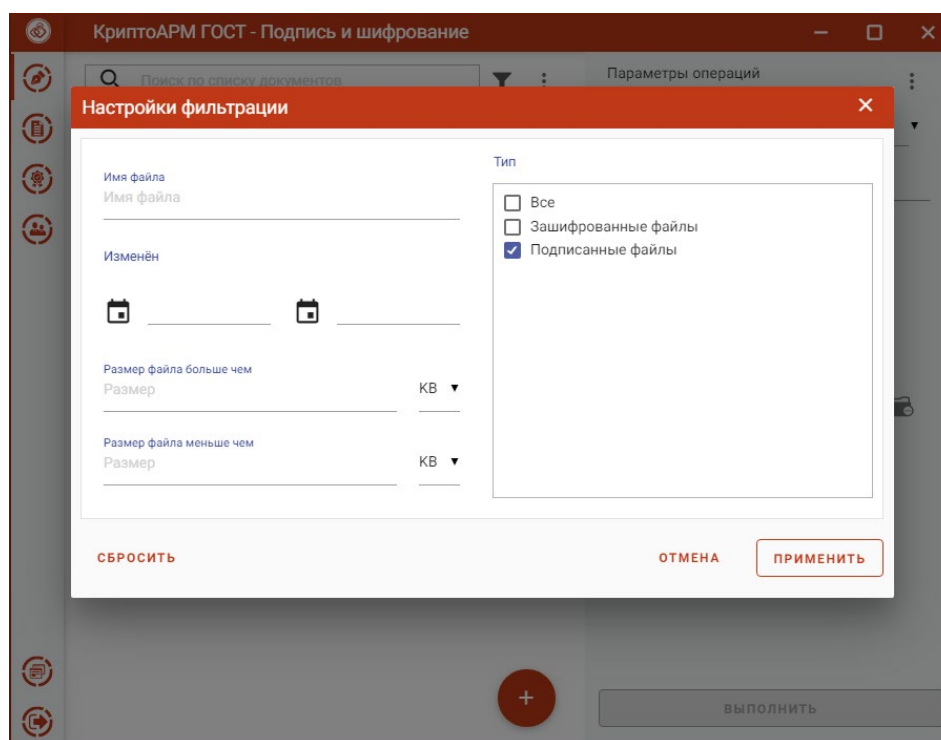


Рисунок 100. Настройки критериев фильтра файлов

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

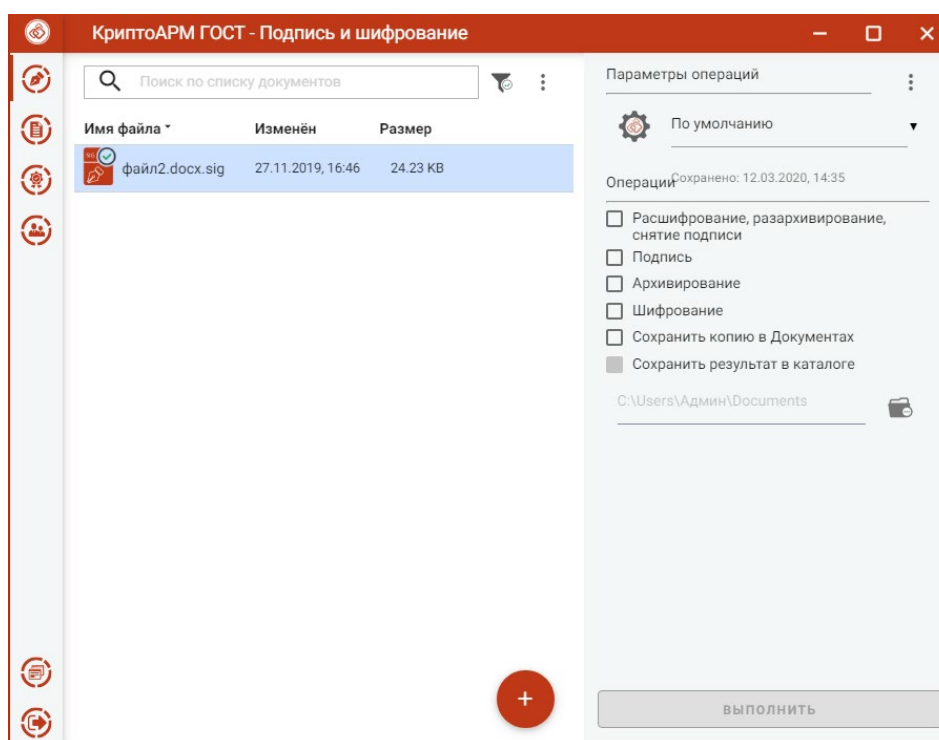


Рисунок 101 Результат применения фильтрации файлов

Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации (Рисунок 100).

3.14 УПРАВЛЕНИЕ ПАРАМЕТРАМИ ОПЕРАЦИИ

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 (Рисунок 102).

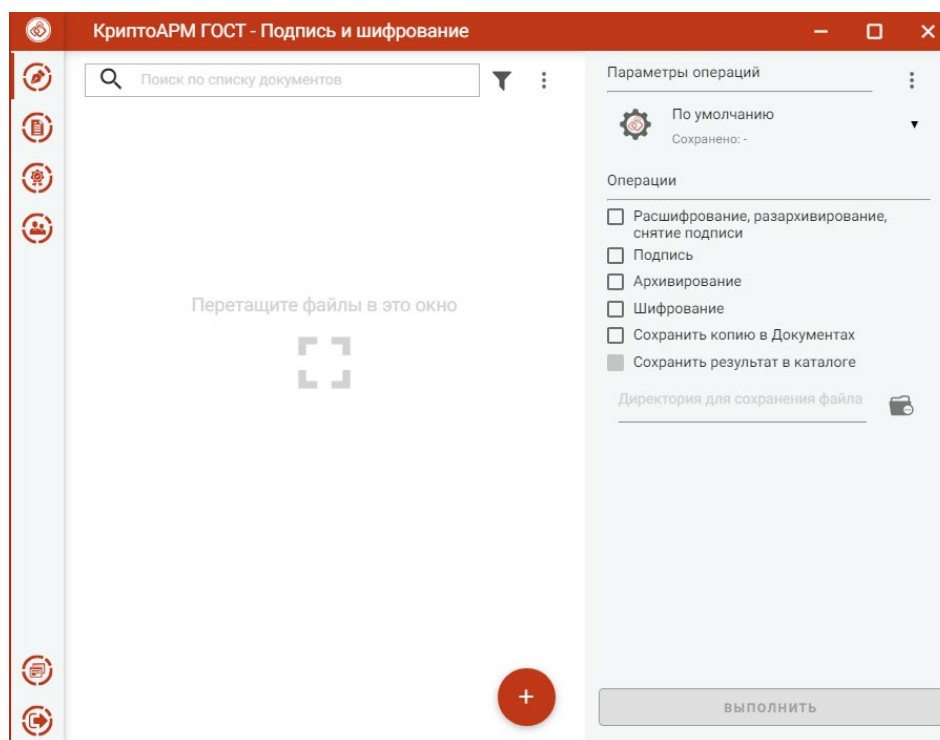


Рисунок 102. Параметры операций по умолчанию

При любом изменении опции операций или параметров операции становится доступна кнопка сохранения изменений **Сохранить параметры** (Рисунок 103).

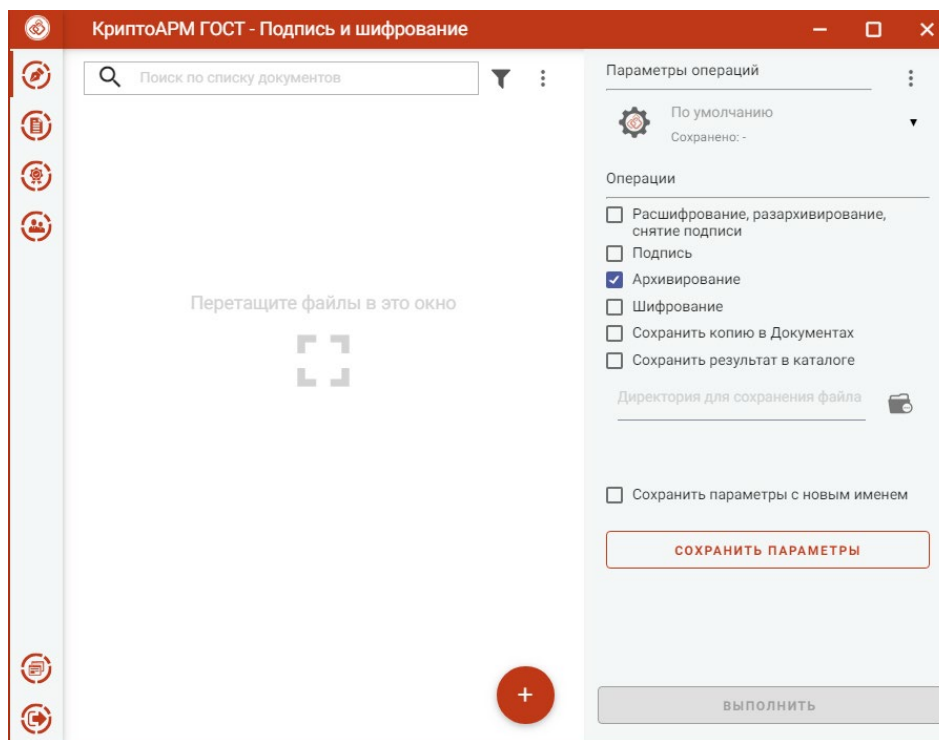


Рисунок 103. Кнопка сохранения изменений параметров операций

При нажатии на кнопку происходит сохранение выбранных параметров в текущие параметры операций. Кнопка **Сохранить параметры** скрывается до изменений (Рисунок 104).

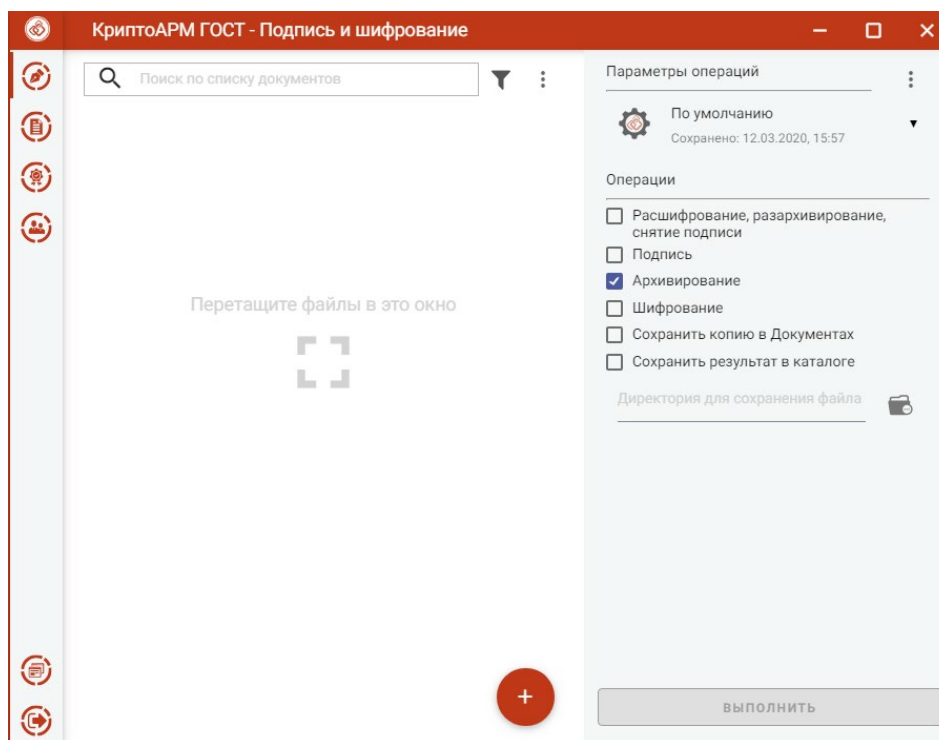


Рисунок 104. Сохранение изменений в текущие параметры операций

Если выбрать опцию **Сохранить параметры с новым именем** и нажать кнопку **Сохранить параметры**, то открывается окно ввода названия параметров операций (Рисунок 105).

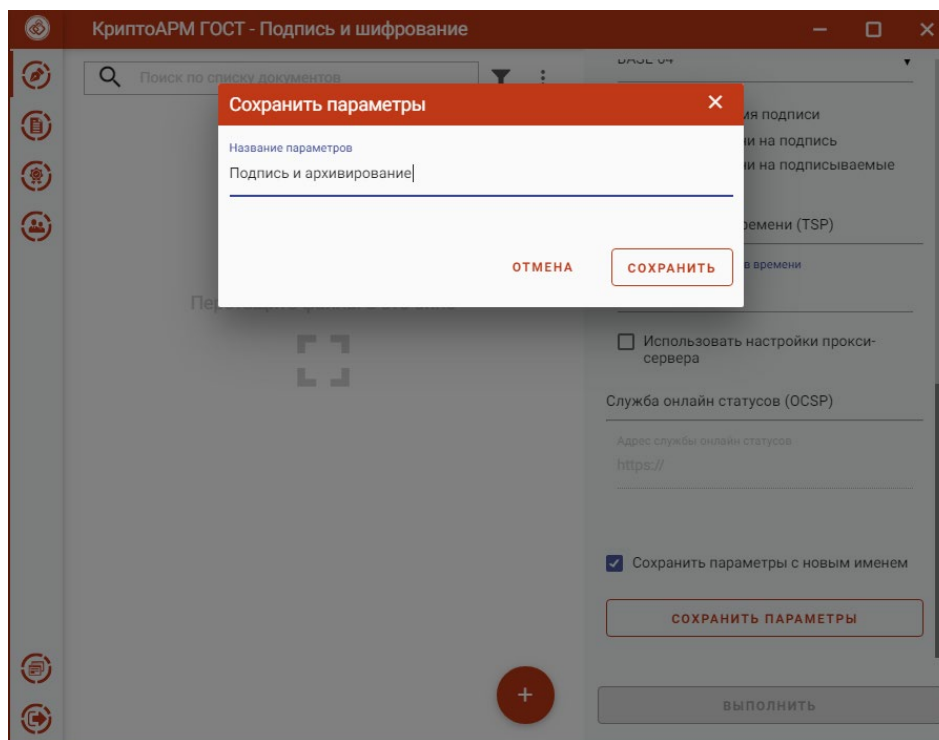


Рисунок 105. Задание названия параметров операций

По кнопке **Сохранить** происходит сохранение выбранных параметров в параметры операций с заданным именем. Выбрать параметры операций можно в выпадающем списке из ранее сохраненных параметров (Рисунок 106).

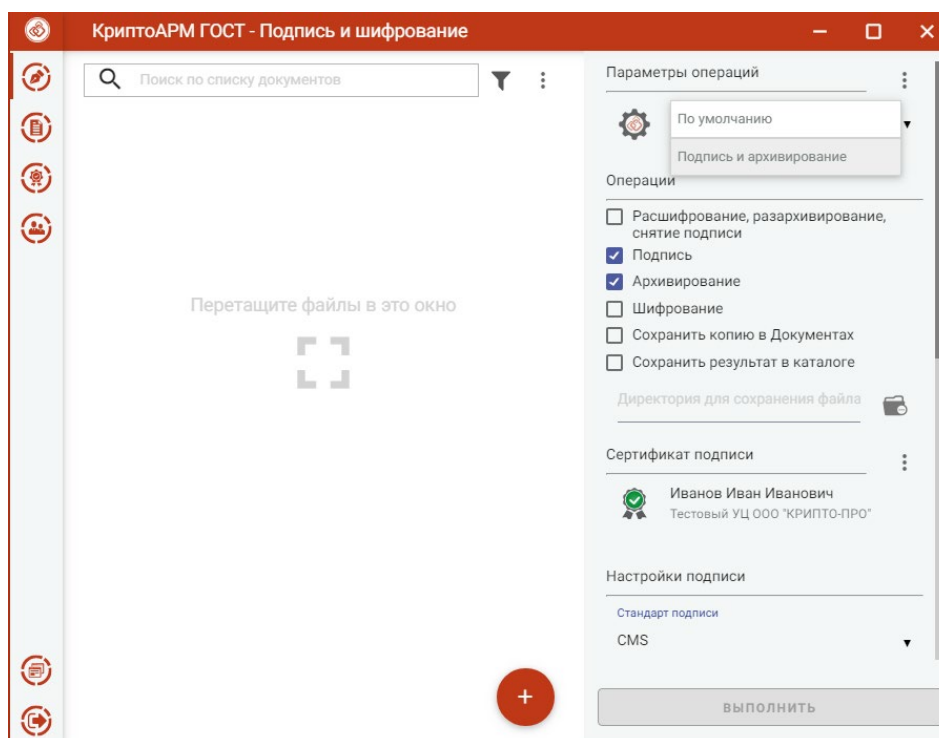


Рисунок 106. Выбор параметров операций

Можно настроить несколько параметров операций и выбирать нужные из списка (Рисунок 107).

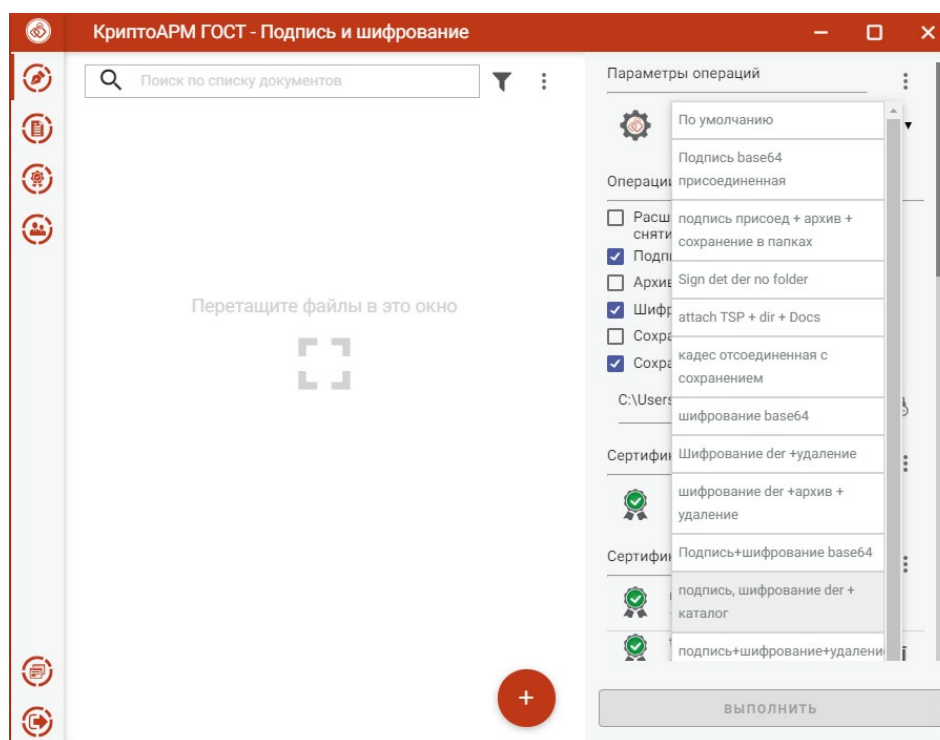


Рисунок 107. Выбор сохраненных параметров операций

Параметры операций можно переименовать или удалить через контекстное меню Параметров операций (Рисунок 108).

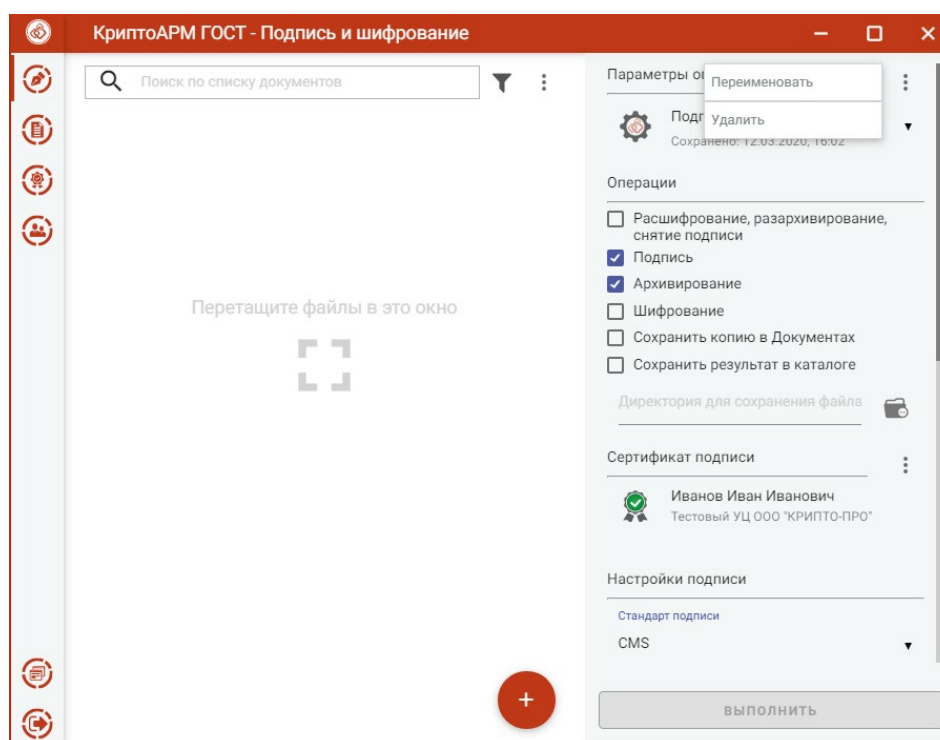


Рисунок 108. Контекстное меню параметров операций

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 (Рисунок 109).

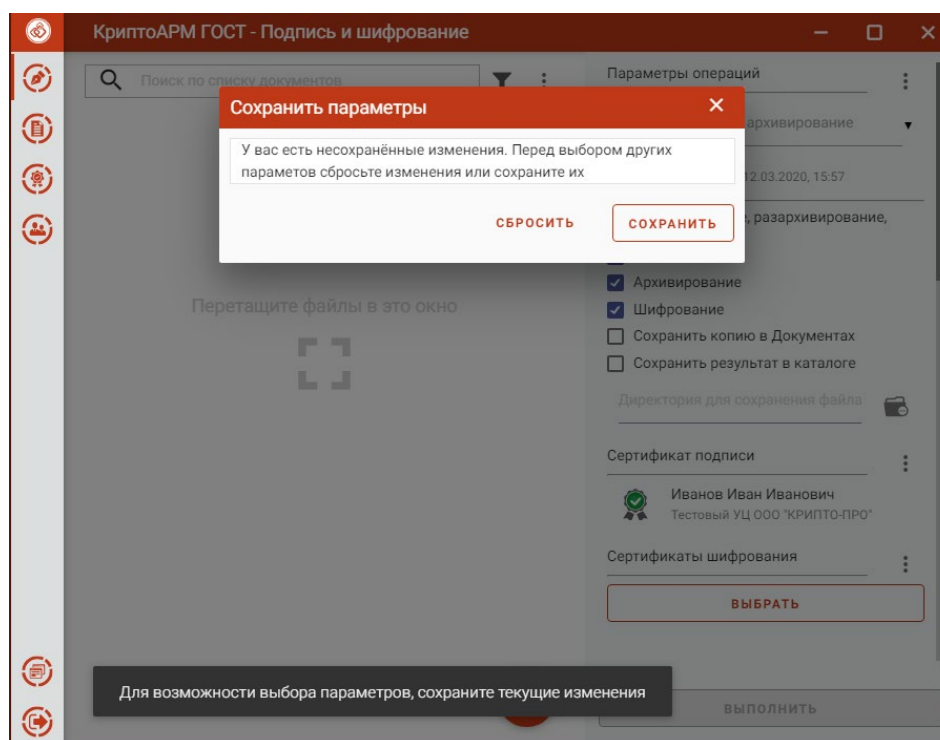


Рисунок 109. Предложение сохранить изменения в параметрах

3.15 Документы

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** (Рисунок 110).

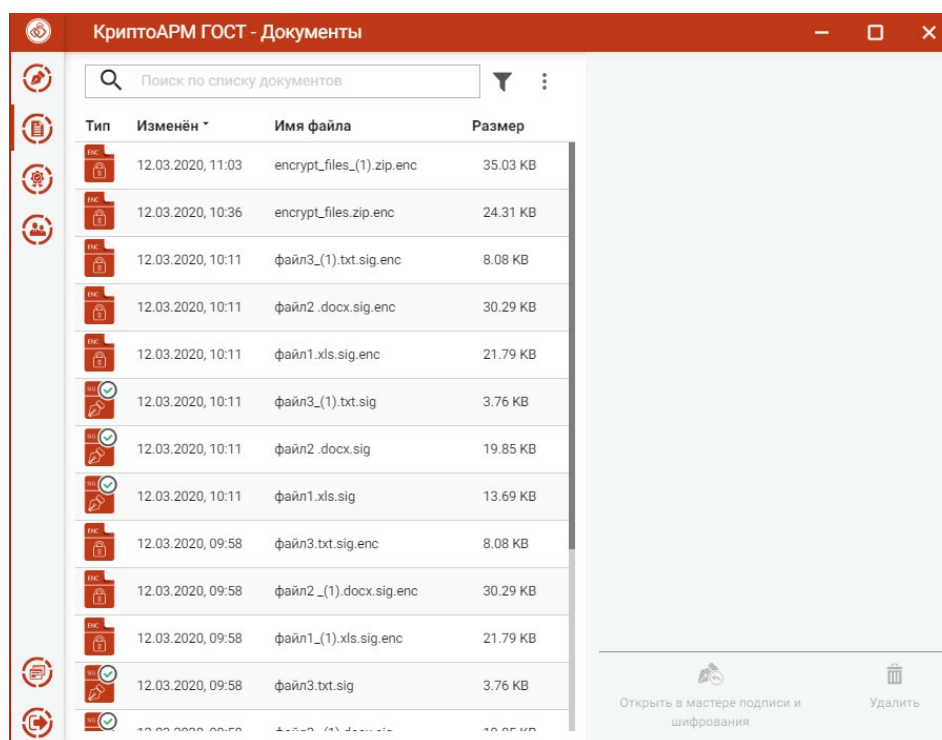


Рисунок 110. Список документов

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

Для списка доступно контекстное меню (Рисунок 111), 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.

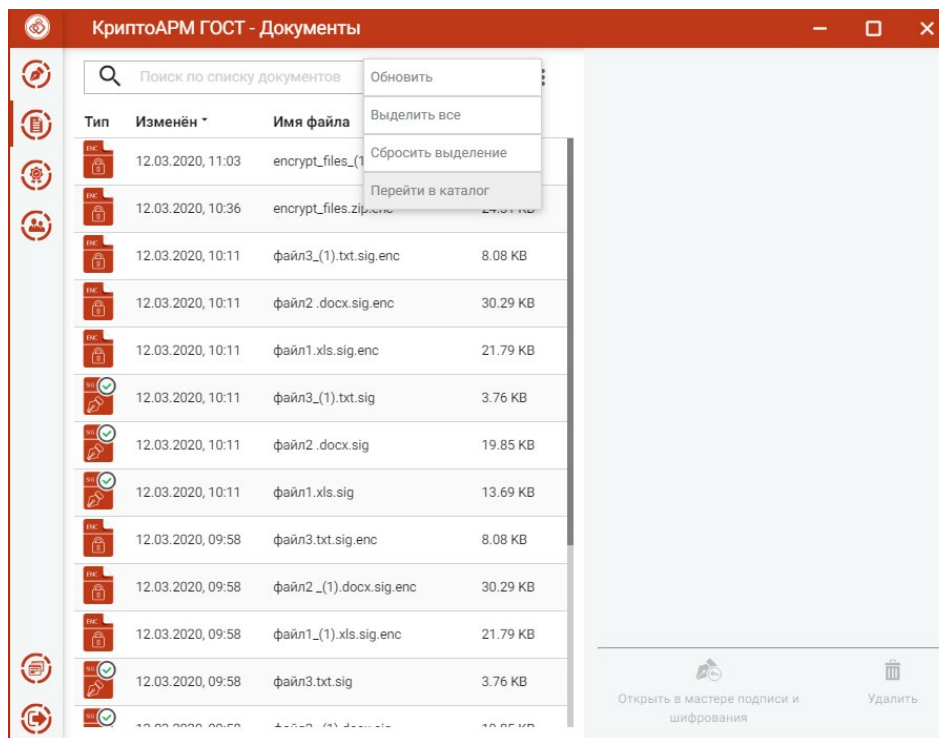


Рисунок 111. Контекстное меню списка Документов

Для каждого файла списка доступны кнопки операции, всплывающие при наведении на файл курсором мыши (Рисунок 112):

- **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.

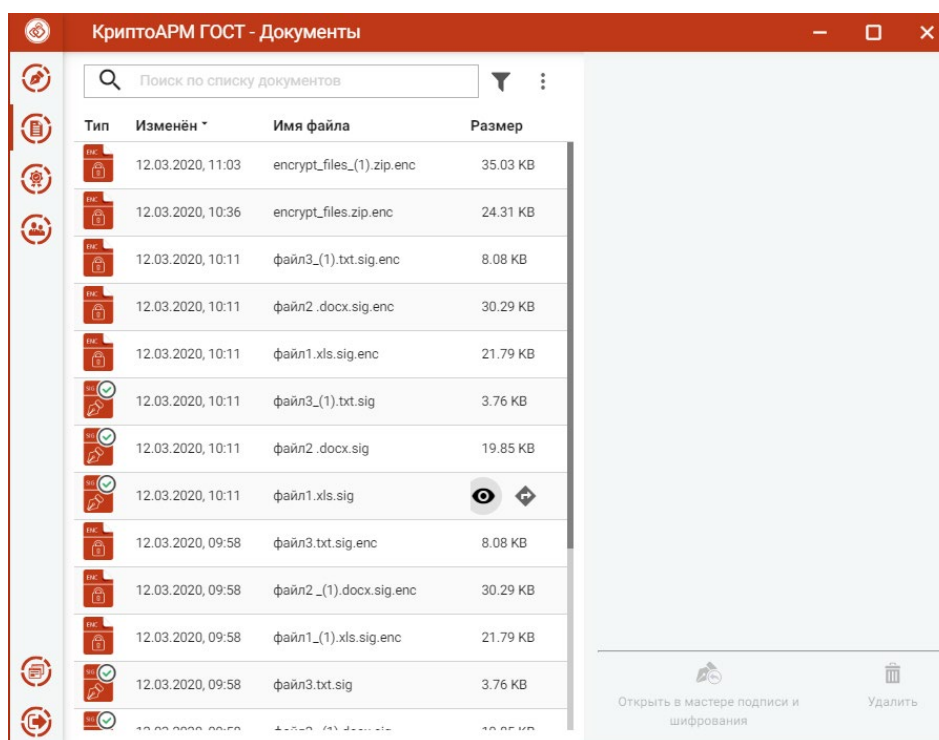


Рисунок 112. Кнопки операций документа

В приложении реализован поиск документов по символьному совпадению (Рисунок 113)

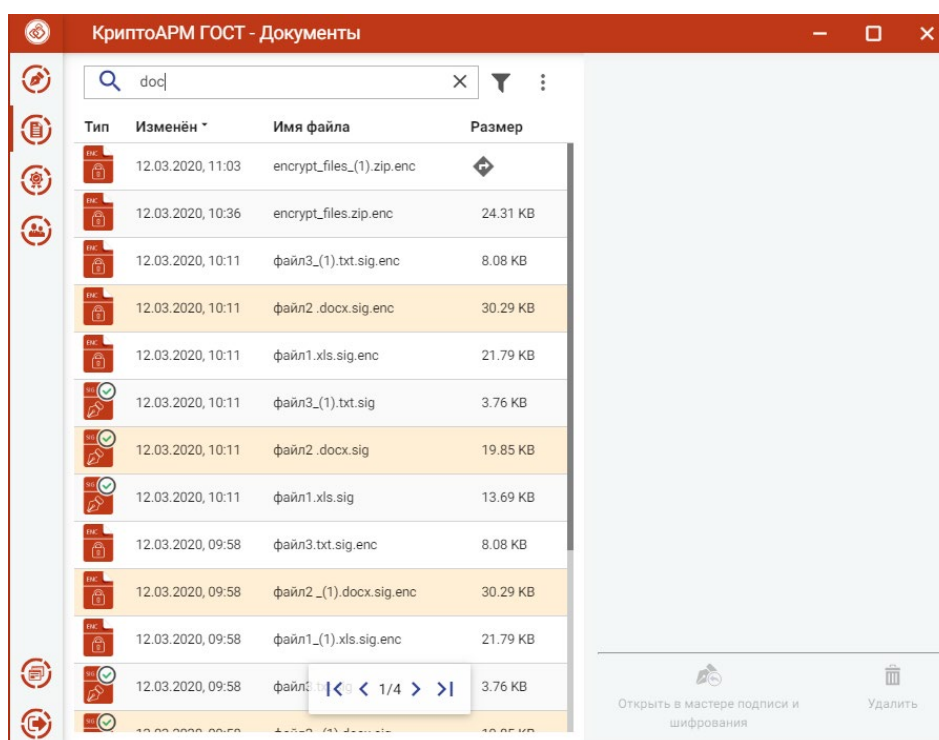


Рисунок 113. Поиск документов

Список документов можно отфильтровать, задав настройки фильтрации (Рисунок 114).

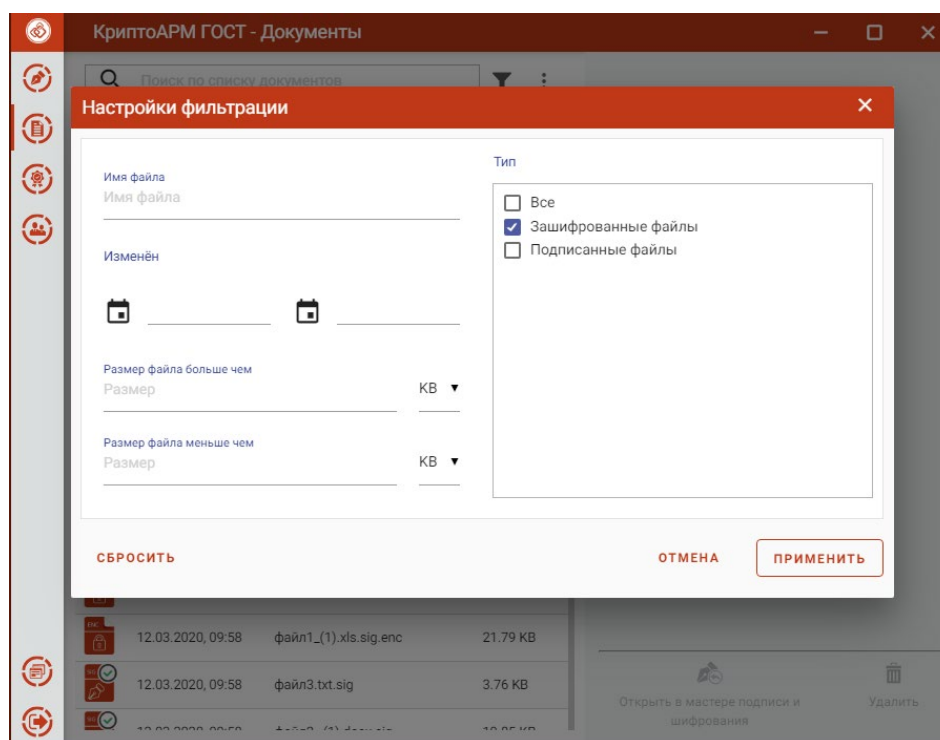


Рисунок 114. Настройки критериев фильтра документов

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

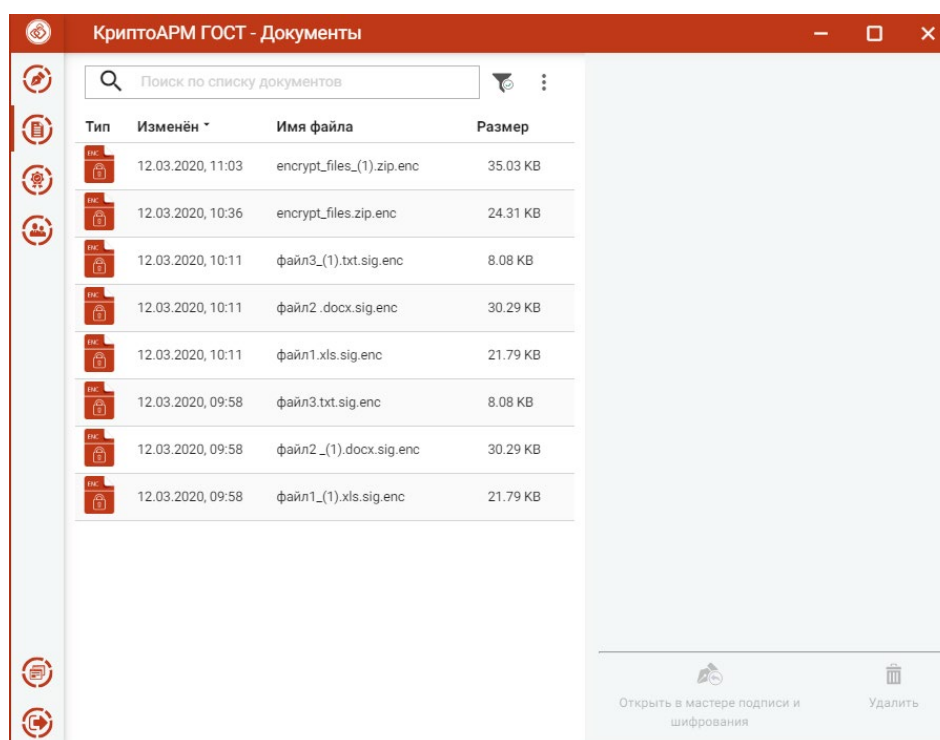


Рисунок 115. Результат применения фильтрации документов

Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации (Рисунок 114).

Для списка файлов в разделе **Документы** доступны операции (Рисунок 116):

- **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\`.

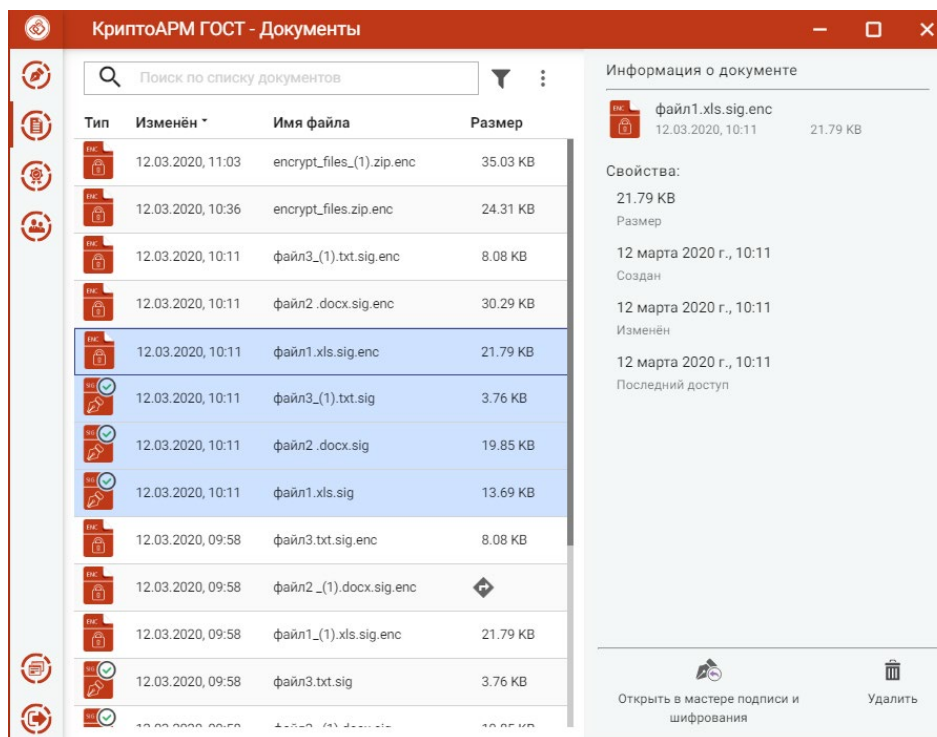


Рисунок 116. Доступные операции для документов

При выделении документов в списке в правой области отображается информация о последнем выделенном документе (Рисунок 116).

Для подписанных файлов отображается информация о подписи (Рисунок 117).

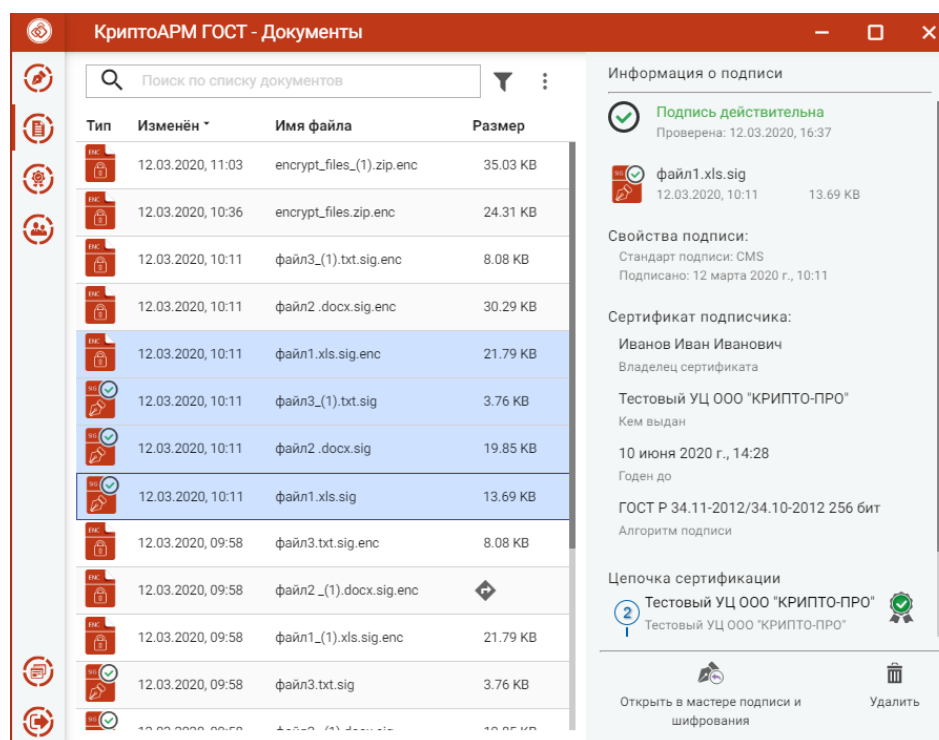


Рисунок 117. Информация о подписи

3.16 СЕРТИФИКАТЫ

Для управления сертификатами в приложении добавлен отдельный пункт меню **Сертификаты**. При выборе данного пункта открывается список личных сертификатов и подменю с категориям сертификатов (Рисунок 118).

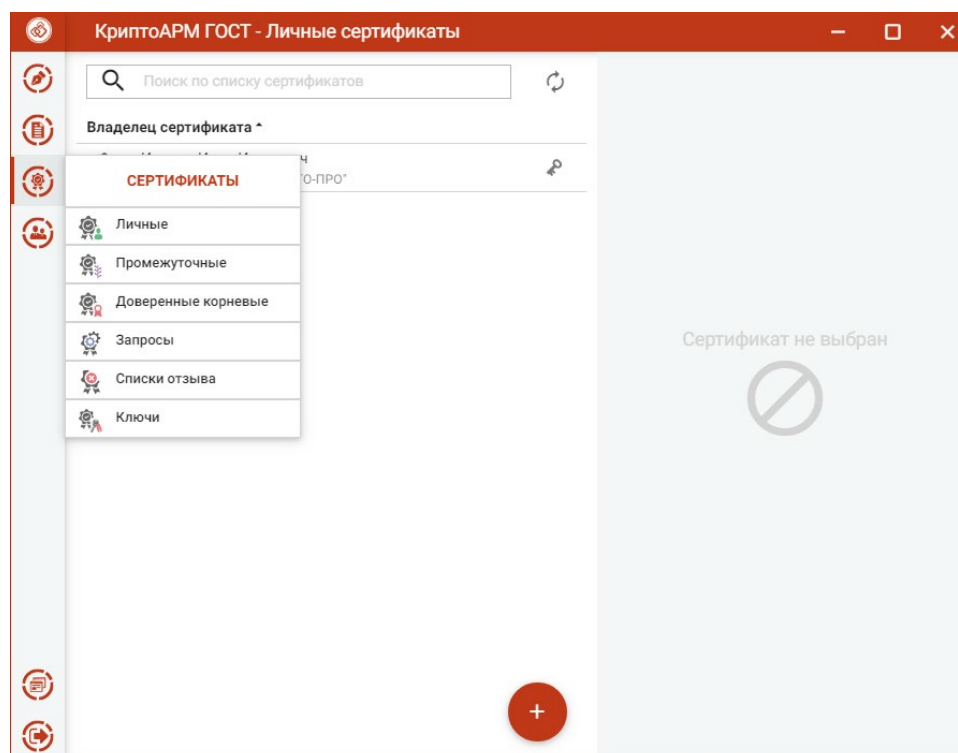


Рисунок 118. Список личных сертификатов с подменю

Подменю содержит пункты:

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

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

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

После выбора сертификата в списке отображается информация о нем (Рисунок 119).

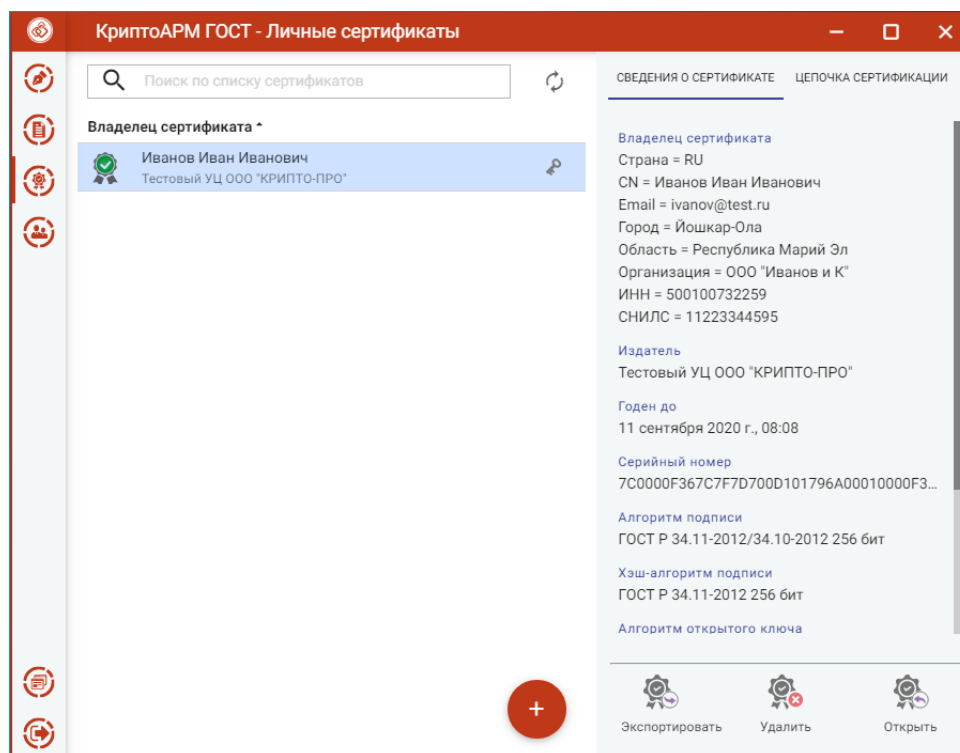


Рисунок 119. Отображение сведений о выбранном сертификате

На вкладке **Цепочка сертификации** отображается общий статус построения цепочки доверия и приводится «дерево» сертификации (Рисунок 120).

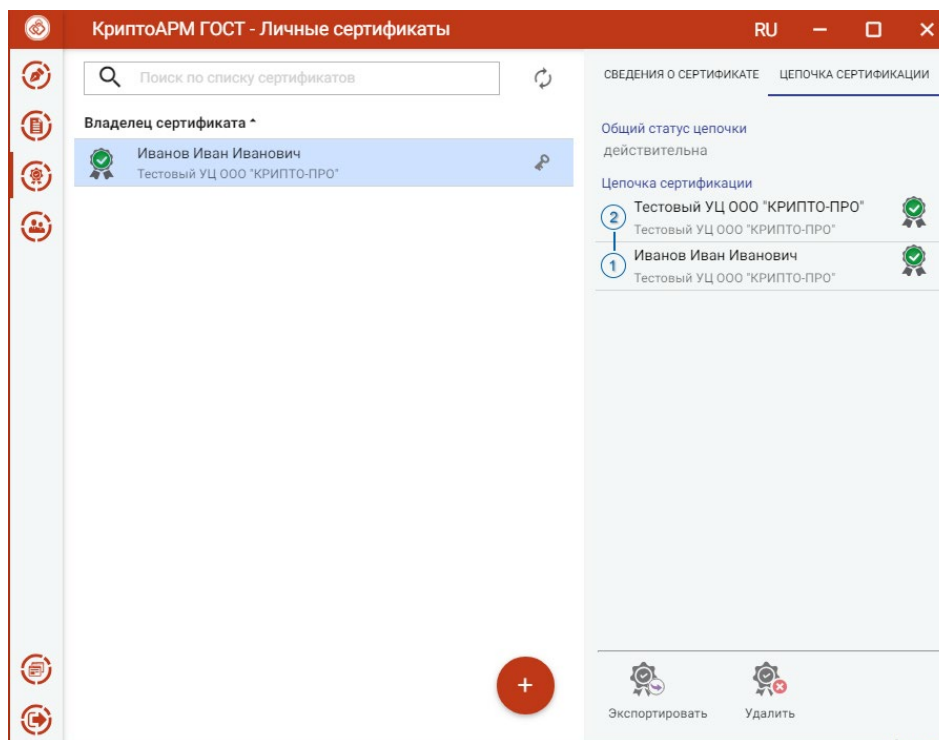
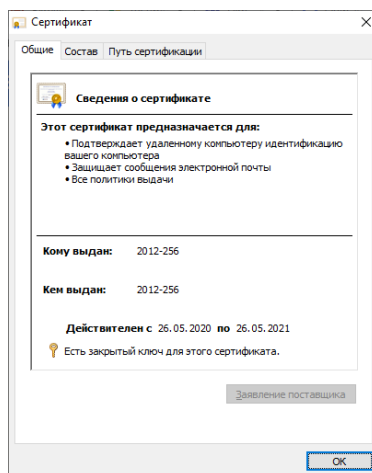


Рисунок 120. Представление цепочки сертификации (цепочки доверия)

Для выбранного сертификата доступны операции **Экспортировать**, **Удалить** и **Открыть** (только для ОС Windows).

Операция **Открыть** доступна только для приложений ОС Windows и открывает просмотр сертификата в стандартными средствами ОС Windows.



3.16.1 ИМПОРТ СЕРТИФИКАТА ИЗ ФАЙЛА

Импорт личного сертификата с привязкой к ключу ЭП. Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»). В открывшемся окне нужно выбрать операцию **Импорт из файла** (Рисунок 121).

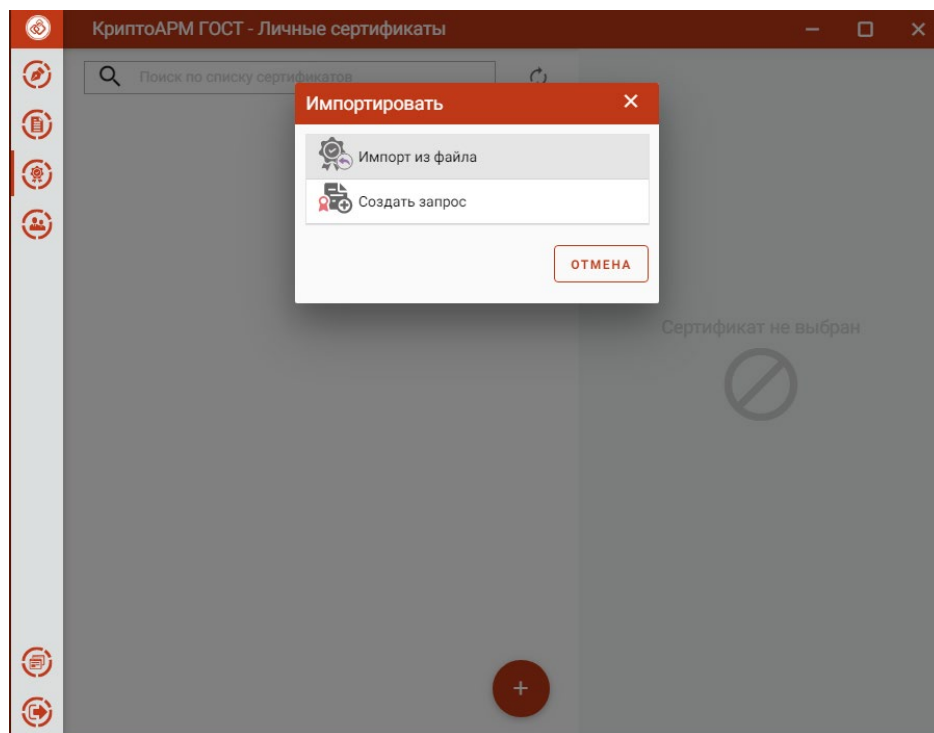


Рисунок 121. Меню выбора способа добавления сертификатов

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

При успешном выполнении операции импорта сертификат автоматически помещается в личные сертификаты (Рисунок 122).

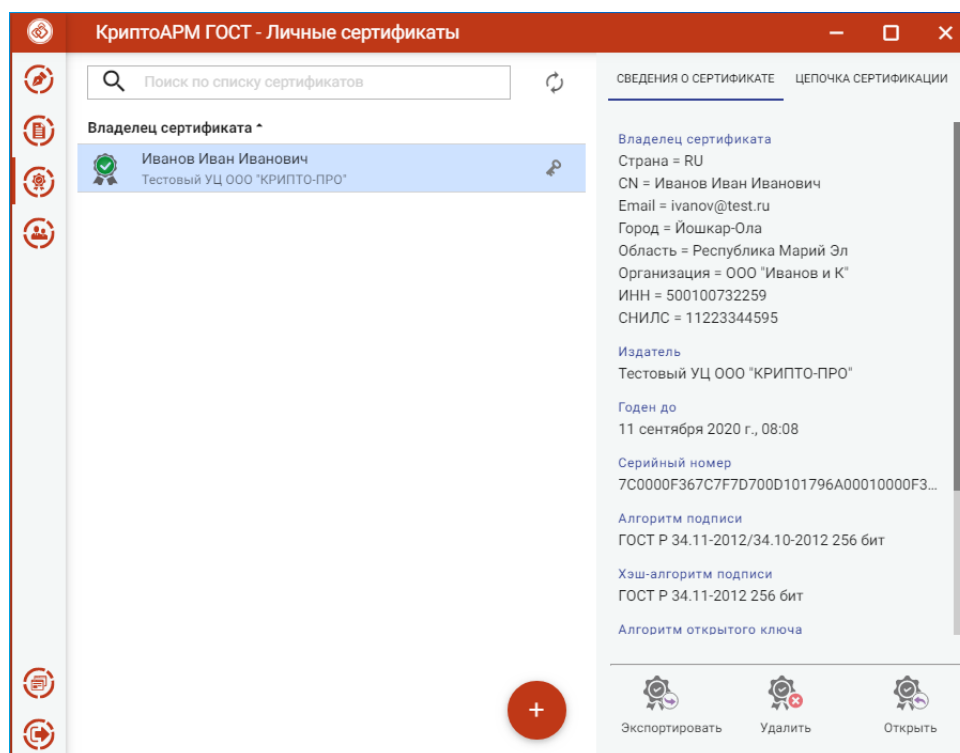


Рисунок 122. Отображение импортированного личного сертификата

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

принудительно в выбранное (Рисунок 123). Если сертификат без ключа ЭП будет установлен в личное хранилище, то с использованием данного сертификата нельзя будет подписывать и расшифровывать файлы.

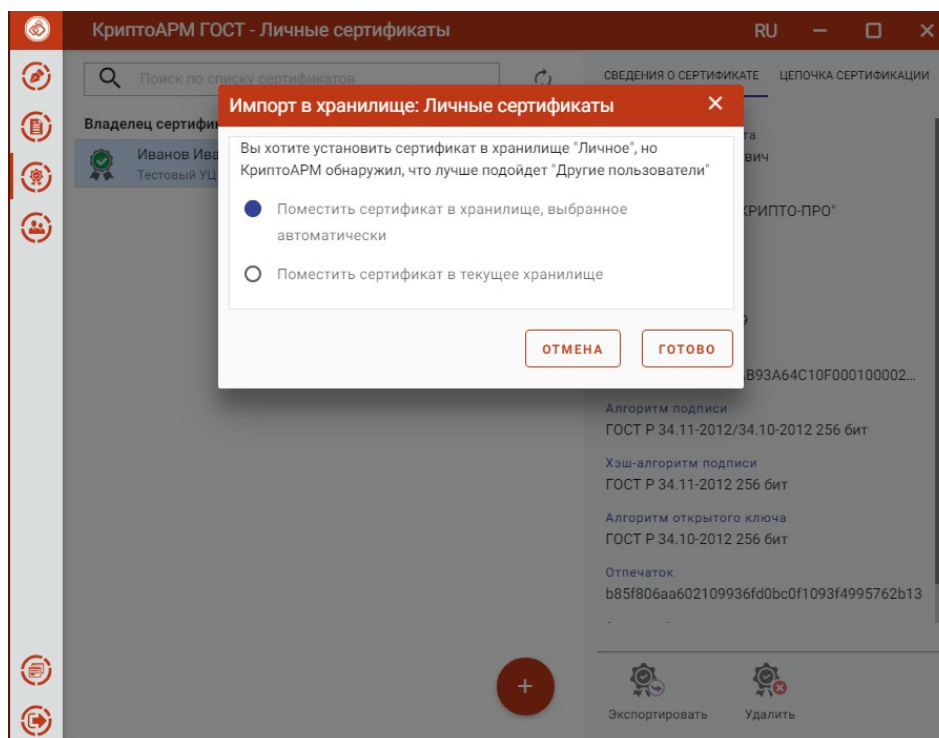


Рисунок 123. Выбор хранилища для установки сертификата

ИМПОРТ СЕРТИФИКАТА БЕЗ ПРИВЯЗКИ К КЛЮЧУ ЭП. Для выполнения импорта нового сертификата в хранилище выполняется кнопкой добавления сертификата («+») и выбора опции **Импорт из файла** (Рисунок 124).

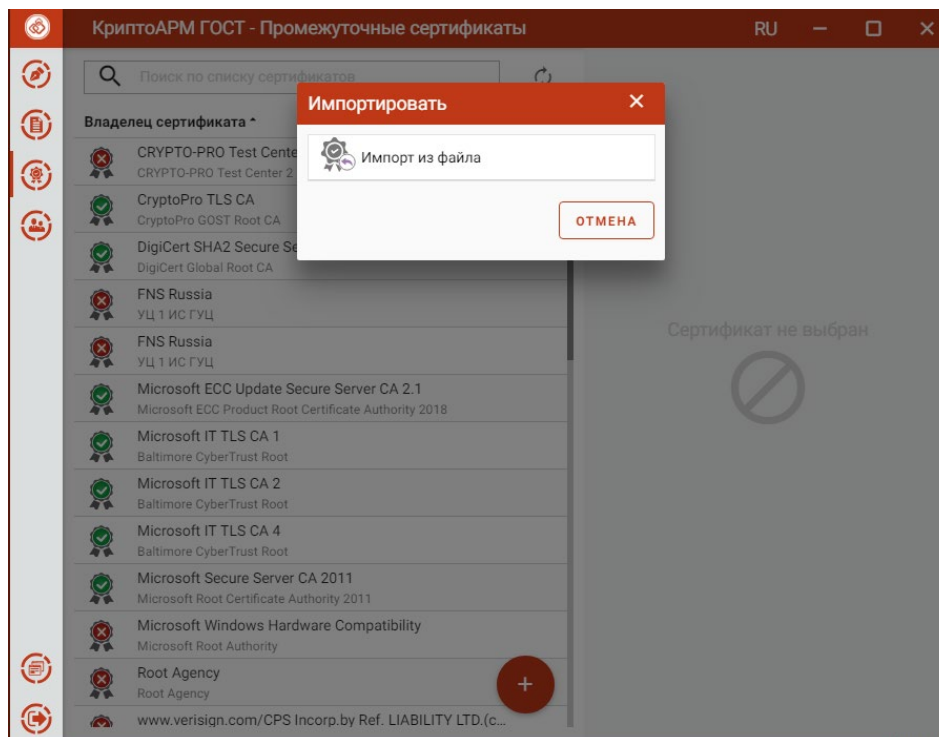


Рисунок 124. Импорт сертификата из файла

В появившемся диалоговом окне нужно выбрать файл сертификата.

При успешном выполнении операции импорта сертификат автоматически помещается в выбранное хранилище (Рисунок 125).

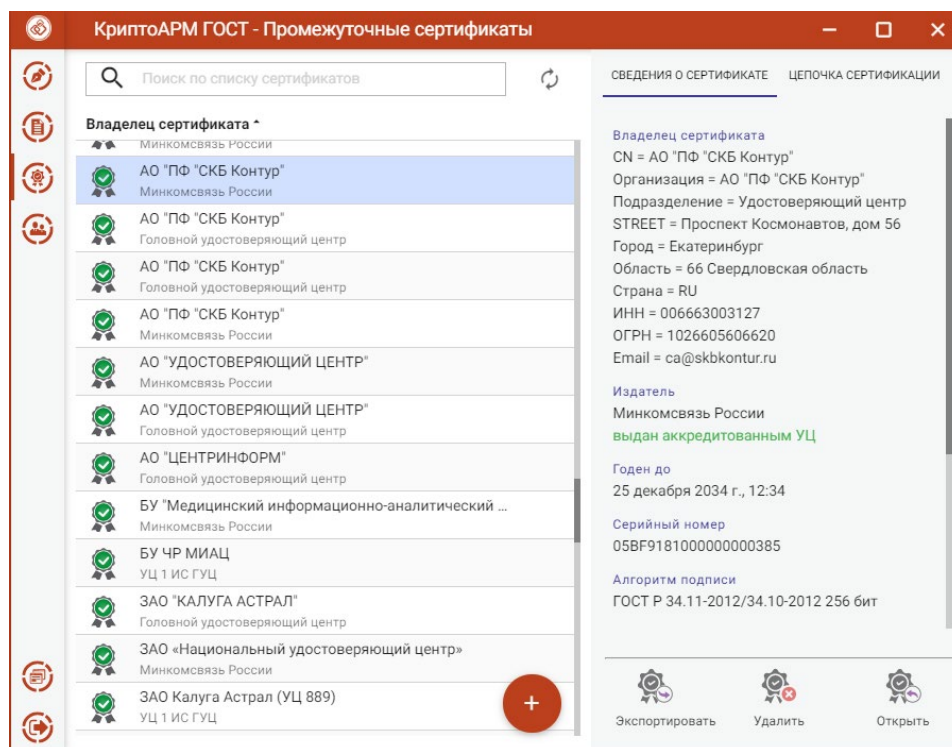


Рисунок 125. Отображение импортированного сертификата

Если при импорте приложение определило, что для данного сертификата лучше подойдет другое хранилище, то возникнет сообщение с предложением установить сертификат в подходящее хранилище или принудительно в выбранное (Рисунок 126).

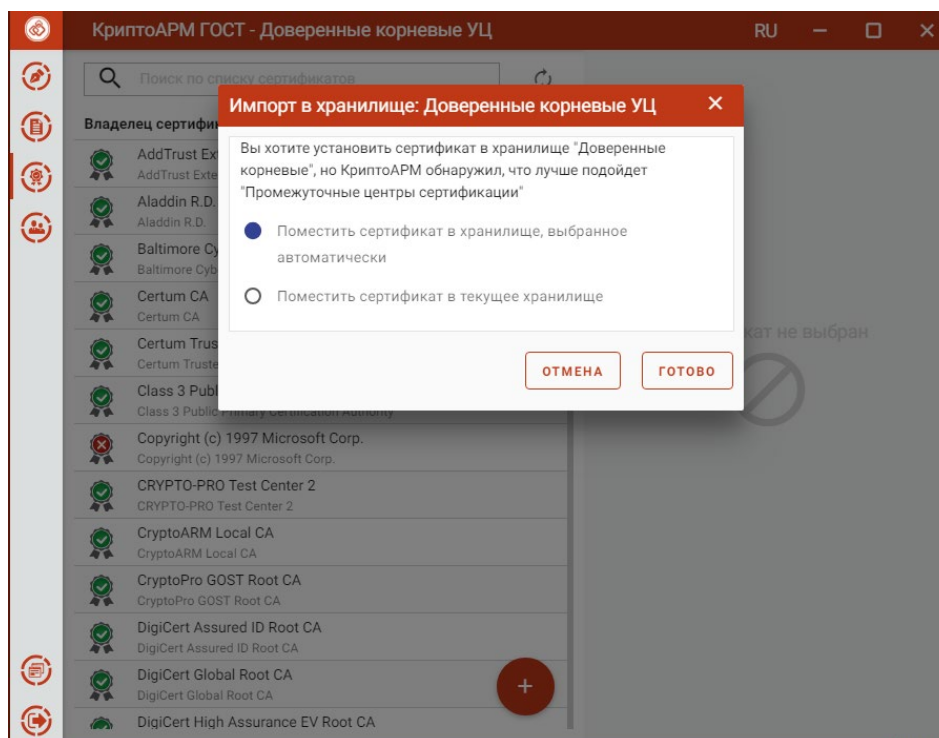


Рисунок 126. Выбор хранилища для установки сертификата

3.16.2 ЭКСПОРТ СЕРТИФИКАТА В ФАЙЛ

Для экспорта сертификата в файл нужно выделить сертификат и нажать кнопку операции **Экспортировать** (Рисунок 127). Если у сертификата экспортируемый ключ ЭП, то такой сертификат можно экспортировать вместе с ключом ЭП.

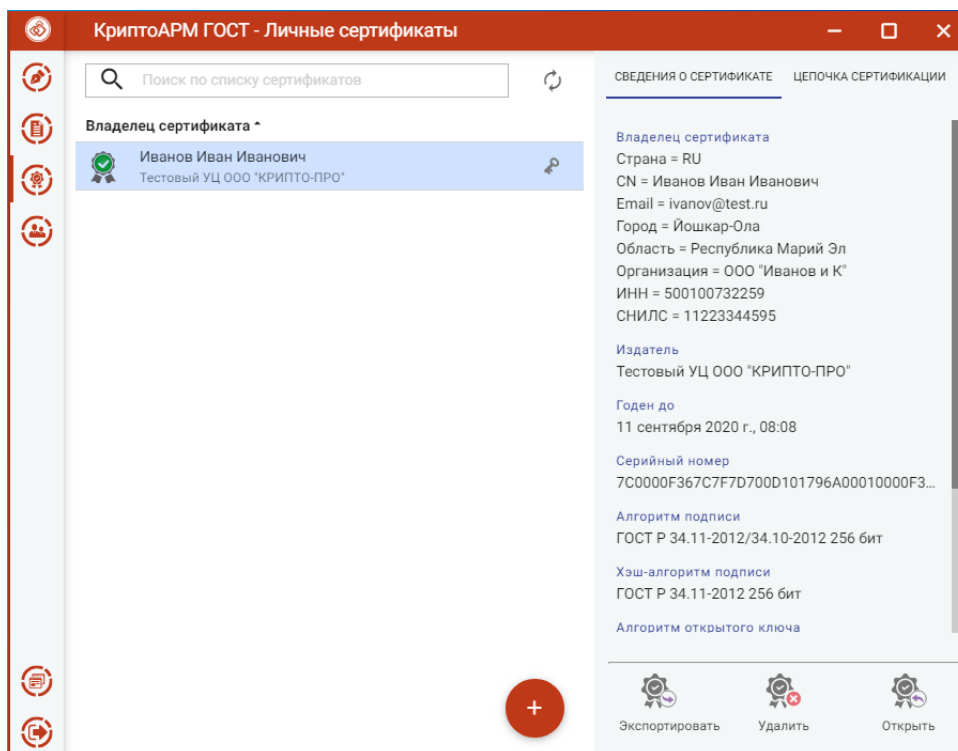


Рисунок 127. Экспорт сертификата

При экспорте сертификата с не экспортируемым ключом ЭП появляется окно, в котором можно выбрать только кодировку файла сертификата (Рисунок 128).

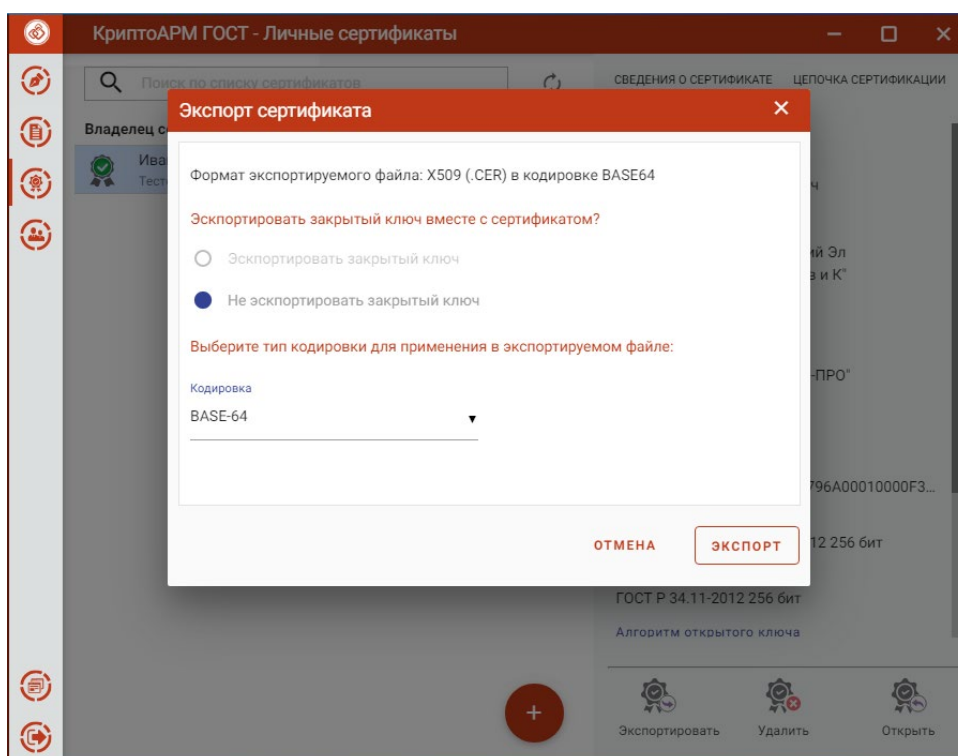


Рисунок 128. Выбор кодировки файла сертификата

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

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

экспортировать только сертификат без ключа ЭП. В таком случае нужно только выбрать кодировку файла сертификата (Рисунок 128).

- Экспортировать сертификат вместе с ключом ЭП. В таком случае надо указать пароль для защиты ключа ЭП (Рисунок 129).

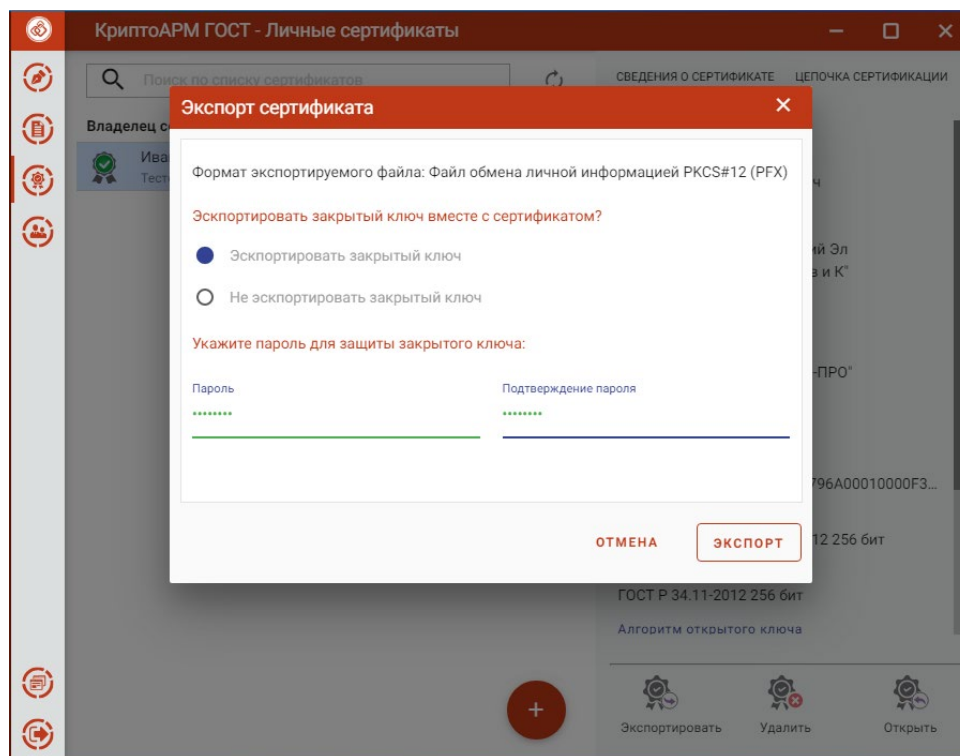


Рисунок 129. Экспорт сертификата вместе с ключом ЭП

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 ключом ЭП необходимо будет вводить пароль к ключевому контейнеру.

3.16.3 УДАЛЕНИЕ СЕРТИФИКАТА

Для удаления сертификата нужно выбрать операцию **Удалить** (Рисунок 130).

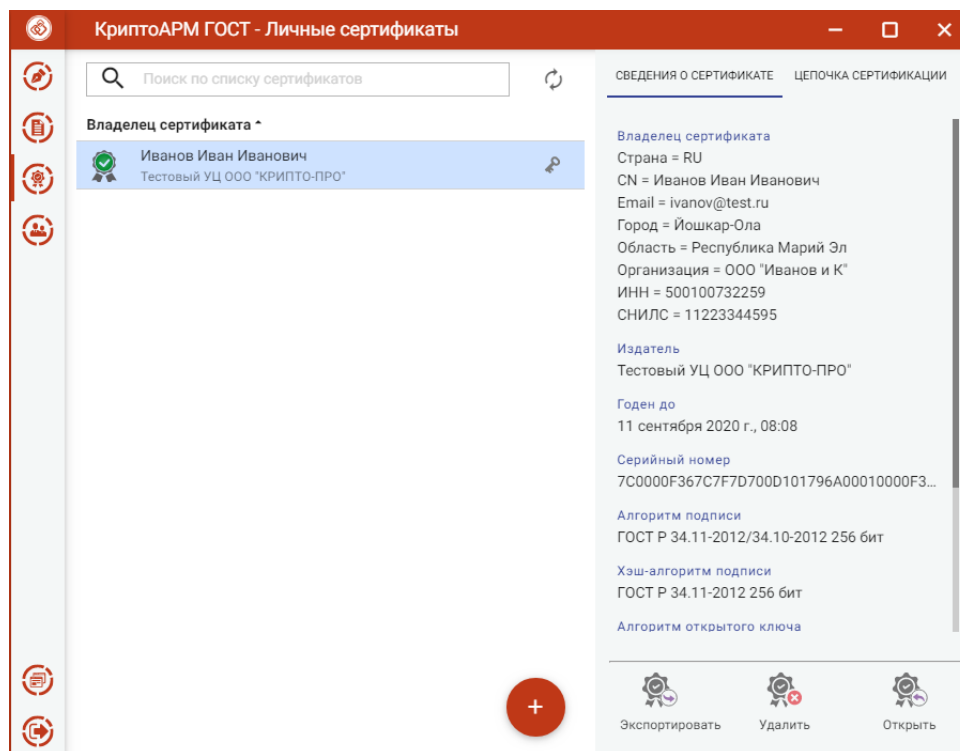


Рисунок 130. Удаление сертификата

В появившемся диалоговом окне нажать **Удалить** для подтверждения удаления (Рисунок 131).

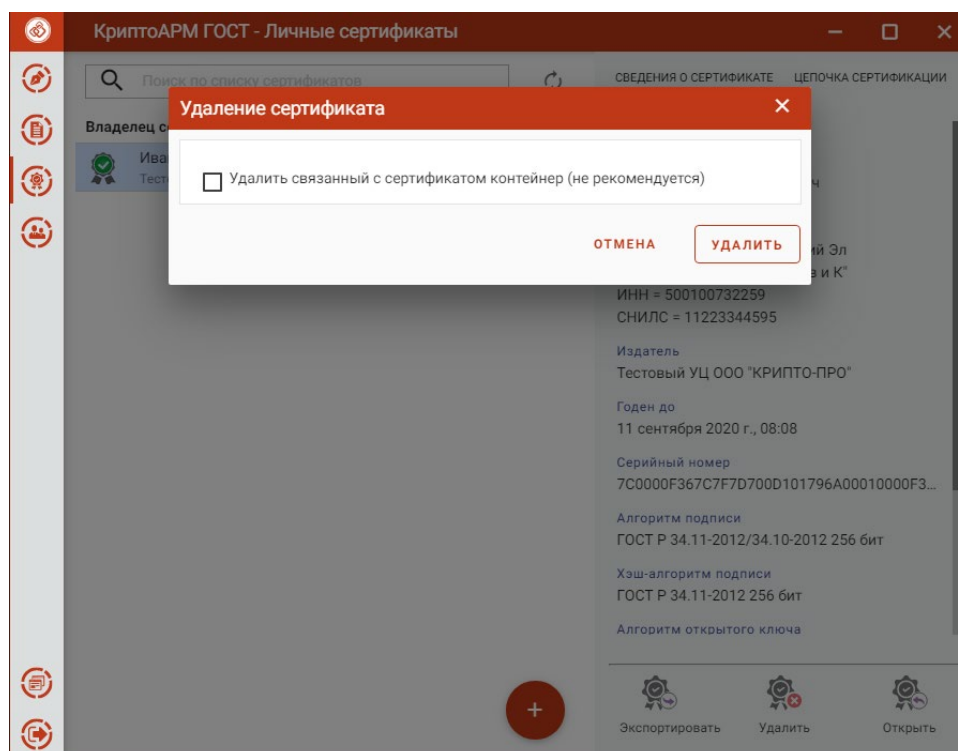


Рисунок 131. Подтверждение удаления сертификата

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

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

3.16.4 СОЗДАНИЕ ЗАПРОСА НА СЕРТИФИКАТ

Для создания запроса на сертификат в окне добавления сертификата следует выбрать операцию **Создать запрос** (Рисунок 132). Создать запрос можно со списка личных сертификатов (Рисунок 132) или со списка запросов (Рисунок 133)

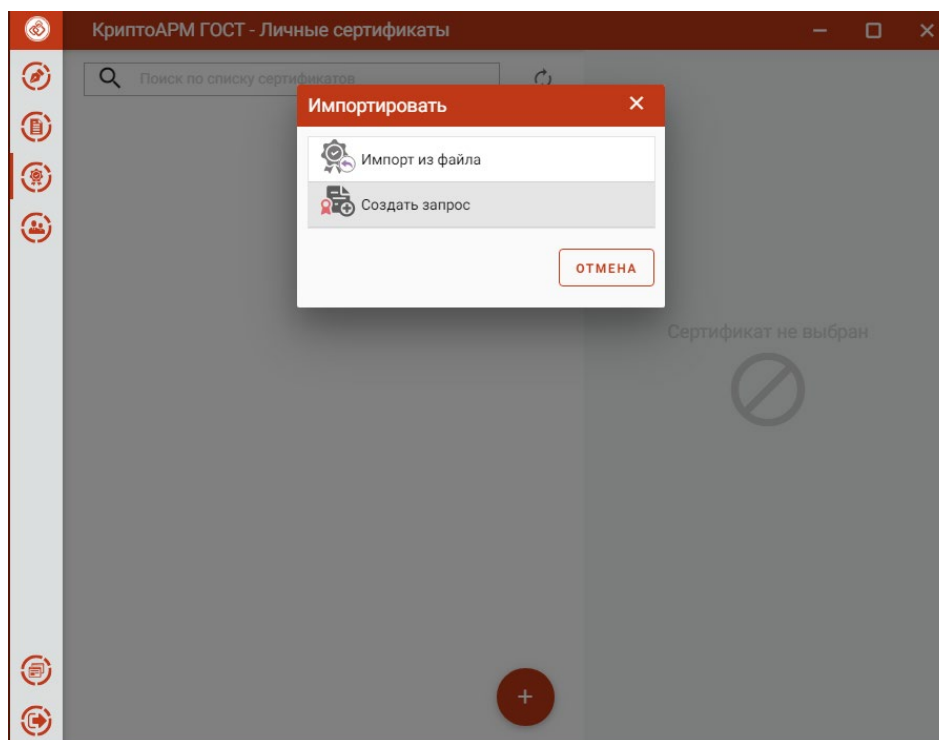


Рисунок 132. Создание запроса на сертификат в списке личных сертификатов

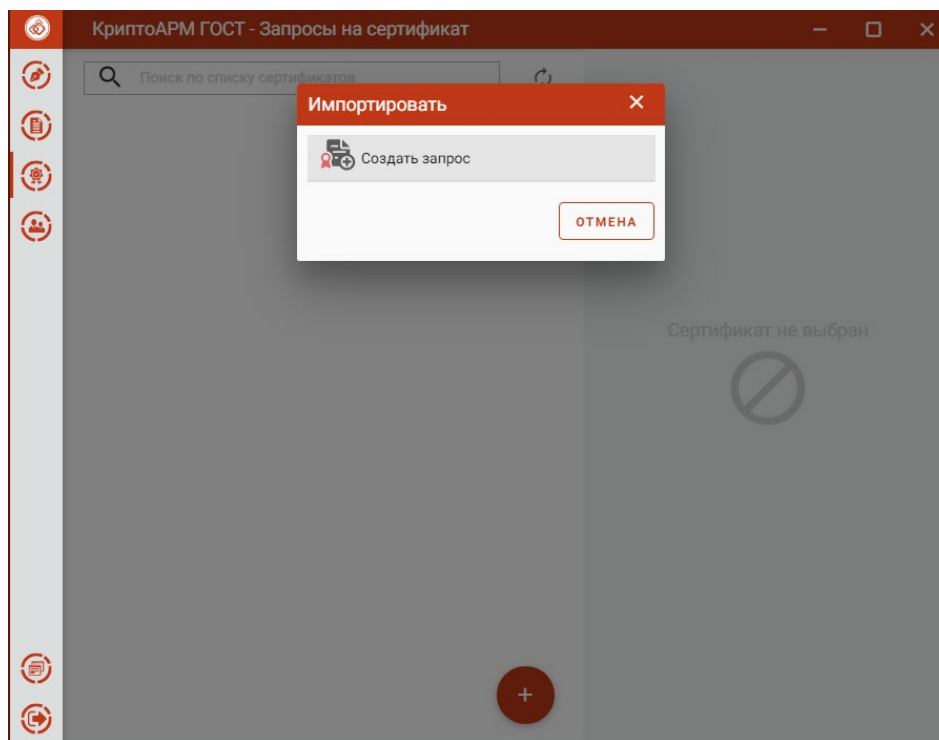


Рисунок 133. Создание запроса на сертификат в списке запросов

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

В параметрах субъекта указывается:

- Шаблон сертификата (Рисунок 134);

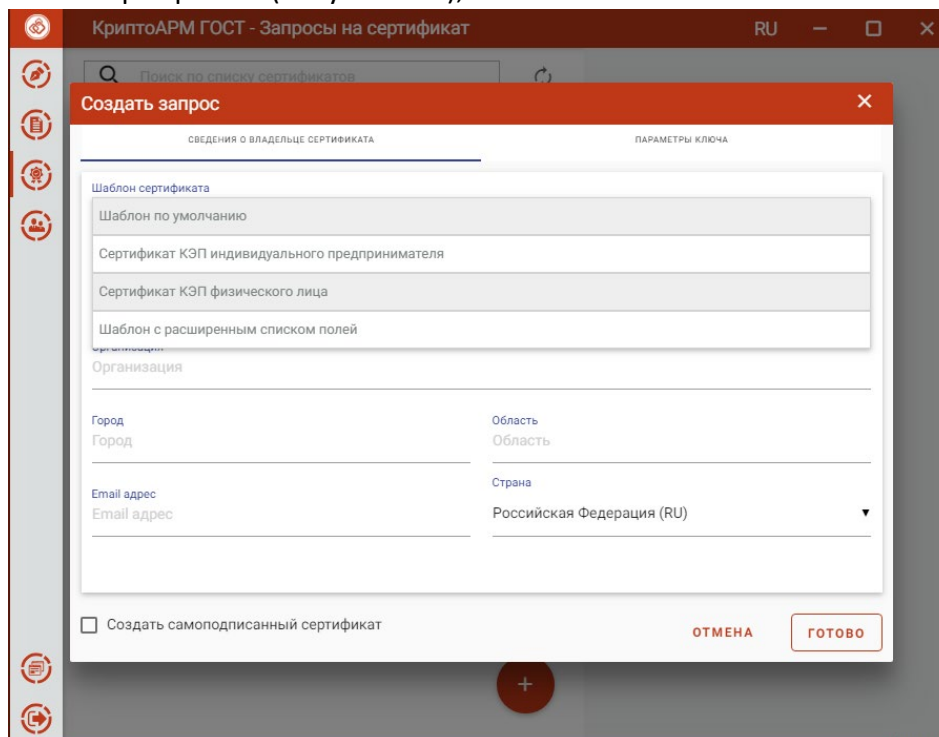


Рисунок 134. Выбор шаблона сертификата

- Основная информация, в которой, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце сертификата (Рисунок 135).

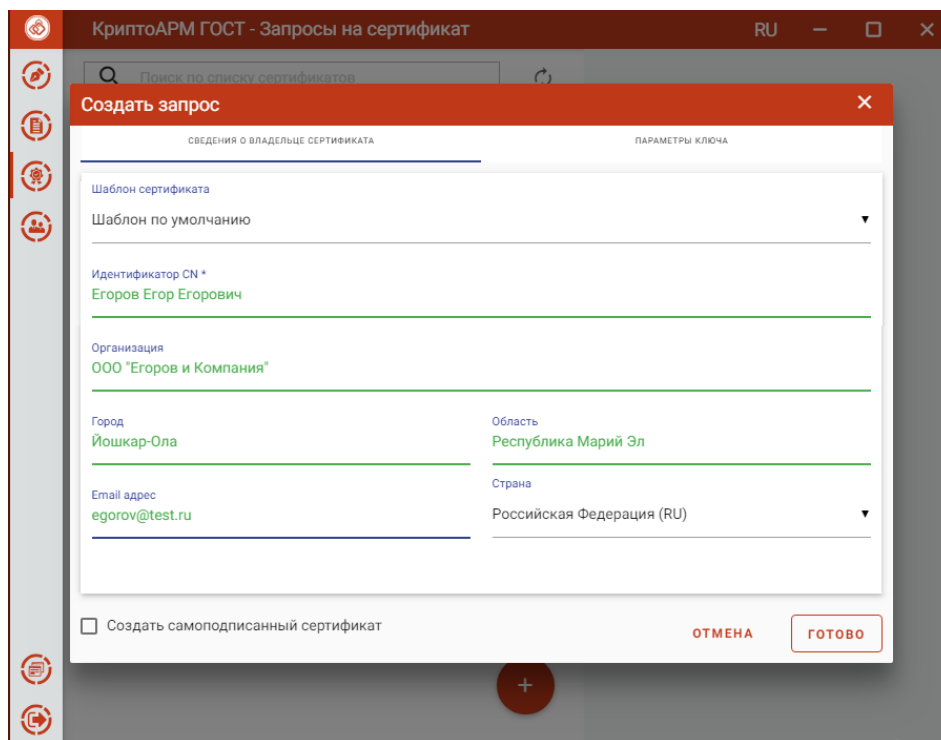


Рисунок 135. Информация о владельце сертификата

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

В параметрах ключа указывается:

- Алгоритм ключа (Рисунок 136);

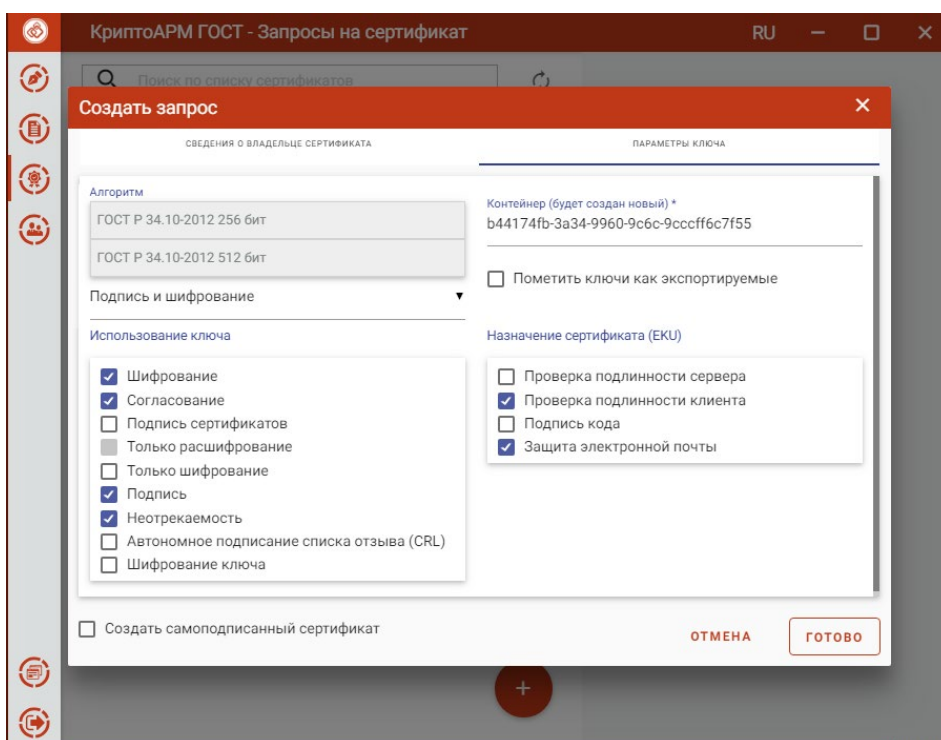


Рисунок 136. Выбор алгоритма ключа

- Назначение ключа (Рисунок 137);

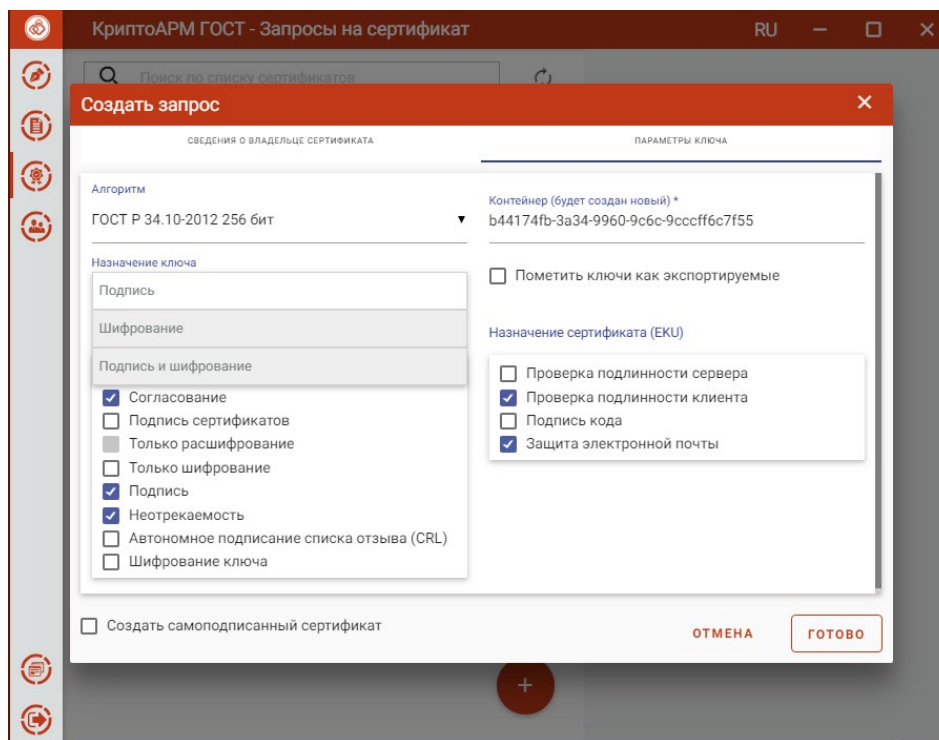


Рисунок 137. Выбор назначения ключа

- Использование ключа (Рисунок 138);

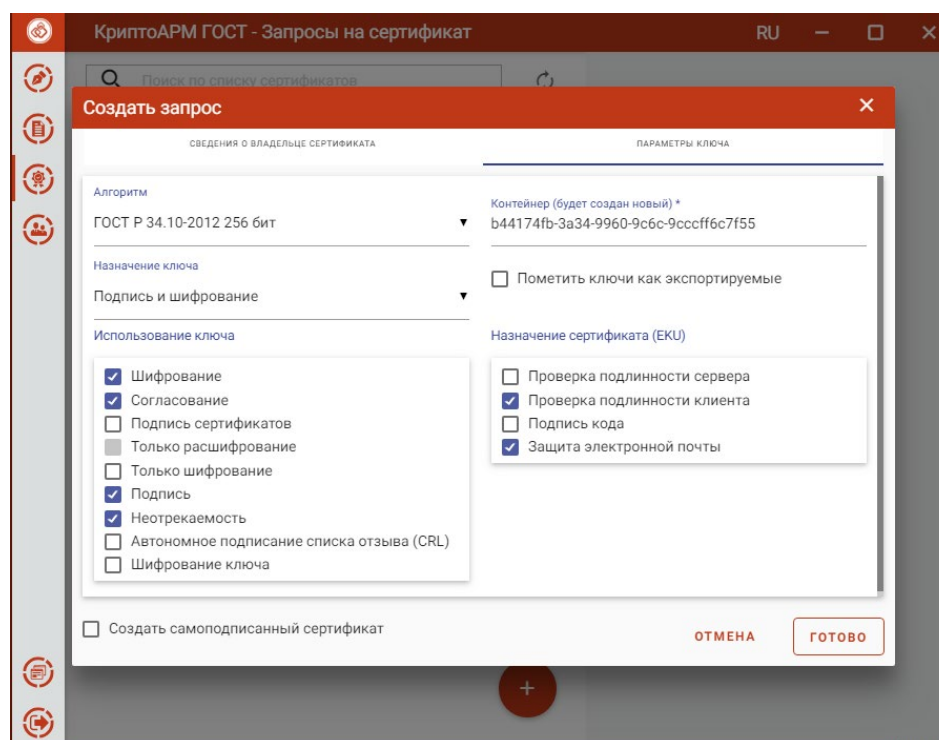


Рисунок 138. Выбор использования ключа

- Контейнер - сертификат будет создан на основе нового ключевого набора. Можно задать свое имя ключевого набора или оставить созданное автоматически.
- Пометить ключи как экспортируемые. Если отметить этот флаг, то можно проводить экспорт сертификата вместе с ключом ЭП.
- 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** (Рисунок 139).

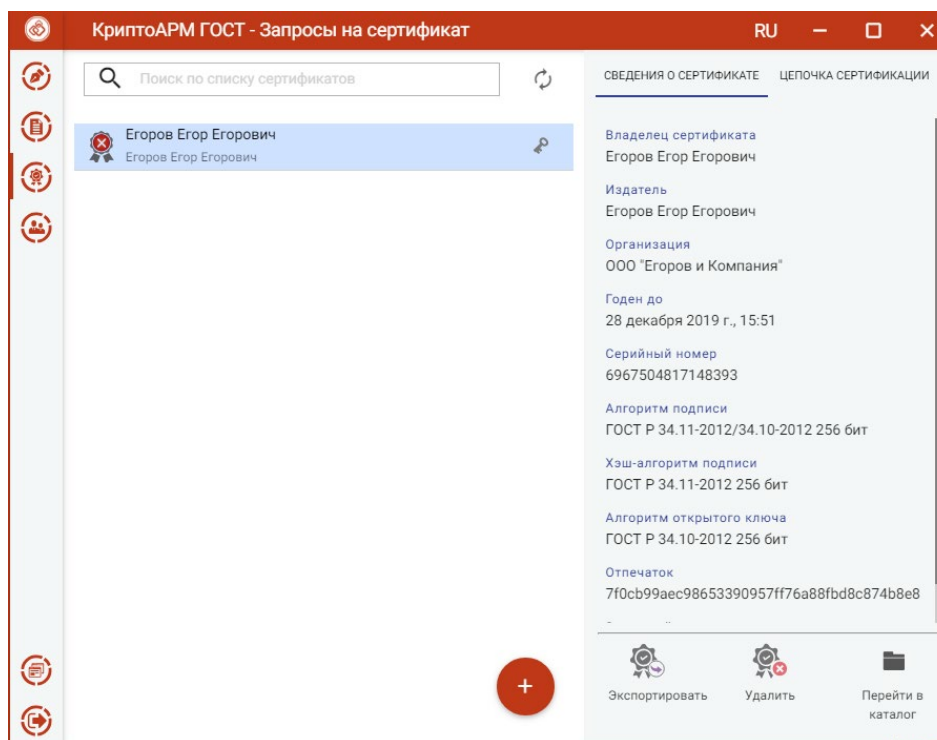


Рисунок 139. Форма просмотра запроса на сертификат

Для запроса доступны следующие операции:

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

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

3.16.5 СОЗДАНИЕ САМОПОДПИСАННОГО СЕРТИФИКАТА

Примечание: Самоподписанный сертификат может использоваться только в тестовых целях.

Для создания самоподписанного сертификата на форме **Создать запрос** следует поставить флаг **Создание самоподписанного сертификата** (Рисунок 140).

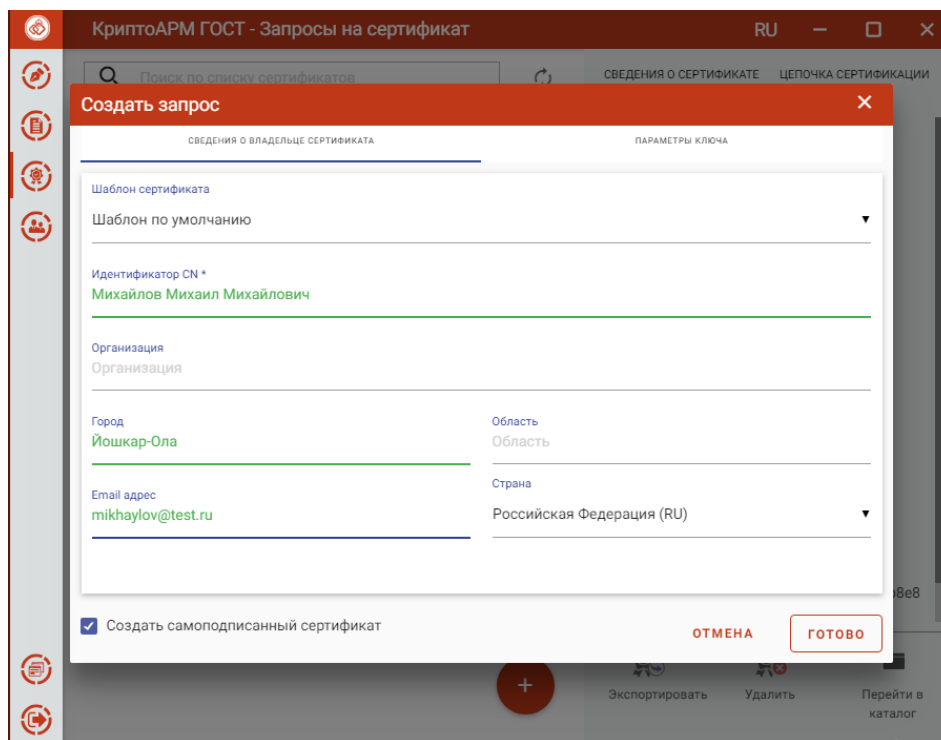


Рисунок 140. Создание самоподписанного сертификата

На основе указанных данных по кнопке **Готово** будет сформирован самоподписанный сертификат. Для сертификата выберите ключевой носитель для хранения контейнера (Реестр, диск, токен). На запрос системы установите пароль на данный контейнер и подтвердите его. После завершения операции возникнет окно с информацией о ее результатах. Сертификат будет в списке **Личных сертификатов** (Рисунок 141)

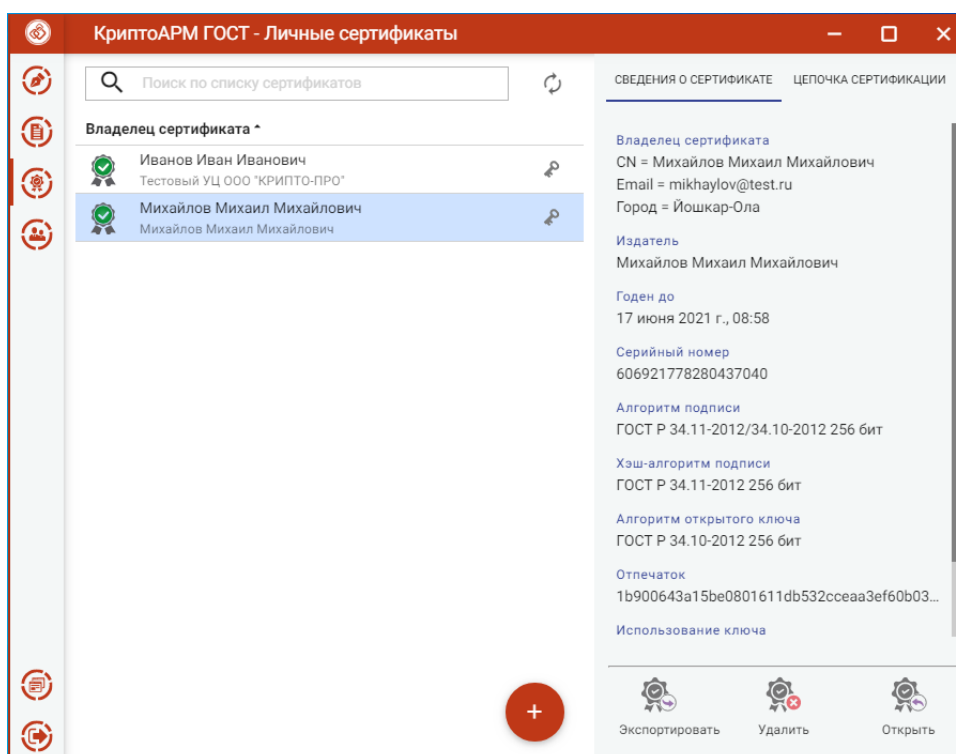


Рисунок 141. Список Личных сертификатов

При генерации самоподписанного сертификата запрос на сертификат не создается.

3.16.6 Списки отзыва сертификатов (СОС)

Для работы со списками отзыва сертификатов в пункт меню сертификаты добавлен подпункт **Списки отзыва сертификатов** (Рисунок 142).

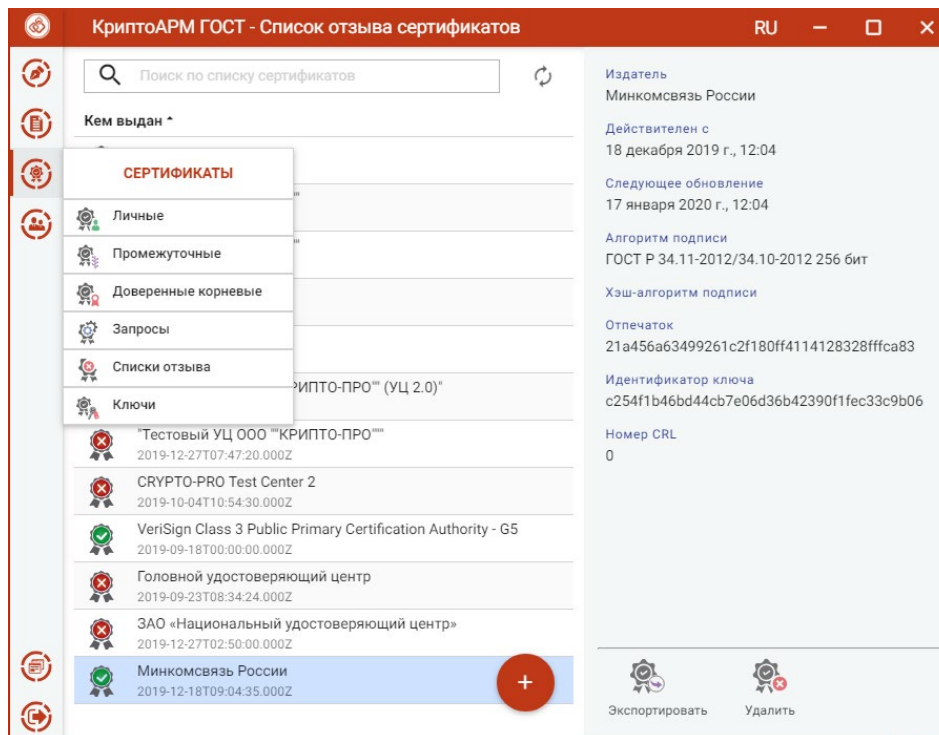


Рисунок 142. Выбор пункт меню для управления списком отзыва

Списки отзыва можно импортировать, экспортировать и удалять.

Для импорта списка отзыва надо нажать кнопку добавления («+») и выбрать опцию **Импорт из файла** (Рисунок 143). В открывшемся окне выбрать файл списка отзыва.

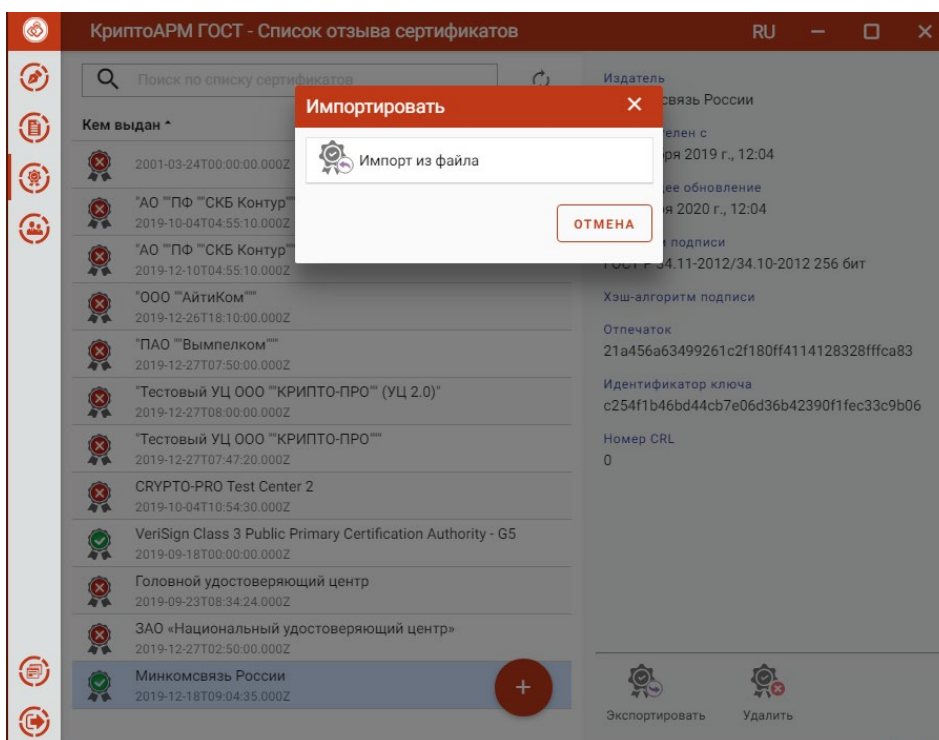


Рисунок 143. Импорт списка отзыва сертификатов

При успешном импорте СОС отображается в разделе **Список отзыва сертификатов** (Рисунок 144).

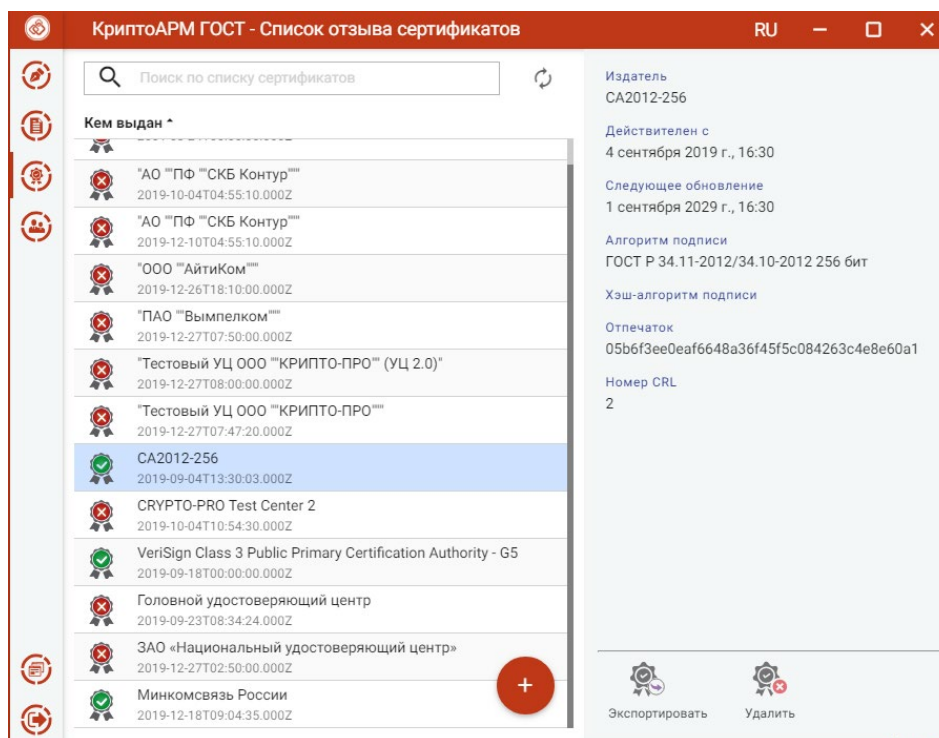


Рисунок 144. Просмотр информации о списке отзыва

ЭКСПОРТ СОС. Для экспорта списка отзыва нужно нажать кнопку **Экспортировать**. Открывается форма выбора кодировки файла (Рисунок 145). При нажатии на **Экспорт** следует выбрать директорию для сохранения и задать имя файла СОС.

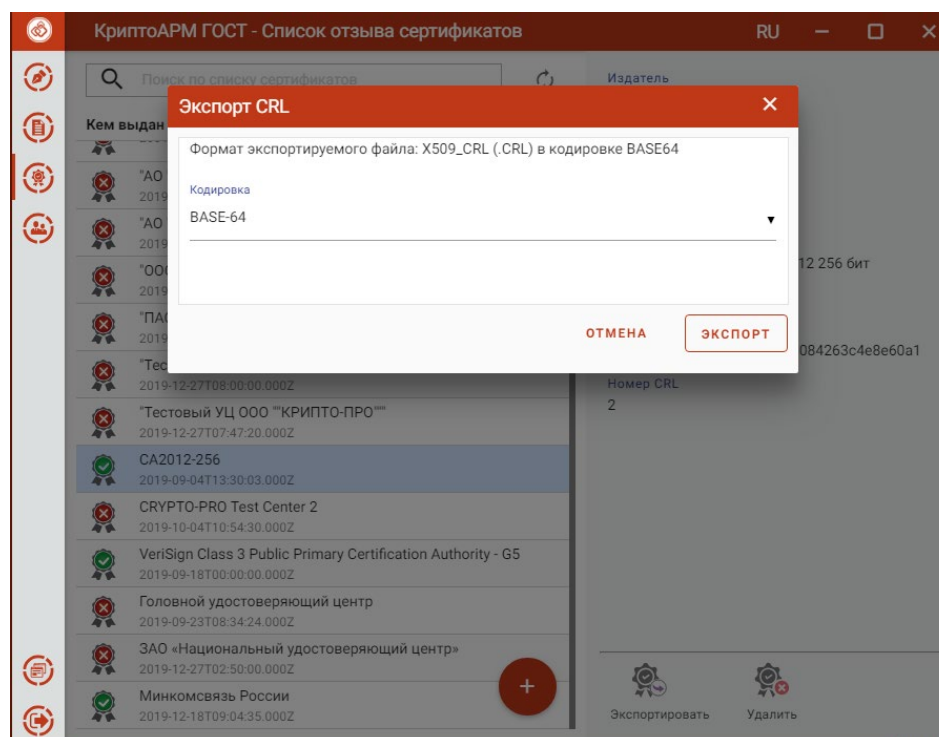


Рисунок 145. Выбор кодировки экспортируемого СОС

УДАЛЕНИЕ СОС. Для удаления СОС надо нажать кнопку **Удалить** и подтвердить удаление в соответствующем окне (Рисунок 146).

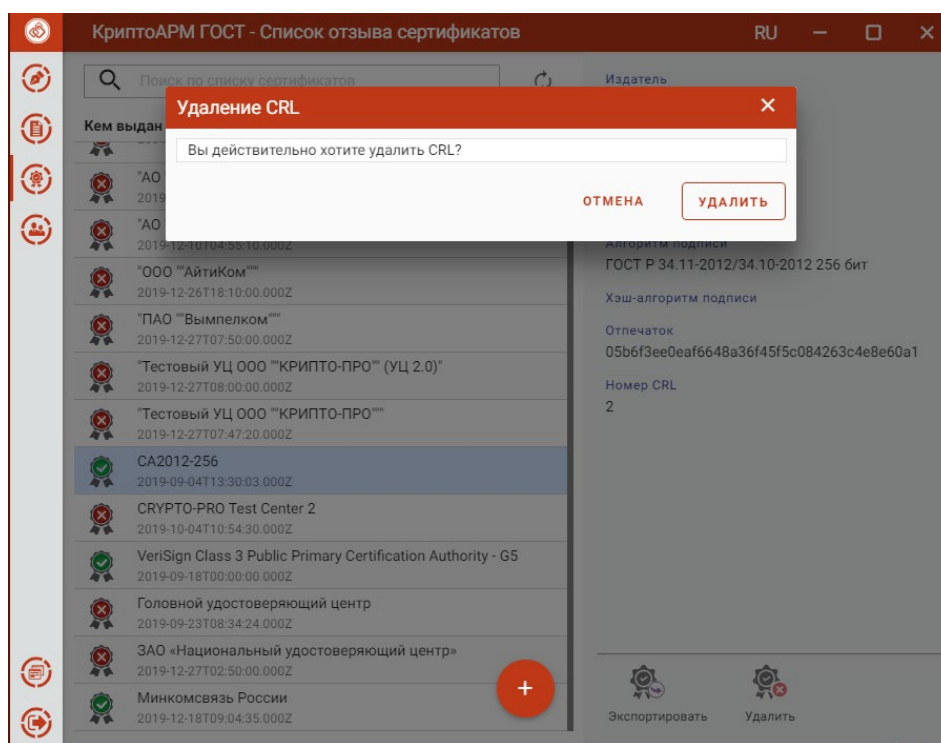


Рисунок 146. Подтверждение удаления СОС

3.16.7 КЛЮЧЕВЫЕ КОНТЕЙНЕРЫ

УСТАНОВКА СЕРТИФИКАТА ИЗ КЛЮЧЕВОГО КОНТЕЙНЕРА. Для установки сертификата из ключевого контейнера нужно выбрать в меню **Сертификаты** подпункт **Ключи**. В левой области представления отображаются все подключенные хранилища контейнеров ключей ЭП. В правой области отображается информация о сертификате в выделенном контейнере (Рисунок 147).

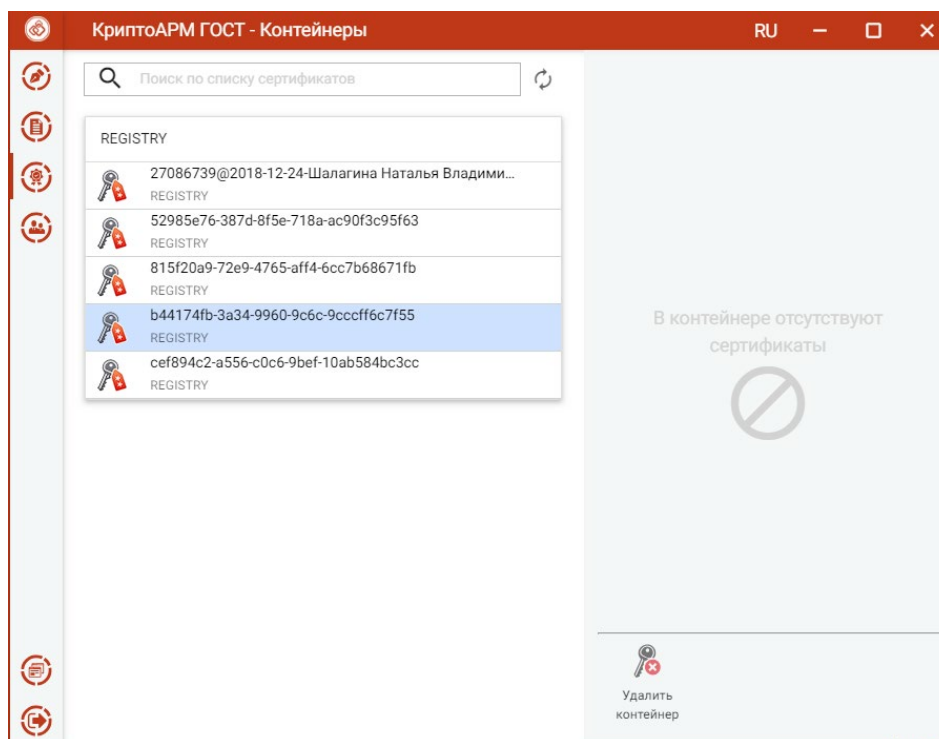


Рисунок 147. Хранилища контейнеров ключей ЭП

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

После выбора контейнера отображается информация о находящемся в нем сертификате (Рисунок 148).

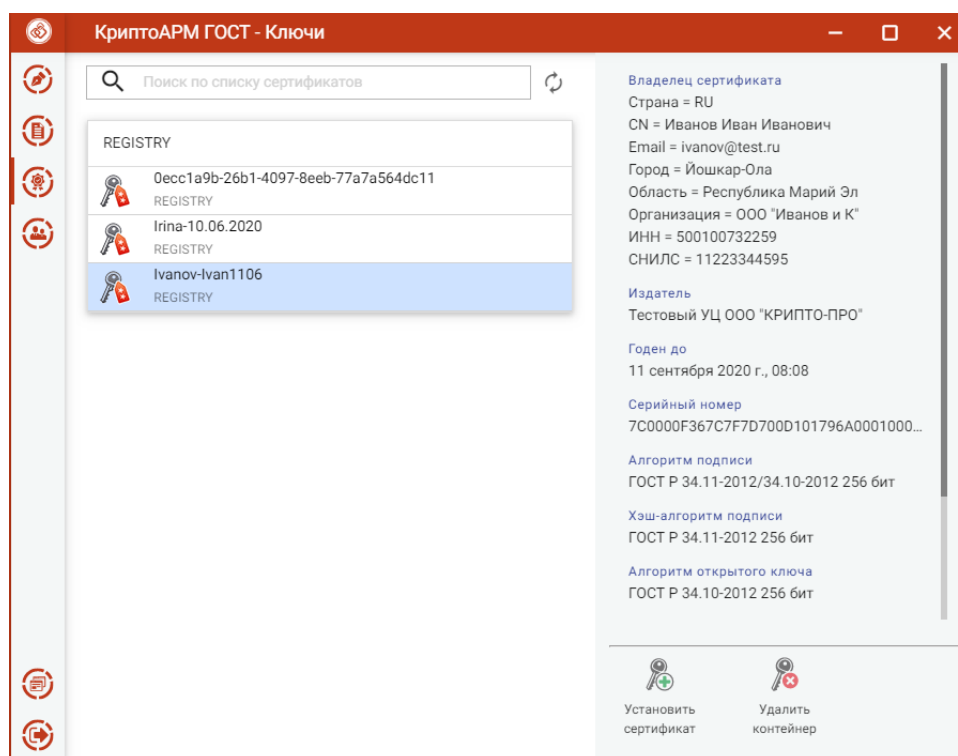


Рисунок 148. Информация о сертификате в контейнере

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

Для удаления контейнера нужно нажать кнопку **Удалить контейнер** и подтвердить операцию (Рисунок 149). 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. С использованием такого сертификата нельзя выполнять операции подписи и расшифрования.

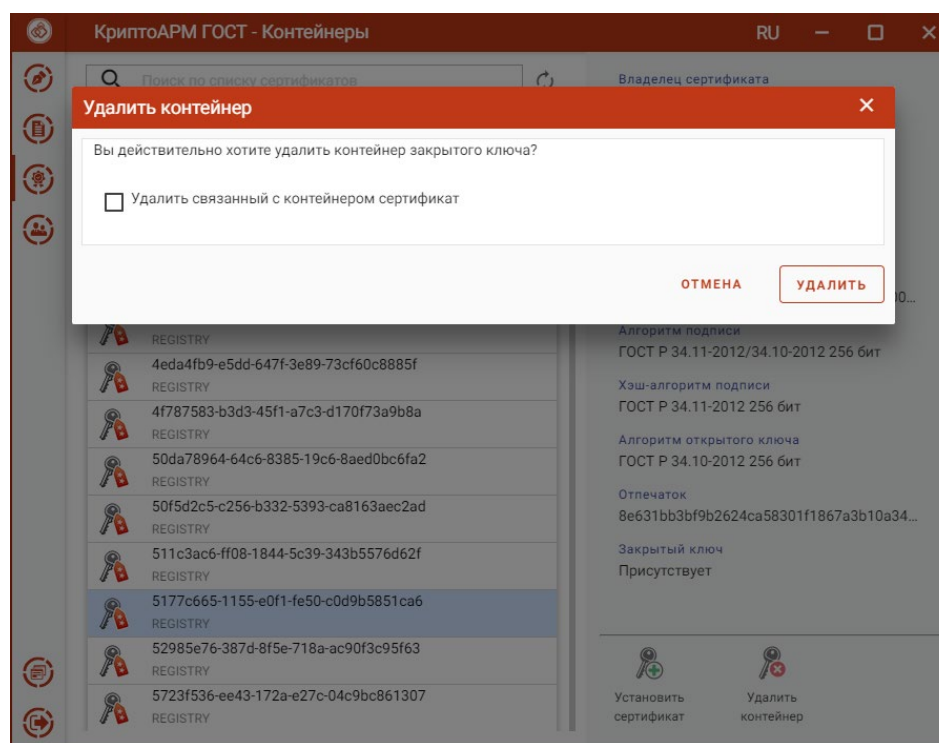


Рисунок 149. Удаление контейнера

В приложении реализован поиск контейнеров по символьному совпадению в названии контейнера (Рисунок 150).

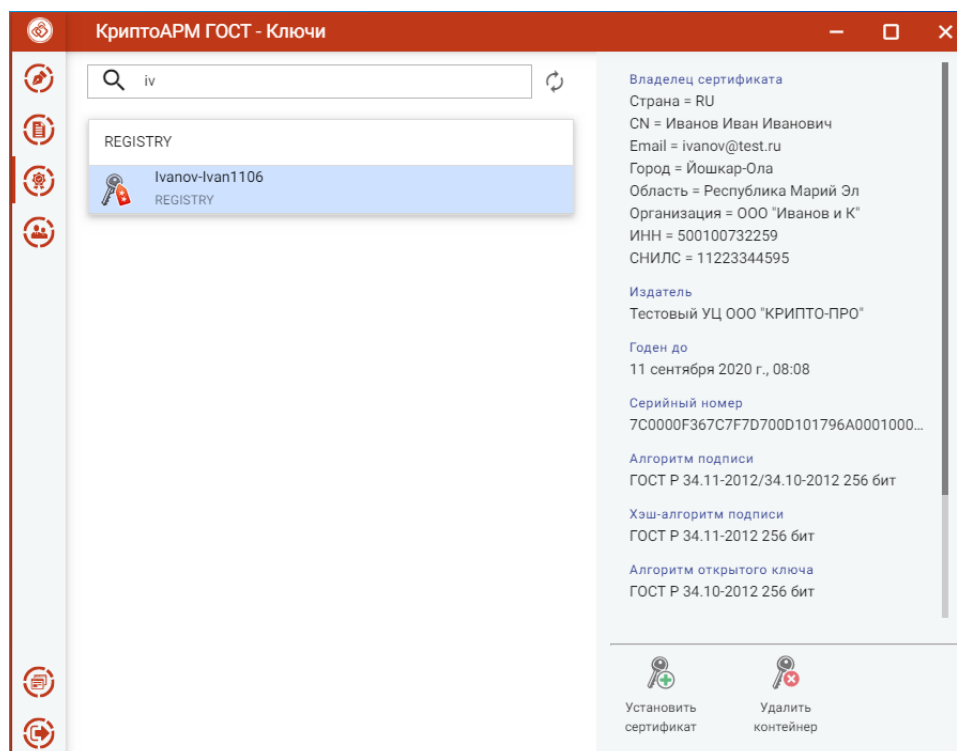


Рисунок 150. Поиск контейнера

3.16.8 ПОИСК СЕРТИФИКАТА

В элементах пользовательского интерфейса, где процесс выполнения операции учитывает выбор сертификата из списка, реализована функция поиска сертификатов (Рисунок 151). Для

включения режима поиска нужно нажать на кнопку **Поиск** и в строке поиска ввести ключевую фразу.

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

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

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

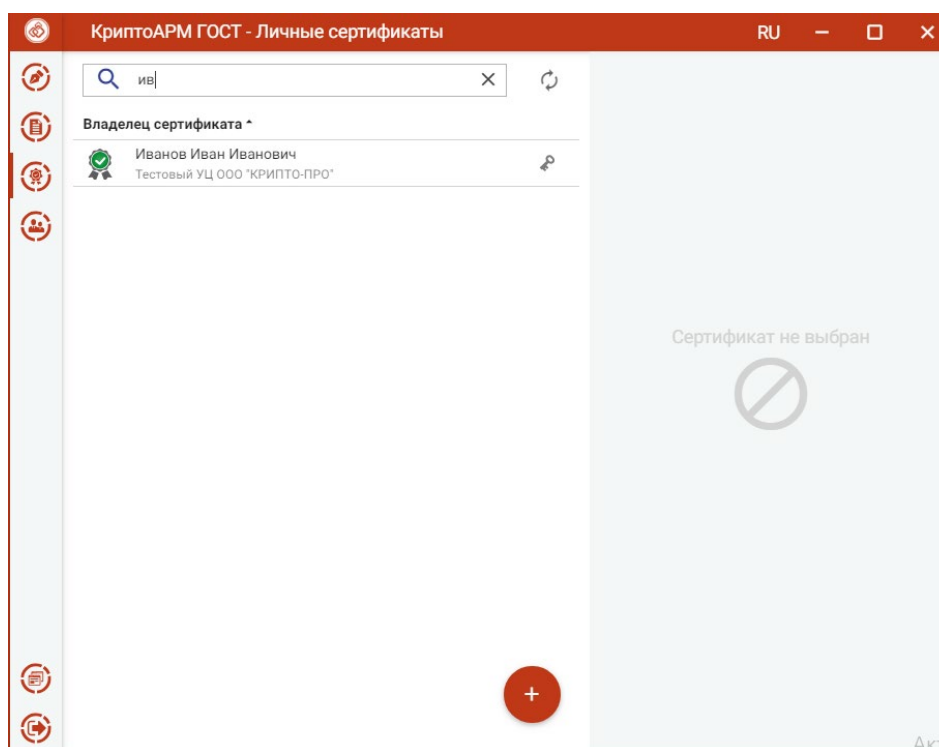


Рисунок 151. Поиск сертификата

3.17 КОНТАКТЫ

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

Переход в список контактов происходит при выборе пункта меню **Контакты** (Рисунок 152).

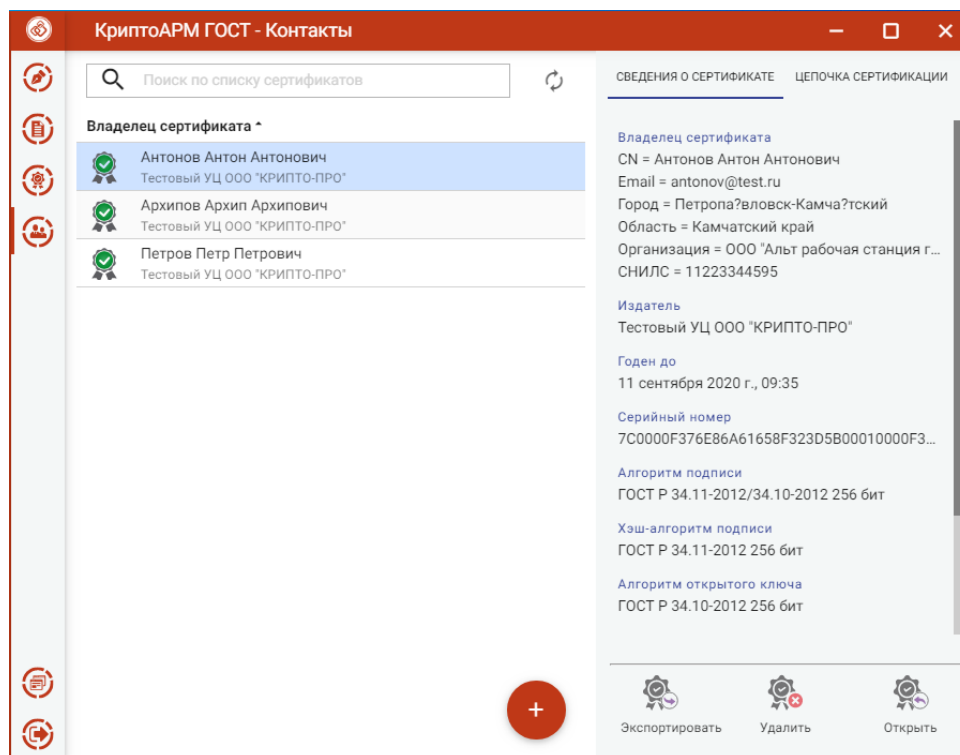
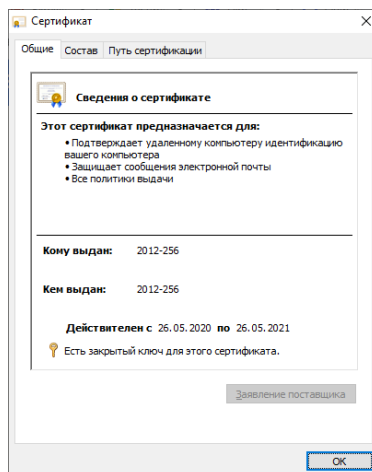


Рисунок 152. Список контактов

Контакты можно импортировать, экспортировать, удалять и открывать (только для ОС Windows). Так же в списке контактов работает поиск.

Операция **Открыть** доступна только для приложений ОС Windows и открывает просмотр сертификата в стандартными средствами ОС Windows.



ИМПОРТ КОНТАКТА. Для выполнения импорта нового контакта выполняется кнопкой добавления контакта («+») и выбрать опцию **Импорт из файла** (Рисунок 152). В появившемся диалоговом окне нужно выбрать файл сертификата.

При успешном выполнении операции импорта контакт появляется в списке (Рисунок 153), а сертификат автоматически помещается в хранилище сертификатов других пользователей.

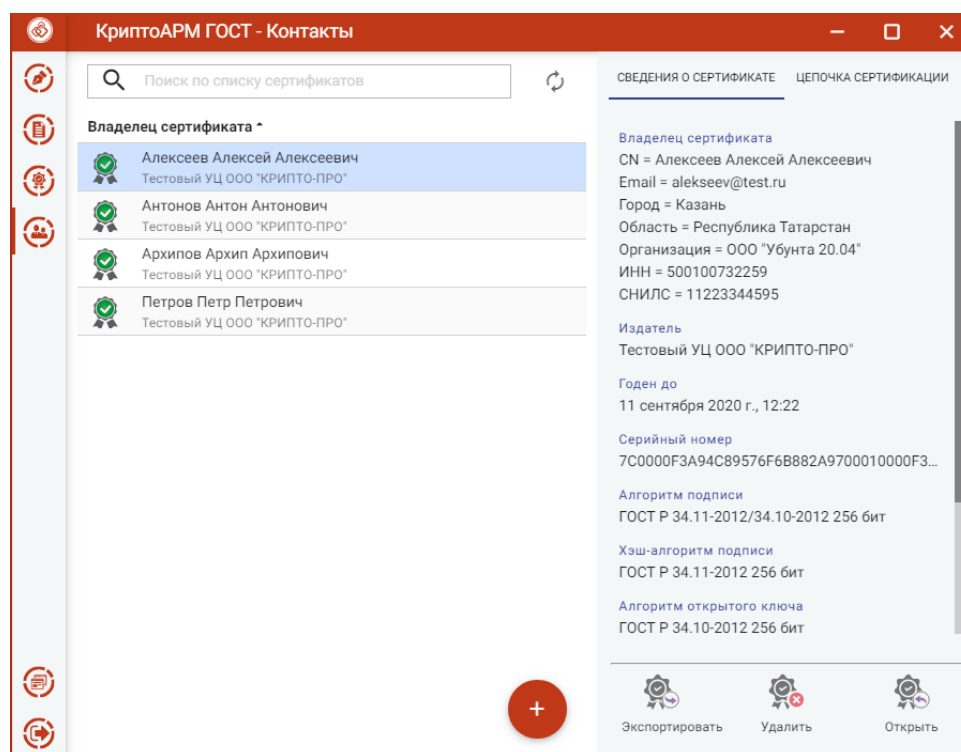


Рисунок 153. Отображение импортированного контакта

ЭКСПОРТ КОНТАКТА В ФАЙЛ. Для экспорта контакта в файл нужно выделить контакт и нажать кнопку операции **Экспортировать** (Рисунок 154).

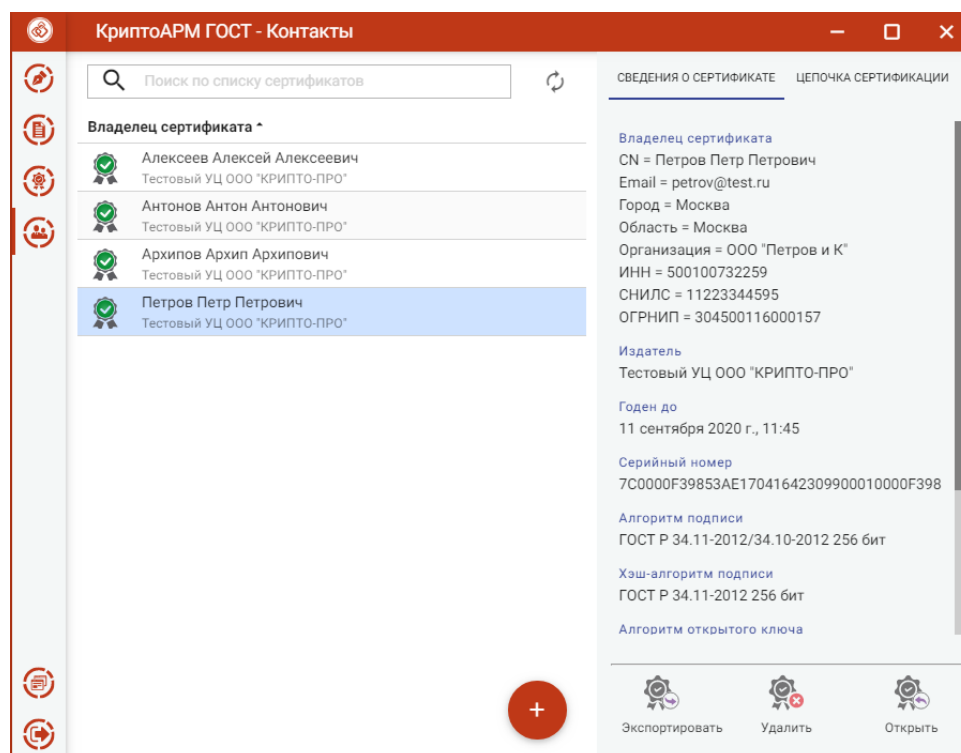


Рисунок 154. Экспорт контактка

При экспорте появляется окно, в котором можно выбрать только кодировку файла сертификата (Рисунок 155).

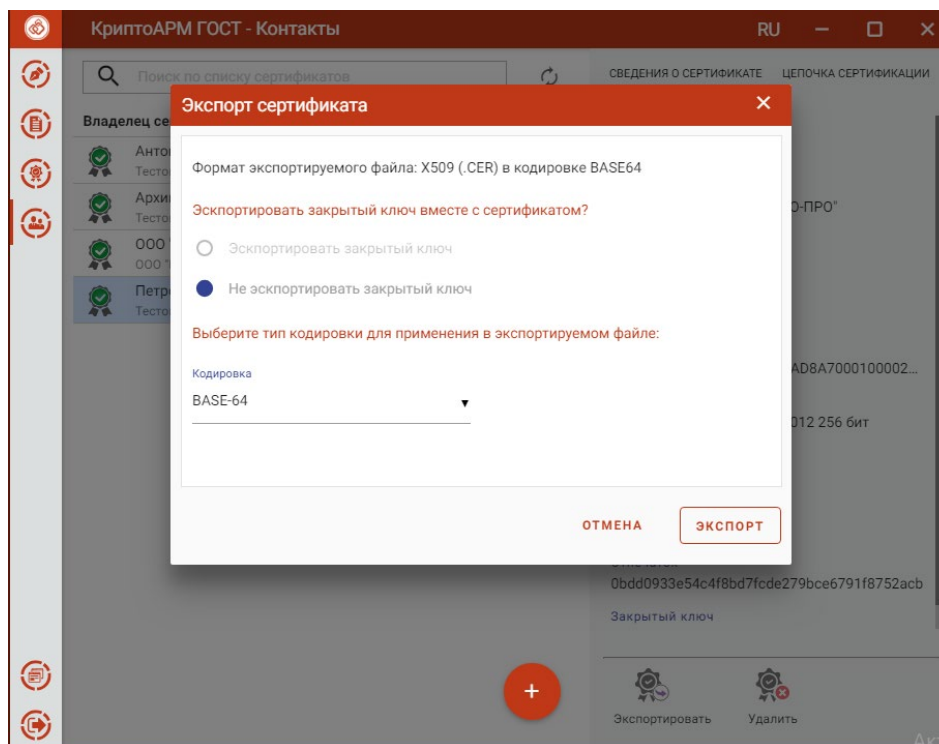


Рисунок 155. Выбор кодировки файла сертификата

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

По окончании операции возникнет сообщение об успешном экспорте сертификата.

УДАЛЕНИЕ КОНТАКТА Для удаления сертификата нужно выбрать операцию **Удалить** (Рисунок 156).

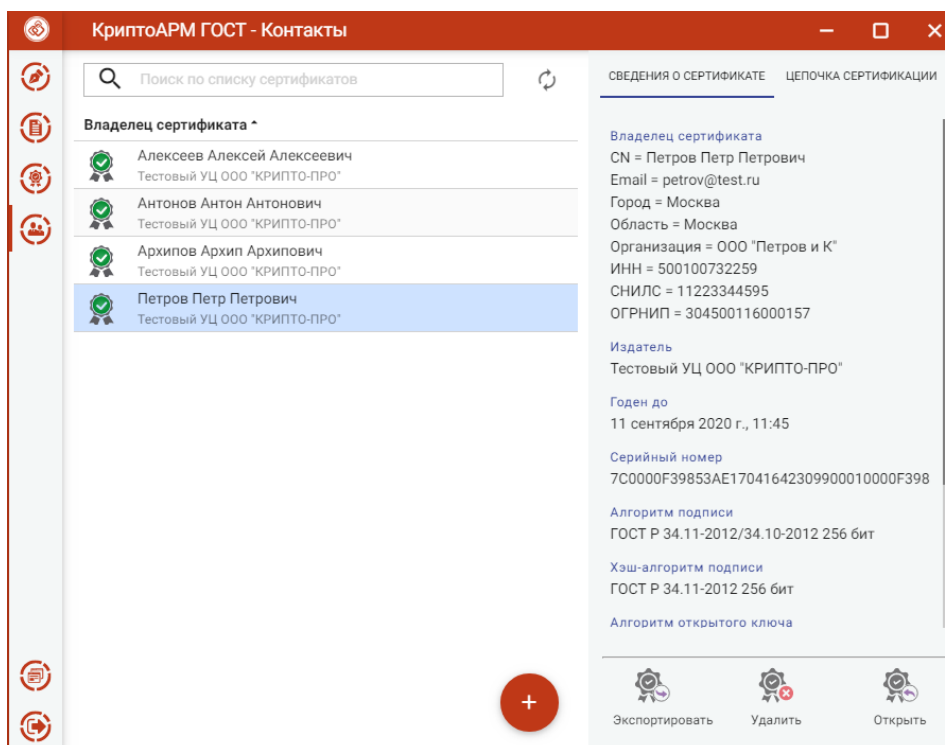


Рисунок 156. Удаление контакта

В появившемся диалоговом окне нажать **Удалить** для подтверждения удаления (Рисунок 157).

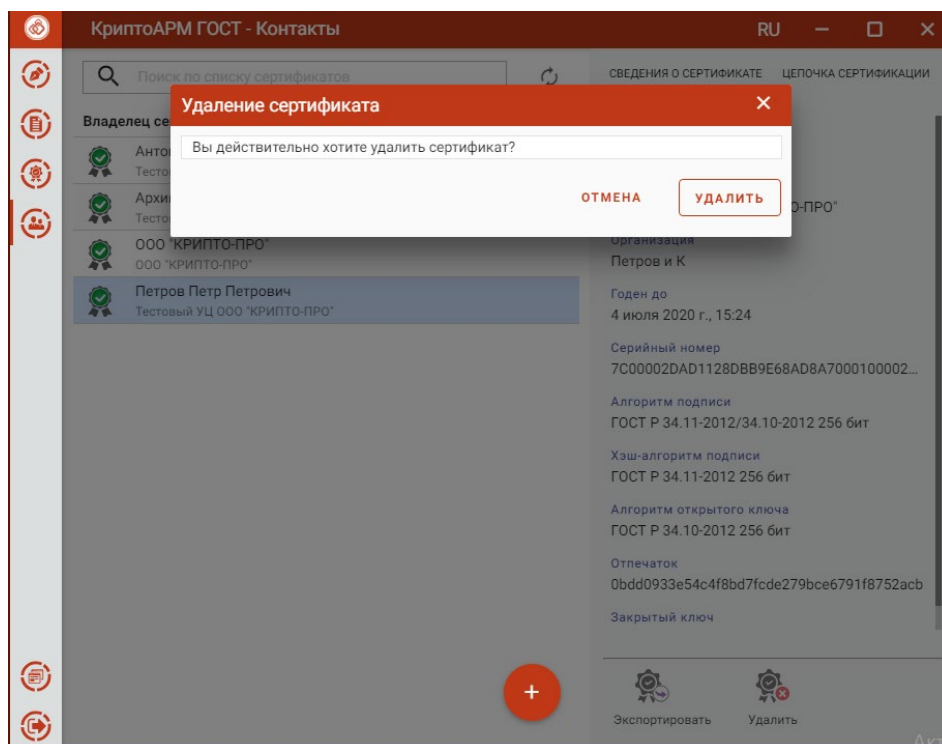


Рисунок 157. Подтверждение удаления контакта

Поиск контакта. Для поиска контакта нужно в строке поиска ввести ключевую фразу (Рисунок 158).

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

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

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

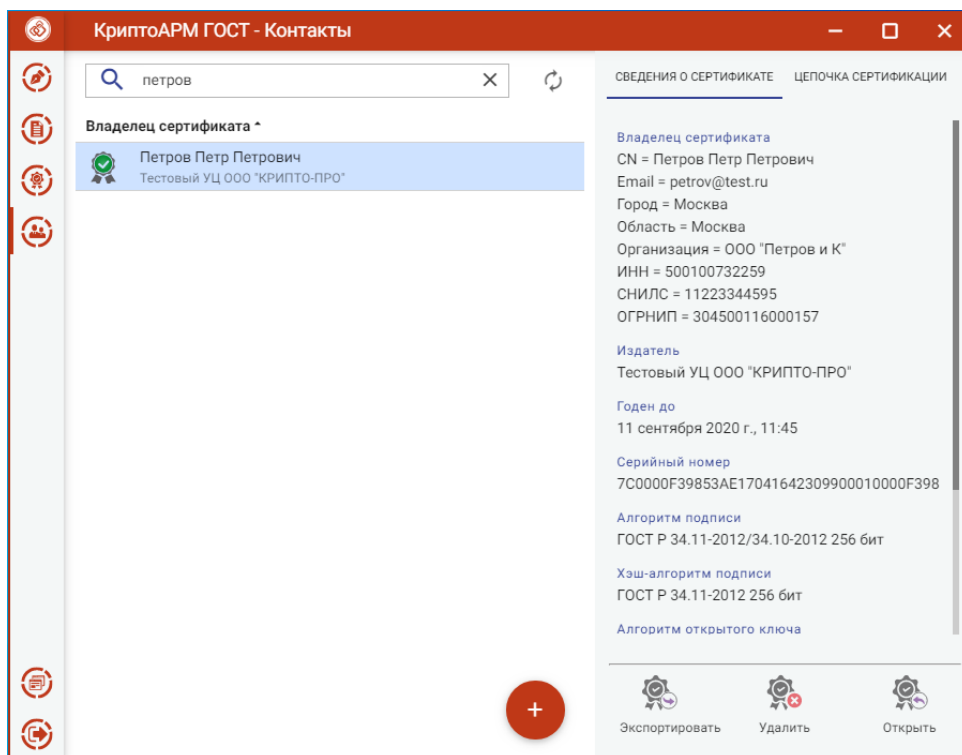


Рисунок 158 Поиск контакта

3.18 О ПРОГРАММЕ

Пункт меню **О программе** содержит подпункты:

- **О программе** – для отображения краткой информации о приложении и лицензиях;
- **Журнал операций** – для отображения выполняемых операций в приложении;

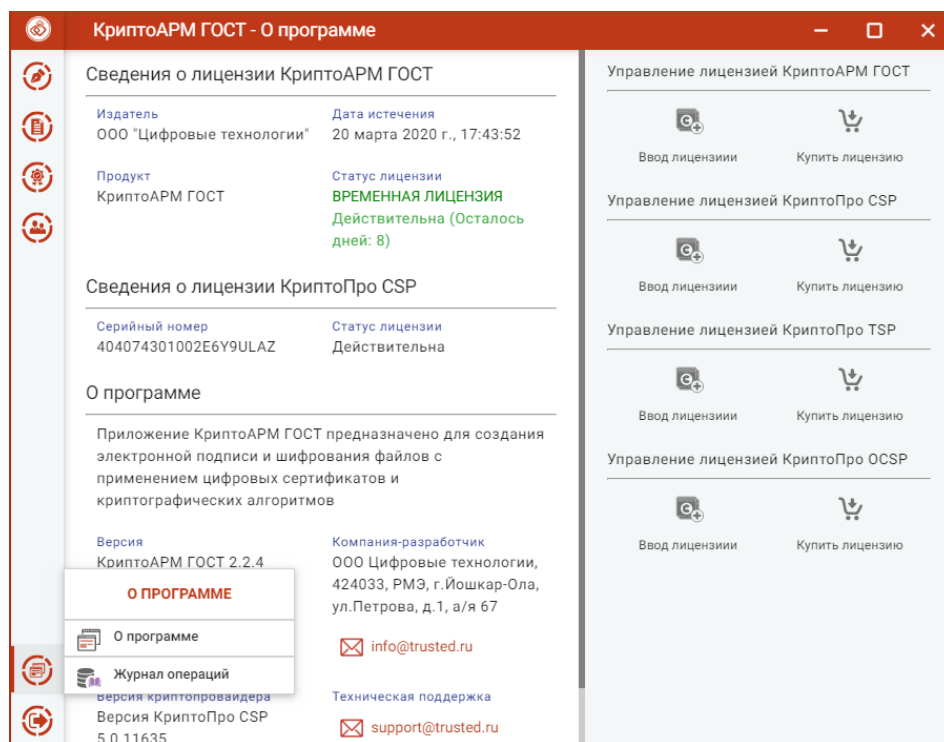


Рисунок 159. Меню О программе

3.18.1 О ПРОГРАММЕ

Краткие сведения о программе, сведения о лицензиях, а также адрес электронной почты для получения дополнительной технической поддержки можно узнать, выбрав подпункт **О программе** (Рисунок 160).

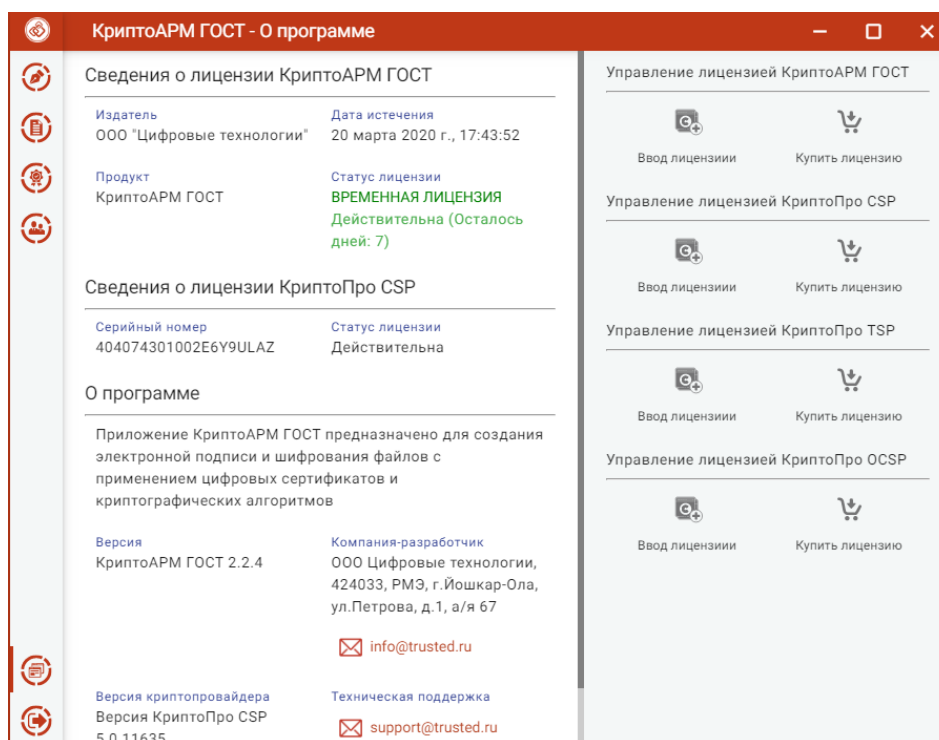
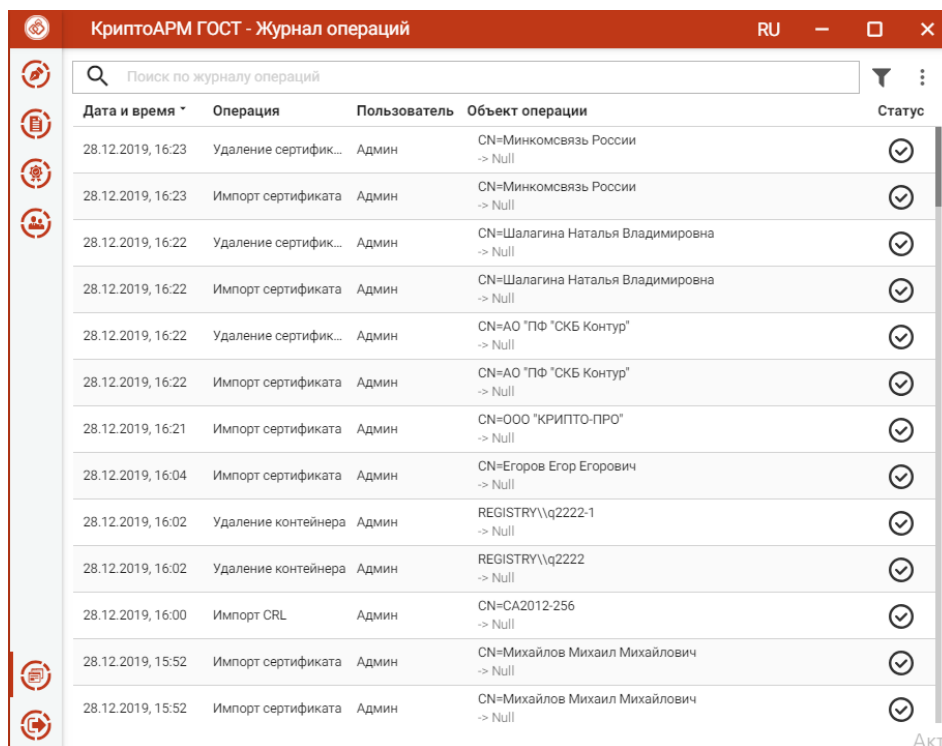


Рисунок 160. Информация о программе

3.18.2 Журнал операций

Журнал операций предназначен для отображения операций, выполняемых пользователем (Рисунок 161).



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

Рисунок 161. Журнал операций

В журнале отображаются следующие типы операций:

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

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

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

При работе с журналом операций предусмотрен режим загрузки ранее сохраненной в архив его части для просмотра, поиска и фильтрации записей. Для этого используется пункт **Загрузить архивный журнал** контекстного меню журнала (Рисунок 162)

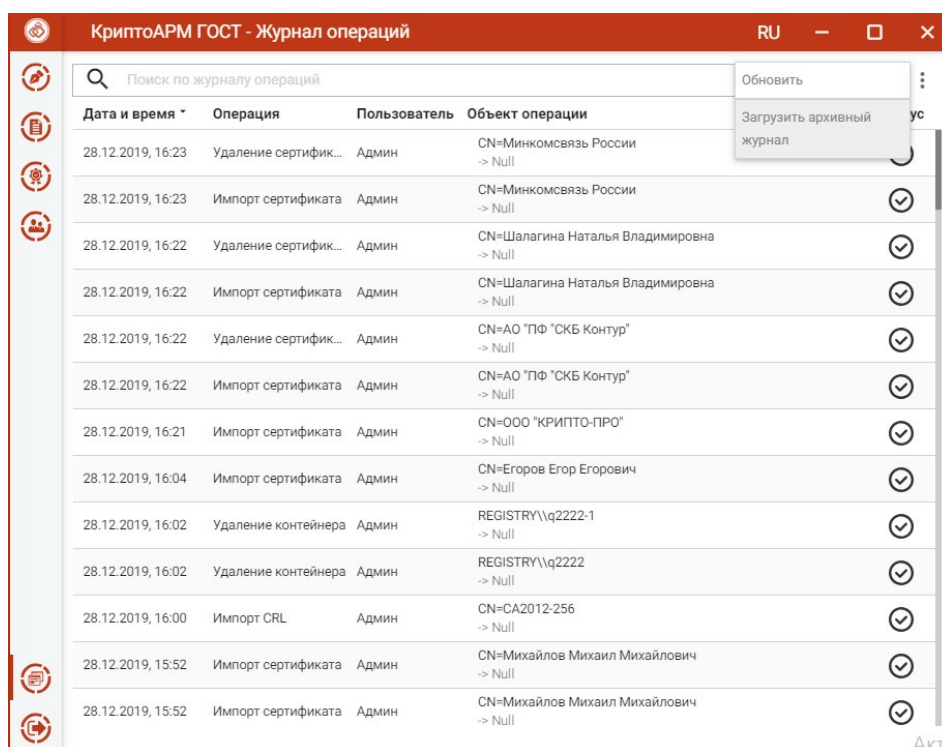


Рисунок 162. Контекстное меню журнала операций

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

Для возврата к текущему журналу операций используется пункт контекстного меню архивного журнала **Вернуться к текущему журналу** (Рисунок 163)

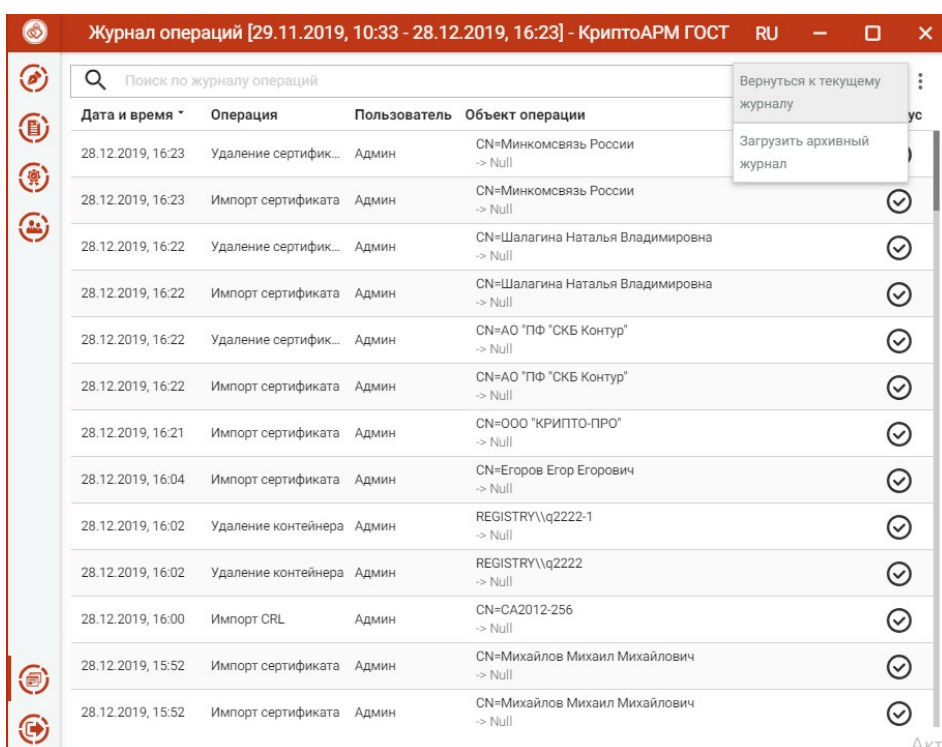


Рисунок 163. Контекстное меню архивного журнала операций

ПОИСК ЗАПИСЕЙ В ЖУРНАЛЕ ОПЕРАЦИЙ. В приложении реализован поиск записей журнала операций по символьному совпадению (Рисунок 164)

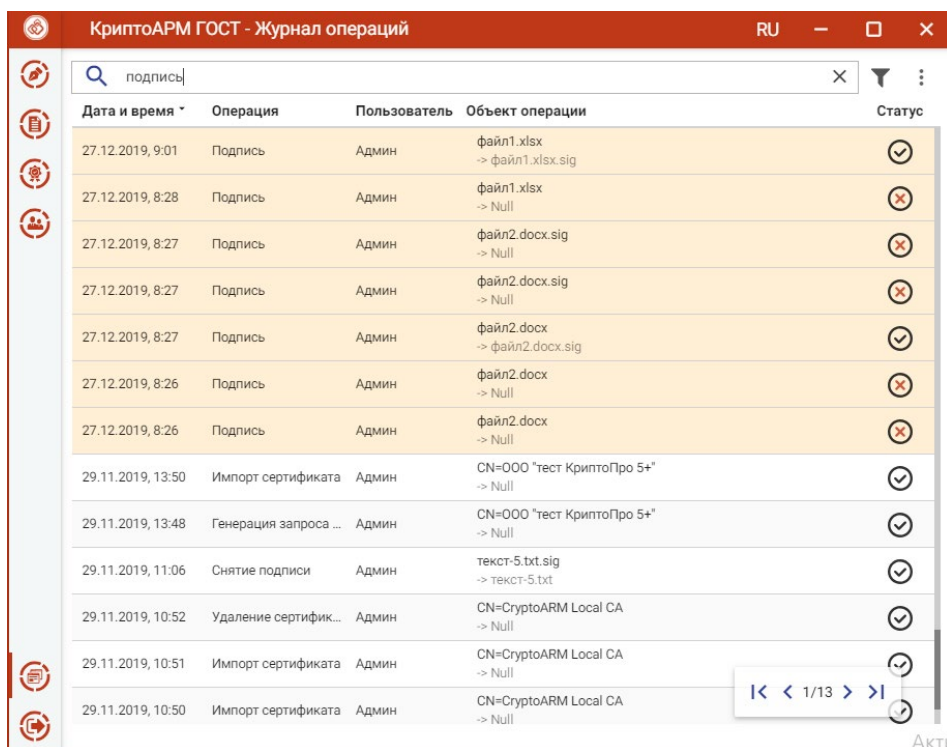


Рисунок 164. Поиск записей в журнале операций

ФИЛЬТРАЦИЯ ЖУРНАЛА ОПЕРАЦИЙ. Для открытия окна настроек критериев фильтра на панели управления имеется кнопка, при нажатии на которую открывается окно настроек фильтрации (Рисунок 165).

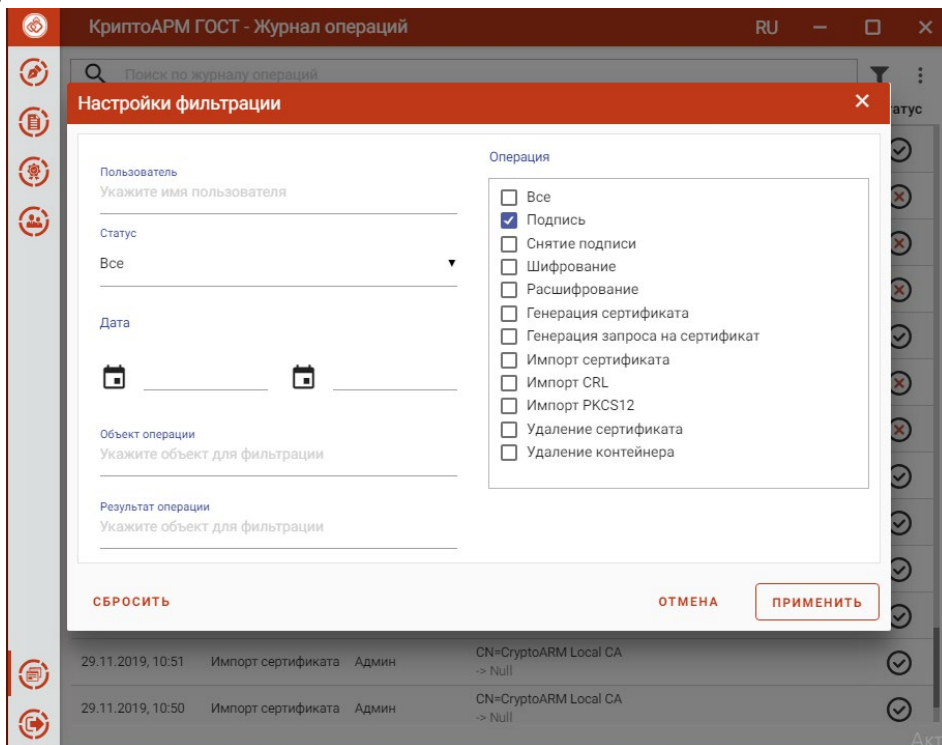
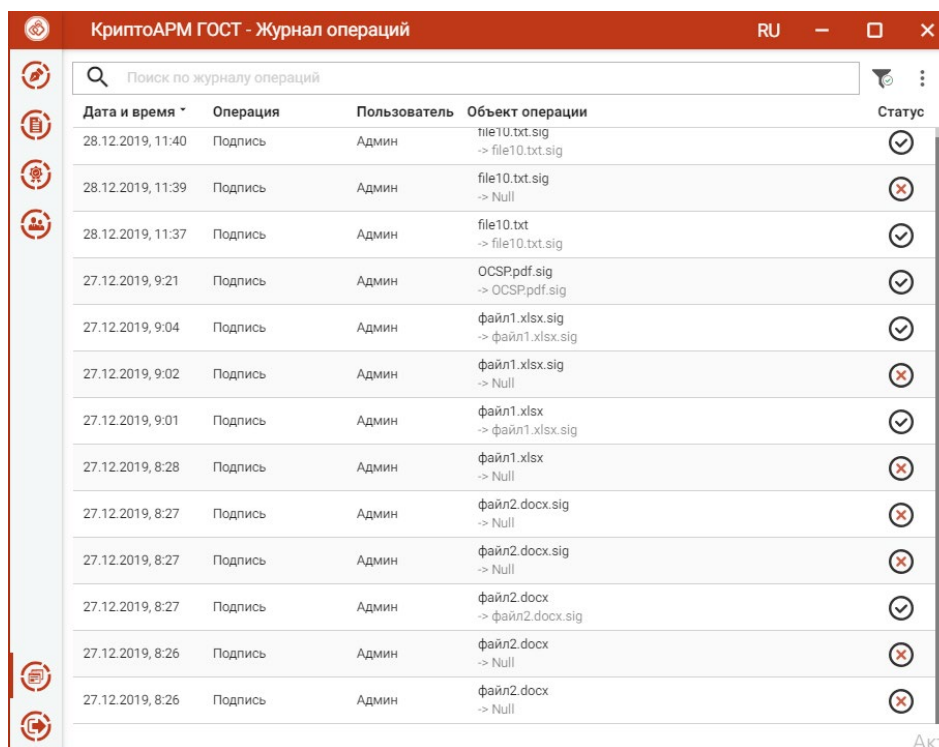


Рисунок 165. Настройки критериев фильтра журнала операций

Применение фильтрации выполняется по нажатию кнопки **Применить**. В зависимости от выставленных критериев фильтра в журнале остаются только те записи, которые удовлетворяют (суммарно) этим критериям (Рисунок 166).



КриптоАРМ ГОСТ - Журнал операций				
Поиск по журналу операций				
Дата и время	Операция	Пользователь	Объект операции	Статус
28.12.2019, 11:40	Подпись	Админ	file10.txt.sig -> file10.txt.sig	✓
28.12.2019, 11:39	Подпись	Админ	file10.txt.sig -> Null	✗
28.12.2019, 11:37	Подпись	Админ	file10.txt -> file10.txt.sig	✓
27.12.2019, 9:21	Подпись	Админ	OCSPPdf.sig -> OCSPPdf.sig	✓
27.12.2019, 9:04	Подпись	Админ	файл1.xlsx.sig -> файл1.xlsx.sig	✓
27.12.2019, 9:02	Подпись	Админ	файл1.xlsx.sig -> Null	✗
27.12.2019, 9:01	Подпись	Админ	файл1.xlsx -> файл1.xlsx.sig	✓
27.12.2019, 8:28	Подпись	Админ	файл1.xlsx -> Null	✗
27.12.2019, 8:27	Подпись	Админ	файл2.docx.sig -> Null	✗
27.12.2019, 8:27	Подпись	Админ	файл2.docx.sig -> Null	✗
27.12.2019, 8:27	Подпись	Админ	файл2.docx -> файл2.docx.sig	✓
27.12.2019, 8:26	Подпись	Админ	файл2.docx -> Null	✗
27.12.2019, 8:26	Подпись	Админ	файл2.docx -> Null	✗

Рисунок 166. Результат применения фильтрации журнала операций

Для сброса заданных критериев фильтрации служит кнопка **Сбросить** в окне настроек фильтрации (Рисунок 165).