



424000, РМЭ, г. Йошкар-Ола, ул. Карла Маркса, 1096  
Телефон 8 (8362) 33-70-50  
<https://trusted.ru>  
E-mail: [info@trusted.ru](mailto:info@trusted.ru)



127018, Москва, Суцёвский Вал, 18  
Телефон: (495) 995 4820  
<https://CryptoPro.ru>  
E-mail: [info@CryptoPro.ru](mailto:info@CryptoPro.ru)

Средство	КриптоПро CSP
Криптографической	Версия 5.0 R3 KC1
Защиты	Исполнение 1-КриптоАРМ ГОСТ 3
Информации	Руководство пользователя iOS

ЖТЯИ.00101-13 92 02  
Листов 41

## Содержание

Аннотация .....	6
1. О продукте .....	6
1.1. Функциональность версии.....	6
1.2. Поддерживаемые криптопровайдеры.....	7
1.3. Поддерживаемые ключевые носители.....	7
1.4. Лицензия на программный продукт.....	8
1.5. Установка приложения КриптоАРМ ГОСТ 3 .....	8
1.6. Системные требования .....	8
2. Начало работы с приложением .....	9
3. Документы .....	10
3.1. Создание профиля подписи .....	10
3.1.1. Как создать профиль подписи.....	10
3.1.2. Описание полей профиля.....	10
3.2. Редактирование профиля подписи.....	12
3.2.1. Редактирование профиля подписи из списка профилей подписи.....	12
3.3. Удаление профиля подписи .....	12
3.3.1. Удаление профиля подписи из списка профилей подписи .....	12
3.3.2. Удаление профиля подписи в главном окне раздела Документы.....	12
3.4. Подписание документа.....	12
3.4.1. Как подписать документ, используя профиль подписи .....	12
3.4.2. Как подписать документ, используя мастер Подпись и шифрование .....	13
3.4.3. Как подписать документ с помощью контекстного меню .....	13
3.4.4. Как создать подпись со штампом времени (TSP) .....	13
3.4.5. Как создать усовершенствованную подпись .....	14
3.4.6. Результат выполнения операции.....	15
3.5. Шифрование документа .....	15
3.5.1. Как зашифровать документ, используя профиль подписи .....	15
3.5.2. Как зашифровать документ, используя мастер Подпись и шифрование .....	16

3.5.3.	Как зашифровать документ с помощью контекстного меню.....	16
3.5.4.	Результат выполнения операции.....	17
3.6.	Архивирование документа .....	17
3.6.1.	Как архивировать документ через мастер Подпись и шифрование .....	17
3.6.2.	Как архивировать документ с помощью профиля подписи.....	17
3.6.3.	Результат выполнения операции.....	18
3.7.	Проверка подписи документа .....	18
3.7.1.	Результат операции.....	18
3.8.	Расшифрование документа .....	18
3.9.	Соподпись (добавление подписи к файлу) .....	19
3.9.1.	Как добавить подпись, используя профиль подписи .....	19
3.9.2.	Как добавить подпись, используя мастер Подпись и шифрование .....	20
3.9.3.	Как добавить подпись к файлу, расположенному в блоке Архив .....	20
3.9.4.	Результат выполнения операции.....	20
3.10.	Снятие подписи с файла .....	20
3.11.	Прямые групповые операции .....	21
3.11.1.	Прямые групповые операции в мастере Подпись и шифрование .....	21
3.11.2.	Прямые групповые операции в профиле подписи .....	21
3.12.	Обратные групповые операции.....	22
4.	Контакты .....	24
4.1.	Экспорт контактов .....	24
4.2.	Импорт контактов .....	24
4.3.	Действия с контактами.....	24
4.4.	Мой контакт .....	25
4.5.	Создание контакта .....	25
4.5.1.	Создание контакта без сертификата в разделе Контакты .....	25
4.5.2.	Создание контакта с сертификатом из файла в разделе Контакты .....	26
4.5.3.	Создание контакта с сертификатом из раздела Личные сертификаты в разделе Контакты .....	26
4.5.4.	Создать контакт из сертификата в разделе Контакты.....	26

4.5.5.	Описание полей формы создания контакта .....	26
4.6.	Просмотреть сведения о созданном/импортированном контакте.....	27
4.7.	Редактирование контакта .....	27
4.7.1.	Редактирование контакта через контекстное меню.....	27
4.7.2.	Редактирование контакта через окно просмотра информации о контакте .....	27
4.8.	Создание группы контактов.....	28
4.8.1.	Создать пользовательскую группу (через виджет Создать).....	28
4.8.2.	Создать пользовательскую группу (через меню групп раздела Контакты) .....	28
4.9.	Просмотреть содержимое группы .....	28
5.	Сертификаты.....	29
5.1.	Установка личного сертификата .....	30
5.1.1.	Установка сертификата из ключевого контейнера .....	30
5.1.2.	Установка сертификата с NFC-носителя .....	30
5.1.3.	Установка сертификата с закрытым ключом из файла .pfx .....	31
5.1.4.	Установка сертификата с привязкой к ключевому контейнеру .....	31
5.1.5.	Установка сертификата с помощью QR-кода.....	31
5.2.	Установка корневого и промежуточного сертификатов .....	32
5.3.	Создание запроса на сертификат .....	32
5.4.	Создание самоподписанного сертификата .....	33
5.5.	Установка списка отзыва сертификатов .....	34
5.6.	Экспорт личного сертификата .....	34
5.6.1.	Экспорт сертификата без закрытого ключа .....	34
5.6.2.	Экспорт сертификата с закрытым ключом в контейнер PFX .....	35
5.7.	Экспорт сертификата .....	35
5.8.	Удаление сертификата .....	35
5.9.	Ключевые контейнеры.....	36
5.9.1.	Как посмотреть сертификат в контейнере .....	36
5.9.2.	Как установить сертификат из ключевого контейнера .....	36
5.9.3.	Удаление сертификата .....	36
5.9.4.	Обновление списка контейнеров .....	36

6.	Оповещения .....	37
6.1.	Журнал операций .....	37
6.2.	Настройки оповещений .....	37
6.2.1.	Сортировка и фильтрация .....	37
7.	Ключевые носители .....	39
7.1.	Подключение защищённых носителей .....	39
7.2.	Установка ключей со смарт-карты Рутокен ЭЦП 3.0 NFC/ USB-токена Рутокен ЭЦП 3.0 NFC бесконтактным способом.....	39
7.3.	Установка ключей с USB-токена Рутокен ЭЦП 3.0 контактным способом.....	39
8.	О приложении .....	40
8.1.	Установка лицензии КриптоАРМ ГОСТ 3 .....	40
8.2.	Установка лицензии КриптоПро CSP .....	40
8.3.	Установка лицензии на КриптоПро TSP Client.....	40
8.4.	Установка лицензии на КриптоПро OCSP Client.....	40
8.5.	Дополнительно .....	41

## Аннотация

Настоящее руководство содержит инструкцию по использованию СКЗИ КriptoПро CSP версия 5.0 R3 KC1 исполнение 1-КriptoАРМ ГОСТ 3 (далее по тексту — КriptoАРМ ГОСТ 3).

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

Настройка и использование СКЗИ КriptoПро CSP версия 5.0 R3 KC1 (исполнение 1-Base), входящего в комплект поставки, должна осуществляться в соответствии с требованиями и рекомендациями эксплуатационной документации на СКЗИ (ЖТЯИ.00101-03).

### 1. О продукте

КriptoАРМ ГОСТ 3— это приложение с графическим пользовательским интерфейсом для выполнения операций по созданию и проверке электронной подписи файлов, шифрования и расшифрования, управления сертификатами, размещенных в хранилищах криптопровайдера.

Приложение КriptoАРМ ГОСТ 3 представлено под платформу iOS. Реализована поддержка российских криптографических стандартов посредством использования криптопровайдера КriptoПро CSP.

В приложении поддерживается работа с ключевыми носителями через криптопровайдер КriptoПро CSP.

#### 1.1. Функциональность версии

Приложение текущей версии рассчитано на выполнение операций:

Операция	
<b>Электронная подпись</b>	электронная подпись произвольных файлов размером до 80 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память
	проверка электронной подписи файлов размером до 80 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память
	создание присоединенной и отсоединенной электронной подписи
	создание подписи со штампом времени на подпись и подписываемые данные
	создание усовершенствованной подписи
	добавление электронной подписи (функция соподписи)
<b>Шифрование/ расшифрование</b>	шифрование и расшифрование файлов размером до 80 Мб на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память
	шифрование по стандарту PKCS#7/CMS

<b>Управление сертификатами и ключами</b>	отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых криптопровайдеров
	проверка корректности выбранного сертификата с построением цепочки доверия
	хранение закрытых ключей на носителях Рутокен (АО «Актив-Софт») при условии использования криптопровайдера КриптоПро CSP
	создание запросов на сертификат
	импорт сертификатов с привязкой к закрытому ключу
	экспорт сертификатов
	удаление сертификатов
	импорт сертификатов через QR-код
<b>Контакты</b>	создание контактов с сертификатами из хранилища Личные сертификаты и из файла
	создание контактов на основе данных сертификатов
	создание групп с контактами
	экспорт/импорт контактов в формате vCard
	создание Мой контакт, с прикрепленными личными сертификатами
<b>Работа с журналом событий и уведомлениями</b>	отображение списка событий по уровням детализации
	просмотр уведомлений о событиях
<b>Работа с файлами в каталоге Архив</b>	сохранение всех результатов операций с файлами в каталоге Архив
<b>Управление списком доверенных сервисов</b>	управление списком доменных имен сайтов, с которых разрешена обработка запросов приложением

## 1.2. Поддерживаемые криптопровайдеры

В приложении осуществляется поддержка криптопровайдера КриптоПро CSP версии 5.0 R3 KC1 (исполнение 1-Base).

## 1.3. Поддерживаемые ключевые носители

В приложении поддерживается работа с ключевыми носителями Рутокен (АО «Актив-Софт») через криптопровайдер КриптоПро CSP.

## **1.4. Лицензия на программный продукт**

При первой установке приложения активируется лицензия на КriptoПро CSP сроком на 90 дней. Для работы с приложением КriptoАРМ ГОСТ 3 необходима лицензия (временная, годовая или бессрочная).

Временная лицензия для знакомства с продуктом выдаётся пользователю на 30 дней однократно, по запросу на сайте: <https://cryptoarm.ru/cryptoarm-gost3/>.

После истечения ознакомительного периода для полнофункциональной работы приложения требуется приобретение и установка годовой или бессрочной лицензии. Без установки лицензии операции подписи, расшифрования выполняться не будут.

Для приобретения лицензий на программный продукт КriptoАРМ ГОСТ 3 и КriptoПро CSP можно обратиться в уполномоченную организацию.

## **1.5. Установка приложения КriptoАРМ ГОСТ 3**

Установка и обновление приложения КriptoАРМ ГОСТ 3 происходит через магазин приложений App Store.

## **1.6. Системные требования**

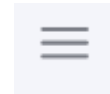
Для приложения сформулированы минимальные системные требования к конфигурации оборудования под платформу iOS:

- Операционная система: iOS 15, iOS 16;
- Оперативная память: 2ГБ и выше;
- Встроенная память: 32ГБ и выше;
- Диагональ экрана: 4.7" и выше;
- Поддержка 3G, 4G, LTE: рекомендуем;
- Фото-камера: рекомендуем, 8МП и выше.



## 2. Начало работы с приложением

Работа с приложением КриптоАРМ ГОСТ 3 начинается с вкладки **Документы**.



Через основное меню приложения осуществляется переход в разделы:

- **О приложении** — содержит сведения о лицензиях и их правообладателях, руководство пользователя, по клику на которое открывается сайт с документацией, и настройка keyAgreement (Согласование ключей).
- **Журнал операций** - содержит сведения о всех операциях в приложении.
- **Документы** — осуществляется переход к мастерам операций и работа с архивными копиями документов.
- **Контакты** — используется для ведения списка контактов, в адрес которых имеется возможность шифровать документы.
- **Сертификаты** — используется для управления сертификатами.

## 3. Документы

Работа с приложением КриптоАРМ ГОСТ начинается с раздела **Документы**.

В верхней панели расположены кнопка **Меню**, название раздела, функция поиска и иконка **Оповещений**.

Блок **Действия** состоит из 4 виджетов и предназначен для добавления документов в Архив, создания профиля, настройки и управления параметрами операций (подпись, шифрование, выбор сертификатов и т. д.) и перехода в мастера **Подпись и шифрование, Проверка и расшифрование**.

Ниже размещён блок **Архив**. Здесь представлен список документов, которые пользователь сохраняет при подписании/шифровании/архивировании файлов. Для этого автоматически активирована функция **Создать копии файлов в Архив**. Если отключить тоггл результаты операции не будут доступны после закрытия приложения. Также в блок **Архив** пользователь может добавить файлы с устройства, нажав на виджет **Добавить документ**.

### 3.1. Создание профиля подписи

Для подписания и шифрования файлов необходимо создать профиль подписи.

**Профиль подписи** — шаблон настроек для выполнения операций подписи, архивирования и шифрования для разных ситуаций. Для обмена документами с бухгалтером вы можете установить и использовать один профиль, с партнерами — второй, с клиентами — третий.

#### 3.1.1. Как создать профиль подписи

1. Выбрать в Меню раздел **Документы**.
2. Нажать на виджет **Создать профиль**. Откроется вкладка **Новый профиль**.
3. Ввести название профиля и **нажать** на ползунки необходимых операций (Подпись, Архивирование, Шифрование). Ниже откроются настройки для каждого вида операций.
4. Нажать на кнопку **Сохранить** в правом верхнем углу.

#### 3.1.2. Описание полей профиля

- **Название профиля** — название профиля подписи для удобства поиска.
- **Операции** — подпись, архивирование, шифрование, другими словами, операции, которые нужно выбрать.

В зависимости от выбранных параметров станут доступны дополнительные поля:

- **Операция Подпись**, доступные поля:
  - **Сохранение результатов на устройстве** — позволяет создать копии файлов в блоке **Архив**.

- **Сертификат подписи** — для выбора доступны личные сертификаты с привязкой к закрытому ключу.
- **Стандарт подписи** — **CAdES-BES** для создания классической подписи или **CAdES-X Long Type 1** и **CAdES-T** — для усовершенствованной подписи. При выборе стандарта CAdES-X Long Type 1 и CAdES-T требуется заполнить поле Служба штампов времени (TSP). Для стандарта подписи CAdES-T ползунок на **Штамп времени на подпись** активирован автоматом. При выборе стандарта подписи CAdES-X Long Type 1 ползунок **Штамп времени на подпись** также активирован автоматом, поле **Параметры службы online статусов** (OCSP) заполняется по необходимости.
- **Кодировка подписи** — сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Формат файла подписи** — выбор расширения для подписываемых документов в форматах .sig, .p7s, .sgn, .sign, .bin.
- **Действия при соподписи** - предназначен для сохранения соподписи в исходный файл либо в копию исходного файла.
- **Штамп времени на подпись** — предназначен для создания подписи со штампом времени на подпись. При включении опции требуется заполнить поле Параметры службы штампов времени (TSP), введя адрес.
- **Штамп времени на данные** — предназначен для создания подписи со штампом времени на данные. При включении опции требуется заполнить поле Служба штампов времени (TSP).
- **Параметры службы штампов времени (TSP)** — адрес службы штампов времени, который можно узнать у поставщика услуг. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры.
- **Параметры службы онлайн статусов (OCSP)** — адрес службы OCSP. Поле отображается, если выбран стандарт подписи CAdES-X Long Type 1 и ползунок **Штамп времени на подпись**. Данное поле не обязательно для заполнения, чаще адрес прописан в самом сертификате, которым создается подпись.
- **Операция Архивирование**, доступная настройка:
  - **Сохранение результатов на устройстве** — позволяет создать копии файлов в блоке Архив.
- **Операция Шифрование**, доступные поля:
  - **Сохранение результатов на устройстве** — позволяет создать копии файлов во вкладке Архив.
  - **Сертификат шифрования** — для выбора доступны контакты, у которых есть привязка к сертификату, и Мой контакт, к которому привязаны личные сертификаты.
  - **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: ГОСТ 28147-89, ГОСТ Р 34.12-2015 Магма, ГОСТ Р 34.12-2015 Кузнечик.

- **Кодировка файлов** — сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.

## 3.2. Редактирование профиля подписи

### 3.2.1. Редактирование профиля подписи из списка профилей подписи

1. В блоке **Профили** нажать на **Все**.
2. Нажать на **Редактировать** у нужного профиля.
3. Изменить нужные параметры.
4. Нажать на **Настройки профиля** (вернуться на предыдущую вкладку).

## 3.3. Удаление профиля подписи

### 3.3.1. Удаление профиля подписи из списка профилей подписи

1. В блоке **Профили** нажать на **Все**.
2. Нажать на кнопку **Удалить** у нужного профиля.



### 3.3.2. Удаление профиля подписи в главном окне раздела Документы

1. В блоке **Профили** нажать на кнопку **Удалить** у нужного профиля.



## 3.4. Подписание документа

Чтобы подписывать документы электронной подписью, нужно установить в Личное хранилище сертификат с привязанным к нему закрытым ключом.

Подписать документы вы можете в мастере **Подписи и шифрования** в разделе **Документы**.

Вы можете подписать документы, выбрав файлы из вкладки **Архив** или выбрав профиль подписи в блоке **Профили подписи**.

### 3.4.1. Как подписать документ, используя профиль подписи


1. Создать профиль подписи, в котором заданы нужные настройки подписи.
2. Открыть раздел **Документы** — нужный профиль подписи. При выборе профиля в мастере автоматически заполняются **Настройки операций**, сохранение результатов на устройстве.
3. **Выбрать сертификат** из списка личных сертификатов.
4. Добавить документы.
5. Нажать кнопку **Выполнить**.

6. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием.
7. Ввести пароль и нажать на **Ок**.

#### 3.4.2. Как подписать документ, используя мастер Подпись и шифрование

1. Нажать на иконку **Подпись и шифрование**.
2. Нажать на **Подпись** в **Настройках профиля**.
3. Настроить нужные параметры (операции, сохранение результатов на устройстве, параметры подписи).
4. Вернуться на предыдущий экран, нажав на стрелку влево в левом верхнем углу рядом с **Настройками профиля**.
5. **Выбрать сертификат**. Откроется список личных сертификатов. Выбрать нужный и нажать на кнопку **Выбрать**.
6. Добавить документы.
7. Нажать кнопку **Выполнить**.
8. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием.
9. Ввести пароль и нажать на **Ок**.

#### 3.4.3. Как подписать документ с помощью контекстного меню

1. Открыть раздел **Документы**.
2. Вызвать контекстное меню у нужного файла в блоке **Архив**. 
3. Выбрать **Профили — Подпись и шифрование**.
4. Настроить нужные параметры (операции, сохранение результатов на устройстве, параметры подписи).
5. Вернуться на предыдущий экран, нажав на стрелку влево в левом верхнем углу рядом с **Настройками профиля**.
6. **Выбрать сертификат**. Откроется список личных сертификатов. Выбрать нужный и нажать на кнопку **Выбрать**.
7. Нажать кнопку **Выполнить**.
8. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием.
9. Ввести пароль и нажать на **Ок**.

#### 3.4.4. Как создать подпись со штампом времени (TSP)

Служба штампов времени используется для простановки штампов времени на документы. Данные, защищенные электронной подписью Службы, содержат надежную информацию о

времени существования электронного документа. Штампы времени используются для привязки факта существования каких-либо данных ко времени.

1. Открыть раздел **Документы**.
2. Создать профиль подписи или открыть мастер **Подпись и шифрование**. Указать следующие параметры подписи:
  - стандарт — CAdES-X Long Type 1 или CAdES-T, вид, кодировку, сохранение результатов в **Архив**;
  - опция **Штамп времени на подпись** включена автоматом;
  - включить опцию **Штамп времени на подписываемые данные** нельзя;
  - заполнить в поле Служба штампов времени (TSP) адрес службы, который можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: <протокол>://<сервер>[:порт][/путь]. В качестве протокола может быть указан "http" и "https".
3. Добавить документы.
4. Нажать на кнопку **Выполнить**.
5. Нажмите **Подтверждаю** для подтверждения прочтения документов перед подписанием.
6. Ввести пароль и нажать на **Ок**.

#### 3.4.5. Как создать усовершенствованную подпись

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.

1. Открыть раздел **Документы**.
2. Создать профиль подписи или открыть мастер **Подписи и шифрования**. Указать следующие параметры подписи:
  - стандарт — CAdES-X Long Type 1 или CAdES-T, вид, кодировку, сохранение результатов в **Архив**;
  - опция **Штамп времени на подпись** включена, отключить нельзя;
  - включить опцию **Штамп времени на подписываемые данные** нельзя;
  - заполнить в поле Служба штампов времени (TSP) адрес службы, который можно узнать у поставщика услуги. Например, услуги службы штампов времени могут

предоставлять удостоверяющие центры. Формат адреса: <протокол>://<сервер>[:порт]/[путь]. В качестве протокола может быть указан "http" и "https";

- для стандарта подписи CAdES-X Long Type 1 заполнить в поле **Служба онлайн статусов (OCSP)** адрес службы OCSP. Чаще всего адрес прописан в самом сертификате, которым создаётся подпись.

3. Добавить документы.

4. Нажать на кнопку **Выполнить**.

5. Нажмите **Подтверждаю** для подтверждения прочтения документов перед подписанием.

6. Ввести пароль и нажать на **Ок**.

### 3.4.6. Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут подписанные файлы.

При нажатии на **контекстное меню** можно:

- **Открыть** - откроется окно с информацией о подписи и исходном документе;
- **Показать свойства** — откроется окно с информацией о документе (полное наименование документа, тип, размер, дату создания и дату изменения документа);
- **Поделиться** через мессенджер, электронную почту, социальные сети, Bluetooth или сохранить в облако, а также копировать на устройство;
- **Профили: Подпись и шифрование, Проверка и расшифрование** - документ загружается в указанный профиль.

## 3.5. Шифрование документа

Шифрование документов доступно в адрес контактов или групп контактов с привязанными сертификатами шифрования.

Зашифровать документы вы можете в мастере **Подписи и шифрования** в разделе **Документы**. Добавить документы в мастер можно, выбрав файлы из блока **Архив**, загрузив файлы с устройства, либо добавить файлы в приложение КриптоАРМ ГОСТ из другого приложения по кнопке **Поделиться**.

### 3.5.1. Как зашифровать документ, используя профиль подписи

1. Создать профиль подписи с заданными настройками для шифрования.


- Ввести название нового профиля.
- Изменить операцию Подпись на операцию Шифрование.
- Настроить нужные параметры (сохранение результатов на устройство, алгоритм шифрования и кодировка файлов)

- Выбрать контакты в поле Получатели. Для выбора доступны контакты с привязанными сертификатами и группы, содержащие один или несколько таких контактов, а также Мой контакт.
  - Шифрование будет произведено в адрес сертификата контакта, выбранного по умолчанию. Для изменения сертификата шифрования нажмите на контакт в поле Получатели и в контекстном меню выберите **Выбрать сертификат**.
2. Открыть раздел **Документы** — нужный профиль подписи. При выборе профиля в мастере автоматически заполняются **Настройки операций**, сохранение результатов на устройстве.
  3. Добавить документы.
  4. Нажать кнопку **Выполнить**.

### 3.5.2. Как зашифровать документ, используя мастер Подпись и шифрование

1. Нажать на виджет **Подпись и шифрование**.
2. Перейти в **Настройки профиля**.
  - Изменить операцию **Подпись** на операцию **Шифрование**.
  - Настроить нужные параметры (сохранение результатов на устройстве, алгоритм шифрования и кодировка файлов) и вернуться на предыдущий экран.
3. Выбрать контакты в поле Получатели. Для выбора доступны контакты с привязанными сертификатами и группы, содержащие один или несколько таких контактов, а также Мой контакт.
4. Шифрование будет произведено в адрес сертификата контакта, выбранного по умолчанию. Для изменения сертификата шифрования нажмите на контакт в поле Получатели и в контекстном меню выберите **Выбрать сертификаты**.
5. Добавить документы.
6. Нажать кнопку **Выполнить**.

### 3.5.3. Как зашифровать документ с помощью контекстного меню

1. Открыть раздел **Документы**.
2. Вызвать контекстное меню у нужного файла в блоке **Архив**. 
3. Выбрать **Подпись и шифрование**.
4. Перейти в **Настройки профиля**.
  - Изменить операцию Подпись на операцию Шифрование.
  - Настроить нужные параметры (сохранение результатов на устройстве, алгоритм шифрования и кодировка файлов) и вернуться на предыдущий экран.
5. Выбрать контакты в поле Получатели. Для выбора доступны контакты с привязанными сертификатами и группы, содержащие один или несколько таких контактов, а также Мой контакт.



6. Шифрование будет произведено в адрес сертификата контакта, выбранного по умолчанию. Для изменения сертификата шифрования нажмите на контакт в поле Получатели и в контекстном меню выберите **Выбрать сертификат**.

7. Нажать кнопку **Выполнить**.

8. Ввести пароль и нажать на **Ок**.

### 3.5.4. Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут зашифрованные файлы.

При нажатии на **контекстное меню** можно:

- изучить **Свойства документа** (название документа, тип, размер, дата создания, дата изменения);
- По нажатию на **Подпись и шифрование/Проверка и расшифрование** зашифрованный документ добавляется в выбранный мастер.
- **Поделиться** через мессенджер, электронную почту, социальные сети, Bluetooth или сохранить в облако, а также копировать на устройство.

## 3.6. Архивирование документа

Архивировать документы можно в мастере **Подписи и шифрования** или создав профиль подписи с операцией Архивирование.

### 3.6.1. Как архивировать документ через мастер Подпись и шифрование

1. Открыть раздел **Документы**.
2. Нажать на иконку мастера **Подпись и шифрование**.
3. Нажать на **Подпись** в **Настройках профиля**.
4. Выбрать операцию **Архивирование**.
5. При необходимости деактивировать флаг **Создать копии файлов в Архив**.
6. Вернуться на предыдущий экран, нажав на стрелку влево в левом верхнем углу рядом с **Настройками профиля**.
7. Добавить документы.
8. Нажать на **Выполнить**.

### 3.6.2. Как архивировать документ с помощью профиля подписи

1. Открыть раздел **Документы**.
2. Выбрать ранее созданный профиль подписи с операцией **Архивирование**.
3. Добавить документы.
4. Нажать на **Выполнить**.

### 3.6.3. Результат выполнения операции

В окне результатов операций мастера **Подписи и шифрования** будут заархивированные файлы. При нажатии на **контекстное меню** можно:

- **Показать свойства** — откроется окно с информацией о документе (полное наименование документа, тип, размер, дату создания и дату изменения документа);
- **Поделиться** через мессенджер, электронную почту, социальные сети, Bluetooth или сохранить в облако, а также копировать на устройство;
- **Профили: Подпись и шифрование, Проверка и расшифрование** - документ загружается в указанный профиль.

## 3.7. Проверка подписи документа

Для проверки подписи достаточно выделить файл расширением .sig, .p7s, .sgn, .sign или .bin, который содержит электронную подпись. Никаких дополнительных настроек при проверке подписи производить не нужно.

1. Открыть раздел **Документы**.
2. Выбрать мастер **Проверка и расшифрование**.
3. Добавить документ.
4. Результаты проверки будут на экране (**Подпись подтверждена** или **Ошибка**).

Надпись **Ошибка** означает, что подпись не подтверждена.

### 3.7.1. Результат операции

В окне результатов операций мастера **Проверки и расшифрования** будут загруженные файлы. При нажатии на **контекстное меню** можно:

- **Открыть** - откроется окно с информацией о подписи и исходном документе;
- **Показать свойства** — откроется окно с информацией о документе (полное наименование документа, тип, размер, дату создания и дату изменения документа);
- **Поделиться** через мессенджер, электронную почту, социальные сети, Bluetooth или сохранить в облако, а также копировать на устройство;
- **Профили: Подпись и шифрование, Проверка и расшифрование** - документ загружается в указанный профиль.

## 3.8. Расшифрование документа

Для расшифрования у вас в хранилище Личных сертификатов должен быть сертификат с привязанным к нему закрытым ключом, который был выбран в качестве сертификата получателя при шифровании.

Для расшифрования нужно выбрать зашифрованные файлы с расширением .enc.

1. Открыть раздел **Документы**.

2. Выбрать мастер **Проверка и расшифрование**.
3. Добавить документ. Начнётся операция расшифрования.
4. Ввести пароль и нажать **Ок**.

Результаты проверки будут на экране (расшифрованный файл или **Ошибка**).

**Ошибка** означает, что на устройстве отсутствует личный сертификат с привязанным к нему закрытым ключом, в адрес которого происходило шифрование.

В окне результатов операций мастера **Проверки и расшифрования** будут расшифрованные файлы. При нажатии на **контекстное меню** можно:

- изучить **Свойства документа** (название документа, тип, размер, дата создания и изменения);
- **Просмотреть документ** — открыть файл с помощью приложения на устройстве (браузер, КриптоАРМ ГОСТ 3, текстовые редакторы);
- **Отправить** через мессенджер, электронную почту, социальные сети, Bluetooth или сохранить в облако, а также копировать на устройство.

### 3.9. Соподпись (добавление подписи к файлу)

Чтобы подписывать документы электронной подписью, нужно установить в Личное хранилище сертификат с привязанным к нему закрытым ключом.

Вы можете добавлять подпись к уже подписанному файлу.

Для этого в мастер **Подпись и шифрование** загрузите файлы с расширением .sig с устройства.

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

Стандарт подписи, использование штампов времени, сертификат подписи, каталог для сохранения подписанного документа вы можете настроить в профиле подписи или в настройках операций в мастере.

Настройка **Действия при соподписи** позволяет добавлять соподпись в исходный файл либо в копию исходного файла.


#### 3.9.1. Как добавить подпись, используя профиль подписи

1. Открыть раздел **Документы**.
2. Выбрать нужный профиль подписи.
3. Выбрать сертификат подписи.
4. Добавить уже подписанные документы с устройства.
5. Нажать на **Выполнить**.
6. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием.


### 3.9.2. Как добавить подпись, используя мастер Подпись и шифрование

1. Открыть раздел **Документы**.
2. Нажать на мастер **Подпись и шифрование**.
3. Задать настройки профиля (операция **Подпись** и иные параметры).
4. Выбрать сертификат подписи.
5. Добавить уже подписанные документы с устройства.
6. Нажать на **Выполнить**.
7. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием.

### 3.9.3. Как добавить подпись к файлу, расположенному в блоке Архив

1. Открыть раздел **Документы**.
2. Нажать на **контекстное меню** подписанного документа. 
3. Выбрать **Подпись и шифрование**.
4. Указать настройки профиля подписи и выбрать сертификат подписи.
5. **Выполнить**.
6. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием.
7. **Ввести** пароль.

### 3.9.4. Результат выполнения операции

В окне результатов операций мастера Подписи и шифрования будут подписанные файлы. При нажатии на контекстное меню можно: 

- **Открыть** - откроется окно с информацией о подписи и об исходном документе
- **Показать свойства** — откроется окно со свойствами о подписанном документе (полное название документа, тип, размер, дата создания и дата изменения).
- **Поделиться** через мессенджер, электронную почту, социальные сети, Bluetooth или сохранить в облако, а также копировать на устройство.
- **Профили: Подпись и шифрование/проверка и расшифрование** - подписанный файл добавиться в выбранный мастер

## 3.10. Снятие подписи с файла

Для снятия подписи достаточно выбрать файлы с расширением .sig, .p7s, .sgn, .sign, .bin, которые содержат электронную подпись. Никаких дополнительных настроек производить не нужно.

1. Открыть раздел **Документы**.

2. Открыть контекстное меню у подписанного документа, расположенного во вкладке **Архив**.
3. Выбрать **Открыть**.
4. В открывшемся окне перейти на вкладку **Документы**

### 3.11. Прямые групповые операции

Вы можете выполнять подпись, архивирование и шифрование за одну операцию. Это будут прямые групповые операции. Они выполняются в мастере Подпись и шифрование.

Вы можете комбинировать операции и выбрать одну из комбинаций:

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

**ВАЖНО!** Чтобы подписывать и зашифровывать документы, у вас должна быть действительная лицензия на криптопровайдер КриптоПро CSP.

Чтобы подписывать документы электронной подписью, нужно установить в Личное хранилище сертификат с привязанным к нему закрытым ключом.

Чтобы шифровать документы, в приложении должны быть контакты, к которым привязаны сертификаты для шифрования.

#### 3.11.1. Прямые групповые операции в мастере Подпись и шифрование

1. Открыть раздел **Документы**.
2. Открыть мастер **Подпись и шифрование**.
3. Открыть настройки профиля, указать нужные операции и их параметры.
4. Выбрать сертификат для подписания документа и контакт, в адрес которого будет проводиться шифрование.
5. Добавить документы с устройства.
6. Нажать на **Выполнить**.
7. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием, если выбрана операция подписи.
8. Ввести пароль и нажать **Ок**.

#### 3.11.2. Прямые групповые операции в профиле подписи

1. Открыть раздел **Документы**.
2. Выбрать нужный профиль подписи, в котором заданы операции и настройки операций.

3. Выбрать сертификат для подписи и контакт, в адрес которого будет проводиться шифрование.
4. Добавить документы с устройства.
5. Нажать на **Выполнить**.
6. Нажмите **Подтверждаю** для подтверждения ознакомления с документом перед подписанием, если выбрана операция подписи.
7. Ввести пароль и нажать **Ок**.

По умолчанию установлен флаг **Создать копию в Архиве** - копия документов сохраняется во вкладке Архив. Если данный флаг не активен, то подписанные/зашифрованные файлы будут недоступны.

### 3.12. Обратные групповые операции

Вы можете выполнять расшифрование, разархивирование, проверку и снятие подписи. Для их выполнения предназначен мастер Проверки и расшифрования.

**ВАЖНО!** Чтобы проверять подпись и расшифровывать документы, у вас на устройстве должна быть действительная лицензия на криптопровайдер КриптоПро CSP.

Чтобы расшифровывать документы, нужно установить в Личное хранилище сертификат с привязанным к нему закрытым ключом.

По итогам проверки подписанных документов в списке выводится информация о подписи.

Для выполнения обратных операций выбор профиля подписи и настройка параметров операций не требуется.

1. Открыть раздел **Документы**.
2. Открыть мастер **Проверка и расшифрование**.
3. Выбрать документ.
4. Ввести пароль и нажать **Ок**, если файл был зашифрован.

На вкладке Проверка и расшифрование отображаются ход и результаты выполнения операций:

- **Подпись подтверждена** означает успешную проверку подписи — подпись была создана для проверяемого документа, в последующем документ не был изменён.
- **Ошибка** означает, что на устройстве отсутствует личный сертификат с привязанным к нему закрытым ключом, в адрес которого происходило шифрование, либо подпись не подтверждена.

В окне результатов операций мастера **Проверки и расшифрования** будут загруженные файлы. При вызове контекстного меню можно:

- **Открыть** - откроется окно с информацией о подписи и об исходном документе либо откроется файл с помощью приложения на устройстве (браузер, текстовые редакторы)
- **Показать свойства** — открывается окно со свойствами о документе (полное наименование документа, размер, дата создания и дата изменения)

- **Поделиться** через мессенджер, электронную почту, социальные сети, Bluetooth или сохранить в облако, а также копировать на устройство.
- **Профили: Подпись и шифрование/Проверка и расшифрование** - открывается выбранный профиль с добавленным документом

## 4. Контакты

Данный раздел **Контакты** предназначен для управления контактами: создание контактов, импорт/экспорт контактов в виде файлов vCard (файл расширения .vcf), привязка к контактам сертификатов, заполнение реквизитов контакта на основе данных сертификата и организовывание контактов в группы.

### 4.1. Экспорт контактов

Для того, чтобы экспортировать всю адресную книгу, нужно:

1. Перейти в раздел **Контакты**
2. Нажать на виджет Экспорт в файл
3. Выбрать приложение/директорию, куда будет отправлен/сохранен файл.

Для того, чтобы экспортировать один или несколько контактов нужно:

1. Перейти в раздел **Контакты**.
2. Перейти в меню выбора контактов. Для этого нажмите на кнопку “Выбрать” или используйте долгое нажатие по контакту.
3. Выделить чек-боксом необходимые для экспорта контакты.
4. Нажать на виджет **Экспортировать в файл** либо клик на **Поделиться** в нижней панели действий.
5. Выбрать приложение/директорию, куда будет отправлен/сохранен файл.

### 4.2. Импорт контактов

Импортировать контакты можно как в просматриваемую группу, так и в группу **Контакты**. При импорте файла vCard, содержащего группы с контактами, в указанной папке будет создана структура групп и контактов в соответствии с файлом.

Для того, чтобы импортировать контакты, нужно:

1. Перейти в раздел Контакты.
2. Нажать на виджет Импорт из файла.
3. Выбрать файл vCard (файл формата .vcf)

### 4.3. Действия с контактами

Можно выполнить следующие действия с контактом:

- **Изменить контакт** - откроется окно для изменения данных контакта;
- **Поделиться** - откроется окно для выбора приложения, в которое будет направлен сформированный файл с данными контакта в формате vCard;
- **Добавить в Избранное** - избранный контакт добавляется в группу Избранное, у контакта появляется значок избранного;



- **Убрать из Избранного** - контакт удален из папки Избранное, значок избранного контакта убран;
- **Переместить** - откроется окно со списком групп для перемещения;
- **Удалить** - после подтверждения удаления контакт пропадает из списка и удаляется навсегда.

#### 4.4. Мой контакт

При установке приложения автоматически создается **Мой контакт**. К контакту привязываются все личные сертификаты, находящиеся в хранилище **Личные сертификаты**.

Можно совершить следующие действия с **Мой контакт**:

- **Просмотреть сведения** - по одиночному клику на контакт открывается окно с просмотром личной информации о контакте и привязанных к контакту сертификатах;
- **Изменить контакт** - откроется окно для изменения данных контакта. Нельзя изменить группу расположения контакта;
- **Поделиться** - откроется окно для выбора приложения, в которое будет направлен сформированный файл с данными контакта в формате vCard;
- **Добавить в Избранное** - контакт добавляется в папку Избранное, у контакта появляется значок избранного;
- **Убрать из Избранного** - контакт удален из папки Избранное, значок избранного контакта убран.

Нельзя удалить **Мой контакт**.

#### 4.5. Создание контакта

Вы можете создать контакты для шифрования в их адрес, для хранения имен, адресов электронной почты, номеров телефонов и других данных.

Можно привязать сертификат другого пользователя к контакту для шифрования документов в его адрес. Привязать сертификат можно из раздела **Личные сертификаты** либо загрузить с устройства файл расширения .crt/.cer.

**Сертификаты, привязанные к контакту с устройства, не сохраняются в хранилище Личные сертификаты и при удалении контакта будут удалены вместе с ним**

При выборе сертификата можно заполнить данные контакта на основании данных сертификата:

- **Только пустые поля;**
- **Перезаполнить все;**
- **Нет.**

##### 4.5.1. Создание контакта без сертификата в разделе Контакты

1. Открыть раздел **Контакты**;
2. Нажать на виджет **Создать**;

3. В контекстном меню выбрать **Создать контакт**;
4. Во вкладке **Данные** заполнить необходимые поля;
5. Нажать на **Сохранить**.

#### **4.5.2. Создание контакта с сертификатом из файла в разделе Контакты**

1. Открыть раздел **Контакты**;
2. Нажать на виджет **Создать**;
3. В контекстном меню выбрать **Создать контакт**
4. Во вкладке **Данные** заполнить необходимые поля
5. Во вкладке **Сертификаты** нажать на текстовую кнопку **Добавить сертификат**
6. В окне **Добавить сертификат** выбрать **Импортировать из файла**
7. Загрузить файл расширения **.cer/.crt**
8. В диалоговом окне выбрать любой из нужных вариантов заполнения полей контакта
9. Нажать на **Сохранить**

#### **4.5.3. Создание контакта с сертификатом из раздела Личные сертификаты в разделе Контакты**

1. Открыть раздел **Контакты**
2. Нажать виджет **Создать**
3. В контекстном меню выбрать **Создать контакт**
4. Во вкладке **Данные** заполнить необходимые поля
5. Во вкладке **Сертификаты** нажать на текстовую кнопку **Добавить сертификат**
6. В окне **Добавить сертификат** выбрать **Добавить из “Личные сертификаты”**
7. Выбрать необходимый сертификат и нажать на **Выбрать**
8. Нажать на кнопку **Сохранить**

Для создания контакта из сертификата необходимо сохранить на устройство один или несколько файлов с сертификатами **.cer/.crt**.

#### **4.5.4. Создать контакт из сертификата в разделе Контакты**

1. Открыть раздел **Контакты**
2. Нажать на виджет **Создать**
3. В контекстном меню выбрать **Создать контакт из сертификата**
4. Выбрать файл расширения **.cer/.crt**

#### **4.5.5. Описание полей формы создания контакта**

Поля сгруппированы по вкладкам **Данные** и **Сертификаты**.

Во вкладке **Данные** отображаются личные данные контакта: имя, фамилия, отчество, дата рождения, телефон, адрес и др.

Во вкладке **Сертификаты** отображается список привязанных к контакту сертификатов. Можно просмотреть свойства сертификата, перевыбрать сертификат, который будет использоваться при операции шифрование, экспортировать и отвязать сертификат от контакта.

#### 4.6. Просмотреть сведения о созданном/импортированном контакте

Для того, чтобы просмотреть информацию о контакте, нужно:

1. Открыть раздел **Контакты**;
2. Нажать на нужный контакт.

Если информация о контакте заполнена (указаны фамилия, отчество, номер телефона, e-mail, иные данные, а также привязан сертификат), то эту информацию можно увидеть соответственно во вкладках **Данные** и **Сертификаты**.

Если заполнены только личные данные, то будет видна только одна вкладка с информацией **Данные** (телефон, электронная почта и т.д.)

Если заполнены личные данные и привязан сертификат, то будут отображаться обе вкладки с соответствующей информацией (личные данные и информация о сертификате).

В окне просмотра информации о контакте есть кнопка **Редактировать контакт**, при нажатии на которую открывается окно, в котором можно заполнить или перезаполнить необходимые поля с личными данными контакта или привязать или отвязать сертификат.

#### 4.7. Редактирование контакта

Можно отредактировать как созданный контакт, так и импортированный.

##### 4.7.1. Редактирование контакта через контекстное меню

1. Открыть раздел **Контакты**.
2. Вызвать у контакта контекстное меню по клику на кнопку **Еще** (три точки).
3. В контекстном меню выбрать **Изменить контакт**.
4. Изменить нужные поля.
5. **Сохранить** изменения.

##### 4.7.2. Редактирование контакта через окно просмотра информации о контакте

1. Открыть раздел **Контакты**.
2. По нажатию на контакт открыть окно просмотра информации о контакте.

3. Перейти в окно редактирования контакта по клику на кнопку **Редактировать** (карандаш) в правом верхнем углу.
4. Изменить нужные поля.
5. **Сохранить** изменения.

#### 4.8. Создание группы контактов

Для организации хранения контактов вы можете создать пользовательские группы и подгруппы.

При установке приложения автоматически установлены группы **Контакты**, **Все контакты** и **Избранные**.

В группе **Все контакты** отображаются все контакты, сохраненные в приложении, без иерархии.

В группе **Избранные** отображаются контакты, отмеченные как избранные.

##### 4.8.1. Создать пользовательскую группу (через виджет Создать)

1. Открыть раздел **Контакты**.
2. Нажать на виджет **Создать**.
3. В контекстном меню выбрать **Создать группу**.
4. Заполнить поле **Название группы** и расположение.
5. Нажать на **Сохранить**.

##### 4.8.2. Создать пользовательскую группу (через меню групп раздела Контакты)

1. Открыть раздел **Контакты**.
2. Открыть окно просмотра списка групп по клику кнопку вызова списка групп (картинка)
3. В окне списка групп клик на кнопку **Создать группу** в правом верхнем углу.
4. Заполнить поле **Название группы** и расположение.
5. Нажать на **Сохранить**.

#### 4.9. Просмотреть содержимое группы

Для того, чтобы просмотреть содержимое группы, нужно:

1. Перейти в раздел **Контакты**.
2. Нажать на нужную группу

Можно выполнить следующие действия с группой:

- **Изменить группу** - откроется окно для изменения названия и расположения группы;
- **Поделиться** - откроется окно для выбора приложения, в которое будет направлен сформированный файл с данными о группе и контактах в формате vCard;
- **Переместить** - откроется окно со списком групп, к котором необходимо выбрать группу для перемещения;
- **Удалить** - после подтверждения удаления группа и все входящие в нее подгруппы и контакты пропадают из списка и удаляются навсегда.

Нельзя удалить и переместить группы **\*\*Избранные\*\*** и **\*\*Все контакты\*\***.

- **Просмотреть сведения** - по одиночному клику на контакт открывается окно с просмотром личной информации о контакте и привязанных к контакту сертификатах;
- **Изменить контакт** - откроется окно для изменения данных контакта. Нельзя изменить группу расположения контакта
- **Поделиться** - откроется окно для выбора приложения, в которое будет направлен сформированный файл в формате vCard;
- **Добавить в Избранное** - контакт добавляется в папку Избранное, у контакта появляется значок избранного.
- **Убрать из Избранного** - контакт удален из папки Избранное, значок избранного контакта убран.
- **Удалить** - после подтверждения удаления группа пропадает из списка групп и удаляется навсегда вместе с вложенными в нее контактами и подгруппами.

## 5. Сертификаты

Раздел содержит информацию по управлению сертификатами и ключевыми контейнерами.

**ВАЖНО!** Чтобы работать с сертификатами, у вас на устройстве должна быть действительная лицензия на криптопровайдер КриптоПро CSP.

Для того чтобы попасть в раздел **Сертификаты**, нужно нажать на кнопку **Меню** и выбрать раздел **Сертификаты**.

В верхней панели расположены кнопка **Меню**, название раздела, функция поиска и иконка **Оповещений**.

Блок **Действия** состоит из 4 виджетов и позволяет подключить носитель, создать запрос на сертификат, импортировать сертификат из файла или добавить сертификат с помощью QR-кода

Ниже размещено хранилище сертификатов.

Вкладка сертификатов состоит следующих хранилищ:

- **Личные сертификаты** — для управления личными сертификатами, у которых есть привязка к закрытому ключу;
- **Удостоверяющие центры** — для управления доверенными корневыми сертификатами;
- **Списки отзыва** — для управления списками отзыва сертификатов;
- **Запросы** — для управления запросами на сертификат;
- **Ключи** — для отображения ключевых контейнеров.

## 5.1. Установка личного сертификата

Если у вас сертификат на защищённом носителе или в локальном хранилище устройства, то воспользуйтесь инструкцией по установке сертификата из ключевого контейнера.

Если у вас есть сгенерированный закрытый ключ и вы получили сертификат в Удостоверяющем центре, то для установки сертификата воспользуйтесь инструкцией по установке сертификата с привязкой к ключевому контейнеру.

Перед импортом личного сертификата убедитесь, что у вас действительная лицензия на криптопровайдер КриптоПро CSP.

**Примечание:** для того чтобы сертификат был действительный, у вас должны быть установлены корневые сертификаты УЦ и актуальный список отзыва сертификатов (COC).

### 5.1.1. Установка сертификата из ключевого контейнера

Данный способ возможен, если сертификат присутствует в контейнере. Иначе функция установки будет недоступна.

1. Подключить защищённый носитель к устройству.
2. Открыть раздел **Сертификаты**.
3. Открыть хранилище **Ключи**.
4. Вызвать контекстное меню у нужного контейнера.
5. Выбрать **Установить сертификат**.
6. При необходимости ввести пароль к ключевому контейнеру.

Сертификат установлен в личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

### 5.1.2. Установка сертификата с NFC-носителя

1. Открыть раздел **Сертификаты**.
2. Нажать виджет **Подключить ноистель**
3. Поднести смарт-карту NFC.
4. Дождаться информера **Сертификаты успешно установлены**

Сертификат установлен в личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

#### **5.1.3. Установка сертификата с закрытым ключом из файла .pfx**

1. Открыть раздел **Сертификаты**.
2. Нажать на **Импортировать из файла**.
3. В файловом менеджере выбрать файл сертификата .pfx.
4. Ввести пароль к контейнеру pfx.
5. Задать новый пароль к ключевому контейнеру.

Сертификат установлен в личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

#### **5.1.4. Установка сертификата с привязкой к ключевому контейнеру**

1. Открыть раздел **Сертификаты**.
2. Нажать на **Импортировать из файла**.
3. В файловом менеджере выбрать файл сертификата .cer или .crt.

Сертификат установлен в личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

#### **5.1.5. Установка сертификата с помощью QR-кода**

1. Установить КриптоПро CSP 5.0 R3 на компьютер.
2. Запустить утилиту **Инструменты КриптоПро**.
3. В списке выбрать раздел **Сертификаты**.
4. Выделить нужный сертификат и нажать на кнопку **Экспортировать ключи**. Сертификат подписи должен быть экспортируемым, в противном случае ключ нельзя будет перенести.
5. В появившемся окне **Ввод пароля на PFX** пропустить, вводить не обязательно.
6. Выбрать опцию **Экспортировать PFX в QR-код**.
7. В выпадающем меню **Выберите приложение** указать КриптоАРМ ГОСТ 3.
8. Ввести пароль и нажать на **Ок**.
9. Запустить КриптоАРМ ГОСТ 3 на смартфоне.
10. Открыть раздел **Сертификаты**.
11. Выбрать **Добавить с QR-кода**.
12. Дать разрешение приложению снимать фото и видео.
13. Отсканировать QR-код с экрана компьютера.
14. Назначить пароль на контейнер.

15. Ввести пароль для контейнера и нажать на **Ок**.

16. Ввести пароль на PFX (см. п. 6, данный пароль может быть не задан при экспорте) и **Далее**.

Сертификат успешно установлен и готов для подписания и расшифрования электронных документов.

## 5.2. Установка корневого и промежуточного сертификатов

Установить корневой или промежуточный сертификат вы можете в хранилище **Удостоверяющие центры** раздела **Сертификаты**.

1. Открыть раздел **Сертификаты**.
2. Перейти в **Удостоверяющие центры**
3. Нажать на кнопку **Добавить сертификат**.



4. Выбрать **Импортировать из файла**.
5. В файловом менеджере выбрать файл сертификата.
6. Подтвердить запрос на установку сертификата.

При успешном импорте сертификат появится в списке хранилища **Удостоверяющие центры**.

## 5.3. Создание запроса на сертификат

Чтобы получить личный сертификат для выполнения криптографических операций, необходимо создать запрос на сертификат и направить его на рассмотрение в Удостоверяющий центр (УЦ).

1. Открыть раздел **Сертификаты**.
2. Нажать на **Создать запрос**.
3. Настроить параметры запроса на сертификат:
  - Шаблон сертификата — По умолчанию / Сертификат КЭП ИП / Сертификат КЭП физического лица / Сертификат КЭП юридического лица / Шаблон с расширенным списком полей;
  - Создать как самоподписанный сертификат;
4. Заполнить сведения о владельце. Набор полей меняется в зависимости от выбранного шаблона.
5. Указать параметры ключа: алгоритм, назначение ключа и возможность его экспортировать (данная опция позволит экспортировать сертификат вместе с привязанным к нему закрытым ключом для переноса на другое устройство).
6. Выбрать назначение сертификата.
7. Нажать на **Готово**.



8. Нажимать на экран в рандомном порядке, пока ключ не будет создан.

9. Ввести и подтвердить пароль, нажать на **Ок**.

На основе указанных данных формируется запрос на сертификат, который отображается в хранилище **Запросы**. Можно изучить его свойства, экспортировать или удалить.

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

#### 5.4. Создание самоподписанного сертификата

**Самоподписанный сертификат [КАА1]** — сертификат, изданный самим пользователем, без обращения к Удостоверяющему центру. Самоподписанный сертификат является одновременно личным и корневым (устанавливается в Личное хранилище сертификатов и Доверенные корневые центры сертификации).

Самоподписанные сертификаты используются для обмена зашифрованными или подписанными документами между людьми, доверяющими друг другу, например, друзьями, коллегами.

1. Открыть раздел **Сертификаты**.
2. Нажать на **Создать запрос** или открыть хранилище **Личные сертификаты — Добавить сертификат — Создать запрос**.
3. Настроить параметры запроса на сертификат:
  - Удостоверяющий центр;
  - Шаблон сертификата — По умолчанию / Сертификат КЭП ИП / Сертификат КЭП физического лица / Сертификат КЭП юридического лица / Шаблон с расширенным списком полей;
  - Подписать запрос;
  - Создать как самоподписанный сертификат — установить данный ползунок;
4. Заполнить сведения о владельце. Набор полей меняется в зависимости от выбранного шаблона.
5. Указать параметры ключа: алгоритм, назначение ключа и возможность его экспортировать (данная опция позволит экспортировать сертификат вместе с привязанным к нему закрытым ключом для переноса на другое устройство).
6. Выбрать назначение сертификата.
7. Нажать на **Готово**.
8. Нажимать на экран в рандомном порядке, пока ключ не будет создан.
9. Ввести и подтвердить пароль, нажать на **Ок**.

На основе указанных данных формируется самоподписанный сертификат.

При успешной генерации сертификат устанавливается в хранилище **Личные сертификаты**.

При генерации самоподписанного сертификата запрос на сертификат не создаётся.

## 5.5. Установка списка отзыва сертификатов

Список отзыва сертификатов (COC/CRL) — документ с электронной подписью уполномоченного лица Удостоверяющего центра, включающий в себя список серийных номеров сертификатов, которые на определенный момент времени были отозваны или действие которых было временно приостановлено.

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Списки отзыва**.
3. Нажать на кнопку **Добавить сертификат**.



4. Выбрать **Импортировать из файла**.
5. В файловом менеджере выбрать файл списка отзыва с расширением .crl.
6. Подтвердить добавление сертификата в списки отзыва, нажав на **Продолжить**.

При успешном импорте СОС отображается в хранилище **Списки отзыва** со статусом *Действителен*.

Можно посмотреть **Свойства** или **Удалить**.


## 5.6. Экспорт личного сертификата

Для обмена шифрованными данными с другими пользователями необходимо экспортировать сертификат без закрытого ключа.

Экспорт сертификата с привязанным к нему закрытым ключом нужен в следующих ситуациях:

- сохранение копии сертификата и связанного с ним закрытого ключа;
- удаление сертификата и его закрытого ключа с устройства для установки на другое устройство.

### 5.6.1. Экспорт сертификата без закрытого ключа

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Личные сертификаты**.
3. Вызвать контекстное меню у нужного сертификата .
4. Выбрать **Экспортировать**.
5. В открывшемся окне выбрать нужные настройки (не экспортировать закрытый ключ, тип кодировки). Выбор экспорта закрытого ключа может быть заблокирован, если ключ не экспортируемый.
6. Нажать на **Выполнить** в правом верхнем углу.
7. Выбрать, куда будет сохранён экспортированный сертификат (копировать на устройство; отправить по e-mail, в социальной сети или в мессенджере, сохранить в облаке, передать по Bluetooth).

### 5.6.2. Экспорт сертификата с закрытым ключом в контейнер PFX

**Важно!** Вы можете экспортировать сертификат вместе с привязанным к нему закрытым ключом, если ключ имеет флаг "экспортируемый". В противном случае эта функция недоступна.

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Личные сертификаты**.
3. Вызвать контекстное меню у нужного сертификата.
4. Выбрать **Экспортировать**.
5. В открывшемся окне выбрать нужные настройки (экспортировать закрытый ключ, тип кодировки). Выбор экспорта закрытого ключа может быть заблокирован, если ключ не экспортируемый. **Задать** пароль к файлу .pfx.
6. **Ввести** пароль к сертификату.
7. Выбрать, куда будет сохранён экспортированный сертификат (копировать на устройство; отправить по e-mail, в социальной сети или в мессенджере, сохранить в облаке, передать по Bluetooth).

При успешном выполнении операции сертификат экспортируется в файл.

### 5.7. Экспорт сертификата

Корневые и промежуточные сертификаты экспортируются без закрытого ключа.

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Удостоверяющие центры**.
3. Вызвать контекстное меню у нужного сертификата.
4. Выбрать **Экспортировать**.
5. Указать тип кодировки DER или BASE64.
6. Нажать **Выполнить**.
7. Выбрать, куда будет сохранён экспортированный сертификат (копировать на устройство; отправить по e-mail, в социальной сети или в мессенджере, сохранить в облаке, передать по Bluetooth).

При успешном выполнении операции сертификат экспортируется в файл.

### 5.8. Удаление сертификата

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище, из которого необходимо удалить сертификат.
3. Вызвать контекстное меню у нужного сертификата.
4. Выбрать **Удалить**.
5. Подтвердить удаление.

Сертификат будет успешно удален из хранилища.

**Важно:** если у сертификата есть привязка к закрытому ключу, то при удалении сертификата удаляется и его контейнер. Контейнер не подлежит восстановлению.

## 5.9. Ключевые контейнеры

В программе отображаются ключевые контейнеры, расположенные на устройстве и на отчуждаемых носителях, например, USB-токенах или смарт-картах.

### 5.9.1. Как посмотреть сертификат в контейнере

1. При необходимости подключить защищённый носитель к устройству.
2. Открыть раздел **Сертификаты**.
3. Открыть хранилище **Ключи**.
4. Нажать на контейнер.

Откроется информация о сертификате в контейнере.

### 5.9.2. Как установить сертификат из ключевого контейнера

**Примечание:** данная функция доступна только для контейнеров, в которых есть сертификат.

1. При необходимости подключить защищённый носитель к устройству.
2. Открыть раздел **Сертификаты**.
3. Открыть хранилище **Ключи**.
4. Вызвать контекстное меню у нужного контейнера.
5. **Установить сертификат**.
6. При необходимости ввести пароль к ключевому контейнеру.

### 5.9.3. Удаление сертификата

**ВАЖНО!** Удаленный контейнер не подлежит восстановлению! Вам придется перевыпускать сертификат.

1. Открыть раздел **Сертификаты**.
2. Открыть хранилище **Ключи**.
3. Вызвать контекстное меню у нужного контейнера.
4. **Удалить**.
5. Подтвердить удаление.

### 5.9.4. Обновление списка контейнеров

Для обновления списка контейнеров необходимо свайпнуть вниз.

## 6. Оповещения

Раздел содержит информацию об оповещениях и журнале событий.

### 6.1. Журнал операций

Информация о событиях, происходящих в рамках приложения, записывается в **Журнал операций** (Оповещения).

Для того чтобы открыть журнал, нужно нажать на "колокольчик" в правом верхнем углу приложения либо через пункт **Журнал операций** в боковом меню приложения.



### 6.2. Настройки оповещений

При нажатии на контекстное меню справа от строки поиска откроются **Настройки оповещений**:

- **Выделить оповещения** — выделяет все оповещения из списка, после чего их можно **Сохранить** (не реализовано в данной версии), **Отправить** (копировать на устройство, сохранить в облаке, отправить в мессенджере, по электронной почте или в социальной сети)
- **Экспортировать оповещения** — сохраняет все оповещения в файл формата .txt для копирования на устройство, сохранения в облаке, отправки в мессенджере, по электронной почте или в социальной сети.

#### 6.2.1. Сортировка и фильтрация

Все оповещения разделены по вкладкам:

- **Общее** — содержит все оповещения, информирующие о действиях;
- **Информация** — содержит оповещения о действиях (например, операция подписи, экспорт сертификата);
- **Ошибки** — содержит оповещения об ошибках в работе приложения;
- **Предупреждения** — содержит оповещения о нештатных ситуациях (например, отсутствие лицензии).

Для фильтрации нужно воспользоваться строкой поиска по символному совпадению. В данном случае останутся записи, удовлетворяющие запросу.

Для более детальной фильтрации можно задать параметры. Для этого нужно нажать на кнопку поиска и кнопку фильтра.



Предусмотрены следующие параметры:

- **Даты** — диапазон дат;

- **Разделы** — раздел, в котором возникло событие;
- **Уровень оповещения** — информация, предупреждение или ошибка.

Фильтр применяется после нажатия на кнопку **Применить**.

Для отмены параметра фильтрации необходимо нажать на отмену для конкретного параметра.



## 7. Ключевые носители

Раздел содержит информацию по работе с ключевыми носителями продуктовой линейки Рутокен (АО «Актив-Софт»).

### 7.1. Подключение защищённых носителей

Для подключения **смарт-карты Рутокен ЭЦП 3.0 NFC** необходимо:

- включить функцию NFC на устройстве;
- нажать на виджет **Подключить носитель**;
- приложить смарт-карту к задней панели устройства.

Для подключения **USB-токена Рутокен ЭЦП 3.0** необходимо:

- подключить через адаптер Lightning-USB (USB-C) токен к устройству

### 7.2. Установка ключей со смарт-карты Рутокен ЭЦП 3.0 NFC/ USB-токена Рутокен ЭЦП 3.0 NFC бесконтактным способом.

1. Запустить приложение КриптоАРМ ГОСТ 3.
2. Открыть раздел **Сертификаты — Подключить носитель**
3. Подключить защищённый носитель.
4. После считывания открытый ключ установится в хранилище **Личные сертификаты**.

### 7.3. Установка ключей с USB-токена Рутокен ЭЦП 3.0 контактным способом

1. Запустить приложение КриптоАРМ ГОСТ 3.
2. Подключить через адаптер Lightning-USB (через адаптер USB-C) токен
3. Открыть раздел **Сертификаты - Ключи**
4. Вызвать контекстное меню у нужного контейнера
5. Нажать **Установить**

## 8. О приложении

### 8.1. Установка лицензии КриптоАРМ ГОСТ 3

Для установки ключа активации лицензии нужно перейти в раздел **Лицензии (Меню — О приложении — лицензия КриптоАРМ ГОСТ — Ввести лицензию)**. Ввести ключ активации лицензии и нажать на **Далее**.

При успешной установке обновится информация о статусе и дате истечения лицензии.

### 8.2. Установка лицензии КриптоПро CSP

Установка ключа активации лицензии производится через пользовательский интерфейс приложения КриптоАРМ ГОСТ 3.

Для установки ключа активации лицензии нужно перейти в раздел **Лицензии (Меню — О приложении — лицензия КриптоПро CSP — Ввести лицензию)**. Вставить ключ активации лицензии на КриптоПро CSP и нажать **Далее**.

При успешной установке обновится информация о статусе лицензии (действительна) и сроке её действия.

В случае если ключ активации лицензии на продукт не введен или лицензия недействительна, то при каждом запуске приложения будет появляться всплывающее сообщение с информацией. Функции по работе с приложением будут ограничены.

### 8.3. Установка лицензии на КриптоПро TSP Client

Для создания подписи со штампом времени на подпись или данные необходима лицензия на модуль TSP. При первой установке приложения единожды активируется пробная лицензия на КриптоПро TSP сроком на 90 дней. По истечении пробного периода для работы с приложением необходима бессрочная лицензия.

Для ввода лицензии необходимо перейти в раздел **Лицензии (Меню — О приложении — лицензия КриптоПро TSP — Ввести лицензию)**. Вставить ключ активации лицензии на КриптоПро TSP и нажать **Далее**.

### 8.4. Установка лицензии на КриптоПро OCSP Client

Для создания усовершенствованной подписи необходима установка лицензионного ключа на модули TSP и OCSP. При первой установке приложения единожды активируется пробная лицензия на КриптоПро OCSP сроком на 90 дней. По истечении пробного периода для дальнейшей работы с приложением необходимо приобрести бессрочная лицензия.

Для ввода лицензии необходимо перейти в раздел **Лицензии (Меню — О приложении — лицензия КриптоПро OCSP — Ввести лицензию)**. Вставить ключ активации лицензии на КриптоПро OCSP и нажать **Далее**.



## 8.5. Дополнительно

Для проверки наличия у сертификата использования ключа атрибута keyAgreement (Согласование ключей) в расширении keyUsage необходимо в разделе **Дополнительно** в меню **О приложении** установить **Проверять Флаг keyAgreement для сертификата ключа получателя**.

Если в сертификате отсутствует атрибут 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 сертификата, имеющего атрибут keyEncryption, без проверки наличия атрибута использования ключа Согласование ключей.

**ВАЖНО!** Шифрование без установленного флага **Проверять флаг keyAgreement для сертификата ключа получателя** возможно только в тестовых целях.