

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](mailto:info@trusted.ru)



127018, Москва, Сущёвский Вал, 18

Телефон: 8 (495) 995-48-20

<https://CryptoPro.ru>

E-mail: [info@CryptoPro.ru](mailto:info@CryptoPro.ru)



Средство

Криптографической

Защиты

Информации

КриптоПро CSP версии 5.0 R2 KC1

Исполнение 1-КриптоАРМ

Руководство пользователя

Android

ЖТЯИ.00101-12 92 03

Листов 59

2021 г

## Содержание

1.	Общие сведения о программном продукте .....	3
1.1	Функциональность версии.....	3
1.2	Поддерживаемые криптопровайдеры.....	4
1.3	Лицензия на программный продукт.....	4
1.4	Установка и настройка приложения КриптоАРМ ГОСТ.....	4
2.	Графический пользовательский интерфейс приложения .....	5
2.1	Начало работы с КриптоАрм ГОСТ .....	5
2.2	Поиск в приложении .....	5
2.3	Создание электронной подписи .....	6
2.4	Проверка электронной подписи .....	12
2.5	Снятие электронной подписи.....	15
2.6	Добавление подписи.....	16
2.7	Шифрование файлов.....	20
2.8	Расшифрование файлов.....	25
2.9	Управление списком файлов для выполнения операций .....	27
2.10	Документы .....	31
2.11	Управление сертификатами.....	34
2.12	Операции над сертификатами.....	35
2.13	Импорт сертификата из файла.....	38
2.14	Создание запроса на сертификат .....	42
2.15	Списки отзыва сертификатов (СОС).....	46
2.16	Управление контейнерами .....	49
2.17	Контакты .....	53
2.18	Лицензии .....	56
2.19	Журнал операций.....	57

## Аннотация

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

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

Использование СКЗИ КриптоПро 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

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

Приложение КриптоАРМ ГОСТ является кроссплатформенным. На каждой из платформ реализована поддержка российских криптографических стандартов посредством использования криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base.

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

### 1.1 Функциональность версии

Приложение текущей версии рассчитано на выполнение операций:

- 
- |                     |   |
|---------------------|---|
| Электронная подпись | — электронная подпись файлов размером до 50 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память;   |
|                     | — Проверка ЭП размером 50 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память;   |
|                     | — добавление электронной подписи к уже существующим (функция создания соподписи) размером до 50 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память; |
|                     | — создание как присоединенной, так и отдельной электронной подписи.   |
- 

- |            |  |
|------------|--|
| Шифрование | — шифрование и расшифрование файлов размером до 50 Мб 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 | — отображение сертификатов и привязанных к ним ключей ЭП |
|------------|--|
-

сертификатами ключами	и	относительно хранилищ криптопровайдера КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base;
	–	проверка корректности выбранного сертификата с построением цепочки доверия;
	–	хранение ключей ЭП на носителях Рутокен (Актив) 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 управление журналом операций	и	– 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 на КриптоАРМ ГОСТ сроком на 14 дней и на КриптоПро CSP на 93 дня. 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».

## 1.4 Установка и настройка приложения КриптоАРМ ГОСТ

Инсталляция, деинсталляция и обновление средства криптографической защиты информации КриптоПро CSP версии 5.0 R2 KC1 Исполнение 1-КриптоАРМ (далее — КриптоАРМ ГОСТ) происходит через магазин приложений Play Маркет. Для этого необходимо найти приложение в магазине и установить.

## 2. Графический пользовательский интерфейс приложения

### 2.1 Начало работы с КриптоАрм ГОСТ

Работа с приложением КриптоАРМ ГОСТ начинается со страницы **Мастер подписи и шифрования** (Рис. 2.1.1).

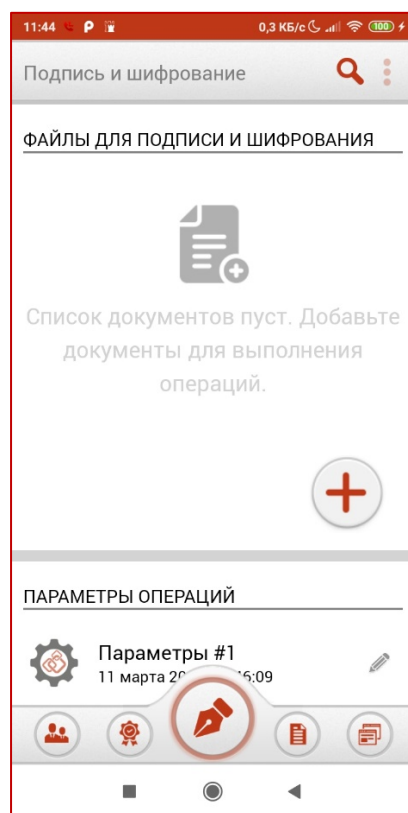


Рис. 2.1.1 Главное окно при запуске приложения

В мастере **Подписи и шифрования** выбранные для операции документы объединены со значениями параметров операций. Эти параметры идут последовательно и разделены на блоки:

- **Параметры операций** - выбор сохраненных параметров операций, сохранение, создание копии и т.д.
- **Операции** - выбор требуемых операций и режимов сохранения, отправки результатов (оригиналов документов).
- **Сертификат подписи** и **Сертификат шифрования** - сертификаты из числа личных сертификатов и контактов, которые используются для операций подписи документов и их шифрования.
- **Параметры подписи** - необходимые настройки для выполнения операции подписи документов.
- **Параметры шифрования** - настройки для выполнения операции шифрования.

### 2.2 Поиск в приложении

В элементах пользовательского интерфейса реализована функция поиска файлов (Рис. 2.2.1). Для включения режима нужно нажать на кнопку **Поиск** и в строке ввести ключевую фразу.

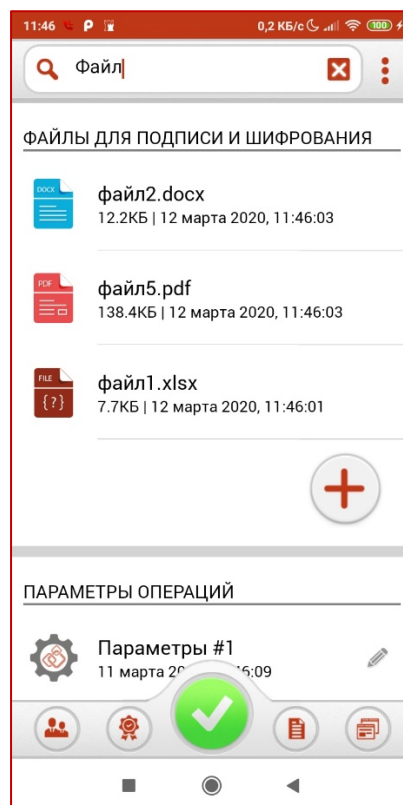


Рис. 2.2.1 Поиск в Мастере подписи и шифрования

Поиск файлов реализован на основе совпадения ключевой фразы с названием файла. В результате вместо полного списка в окне остаются только файлы, удовлетворяющие критерию поиска.

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

*Примечание.* В случае неправильно указанного критерия поиска список файлов может оказаться пустым, о чем будет свидетельствовать надпись - «Ничего не найдено».

## 2.3 Создание электронной подписи

Для подписи файлов нужно в **Мастере подписи и шифрования** выбрать подписываемые файлы, сертификат подписи и задать параметры подписи.

### Выбор подписываемых файлов

В КриптоАрм ГОСТ можно подписывать один или сразу несколько файлов. Размер подписываемого файла зависит от модели телефона, не рекомендуется подписывать файлы больше 50 Мб.

Файлы добавляются в раздел **Файлы для подписи и шифрования**. В данном разделе необходимо нажать на кнопку добавления  или импортировать файлы через стороннее приложение.

Файлы отобразятся в списке (Рис. 2.3.1).

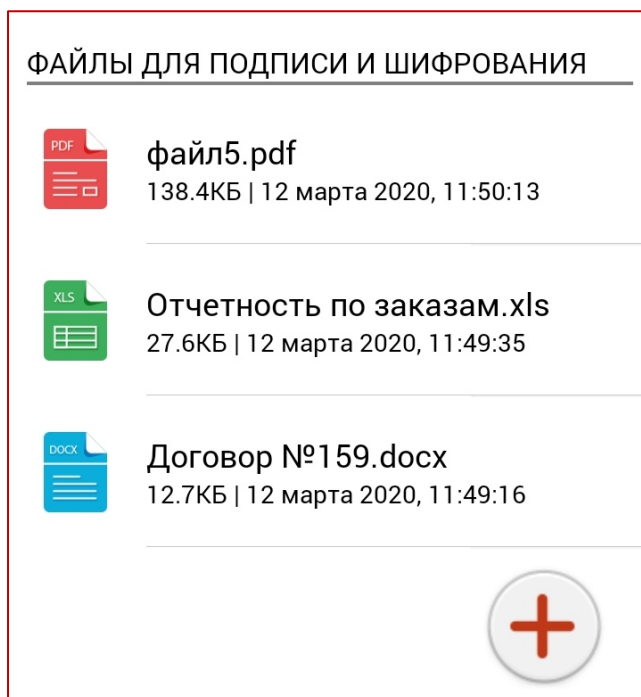


Рис. 2.3.1 Выбор файлов для подписи

Для данного списка доступны поиск, управление файлами в списке через контекстное меню и свайп для каждого файла (Рис. 2.3.2).

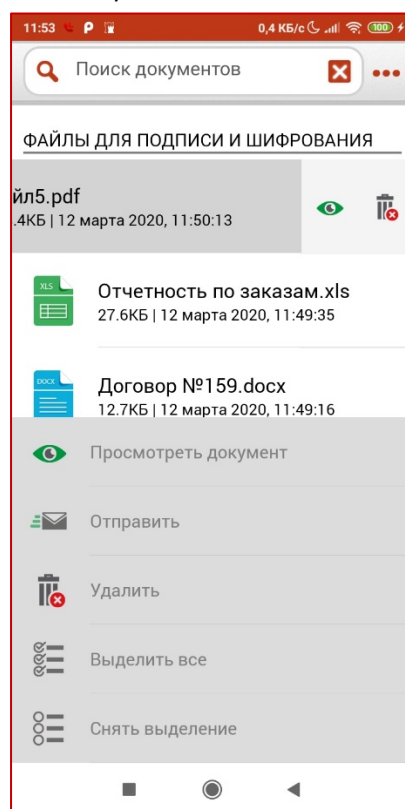



Рис. 2.3.2 Операции над списком файлов

### **Выбор сертификата подписи**

Для того, чтобы выполнить подпись необходимо выбрать сертификат с ключом ЭП из списка **Личных сертификатов**. Эта операция производится нажатием на иконку карандаша  в разделе **Сертификат подписи** (Рис. 2.3.3).

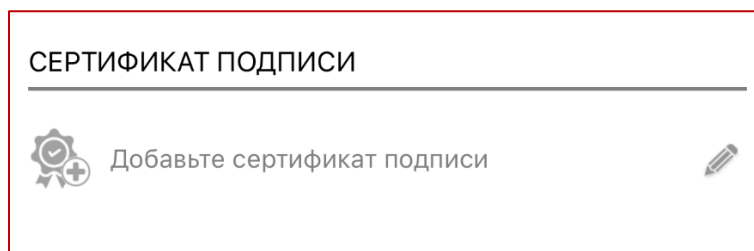


Рис. 2.3.3 Сертификат подписи не выбран

В появившемся представлении отображаются личные сертификаты (Рис. 2.3.4).

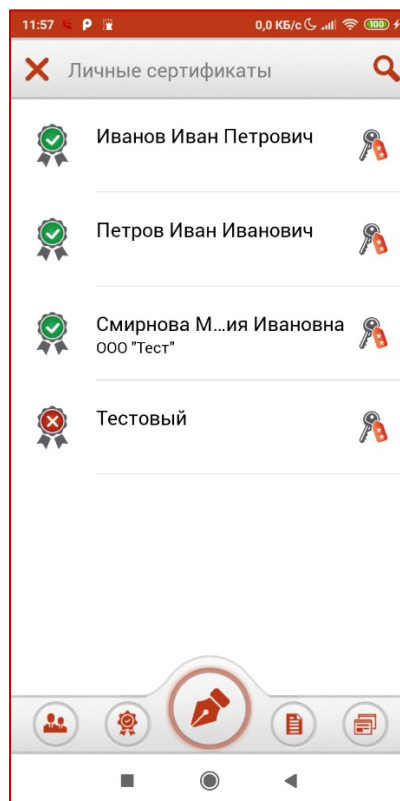



Рис. 2.3.4 Список личных сертификатов

Выбор сертификата подписи осуществляется его выделением. Если был выбран неправильный сертификат, то его можно заменить повторным нажатием на иконку .

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

После успешного выбора сертификат отображается в разделе **Сертификат подписи** (Рис. 2.3.5).

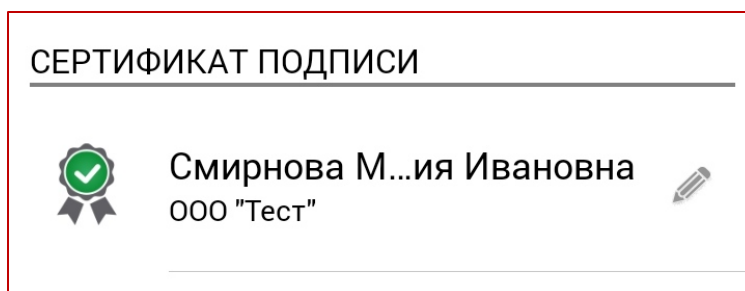


Рис. 2.3.5 Сертификат подписи выбран

### Установка параметров подписи



Параметры подписи задаются в разделе **Параметры подписи** (Рис. 2.3.6).

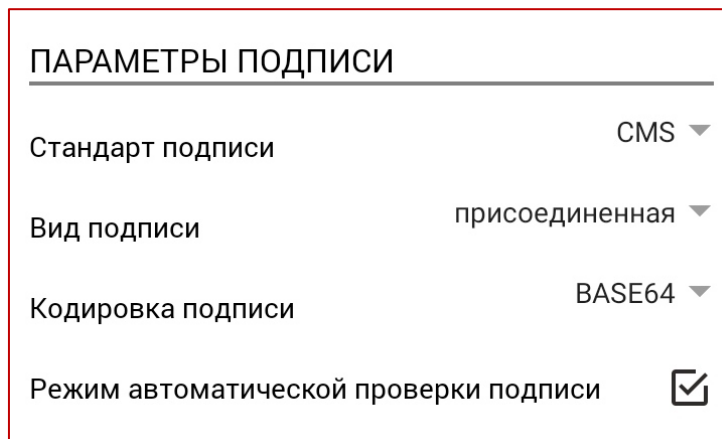


Рис. 2.3.6 Параметры подписи

В параметрах можно настроить:

- **Стандарт подписи** - CMS для создания классической подписи.
- **Вид подписи** – присоединённая или отсоединённая.
- **Кодировка** - сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Режим автоматической проверки подписи** – корректность подписи проверяется сразу же после добавления или создания подписанного файла.

### Подпись файлов

Для подписи файлов в разделе **Операции** необходимо установить переключатель **Подпись файлов** (Рис. 2.3.7).

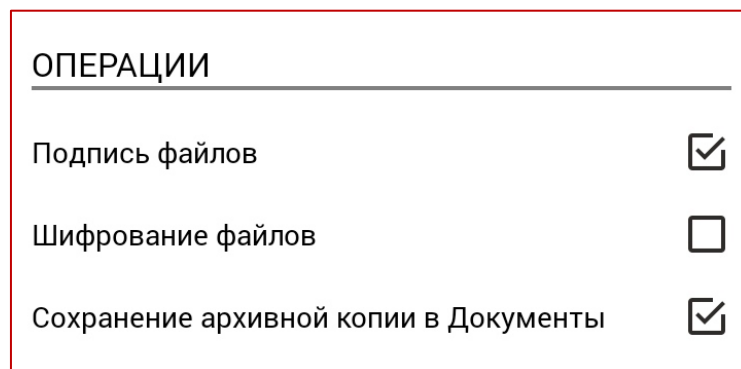


Рис. 2.3.7 Выбор операций в Мастере подписи и шифрования

После выполнения всех условий:

- добавлен хотя бы один файл;
- выбран сертификат подписи;
- установлен переключатель **Подпись** (если необходимо только подписать файлы, переключатель **Шифрование** должен быть не активен);

появляется кнопка **Выполнить** .

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

Подписываемые файлы обязательно необходимо просмотреть перед операцией. Далее появляется диалоговое окно с вопросом: «Документы просмотрены перед подписанием?»

(Рис. 2.3.8). Если документы просмотрены, то необходимо нажать **Да** и начнется процесс подписи. В противном случае, рекомендуется нажать **Отмена** и просмотреть документы.

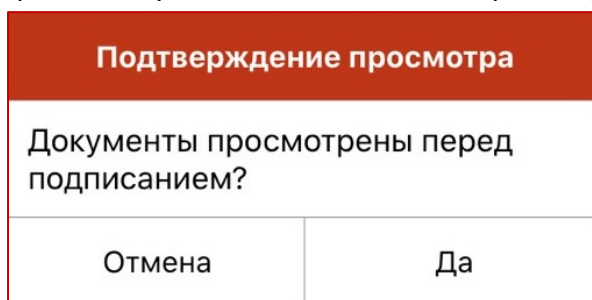


Рис. 2.3.8 Подтверждение просмотра документов

Выбранные файлы подписываются по очереди. Если сертификат защищен паролем, при подписи появится диалоговое окно для подтверждения пароля (Рис. 2.3.9). По кнопке **Отмена** операция подписи не выполняется.

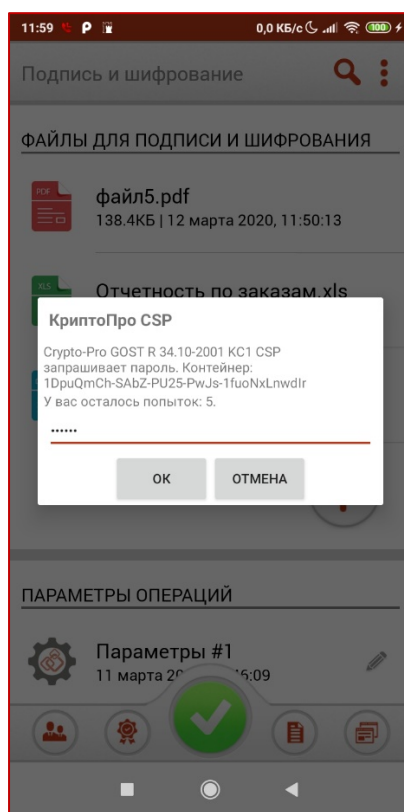


Рис. 2.3.9 Ввод пароля

Для подписанных файлов меняется иконка, наименование, дата создания.

Если в разделе **Операции** стоит флаг **Сохранение архивной копии в Документы** (Рис. 2.3.7), то подписанные файлы сохраняются в представление **Документы**. Независимо от наличия сохранения в документы, результат операции подписания отображается в разделе **Мастер подписи и шифрования** (Рис. 2.3.10).



Рис. 2.3.10 Результат подписи

*Примечание:* По кнопке **Сохранить параметры операций** можно сохранить текущие настройки, для последующего подписания документов (Рис. 2.3.10).

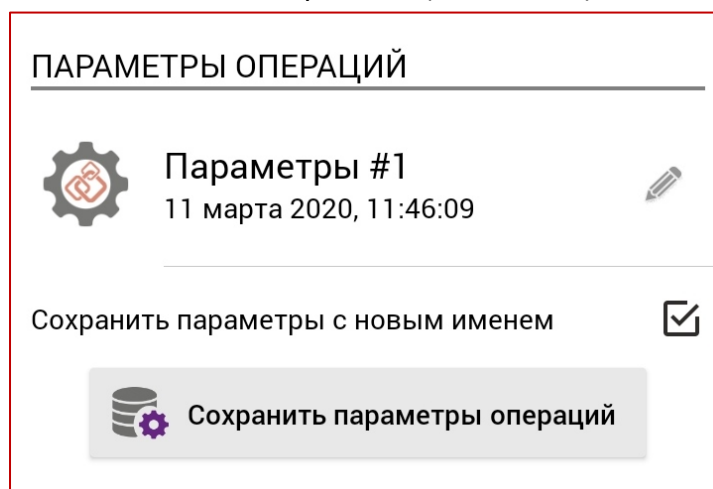


Рис. 2.3.11 Текущая настройка

Если установлен переключатель напротив **Сохранить параметры с новым именем**, то будет создана новая настройка, где сохранены изменения из разделов **Операции**, **Сертификат подписи**, **Сертификат шифрования**, **Параметры подписи**, **Параметры шифрования** (Рис. 2.3.12).

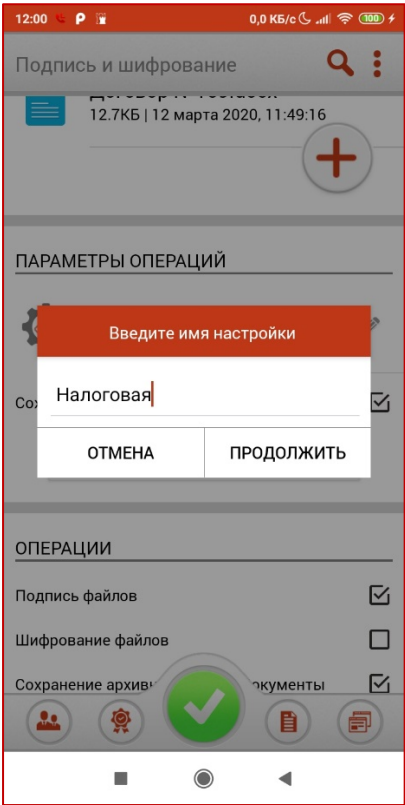



Рис. 2.3.12 Сохранение настройки под новым именем




2.4 Проверка электронной подписи

Для проверки подписи достаточно выделить файлы с расширением **.sig**, которые содержат электронную подпись. В результате иконка подписанного файла меняется на иконку с отображением статуса подписи.

Результатом проверки подписи является отображение информации о подписи документа в виде изменения иконки подписанного файла  на иконку, содержащую статус подписи (Рис. 2.4.1).

Все возможные статусы продемонстрированы в таблице 1.

Таблица 1. Описание статусов подписей

3. Статус подписи	4. Описание
	Подпись корректна.
	Подпись некорректна.
	Невозможно проверить подпись. Статус выставляется в том случае, например, когда проверку осуществляется через API внешнего сервиса и в текущий момент времени необходимый ответ не получен или не установлено соединение.

Данный статус появляется, если подпись - отсоединенная и в списке мастера отсутствует оригинальный документ, необходимый для проверки.

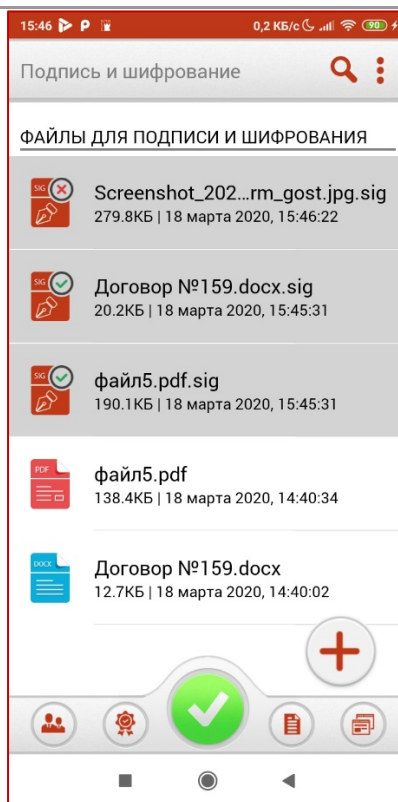


Рис. 2.4.1 Результат проверки подписи

Если в списке выделен один подписанный файл, то при вызове контекстного меню, среди доступных операций имеется операция **Свойства подписи**, которая открывает результат проверки подписи в отдельном представлении. На Рис. 2.4.2 показано представление для отображения свойств подписи документа. Свойства подписи отображаются единым списком с полосой прокрутки.

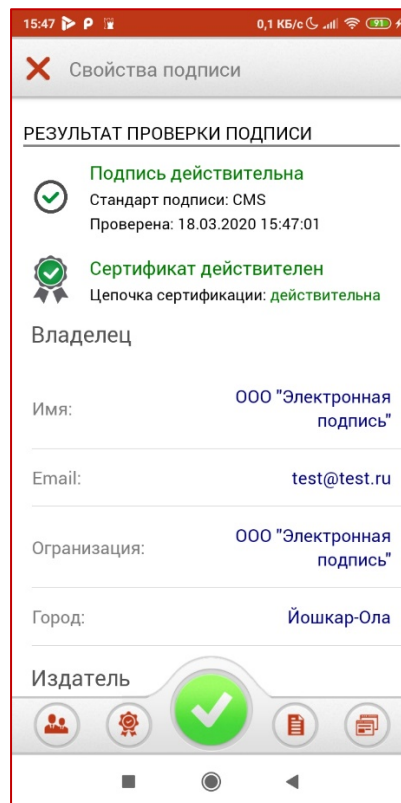


Рис. 2.4.2 Отображение свойств подписанного файла

Если документ подписан несколькими подписями (имеет соподписи), то для просмотра информации о подписи нужно выбрать сертификат подписи (Рис. 2.4.3).

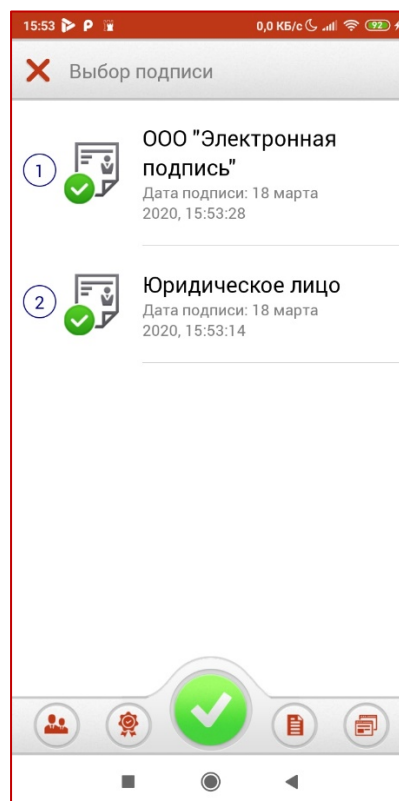


Рис. 2.4.3 Отображение свойств соподписи

## 4.1 Снятие электронной подписи

Для снятия подписи достаточно выбрать подписанный файл - файл с расширением .sig, который содержит электронную подпись и нажать на кнопку **Снять подпись** в контекстном меню (Рис. 2.5.1).

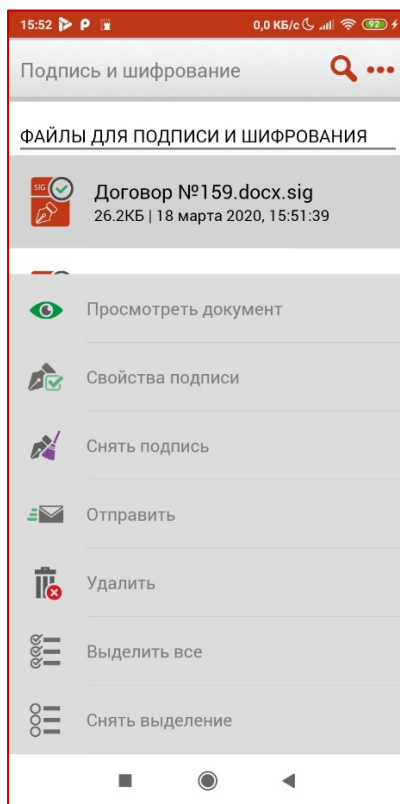


Рис. 2.5.1 Вызов контекстного меню для снятия подписи

При снятии подписи у файлов меняется иконка, наименование, дата создания (Рис. 2.5.2). У отдельной подписи при выполнении операции снятия подписи возникает сообщение об ошибке.

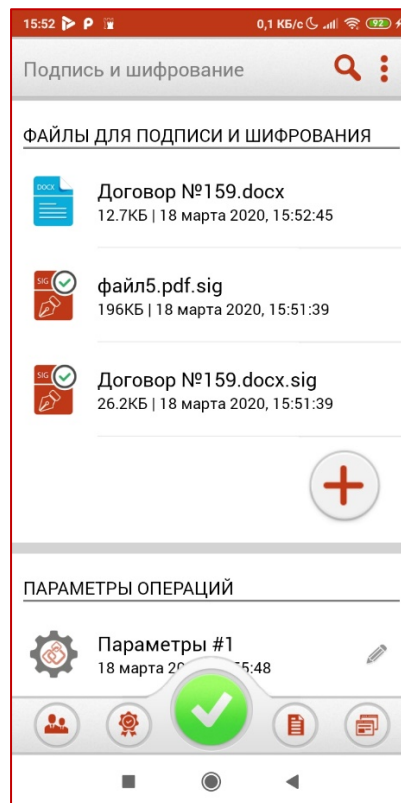


Рис. 2.5.2 Подпись с документов снята

## 4.2 Добавление подписи

Приложение КриптоАРМ ГОСТ позволяет добавлять электронные подписи к уже подписанному файлу. Добавление подписи осуществляется по нажатию на кнопку **Выполнить**



. Для того, чтобы кнопка выполнения стала активной необходимо выполнение следующих условий:

- добавлен хотя бы один подписанный файл (Рис. 2.6.1);



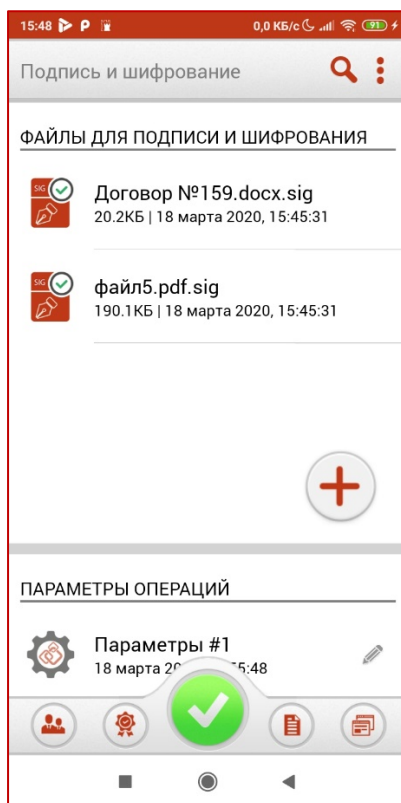


Рис. 2.6.1 Исходные файлы

- выбран сертификат подписи (Рис. 2.6.2);

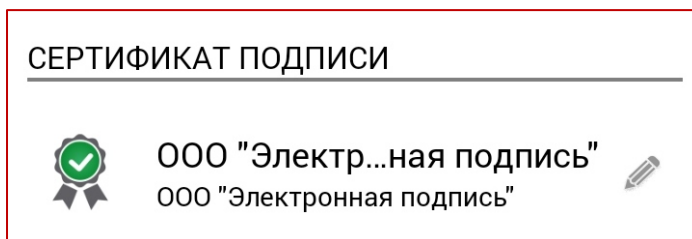


Рис. 2.6.2 Выбран сертификат подписи

- установлен переключатель **Подпись**. Если необходимо только подписать файлы, переключатель **Шифрование** должен быть не активен. (Рис. 2.6.3).

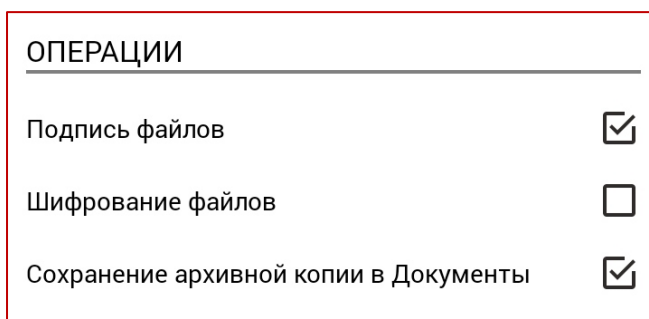


Рис. 2.6.3 Выбор операции

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

Подписываемые файлы обязательно необходимо просмотреть перед операцией. Далее появляется диалоговое окно с вопросом: «Документы просмотрены перед подписанием?» (Рис. 2.6.4). Если документы просмотрены, то необходимо нажать **Да** и начнется процесс подписи. В противном случае, рекомендуется нажать **Отмена** и просмотреть документы.

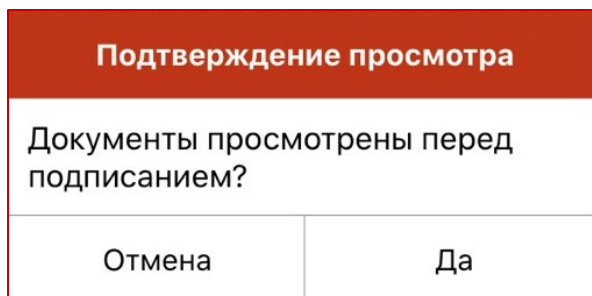


Рис. 2.6.4 Подтверждение просмотра документов

Результат добавления подписи отображается тут же в **Мастере подписи и шифрования**. Если в разделе **Операции** выбрано **Сохранение архивной копии в Документы**, то дополнительно результат подписи добавляется в компонент **Документы** (Рис. 2.6.5)

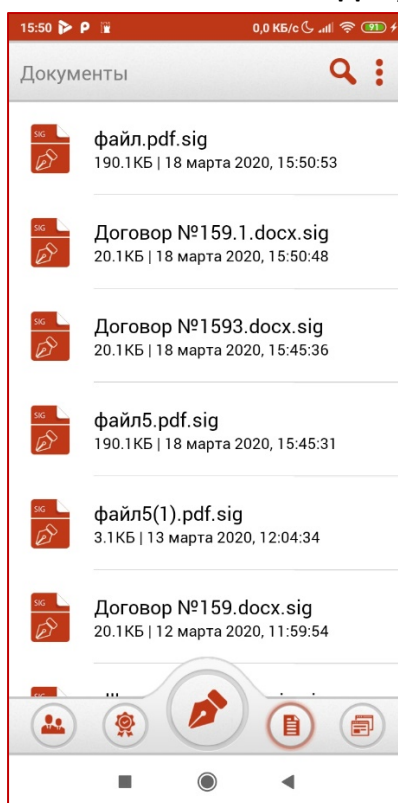


Рис. 2.6.5 Отображение результата операций в документах

Если имя добавляемого файла в **Документы** не уникально, то появляется окно для ввода нового названия документа (Рис. 2.6.6).

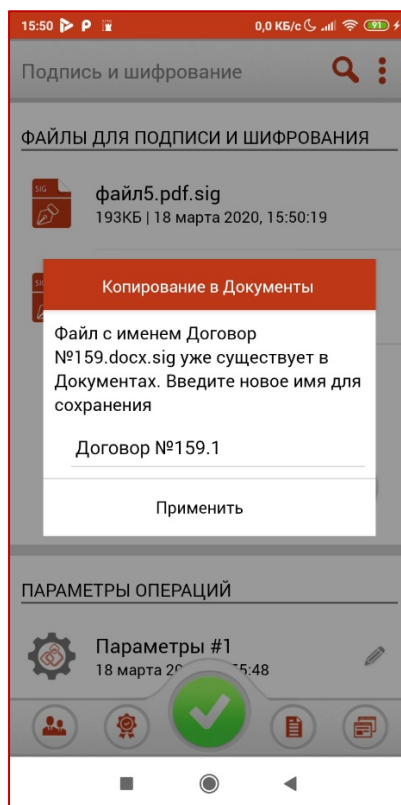


Рис. 2.6.6 Ввод нового названия документа

В информации о подписи содержатся сведения о всех подписях. Чтобы посмотреть информацию о конкретной подписи, нужно выбрать сертификат из списка, нажав на **Свойства подписи** (Рис. 2.6.7).

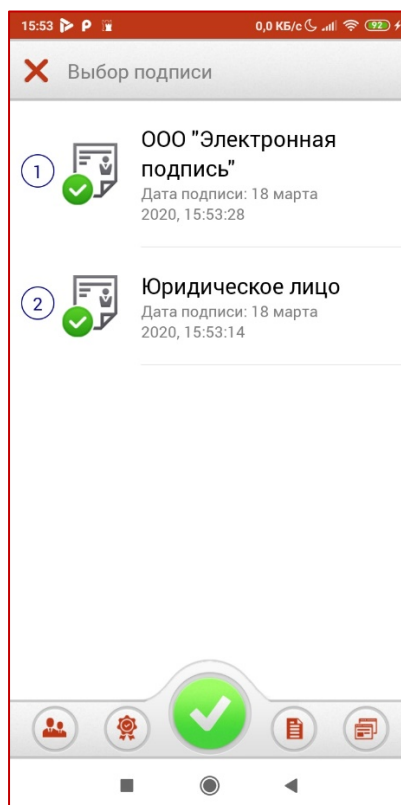



Рис. 2.6.7 Отображение свойств добавленной подписи

### 4.3 Шифрование файлов

Для шифрования файлов нужно в **Мастере подписи и шифрования** выбрать шифруемые файлы, сертификат шифрования и задать параметры шифрования.

#### Выбор шифруемых файлов

В КриптоАрм ГОСТ шифровать можно один или сразу несколько файлов. Размер шифруемого файла зависит от модели телефона, не рекомендуется шифровать файлы больше 50 Мб.

Файлы добавляются в раздел **Фалы для подписи и шифрования**. В данном разделе необходимо нажать на кнопку добавления файлов  или добавить файлы из стороннего приложения. Файлы должны отображаться в разделе **Файлы для подписи и шифрования** (Рис. 2.7.1).

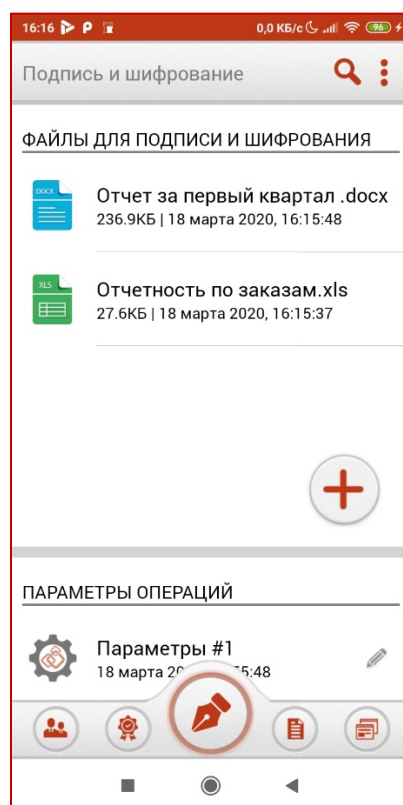


Рис. 2.7.1 Выделение файлов для шифрования

Для данного списка доступны поиск, управление файлами в списке через контекстное меню и свайп для каждого файла (Рис. 2.7.2).

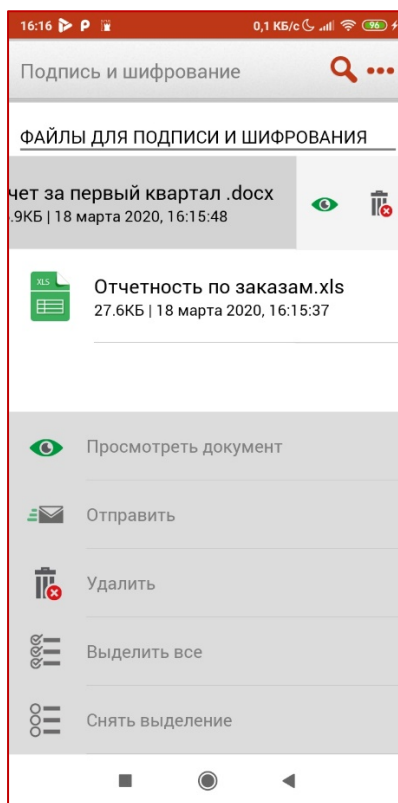



Рис. 2.7.2 Операции над списком файлов

### **Выбор сертификата шифрования**

Для того, чтобы выполнить шифрование необходимо выбрать сертификаты получателей.

Эта операция производится нажатием на иконку карандаша  в разделе **Сертификат шифрования** (Рис. 2.7.3).

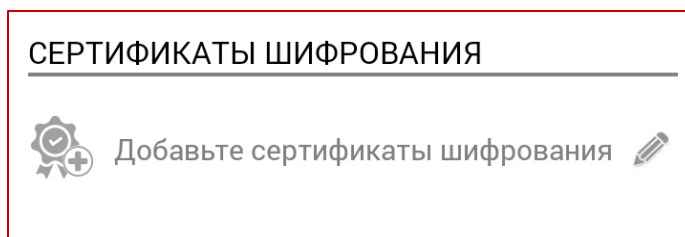



Рис. 2.7.3 Сертификаты шифрования не выбраны

Выбор сертификатов шифрования осуществляется из списка **Контакты**, в составе которого отображаются и личные сертификаты (Рис. 2.7.4). В списке **Контакты** возможен множественный выбор сертификатов, поэтому окончательный набор элементов фиксируется кнопкой  и передается в мастер подписи и шифрования.

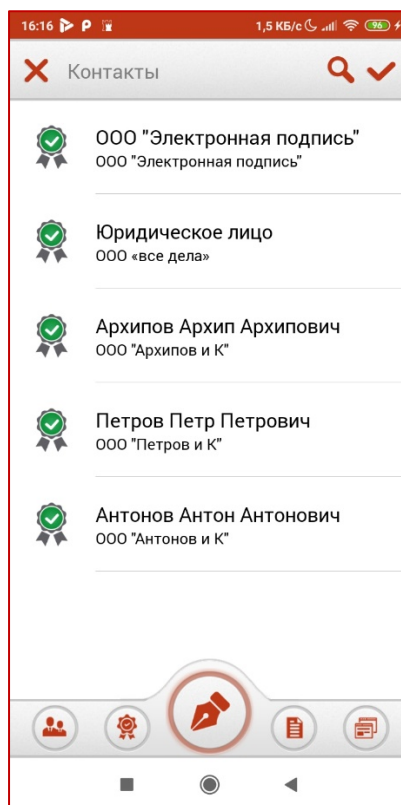



Рис. 2.7.4 Выбор сертификатов шифрования

Если был выбран неправильный сертификат, то его можно заменить повторным нажатием на иконку .

Если в хранилище отсутствуют сертификаты, то их можно создать или импортировать в разделе **Сертификаты**.

После успешного выбора сертификаты отображаются в разделе **Сертификаты шифрования** (Рис. 2.7.5).

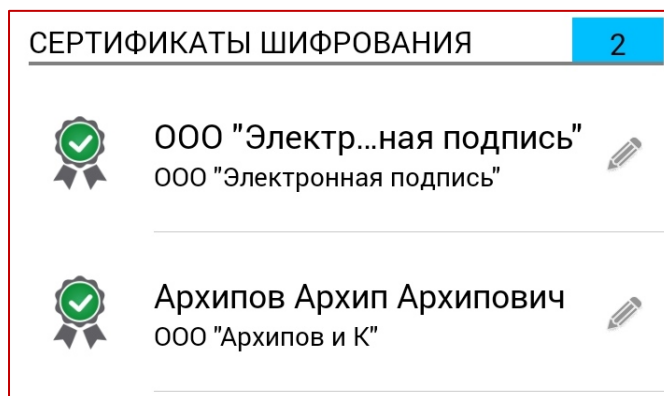


Рис. 2.7.5 Сертификаты шифрования выбраны

### Установка параметров шифрования

Параметры шифрования задаются в разделе **Параметры шифрования** (Рис. 2.7.6).

ПАРАМЕТРЫ ШИФРОВАНИЯ	
Алгоритм шифрования	ГОСТ 28147-89 ▼
Кодировка шифрования	BASE64 ▼
Архивировать файлы перед шифрованием	<input type="checkbox"/>
Проверять keyAgreement	<input type="checkbox"/>

Рис. 2.7.6 Параметры шифрования

В параметрах можно настроить:

- **Кодировка** - сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Архивировать перед шифрованием** - файлы архивируются (ZIP) перед выполнением операции шифрования. Шифруется созданный ZIP-архив.
- **Проверять keyAgreement** - 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.

### Шифрование файлов

Для шифрования файлов в разделе **Операции** необходимо установить переключатель **Шифрование файлов** (Рис. 2.7.7).

ОПЕРАЦИИ	
Подпись файлов	<input type="checkbox"/>
Шифрование файлов	<input checked="" type="checkbox"/>
Сохранение архивной копии в Документы	<input checked="" type="checkbox"/>

Рис. 2.7.7 Выбор операции

После выполнения всех условий:

- установлен переключатель **Шифрование**;
- добавлен хотя бы один файл;
- выбран хотя бы один сертификат шифрования



появляется кнопка **Выполнить**.

Нажатие на кнопку **Выполнить** запускает процесс шифрования. Выбранные файлы шифруются по очереди. Для зашифрованных файлов меняется иконка, расширение, дата создания (Рис. 2.7.8).

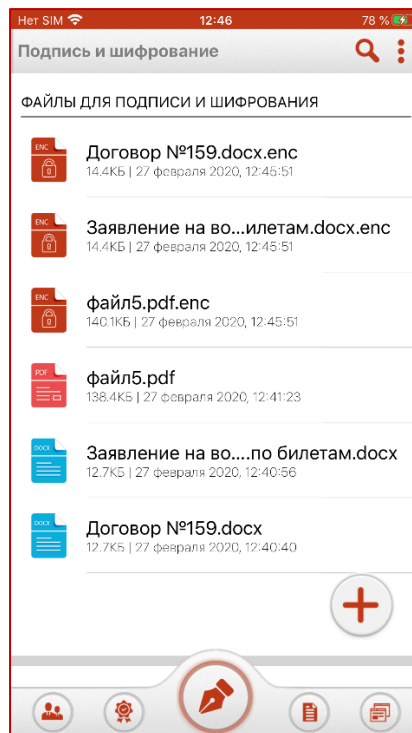


Рис. 2.7.8 Результат операции шифрования

Если в разделе **Операции** стоит флаг **Сохранение архивной копии в Документы** (Рис. 2.7.7), то зашифрованные файлы сохраняются в представление **Документы**. Не зависимо от наличия сохранения в **Документы**, результат операции подписания отображается в разделе **Мастер подписи и шифрования**.

*Примечание:* По кнопке **Сохранить параметры операций** можно сохранить текущие настройки, для последующего шифрования документов (Рис. 2.7.9).

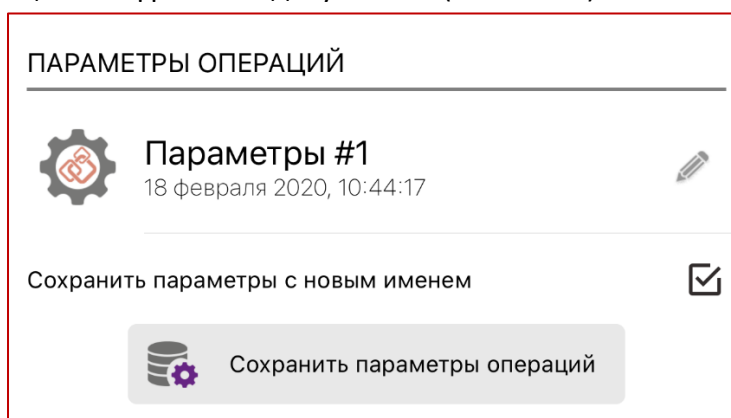


Рис. 2.7.9 Сохранение текущих настроек

Если установлен переключатель напротив **Сохранить параметры с новым именем**, то будет создана новая настройка, где сохранены изменения из разделов **Операции**, **Сертификат**



**подписи, Сертификат шифрования, Параметры подписи, Параметры шифрования** (Рис. 2.7.10).

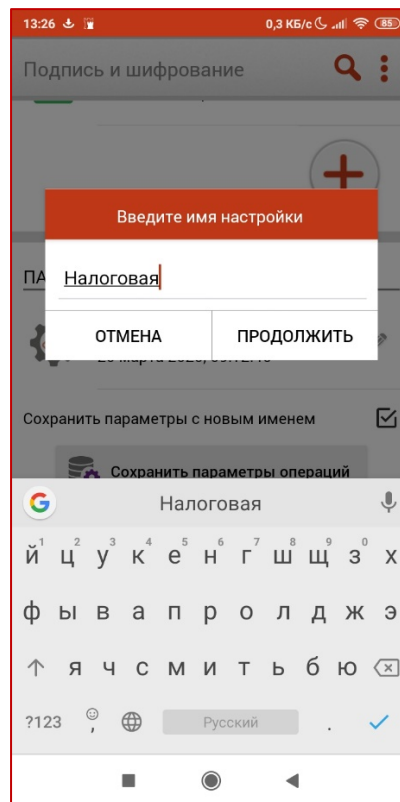


Рис. 2.7.10 Ввод нового имени настройки

#### 4.4 Расшифрование файлов

Для расшифрования достаточно выбрать файл с расширением .enc, и нажать на кнопку **Расшифровать файл** (Рис. 2.8.1). Размер зашифрованного файла зависит от модели телефона, не рекомендуется расшифровывать файлы больше 20 Мб.

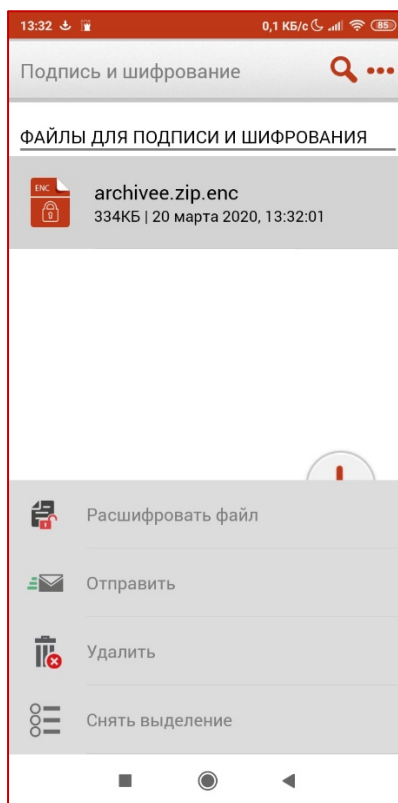


Рис. 2.8.1 Выбор файла для расшифрования

Если в хранилище сертификатов не окажется сертификата с ключом ЭП, который был выбран в качестве сертификата получателя при шифровании, расшифрование не будет выполнено. Если сертификат с ключом ЭП в хранилище присутствует, то далее необходимо ввести пароль от контейнера (Рис. 2.8.2).

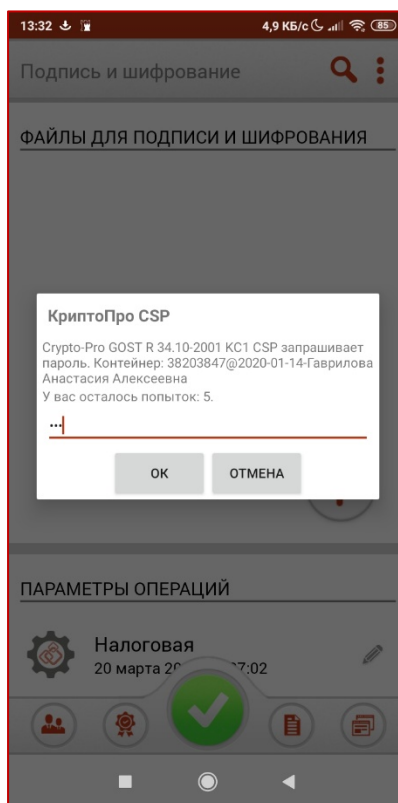


Рис. 2.8.2 Ввод пароля

При расшифровании у файлов меняется иконка, наименование, дата создания (Рис. 2.8.3).

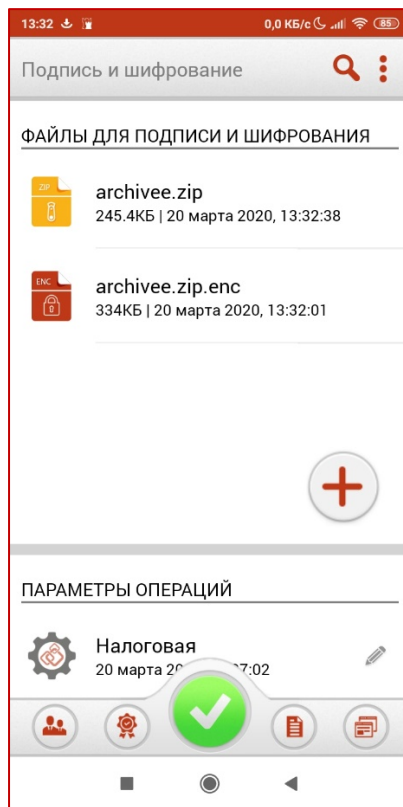



Рис. 2.8.3 Файл расшифрован

#### 4.5 Управление списком файлов для выполнения операций

Файлы в **Мастер подписи и шифрования** можно добавить двумя способами: через кнопку **Добавить** файлы  или открыть файл из стороннего приложения (например, открыть файл через диск, почту, галерею) (Рис. 2.9.1).

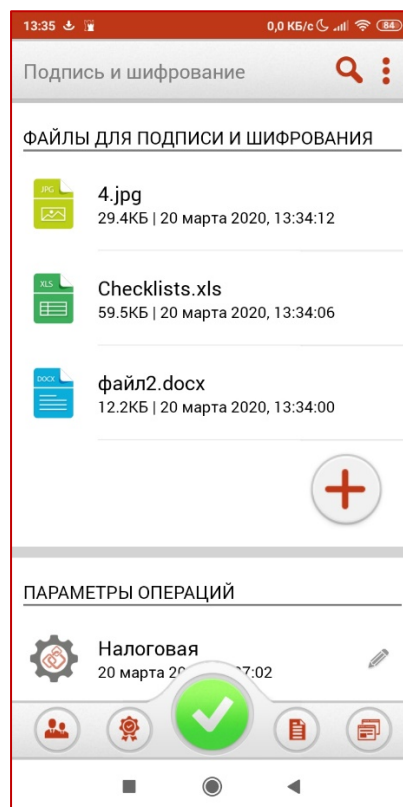



Рис. 2.9.1 Отображение добавленных файлов

Для списка документов доступно контекстное меню, открывающееся при нажатии на кнопку . В меню предоставлены операции, описанные в таблице 2.

Таблица 2. Список операций в контекстном меню

5. Операция	6. Действие
7.  Выделить все	Происходит выделение всех элементов списка документов.
Снять выделение	При выборе операции выделение с файлов в списке сбрасывается. Меню операций закрывается. После сброса выделения в меню остается только операция Выделить все.
Просмотреть документ	Выполняется передача документа на просмотр стороннему приложению через диалог выбора. Операция отображается только в том случае, если в списке выделен один документ.
Отправить	Данная операция осуществляет передачу выбранного документа любому приложению из отображаемого списка для последующей обработки.
Удалить	Операция позволяет удалить выбранный документ из текущего списка.

 Свойства подписи	Выполняется открытие представления с отображением информации о подписи. Эта операция в меню доступна только при выделении одного подписанного документа.
Снять подпись	Процесс снятия подписи с документов более подробно описан в пункте 2.5 Снятие электронной подписи
Расшифровать документ	Процесс расшифрования документов более подробно описан в пункте 2.8 Расшифрование файлов

Пример вызова контекстного меню для одного подписанного файла (Рис. 2.9.2):

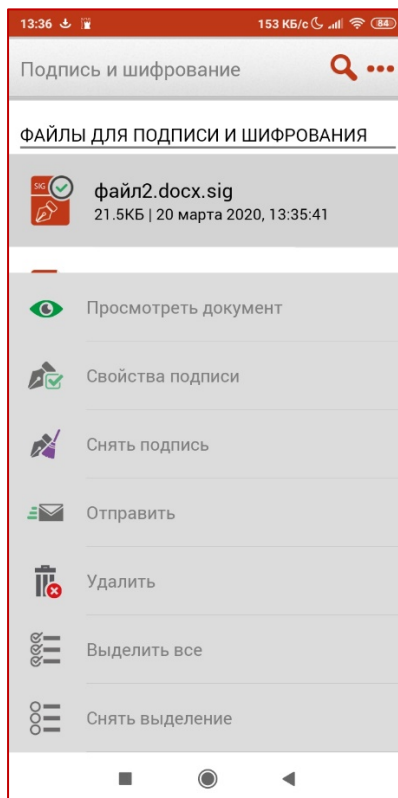


Рис. 2.9.2 Операции для одного подписанного файла

Пример вызова контекстного меню для одного зашифрованного файла (Рис. 2.9.3):

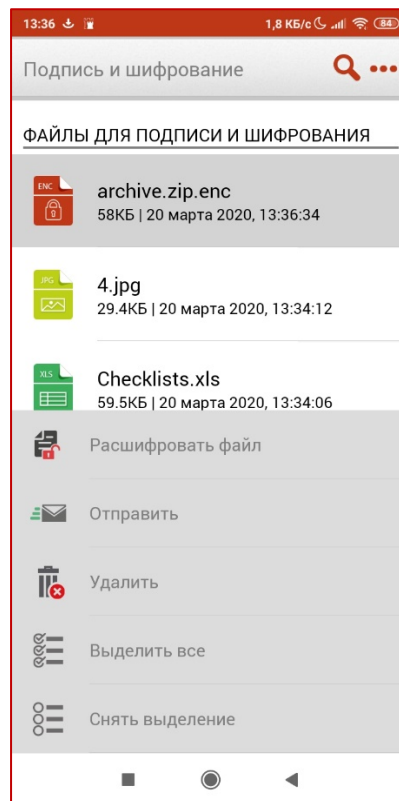


Рис. 2.9.3 Операции для одного зашифрованного файла

Для каждого файла списка доступны кнопки операции, появляющиеся при свайпе влево (Рис. 2.9.4):

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

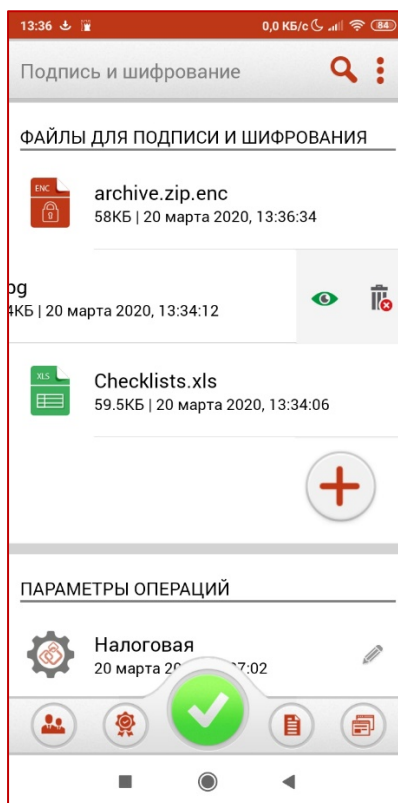



Рис. 2.9.4 Операции над одним конкретным элементом

## 7.1 Документы

По нажатию на кнопку  открывается представление **Документы** (Рис. 2.10.1).

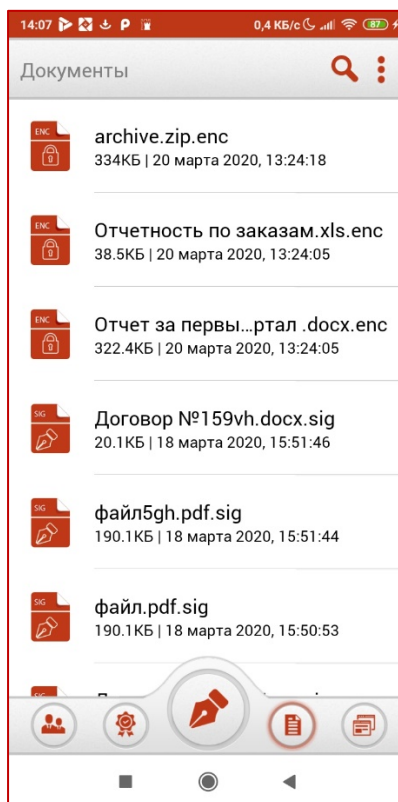


Рис. 2.10.1 Отображение представления Документы

**Документы** – это список файлов из предустановленного каталога приложения, куда сохраняются результаты операций - подписанные и зашифрованные документы, при включении режима **Сохранение архивной копии в Документы** в параметрах операций **Мастера подписи и шифрования** (Рис. 2.10.2).

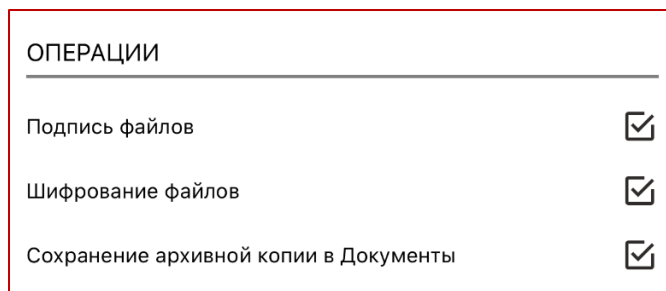








Рис. 2.10.2 Выбор режима "Сохранение архивной копии"

В каталоге **Документы** нельзя выполнять какие-либо операции по подписи и шифрованию, добавлении в него файлов, минуя **Мастер подписи и шифрования**. Среди автоматически выполняемых операций – это проверка подписи под документами.


Все файлы представления **Документы** можно передать в **Мастер подписи и шифрования** для выполнения операций.

Операции в представлении **Документы** при выделении подписанного документа (Рис. 2.10.3) представлены в таблице 3.

Таблица 3 Операции над документами

8. Операция	9. Описание
10.  Выделить все	Происходит выделение всех элементов списка документов.
 Снять выделение	При выборе операции выделение с документов сбрасывается.
 Просмотреть документ	Просмотр документа. Доступно при выделении одного документа.
 Свойства подписи	Проверка подписи выделенного документа означает открытие представления с информацией о подписи.
 Открыть в мастере подписи и шифрования	Выбранный документ передается в мастер подписи и шифрования для выполнения операций.
 Отправить	Данная операция осуществляет передачу выбранного



	документа любому приложению из отображаемого списка для последующей обработки.
 Удалить	Операция позволяет удалить выбранный документ из текущего списка.

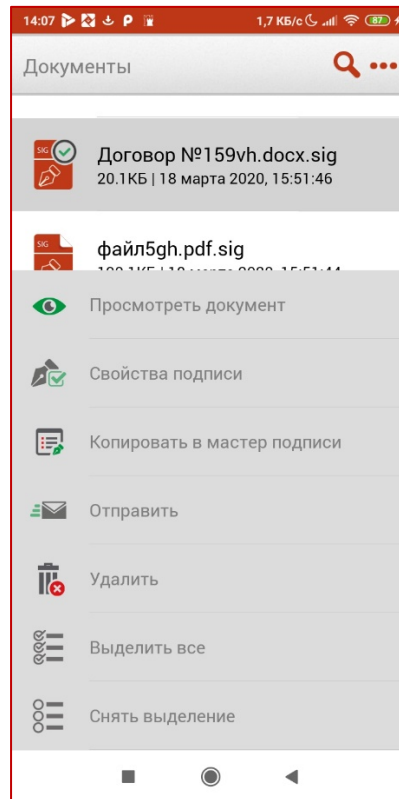



Рис. 2.10.3 Контекстное меню в Документах

## 10.1 Управление сертификатами

Для управления сертификатами в приложении добавлен отдельный пункт меню  **Сертификаты**. При выборе данного пункта меню открывается список личных сертификатов. 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 действительный, сертификат не действительный (Рис. 2.11.1).

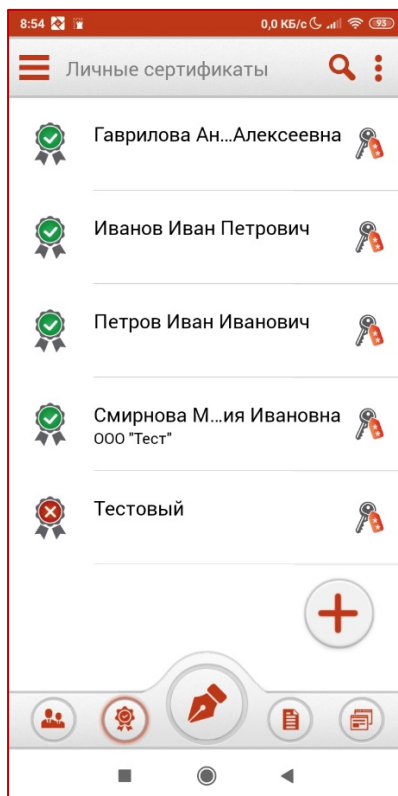


Рис. 2.11.1 Список личных сертификатов

По нажатию на кнопку выбора раздела  открывается меню разделов (Рис. 2.11.2).

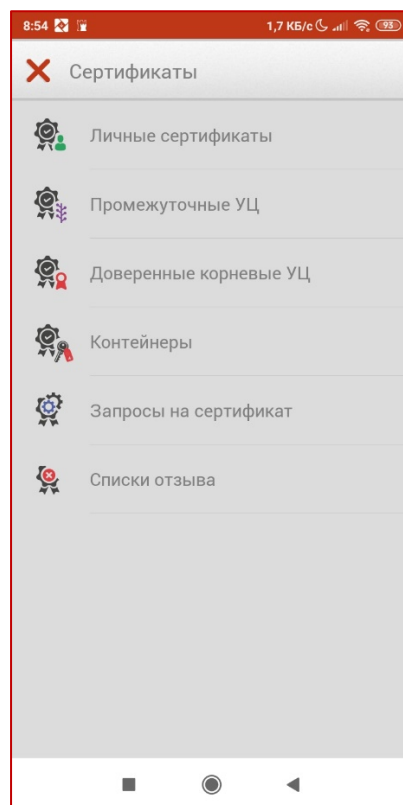



Рис. 2.11.2. Меню сертификатов

При этом кнопка меню заменяется на кнопку , по нажатию на которую происходит возврат назад к списку личных сертификатов. Меню содержит пункты:

- **Личные сертификаты** – для управления личными сертификатами, у которых есть привязка к ключу ЭП.
- **Промежуточные УЦ** – раздел с промежуточными сертификатами, необходимыми для корректного построения цепочек сертификации.
- **Корневые доверенные УЦ** – раздел с доверенными корневыми сертификатами, т.е. сертификатами корневых удостоверяющих центров. В данном разделе также отображаются сертификаты сервисов УЦ (например, КриптоПро УЦ 2.0) со статусами созданных подключений. При получении сертификатов сервисов УЦ они автоматически устанавливаются в данный раздел.
- **Контейнеры** – раздел с ключевыми контейнерами. В данном разделе отображаются ключевые контейнеры локального хранилища КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base, подключенных устройств с возможностью установки сертификатов из контейнера.
- **Запросы на сертификат** – содержит созданные в приложении запросы на сертификат.
- **Списки отзыва** – раздел со списками отзыва на сертификаты. Необходимы для выполнения локальной проверки сертификатов на действительность.

## 10.2 Операции над сертификатами

### Просмотр сертификата.

Для просмотра сертификата при свайпе или в контекстном меню необходимо выбрать операцию **Просмотр сертификата** (Рис. 2.12.1).

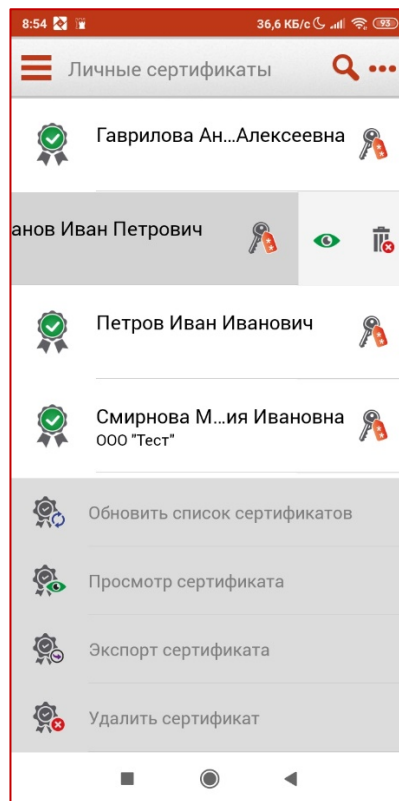


Рис. 2.12.1. Операции над списком сертификатов

Открывается форма просмотра сертификата, содержащая пункты:

- **Сертификат** - содержит сведения о владельце сертификата, издателе и самом сертификате;
- **Цепочка доверия** - отображает общий статус построения цепочки доверия и приводится «дерево» сертификации.

#### Экспорт сертификата.

Для экспорта сертификата в контекстном меню необходимо выбрать операцию **Экспорт сертификата** (Рис. 2.12.1).

Открывается форма выбора настроек формата файла экспортируемого сертификата. Экспортировать сертификат можно только без ключа ЭП(Рис. 2.12.2). В таком случае нужно только выбрать кодировку файла сертификата.

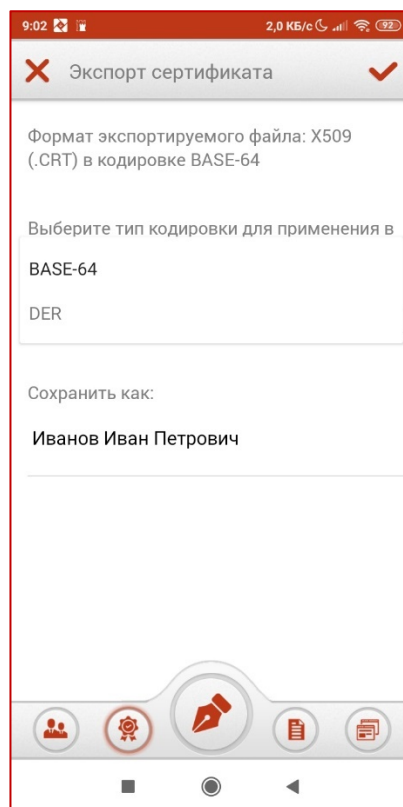


Рис. 2.12.2 Экспорт сертификата без ключа ЭП

После нажатия кнопки **Экспортировать** открывается меню выбора приложения, куда будет сохранен файл сертификата. По окончании операции возникнет сообщение об успешном экспорте сертификата.

#### **Удаление сертификата.**

Для удаления сертификата при свайпе или в контекстном меню необходимо выбрать операцию **Удалить сертификат** (Рис. 2.12.1).

В появившемся диалоговом окне нажать (Рис. 2.12.3):

- **Отмена** - для удаления сертификата без ключевого контейнера;
- **Да** - для удаления сертификата вместе с ключевым контейнером. *Примечание: Не рекомендуется удалять контейнер ключа ЭП, так как он не подлежит восстановлению.*

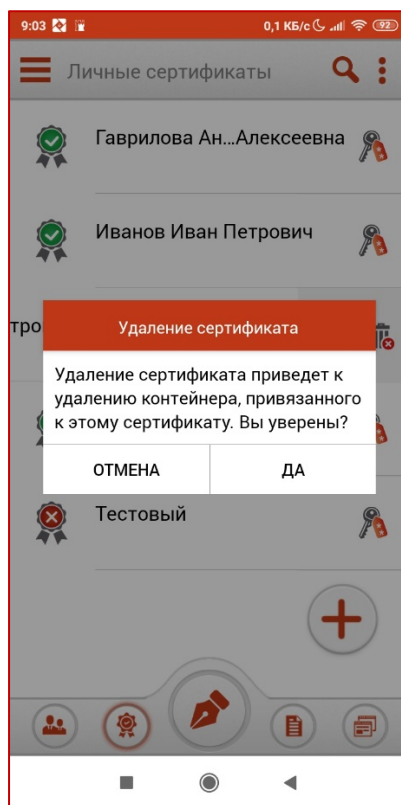


Рис. 2.12.3 Удаление сертификата

### 10.3 Импорт сертификата из файла

Импорт сертификатов может понадобиться для выполнения следующих задач:

- Установка личного сертификата с привязкой к ключевому контейнеру для выполнения операций подписи и расшифрования;
- Установка сертификата, который был отправлен другим пользователем, компьютером или центром сертификации.

#### Импорт личного сертификата с привязкой к ключу ЭП.

Импорт нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»). В открывшемся окне нужно выбрать операцию **Импортировать сертификат из файла** (Рис. 2.13.1).

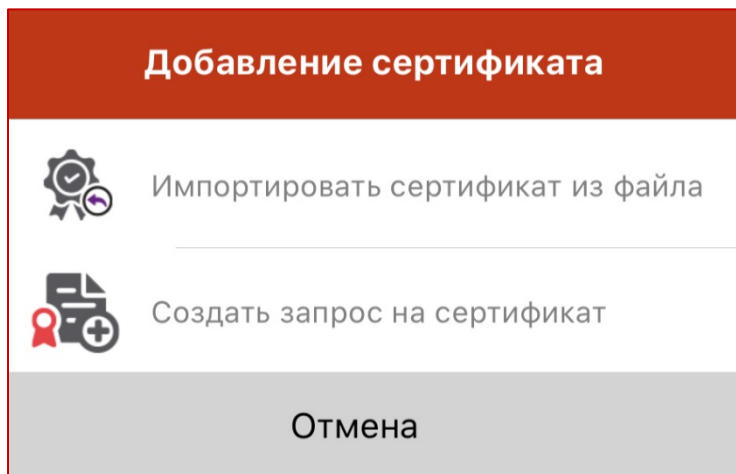


Рис. 2.13.1 Добавление сертификата

Если в приложении ранее был создан ключевой контейнер, и обработан запрос на сертификат в Удостоверяющем центре (УЦ), то в качестве файла сертификата нужно выбрать сертификат, полученный из УЦ. Сертификат отображается в категории **Личные сертификаты**. Данным сертификатом можно подписывать и расшифровывать документы.

Если у пользователя есть сертификат с ключом ЭП в формате PKCS #12 (.pfx), то в качестве файла сертификата нужно выбрать данный сертификат. На запрос ввода пароля ввести пароль к ключевому контейнеру (Рис. 2.13.2).

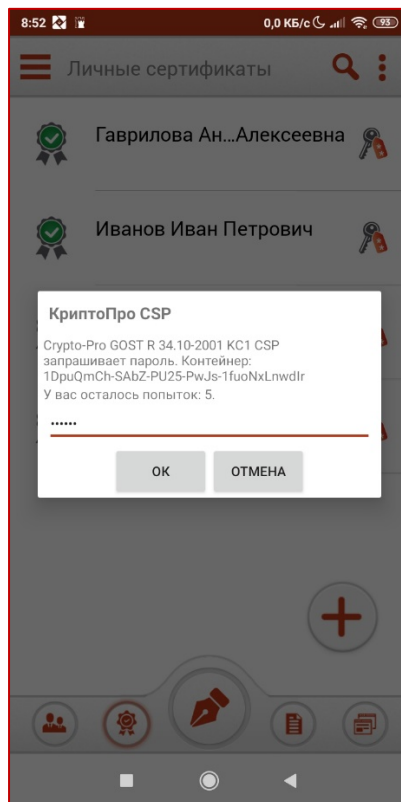


Рис. 2.13.2 Ввод пароля

Далее задать новый пароль. Сертификат устанавливается в хранилище **Личных сертификатов** (Рис. 2.13.3). У данного сертификата есть контейнер с ключом ЭП. Данным сертификатом можно подписывать и расшифровывать документы.

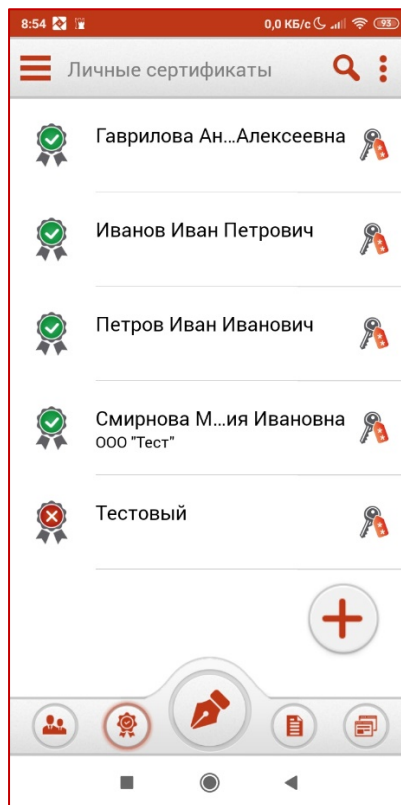


Рис. 2.13.3 Сертификат добавлен в список Личных сертификатов

Если при импорте не будет найден ключ ЭП, соответствующий сертификату, то возникнет сообщение об ошибке (Рис. 2.13.4).

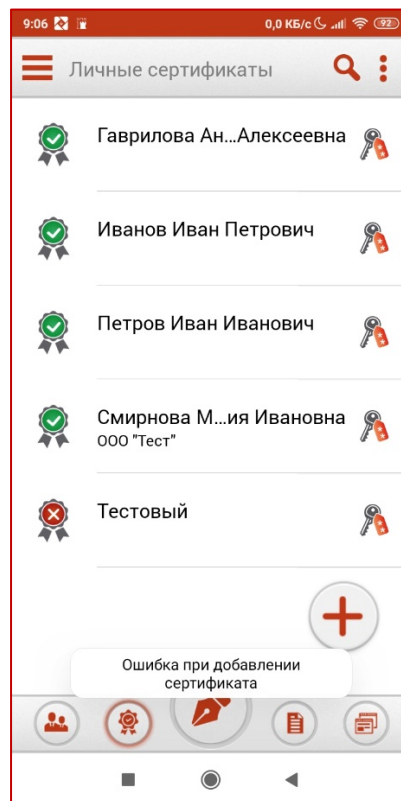


Рис. 2.13.4 Сообщение об ошибке при добавлении сертификата без ключа ЭП



### **Импорт сертификата без привязки к ключу ЭП.**

Импорт нового сертификата в хранилище выполняется кнопкой добавления сертификата («+»). Далее необходимо найти файл в хранилище и выбрать для добавления. При успешном выполнении операции импорта сертификат автоматически помещается в выбранное хранилище (Рис. 2.13.5).

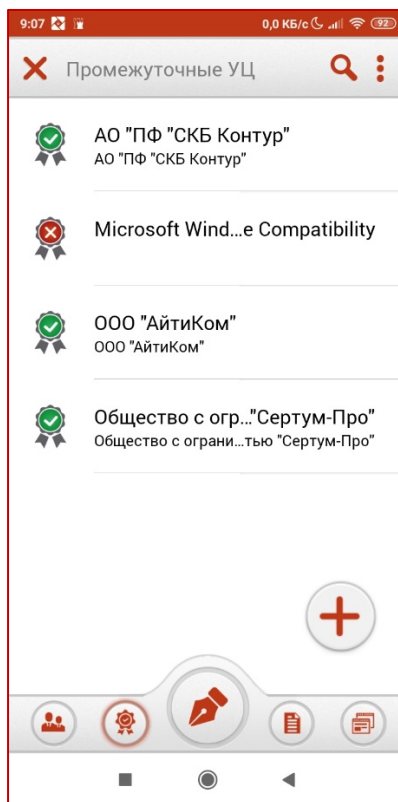


Рис. 2.13.5 Список промежуточных УЦ

Если при импорте приложение определило, что для данного сертификата лучше подойдет другое хранилище, то возникнет сообщение об ошибке, с возможностью принудительной установки в выбранное хранилище (Рис. 2.13.6).

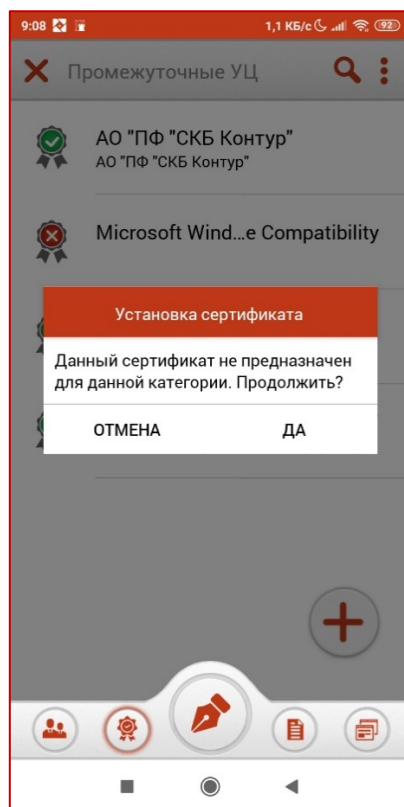


Рис. 2.13.6 Сообщение о принудительной установке сертификата

## 10.4 Создание запроса на сертификат

Создать запрос на сертификат можно, нажав кнопку **Добавить** ("+" ):

- на форме **Личные сертификаты** (Рис. 2.14.1);
- на форме **Запросы**.

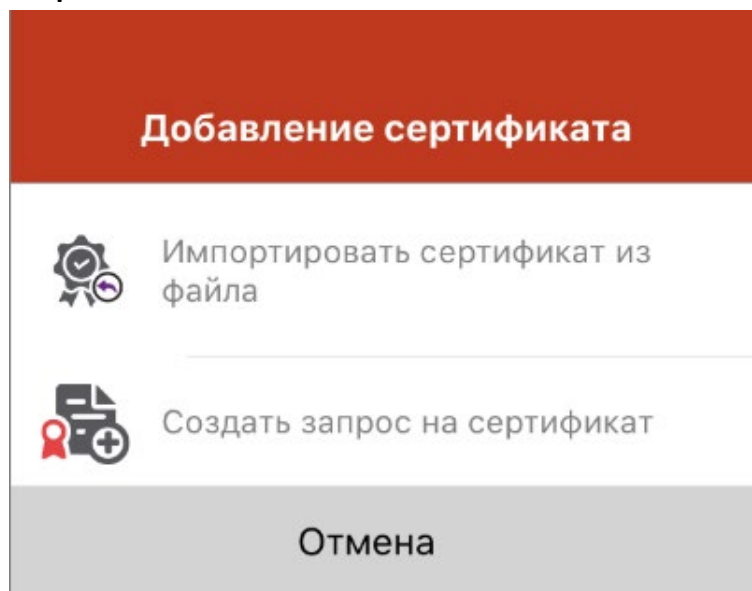


Рис. 2.14.1 Меню для добавления сертификата

Открывается форма создания запроса на сертификат, содержащая поля для сбора необходимых сведений.

В зависимости от назначения сертификата выбирается **Тип владельца сертификата**, **Алгоритм** и **Назначение ключа** (Рис. 2.14.2).

Тип владельца сертификата	Пользователь
Алгоритм	GOST R 34.10-2012 256-bit
Назначение ключа	Подпись и шифрование
Создать как самоподписанный сертификат	<input type="checkbox"/>
Экспортируемый ключ	<input checked="" type="checkbox"/>

Рис. 2.14.2 Параметры сертификата

При включении опции **Создать как самоподписанный сертификат** происходит создание самоподписанного сертификата и его автоматическая установка в личное хранилище пользователя и в хранилище доверенных корневых сертификатов. Запросы на самоподписанные сертификаты не создаются.

При включении опции **Экспортируемый ключ** можно проводить экспорт сертификата вместе с ключом ЭП.

В разделе **Параметры субъекта** указывается идентификационная информация о владельце сертификата согласно выбранному типу владельца сертификата (Рис. 2.14.3).

9:16 3,1 КБ/с 81

Создание запроса

ПАРАМЕТРЫ СУБЪЕКТА

Общее имя\*: Иванов Иван Иванович

Страна/регион\*: RU

Область\*: 12 Республика Марий Эл

Город\*: Йошкар-Ола

Адрес E-Mail: iv3567@mail.ru

Адрес: Ул. Иванова 120

СНИЛС\*: 000000000000

ИНН: 0000000000

Рис. 2.14.3 Параметры субъекта

Назначение сертификата (EКУ) (Рис. 2.14.4).

9:16 0,2 КБ/с 91

✕ Создание запроса ✓

Адрес E-Mail: iv3567@mail.ru

Адрес: Ул. Иванова 120

СНИЛС\*: 00000000000

ИНН: 00000000000

\* - поля обязательные для заполнения.

НАЗНАЧЕНИЕ СЕРТИФИКАТА ^

Проверка подлинности сервера ☐

Проверка подлинности клиента ☒

Подпись кода ☐

Защита электронной почты ☒

Icons: Users, Settings, Pen (selected), Documents, Calendar

Рис. 2.14.4 Назначение сертификата

По кнопке **Галочка** в правом верхнем углу будет открыта форма генерации ключевого контейнера (Рис. 2.14.5).

9:16 64,4 КБ/с 91

КриптоПро CSP

Биологический датчик случайных чисел.  
Нажимайте на экран, пока ключ  
не будет создан.

Отмена

Рис. 2.14.5 Генерация ключевого контейнера

На запрос системы, установите пароль на данный контейнер и подтвердите его (Рис. 2.14.6).

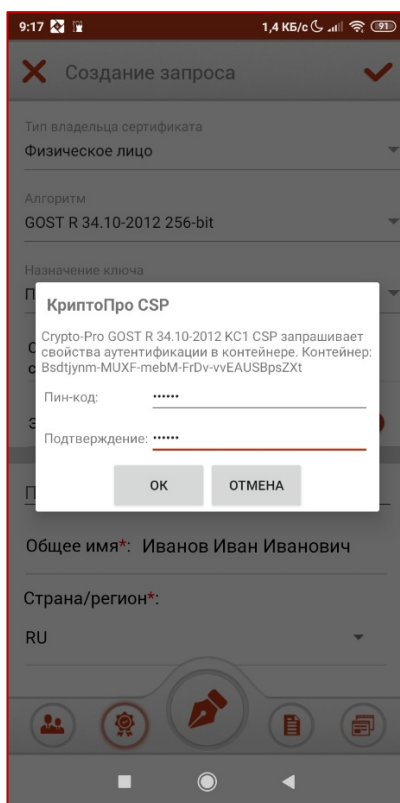


Рис. 2.14.6 Установка пароля на ключевой контейнер

После завершения операции возникнет окно с информацией о ее результатах и, сформированный запрос, отобразится на вкладке **Запросы на сертификат** в разделе **Сертификаты** (Рис. 2.14.7).

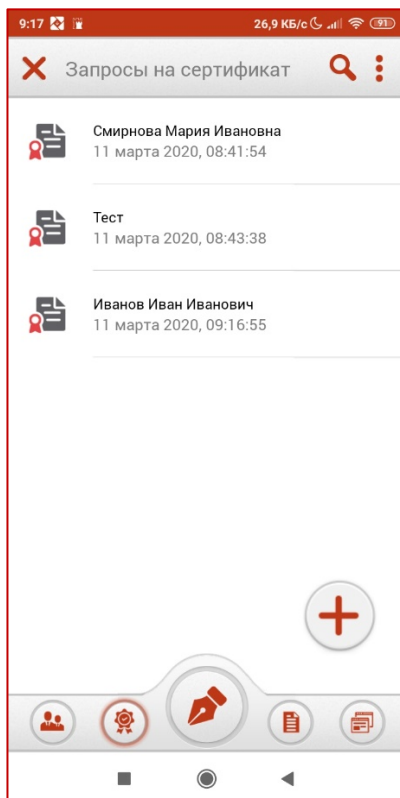


Рис. 2.14.7 Список запросов

Для запроса доступны следующие операции:

- **Просмотр** – для просмотра свойств запроса;
- **Экспортировать** – для сохранения сертификата в файл;
- **Удалить** – для удаления запроса из списка.

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

## 10.5 Списки отзыва сертификатов (СОС)

Для работы со списками отзыва сертификатов в пункт меню сертификаты добавлен подпункт **Списки отзыва сертификатов** (Рис. 2.15.1).

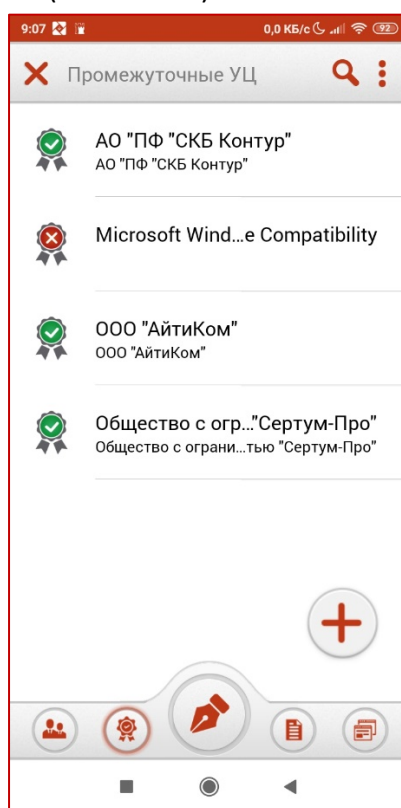



Рис. 2.15.1 Список СОС

По кнопке  можно установить список отзыва из хранилища. При успешном импорте файл отображается в разделе Список отзыва сертификатов.

Для списков отзыва могут быть следующие обозначения:



– список отзыва сертификатов с корректной подписью;



– список отзыва сертификатов с некорректной подписью.

### Обновление списка отзыва

Для обновления списка отзыва в контекстном меню необходимо выбрать операцию **Обновить список отзывов**. При вызове контекстного меню операция появляется всегда (Рис. 2.15.2).

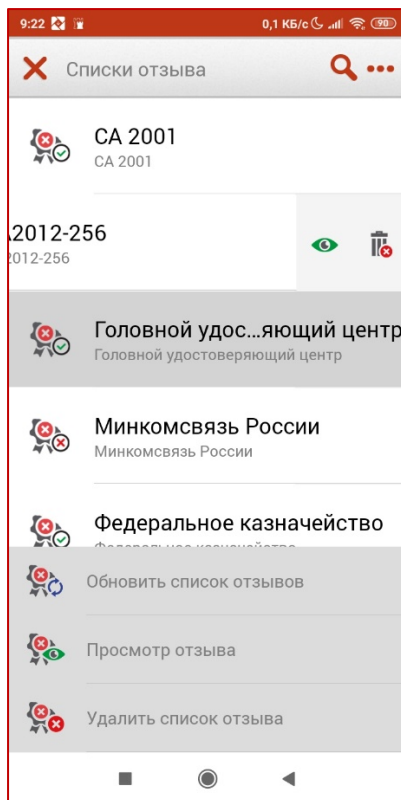


Рис. 2.15.2 Операции для СОС

Данная операция позволяет снова проверить корректность списка отзыва, и, если произошли изменения, то они отражаются в изменении статусов иконок.

#### Просмотр списка отзыва

Для просмотра свойств списка отзыва сертификата при свайпе или в контекстном меню необходимо выбрать операцию **Просмотр** (Рис. 2.15.2). При выделении множества элементов операция просмотра свойств списка отзыва скрывается. Свойства отображаются в отдельном компоненте (Рис. 2.15.3).

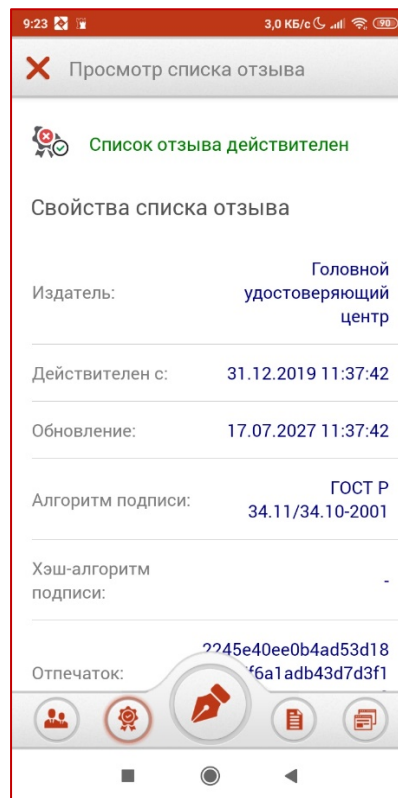


Рис. 2.15.3 Просмотр свойств СОС

### Удаление СОС

Для удаления списка отзыва сертификата при свайпе или в контекстном меню необходимо выбрать операцию **Удалить** (Рис. 2.15.2). Удалять можно один элемент или сразу несколько. При удалении необходимо подтвердить действие в соответствующем окне (Рис. 2.15.4).



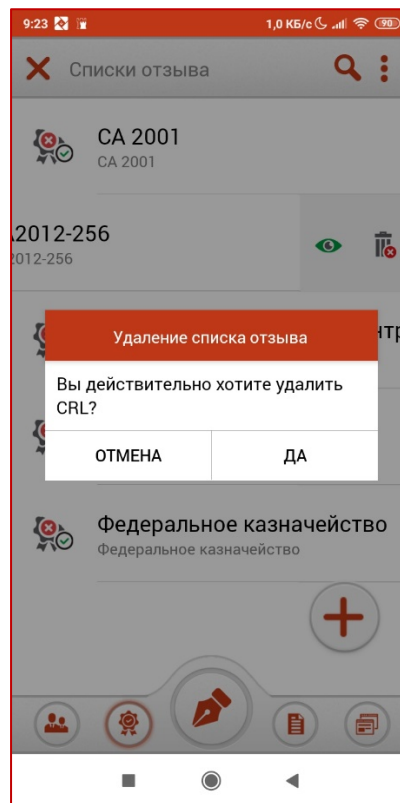



Рис. 2.15.4 Удаление СОС

## 10.6 Управление контейнерами

При открытии представления **Контейнеры** отображается список контейнеров, которые установлены в локальное хранилище КриптоПро CSP версия 5.0 R2 KC1 исполнение 1-Base (Рис. 2.16.1). В представлении кроме кнопки возврата назад (закрытия) и поиска имеется кнопка вызова меню операций .

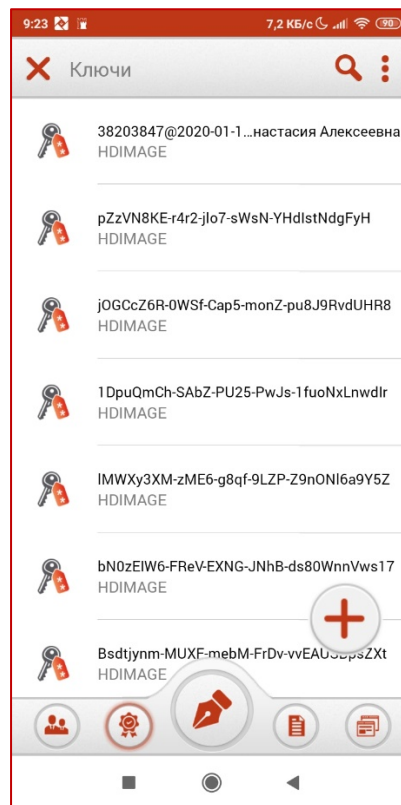


Рис. 2.16.1 Отображение представления Контейнеры

### **Обновление списка ключей**

Для перечитывания контейнеров из локального хранилища необходимо выбрать пункт **Обновить список ключей** в меню операций (Рис. 2.16.2). Обновить список ключей необходимо при:

- подключении рутокена;
- добавлении нового сертификата.

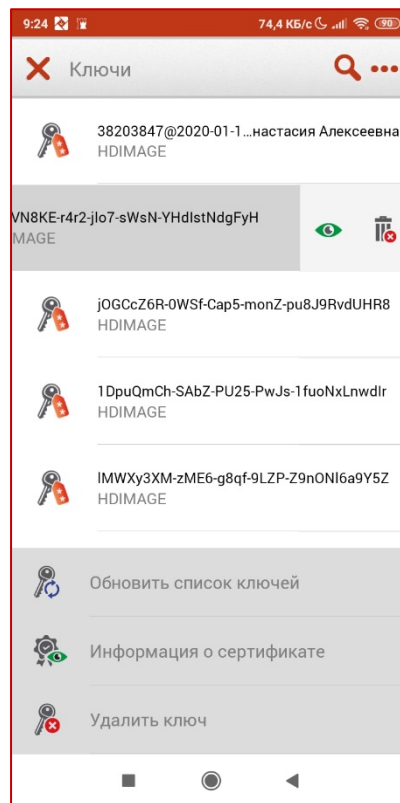


Рис. 2.16.2 Операции над контейнерами

### Просмотр информации о сертификате

Если в контейнере есть сертификат, то можно посмотреть информацию о нем, нажав **Информация о сертификате** в меню операций или при свайпе (Рис. 2.16.2). Данный пункт отображается в меню только в том случае, если в контейнере имеется сертификат пользователя.

По нажатию на кнопку операции открывается форма просмотра информации о сертификате (Рис. 2.16.3)

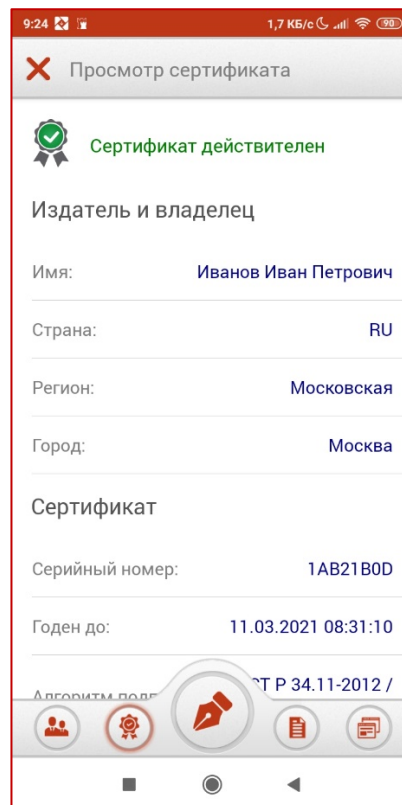


Рис. 2.16.3 Информация о сертификате в контейнере

### Удаление контейнера

При выборе операции **Удалить ключ** в меню операций или при свайпе (Рис. 2.16.2) возникает диалоговое окно для выбора способа удаления контейнера, вместе с сертификатом, связанным с контейнером, или без сертификата (Рис. 2.16.4). Если удалить контейнер без связанного с ним сертификата, то в хранилище сертификатов останется сертификат без ключевого контейнера. Таким сертификатом нельзя выполнять операции подписи и расшифрования.

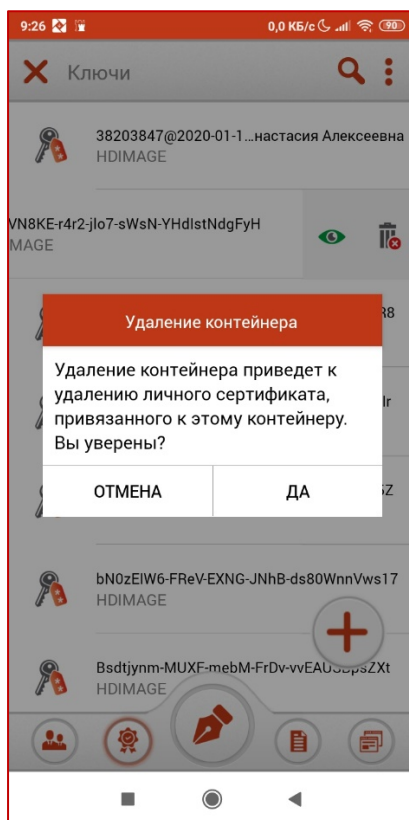


Рис. 2.16.4 Удаление ключевого контейнера

## 10.7 Контакты

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

Переход в список контактов происходит при выборе пункта меню **Контакты** (Рис. 2.17.1).

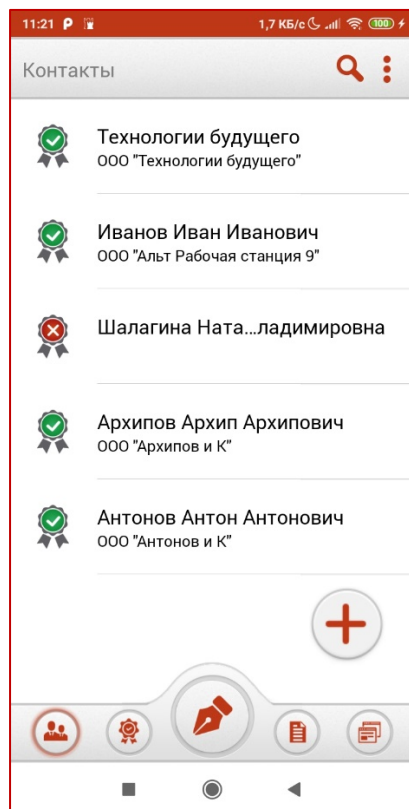



Рис. 2.17.1 Отображение представления Контакты

Контакты можно импортировать, просматривать, экспортировать и удалять. Так же для списка контактов работает поиск.

### Импорт нового контакта

Импорт нового контакта выполняется кнопкой добавления . Из хранилища нужно выбрать файл сертификата с расширением .cer или .crt.

При успешном выполнении операции импорта контакт появляется в списке (Рис. 2.17.1).

### Просмотр свойств контакта

Для просмотра свойств контакта при свайпе или в меню операций необходимо выбрать пункт **Просмотр сертификата** (Рис. 2.17.2).

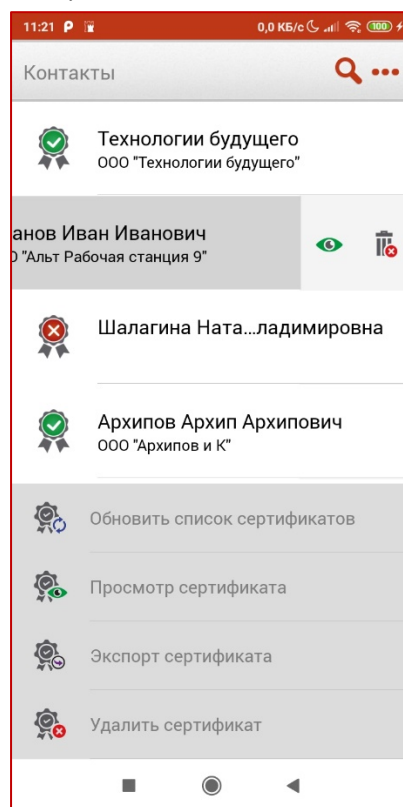


Рис. 2.17.2 Операции над Kontakтами

### Экспорт контакта в файл

Для экспорта контакта в меню операций необходимо выбрать пункт **Экспорт сертификата** (Рис. 2.17.2).

При экспорте появляется представление, в котором нужно выбрать кодировку и задать имя сертификата (по умолчанию задается текущее имя сертификата) (Рис. 2.17.3).

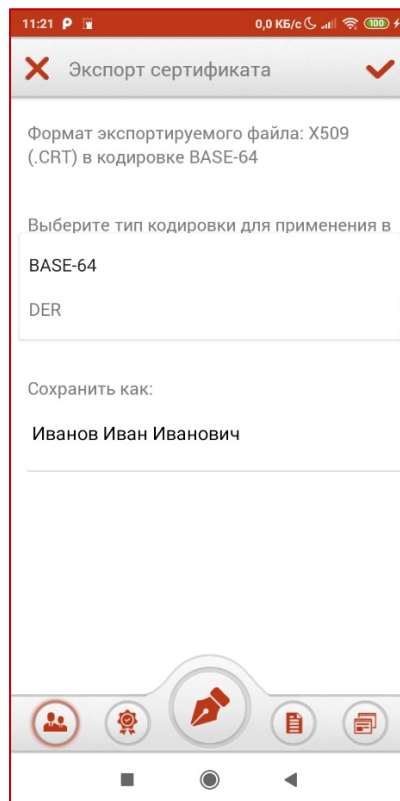


Рис. 2.17.3 Экспорт контакта

### Удаление контакта

Для удаления контакта при свайпе или в меню операций необходимо выбрать пункт **Удалить сертификат** (Рис. 2.17.2). В появившемся диалоговом окне подтвердить операцию удаления (Рис. 2.17.4).

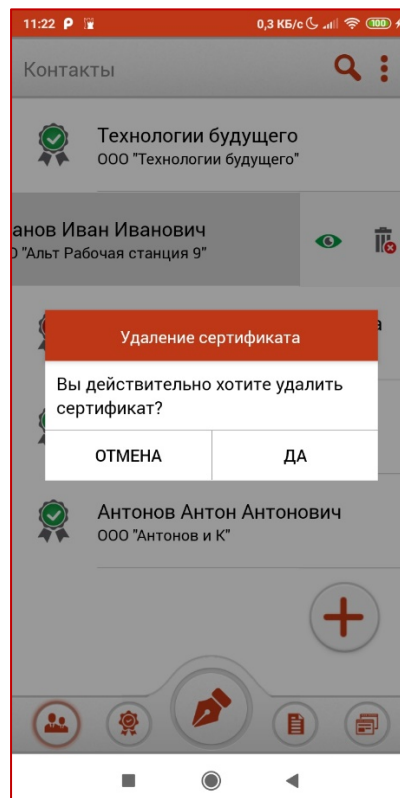


Рис. 2.17.4 Удаление контакта

## 10.8 Лицензии

Раздел Лицензии предназначен для установки лицензий на приложение (Рис. 2.18.1).

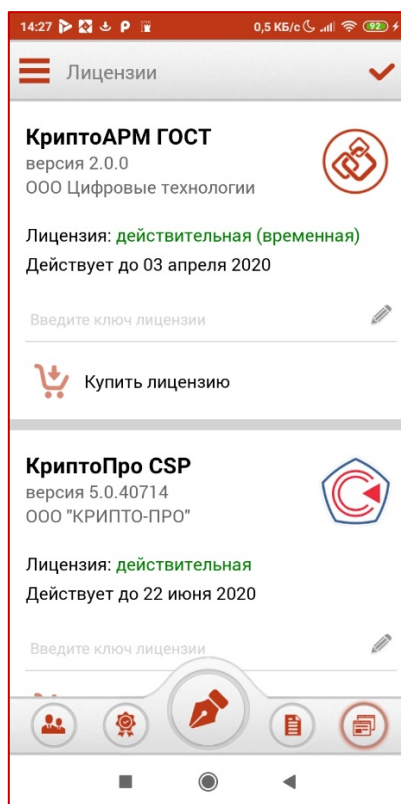



Рис. 2.18.1 Отображение представления Лицензии

При установке приложения доступны временные тестовые лицензии: на КриптоАРМ ГОСТ на 14 дней, на КриптоПро CSP на 93 дня.

Без лицензии на приложение КриптоАРМ ГОСТ доступны операции проверки подписи и шифрования. Для выполнения операций подписи, расшифрования и генерации сертификата должна быть установлена лицензия на приложение.

Без лицензии на КриптоПро CSP доступны операции проверки подписи, шифрования, генерации сертификата. Для выполнения операций подписи и расшифрования должна быть установлена лицензия на КриптоПро CSP.

При нажатии на  в разделе **Лицензии** открывается меню со следующими пунктами (Рис. 2.18.2):

- **Лицензии** – возврат в компонент Лицензии;
- **Журнал операций** – для отображения выполняемых операций в приложении;
- **Справочная помощь** – для открытия полного руководства пользователя приложения.
- **Контроль целостности** – для проверки целостности приложения.
- **Подключение к КриптоПро УЦ 2.0** – для создания и отправки запросов на сертификат и получения сертификата через КриптоПро УЦ 2.0.



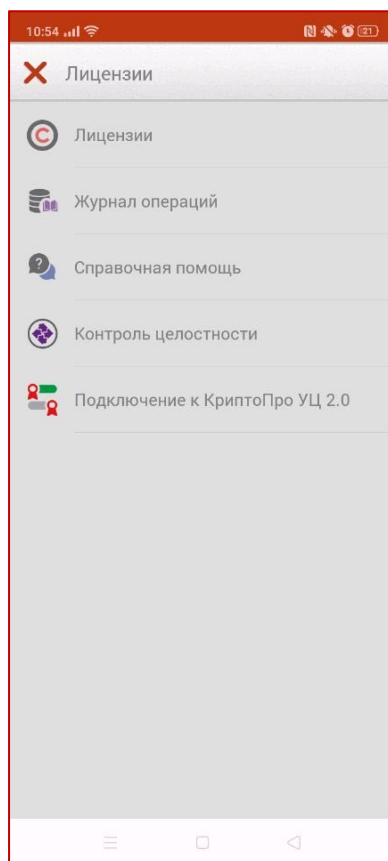


Рис. 2.18.2 Меню операций в лицензиях

## 10.9 Журнал операций

Журнал операций предназначен для отображения операций, выполняемых пользователем (Рис. 2.19.1).

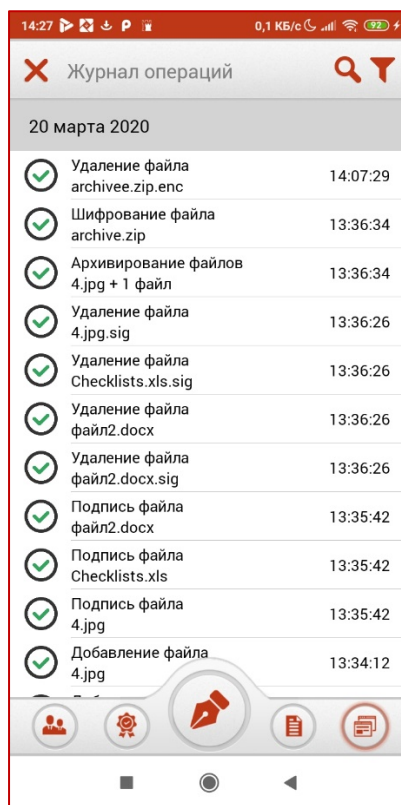


Рис. 2.19.1 Журнал операций

В журнале отображаются следующие типы операций:

- добавление подписи;
- снятие подписи;
- шифрование;
- расшифрование;
- архивирование;
- разархивирование;
- добавление файла;
- удаление файла;
- экспорт файла;
- добавление сертификата;
- добавление pkcs12;
- удаление сертификата
- генерация сертификата
- генерация запроса;
- экспорт запроса;
- удаление запроса;
- установка сертификата;
- удаление контейнера;
- установка crl;
- удаление crl.

Для записей в журнале операций предусмотрена фильтрация (Рис. 2.19.2).

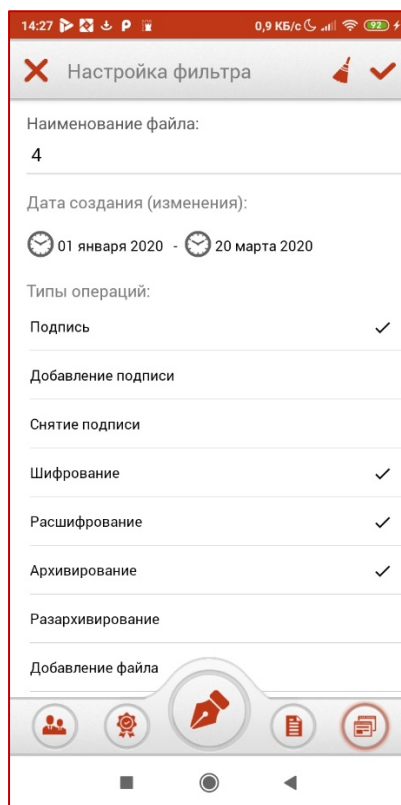



Рис. 2.19.2 Настройки фильтра журнала операций

Применение фильтрации выполняется по нажатию на кнопку . В зависимости от выставленных критериев фильтра в журнале остаются только те записи, которые удовлетворяют (суммарно) этим критериям (Рис. 2.19.3). Для сброса фильтра используется кнопка сброса на форме настроек фильтрации.

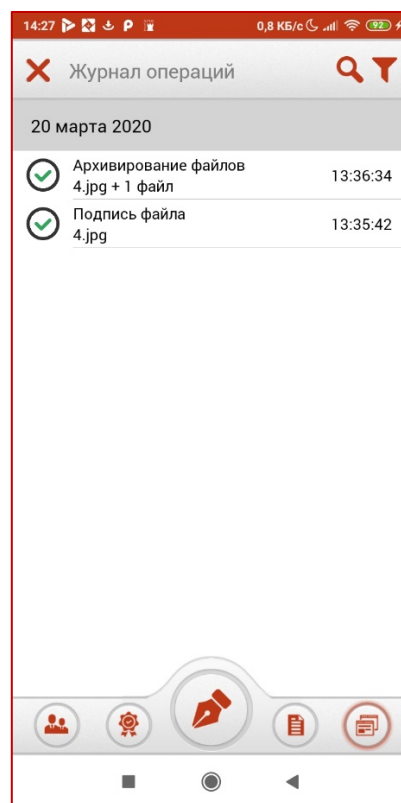


Рис. 2.19.3 Применение фильтра журнала