Цифровые технологии

КриптоАРМ Mobile · Android

Документация продукта

Релиз v1.2

Исходная документация на Trusted.ru

Редакция от 24.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Общие сведения

О продукте ... 4

Функциональность ... 6

Лицензирование ... 10

Начало работы

Установка и первый запуск ... 12

Проверка рабочего места ... 17

Установка лицензий ... 23

Настройки

Личные сертификаты и запросы

Установка личного сертификата ... 27

Создание самоподписанного сертификата ... 36

Создание запроса ... 41

Просмотр и проверка статуса сертификата ... 50

Экспорт личного сертификата ... 54

Удаление сертификата ... 58

Сертификаты удостоверяющих центров и списки отзыва

Установка корневого и промежуточного сертификатов ... 61

Установка списка отзыва ... 65

Сертификаты других пользователей

Установка сертификатов других пользователей ... 69

Экспорт и удаление сертификата другого пользователя ... 72

Профили подписи

Управление профилями ... 75

Настройка профиля ... 85

Прочие настройки

Настройка интерфейса ... 100

Общие настройки ... 102

Подпись и шифрование

Обзор операций ... 106

Групповая подпись ... 111

Подпись PDF ... 120

Добавление соподписи ... 134

Шифрование ... 140

Проверка и расшифрование

Проверка подписи ... 147

Снятие подписи ... 156

Расшифрование ... 161

Архив

Действия с документами ... 166

Группировка документов ... 172

Работа с облачными папками ... 178

Контакты

Создание контакта ... 183

Действия с контактами ... 193

Управление сертификатами контакта ... 207

Группы контактов ... 215

Импорт и экспорт контактов ... 223

Мои контакты ... 231

Поиск

Глобальный поиск ... 234

Журнал

Журнал событий ... 238

FAQ

Часто задаваемые вопросы ... 245

Глоссарий ... 247

Дополнительные статьи

Product overview ... 251

Открыть статью на сайте

О приложении КриптоАРМ Подпись и шифрование

КриптоАРМ Подпись и шифрование — приложение для электронной подписи и шифрования на мобильных устройствах.

КриптоАРМ Подпись и шифрование может использоваться для безопасного хранения и передачи электронных документов в системах корпоративной защищенной мобильности. Поддерживает алгоритмы ГОСТ Р 34.10-2012 (ГОСТ 34.10-2018), ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018).

Основные возможности

1. **Электронная подпись**:
    - Создание присоединенной и отсоединенной электронной подписи
    - Создание подписи со штампом времени на подпись и подписываемые данные
    - Создание усовершенствованной подписи
    - Добавление соподписи
    - Подпись сертификатом DSS
2. **Шифрование и расшифрование**:
    - Шифрование и расшифрование файлов
    - Шифрование по стандарту PKCS#7 и CMS
    - Удаление исходных файлов после шифрования
    - Расшифрование сертификатом DSS
3. **Управление контактами**:
    - Создание контактов
    - Добавление сертификата к контакту
    - Шифрование документов в адрес контактов
4. **Управление сертификатами и ключами**:
    - Отображение сертификатов и привязанных к ним закрытых ключей
    - Создание запросов на сертификат
    - Импорт и экспорт сертификатов

Совместимость

Поддерживаемые криптопровайдеры

В приложении осуществляется поддержка криптопровайдера КриптоПро CSP версии 5.0 и выше.

> ⚠️ Криптопровайдер КриптоПро CSP является частью приложения КриптоАРМ и устанавливается одновременно с ним. Никаких дополнительных действий для установки КриптоПро CSP не требуется.

Поддерживаемые ключевые носители

Поддерживаются ключевые носители Рутокен (поддерживаемые форм-факторы указаны в формуляре на Рутокен ЭЦП 3.0), JaCarta, eSMART.

Ознакомиться со списком поддерживаемых ключевых носителей можно в формуляре криптопровайдера КриптоПро CSP или на сайте компании КриптоПро.

Системные требования

- Операционная система Android 10 и выше;
- Оперативная память 4Гб и выше;
- Встроенная память 32ГБ и выше;
- Диагональ экрана 5,5 дюйма и выше;
- Поддержка 3G, 4G, LTE рекомендуется;
- Фото-камера 8МП и выше;
- Наличие функции USB-host.

Инструкции по теме

- Функциональность КриптоАРМ Подпись и шифрование
- Лицензирование КриптоАРМ Подпись и шифрование

Открыть статью на сайте

Функциональность КриптоАРМ Подпись и шифрование

Возможности	Описание
Электронная подпись	Электронная подпись произвольных файлов размером до 50 МБ. Размер файла не может превышать объем свободной оперативной памяти устройства.
	Создание присоединенной и отсоединенной электронной подписи
	Поддержка стандартов электронной подписи ГОСТ Р 34.10-2012 и ГОСТ Р 34.12-2015
	Создание подписи с меткой доверенного времени CAdES-T
	Создание усовершенствованной электронной подписи CAdES-X Long Type 1
	Создание электронных подписей в форматах CAdES и PAdES
	Групповое подписание нескольких документов за одну операцию
	Соподписание ранее подписанных документов
	Снятие электронной подписи с документа
	Добавление машиночитаемой доверенности (МЧД) к подписываемым документам
Подпись PDF-документов	Создание электронной подписи PDF-документов по стандарту PAdES
	Добавление визуального штампа электронной подписи в PDF-документ
	Настройка внешнего вида и расположения визуального штампа
	Добавление изображения рукописной подписи в PDF-документ
	Создание рукописной подписи непосредственно в приложении

Возможности	Описание
	Добавление рукописной подписи без создания электронной подписи
	Создание печатной формы PDF-документа с визуальным отображением подписи
Проверка электронной подписи	Проверка электронной подписи файлов размером до 50 МБ. Размер файла не может превышать объем свободной оперативной памяти устройства.
	Проверка электронных подписей в форматах CAdES и PAdES
	Групповая проверка электронных подписей нескольких документов за одну операцию
	Проверка присоединенных и отсоединенных электронных подписей
	Проверка соподписей
	Просмотр результатов проверки электронной подписи
	Просмотр визуального штампа электронной подписи в PDF-документе
Шифрование и расшифрование	Шифрование и расшифрование файлов размером до 50 МБ. Размер файла не может превышать объем свободной оперативной памяти устройства.
	Шифрование по стандартам PKCS#7 и CMS
	Поддержка алгоритмов ГОСТ Р 34.12-2015 (Магма, Кузнечик) и ГОСТ 28147-89
Управление сертификатами и ключами	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 (Актив) при условии использования криптопровайдера КриптоПро CSP
	Создание запросов на сертификат
	Создание самоподписанного сертификата
	Импорт сертификатов с привязкой к закрытому ключу

Возможности	Описание
	Экспорт сертификатов
	Удаление сертификатов
	Импорт сертификатов с помощью QR-кода
Контакты	Создание контактов с сертификатами из хранилища «Личные сертификаты» и из файла
	Создание контактов на основе сертификатов
	Создание групп контактов
	Экспорт и импорт контактов в формате vCard
	Создание личного контакта с личными сертификатами
Работа с облачными документами	Подключение к внешним информационным системам с помощью сетевых профилей
	Просмотр документов в облачных папках «Входящие», «Исходящие» и пользовательских папках
	Просмотр документов, направленных пользователю на подпись
	Подписание входящих документов с автоматической выгрузкой электронной подписи в информационную систему
	Просмотр списка подписантов документов
	Отслеживание статусов подписания документов
	Синхронизация содержимого облачных папок с внешней информационной системой
Работа с файлами в каталоге «Архив»	Сохранение результатов операций с файлами в разделе «Архив»
	Просмотр PDF-документов во встроенном просмотрщике приложения
	Открытие файлов во внешних приложениях, установленных на устройстве
	Архивирование документов в ZIP-формат
Настройка профилей	Создание и настройка локального профиля подписи

Возможности	Описание
	Создание сетевого профиля для подключения к внешней информационной системе
	Настройка последовательности операций: подпись, архивирование и шифрование
	Настройка параметров электронной подписи и шифрования
	Настройка параметров подписи PDF-документов
	Настройка сохранения результатов обработки документов
Работа с журналом событий и уведомлениями	Отображение списка событий по уровням детализации
	Просмотр уведомлений о событиях
Поддержка тем	Поддержка и переключение тем оформления
Проверка рабочего места	Проверка готовности приложения к работе
Проверка контроля целостности приложения	Контроль целостности приложения для обеспечения безопасности данных и предотвращения несанкционированного доступа к информации
Проверка флага KeyAgreement	Контроль соответствия сертификатов требованиям к использованию ключей для согласования общего ключа

Инструкции по теме

- О приложении КриптоАРМ Подпись и шифрование
- Лицензирование КриптоАРМ Подпись и шифрование

Открыть статью на сайте

Лицензирование КриптоАРМ Подпись и шифрование

- Общая информация о лицензиях
- Пробная лицензия
- Лицензия на рабочее место
- Лицензия пользователя информационной системы
- Инструкции по теме

Общая информация о лицензиях

Для выполнения криптографических операций с алгоритмами ГОСТ требуется лицензия.

Доступны следующие варианты лицензии:

- **Пробная лицензия**
- **Лицензия на рабочее место**
- **Лицензия пользователя информационной системы**

Пробная лицензия

При первом запуске **КриптоАРМ Подпись и шифрование** автоматически активируется **30-дневная пробная лицензия**, которая позволяет ознакомиться со всеми функциями продукта и протестировать работу криптографических операций с алгоритмами ГОСТ.

Если для знакомства со всеми возможностями **КриптоАРМ Подпись и шифрование** недостаточно ознакомительного периода, вы можете получить дополнительную лицензию, написав в техническую поддержку support@trusted.ru.

Лицензия на рабочее место

Локальная лицензия устанавливается на конкретное рабочее место (устройство) и используется для выполнения операций непосредственно в приложении.

Особенности:

- Привязана к устройству пользователя.
- Требует ввода лицензионного ключа.
- Работает независимо от внешних сервисов.
- Может быть **годовой** и **бессрочной**.

Приобрести лицензии можно в официальном интернет-магазине cryptoarm.ru.

Лицензия пользователя информационной системы

Лицензия пользователя информационной системы предназначена для работы с **КриптоАРМ Подпись и шифрование**, который интегрирован с внешней системой через API.

Такая лицензия предоставляется пользователю через сетевой профиль и не требует установки на конкретное устройство.

Особенности:

- Лицензия привязана не к устройству, а к пользователю внутри вашей ИС.
- Не зависит от рабочего места.
- Может использоваться на разных устройствах (ПК, ноутбук, мобильное устройство) — без привязки к рабочему месту.
- Может быть **стандартной** и **расширенной**.

Расширенная лицензия

Расширенная версия предназначена для организации полноценного юридически значимого электронного документооборота с внешними контрагентами.

Как работает расширенная лицензия:

Владелец расширенной лицензии выбирает получателя документа, запрашивает подпись с его стороны и вместе со ссылкой на документ передает получателю лицензию на выполнение операции. Получатель может подписать документ в **КриптоАРМ Подпись и шифрование**, даже если у него нет собственной установленной лицензии.

Приобрести лицензии можно в официальном интернет-магазине cryptoarm.ru.

Инструкции по теме

- Установка и первый запуск
- Проверка рабочего места

Открыть статью на сайте

Как установить КриптоАРМ Подпись и шифрование

- Где скачать КриптоАРМ
- Первый запуск
- Режим усиленного контроля использования ключей КриптоПро CSP
- Инструкции по теме

Где скачать КриптоАРМ

Загрузить и установить приложение **КриптоАРМ Подпись и шифрование** можно из официального магазина приложений **RuStore**.

→ 📲 Перейти к приложению в RuStore

> 💡 Криптопровайдер **КриптоПро CSP** входит в состав приложения **КриптоАРМ** и устанавливается вместе с ним. Отдельная установка не требуется.

Установка

1. Откройте магазин **RuStore** на вашем устройстве.
2. Найдите приложение **КриптоАРМ Подпись и шифрование** через поиск или перейдите по ссылке выше.
3. Нажмите **Установить**.

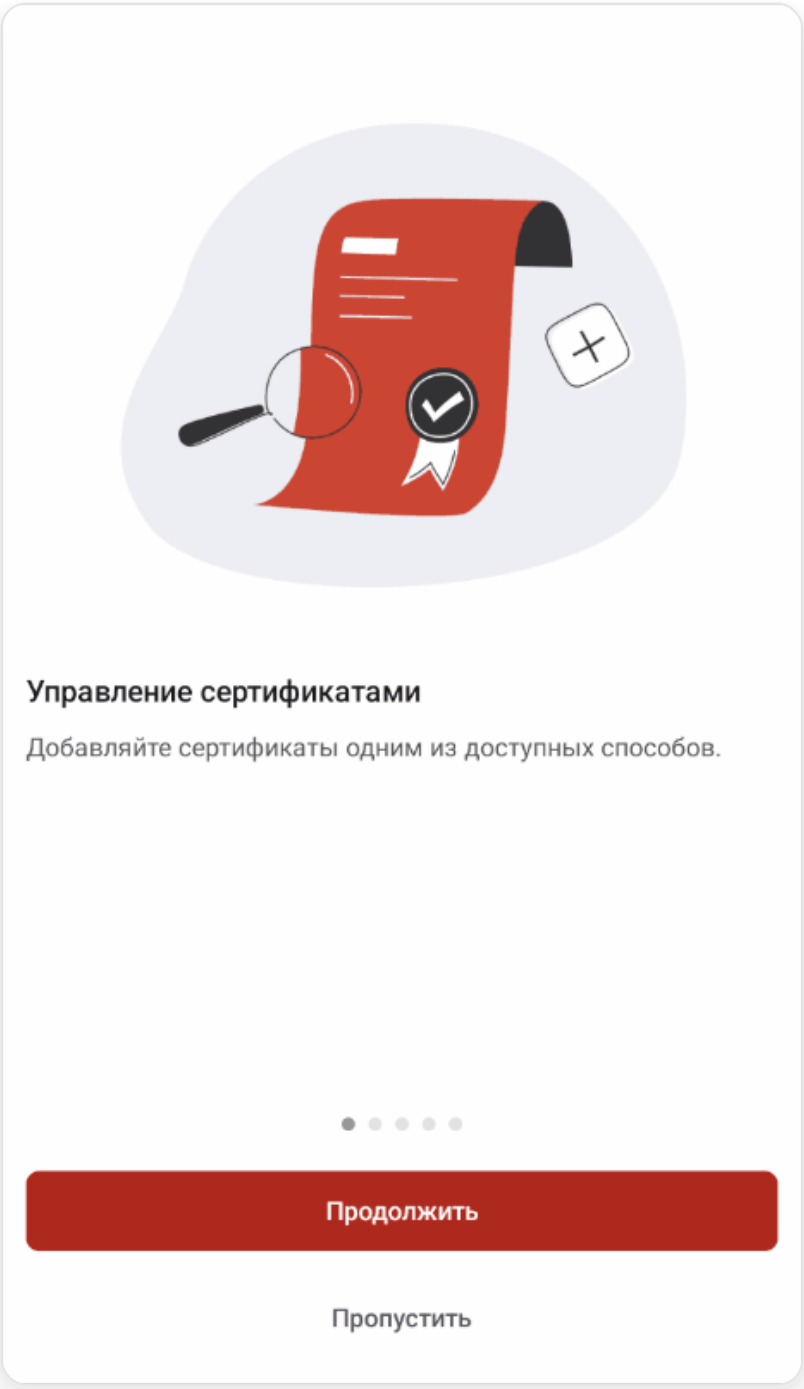
Обновление

Все обновления устанавливаются автоматически через **RuStore**, как и для других приложений. Вы можете проверить наличие новой версии вручную в разделе **Мои приложения**.

Первый запуск

При первом запуске отображается онбординг, в котором можно ознакомиться с основными возможностями приложения.

На этом этапе вы также можете настроить режим усиленного контроля использования ключей **КриптоПро CSP**.


Управление сертификатами
Добавляйте сертификаты одним из доступных способов.
Продолжить
Пропустить

Режим усиленного контроля использования ключей КриптоПро CSP

Что это такое?

Режим усиленного контроля использования ключей обеспечивает:

- контроль срока действия долговременных ключей электронной подписи и ключевого обмена;
- контроль доверенности ключей проверки электронной подписи;
- контроль корректного использования программного датчика случайных чисел.

Как включить режим

1. Нажмите **Продолжить** на последнем шаге онбординга.
2. Нажимайте на экран, пока не завершится генерация ключа.
3. Укажите пароль на контейнер. Поле можно оставить пустым.



💡 После настройки режима рекомендуется выполнить Проверку рабочего места.

Инструкции по теме

- Проверка рабочего места
- Как установить лицензионный ключ КриптоАРМ
- Как установить лицензионный ключ КриптоПро CSP

- Как изменить тему приложения

Открыть статью на сайте

Как проверить рабочее место в КриптоАРМ Подпись и шифрование

- Зачем нужна проверка
- Как запустить проверку
- Результаты проверки
- Что проверяет система
- Системный отчет
- Инструкции по теме

Зачем нужна проверка

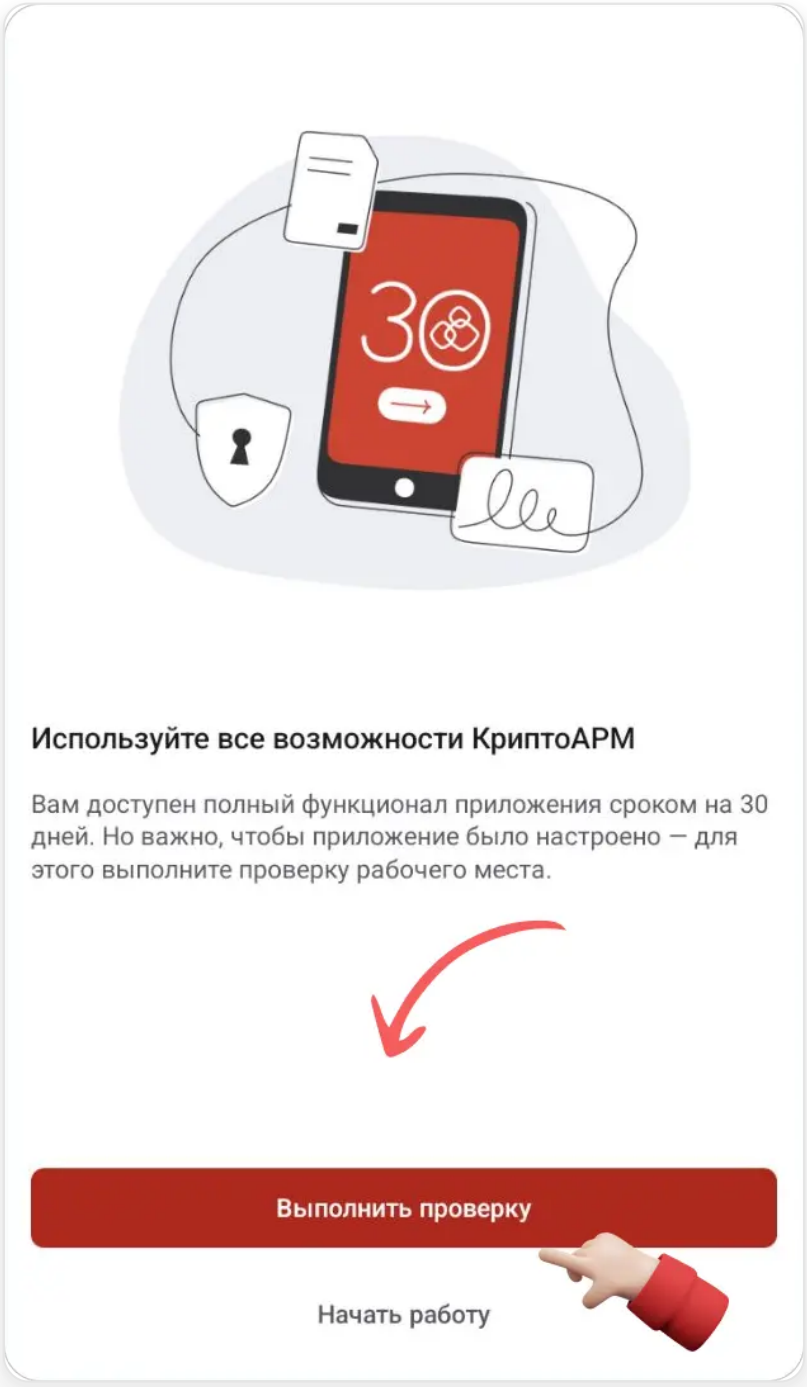
Проверка рабочего места — это инструмент, который помогает убедиться, что все компоненты для работы с электронной подписью установлены и готовы к использованию.

Если что-то не настроено, приложение подскажет, какие действия нужно выполнить.

Как запустить проверку

Автоматически при первом запуске

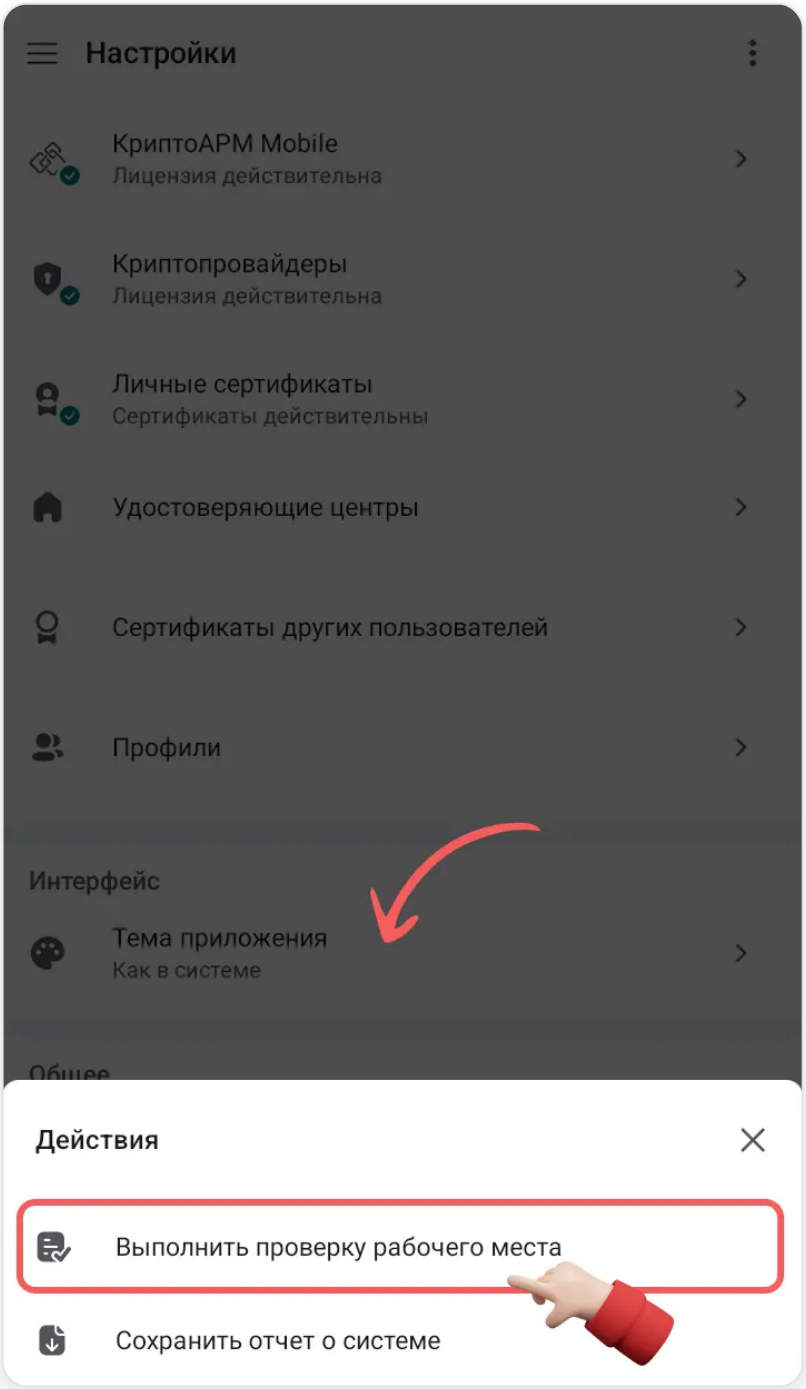
После онбординга приложение предложит пройти проверку рабочего места. Чтобы перейти к проверке, выберите действие **Выполнить проверку** на последнем экране онбординга.



Ручной запуск

В дальнейшем проверку можно запустить самостоятельно:

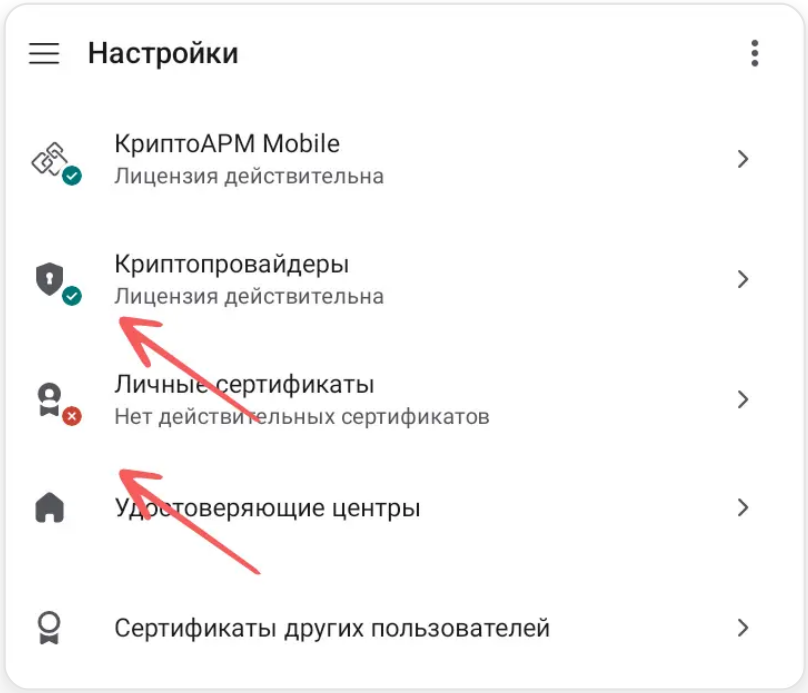
1. Перейдите в раздел **Настройки**.
2. Нажмите кнопку **Еще** и выберите пункт **Действия**.
3. Выберите **Выполнить проверку рабочего места**.



Результаты проверки

Результаты проверки отображаются в виде индикатора с пояснением:

- ✅ Зеленый — компонент готов к работе
- ❌ Красный — требуются действия пользователя



Что проверяет система

Во время проверки приложение оценивает ключевые параметры, необходимые для подписания файлов:

1. Наличие и актуальность лицензий **КриптоАРМ** и **КриптоПро CSP**. Подробнее о лицензировании читайте в инструкции.
2. Наличие действующих личных сертификатов.

Системный отчет

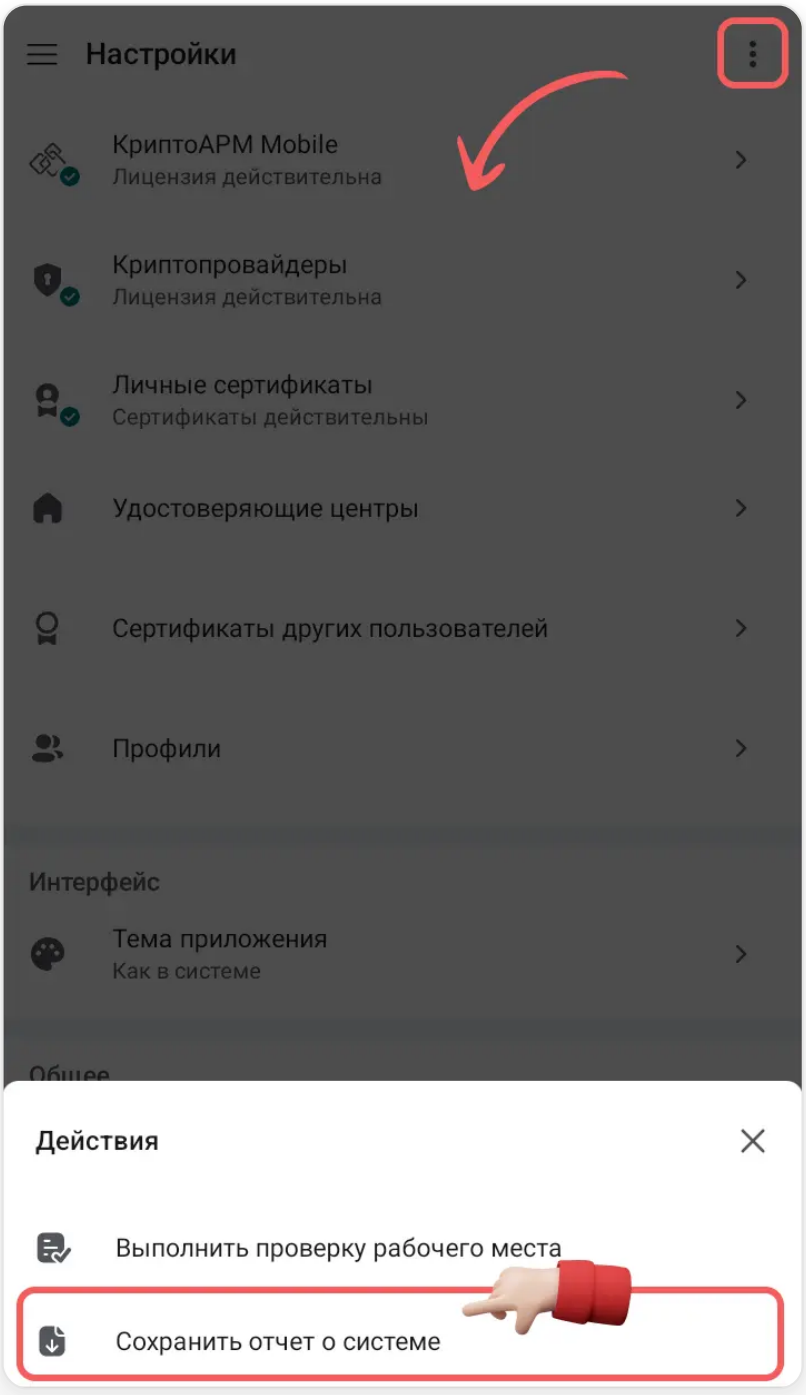
При необходимости можно сохранить подробный системный отчет.

Отчет выгружается в файл `system-info.txt` со следующей информацией:

- данные об устройстве и ОС (модель, версия),
- информация о лицензии и версии КриптоАРМ,
- информация о лицензии и версии КриптоПро CSP,
- количество действующих личных сертификатов,
- количество сертификатов в хранилище «Удостоверяющие центры»,
- количество сертификатов в хранилище «Другие пользователи»,
- общее количество контактов.

Как сохранить отчет

1. Перейдите в раздел **Настройки**.
2. Нажмите кнопку **Еще** и выберите пункт **Действия**.
3. Выберите **Сохранить отчет о системе**.



4. Укажите место для сохранения файла или выберите приложение для его отправки.

Инструкции по теме

- Как установить лицензионный ключ КриптоАРМ
- Как установить лицензионный ключ КриптоПро CSP
- Как установить личный сертификат
- Как импортировать корневой или промежуточный сертификат

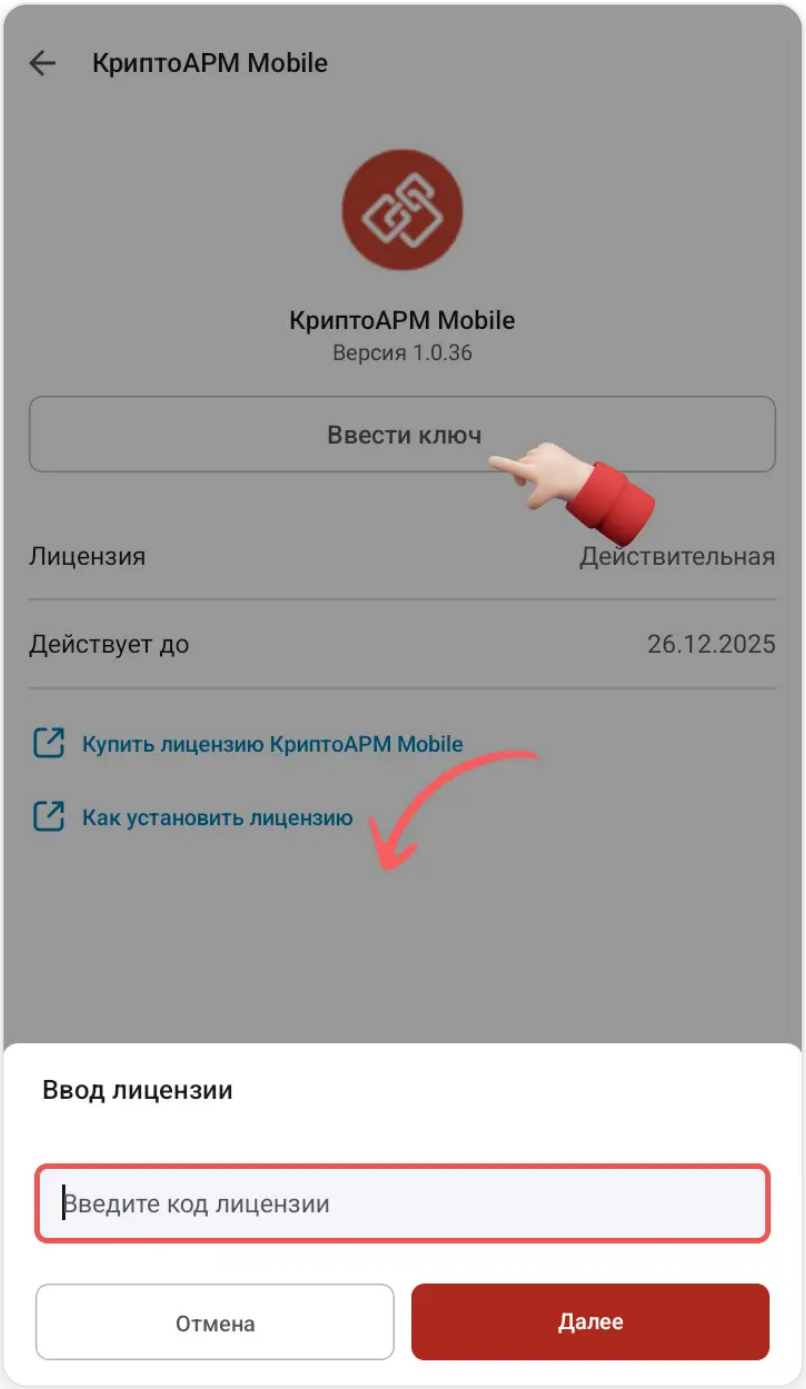
Открыть статью на сайте

Как установить лицензионный ключ в КриптоАРМ Подпись и шифрование

- Установка лицензионного ключа КриптоАРМ
- Установка лицензионного ключа КриптоПро CSP
- Инструкции по теме

Установка лицензионного ключа КриптоАРМ

1. Перейдите в раздел **Настройки**.
2. В блоке **Проверка рабочего места** выберите **КриптоАРМ**.
3. В открывшемся окне нажмите кнопку **Ввести ключ**.
4. Введите лицензионный ключ и нажмите **Далее**.



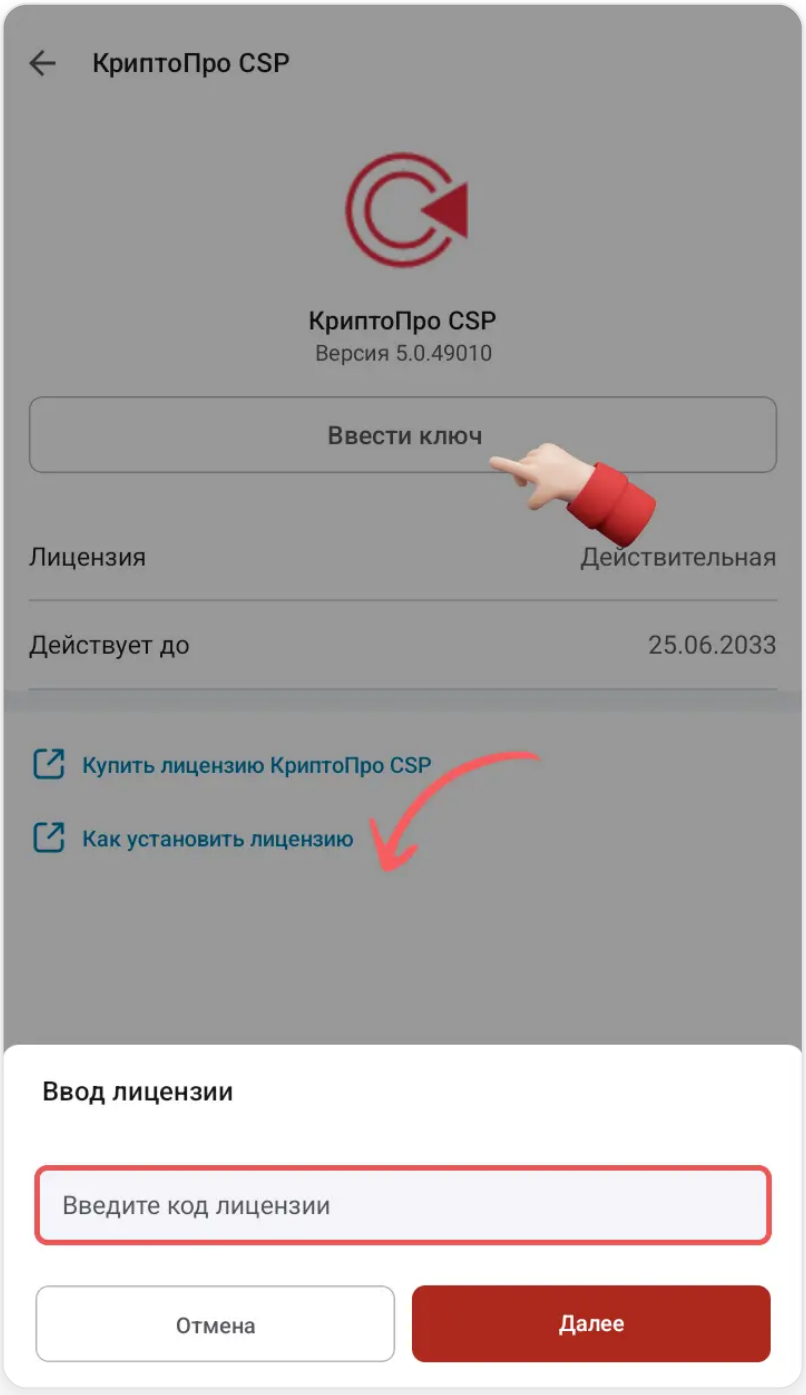
Дождитесь окончания активации лицензии.

После успешной активации лицензии обновится информация о статусе лицензии и сроке ее действия.

Установка лицензионного ключа КриптоПро CSP

1. Перейдите в раздел **Настройки**.
2. В блоке **Проверка рабочего места** выберите **Криптопровайдеры**.

3. В открывшемся окне нажмите на кнопку **Ввести ключ**.
4. Введите лицензионный ключ и нажмите **Далее**.



Дождитесь окончания активации лицензии.

При успешной активации лицензии обновится информация о статусе лицензии и сроке ее действия.

Инструкции по теме

- Лицензирование
- Проверка рабочего места
- Как изменить тему приложения

Открыть статью на сайте

Как установить личный сертификат в КриптоАРМ Подпись и шифрование

- Перед началом работы
- Установка с защищенного носителя Рутокен
- Установка сертификата из файла .pfx
- Установка сертификата с помощью QR-кода
- Возможные ошибки
- Инструкции по теме

Перед началом работы

Перед импортом личного сертификата убедитесь, что:

- установлены корневые сертификаты удостоверяющего центра, который выдал этот сертификат,
- загружен актуальный список отозванных сертификатов (CRL).

> 🔍 Подробнее в инструкциях:
> - Установка корневого и промежуточного сертификатов,
> - Установка списка отзыва.

Установка с защищенного носителя Рутокен

Поддерживаемые устройства

В приложении поддерживается работа с ключевыми носителями через криптопровайдер КриптоПро CSP:

- Рутокен ЭЦП 2.0 (USB/Type-C),
- Рутокен ЭЦП 3.0 (USB/Type-C),
- Смарт-карта Рутокен ЭЦП 3.0 NFC.

> ⚠️ В предыдущих версиях **КриптоАРМ** требовалось установить приложение «Панель управления Рутокен», теперь токены работают без него.

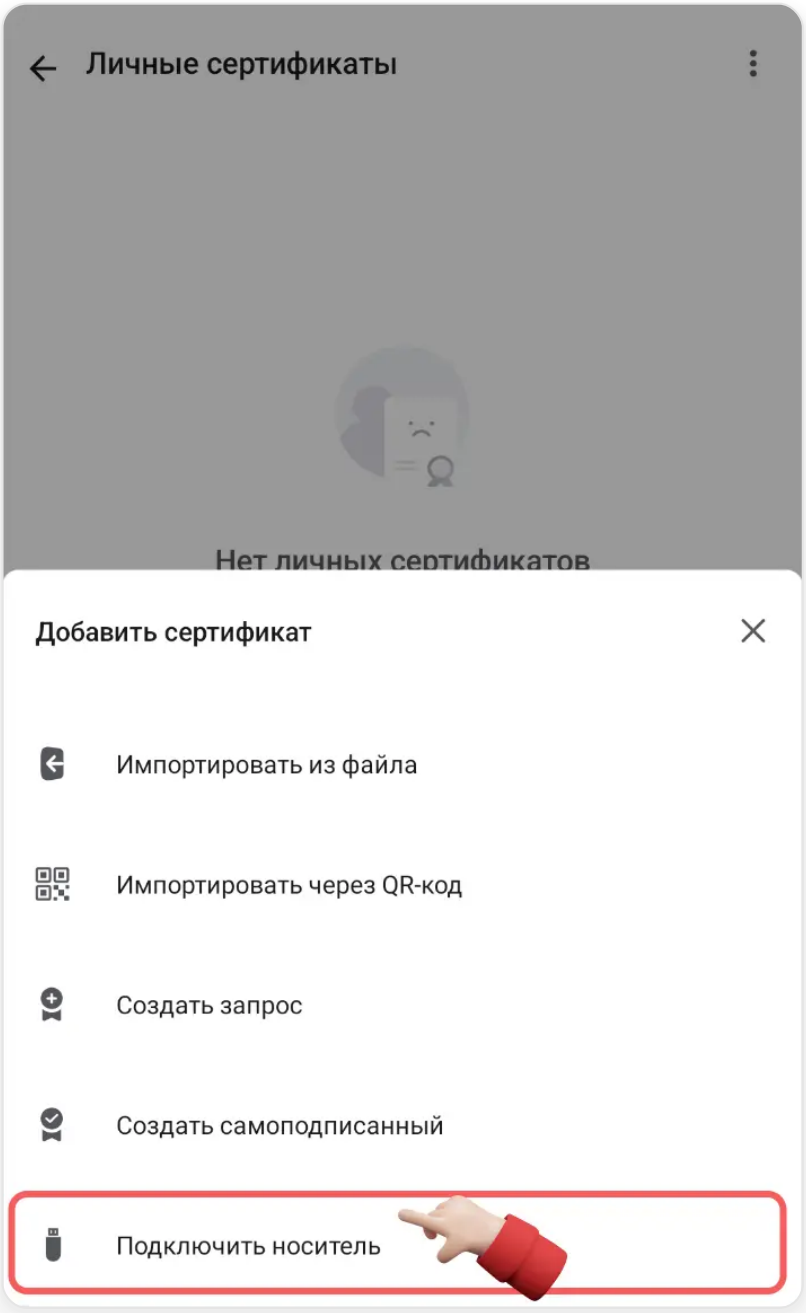
Требования к устройству

- Устройство должно поддерживать функцию **USB-OTG** для работы с USB-токенами.
- На некоторых моделях (Tecno, OPPO) OTG нужно включить в настройках. Подробнее — на Портале документации Рутокен.

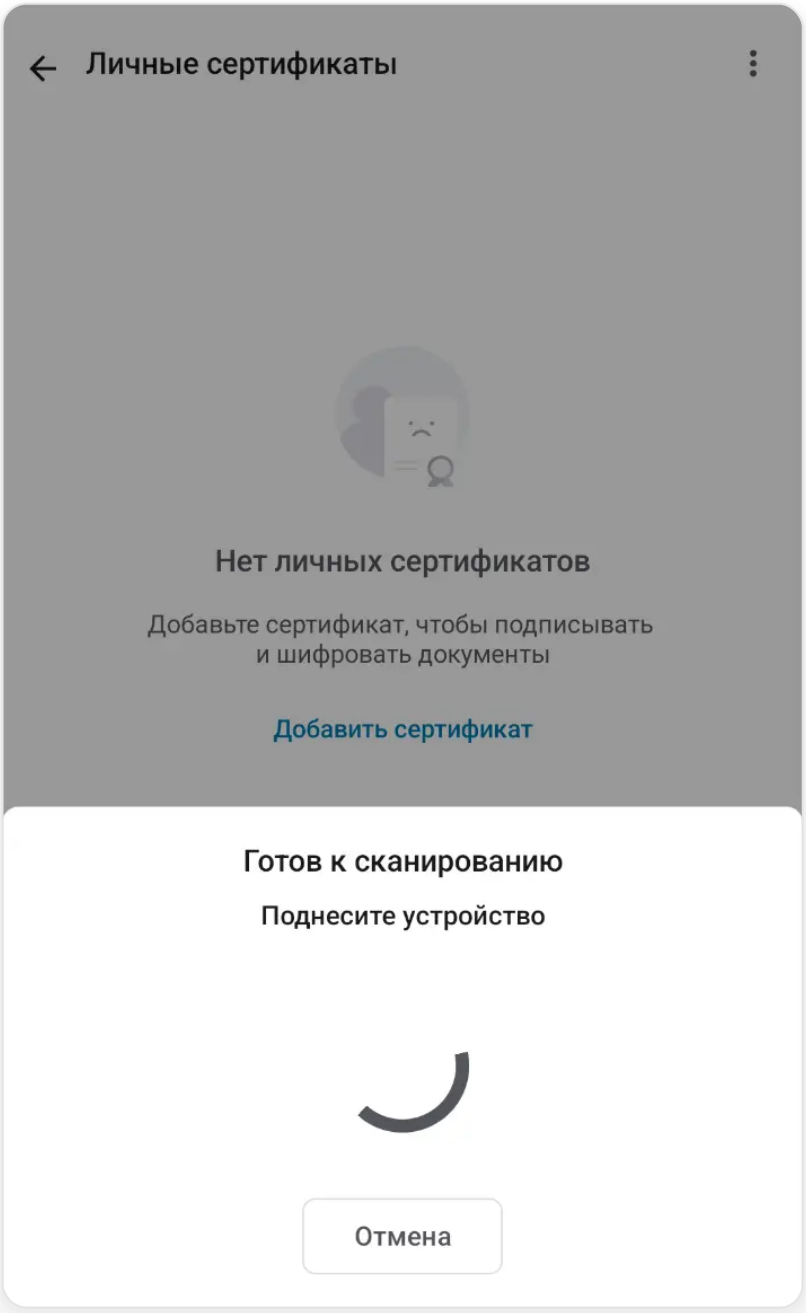
> 📌 **OTG** – это технология, связывающая два устройства без дополнительного USB-хоста, благодаря ей телефон может считывать данные со съемного носителя и передавать данные на другое устройство.

Как подключить носитель

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий **Добавить сертификат** одним из способов:
   - Нажмите на кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
   - Вызовите меню по кнопке **Еще** ⋮ и выберите действие **Добавить сертификат**.
3. В появившемся меню выберите действие **Подключить носитель**.



4. Запустится процесс сканирования.

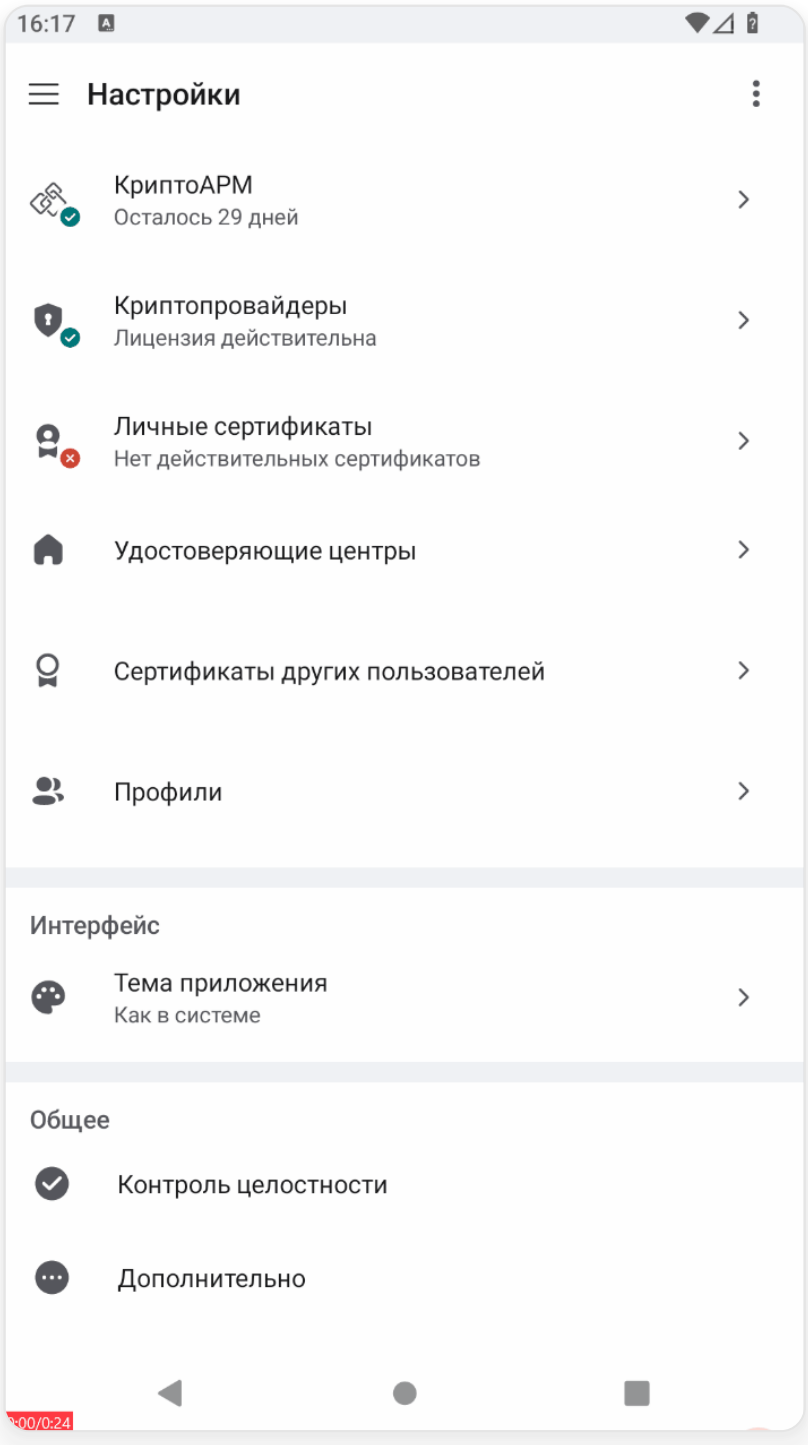


5. Подключите или поднесите носитель к устройству.
    - **Type-C** → вставьте напрямую,
    - **USB** → используйте переходник Type-C–USB,
    - **NFC-карта** → включите NFC и поднесите карту.
6. Откроется окно с обнаруженными сертификатами.
7. Выберите нужный сертификат из списка.
8. Нажмите **Установить**.

Установка сертификата из файла .pfx

> 💡 Перед установкой убедитесь, что файл `.pfx` сохранен на устройстве.

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий **Добавить сертификат** одним из способов:
   - Нажмите на кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
   - Вызовите меню по кнопке **Еще** и выберите действие **Добавить сертификат**.
3. Выберите действие **Импортировать из файла**.
4. Укажите путь к файлу с сертификатом `.pfx`.
5. Введите пароль для pfx-контейнера, если он задан.
6. При необходимости задайте новый пароль к ключевому контейнеру.



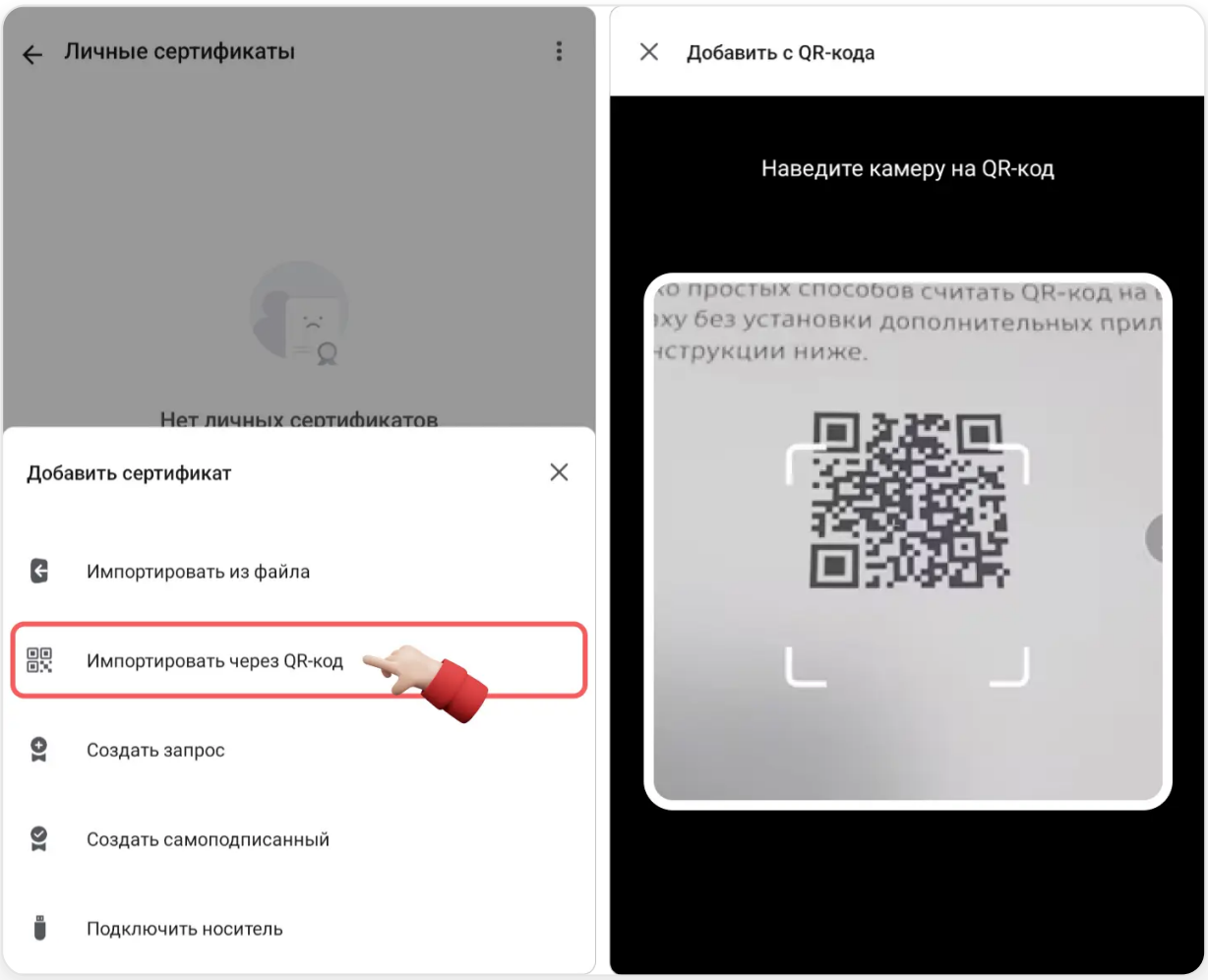
После успешного импорта сертификат отобразится в списке и появится сообщение **Сертификат успешно добавлен**.

Установка сертификата с помощью QR-кода

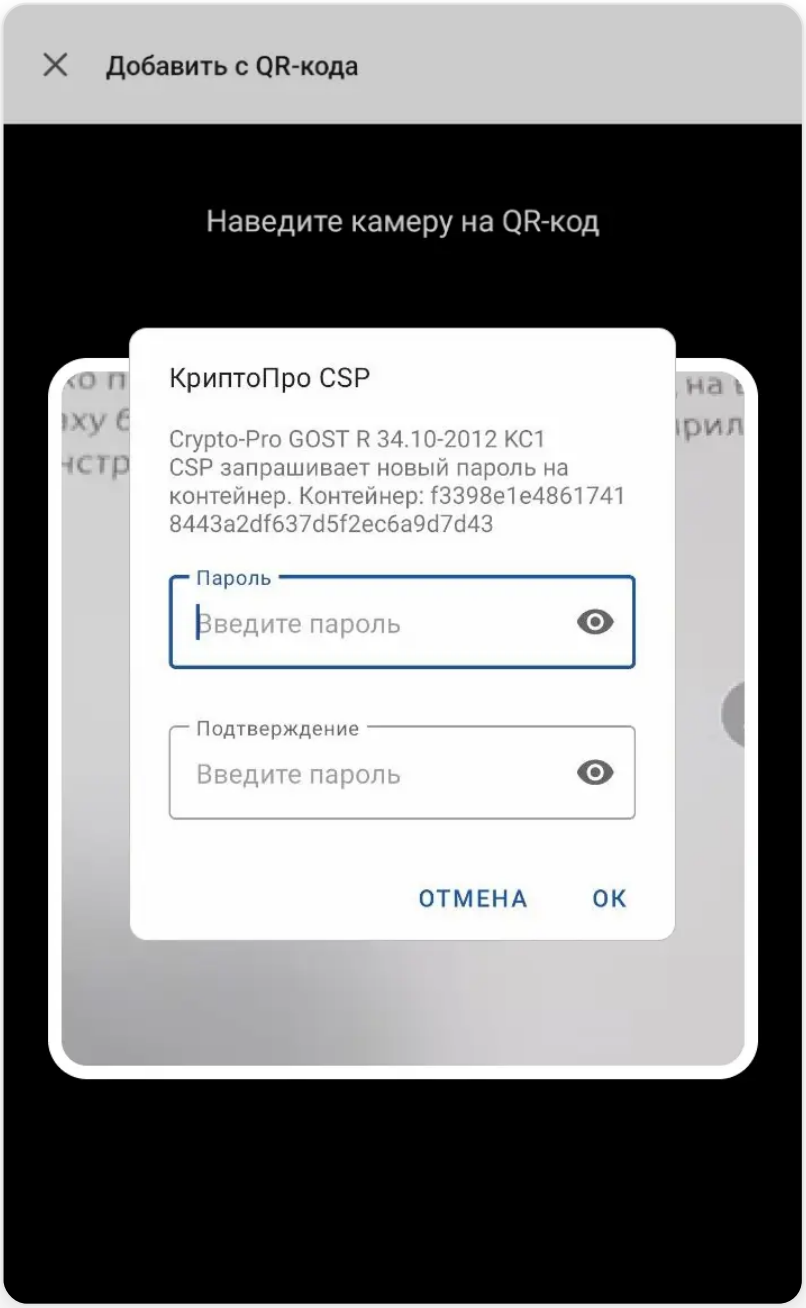
> 💡 Как создать QR-код с помощью КриптоПро CSP, смотрите в нашей видеоинструкции.

> 🚨 **Условие**: Сертификат должен допускать экспорт закрытого ключа, иначе ключ не получится перенести.

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий **Добавить сертификат** одним из способов:
   - Нажмите на кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
   - Вызовите меню по кнопке **Еще** ⋮ и выберите действие **Добавить сертификат**.
3. Выберите действие **Импортировать через QR-код**.
4. При необходимости предоставьте приложению разрешение на съемку фото и видео.
5. Отсканируйте QR-код.



6. Введите пароль для PFX-контейнера, если он задан.
7. При необходимости задайте новый пароль к ключевому контейнеру.



После успешного импорта сертификат отобразится в списке.

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана.

Для просмотра подробной информации нажмите **Просмотреть события** в меню **Действия**.

> 📚 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Описание	Рекомендуемые действия
Превышено максимальное число попыток ввода пароля	Блокировка после нескольких неудачных попыток ввода пароля	Проверьте правильность ввода (учитывайте регистр)
Ошибка при импорте сертификата	Файл с сертификатом поврежден или содержит несовместимые параметры	1. Скачайте файл заново 2. Проверьте целостность файла 3. Попробуйте импортировать на другом устройстве 4. Экспортируйте сертификат заново
Ошибка при импорте сертификата	Сертификат уже существует в хранилище	Проверьте хранилище на наличие сертификата
Неверное расширение файла	Файл не содержит сертификат	1. Убедитесь, что файл содержит сертификат 2. Проверьте, что файл экспортирован корректно 3. Импортируйте сертификат заново
Сертификат будет помещен в хранилище «Другие пользователи» или «УЦ»	Закрытый ключ не найден	1. Экспортируйте сертификат с включенной опцией «Экспортировать закрытый ключ» 2. Импортируйте сертификат заново

Инструкции по теме

- Как создать запрос на сертификат
- Как создать самоподписанный сертификат
- Как импортировать корневой или промежуточный сертификат

Открыть статью на сайте

Как создать самоподписанный сертификат в КриптоАРМ Подпись и шифрование

- Что такое самоподписанный сертификат?
- Как создать самоподписанный сертификат
- Инструкции по теме

Что такое самоподписанный сертификат?

Самоподписанный сертификат — это сертификат электронной подписи, созданный пользователем самостоятельно без обращения в Удостоверяющий центр.

Особенности

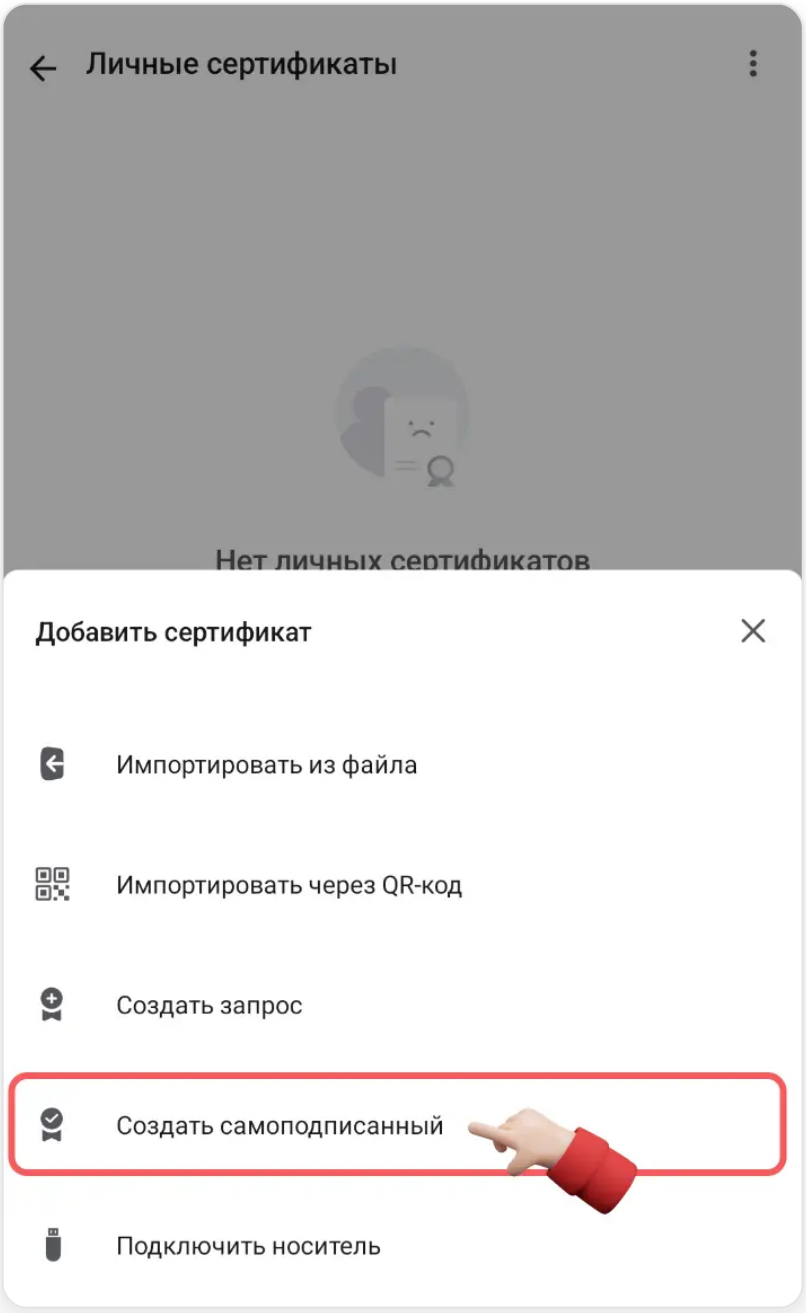
- Совмещает функции личного сертификата и корневого сертификата.
- Подходит только для личного или внутреннего использования, например, для тестирования или обмена документами внутри доверенной группы.

❌ Не подходит для официального документооборота:

- **Нет независимой проверки** — сертификат создан вами, и сторонние организации не могут проверить его подлинность.
- **Не обеспечивает юридическую значимость в официальном документообороте** — государственные порталы, банки и официальные системы требуют сертификаты, выданные доверенными Удостоверяющими центрами.
- **Риск подделки** — любой может создать сертификат с вашим именем, поэтому внешние системы не могут доверять такой подписи автоматически.

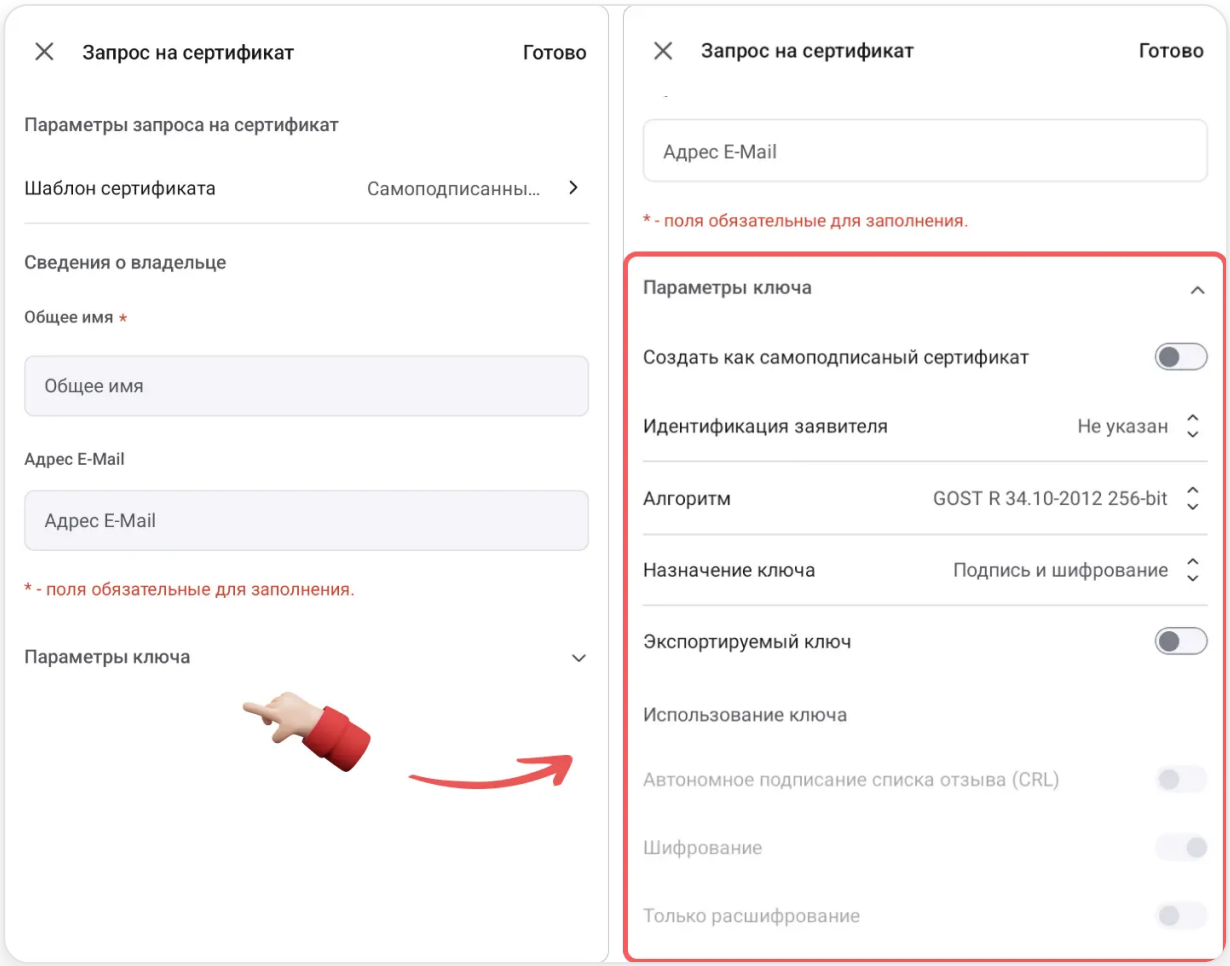
Как создать самоподписанный сертификат

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий **Добавить сертификат** одним из способов:
    - Нажмите кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
    - Выберите **Добавить сертификат** в меню действий.
3. Выберите **Создать самоподписанный**.



4. Откроется окно **Запрос на сертификат**.

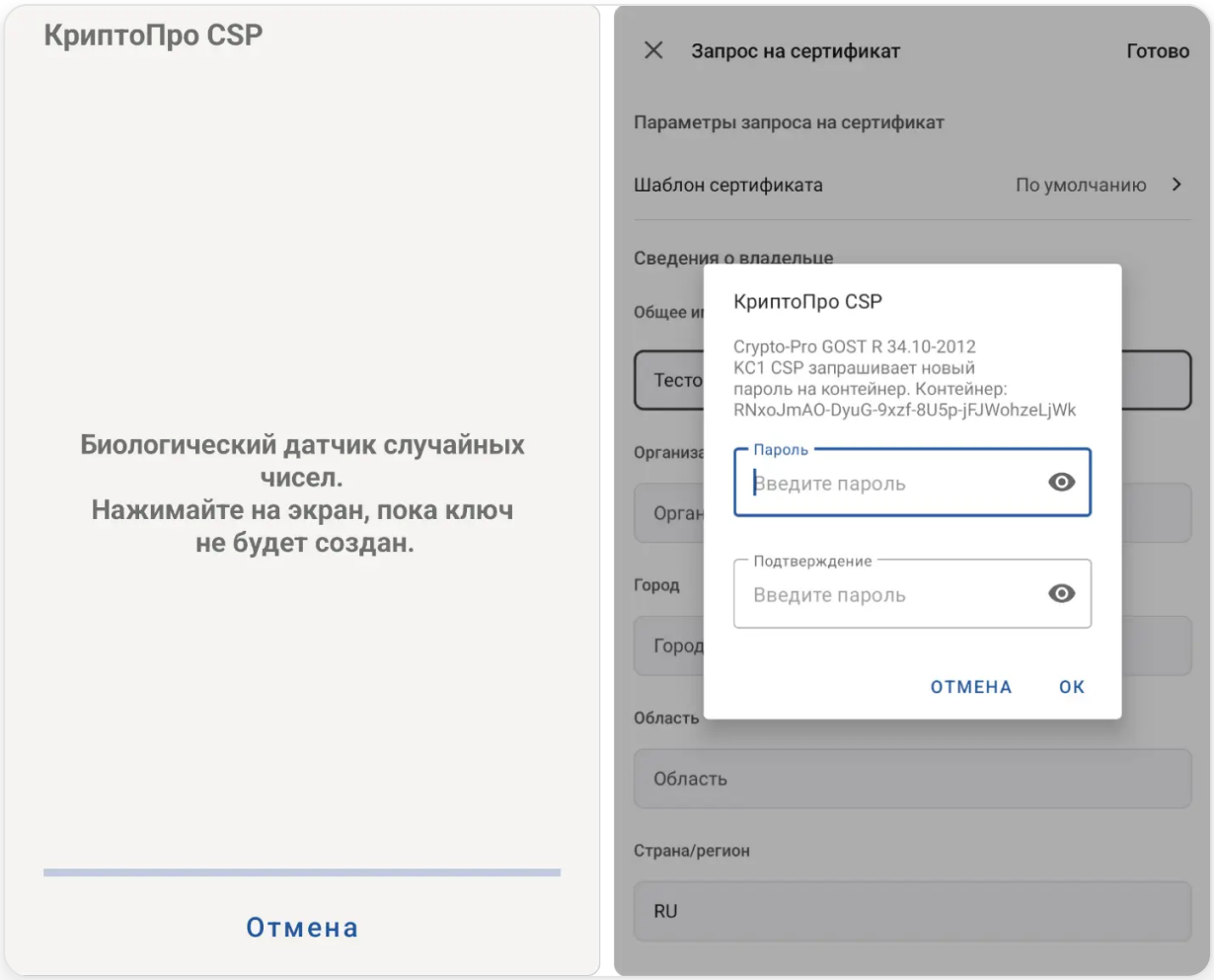
   - Заполните обязательные поля в блоке **Сведения о владельце**.
   - При необходимости внесите изменения в блок **Параметры ключа**.
   - Нажмите **Готово**.



5. Откроется окно КриптоПро CSP с датчиком случайных чисел.

6. Нажимайте на экран, пока не завершится генерация ключа.

7. Укажите пароль для контейнера. Поле ввода пароля можно оставить пустым.



После этого сертификат будет создан и установлен в хранилище **Личные сертификаты**.

> ⚠️ **Важно:** чтобы приложение корректно определяло статус самоподписанного сертификата, необходимо выполнить дополнительный шаг:

1. Экспортировать сертификат без закрытого ключа.
2. Импортировать его в хранилище «Удостоверяющие центры».

> 🔍 Как экспортировать сертификат без закрытого ключа
> 🔍 Как импортировать сертификат в «Удостоверяющие центры»

Инструкции по теме

- Как установить личный сертификат
- Как создать запрос на сертификат

- Как импортировать корневой или промежуточный сертификат

Открыть статью на сайте

Как создать запрос на сертификат в КриптоАРМ Подпись и шифрование

- Что такое запрос на сертификат?
- Как создать запрос на сертификат
- Дальнейшие действия после создания запроса
- Описание настроек запроса

Что такое запрос на сертификат?

Запрос на сертификат — это электронный документ, содержащий необходимые данные для получения сертификата электронной подписи от Удостоверяющего центра.

Зачем нужен запрос

Когда вы хотите получить сертификат для подписи или шифрования документов, Удостоверяющий центр должен убедиться, что ключи принадлежат вам, а данные о владельце верны. Запрос на сертификат содержит всю необходимую информацию для этого процесса.

Что включает запрос на сертификат

1. **Сведения о владельце**
    - ФИО, должность, организация и контактная информация.
    - Эти данные будут указаны в самом сертификате.
2. **Параметры ключевой пары**
    - Тип и длина ключа,
    - Назначение ключа,
    - Возможность экспорта ключа для переноса на другие устройства.
3. **Технические требования к сертификату**
    - Политики безопасности,
    - Срок действия сертификата,
    - Настройки использования ключа.

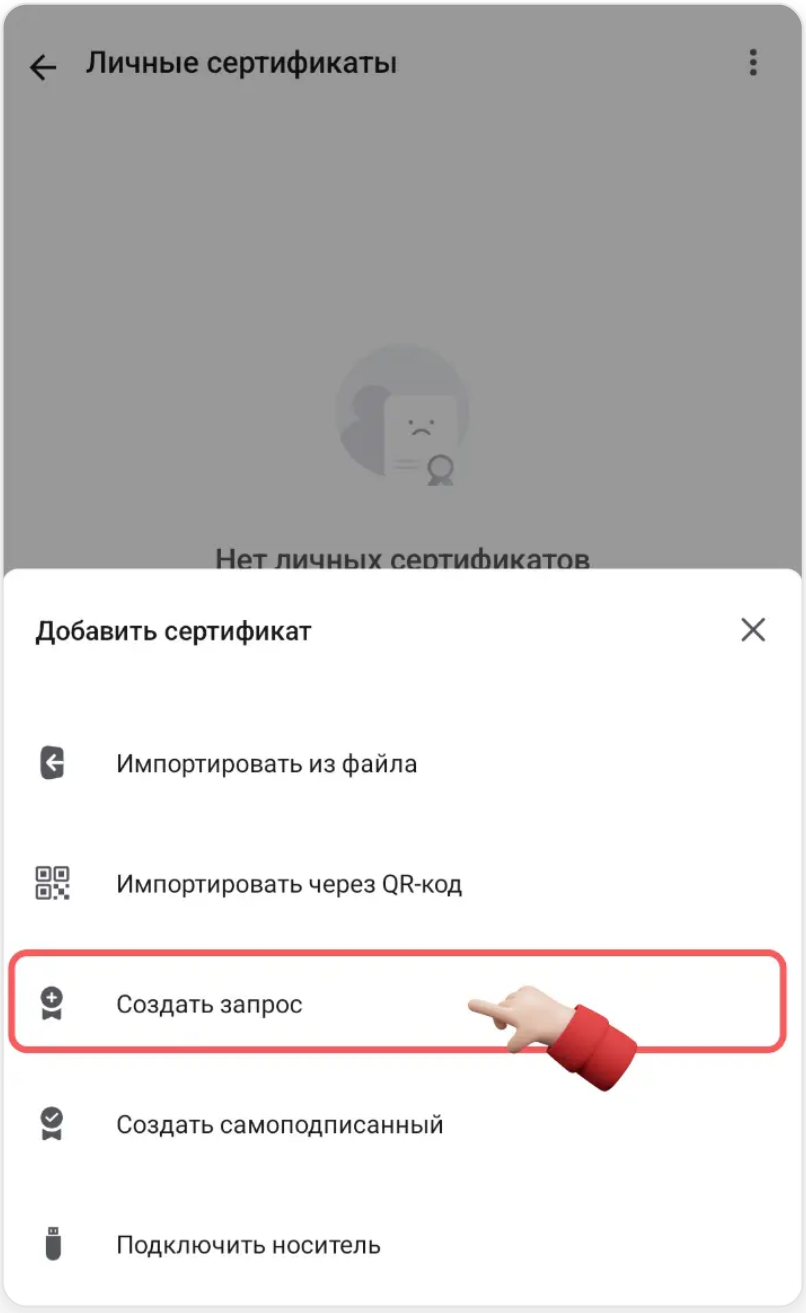
Как используется запрос

- После создания файла запроса его отправляют в Удостоверяющий центр.
- Удостоверяющий центр проверяет предоставленные данные и создаёт сертификат, который соответствует указанным параметрам.

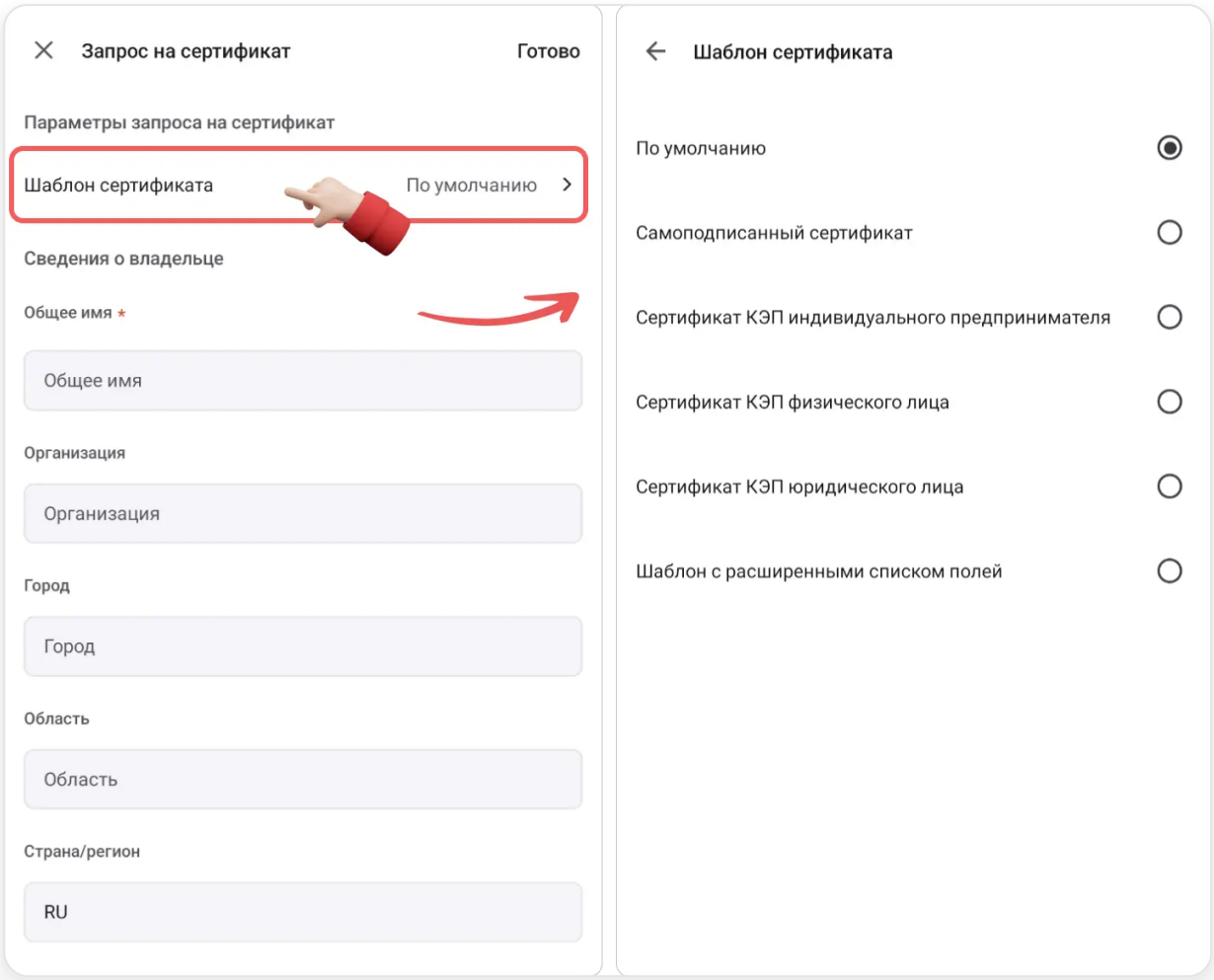
- После получения сертификата его импортируют в приложение, и он становится готовым для подписания и шифрования документов.

Как создать запрос на сертификат

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий **Добавить сертификат** одним из способов:
    - Нажмите кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
    - Вызовите меню действий и выберите **Добавить сертификат**.
3. Выберите действие **Создать запрос**.



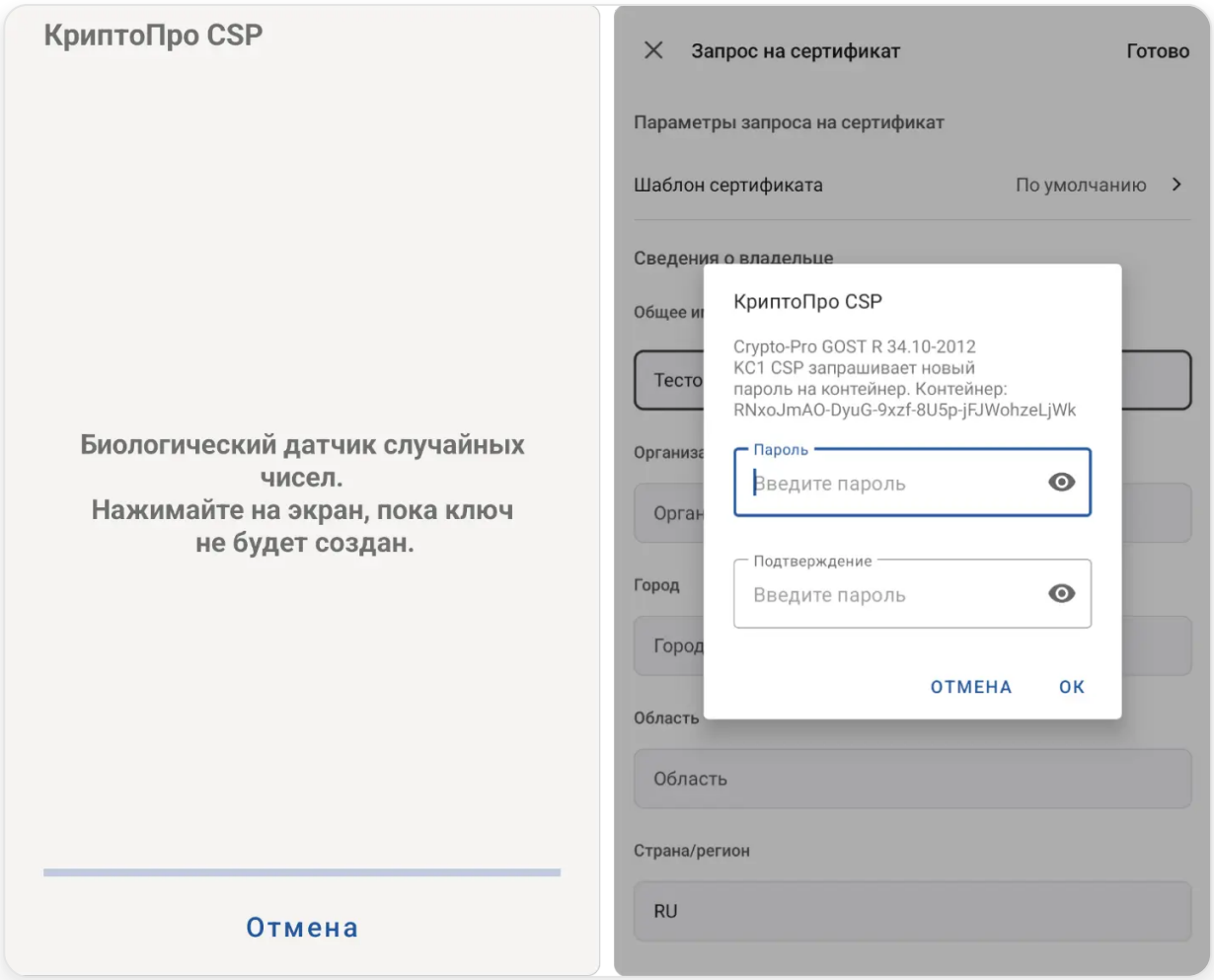
4. Откроется форма создания запроса.



5. Выберите шаблон сертификата.
6. Заполните обязательные поля в блоке **Сведения о владельце**. Набор полей меняется в зависимости от шаблона, выбранного на предыдущем шаге.
7. При необходимости внесите изменения в блок **Параметры ключа**.

> 🔍 Полный список настроек приведен в разделе Описание настроек запроса.

8. Нажмите **Готово**.
9. Откроется окно КриптоПро CSP.
10. Нажимайте на экран, пока не завершится генерация ключа.
11. Укажите пароль для контейнера. Поле ввода пароля можно оставить пустым.



На основе указанных данных будет сформирован запрос на сертификат.

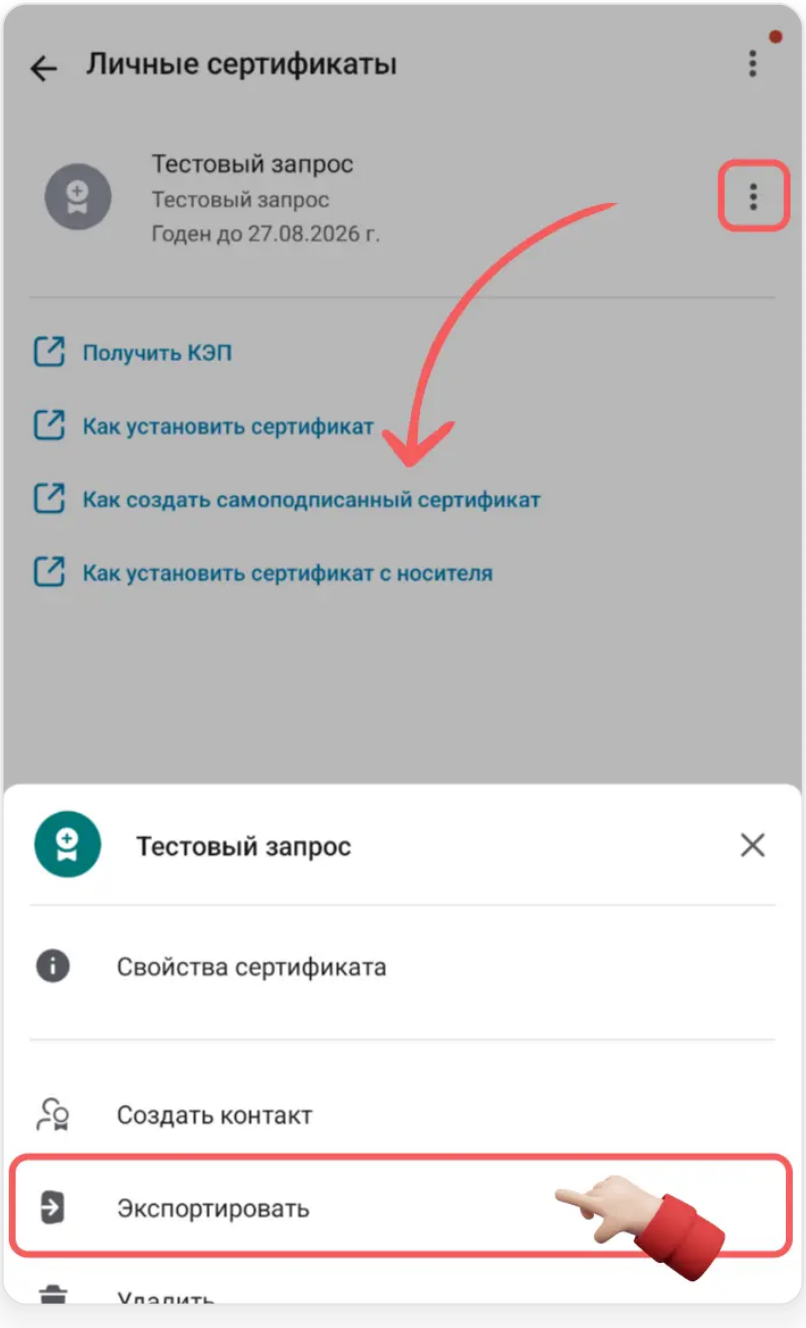
Дальнейшие действия после создания запроса

После создания запроса на сертификат необходимо отправить его в Удостоверяющий центр для обработки.

> ⚠️ Правила отправки и формат запроса определяются самим УЦ. Перед отправкой уточните эти требования.

Выгрузка запроса из приложения

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий по кнопке **Еще** , расположенной на панели с запросом.
3. Выберите действие **Экспортировать**.



4. Укажите место для сохранения файла или выберите приложение для его отправки.

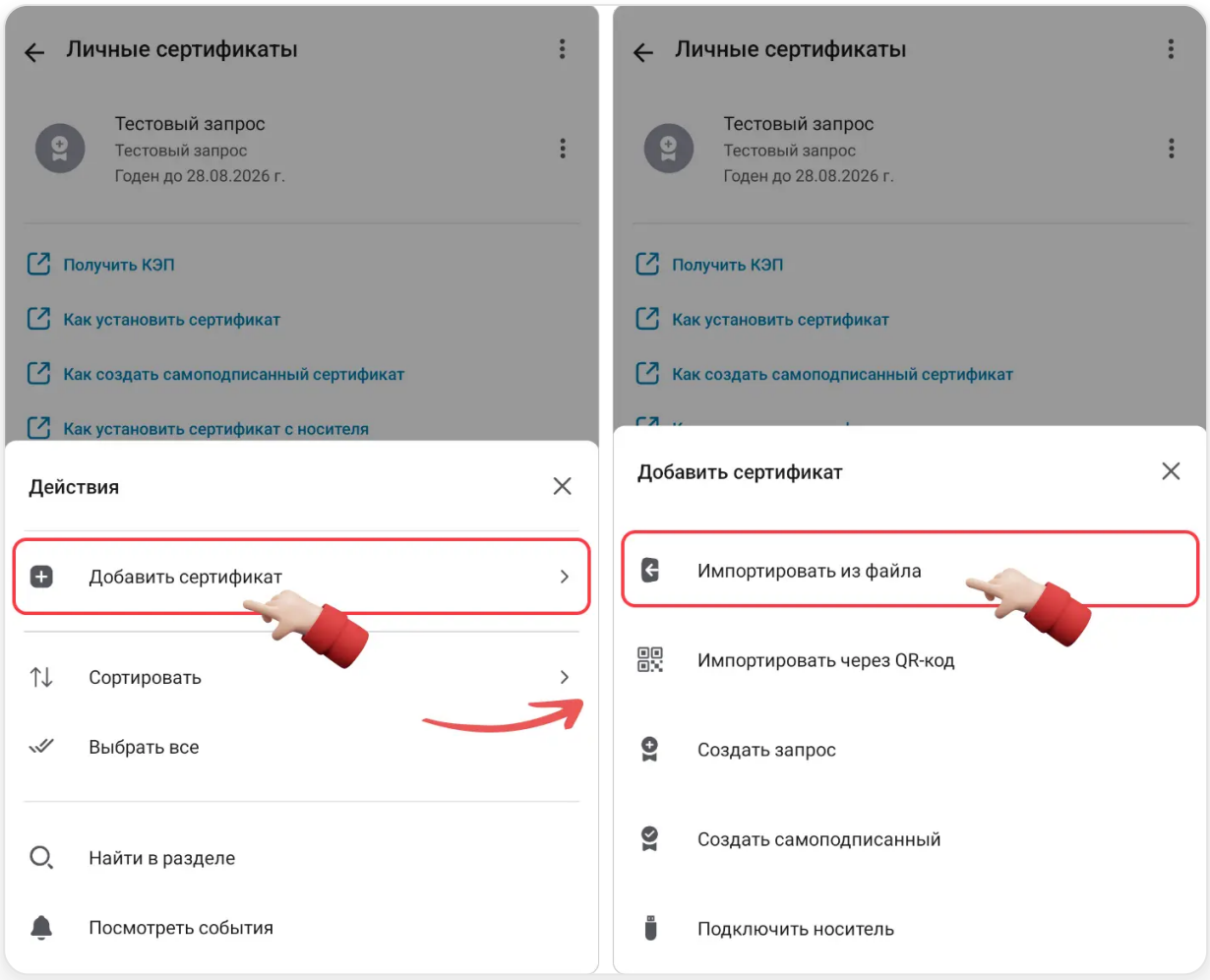
После этих действий файл запроса готов для передачи в УЦ.

Импорт готового сертификата

После проверки запроса УЦ выдаст готовый сертификат в виде файла `.cer`.

Чтобы импортировать сертификат:

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню по кнопке **Еще** ⋮ и выберите действие **Добавить сертификат**.
3. Выберите действие **Импортировать из файла**.



4. Укажите путь к файлу с сертификатом `.cer`.
5. Дождитесь окончания импорта.

После успешного импорта сертификат можно использовать для подписания и шифрования документов.

> 💡 Чтобы статус сертификата определялся правильно, убедитесь, что установлены корневые и промежуточные сертификаты. Подробнее об установке читайте в инструкции.

Описание настроек запроса

Параметры ключа

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Алгоритм		Алгоритм подписи	

Название настройки	Значение по умолчанию	Описание	Допустимые значения
	ГОСТ Р 34.10-2012 256 бит		- ГОСТ Р 34.10-2012 256 бит, - ГОСТ Р 34.10-2012 512 бит
Назначение ключа	Подпись и шифрование	Назначение ключа	- Подпись, - Подпись и шифрование, - Шифрование
Пометить ключи как экспортируемые	Не экспортируемый	Позволяет экспортировать закрытый ключ вместе с сертификатом для переноса на другое устройство	Экспортируемый / Не экспортируемый
Средство электронной подписи владельца	КриптоПро CSP (версия 5.0)	Шифровальное (криптографическое) средство, которое используется для реализации криптографических функций	-
Политики сертификата	Класс средства ЭП КС1	Класс средства ЭП зависит от используемого средства подписи и указывает на уровень защиты информации	КС1, КС2, КС3, КВ1, КВ2 и КА

Использование ключа

> 💡 Таблица показывает значения по умолчанию. Их можно изменить при необходимости, исходя из требований УЦ и задач использования сертификата.

Назначение ключа	Подпись	Шифрование	Подпись и шифрование
Подпись (digitalSignature)	✅		✅
Шифрование ключей (keyEncipherment)		✅	✅
Неотрекаемость (nonRepudiation/ contentCommitment)	✅		✅

Назначение ключа	Подпись	Шифрование	Подпись и шифрование
Шифрование данных (dataEncipherment)		✅	✅
Согласование ключей (keyAgreement)	✅	✅	✅
Подпись сертификатов (keyCertSign)			
Подпись CRL (cRLSign)			
Только шифрование (encipherOnly)			
Только расшифрование (decipherOnly)			
Защищенная почта	✅	✅	✅
Проверка подлинности сервера			
Проверка подлинности клиента	✅	✅	✅
Подпись кода			

Инструкции по теме

- Как установить личный сертификат
- Как создать самоподписанный сертификат
- Как импортировать корневой или промежуточный сертификат

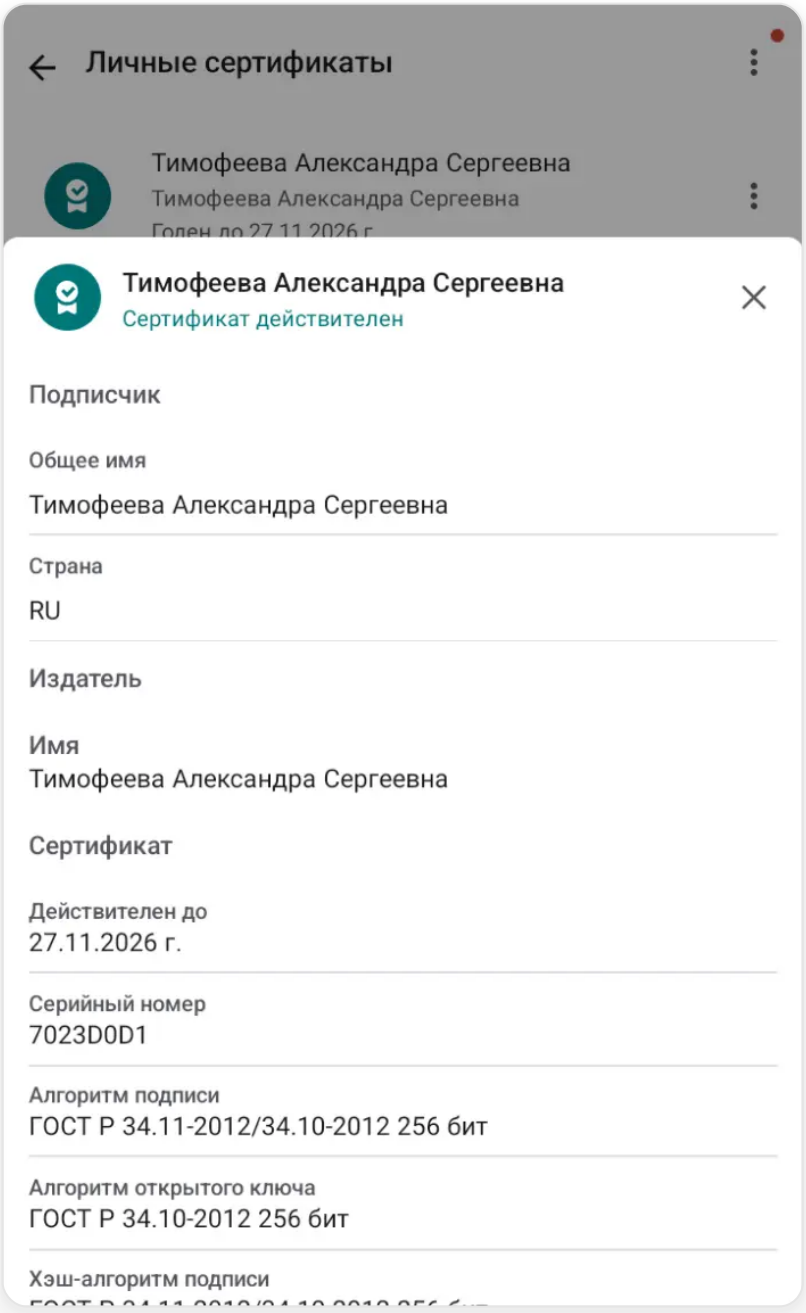
Открыть статью на сайте

Как проверить статус сертификата

- Просмотр сведений о сертификате
- Проверка статуса сертификата
- Инструкции по теме

Просмотр сведений о сертификате

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Найдите нужный сертификат в списке:
    - нажмите на название сертификата для быстрого просмотра,
    - откройте меню по кнопке **Еще** и выберите действие **Просмотреть сведения**.
3. Откроется окно со сведениями о сертификате.



Проверка статуса сертификата

Статус сертификата проверяется по следующим параметрам:

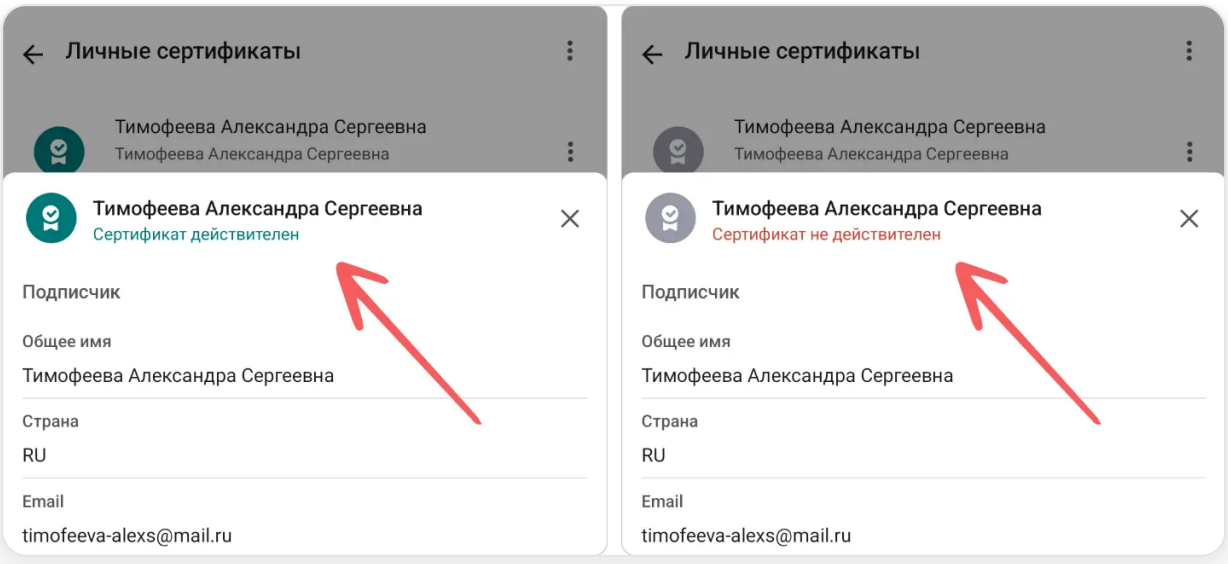
Критерий проверки	Что означает	Почему это важно
Срок действия	Проверка срока действия сертификата	Гарантирует, что сертификат не просрочен
Подпись УЦ	Проверка подписи Удостоверяющего центра	

Критерий проверки	Что означает	Почему это важно
		Подтверждает, что сертификат подписан соответствующим Удостоверяющим центром и не был изменен
Цепочка доверия	Построение полной цепочки до корневого сертификата	Позволяет проверить связь сертификата с доверенным корневым сертификатом
Статус отзыва	Проверка по актуальным спискам CRL	Исключает использование отозванных сертификатов

Возможные статусы сертификата

В приложении возможны два статуса сертификата:

1. **Действительный** (● зеленый индикатор) — если выполняются следующие условия:
    - Подпись Удостоверяющего центра корректна.
    - Срок действия сертификата не истек.
    - Назначение сертификата соответствует выполняемой операции.
    - Сертификат не отозван и его действие не приостановлено.
2. **Недействительный** (● серый индикатор) — если не выполняется хотя бы одно из перечисленных условий.



Распространенные проблемы с сертификатами

Некоторые причины недействительности сертификата:

Проблема	Можно исправить?	Что делать
Срок действия истек	❌ Нет	Оформите новый сертификат
Сертификат отозван	❌ Нет	Оформите новый сертификат
Неполная цепочка доверия	✅ Да	Установите недостающие корневые и промежуточные сертификаты. Об установке корневых сертификатов читайте в инструкции Установка корневого и промежуточного сертификатов.

Инструкции по теме

- Как установить личный сертификат
- Как создать запрос на сертификат
- Как создать самоподписанный сертификат
- Как импортировать корневой или промежуточный сертификат
- Как удалить сертификат

Открыть статью на сайте

Как экспортировать личный сертификат

- Основные принципы экспорта
- Экспорт без закрытого ключа
- Экспорт с закрытым ключом
- Инструкции по теме

Основные принципы экспорта

Экспорт сертификата — это сохранение его в файл для дальнейшего использования или передачи другим пользователям.

Для безопасного обмена зашифрованными данными необходимо правильно экспортировать сертификаты.

Существует два основных варианта экспорта:

1. **Без закрытого ключа** — стандартный и безопасный способ.
    - Используется для передачи сертификата коллегам, партнёрам или сервисам.
    - Получатели смогут зашифровать данные для вас или проверить вашу подпись.
    - При этом ваш закрытый ключ остаётся в безопасности.
2. **С закрытым ключом** — используется только в особых случаях.
    - Позволяет перенести сертификат на другое устройство или создать резервную копию.
    - Хранение и передача таких файлов требует строгой защиты.

> ⚠️ **Важно**: экспорт с закрытым ключом доступен только если при создании сертификата был установлен флаг «Экспортируемый». Если он не был задан, выполнить экспорт ключа невозможно.

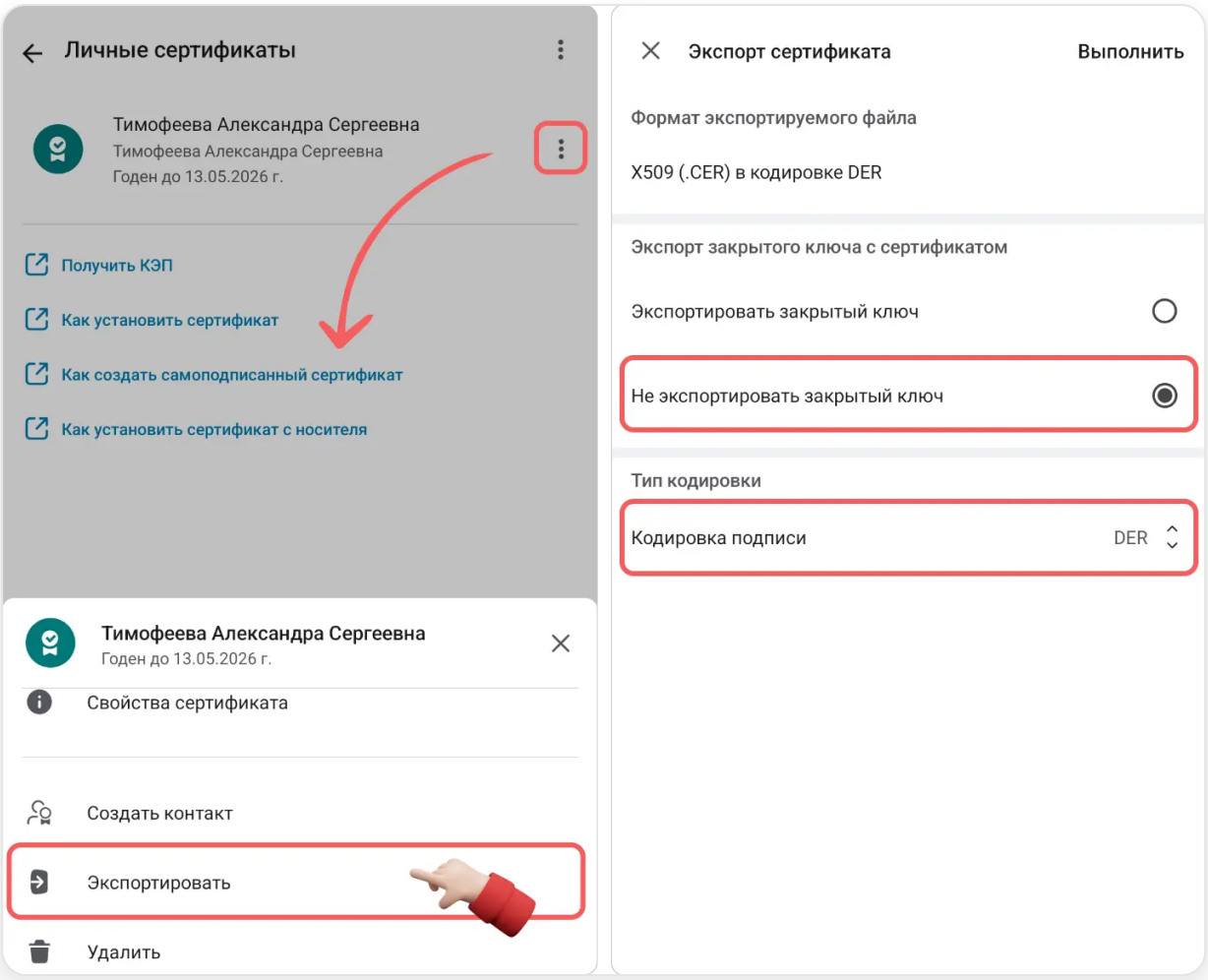
Сравнение способов экспорта

Параметр	Без закрытого ключа	С закрытым ключом
Назначение	Передача сертификата другим людям или системам	Перенос сертификата на другое устройство, резервное копирование
Можно использовать для	Проверка подписей и шифрование данных в ваш адрес	Создания подписей и расшифрования данных на другом устройстве

Параметр	Без закрытого ключа	С закрытым ключом
Безопасность	Безопасно, т.к. закрытый ключ остаётся у вас	Требует осторожного хранения: при получении файла и пароля посторонний может воспользоваться закрытым ключом
Кому можно передавать	Любому получателю, кому нужно знать ваш открытый ключ	Не передавайте файл другим лицам. Используйте его только для переноса ключа или резервного копировани
Формат файла	`.cer`	`.pfx` (пароль обязателен)

Экспорт без закрытого ключа

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий с сертификатом.
3. Выберите действие **Экспортировать**.



4. Откроется окно **Экспорт сертификата**:
    - Выберите опцию **Не экспортировать закрытый ключ**.
    - Укажите **Тип кодировки**.
5. Нажмите **Выполнить**.
6. В появившемся окне укажите место для сохранения сертификата или выберите приложение для его отправки.

Экспорт с закрытым ключом

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий с сертификатом.
3. Выберите действие **Экспортировать**.
4. Откроется окно **Экспорт сертификата**:
    - Выберите опцию **Экспортировать закрытый ключ**. Экспорт закрытого ключа может быть недоступен, если ключ создан как неэкспортируемый.

- Укажите **Тип кодировки**.
- Укажите пароль от PFX-контейнера.

5. Нажмите **Выполнить**.
6. В появившемся окне укажите место для сохранения сертификата или выберите приложение для его отправки.

> ⚠️ **Совет по безопасности**: храните PFX-файл только в надёжном месте и не передавайте его без необходимости.

Инструкции по теме

- Как экспортировать сертификат другого пользователя
- Как удалить сертификат
- Как импортировать корневой или промежуточный сертификат
- Как импортировать сертификат другого пользователя
- Как импортировать список отзыва

Открыть статью на сайте

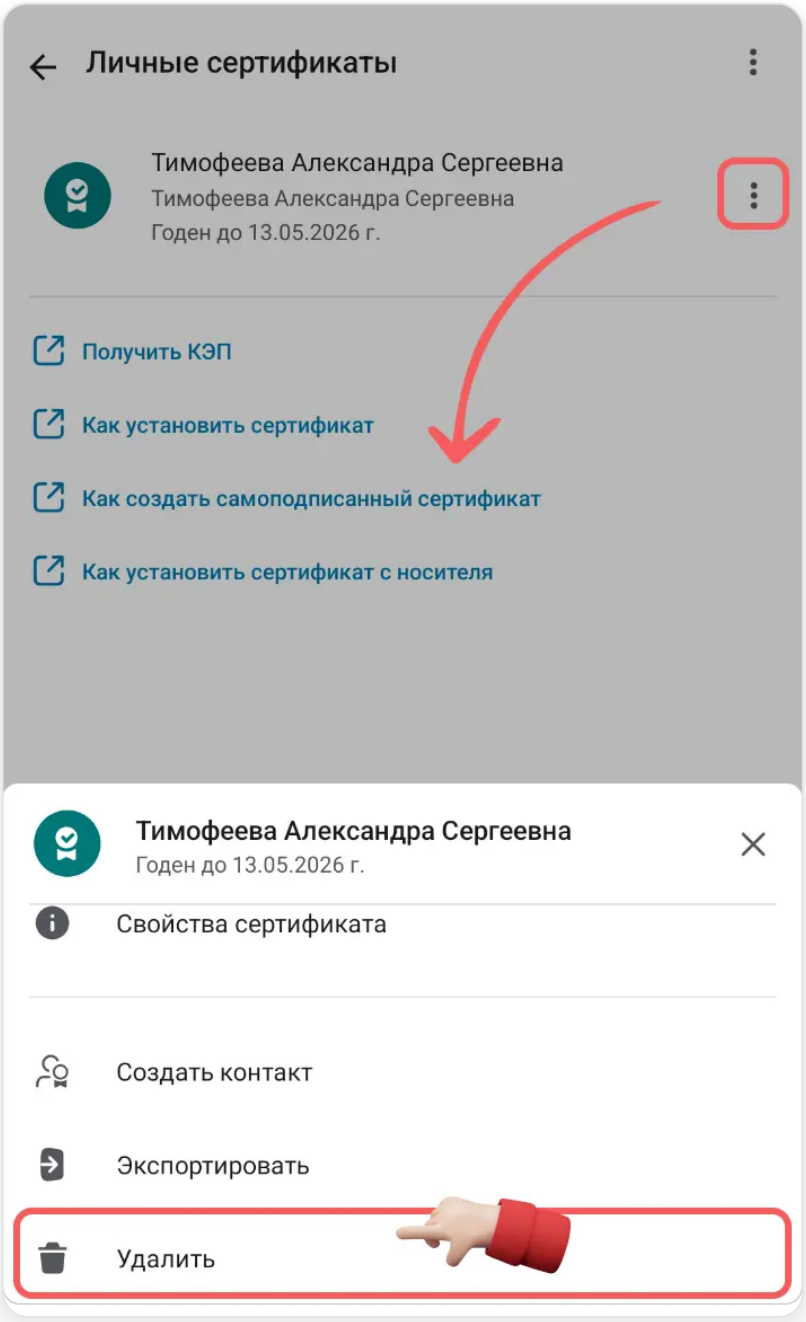
Как удалить сертификат в КриптоАРМ Подпись и шифрование

> 💡 **Совет**: Вы можете удалить сертификат, если он больше не нужен, например, если срок его действия истек или в приложении появился его дубликат.

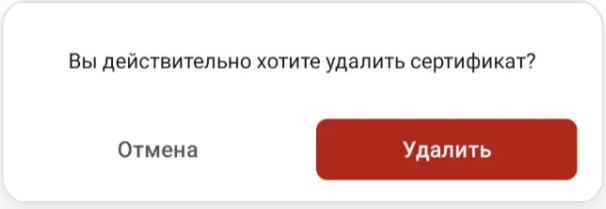
Удаление одного сертификата

Чтобы удалить сертификат:

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Откройте меню по кнопке **Еще** , расположенной на панели с сертификатом.
3. Выберите действие **Удалить**.



4. Подтвердите удаление сертификата в модальном окне.



После этого сертификат будет удален из хранилища приложения.

Групповое удаление

Чтобы удалить несколько сертификатов одновременно:

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Выбрать сертификаты для удаления можно одним из следующих способов:
   - Вызовите меню действий по кнопке **Еще** и выберите действие **Выбрать все** . В списке сертификатов отобразятся флажки. Установите флажки напротив тех профилей, которые необходимо удалить.
   - Нажмите панель сертификата и удерживайте ее. Рядом с панелью сертификата появится флажок. Выберите другие сертификаты.
3. Вызовите меню действий по кнопке **Еще** и выберите действие **Удалить**.
4. Подтвердите удаление сертификатов в модальном окне.

Инструкции по теме

- Как установить личный сертификат
- Как экспортировать сертификат другого пользователя
- Как импортировать корневой или промежуточный сертификат
- Как импортировать сертификат другого пользователя
- Как импортировать список отзыва

Открыть статью на сайте

Как установить сертификаты УЦ в КриптоАРМ Подпись и шифрование

- Основные понятия
- Импорт корневого или промежуточного сертификата
- Возможные ошибки
- Инструкции по теме

Основные понятия

Корневой сертификат — это цифровой документ, в котором содержится информация об удостоверяющем центре. Именно с него начинается «цепочка доверия».

- **Корневые сертификаты** выпускаются только аккредитованными организациями.
- В России функции головного удостоверяющего центра выполняет Минцифры России.
- Минцифры подписывает сертификаты удостоверяющих центров своим корневым сертификатом — они называются **промежуточными**.
- Удостоверяющие центры выпускают **пользовательские сертификаты**, формируя цепочку доверия через промежуточные сертификаты.

Таким образом, цепочка доверия включает пользовательский, промежуточный и корневой сертификаты: Пользовательский → Промежуточный → Корневой.

> 🚨 Для корректной проверки статуса сертификата в приложении должны быть установлены **все звенья цепочки доверия** — корневой и все промежуточные сертификаты.

Где взять корневой сертификат

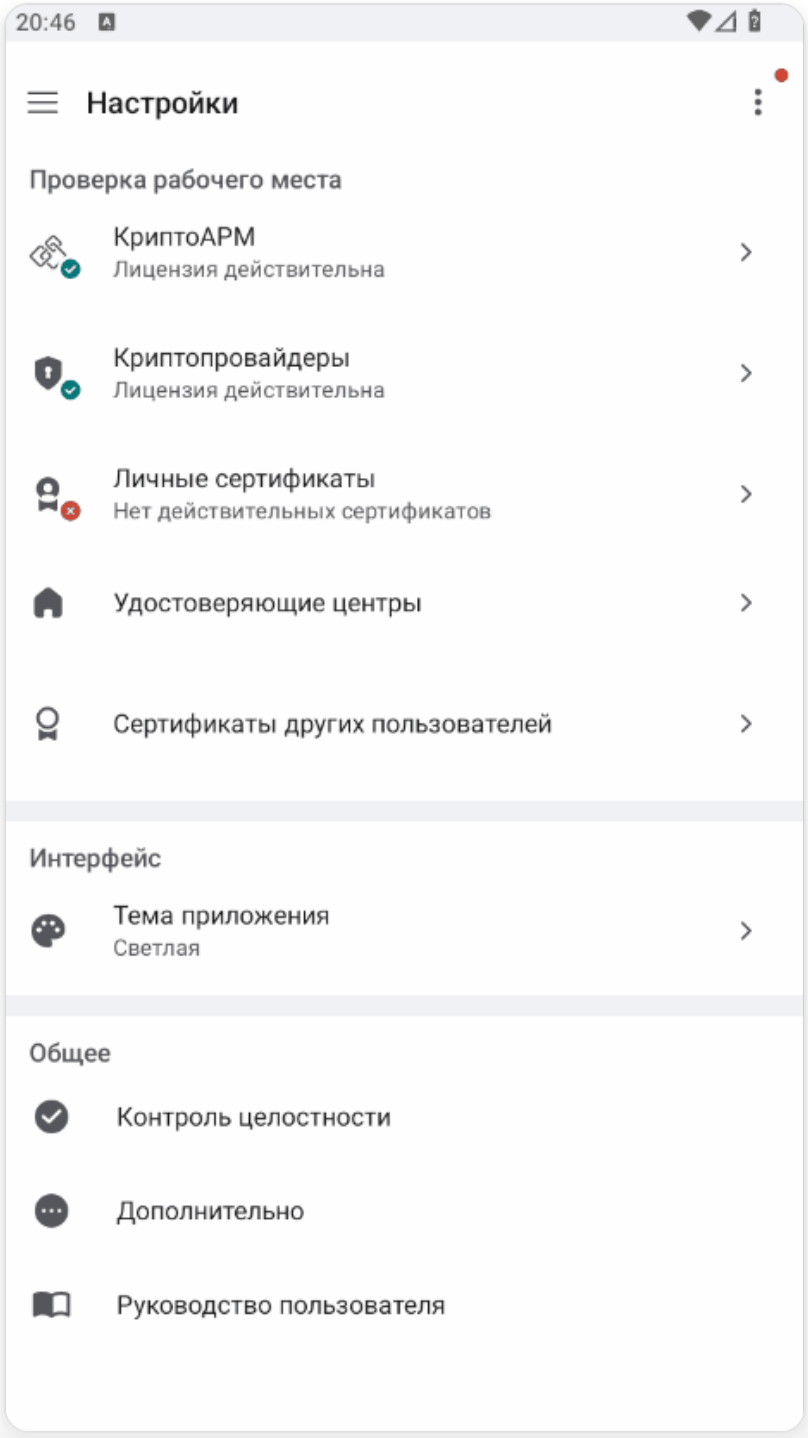
- **На официальном сайте удостоверяющих центров**: обычно в разделе «Поддержка» или «Загрузки» доступны актуальные корневые и промежуточные сертификаты, а также списки отзыва.

> ⚠️ Всегда скачивайте сертификаты только с официальных сайтов УЦ.

Импорт корневого или промежуточного сертификата

> 💡 **Совет**: Перед началом убедитесь, что на устройстве сохранен корректный файл сертификата с расширением `.cer`.

1. Перейдите в раздел **Настройки** → **Удостоверяющие центры**.
2. Вызовите меню **Добавить сертификат** одним из способов:
   - Нажмите кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
   - Вызовите меню по кнопке **Еще** и выберите действие **Добавить сертификат**.
3. Выберите действие **Импортировать из файла**.
4. Укажите путь к файлу с сертификатом `.cer`.



Дождитесь окончания импорта.

После успешного импорта сертификат отобразится в списке.

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана.

Для просмотра подробной информации нажмите **Просмотреть события** в меню **Действия**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Описание	Рекомендуемые действия
Ошибка при импорте сертификата	Файл поврежден, не полностью скачан или содержит неподдерживаемые параметры	1. Скачайте файл заново 2. Проверьте целостность файла 3. Попробуйте импортировать сертификат на другом устройстве 4. Если файл получен от УЦ, запросите сертификат повторно или скачайте его заново с официального сайта
Неверное расширение файла	Файл не содержит сертификат	1. Убедитесь, что файл содержит сертификат 2. Проверьте, что файл экспортирован корректно 3. Импортируйте сертификат заново

Инструкции по теме

- Как установить личный сертификат
- Как создать запрос на сертификат
- Как создать самоподписанный сертификат
- Как импортировать сертификат другого пользователя
- Как импортировать список отзыва

Открыть статью на сайте

Как установить список отзыва в КриптоАРМ Подпись и шифрование

- Основные понятия
- Импорт списка отзыва
- Возможные ошибки
- Инструкции по теме

Основные понятия

Список отзыва сертификатов (СОС) или **Certificate Revocation List** (CRL) — это специальный цифровой документ, публикуемый удостоверяющим центром. В нем содержатся сведения о сертификатах, отозванных до окончания срока их действия.

СОС используется для проверки статуса сертификатов и выявления отозванных сертификатов.

Основные причины отзыва:

- Компрометация закрытого ключа (потеря, кража токена)
- Изменение данных владельца (смена фамилии, реквизитов организации)
- Ошибки при выпуске сертификата
- Прекращение деятельности удостоверяющего центра
- Нарушение условий использования

> 📌 **Проверка СОС** — обязательная часть процесса подтверждения подлинности сертификатов. Если сертификат присутствует в списке отзыва, его использование считается недопустимым.

Где взять список отзыва

Списки отзыва публикуются удостоверяющими центрами, которые выпускают сертификаты.

Получить списки отзыва можно несколькими способами:

1. **На официальном сайте удостоверяющих центров**: обычно в разделе «Поддержка» или «Загрузки» доступны актуальные версии СОС вместе с корневыми и промежуточными сертификатами.
2. **По ссылке из личного сертификата**: в свойствах сертификата есть поле **CRL Distribution Point (CDP)**. По указанному адресу (`http://...`) можно скачать актуальный СОС.

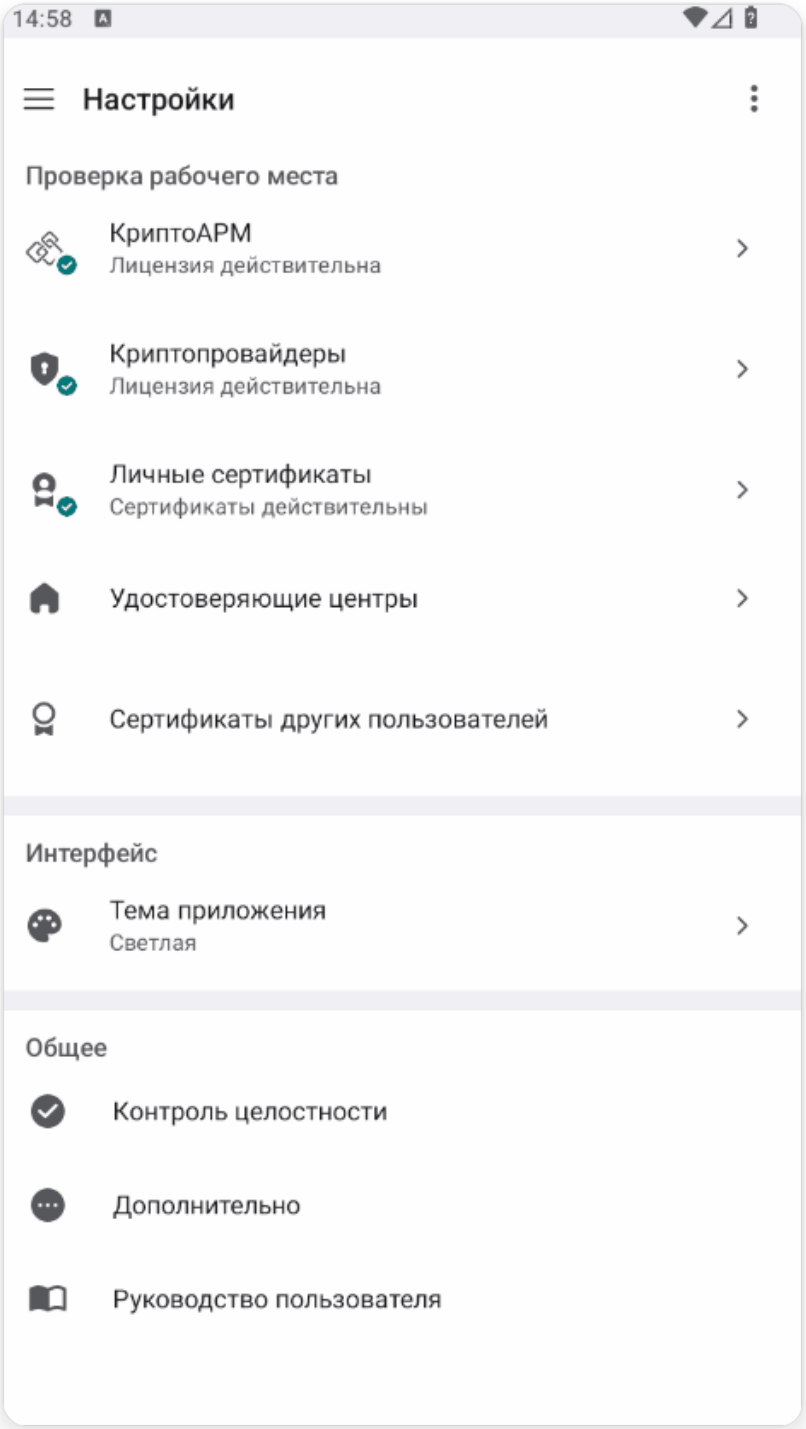
> ⚠️ Списки отзыва имеют ограниченный срок действия. После его окончания необходимо скачать актуальную версию.
>
> ⚠️ Всегда скачивайте списки отзыва только с официальных сайтов УЦ.

Импорт списка отзыва

> 💡 **Совет**: Перед началом убедитесь, что на устройстве сохранен корректный файл со списком отзыва с расширением `.crl`.

Чтобы импортировать список отзыва:

1. Перейдите в раздел **Настройки** → **Удостоверяющие центры**.
2. Откройте вкладку **Списки отзыва**.
3. Вызовите меню **Добавить список** одним из способов:
   - Нажмите на кнопку **Добавить список** в центре окна, если в приложении отсутствуют списки.
   - Вызовите меню по кнопке **Еще** и выберите действие **Добавить список**.
4. Выберите действие **Импортировать из файла**.
5. Укажите путь к файлу со списком отзыва `.crl`.



Дождитесь окончания импорта.

После успешного импорта список отобразится в окне **Списки отзыва**.

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана. Для просмотра подробной информации нажмите **Просмотреть события** в меню **Действия**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Описание	Рекомендуемые действия
Ошибка при импорте	Возможно, файл поврежден или содержит несовместимые параметры	1. Скачайте файл повторно с официального сайта УЦ и попробуйте импортировать его еще раз 2. Проверьте целостность файла
Неверное расширение файла	Файл не содержит список отзыва	Убедитесь, что файл содержит список отзыва

Инструкции по теме

- Как установить личный сертификат
- Как импортировать корневой или промежуточный сертификат
- Как импортировать сертификат другого пользователя
- Как создать запрос на сертификат
- Как создать самоподписанный сертификат

Открыть статью на сайте

Как установить сертификаты других пользователей в КриптоАРМ Подпись и шифрование

- Зачем нужны сертификаты других пользователей
- Импорт сертификата другого пользователя
- Возможные ошибки
- Инструкции по теме

Зачем нужны сертификаты других пользователей

Сертификаты других пользователей нужны для безопасного обмена зашифрованными документами.

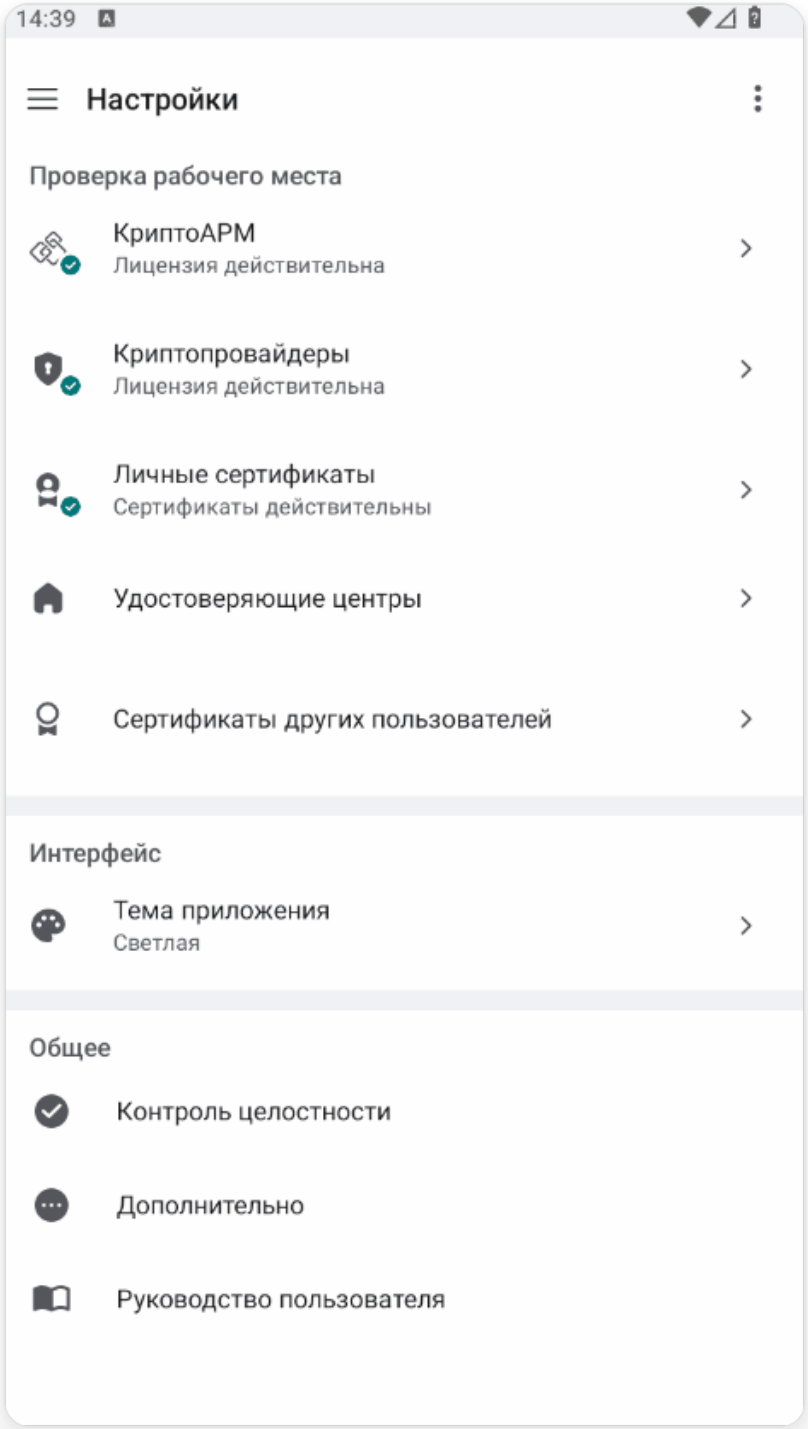
При отправке коллеге или партнеру конфиденциальной информации (например, договор, отчет или персональные данные), документ шифруется с использованием открытого ключа получателя, который хранится в его сертификате.

> 💡 **Совет**: Чтобы упростить работу, привяжите сертификат к контакту пользователя — это ускорит поиск и исключит ошибки при выборе сертификата.

Импорт сертификата другого пользователя

> 💡 **Совет**: Перед началом убедитесь, что на устройстве сохранен корректный файл с сертификатом с расширением `.crt`.

1. Перейдите в раздел **Настройки** → **Сертификаты других пользователей**.
2. Вызовите меню **Добавить сертификат** одним из способов:
   - Нажмите на кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
   - Вызовите меню по кнопке **Еще** и выберите действие **Добавить сертификат**.
3. Выберите действие **Импортировать из файла**.
4. Укажите путь к файлу с сертификатом `.cer`.



Дождитесь окончания импорта.

После успешного импорта сертификат отобразится в списке.

Возможные ошибки

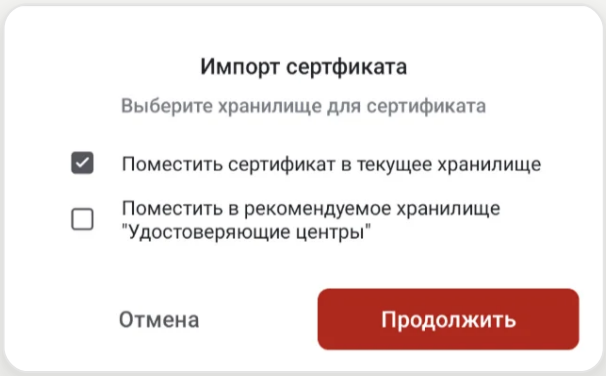
Уведомления об ошибках отображаются в нижней части экрана.

Для просмотра подробной информации нажмите **Просмотреть события** в меню **Действия**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Описание	Рекомендуемые действия
Ошибка при импорте сертификата	Возможно, файл с сертификатом поврежден или содержит несовместимые параметры	1. Скачайте файл заново 2. Проверьте целостность файла 3. Попробуйте импортировать на другом устройстве 4. Экспортируйте сертификат заново
Неверное расширение файла	Файл не содержит сертификат	1. Убедитесь, что файл содержит сертификат 2. Проверьте, что файл экспортирован корректно 3. Импортируйте сертификат заново

> ⚠️ **Примечание**: Если вы выберете сертификат, не подходящий для установки в выбранное хранилище, КриптоАРМ попросит подтверждение. Чтобы установить сертификат, выберите опцию "Поместить сертификат в текущее хранилище".



Инструкции по теме

- Как установить личный сертификат
- Как импортировать корневой или промежуточный сертификат
- Как импортировать список отзыва
- Как создать запрос на сертификат
- Как создать самоподписанный сертификат

Открыть статью на сайте

Как экспортировать и удалять сертификаты другого пользователя в КриптоАРМ Подпись и шифрование

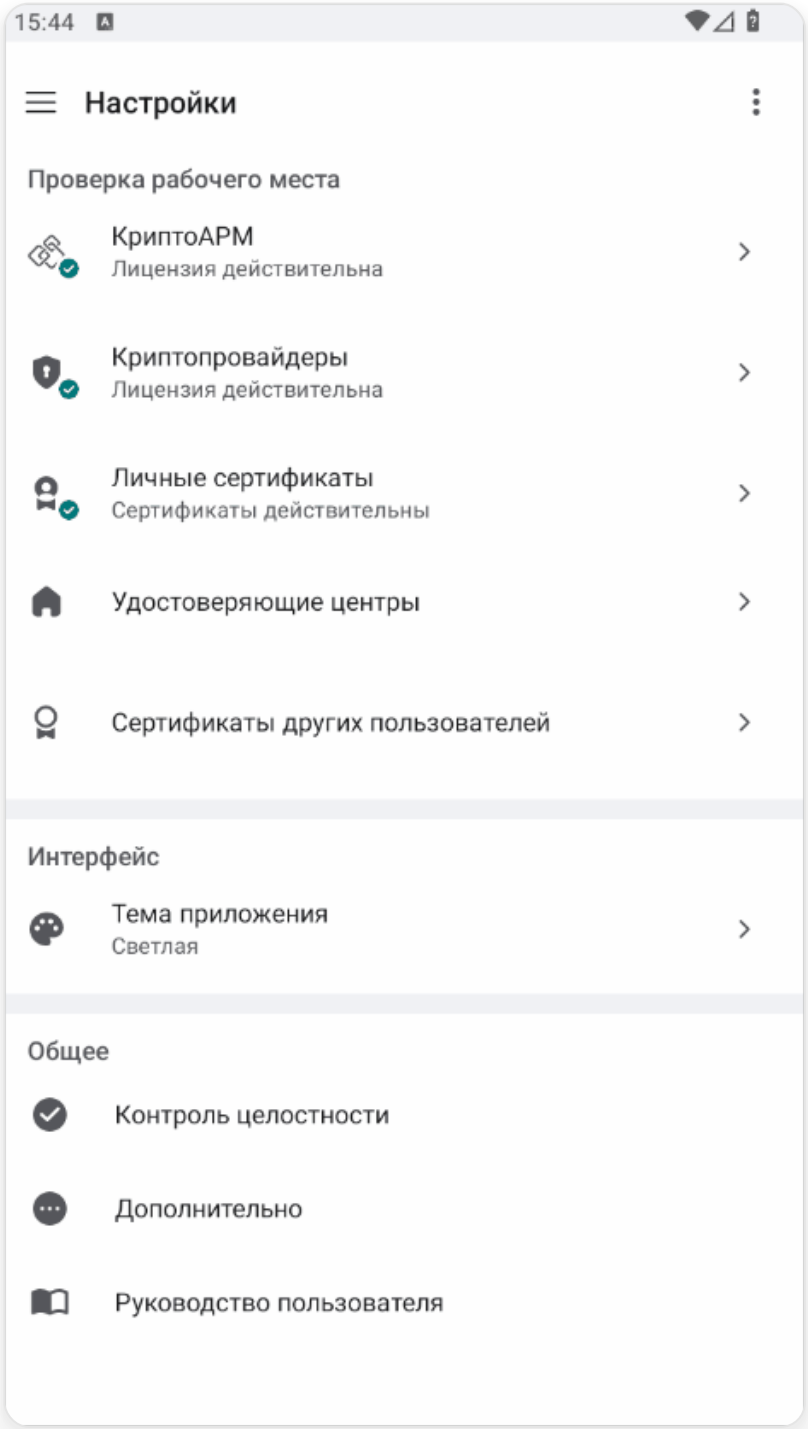
- Экспорт сертификата другого пользователя
- Удаление сертификата другого пользователя
- Инструкции по теме

Экспорт сертификата другого пользователя

> ⚠️ **Примечание**: Сертификаты других пользователей, а также корневые и промежуточные сертификаты экспортируются без закрытого ключа.

Чтобы экспортировать сертификат:

1. Перейдите в раздел **Настройки** → **Сертификаты других пользователей**.
2. Вызовите меню действий по кнопке **Еще** , размещенной на панели с сертификатом, который необходимо экспортировать.
3. Выберите действие **Экспортировать**.
4. Откроется окно **Экспорт сертификата**.
5. Укажите **Тип кодировки**.
6. Нажмите **Выполнить** в правом верхнем углу.



7. В появившемся окне укажите место для сохранения сертификата или выберите приложение для отправки.

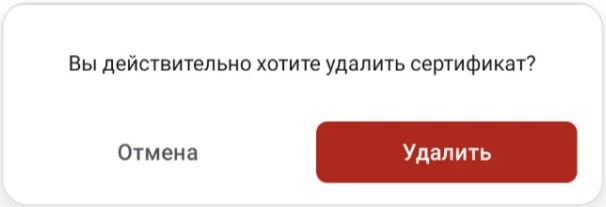
Удаление сертификата другого пользователя

Если срок действия сертификата истек или вы создали дубликат уже существующего в приложении сертификата, вы можете его удалить.

> 💡 **Совет**: Чтобы совершить действие сразу с несколькими сертификатами, нажмите **Выбрать все** в меню по кнопке **Еще** , отметьте нужные документы и выберите действие **Удалить**.

Чтобы удалить сертификат:

1. Перейдите в раздел **Настройки** → **Сертификаты других пользователей**.
2. Вызовите меню действий по кнопке **Еще** , размещенной на панели с сертификатом.
3. Выберите действие **Удалить**.
4. Подтвердите действие в модальном окне.



Сертификат будет успешно удален из хранилища.

Инструкции по теме

- Как экспортировать личный сертификат
- Как удалить сертификат
- Как импортировать корневой или промежуточный сертификат
- Как импортировать список отзыва

Открыть статью на сайте

Управление профилями в КриптоАРМ Подпись и шифрование

- О профилях подписи
- Локальный профиль
- Сетевой профиль
- Установка профиля по умолчанию
- Изменение настроек профиля
- Импорт профиля подписи
- Экспорт профиля подписи
- Удаление профиля
- Инструкции по теме

О профилях подписи

Профили подписи — это готовые наборы настроек, которые **КриптоАРМ Подпись и шифрование** использует при работе с документами и подключенными сервисами.

Профиль позволяет сохранить настройки и использовать их повторно, не задавая параметры при каждой операции.

В приложении доступны два типа профилей: локальные и сетевые.

Локальный профиль

Локальный профиль создается и настраивается пользователем непосредственно в приложении **КриптоАРМ Подпись и шифрование**.

В профиле можно сохранить параметры, необходимые для работы с документами, например настройки электронной подписи и шифрования.

Вы можете создать профиль подписи вручную или на основе уже установленного сертификата.

Советы по работе:

- Создавайте отдельные профили для разных задач и типов операций,
- Проверяйте актуальность сертификатов в профилях,
- Используйте экспорт и импорт, чтобы переносить профили между устройствами,
- Для важных операций проверяйте актуальность параметров профиля.

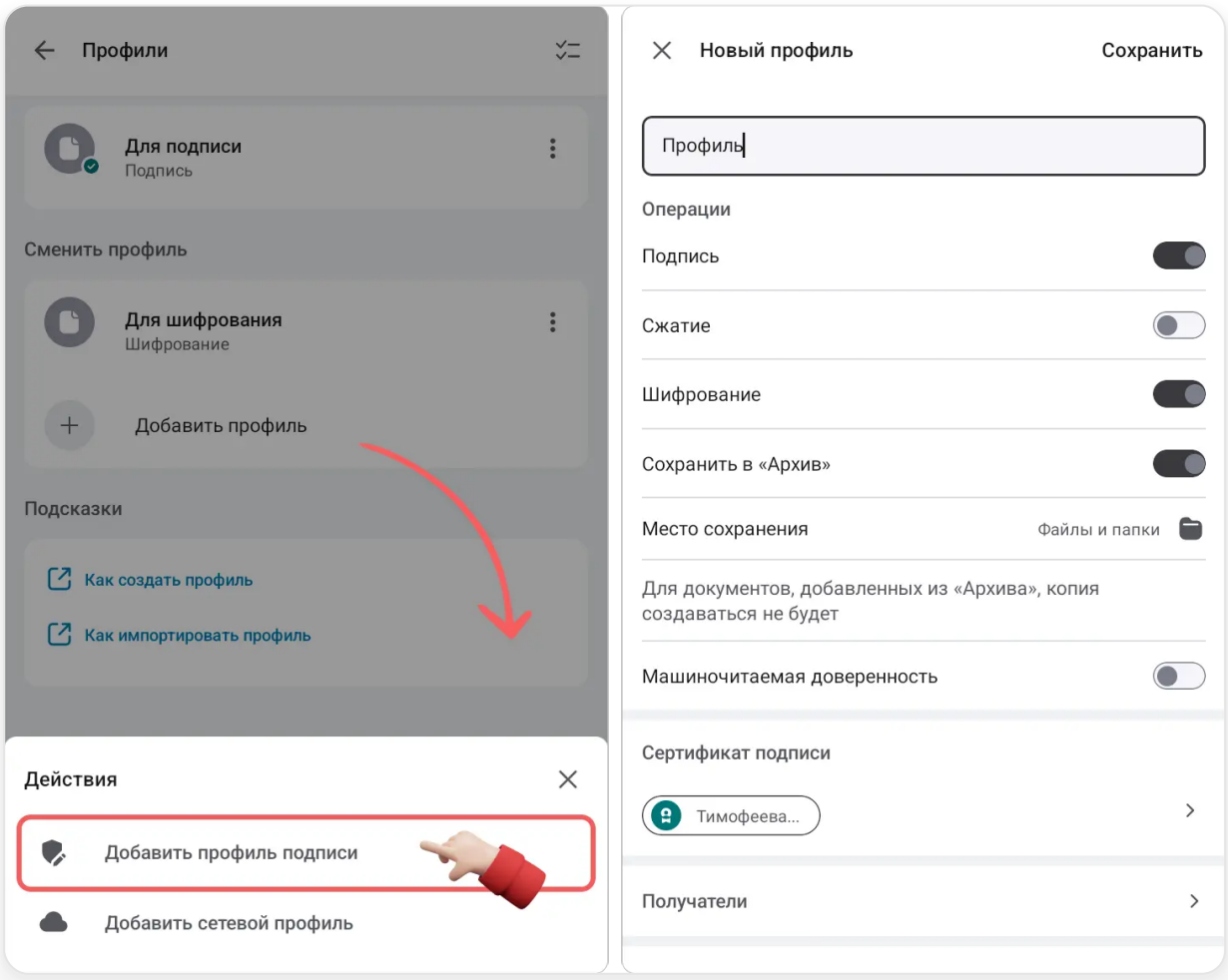
> ⚠️ **Примечание**: При установке приложения автоматически создается профиль подписи с активными операциями «Подпись» и «Шифрование».

Создание локального профиля подписи

Чтобы создать профиль:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Выберите действие **Добавить профиль** → **Добавить профиль подписи**.
4. Откроется окно **Новый профиль**.
5. Укажите настройки профиля.

> 🔍 Подробнее про настройки читайте в инструкции Описание настроек профиля.



6. Нажмите **Сохранить**.

После успешного создания профиля появится уведомление: **Профиль создан**.

Новый профиль отобразится в окне **Профили**.

> 💡 **Совет**: Чтобы автоматически использовать профиль при выполнении операций, установите его в качестве профиля по умолчанию.

Сетевой профиль

Сетевой профиль содержит параметры, необходимые для подключения **КриптоАРМ Подпись и шифрование** к информационной системе.

В текущей версии **КриптоАРМ Подпись и шифрование** поддерживается подключение к продукту КриптоАРМ Документы. После подключения документы, хранящиеся в информационной системе, становятся доступны в разделе **Документы** КриптоАРМ.

В профиле сохраняются адрес информационной системы, сведения о её сертификатах, параметры подписи и шифрования, а также другие настройки, необходимые для работы с информационной системой.

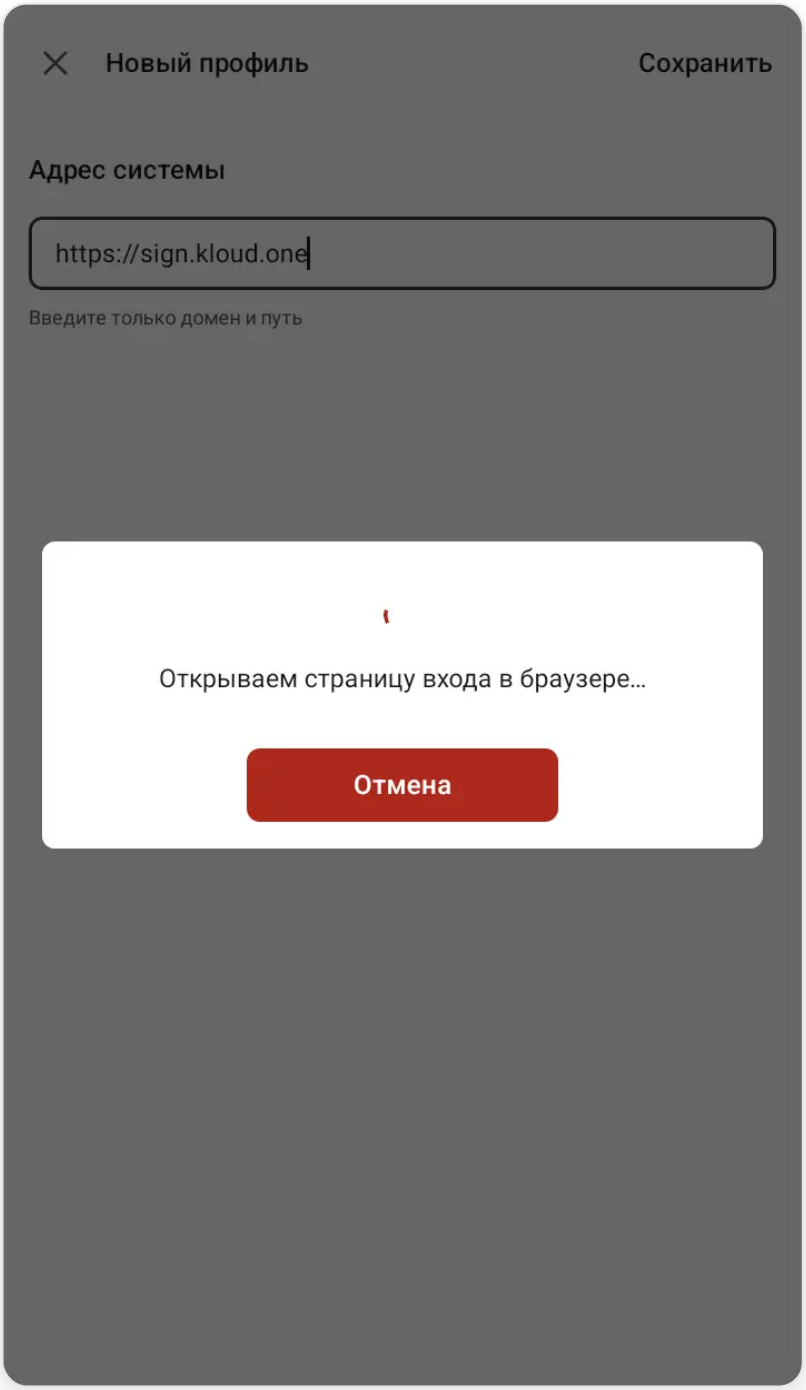
Параметры подписи и шифрования могут быть настроены непосредственно в приложении или получены из внешнего источника.

Создание сетевого профиля

Чтобы создать сетевой профиль:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Выберите действие **Добавить профиль** → **Добавить профиль подписи**.
4. Укажите **Адрес информационной системы** и нажмите **Сохранить**.

> 🔍 Подробнее о параметрах сетевого профиля читайте в инструкции Описание настроек профиля.



5. В открывшемся окне браузера выполните авторизацию в информационной системе.

6. После успешной авторизации браузер автоматически вернет вас в приложение.

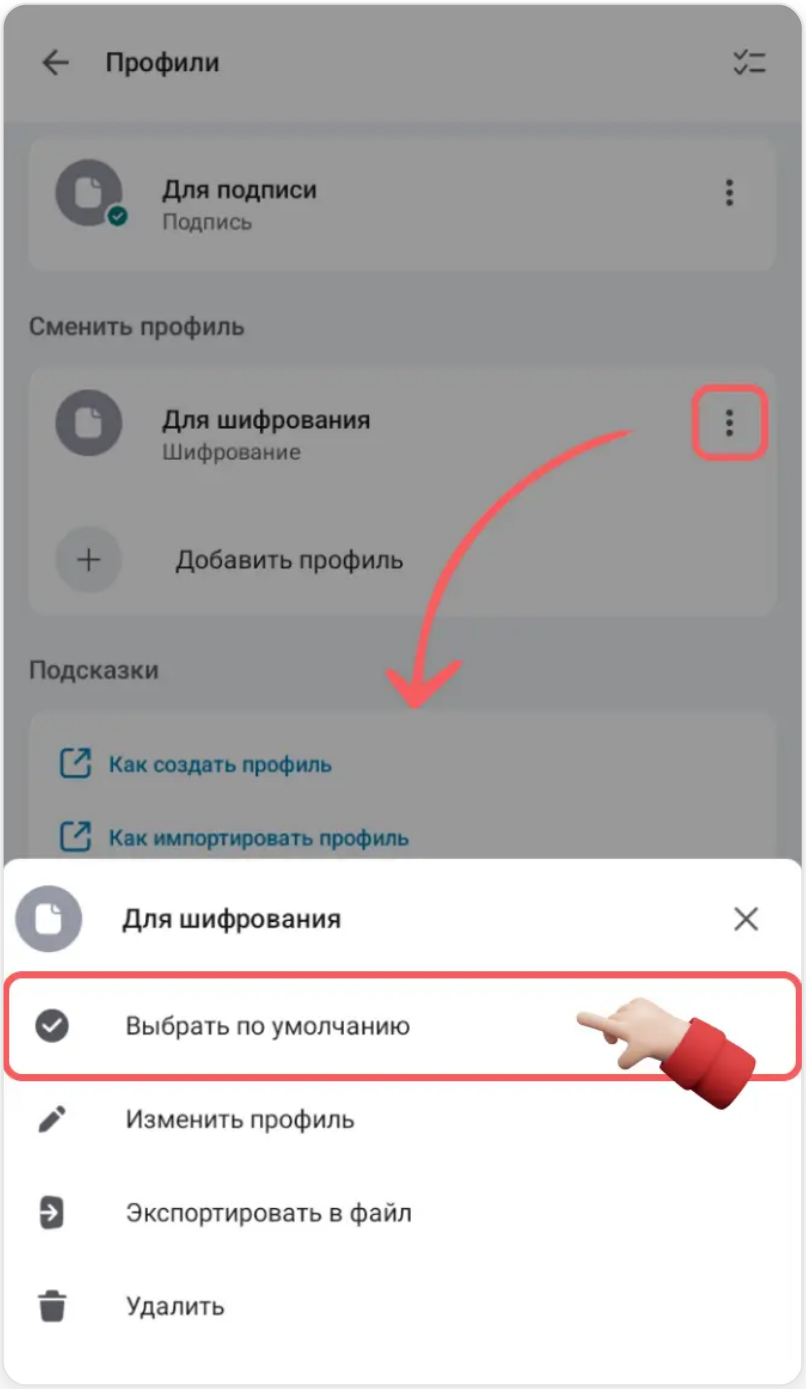
> 📌 **Важно**: Для одной информационной системы нельзя создать несколько сетевых профилей.

Установка профиля по умолчанию

Профиль по умолчанию используется автоматически при всех операциях с файлами.

Чтобы установить профиль по умолчанию:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Вызовите меню действий для профиля, который необходимо установить в качестве профиля по умолчанию.
4. Выберите действие **Выбрать по умолчанию**.



Профиль будет установлен в качестве профиля по умолчанию, и его настройки будут автоматически применяться при выполнении операций с файлами.

> 💡 Профиль по умолчанию отмечается иконкой в виде галочки .

Изменение настроек профиля

Чтобы изменить настройки профиля:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Открыть настройки профиля можно одним из следующих способов:
   - Нажмите на панель профиля.
   - Вызовите меню действий по кнопке **Еще** , размещенной на панели с профилем и выберите действие **Изменить профиль**.
4. Откроется окно редактирования настроек.
5. Внесите необходимые изменения.

> 🔍 Подробнее о настройках читайте в инструкции Описание настроек профиля.

6. Нажмите **Сохранить**.

> 📌 Изменение настроек профиля также доступно в разделе **Подпись и шифрование**.

Импорт профиля подписи

Профили подписи можно импортировать в приложение из файлов в формате `.pcarm`, `.json` или `.xml`.

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Вызовите меню **Действия** по кнопке **Еще** , расположенной в верхней части окна.
4. Выберите действие **Импорт из файла**.
5. Откроется системное окно файлового менеджера.
6. Укажите путь к файлу с профилями.

Дождитесь завершения операции. При успешном импорте профиль сохранится в приложении и будет отображаться в списке профилей.

Экспорт профиля подписи

> 💡 Экспорт позволяет сохранить настройки профиля для переноса на другое устройство, резервного хранения или обмена с коллегами.

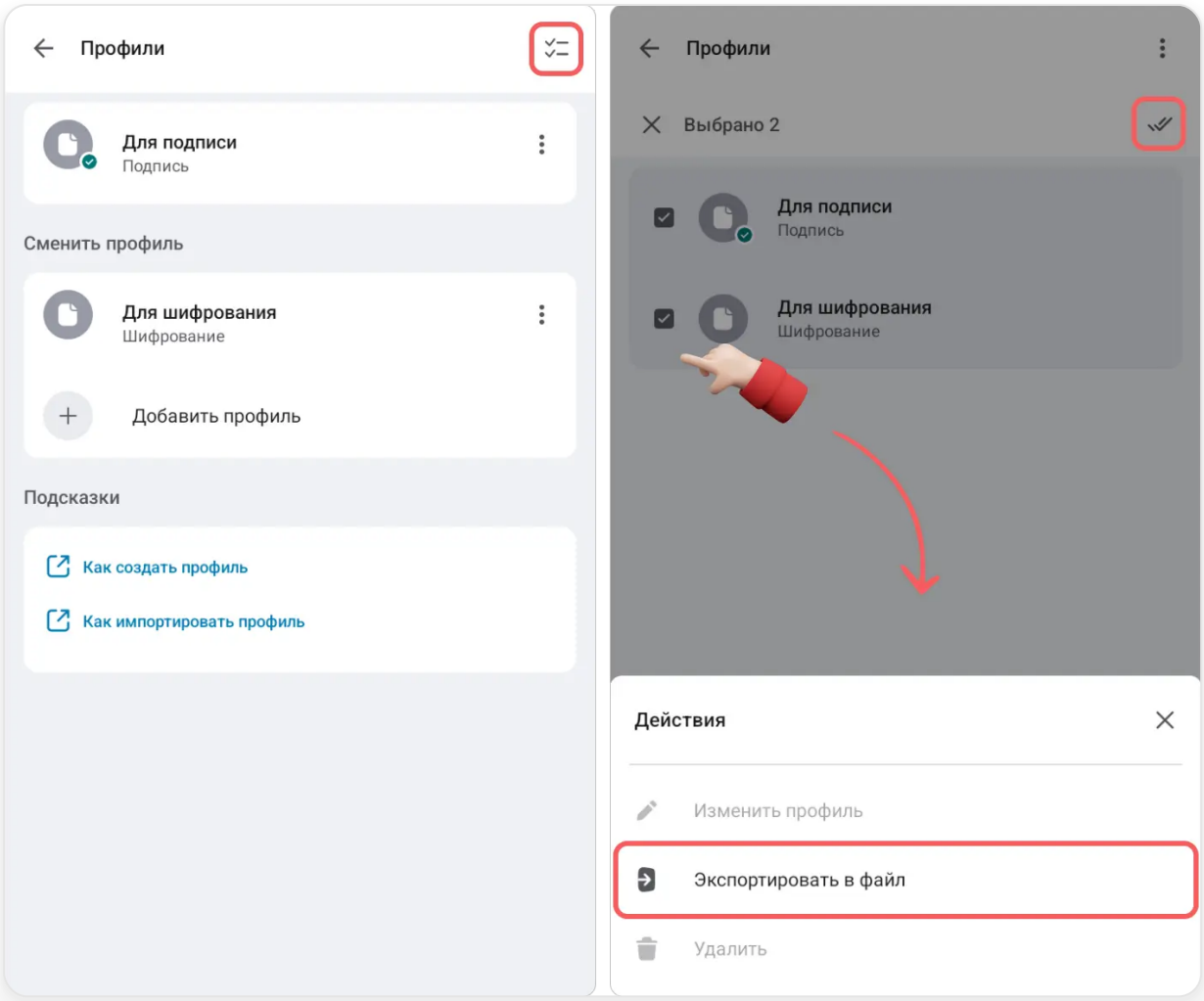
1. Экспорт профиля в файл

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Вызовите меню **Действия** по кнопке **Еще** , расположенной на панели с профилем, который необходимо экспортировать.
4. Выберите действие **Экспорт в файл**.
5. Откроется системное окно со списком приложений.
6. Выберите приложение для отправки или сохранения файла с профилем.

2. Групповой экспорт в файл

Чтобы экспортировать несколько профилей подписи:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Отметьте флажками профили одним из способов:
   - Нажмите на кнопку **Выбрать все** . В списке профилей отобразятся флажки. Установите флажки напротив тех профилей, которые необходимо экспортировать.
   - Нажмите и удерживайте панель профиля. Рядом с профилем появится флажок. Отметьте флажками другие профили.
4. Вызовите меню **Действия** по кнопке **Еще** , расположенной в верхней части окна.
5. Выберите действие **Экспорт в файл**.
6. Откроется системное окно со списком приложений.
7. Выберите приложение для отправки или сохранения файла с профилем.



Удаление профиля

1. Как удалить профиль

Чтобы удалить профиль подписи:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Вызовите меню **Действия** по кнопке **Еще** , расположенной на панели с профилем, который необходимо удалить.
4. Выберите действие **Удалить**.
5. Подтвердите действие в модальном окне. После удаления появится соответствующее уведомление.

2. Групповое удаление

Чтобы удалить несколько профилей подписи:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Отметьте флажками профили одним из способов:
   - Нажмите на кнопку **Выбрать все** . В списке профилей отобразятся флажки. Установите флажки напротив тех профилей, которые необходимо удалить.
   - Нажмите на панель с профилем и удерживайте ее. Напротив панели с профилем отобразится флажок. Отметьте флажками другие профили.
4. Вызовите меню **Действия**.
5. Выберите действие **Удалить**.
6. Подтвердите действие в модальном окне. После успешного удаления появится соответствующее уведомление.

Инструкции по теме

- Описание настроек профиля
- Как установить личный сертификат
- Как создать самоподписанный сертификат
- Как импортировать корневой или промежуточный сертификат

Открыть статью на сайте

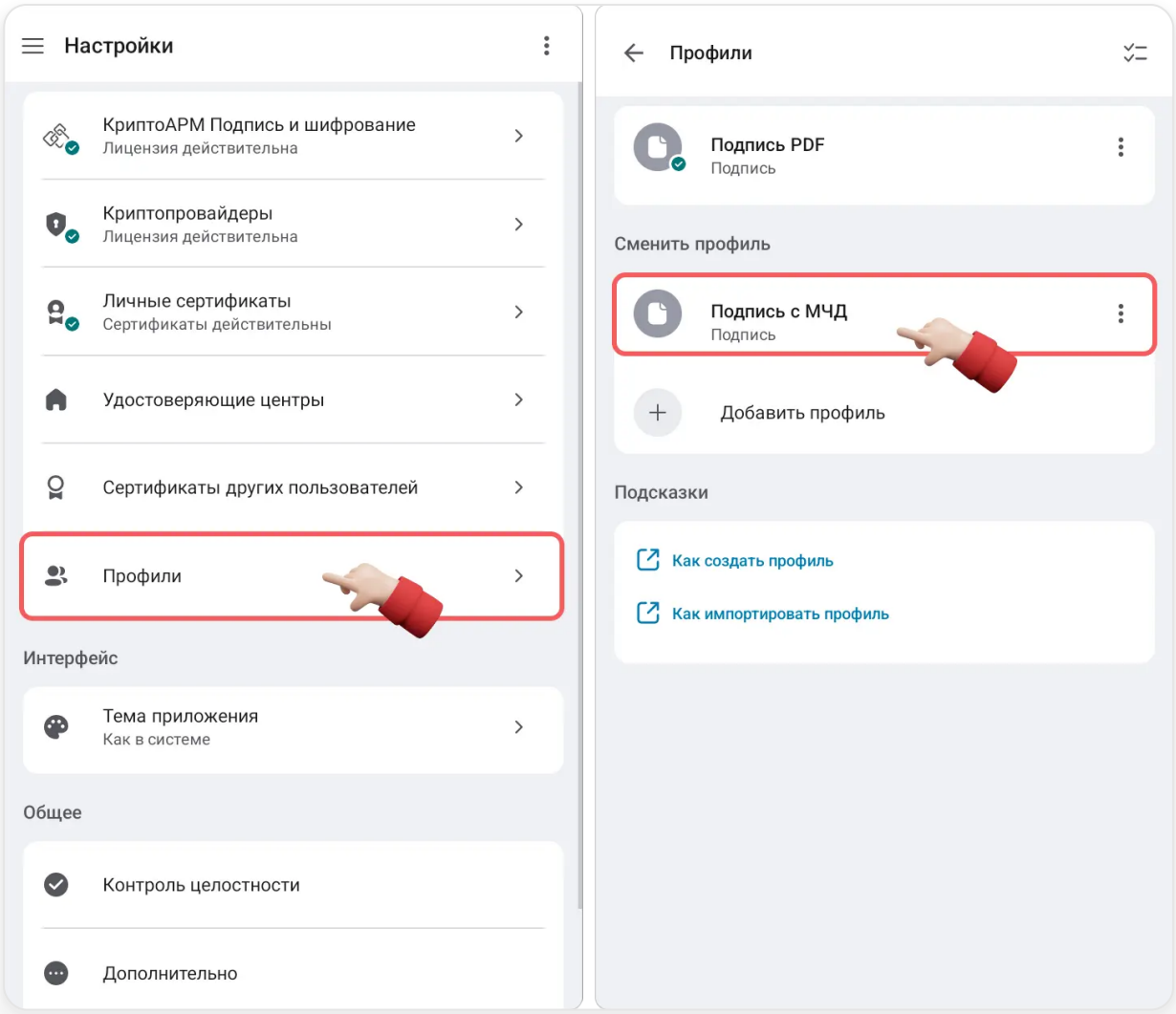
Настройки профиля в КриптоАРМ Подпись и шифрование

- Как открыть настройки профиля
- Настройки локального профиля
- Настройки сетевого профиля подписи
- Инструкции по теме

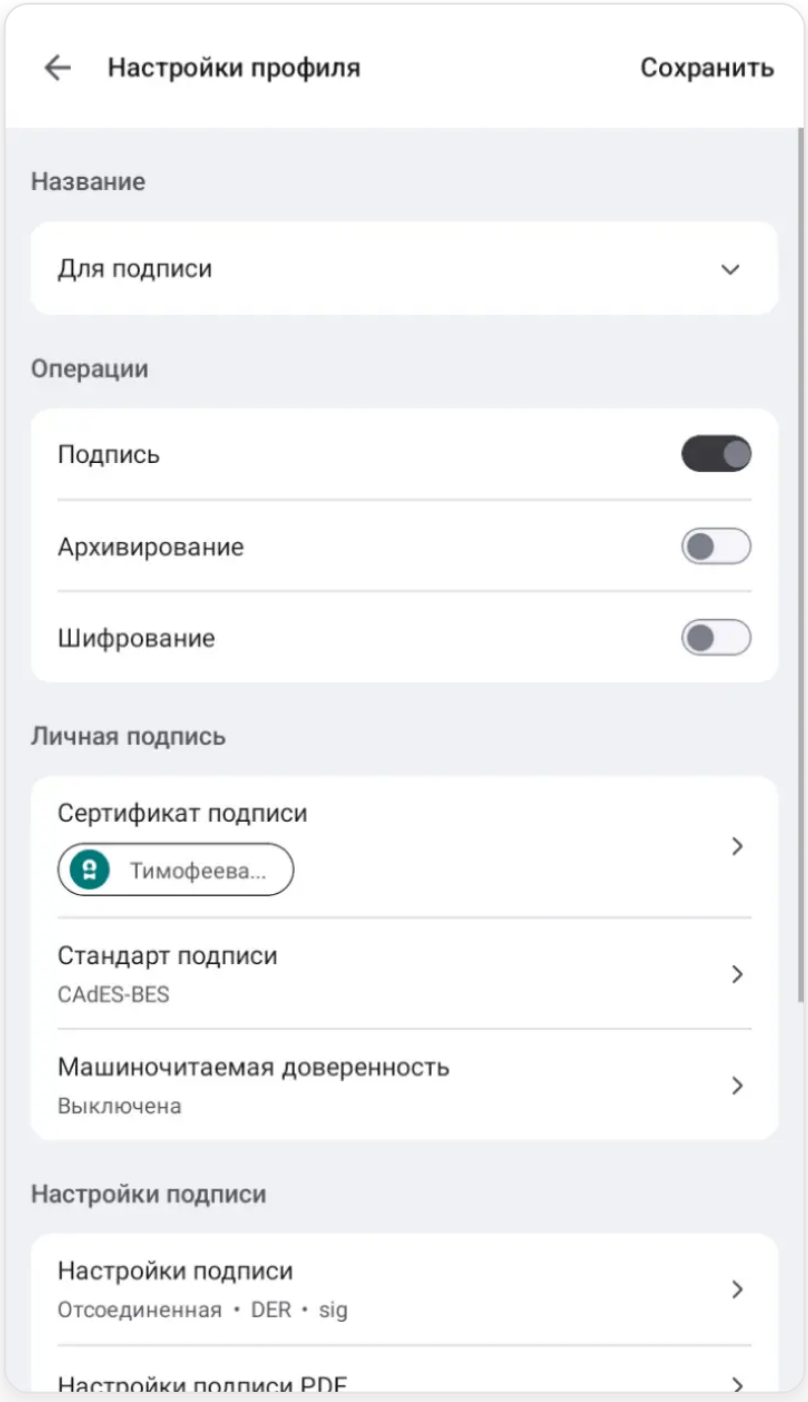
Как открыть настройки профиля

Чтобы открыть настройки профиля:

1. Перейдите в раздел **Настройки** → **Профили**.
2. В открывшемся списке найдите нужный профиль.



3. Нажмите на панель профиля, либо выберите **Изменить профиль** в меню действий с профилем.



💡 **Совет:** Профили также можно открывать и редактировать прямо в мастерах **Подпись и шифрование** и **Подпись и защита PDF**.

Настройки локального профиля

Операции

В разделе **Операции** можно выбрать действия, которые будут выполняться при обработке документов в мастере **Подпись и шифрование**.

Можно выбрать одну или несколько операций. Если выбрано несколько, они выполняются последовательно — в том порядке, в котором перечислены в настройках профиля:

1. **Подпись** — создание электронной подписи документа.
2. **Архивирование** — помещение документа в ZIP-архив.
3. **Шифрование** — шифрование документа.

Например, если выбраны операции **Подпись** и **Шифрование**, сначала документ будет подписан, а затем зашифрован.

Для настройки операций:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. В блоке **Операции** выберите необходимые операции.
3. Сохраните изменения профиля.

Личная подпись

В разделе **Личная подпись** указывается сертификат, которым будет подписан документ, стандарт подписи и машиночитаемая доверенность.

Сертификат подписи

Личный сертификат — сертификат из хранилища **Личные**, который используется для создания электронной подписи.

Чтобы выбрать сертификат:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. В разделе **Личная подпись** нажмите на **Сертификат подписи**.
3. В открывшемся окне выберите нужный сертификат.
4. Сохраните изменения профиля.

Стандарт подписи

В этом разделе можно выбрать стандарт электронной подписи и указать параметры служб, используемых при создании и проверке электронной подписи.

Чтобы настроить стандарт подписи:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. В разделе **Личная подпись** нажмите **Стандарт подписи**:

3. В открывшемся окне выберите нужный стандарт:
    - **CAdES-BES** — базовая электронная подпись без штампа времени.
    - **CAdES-T** — электронная подпись со штампом времени, который подтверждает существование подписи на указанную дату и время.
    - **CAdES-X Long Type 1** — усовершенствованная электронная подпись, которая содержит данные, необходимые для проверки ее действительности: сведения о времени подписания, информацию о статусе сертификата и подтверждение его действительности на момент подписания.
4. Если выбран стандарт **CAdES-T**, укажите адрес службы штампов времени (TSP). Его можно узнать у поставщика услуги. Адрес указывается в формате: `https://<сервер>[:порт][/путь]`.
5. Если выбран стандарт **CAdES-X Long Type 1**, помимо адреса службы штампов времен, укажите адрес службы онлайн-статусов. Поле необязательно для заполнения: как правило, адрес службы уже указан в сертификате подписи.
6. Сохраните изменения профиля.

Машиночитаемая доверенность

В этом разделе можно настроить добавление машиночитаемой доверенности (МЧД) к подписываемым документам. Доверенность прикладывается к подписанному пакету документов в мастерах **Подпись и шифрование** и **Подпись и защита PDF**. Кроме того, в мастере **Подпись и защита PDF** номер МЧД можно вывести в визуальном штампе.

Чтобы добавить МЧД:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. В разделе **Личная подпись** нажмите на **Машиночитаемая доверенность**.
3. В открывшемся окне включите опцию **Добавлять МЧД к подписываемым документам** и укажите путь к файлам:
    - **Файл МЧД** — XML-файл доверенности,
    - **Файл подписи** — файл электронной подписи доверителя в формате .sig.
4. Сохраните изменения профиля.

Настройки подписи CAdES

В разделе **Настройки подписи** можно настроить формат создания подписи, способ кодирования, расширение файла и действия при добавлении соподписи.

Чтобы настроить подпись CAdES:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.

2. В разделе **Настройки подписи** укажите:
   - **Вид подписи** — определяет, будет ли подпись храниться вместе с документом в одном файле (присоединенная) или отдельно от него (отсоединенная).
   - **Кодировка подписи** — определяет способ представления данных подписи: `DER` (бинарная кодировка) или `BASE-64` (текстовая кодировка).
   - **Формат файла подписи** — задает расширение файла, в котором будет сохранена подпись: `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin`.
   - **Действия при соподписи** — определяет, как будет добавлена новая подпись к документу, который был ранее подписан и добавлен в мастер из раздела «Архив»:
     - **Добавлять в исходный документ** — новая подпись добавляется непосредственно в исходный документ.
     - **Добавлять в копию исходного документа** — для добавления новой подписи создается копия исходного документа.
3. Сохраните изменения профиля.

Настройки подписи PDF (PAdES)

В этом разделе настраиваются параметры подписания PDF-документов: способ создания подписи, содержание и оформление визуального штампа, использование рукописной подписи, сертификация документа и создание печатной формы.

Способ подписания PDF

В этом разделе можно выбрать, каким способом будут подписываться PDF-документы: с помощью встроенной подписи PAdES или обычной подписи CAdES.

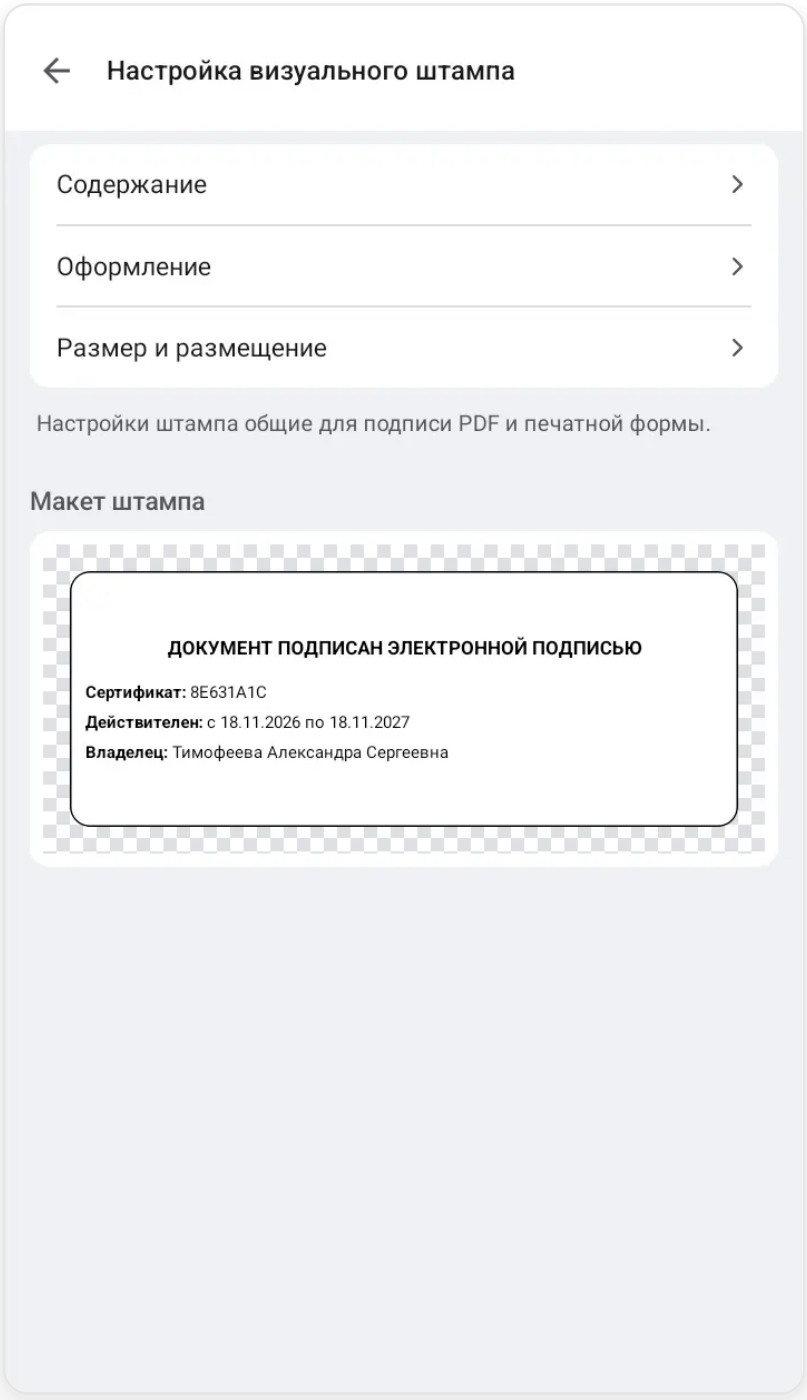
Чтобы настроить способ подписания PDF:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. Перейдите в раздел **Настройки подписи PDF** → **Способ подписания PDF** и выберите нужный вариант:
   - **Встроенная подпись PAdES** — встроенная подпись, которая добавляется непосредственно в PDF-документ. Дополнительно можно настроить визуальный штамп, изображение рукописной подписи и защиту от неразрешенных изменений.
   - **Обычная подпись CAdES** — подпись создается по стандарту CAdES. Дополнительно можно включить создание печатной формы с визуальным штампом и изображением рукописной подписи.
3. Сохраните изменения профиля.

Настройка визуального штампа

В этом разделе можно настроить содержание и оформление визуального штампа, а также его размер и расположение на странице PDF-документа.

> 📌 Настройки визуального штампа общие для встроенной подписи PAdES и печатной формы.



Содержание

В этом разделе можно выбрать, какие реквизиты будут отображаться в визуальном штампе.

Чтобы настроить содержание штампа:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.

2. Перейдите в раздел **Настройки подписи PDF** → **Настройка визуального штампа** → **Содержание**.

3. Настройте набор отображаемых реквизитов в штампе в подразделе **Отображение**:

   - **По ГОСТ** — для вывода реквизитов в соответствии с **ГОСТ Р 7.0.97-2016** (Заголовок «Документ подписан электронной подписью», серийный номер сертификата, имя его владельца и срок действия).
   - **Произвольно** — для ручной настройки выводимых полей и их значений.

> 📌 **Примечание:** по умолчанию в поле **Владелец** отображается общее имя (CN) из сертификата. Если в сертификате указано название организации, а в штампе необходимо отобразить ФИО подписанта, выберите тип штампа **Произвольно** и включите реквизит **ФИО**.

4. Сохраните изменения профиля.

Оформление

В этом разделе можно настроить внешний вид визуального штампа: добавить логотип, фон и рамку, выбрать цвет текста и рамки, а также задать непрозрачность.

Чтобы настроить оформление штампа:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. Перейдите в раздел **Настройки подписи PDF** → **Настройка визуального штампа** → **Оформление**.
3. В блоке **Логотип** загрузите изображение с гербом или эмблемой. Поддерживаются форматы .jpeg, .jpg и .png. Максимальный размер файла — 10 МБ.

4. В блоке **Фон и граница** при необходимости включите параметры:

   - **Добавить фон** — добавляет белый фон.
   - **Добавить рамку** — добавляет границу вокруг штампа.

5. В блоке **Цвет текста и рамки** выберите цвет текста и границы с помощью палитры или укажите HEX-код.

6. В блоке **Непрозрачность** настройте степень непрозрачности штампа.
7. Сохраните изменения профиля.

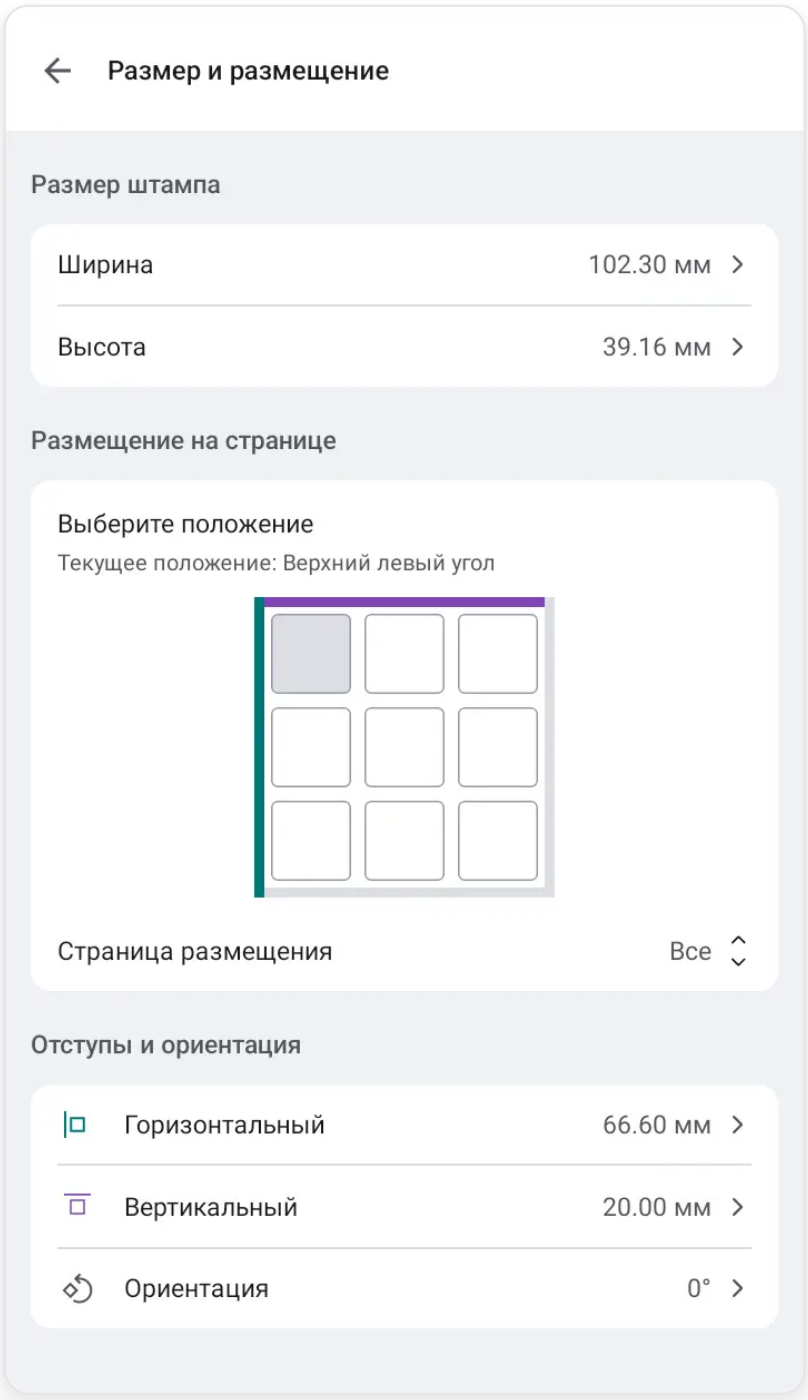
Размер и размещение

В этом разделе можно задать размеры визуального штампа, выбрать его положение на странице и настроить отступы.

Чтобы настроить размер и размещение штампа:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.

2. Перейдите в раздел **Настройки подписи PDF** → **Настройка визуального штампа** → **Размер и размещение**.



3. В блоке **Размер штампа** укажите ширину и высоту штампа в миллиметрах.
4. В блоке **Размещение на странице** выберите положение штампа и страницу, на которой он будет размещен.
5. В блоке **Отступы и ориентация** укажите координаты размещения штампа в миллиметрах и задайте его ориентацию.
6. Сохраните изменения профиля.

Настройка рукописной подписи

В этом разделе можно загрузить изображение рукописной подписи, а также настроить его размер и расположение на странице документа.

Рукописную подпись можно добавить в печатную форму вместе с визуальным штампом или непосредственно в PDF-документ без создания электронной подписи.

Чтобы настроить рукописную подпись:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. Перейдите в раздел **Настройки подписи PDF** → **Настройки рукописной подписи**.
3. Перейдите в блок **Изображение подписи** и загрузите изображение подписи. Поддерживаются форматы .jpeg, .jpg и .png. Максимальный размер файла — 10 МБ.
4. Перейдите в блок **Размер и размещение** и укажите:
   - ширину и высоту изображения подписи в миллиметрах,
   - положение изображения подписи и страницу размещения,
   - укажите координаты размещения в миллиметрах и значение для ориентации изображения подписи.
5. Сохраните изменения профиля.

Чтобы включить добавление рукописной подписи при создании встроенной подписи PAdES в мастерах **Подпись и шифрование** и **Подпись и защита PDF**, перейдите в раздел **Способ подписания PDF** и включите опцию **Добавить рукописную подпись**.

Чтобы включить добавление рукописной подписи в печатную форму при создании подписи CAdES, перейдите в раздел **Способ подписания PDF** и включите опцию **Добавить рукописную подпись** в блоке **Состав печатной формы**.

Защита и обработка PDF

В этом разделе можно включить сертификацию PDF-документа. Она позволяет определить, какие изменения разрешены после создания электронной подписи.

Чтобы включить сертификацию:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. Перейдите в раздел **Настройки подписи PDF** → **Защита и обработка PDF**.
3. Включите настройку **Сертификация**.
4. Сохраните изменения профиля.

Печатная форма

Печатная форма — это визуальная копия PDF-документа с изображением штампа и, при необходимости, рукописной подписи. Она создается отдельно от электронной подписи и не содержит криптографических данных, поэтому не подтверждает подлинность документа и не защищает его от изменений.

Создание печатной формы доступно при использовании обычной подписи CAdES в мастере **Подпись и шифрование**.

Чтобы включить создание печатной формы:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. Перейдите в раздел **Настройки подписи PDF** → **Способ подписания PDF** и выберите настройку **Обычная подпись CAdES**.
3. В блоке **Печатная форма** включите **Создать печатную форму для подписываемых PDF-документов**.
4. В блоке **Состав печатной формы** включите:
   - Добавить визуальный штамп,
   - Добавить рукописную подпись.
5. Сохраните изменения профиля.

Настройки шифрования

В этом разделе можно выбрать сертификаты получателей, для которых будет доступно расшифрование документов, а также настроить алгоритм шифрования и кодировку зашифрованных файлов.

Сертификаты шифрования — сертификаты получателей, с помощью которых можно будет расшифровать зашифрованный документ.

> 💡 **Совет**: добавьте в список получателей свой личный сертификат, если планируете самостоятельно расшифровывать документ после шифрования.

Чтобы настроить параметры шифрования:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. В блоке **Настройки шифрования** укажите:
   - **Сертификаты шифрования** — выберите сертификаты получателей, которым необходимо предоставить возможность расшифровать документ.
   - **Алгоритм шифрования** — выберите алгоритм, который будет использоваться для защиты данных: `ГОСТ 28147-89` (устаревший), `ГОСТ Р 34.12-2015 Магма`, `ГОСТ Р 34.12-2015 Кузнечик` (рекомендуется).
   - **Кодировка файлов** — выберите способ представления зашифрованных данных: `DER` или `BASE-64`.
3. Сохраните изменения профиля.

Сохранение результатов

В этом разделе можно настроить, куда будут сохраняться результаты обработки документов: в архив приложения или в выбранную папку на устройстве.

Чтобы настроить сохранение результатов:

1. Откройте настройки профиля, как описано в разделе Как открыть настройки профиля.
2. В блоке **Сохранение результатов** укажите нужные параметры:
   - **Сохранить в «Архив»** — включите эту опцию, если хотите сохранять результаты обработки документов в архиве приложения.
   - **Место сохранения** — выберите папку на устройстве, в которую будут сохраняться результаты обработки документов.
3. Сохраните изменения профиля.

Настройки сетевого профиля подписи

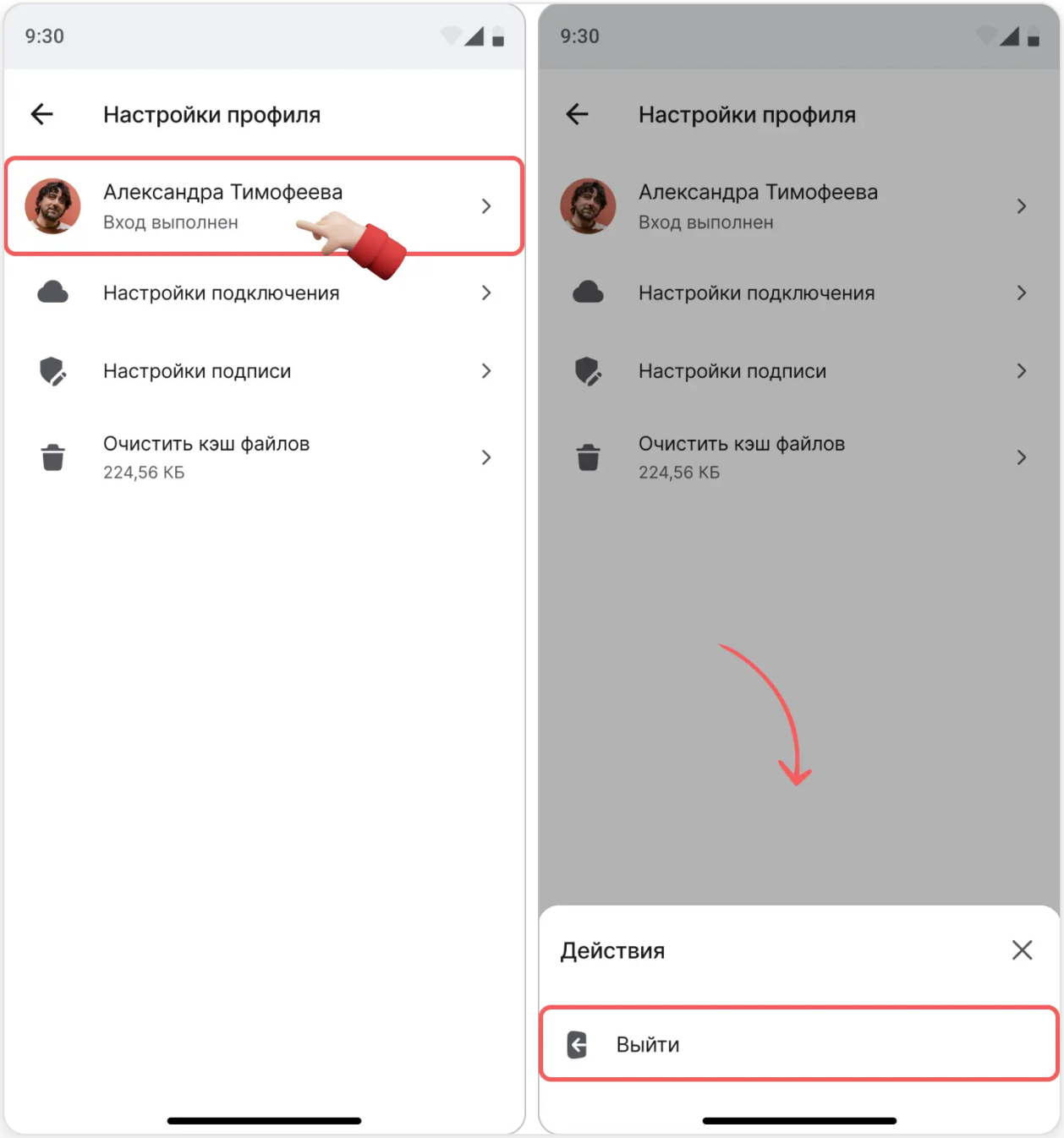
Сетевой профиль подписи предназначен для работы с документами в подключенной информационной системе. В его настройках можно управлять учетной записью и подключением к системе, задавать параметры электронной подписи и очищать кэш загруженных файлов.

Учетная запись

В разделе **Учетная запись** отображается информация об учетной записи, под которой выполнен вход в информационную систему, и текущий статус авторизации. Здесь также можно выйти из учетной записи.

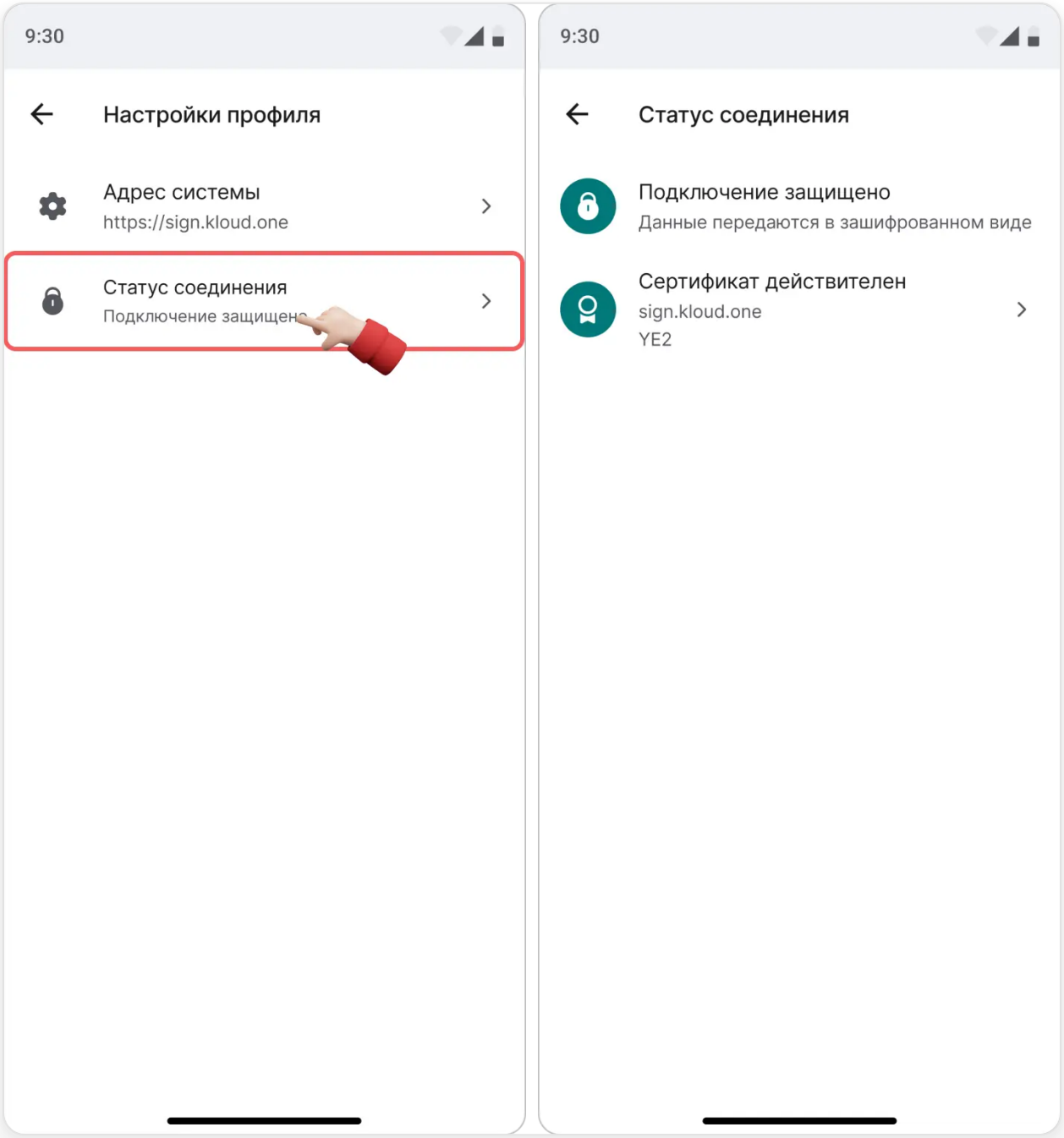
Чтобы выйти из учетной записи:

1. Откройте настройки сетевого профиля.
2. Нажмите на панель с учетной записью.
3. В открывшемся меню выберите действие **Выйти**.
4. Подтвердите действие в модальном окне.



Настройки подключения

В разделе **Настройки подключения** отображаются параметры подключения и текущий статус соединения.



Настройки подписи сетевого профиля

В разделе **Настройки подписи** можно настроить параметры электронной подписи и шифрования. Набор настроек аналогичен настройкам подписи в локальном профиле.

Очистка кэша

Чтобы очистить кэш:

1. Откройте настройки сетевого профиля.
2. Выберите действие **Очистить кэш файлов** и подтвердите действие.

После очистки кэша локальные копии загруженных файлов будут удалены с устройства. Список документов при этом сохранится, а файлы будут повторно загружены при следующем обращении к ним.

Инструкции по теме

- Управление профилями
- Как установить личный сертификат
- Как создать самоподписанный сертификат
- Как импортировать корневой или промежуточный сертификат

Открыть статью на сайте

Как настроить интерфейс в КриптоАРМ Подпись и шифрование

Тема приложения

В приложении поддерживается светлая и темная темы. Вы можете выбрать светлый, темный или системный (автоматический) режим в зависимости от времени суток или личных предпочтений.

> 💡 **Совет**: Темная тема снижает нагрузку на глаза при работе в условиях слабого освещения, а светлая обеспечивает лучшую читаемость документов днем.

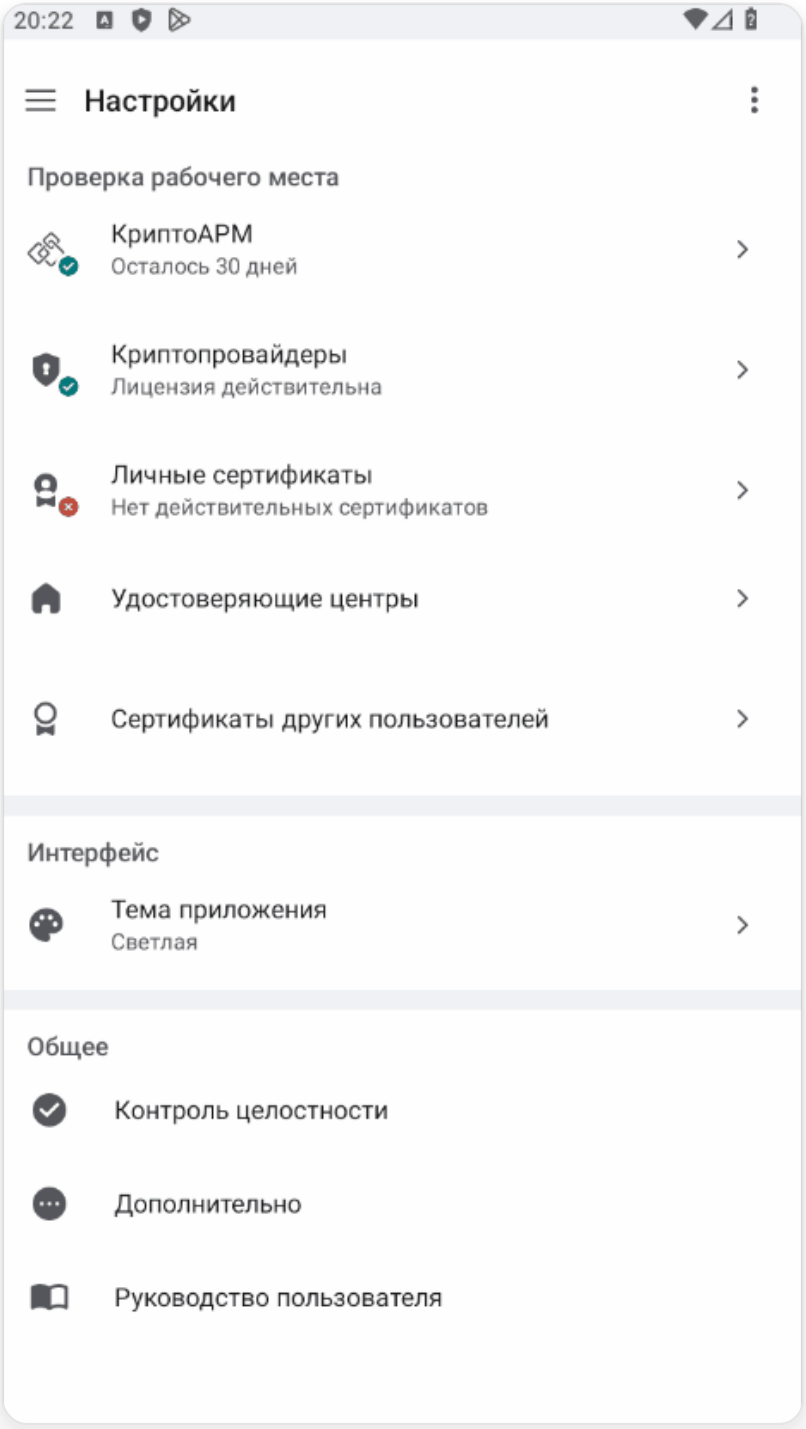
Изменение темы приложения

По умолчанию используется системная тема.

Чтобы изменить тему приложения:

1. Перейдите в раздел **Настройки**.
2. В блоке **Интерфейс** нажмите на панель **Тема приложения**.
3. В появившемся окне выберите необходимую тему.

   После выбора тема будет применена автоматически.



Инструкции по теме

- Лицензирование
- Проверка рабочего места
- Управление профилями
- Как установить личный сертификат

Открыть статью на сайте

Настройка безопасности и проверки ключей в КриптоАРМ Подпись и шифрование

- Контроль целостности приложения
- Проверка атрибута KeyAgreement
- Портал документации
- Инструкции по теме

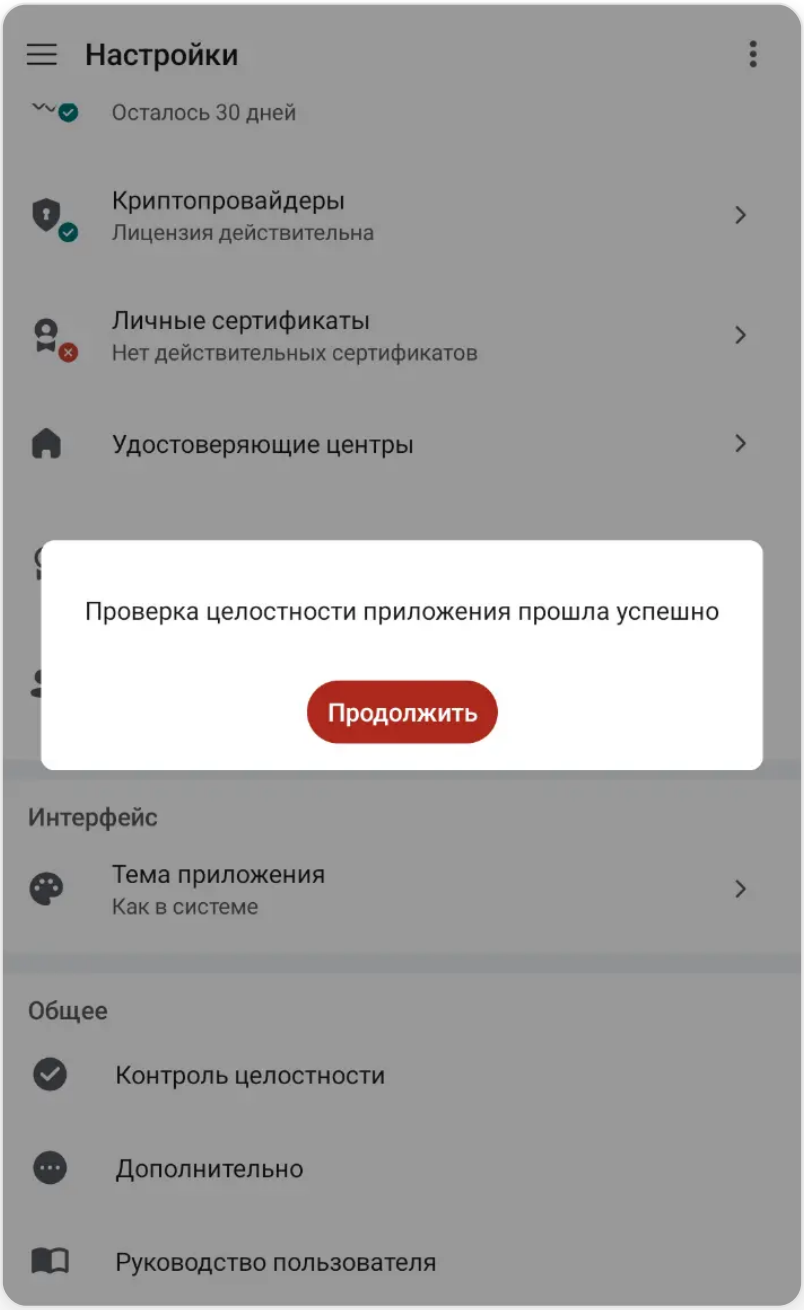
Контроль целостности приложения

> 💡 **Контроль целостности приложения** — это встроенный механизм безопасности, который проверяет, что файлы, реестр и конфигурация приложения не были изменены. Эта функция помогает защитить ваши данные и вовремя обнаружить возможное вмешательство.

Чтобы выполнить проверку:

1. Перейдите в раздел **Настройки**.
2. В блоке **Общее** нажмите **Контроль целостности**.
3. Дождитесь окончания проверки.

В результате проверки будет выведено уведомление со статусом.



Проверка атрибута KeyAgreement

Зачем нужна проверка

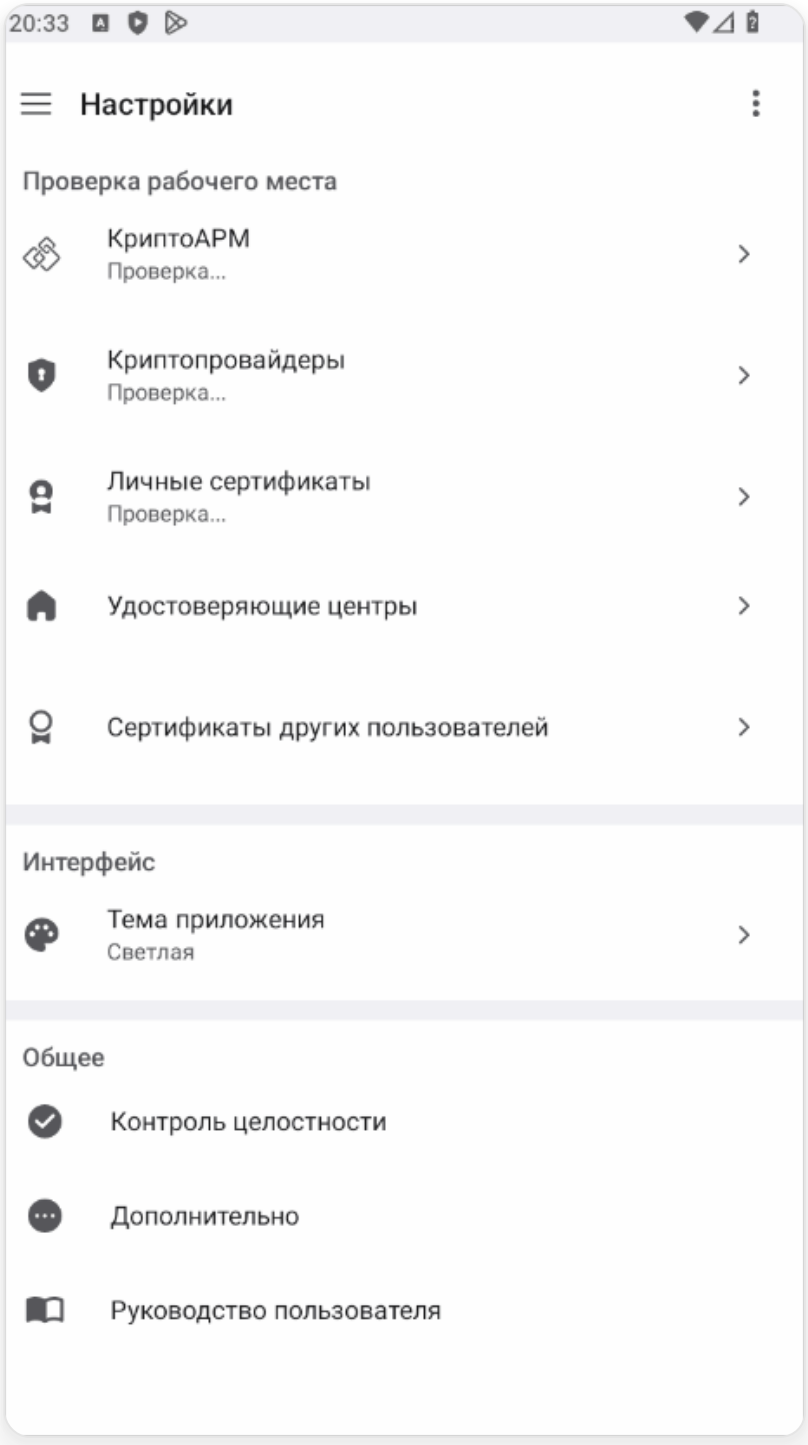
Атрибут **KeyAgreement** (согласование ключей) в расширении **keyUsage** указывает, что сертификат можно использовать для безопасного обмена ключами при шифровании.

- Если проверка включена, операция шифрования возможна только для сертификатов с атрибутом **KeyAgreement**.
- Если проверка отключена, допускается использование сертификатов с атрибутом **keyEncipherment** даже без «согласования ключей».

По умолчанию проверка **KeyAgreement** отключена.

Включение проверки KeyAgreement

1. Перейдите в раздел **Настройки**.
2. В блоке **Общее** нажмите **Дополнительно**.
3. Откроется окно с дополнительными настройками.
4. Нажмите на панель **Флаг keyAgreement**.
5. В появившемся окне выберите **Проверять**.



Портал документации

Руководство пользователя, ответы на часто задаваемые вопросы размещены на портале документации на сайте cryptoarm.ru.

Чтобы перейти на портал прямо из приложения:

1. Перейдите в раздел **Настройки**.
2. В блоке **Общее** нажмите на **Руководство пользователя**.
3. Откроется браузер с порталом документации КриптоАРМ.

Инструкции по теме

- Лицензирование
- Проверка рабочего места
- Управление профилями
- Как установить личный сертификат

Открыть статью на сайте

Обзор операций КриптоАРМ Подпись и шифрование

В этом разделе вы узнаете, как работать с документами в **КриптоАРМ Подпись и шифрование**: создавать подписи по стандартам CAdES и PAdES, шифровать файлы и выбирать подходящий мастер для конкретной задачи.

Этот обзор поможет быстро сориентироваться в возможностях приложения и перейти к нужному сценарию работы.

Содержание:

- Основные операции
- Электронная подпись в КриптоАРМ Подпись и шифрование
- Выбор мастера

Основные операции

В **КриптоАРМ Подпись и шифрование** все действия с документами выполняются в виде операций — последовательных процессов, которые позволяют создавать электронные подписи, шифровать файлы, проверять подписи и расшифровывать защищенные данные.

Операции выполняются с помощью мастеров — пошаговых инструментов, которые позволяют решать задачи. В рамках одной операции можно выполнять одну или несколько задач одновременно, например:

- только создание электронной подписи,
- создание подписи, архивирование и шифрование,
- расшифрование и проверка подписи.

Параметры операций можно сохранить в профиле подписи, чтобы в дальнейшем применять готовые настройки без повторной ручной конфигурации.

Электронная подпись в КриптоАРМ Подпись и шифрование

Электронная подпись используется для подтверждения подлинности, целостности и юридической значимости электронных документов.

Приложение **КриптоАРМ Подпись и шифрование** позволяет создавать подписи со стандартами:

- **CAdES** — для любых файлов (DOCX, XLSX, XML и других типов данных)
- **PAdES** — для PDF-документов с возможностью видимого штампа подписи

Выбор стандарта подписи зависит от типа документа, требований к его хранению и способа проверки подписи.

Ниже приведено краткое сравнение стандартов электронной подписи:

Стандарт	Для каких файлов	Тип подписи	Визуальный штамп
CAdES	Любые (docx, xlsx, pdf, xml и др.)	Отсоединенная / Присоединенная	Нет (кроме печатной формы)
PAdES	Только PDF	Встроенная	Да / Нет

Помимо электронной подписи, в **КриптоАРМ Подпись и шифрование** можно использовать изображение рукописной подписи. Оно используется для визуального оформления документа и не является электронной подписью: не подтверждает подлинность документа и не защищает его от изменений. Рукописную подпись можно использовать как при подписании PDF по стандарту PAdES, так и при создании печатной формы для CAdES.

Подпись со стандартом CAdES

CAdES используется для подписания файлов любых форматов. В зависимости от требований к документу можно создать:

- **CAdES-BES** — базовая подпись без меток времени;
- **CAdES-T** — подпись со штампом времени, подтверждающим момент создания подписи;
- **CAdES-X Long Type 1** — усовершенствованная электронная подпись, которая включает все необходимые данные для проверки ее действительности: сведения о времени подписания, информацию для подтверждения валидности подписи, а также подтверждение валидности сертификата подписанта на момент подписания.

Подпись CAdES может быть:

- **присоединенной** — подпись и документ объединяются в один файл;
- **отсоединенной** — подпись сохраняется отдельно (обычно с расширением `.p7s` или `.sig`), при этом исходный документ не изменяется.

Такой подход позволяет выбрать оптимальный вариант хранения и передачи документов в зависимости от требований процесса.

Печатная форма

Для PDF-документов, подписываемых подписью CAdES, доступно создание печатной формы.

Печатная форма — это PDF-документа с визуальным отображением штампа электронной подписи и, при необходимости, изображения рукописной подписи. Она не содержит электронную подпись и криптографические данные.

> ⚠️ **Примечание**: печатная форма предназначена только для визуального ознакомления с документом. Она не подтверждает подлинность документа и не заменяет электронную подпись.

Подпись со стандартом PAdES

PAdES — стандарт электронной подписи для PDF-документов. Подпись встраивается непосредственно в PDF-файл, поэтому отдельный файл подписи не создается. Подписанный документ сохраняет формат PDF и открывается в обычных просмотрщиках PDF.

> 📌 В текущей версии **КриптоАРМ Подпись и шифрование** при подписании PDF-документа по стандарту PAdES создается видимая подпись с визуальным штампом. Дополнительно можно добавить изображение рукописной подписи.

В КриптоАРМ доступны подписи PAdES без меток времени, подписи со штампом времени, а также усовершенствованный вариант.

Сертифицирующая подпись PDF

Сертифицирующая подпись — особый тип электронной подписи, который устанавливается в PDF-документ первой и определяет правила его дальнейшего изменения.

При сертификации можно разрешить отдельные действия, например добавление последующих подписей или изменение определенных элементов документа.

После установки сертифицирующей подписи создать новую область для подписи нельзя. Подписать документ другим сертификатом можно только в области, которая была размечена заранее.

Если документ изменен способом, не предусмотренным установленными правилами, сертифицирующая подпись становится недействительной.

Рукописная подпись

Рукописная подпись — это изображение подписи, которое можно добавить в PDF-документ. Она предназначена для визуального оформления документа и сама по себе не является электронной подписью: не подтверждает подлинность документа и не защищает его от изменений.

В **КриптоАРМ Подпись и шифрование** рукописную подпись можно использовать двумя способами:

- **Самостоятельно** — добавить изображение рукописной подписи в PDF-документ и сохранить его без создания электронной подписи.
- **Вместе с электронной подписью** — добавить изображение рукописной подписи при создании PAdES-подписи или печатной формы для CAdES.

Рукописную подпись можно создать непосредственно в приложении, нарисовав ее пальцем на экране, или использовать изображение и настройки, сохраненные в профиле подписи. Подробнее про ручное создание рукописной подписи читайте в инструкции Настройки профиля в КриптоАРМ Подпись и шифрование.

Выбор мастера

Выбор мастера в **КриптоАРМ Подпись и шифрование** зависит от типа документа и выполняемой операции. Ниже приведено краткое описание основных мастеров и сценариев их использования.

- Подпись и шифрование — предназначен для групповой работы с файлами. Позволяет подписывать и шифровать несколько документов одновременно, создавать архивы и использовать стандарты CAdES и PAdES.
- Подпись и защита PDF — подходит для работы с одним PDF-документом. Предоставляет инструменты просмотра, проверки подписей, разметки областей и добавления новых подписей в одном интерфейсе.

Задача / Сценарий	Рекомендуемый мастер	Почему
Подписать / зашифровать **много файлов** сразу	Подпись и шифрование	Групповая обработка, CAdES + PAdES, архивы, шифрование
Работать с **одним PDF**: просмотр, подпись, проверка подписи	Подпись и защита PDF	Встроенный просмотрщик, автоматическая проверка подписей, сертификация
Проверить подпись / расшифровать документ	Подпись и шифрование	Автоматически определяет тип файла и выполняет необходимые действия
Добавить еще одну подпись к уже подписанному файлу	Подпись и шифрование или Подпись и защита PDF	-

---

Инструкции по теме

- Как создать профиль подписи
- Как подписать документ

- Как зашифровать документ
- Как проверить подпись документа
- Как добавить подпись к файлу (соподпись)
- Как снять подпись с файла

Открыть статью на сайте

Как подписать документы в КриптоАРМ Подпись и шифрование

- Как подписать документы
- Возможные ошибки при подписании документов
- Инструкции по теме

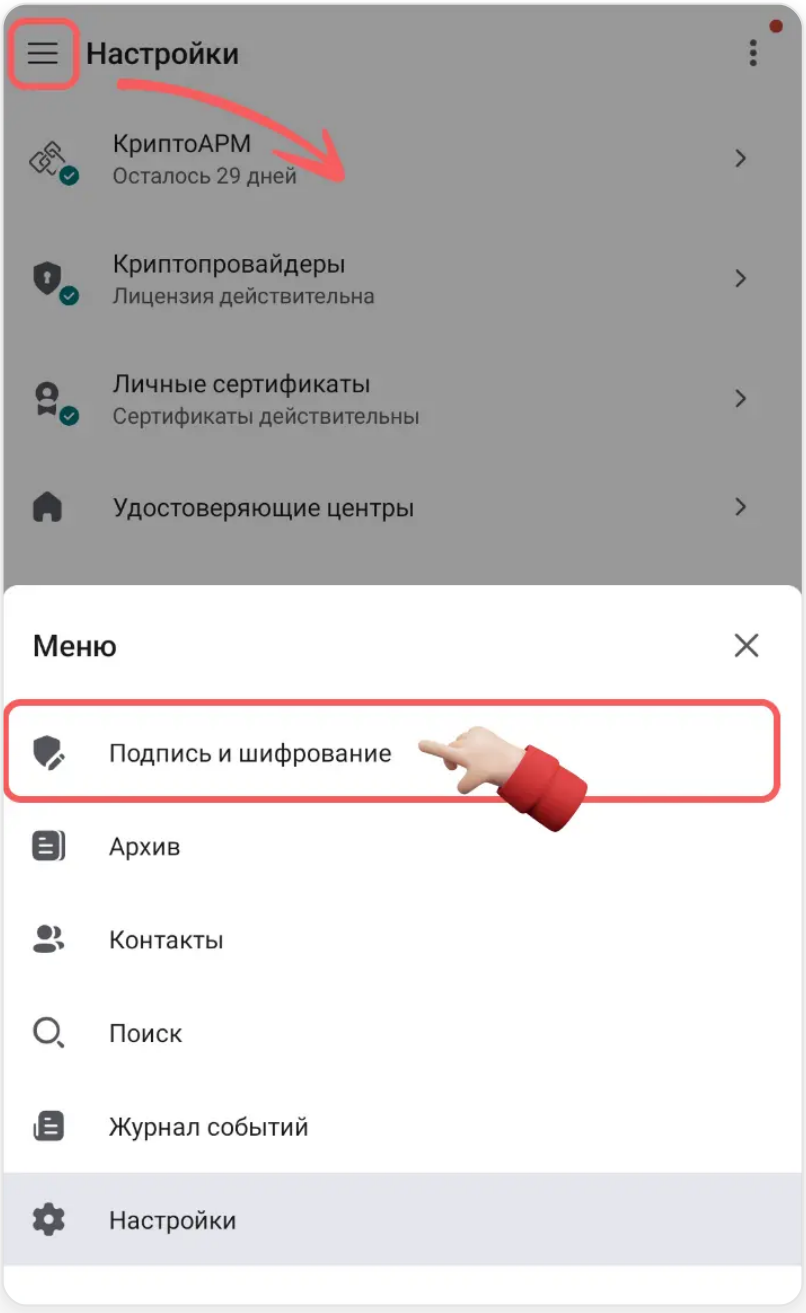
Как подписать документы

В этой инструкции описан порядок подписания документов в мастере **Подпись и шифрование**. С его помощью можно подписать как один документ, так и несколько документов за одну операцию (групповое подписание).

> 💡 **Совет**: Чтобы оценить, готово ли ваше рабочее место для подписи документов, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Откройте главное меню по кнопке .
2. Выберите пункт **Подпись и шифрование**.

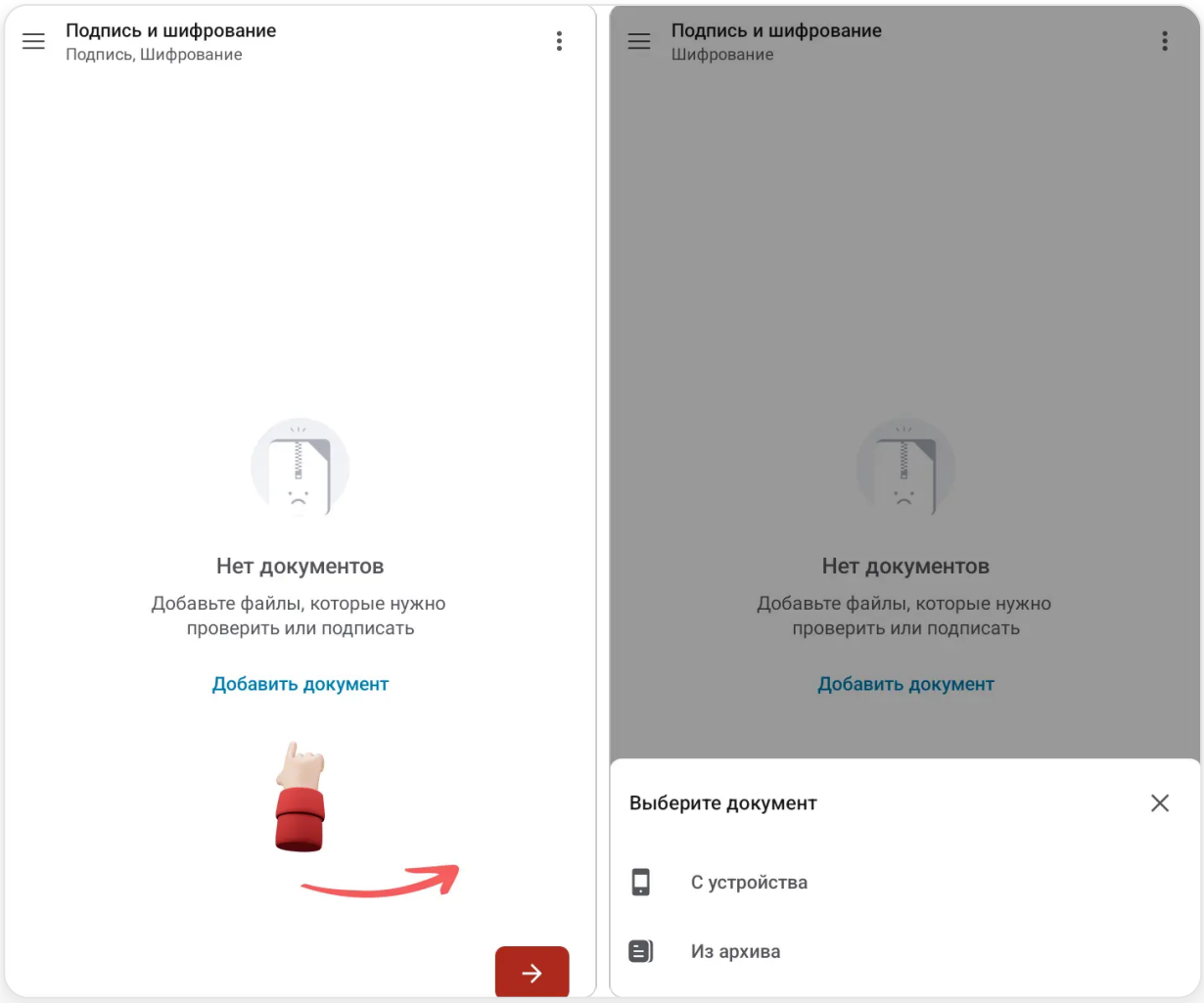


Шаг 2. Добавление документов

Добавить документы можно непосредственно из мастера или передать их из стороннего приложения.

Из мастера

1. В окне **Подпись и шифрование** нажмите на кнопку **Добавить документ**.
2. В появившемся меню выберите:
   - **С устройства** — для выбора файлов, сохраненных на устройстве,
   - **Из архива** — для выбора файлов, сохраненных в разделе **Архив**.



> 💡 **Совет**: Если вы уже находитесь в разделе **Архив**, выберите один или несколько файлов и нажмите на **Добавить в «Подпись и шифрование»**.

Из сторонних приложений

1. Выберите файлы в любом стороннем приложении.
2. Нажмите **Открыть с помощью** и выберите **КриптоАРМ**.

> 💡 **Совет**: Ненужный файл можно удалить из списка через меню **Еще** → **Удалить**.

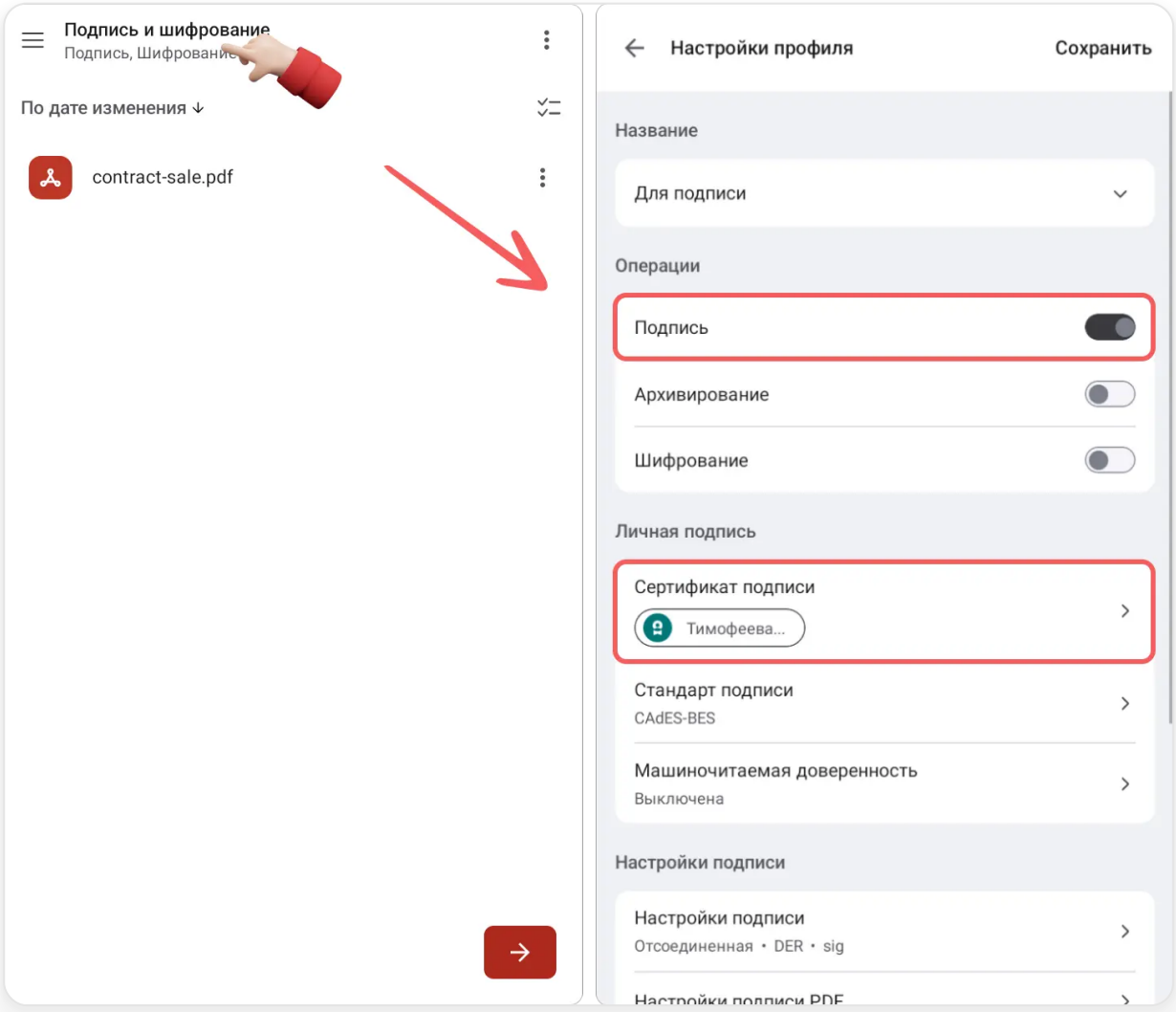
Шаг 3. Настройка параметров подписи

Для настройки операции используется активный профиль. По умолчанию мастер применяет сохраненные в нем параметры.

> 💡 **Профиль** — это сохраненный набор настроек подписи. Используя профили, вы можете быстро переключаться между разными сценариями. Подробнее о профилях читайте в инструкции Управление профилями.

Чтобы изменить параметры операции:

1. Нажмите на название профиля в верхней части экрана.
2. Откроется окно с настройками.
3. Убедитесь, что операция **Подпись** активна.
4. В блоке **Личная подпись** выберите **сертификат подписи**. Для этого нажмите на соответствующую панель и в открывшемся окне укажите один из личных сертификатов.



Дополнительно можно:

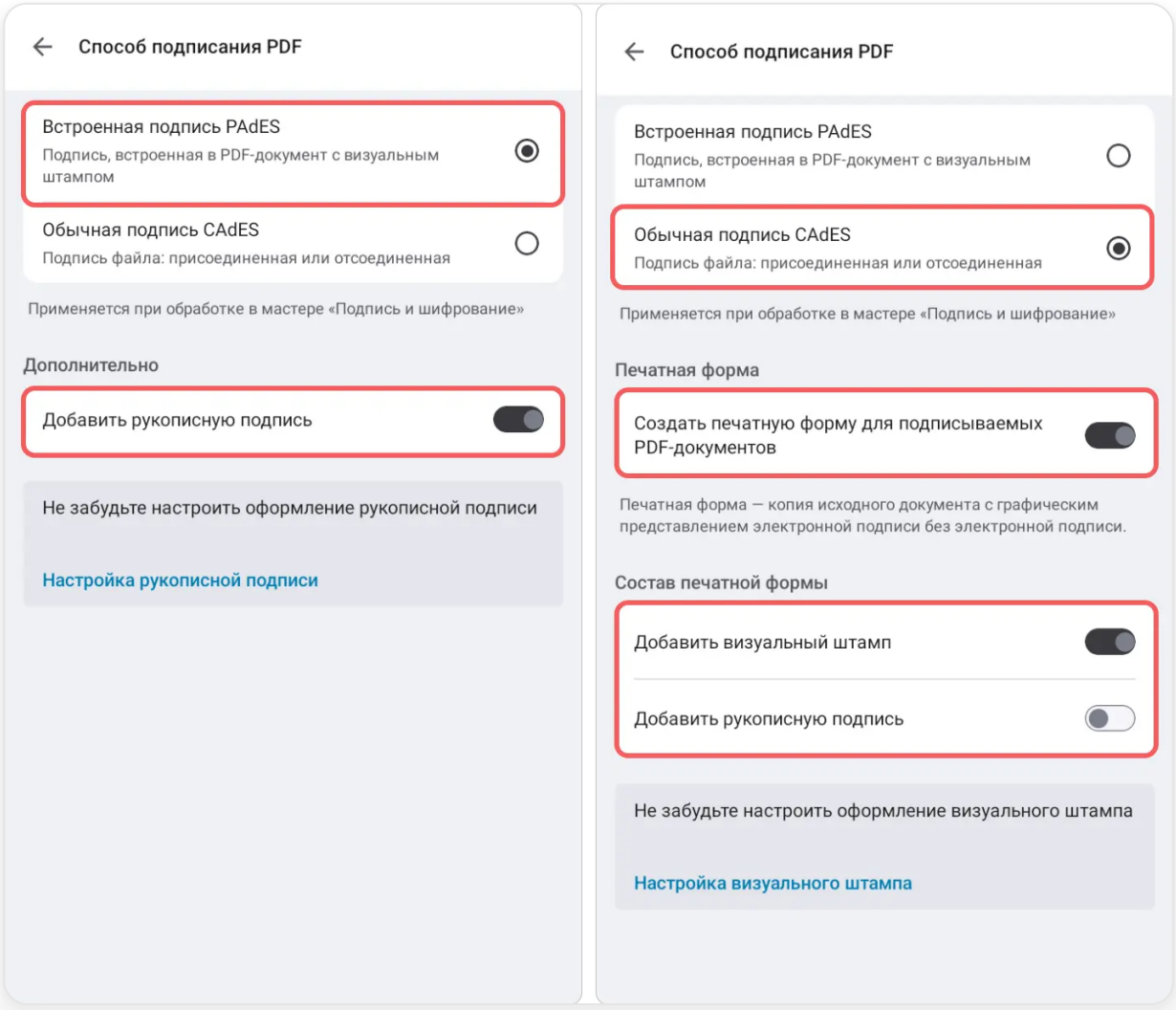
- указать машиночитаемую доверенность (МЧД),
- выбрать стандарт подписи.

> 💡 **Совет**: Чтобы создать подпись с меткой времени, выберите стандарт подписи **CAdES-X Long Type 1** или **CAdES-T** и настройте службы штампов времени. Подробнее о настройке читайте в инструкции Настройки для стандартов со штампами.

5. В блоке **Настройки подписи** при необходимости укажите тип и кодировку подписи, а также настройте расширение файла подписи.

6. Если среди добавленных документов есть PDF, в блоке **Настройки подписи PDF** выберите **Способ подписания PDF**:

   - **Встроенная подпись PAdES** — встроенная подпись, которая добавляется непосредственно в PDF-документ. Дополнительно можно настроить визуальный штамп, изображение рукописной подписи и защиту от неразрешенных изменений.
   - **Обычная подпись CAdES** — подпись создается по стандарту CAdES. Дополнительно можно включить создание печатной формы с визуальным штампом и изображением рукописной подписи.

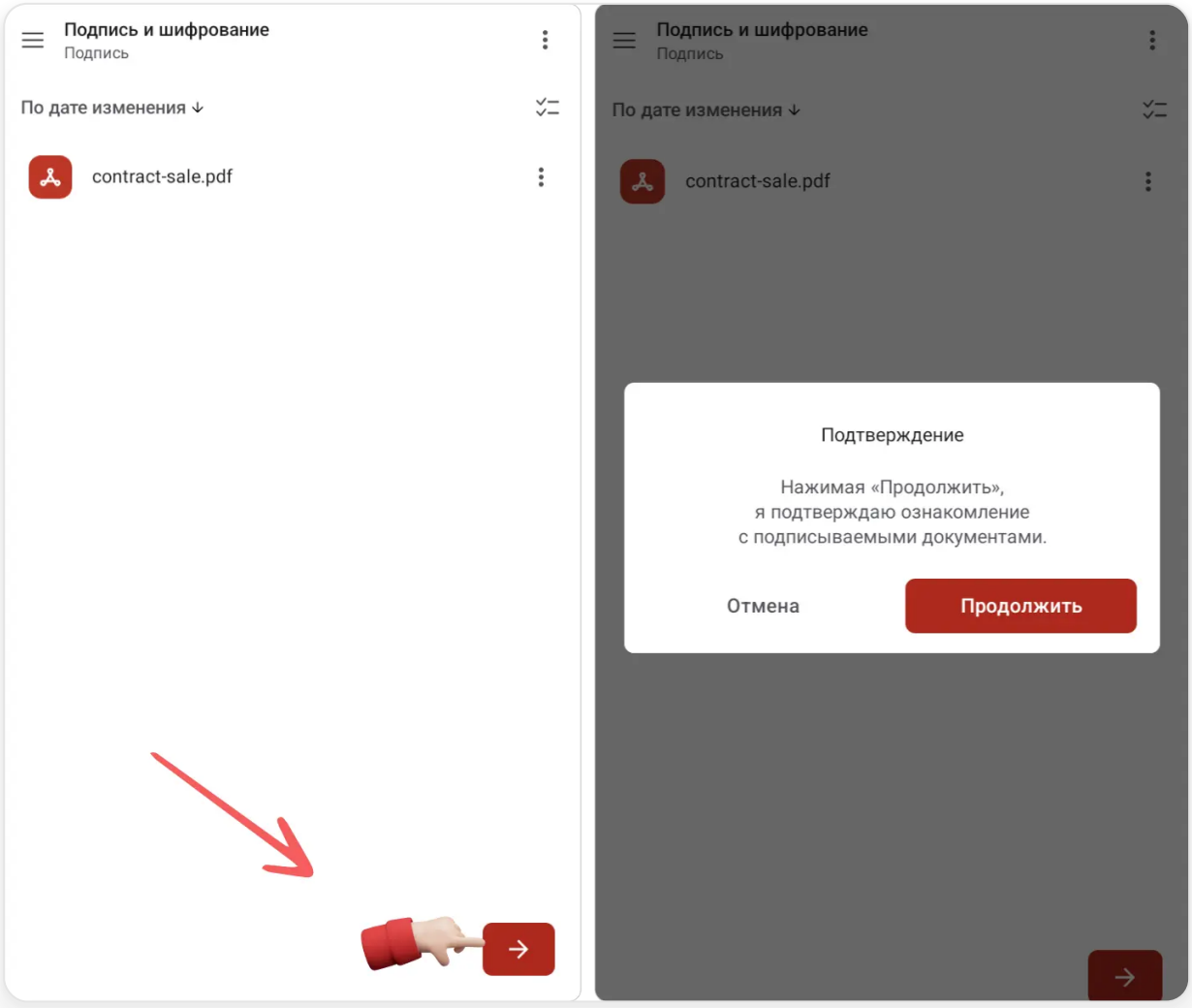


7. При необходимости включите сохранение копии подписанных файлов с помощью настройки **Сохранить в «Архив»**
8. Примените настройки профиля.

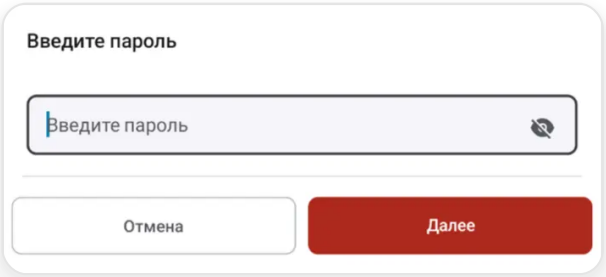
> 💡 **Совет**: Чтобы переключить профиль, нажмите кнопку ⌄ рядом с его названием и выберите нужный профиль из выпадающего списка.

Шаг 4. Подтверждение и выполнение операции

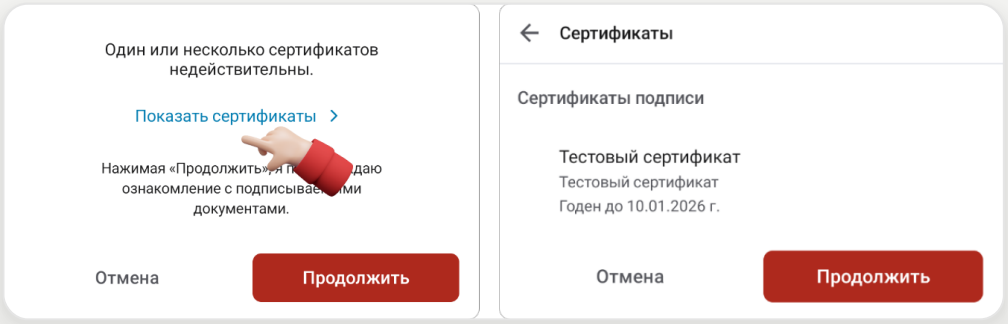
1. Нажмите кнопку **Выполнить** в нижней части окна **Подпись и шифрование**.
2. В окне подтверждения нажмите **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.



3. Если контейнер закрытого ключа защищен паролем, необходимо ввести его.



🚨 Если сертификат подписи недействителен, будет показано предупреждение. Подпись все равно будет выполнена, но ее юридическая значимость может быть поставлена под сомнение.



Шаг 5. Результат

Время выполнения операции зависит от количества документов и производительности устройства.

- Если операция выполнена успешно, на панели с файлом отобразится статус **Подписан**.
- Если в профиле была активна настройка **Сохранить в «Архив»**, то подписанные документы будут сохранены в указанную папку раздела **Архив**.
- Если в настройках профиля выбрана отсоединенная подпись, то в раздел **Архив** помимо файла подписи сохранится копия исходного файла.
- Если включено создание печатной формы, в раздел **Архив** дополнительно сохранится копия документа с визуальным отображением штампа электронной подписи и рукописной подписи, если она была настроена.

💡 В окне с результатами операции вы можете ознакомиться с информацией о подписи и поделиться файлами.

Возможные ошибки при подписании документов

Уведомления об ошибках отображаются в нижней части экрана.

Просмотр подробной информации доступен в разделе **Журнал событий**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Общие ошибки

Ошибка	Описание	Рекомендуемые действия
Ошибка при подписи файла	Файлы недоступны или имеют нулевой размер	1. Проверьте наличие и доступность файлов. Добавьте файлы в мастер повторно 2. Убедитесь, что файлы не пустые 3. Освободите место на устройстве
Произошла ошибка	Введен неверный пароль для доступа к закрытому ключу	Повторно введите пароль от контейнера закрытого ключа. Убедитесь, что пароль указан правильно.
Произошла ошибка	Не обнаружена действующая лицензия криптопровайдера КриптоПро CSP	1. Приобретите лицензию КриптоПро CSP 2.Установите лицензию в настройках приложения.
Произошла ошибка	Не построилась цепочка доверия для сертификата TSP-сервера	Убедитесь, что в приложении установлены все сертификаты, входящие в цепочку доверия TSP-сервера (корневой и промежуточные)
Отсутствует лицензия на приложение КриптоАРМ	Истек срок действия или не активирована лицензия КриптоАРМ	1. Приобретите лицензию КриптоАРМ 2. Установите лицензию в настройках приложения
Выберите сертификат подписи	Не выбран сертификат для выполнения операции подписи	Выберите сертификат в профиле подписи
Не указан адрес службы TSP	Отсутствуют настройки сервера штампов времени	Укажите корректный адрес TSP-сервера в профиле подписи
Произошла ошибка		

Ошибка	Описание	Рекомендуемые действия
	Проблема с подключением к серверу штампов времени. Сервер недоступен или адрес неверный.	1. Проверьте правильность введенного адреса 2. Убедитесь в доступности сервера
Выбранный сертификат подписи не подходит для усовершенствованной подписи	Несоответствие характеристик сертификата требованиям стандарта	Выберите подходящий сертификат или измените настройки стандарта подписи
Произошла ошибка	Отсутствует сетевое подключение	Проверьте подключение

Ошибки при подписании PDF (PAdES и печатная форма)

Ошибка	Описание	Рекомендуемые действия
Не удалось подписать файл: Страница не найдена	Указанный номер страницы для размещения штампа подписи отсутствует в документе	1. Проверьте общее количество страниц в PDF 2. Укажите существующий номер страницы
Не удалось подписать файл	Размер или положение штампа выходят за границы страницы документа.	Уменьшите размер штампа или сдвиньте его ближе к центру страницы
Не удалось подписать файл	Возможно, файл имеет ограничения на редактирование, чтение или подпись	1. Запросите у отправителя пароль для снятия защиты 2. Попросите предоставить незащищенную версию
Не удалось подписать сертифицированный документ	Файл уже содержит сертифицирующую подпись, запрещающую дальнейшие изменения	Запросите у владельца исходную (не сертифицированную) версию

Инструкции по теме

- Как создать профиль подписи
- Как установить личный сертификат
- Как зашифровать документ
- Как проверить подпись документа
- Как добавить подпись к файлу (соподпись)
- Как снять подпись с файла

Открыть статью на сайте

Как подписать и защитить PDF

- Как подписать PDF-документ
- Как создать сертифицирующую подпись
- Как поставить подпись в размеченную область
- Как поставить рукописную подпись
- Как проверить подпись PDF-документа
- Возможные ошибки при подписании документов
- Инструкции по теме

Как подписать PDF-документ

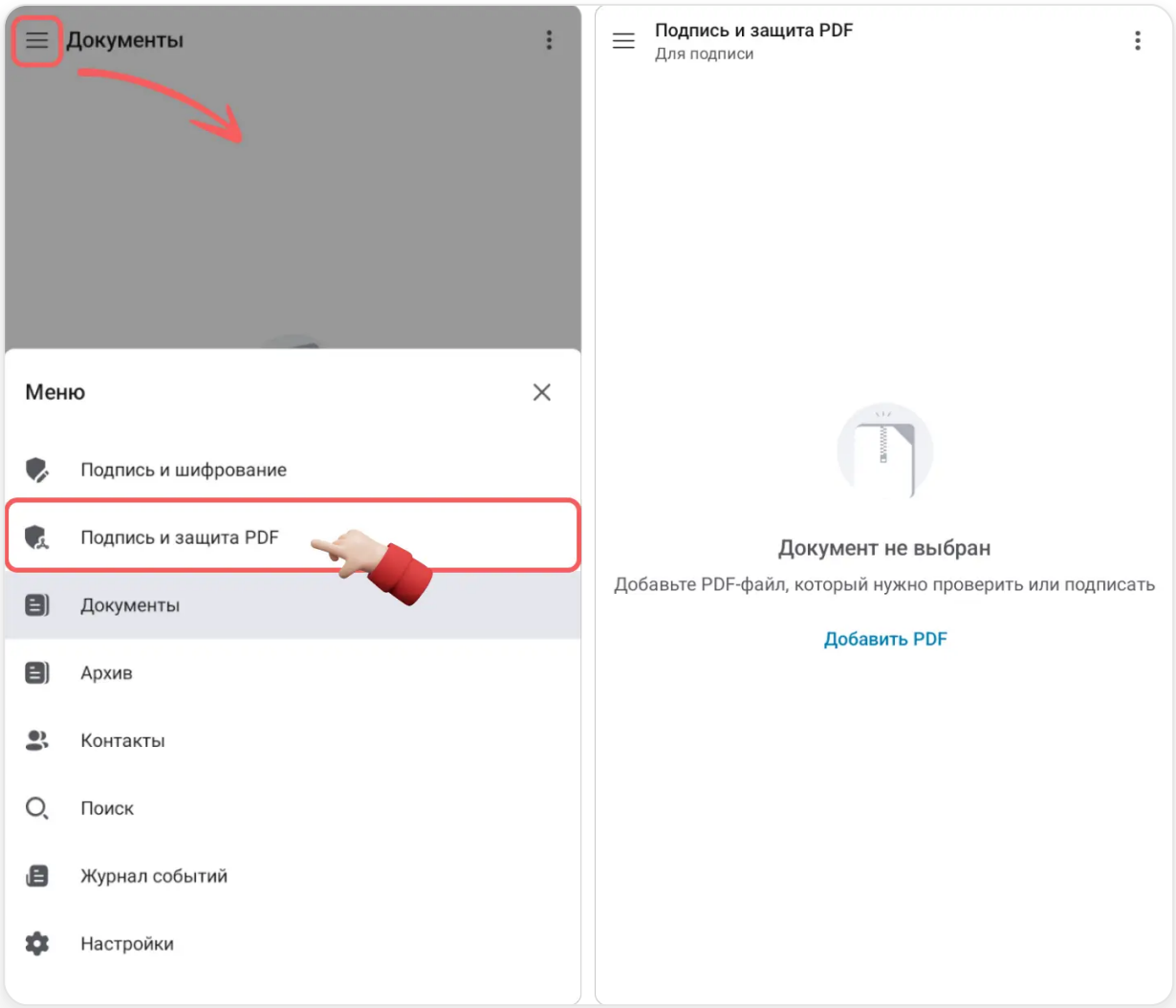
В этой инструкции описан порядок подписания PDF-документа в мастере **Подпись и защита PDF**. С его помощью можно подписать один документ за одну операцию, создав обычную или сертифицирующую подпись с визуальным штампом.

Чтобы подписать несколько PDF-документов за одну операцию, воспользуйтесь мастером Подпись и шифрование. Он поддерживает групповые операции подписания, архивирования и шифрования, а также работу со стандартами CAdES и PAdES.

> 💡 **Совет**: Чтобы проверить готовность рабочего места к подписанию документов, воспользуйтесь инструкцией Проверка рабочего места.

Шаг 1. Запуск мастера

1. Откройте главное меню по кнопке .
2. Выберите пункт **Подпись и защита PDF**.



Шаг 2. Открытие PDF-документа

Открыть PDF-документ в мастере можно несколькими способами.

Из мастера

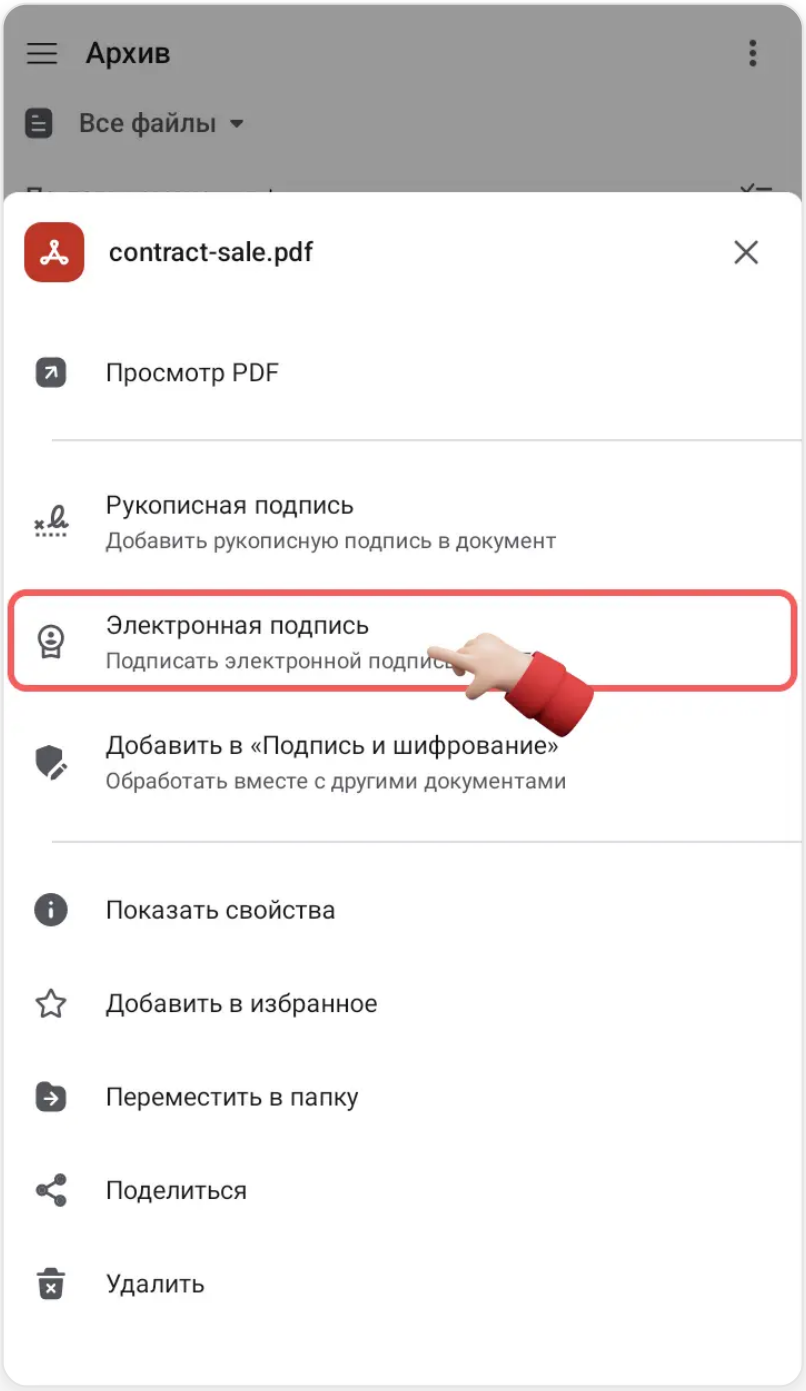
1. В окне **Подпись и защита PDF** нажмите **Добавить PDF**.
2. В появившемся меню выберите:
   - **С устройства** — для выбора файла, сохраненного на устройстве,
   - **Из архива** — для выбора файла, сохраненного в разделе **Архив**.

> 💡 **Совет**: Если вы уже находитесь в разделе **Архив**, выберите нужный файл и нажмите **Электронная подпись** в меню действий с файлом.

Из других разделов приложения

1. Откройте меню действий с файлом в другом разделе приложения.

2. Выберите **Электронная подпись**.



Из сторонних приложений

1. Выберите PDF-файл в любом стороннем приложении.
2. Нажмите **Открыть с помощью** и выберите **КриптоАРМ**.

Шаг 3. Просмотр PDF-документа

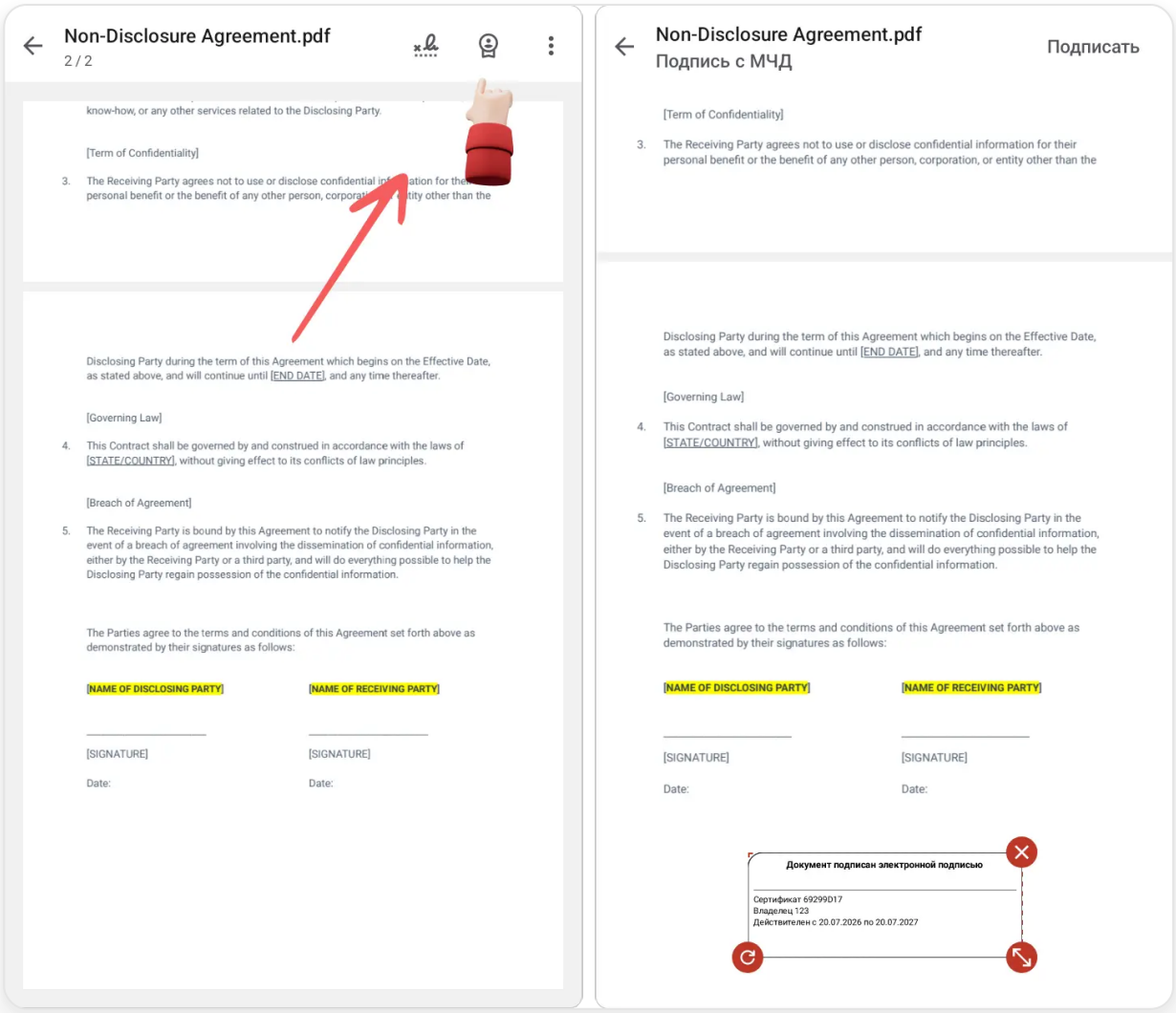
После добавления в мастер PDF-документ откроется в режиме просмотра.

Если документ содержит электронные подписи, **КриптоАРМ Подпись и шифрование** автоматически запустит их проверку. Подробнее об этом читайте в разделе Как проверить подпись PDF-документа.

Чтобы перейти к настройке подписи:

1. Нажмите **Электронная подпись** в верхней части окна.
2. Откроется редактор, в котором применятся настройки активного профиля подписи.

> 💡 **Профиль** — это сохраненный набор настроек подписи. Используя профили, вы можете быстро переключаться между разными сценариями. Подробнее про профили читайте в инструкции Управление профилями.

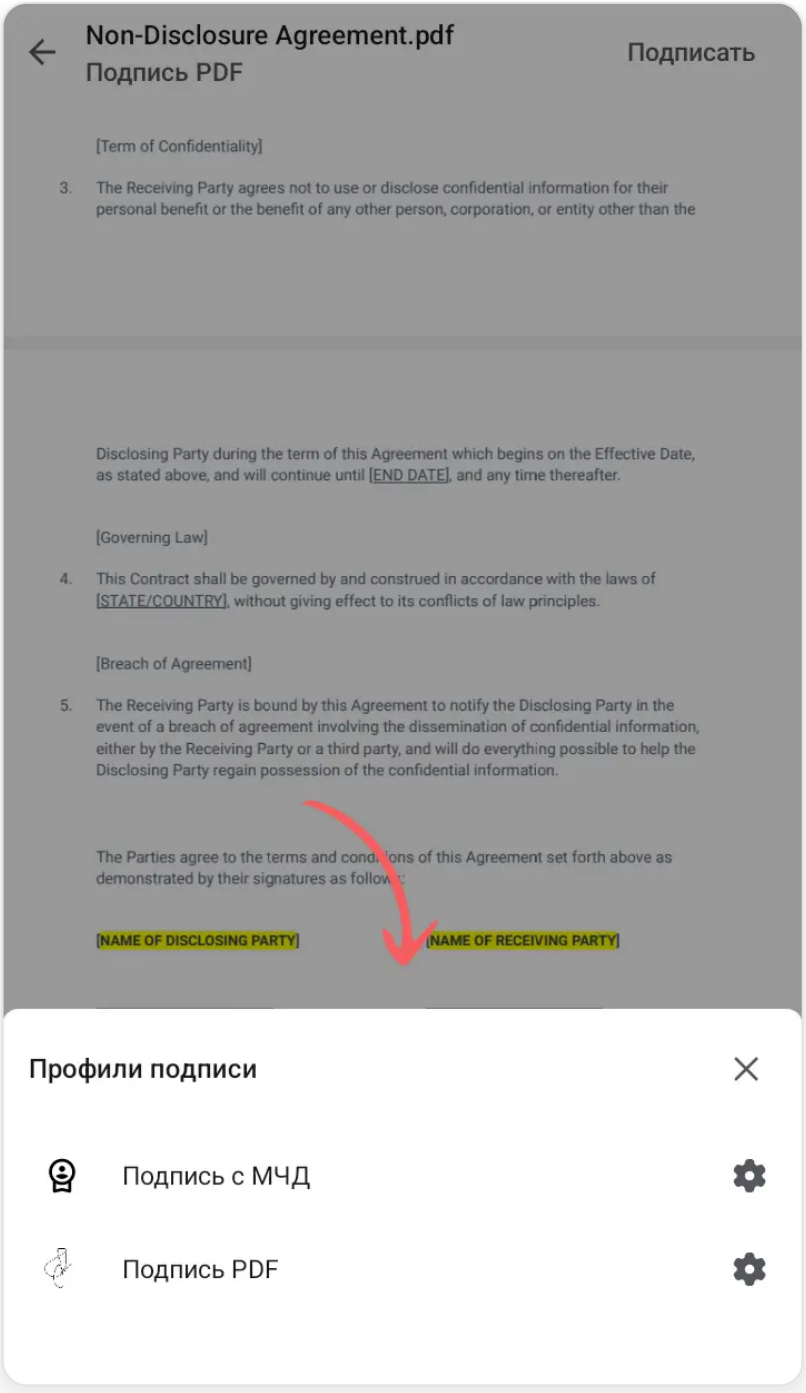


Шаг 4. Настройка параметров подписи

В редакторе можно перемещать визуальный штамп по страницам документа, изменять его размер и угол поворота, а также удалять. После удаления штампа мастер возвращается в режим просмотра.

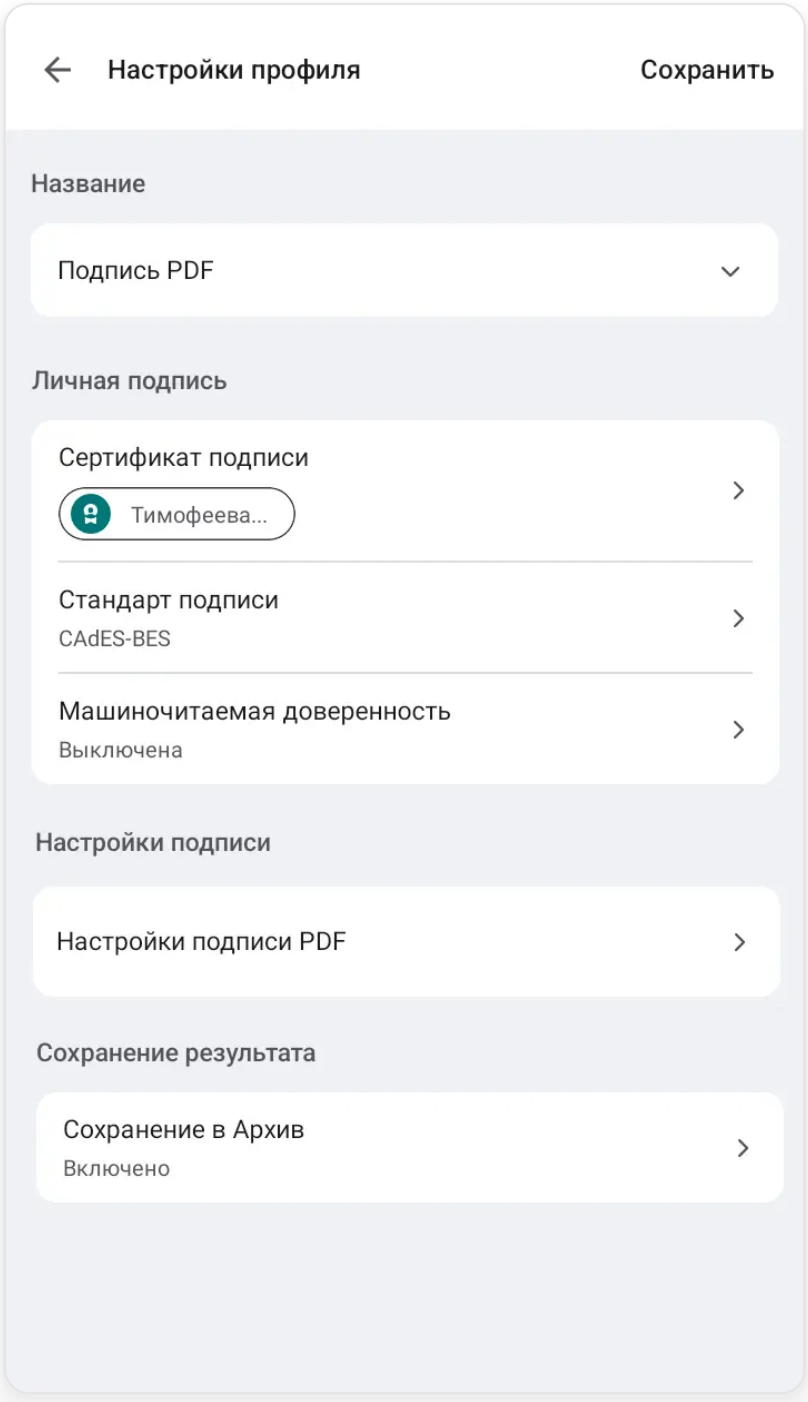
Чтобы изменить параметры подписи:

1. Нажмите на название профиля в верхней части экрана.
2. Выберите нужный профиль. Чтобы изменить его настройки, нажмите на **Настройки** на панели активного профиля.

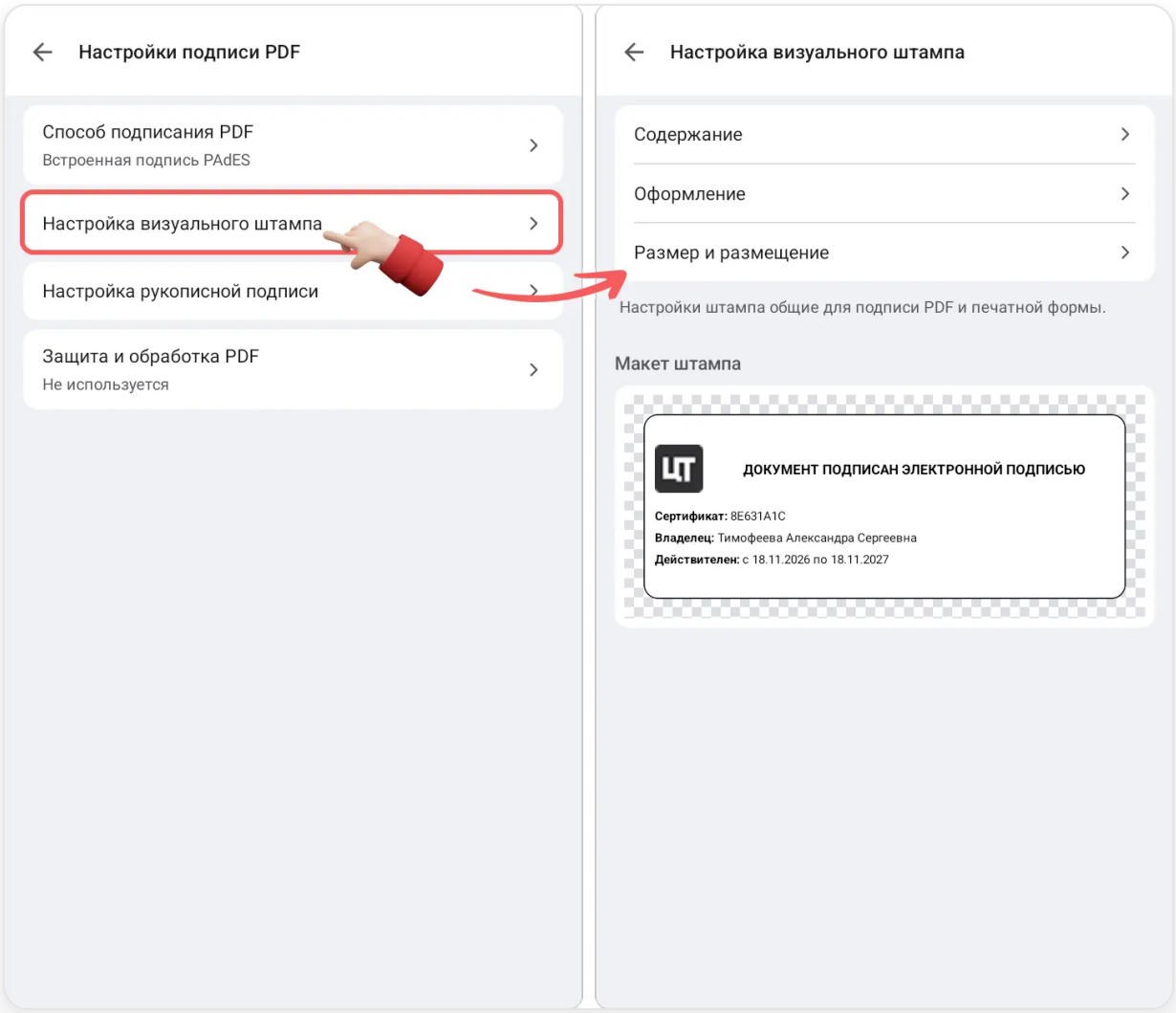


3. В открывшемся окне выберите **сертификат подписи**. Для этого нажмите на соответствующую панель и в открывшемся окне укажите один из личных сертификатов.

   Дополнительно можно выбрать стандарт подписи. Чтобы создать подпись с меткой времени, выберите стандарт подписи **CAdES-X Long Type 1** или **CAdES-T** и настройте службы штампов времени. Про описание настроек читайте в инструкции Настройки для стандартов со штампами.



4. В блоке **Настройки подписи PDF** настройте внешний вид, размер и размещение визуального штампа.



5. При необходимости добавьте изображение рукописной подписи в разделе **Способ подписания PDF** и настройте его в подразделе **Настройки рукописной подписи**.

6. При необходимости включите настройку **Сохранить в «Архив»**, чтобы сохранить копию подписанного документа в архиве.
7. Примените настройки профиля.

Шаг 5. Подтверждение и выполнение операции

1. Нажмите кнопку **Подписать** в верхней части окна.
2. В окне подтверждения нажмите **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.
3. Если контейнер закрытого ключа защищен паролем, необходимо ввести его.

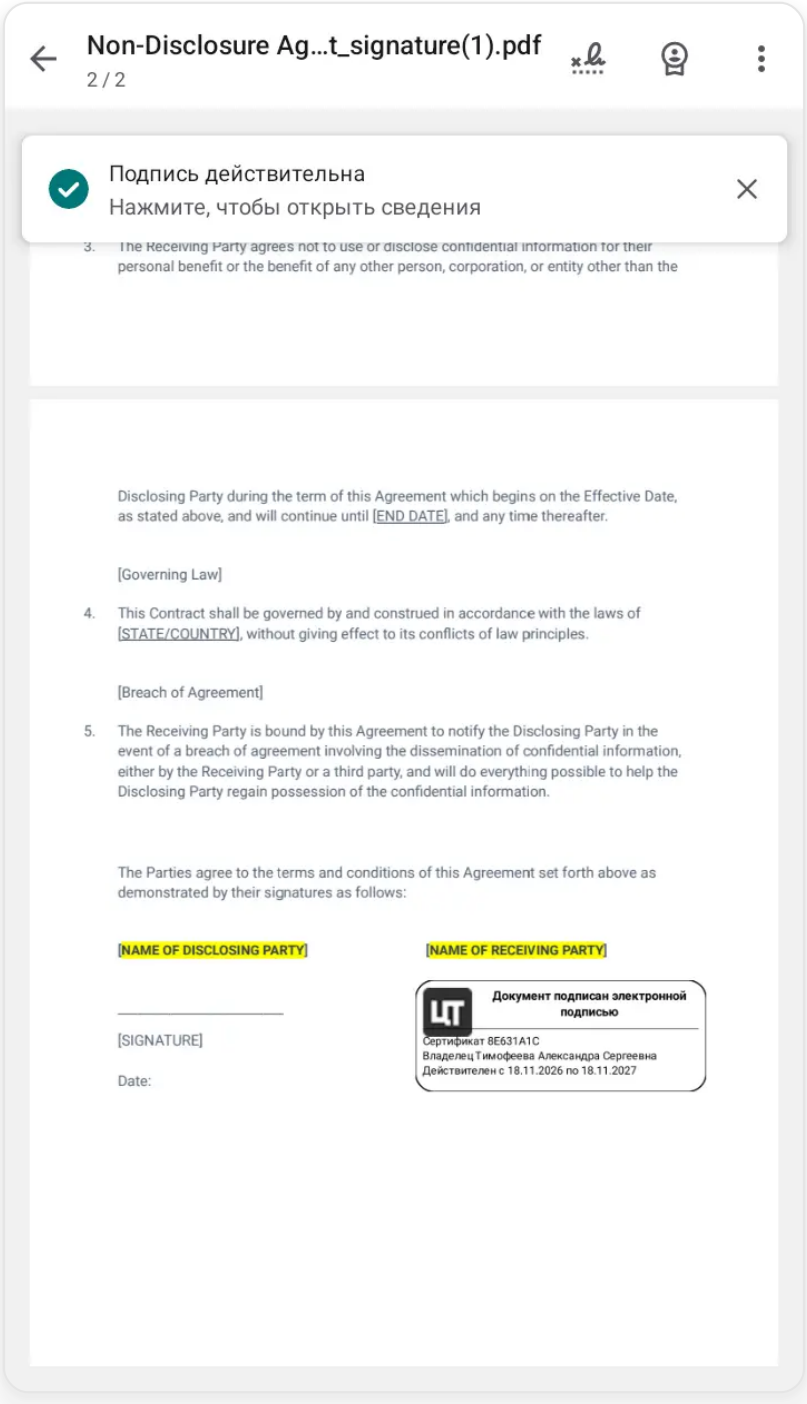
> 🚨 **Внимание:** если сертификат подписи недействителен, **КриптоАРМ Подпись и шифрование** покажет предупреждение. Подпись можно создать, но она может не быть признана действительной.

Шаг 6. Результат

Время выполнения операции подписи зависит от объема документа и производительности устройства.

После успешного подписания файл будет сохранен в соответствии с настройками профиля.

Затем документ откроется в режиме просмотра. В нем можно ознакомиться с результатом проверки созданной подписи.



Как создать сертифицирующую подпись

Сертифицирующая подпись — это особый тип электронной подписи, который подтверждает авторство и целостность документа, а также устанавливает ограничения на его дальнейшее изменение. Подробнее читайте в инструкции Обзор операций КриптоАРМ Подпись и шифрование.

Чтобы создать сертифицирующую подпись:

1. Откройте мастер, добавьте PDF-файл и установите настройки подписи, как описано в разделе Как подписать PDF-документ.
2. В настройках профиля откройте **Настройки подписи PDF** → **Защита и обработка PDF** и включите опцию **Сертификация**.
3. Примените настройки профиля в редакторе.
4. Нажмите **Подписать**.

Далее выполните стандартные действия для завершения операции: подтвердите подписание, введите пароль контейнера закрытого ключа (если требуется) и дождитесь результата. Подробнее эти действия описаны в разделе Как подписать PDF-документ.

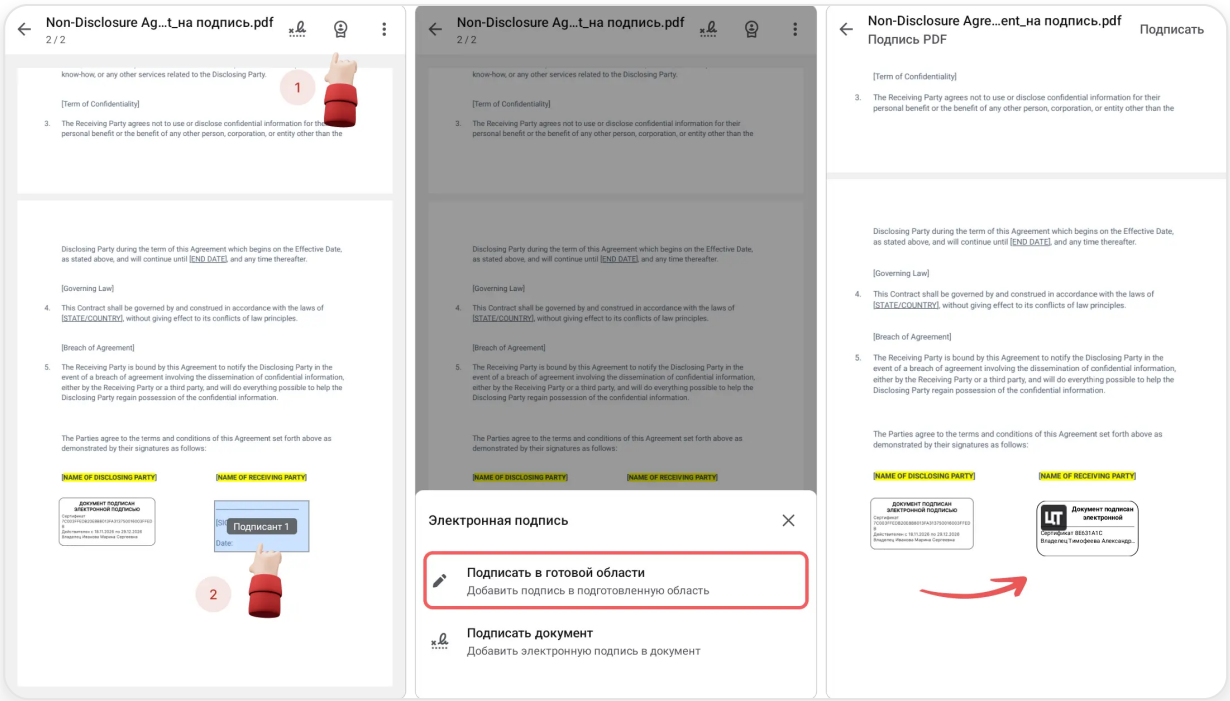
Как поставить подпись в размеченную область

Если в PDF-документе подготовлены размеченные области для подписантов, вы можете установить подпись в одну из них. Области для видимых подписей отображаются непосредственно на странице документа.

Чтобы поставить подпись в размеченную область:

1. Откройте мастер и добавьте PDF-файл, как описано в разделе Как подписать PDF-документ.

2. Нажмите на незаполненную область подписи, либо нажмите на кнопку **Электронная подпись** в верхней части окна, затем выберите действие **Подписать в готовой области**.



3. Установите настройки подписи, как описано в разделе Как подписать PDF-документ.
4. Нажмите **Подписать**.

Далее выполните стандартные действия для завершения операции: подтвердите подписание, введите пароль контейнера закрытого ключа (если требуется) и дождитесь результата. Подробнее эти действия описаны в разделе Как подписать PDF-документ.

Как поставить рукописную подпись

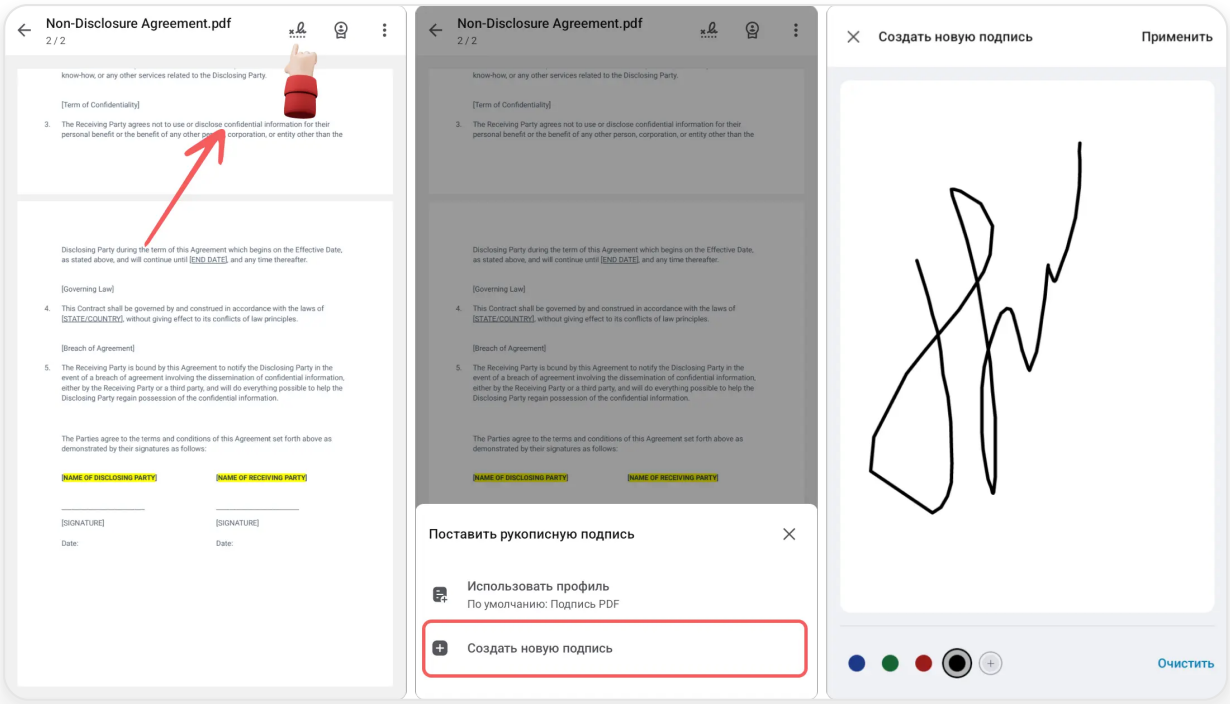
Рукописная подпись в **КриптоАРМ Подпись и шифрование** — это изображение подписи, которое можно добавить в PDF-документ. Она не является электронной подписью и сама по себе не подтверждает подлинность документа или личность подписавшего.

Рукописную подпись можно добавить отдельно, без создания электронной подписи, или использовать вместе с электронной подписью.

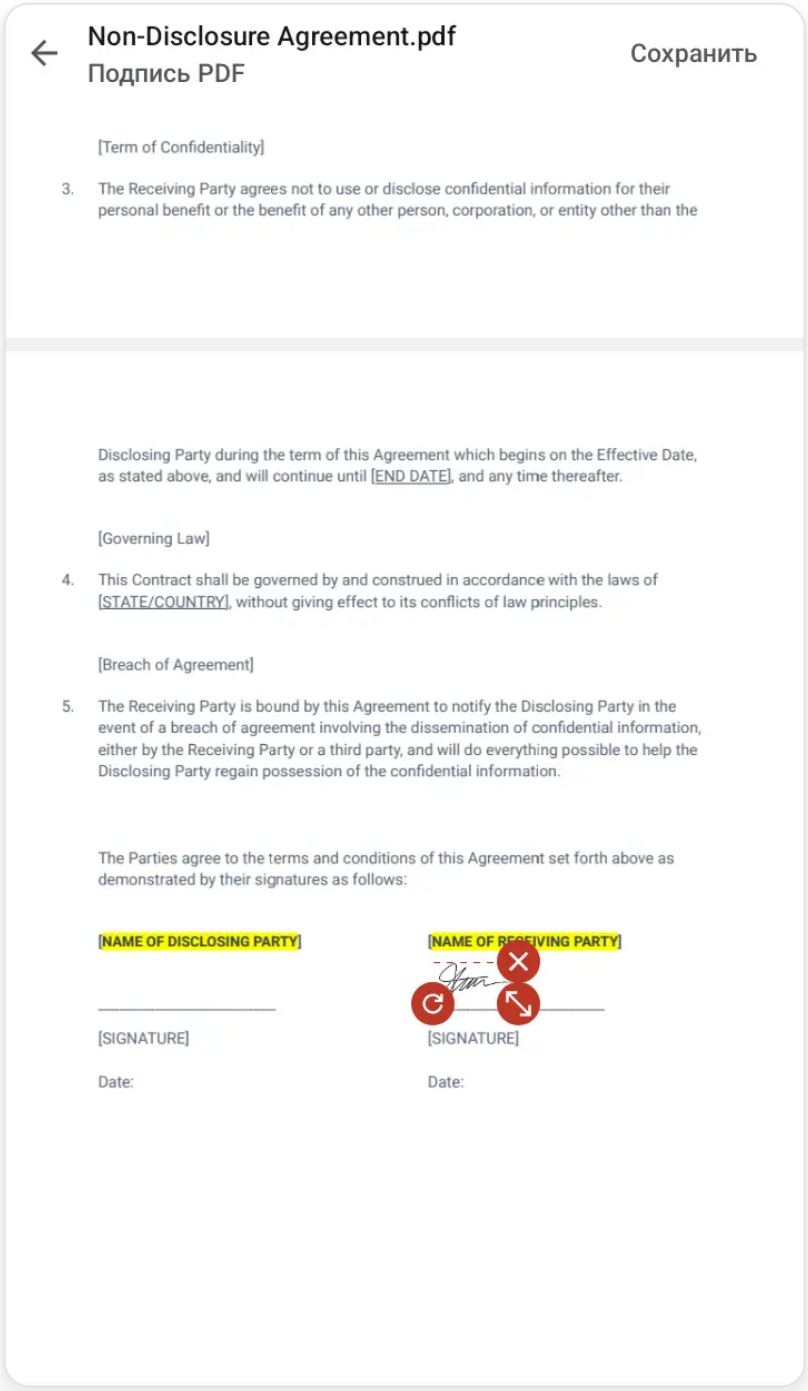
Чтобы поставить только рукописную подпись:

1. Откройте мастер и добавьте PDF-файл, как описано в разделе Как подписать PDF-документ.
2. Нажмите **Рукописная подпись**.
3. В открывшемся окне выберите один из вариантов:
   - **Использовать профиль** — использовать изображение и настройки размещения рукописной подписи, сохраненные в профиле.
   - **Создать новую подпись** — создать подпись вручную.

Чтобы создать новую подпись, проведите пальцем по области рисования. При необходимости выберите цвет подписи. Когда закончите, нажмите **Применить**.



4. После выбора или создания подписи откроется редактор PDF-документа. На странице появится изображение рукописной подписи. Его можно перемещать по странице, изменять размер и угол поворота, а также удалять.



5. Нажмите **Сохранить**.

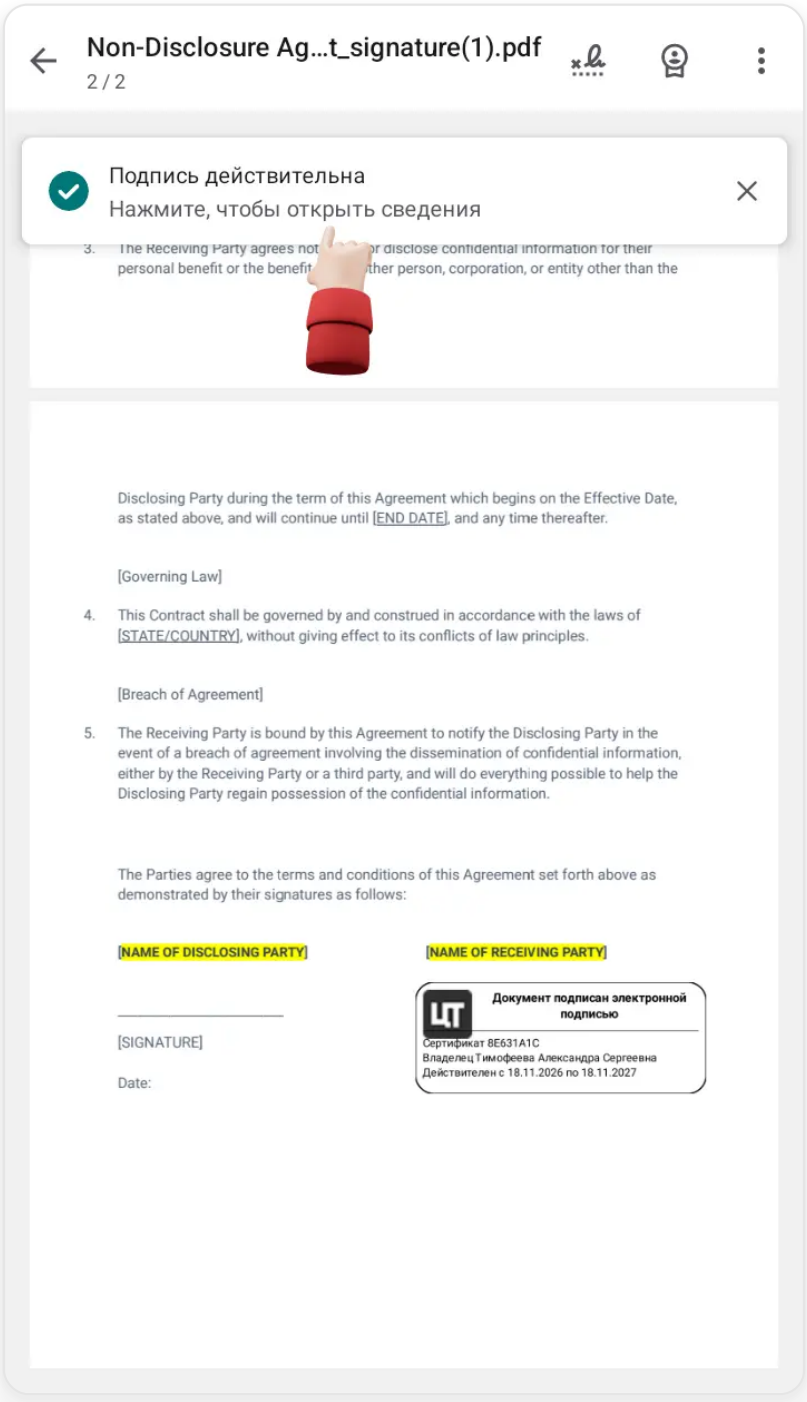
Дождитесь завершения сохранения документа. После успешного выполнения операции файл будет сохранен в соответствии с настройками профиля.

Затем документ откроется в режиме просмотра.

Как проверить подпись PDF-документа

В мастере **Подпись и защита PDF** проверка электронных подписей запускается автоматически при открытии документа и после выполнения операции подписания.

Общий статус подписи отображается в виде уведомления в верхней части окна.



🔍 Подробнее о проверке электронных подписей читайте в инструкции Как проверять электронную подпись в КриптоАРМ Подпись и шифрование.

Возможные ошибки при подписании документов

При выполнении подписи могут возникнуть ошибки, связанные с настройками профиля, сертификатом или выполнением криптографической операции.

Описание распространенных ошибок и способы их устранения приведены в инструкции Ошибки при подписании PDF.

Инструкции по теме

- Как создать профиль подписи
- Как установить личный сертификат
- Как зашифровать документ
- Как проверить подпись документа
- Как добавить подпись к файлу (соподпись)
- Как снять подпись с файла

Открыть статью на сайте

Как добавить соподпись в КриптоАРМ Подпись и шифрование

- Что такое соподпись?
- Как добавить соподпись
- Возможные ошибки
- Инструкции по теме

Что такое соподпись?

Соподпись — это дополнительная электронная подпись, которую добавляют к документу, уже содержащему другую подпись. При этом исходная подпись сохраняется, а новая добавляется к ней. В результате документ содержит несколько электронных подписей.

В **КриптоАРМ Подпись и шифрование** соподпись поддерживается для двух стандартов электронной подписи:

- **CAdES** — новая подпись создается для исходного документа или файла подписи. В зависимости от выбранного типа CAdES она может быть присоединенной или отсоединенной.
- **PAdES** — новая подпись встраивается непосредственно в PDF-документ. Предыдущие подписи сохраняются, если документ допускает добавление последующих подписей.

Каждый участник подписывает документ своим сертификатом. Проверить подлинность и действительность подписей можно отдельно для каждой подписи.

Особенности соподписи

- Все подписи (первичная и соподписи) имеют равный юридический статус,
- Порядок добавления подписей не влияет на их значимость,
- Каждая подпись содержит полный набор атрибутов (дата, время, сертификат).

> 🚨 **Важно:** Статус документа с соподписями считается действительным в случае действительности всех подписей.

Рекомендации для CAdES

- **Присоединенная подпись**: если исходный документ содержит присоединенную подпись, рекомендуется делать соподпись также **присоединенной**, чтобы все подписи хранились в одном файле.

- **Отсоединенная подпись**: если исходный документ содержит отсоединенную подпись, соподпись лучше делать **отсоединенной**, чтобы сохранить согласованную схему хранения подписей.

> ⚠️ Несоблюдение согласованного типа подписи может привести к путанице при проверке и хранении документа.

Как добавить соподпись

> 💡 **Совет**: Чтобы оценить, готово ли ваше рабочее место для подписи документов, воспользуйтесь Проверкой рабочего места.

Шаг 1. Подготовка

1. Откройте мастер **Подпись и шифрование** и добавьте в него подписанные файлы по инструкции:
   - Шаг 1. Запуск мастера
   - Шаг 2. Добавление документов
2. Проверьте валидность всех существующих подписей и убедитесь, что документ не изменялся после последнего подписания.

   Проверка запускается автоматически после добавления документов.

   Статус подписи отобразится на панели с документом:

   - **Подпись действительная** — для файлов, подпись которых успешно проверена;
   - **Ошибка** — для файлов, чья подпись по какой-либо причине оказалась недействительной или ее не удалось проверить.

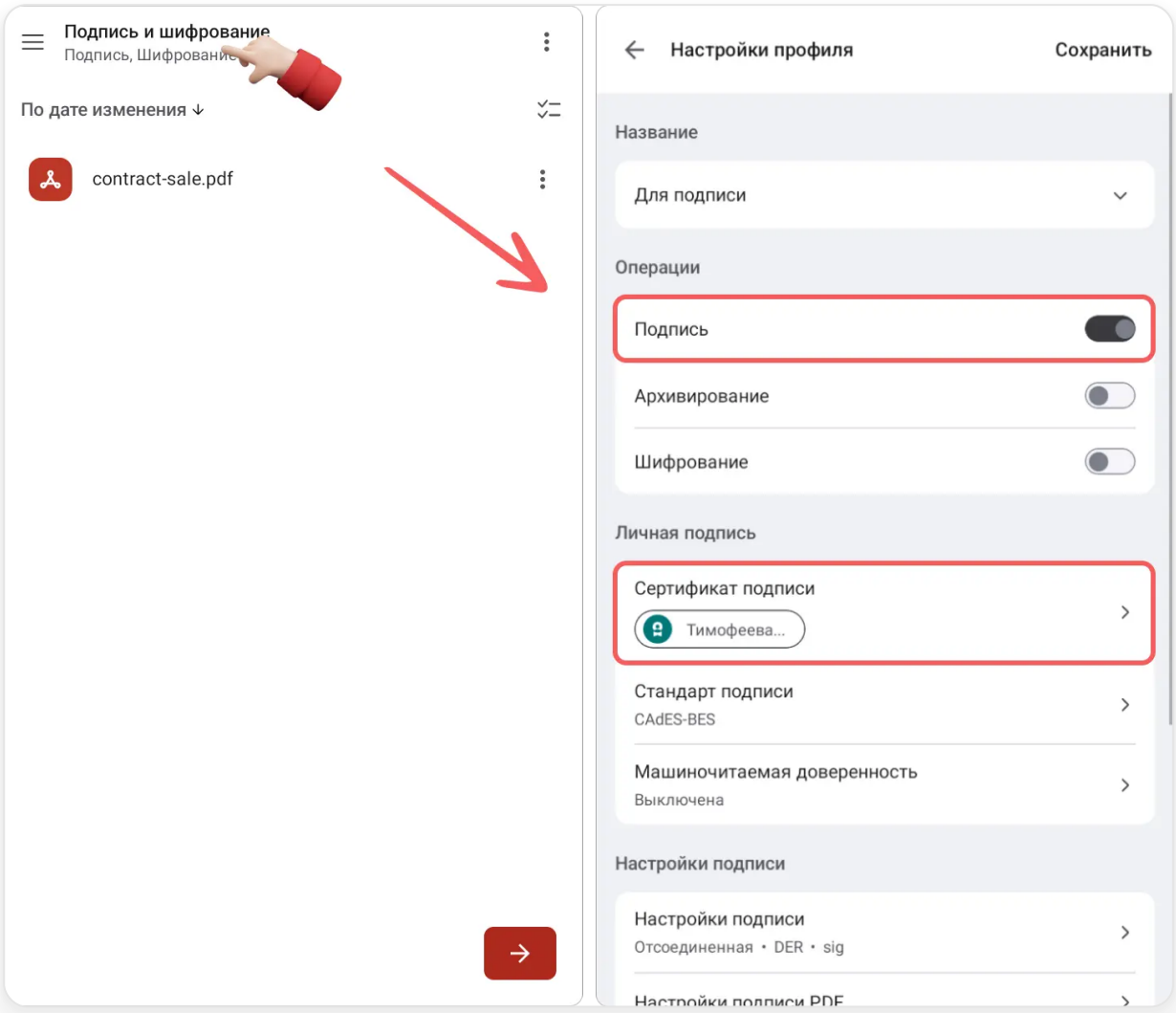
   > 🔍 Подробнее о проверке подписи читайте в инструкции Проверка подписи документа.

Шаг 2. Настройка параметров подписи

Для настройки операции используется активный профиль. Порядок настройки аналогичен обычному подписанию документов.

Чтобы изменить параметры операции:

1. Нажмите на название профиля в верхней части экрана.
2. Откроется окно с настройками.
3. Убедитесь, что операция **Подпись** активна.
4. В блоке **Личная подпись** выберите **сертификат подписи**.



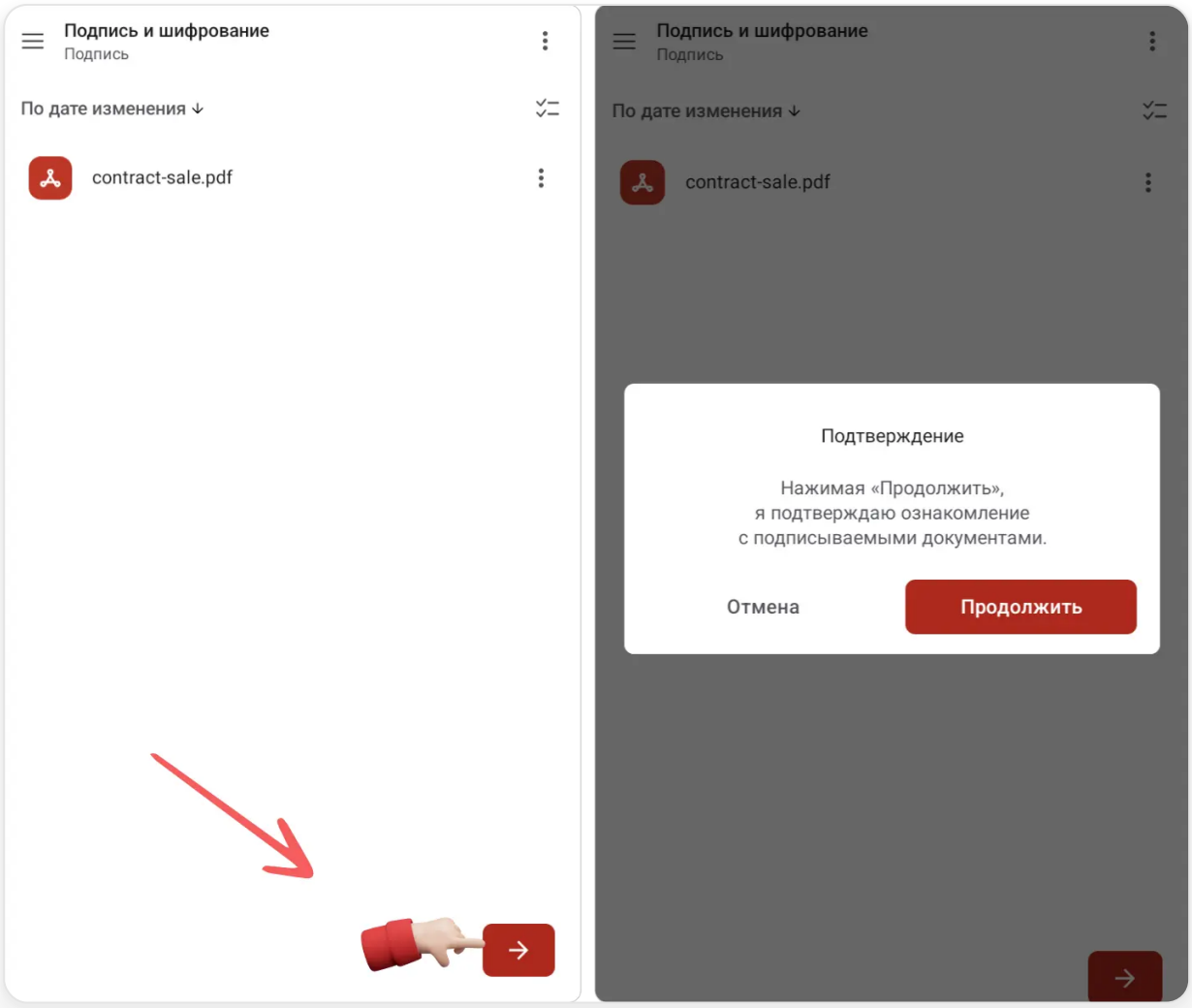
5. В блоке **Настройки подписи** проверьте стандарт и остальные параметры новой подписи.
6. При необходимости настройте дополнительные параметры выбранного способа подписания.

> 🔍 Подробнее о настройке профиля читайте в инструкции Как подписать документы.

7. Примените настройки профиля.

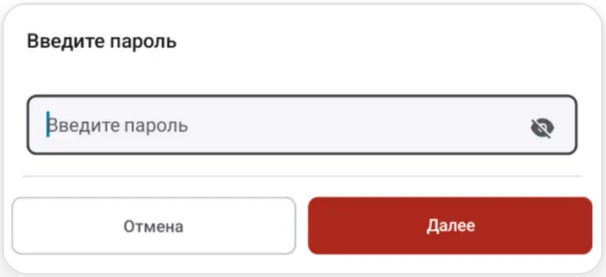
Шаг 3. Подтверждение и выполнение операции

1. Нажмите кнопку **Выполнить** в нижней части окна **Подпись и шифрование**.

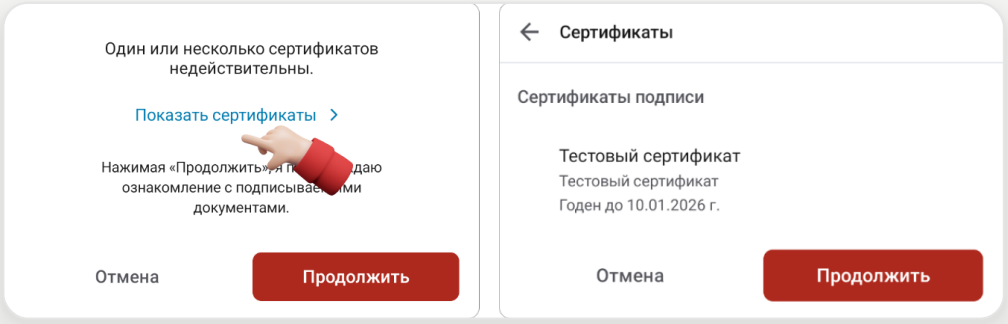


2. В окне подтверждения нажмите **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.

3. Если контейнер закрытого ключа защищен паролем, необходимо ввести его.



🚨 Если сертификат подписи недействителен, будет показано предупреждение. Подпись все равно будет выполнена, но ее юридическая значимость может быть поставлена под сомнение.



Шаг 4. Результат

Время выполнения операции зависит от количества документов и производительности устройства.

- Если операция выполнена успешно, на панели с файлом отобразится статус **Подписан**.
- Если в профиле была активна настройка **Сохранить в «Архив»**, то подписанные документы будут сохранены в указанную папку раздела **Архив**.
- Если в настройках профиля выбрана отсоединенная подпись, то в раздел **Архив** помимо файла подписи сохранится копия исходного файла.
- Если включено создание печатной формы, в раздел **Архив** дополнительно сохранится копия документа с визуальным отображением штампа электронной подписи и рукописной подписи, если она была настроена.

💡 В окне с результатами операции вы можете ознакомиться с информацией о подписи и поделиться файлами.

Возможные ошибки

При выполнении соподписи могут возникнуть ошибки, связанные с настройками профиля, сертификатом или выполнением криптографической операции.

Описание распространенных ошибок и способы их устранения приведены в инструкции Возможные ошибки при подписании документов.

Инструкции по теме

- Как создать профиль подписи
- Как подписать документ
- Как снять подпись с файла
- Как установить личный сертификат
- Как установить корневой и промежуточный сертификаты

Открыть статью на сайте

Как шифровать документы в КриптоАРМ Подпись и шифрование

- О шифровании
- Как зашифровать документы
- Возможные ошибки
- Инструкции по теме

О шифровании

Шифрование — это процесс преобразования данных в форму, которая делает их недоступными для чтения без использования специальных средств, таких как ключ шифрования. Основная цель этой процедуры — обеспечить конфиденциальность информации, скрыв её от посторонних глаз, даже если у них есть доступ к зашифрованным данным.

Для шифрования файла вам понадобится открытый ключ получателя зашифрованных данных.

Как это работает?

- Вы выбираете сертификаты получателей или контакты с привязанными сертификатами.
- КриптоАРМ выполняет шифрование в адрес этих сертификатов.
- Получатели расшифровывают данные с помощью своего закрытого ключа.

> 💡 **Совет**: Для успешного шифрования убедитесь, что сертификаты получателей действительны и установлены в приложении.

Рекомендации

1. Добавление себя как получателя
    - Всегда добавляйте **свой личный сертификат** к списку получателей, если вы планируете в дальнейшем расшифровывать файл.
    - Если вы не добавите себя, то после шифрования не сможете открыть файл, даже если имели доступ к исходным данным.
2. Последовательность добавления получателей
    - Порядок сертификатов в списке **не влияет** на результат шифрования.
    - Главное — убедиться, что каждый сертификат действителен и предназначен для шифрования (имеет атрибут KeyAgreement, если включена проверка KeyAgreement).

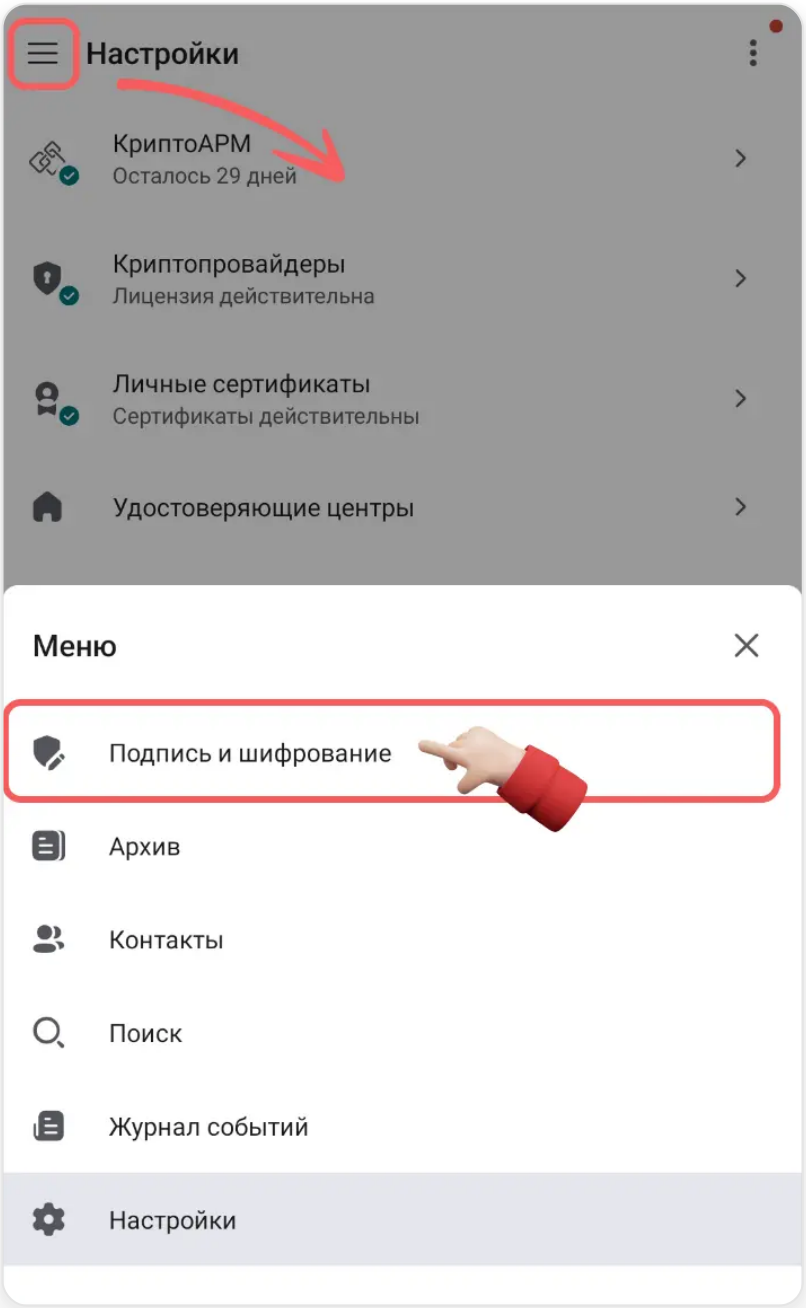
3. Профили
    - При работе с несколькими получателями **используйте профиль шифрования**, чтобы сохранить настройки.
    - В профиле можно указать: включение архивации файлов, сохранение копий в «Архив», автоматическое добавление собственного сертификата как получателя.
4. Настройки безопасности
    - Убедитесь, что используемые алгоритмы шифрования соответствуют внутренним требованиям организации.
    - Если получатели используют разные криптопровайдеры, проверьте совместимость сертификатов перед шифрованием.

Как зашифровать документы

> 💡 **Совет**: Чтобы оценить, готово ли ваше рабочее место для шифрования документов, воспользуйтесь Проверкой рабочего места.

Шаг 1. Запуск мастера

1. Вызовите главное меню по кнопке , размещенной в верхнем левом углу окна приложения.
2. Выберите пункт **Подпись и шифрование**.



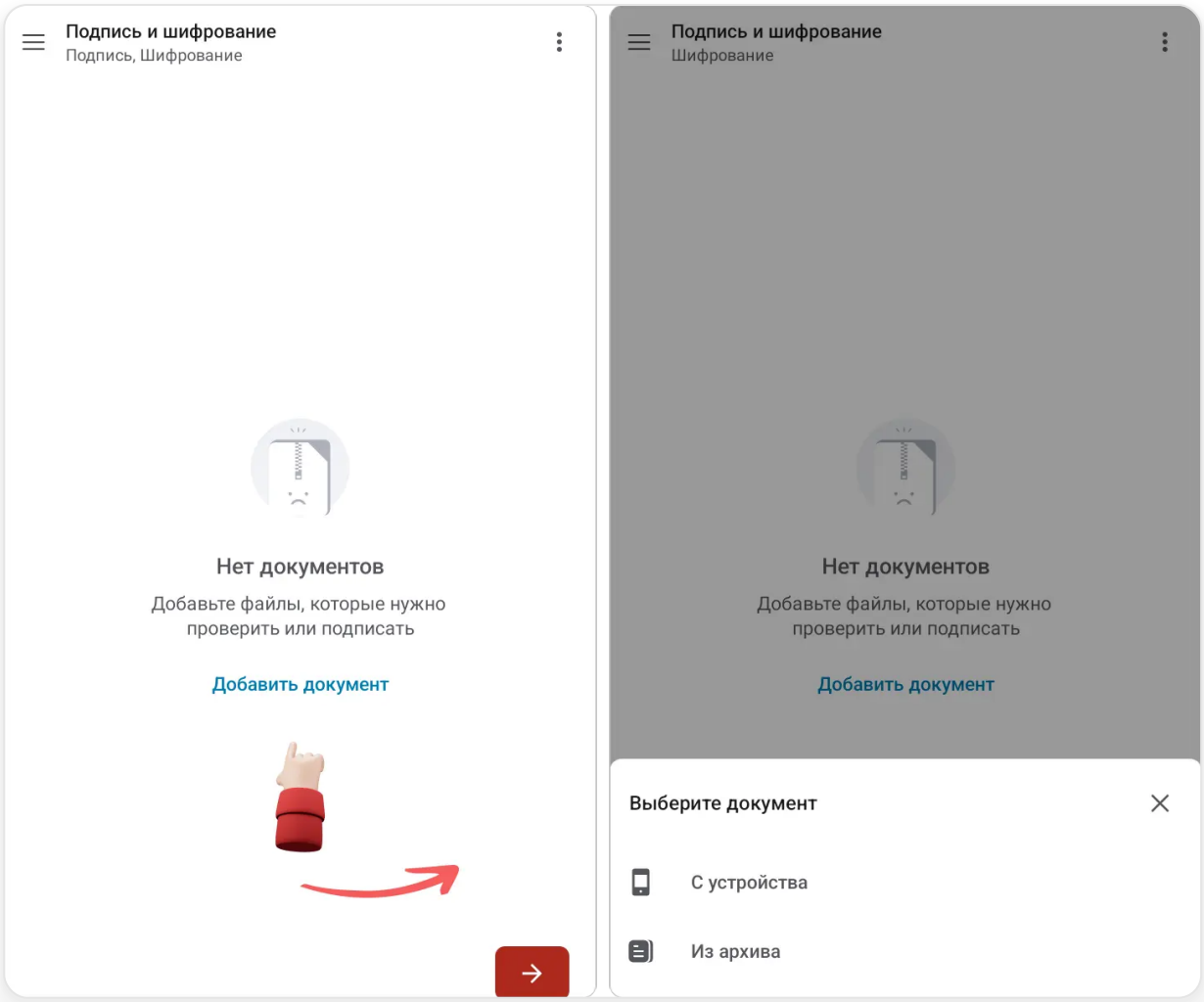
💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

Шаг 2. Добавление документов

Из мастера

1. В окне **Подпись и шифрование** нажмите на кнопку **Добавить документ**.
2. В появившемся меню выберите:
    - **С устройства** — для выбора файлов, сохраненных на устройстве,

- **Из архива** — для выбора файлов, сохраненных в разделе **Архив**.



Из сторонних приложений

1. Выберите файлы в любом стороннем приложении.
2. Нажмите **Открыть с помощью** и выберите **КриптоАРМ**.

> 💡 **Совет**: Ненужный файл можно удалить из списка через меню **Еще** → **Удалить**.

Шаг 3. Настройка параметров шифрования

По умолчанию в мастере используются настройки операции из активного профиля.

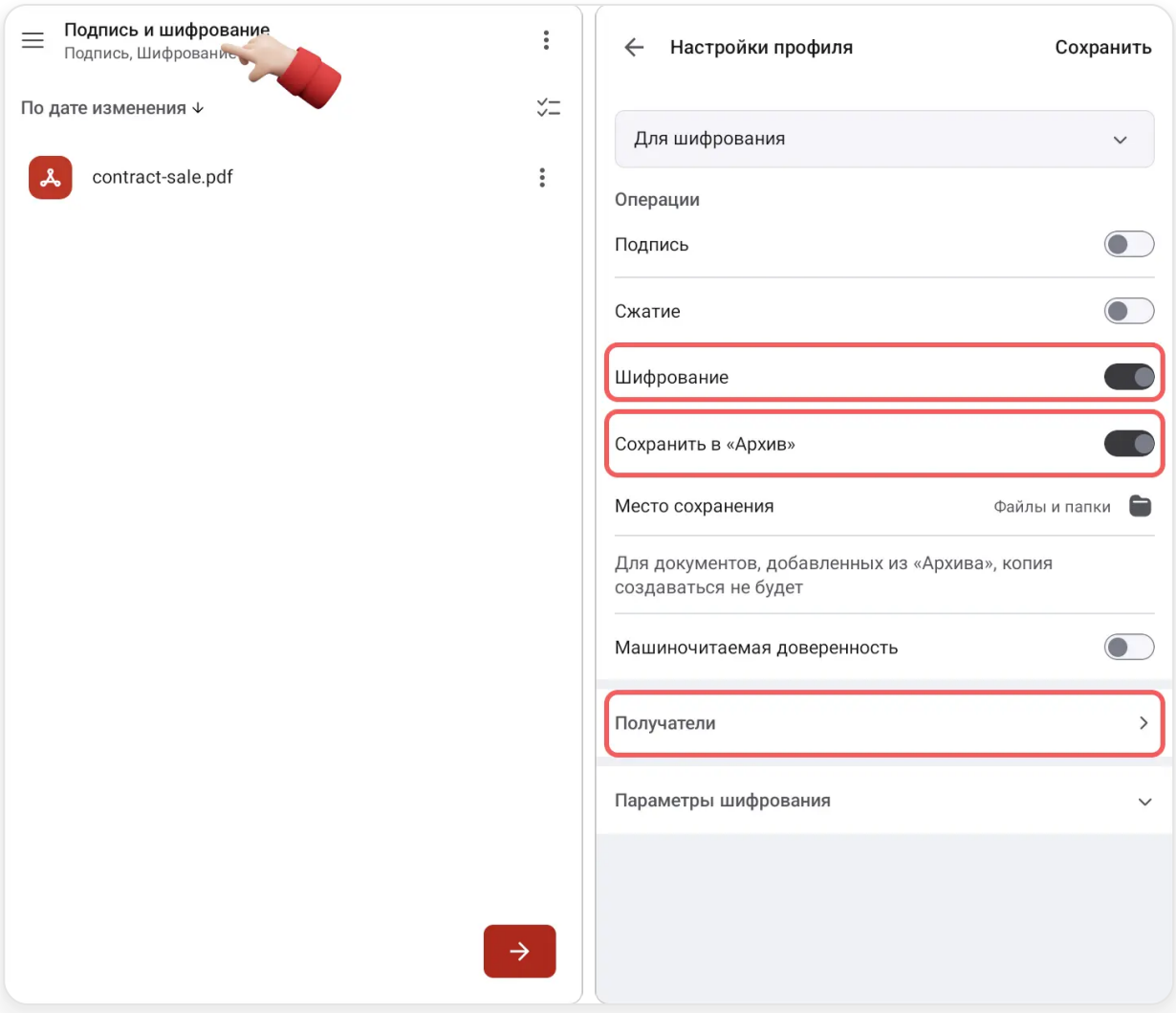
> 💡 **Профиль** — это сохранённый набор настроек подписи. Используя профили, вы можете быстро переключаться между разными сценариями. Подробнее про профили читайте в инструкции Управление профилями.

Чтобы изменить настройки профиля:

1. Нажмите на название профиля в нижней части экрана.
2. Откроется окно с настройками профиля:
    - Выберите **Шифрование** в блоке **Операции**.

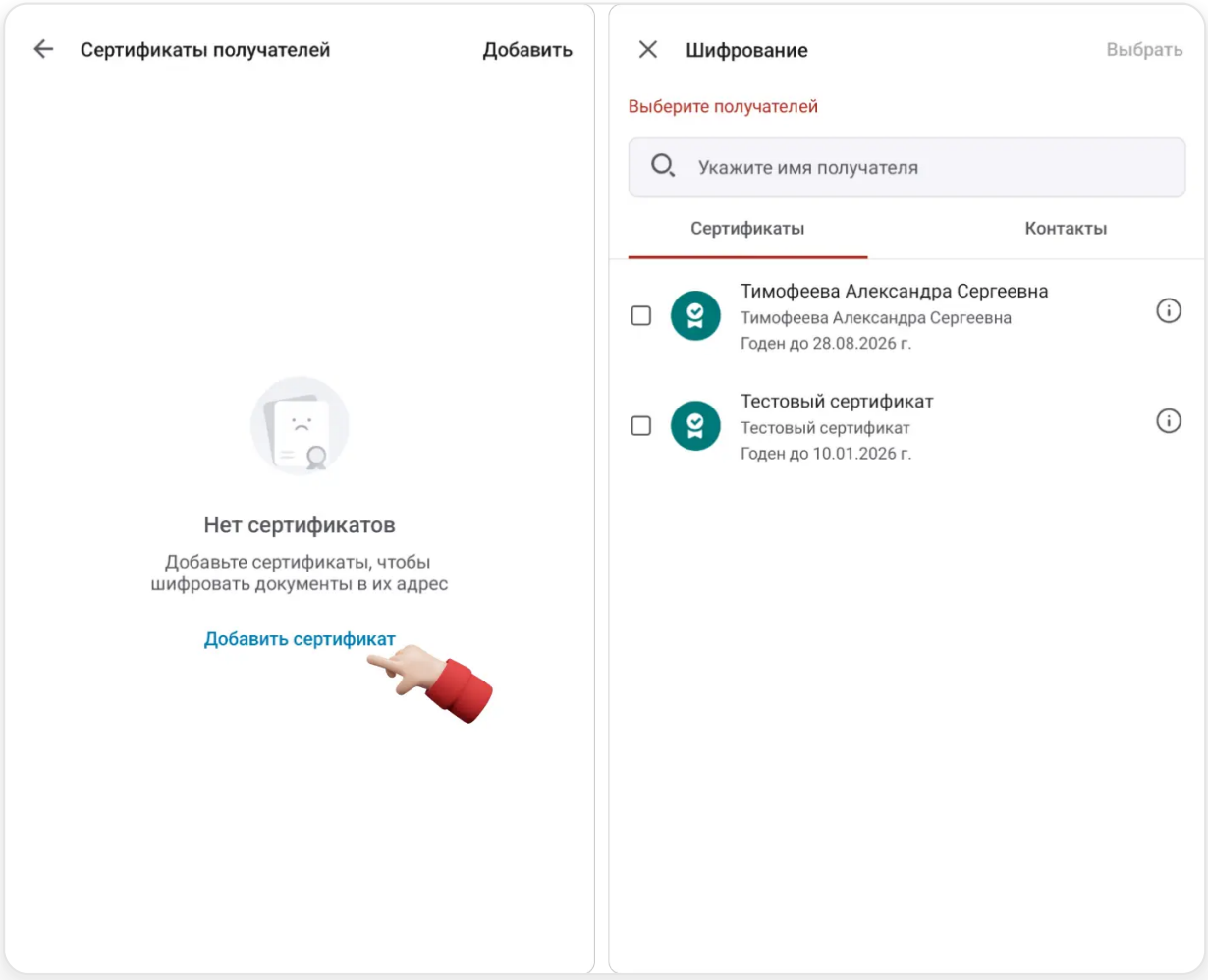
> 💡 **Совет**: Для создания одного зашифрованного архива включите **Архивирование** — все файлы будут помещены в архив и зашифрованы.

    - При необходимости включите опцию **Сохранить в «Архив»** и укажите папку для сохранения результатов.



    - Выберите **Получателей**. Для этого нажмите на соответствующую панель и в открывшемся окне укажите сертификаты или контакты получателей.

> 💡 **Совет**: Чтобы иметь возможность расшифровать зашифрованный файл, добавьте личный сертификат к сертификатам шифрования.



- При необходимости откройте **Параметры шифрования** для дополнительных настроек, например: алгоритмы шифрования, параметры архивирования.

3. Сохраните настройки профиля.

Шаг 4. Подтверждение и выполнение операции

1. Нажмите кнопку **Выполнить** в нижней части окна **Подпись и шифрование**.
2. Перед выполнением операции будет запрошено ее подтверждение.

   Нажав «Продолжить» в окне, вы подтверждаете, что ознакомились с подписываемыми данными.

   После подтверждения будет запущено выполнение операции.

Шаг 5. Результат операции

Выполнение операции занимает определенное время и зависит от их объема и производительности устройства.

- Если операция выполнена успешно, на панели с файлом отобразится статус **Зашифрован**.
- Если в профиле была активна настройка **Сохранить в «Архив»**, то зашифрованные документы будут сохранены в указанную папку раздела **Архив**.

> 💡 **Совет**: Зашифрованные файлы можно передавать получателям, а их расшифровка возможна только с использованием соответствующих закрытых ключей.

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана.

Просмотр подробной информации доступен в разделе **Журнал событий**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Описание	Рекомендуемые действия
Выберите сертификат шифрования	Не выбран сертификат для выполнения операции шифрования	Выберите сертификат в профиле подписи
Ошибка при подписи файла	Файлы недоступны или имеют нулевой размер	1. Проверьте наличие и доступность файлов. Повторите добавление файлов в мастер 2. Убедитесь, что файлы не пустые (имеют ненулевой размер) 3. Освободите место на устройстве

Инструкции по теме

- Как расшифровать документ
- Как добавить сертификат в контакту
- Как создать профиль подписи
- Как подписать документ
- Как проверить подпись документа

Открыть статью на сайте

Как проверять электронную подпись в КриптоАРМ Подпись и шифрование

- О проверке подписи
- Проверка подписи документа
- Особенности проверки отсоединенной подписи
- Проверка подписи документа с соподписями
- Распространенные проблемы
- Печать отчета о проверке подписи
- Возможные ошибки
- Инструкции по теме

О проверке подписи

Проверка электронной подписи позволяет установить, действительна ли подпись и не изменялся ли документ после подписания. Во время проверки приложение анализирует электронную подпись, сертификат подписанта и другие необходимые данные.

Успешная проверка подтверждает, что подпись действительна, а документ не изменялся после подписания. Кто именно подписал документ, определяется по сертификату подписанта; доверие к этому сертификату зависит от настроек проверки.

КриптоАРМ Подпись и шифрование поддерживает проверку подписей, созданных по стандартам PAdES и CAdES с использованием алгоритмов ГОСТ. Для CAdES-подписей поддерживаются файлы с расширениями `.sig`, `.p7s`, `.sgn`, `.sign` и `.bin`.

В приложении доступны два способа проверки электронной подписи:

Способ проверки	Мастер	Возможности
Групповая проверка PAdES и CAdES	**Подпись и шифрование**	Проверка подписей нескольких документов, просмотр статуса и сведений о подписях, формирование отчета о проверке
Одиночная проверка PAdES	**Подпись и защита PDF**	Проверка подписи одного PDF-документа и просмотр визуального штампа

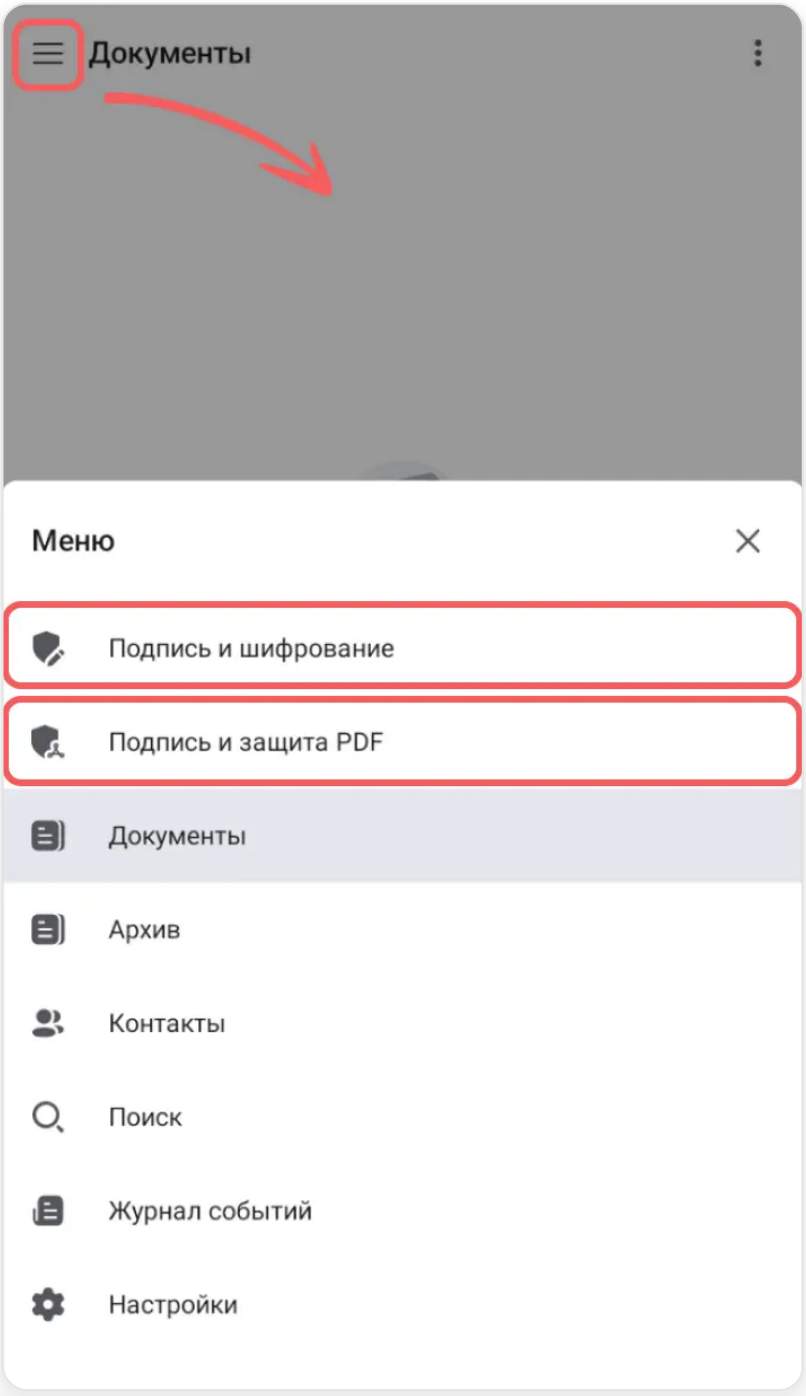
Выберите способ в зависимости от типа подписи и задачи: для одного PDF-документа подойдет мастер **Подпись и защита PDF**, для нескольких документов и формирования отчета — мастер **Подпись и шифрование**.

> 💡 **Совет:** Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Проверка подписи документа

Шаг 1. Запуск мастера

1. Вызовите главное меню по кнопке .
2. Выберите мастер **Подпись и шифрование** или **Подпись и защита PDF**.

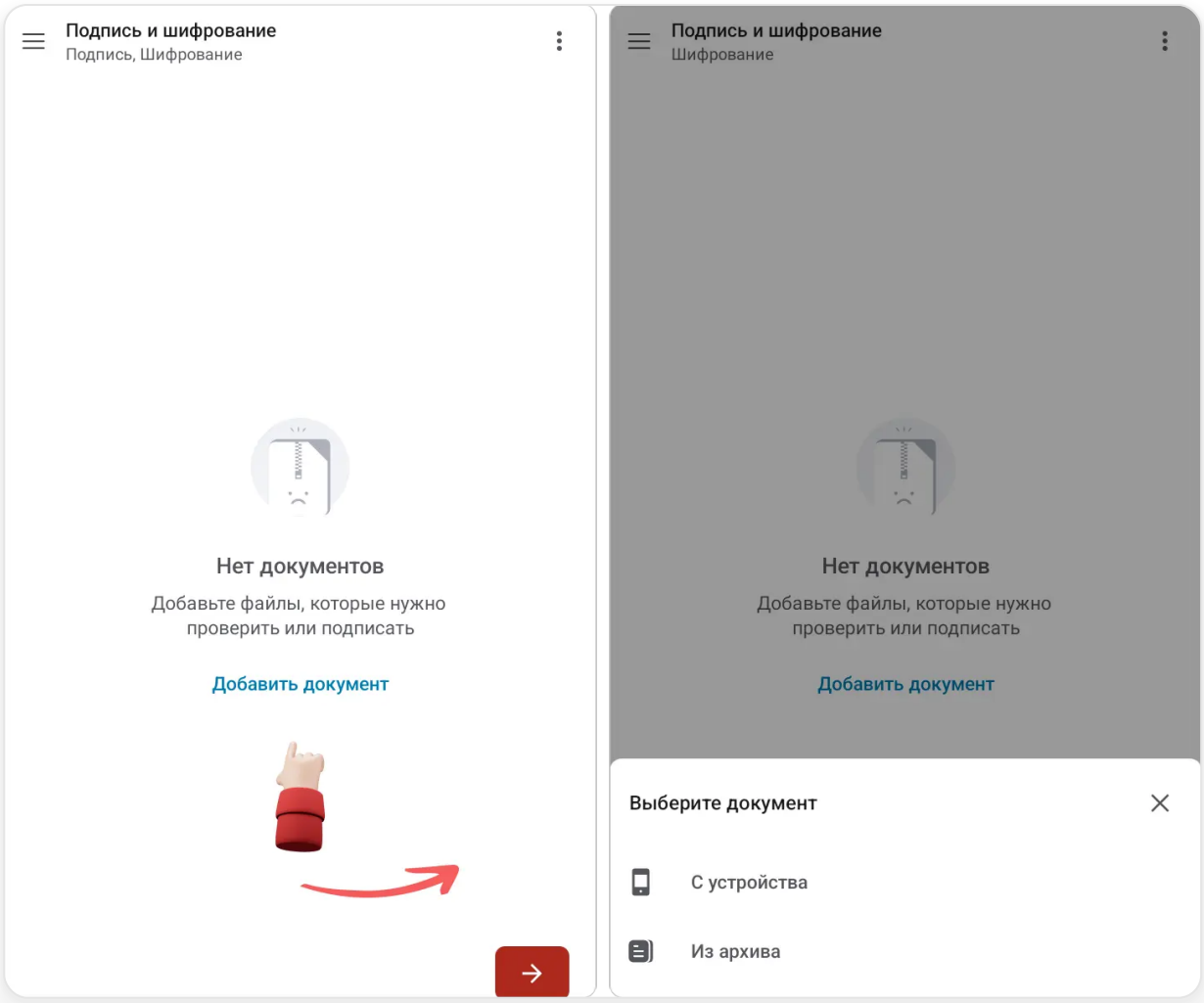


Шаг 2. Добавление документов

Добавить документы в мастер можно несколькими способами.

Из мастера

1. В окне мастера нажмите **Добавить документ**.
2. В появившемся меню выберите:
   - **С устройства** — для выбора файлов, сохраненных на устройстве,
   - **Из архива** — для выбора файлов, сохраненных в разделе **Архив**.



> 💡 **Совет**: Если вы уже находитесь в разделе **Архив**, выберите один или несколько файлов и выберите необходимое действие.

Из сторонних приложений

1. Выберите файлы в любом стороннем приложении.
2. Нажмите **Открыть с помощью** и выберите **КриптоАРМ**.

Шаг 3. Результаты проверки

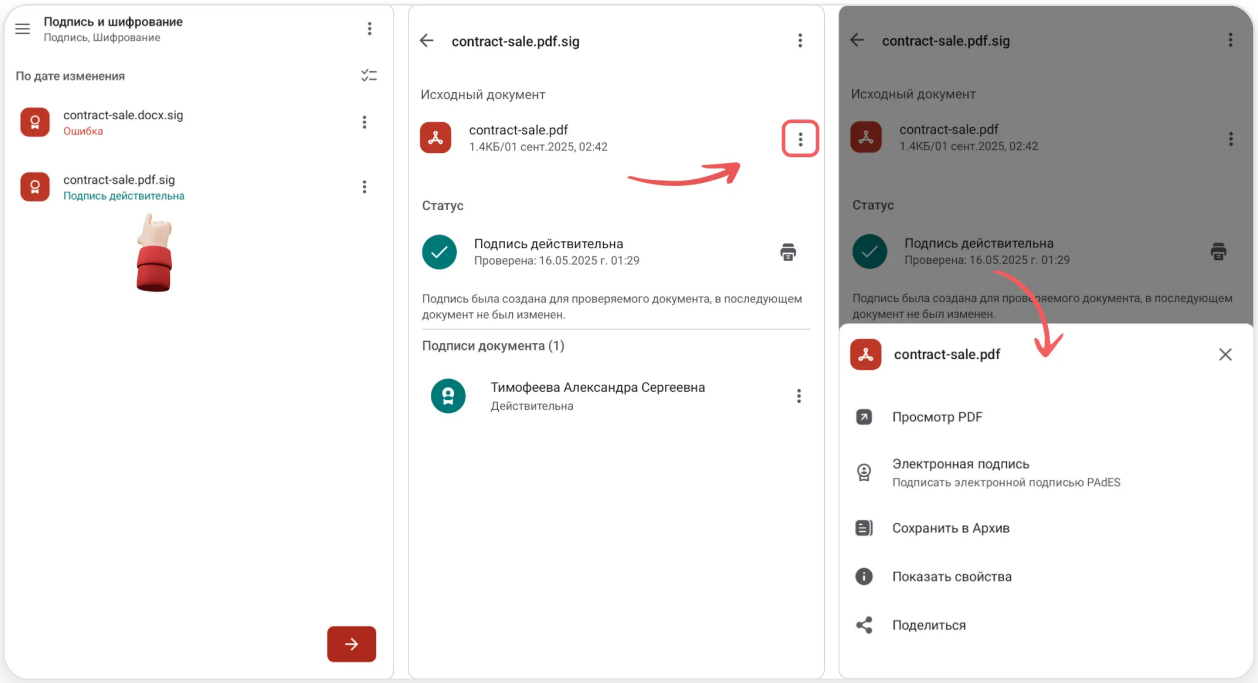
Проверка запускается автоматически после добавления документов.

Мастер «Подпись и шифрование»

Статус подписи отображается на панели с документом:

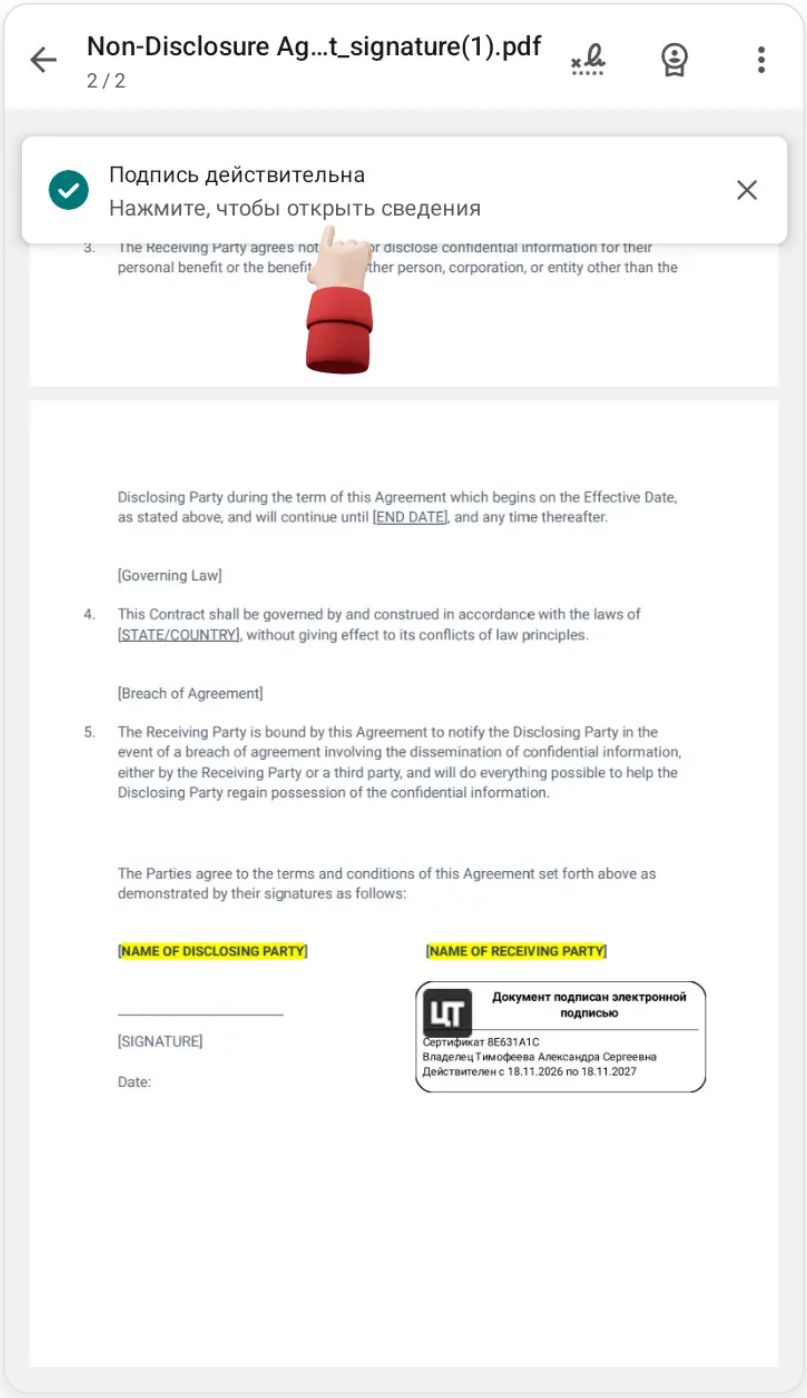
- **Подпись действительна** — подпись успешно проверена;
- **Ошибка** — подпись недействительна или ее не удалось проверить.

Чтобы просмотреть сведения о подписи, нажмите на панель с документом. Откроется окно с общим статусом подписи и списком подписей. Нажмите на панель с подписью, сведения о которой необходимо просмотреть.



Мастер «Подпись и защита PDF»

Статус подписи отображается в виде уведомления в верхней части окна.



Чтобы просмотреть подробные сведения о подписи нажмите на уведомление. Откроется окно с общим статусом подписи и списком подписей. Нажмите на панель с подписью, сведения о которой необходимо просмотреть.

Особенности проверки отсоединенной подписи

Для проверки отсоединенной подписи необходимо добавить в мастер файл подписи и исходный документ.



КриптоАРМ Подпись и шифрование автоматически определяет исходный документ:

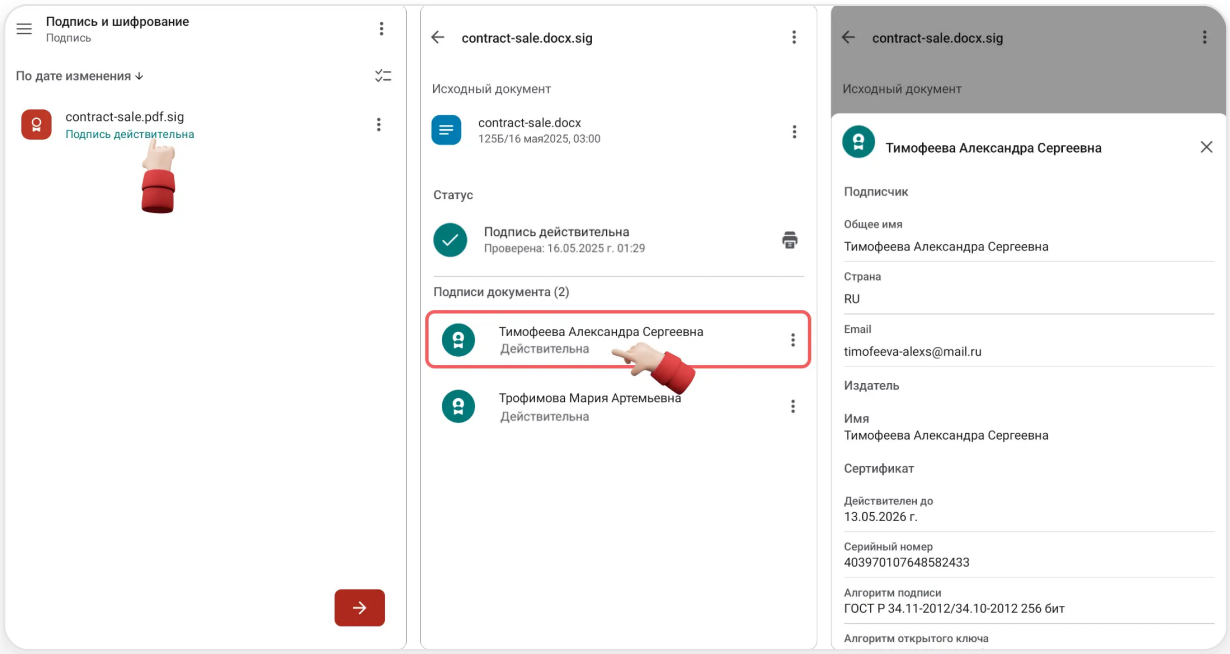
- Сначала приложение ищет документ по имени файла.
- Если документ с соответствующим именем не найден, приложение использует первый неподписанный файл из списка.
- Если в списке несколько неподписанных файлов, для проверки используется первый из них.

> 💡 **Совет**: Если приложение выбрало неподходящий документ, удалите лишние файлы из списка. После удаления файлов приложение повторно проверит возможность сопоставления подписи с исходным документом.

Проверка подписи документа с соподписями

> 🚨 **Важно**: Общий статус подписи документа с соподписями считается действительным в случае действительности всех подписей.

1. Выполните шаги из инструкции Проверка подписи документа.
2. Чтобы просмотреть список подписей документа:
    - Нажмите на панель с документом,
    - Откроется окно с общим статусом подписи и списком подписей.



Распространенные проблемы

Почему подпись не проходит проверку или недействительна:

Причина	Возможность исправления	Рекомендуемые действия
Срок действия сертификата истек или сертификат отозван	❌ Невозможно исправить	Запросите новый документ, подписанный действующим сертификатом
Документ изменен после подписания	❌ Невозможно исправить	Запросите оригинальную подписанную версию документа
Не построилась цепочка сертификации	✅ Можно исправить	Установите корневой и промежуточный сертификаты удостоверяющего центра, который выпустил ваш сертификат
Неактуальный список отзыва (CRL)	✅ Можно исправить	Загрузите актуальный список отозванных сертификатов (CRL)

Печать отчета о проверке подписи

1. Выполните шаги из инструкции Проверка подписи документа.
2. Нажмите на панель с документом.
3. Откроется окно с общим статусом подписи и списком подписей.

4. Нажмите на кнопку **Печать** , расположенную в блоке с общим статусом подписи.
5. Откроется печатная форма с отчетом о проверке электронной подписи.

Отчет можно распечатать или скачать на устройство.

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана.

Просмотр подробной информации доступен в разделе **Журнал событий**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Рекомендуемые действия
Не найден подписанный документ. Невозможно проверить подпись	Добавьте в мастер исходный файл, для которого была сделана отсоединенная подпись. Или укажите путь к файлу в окне просмотра информации о подписи.

Инструкции по теме

- Как расшифровать документ
- Как снять подпись с документа
- Как зашифровать документ
- Как подписать документ

Открыть статью на сайте

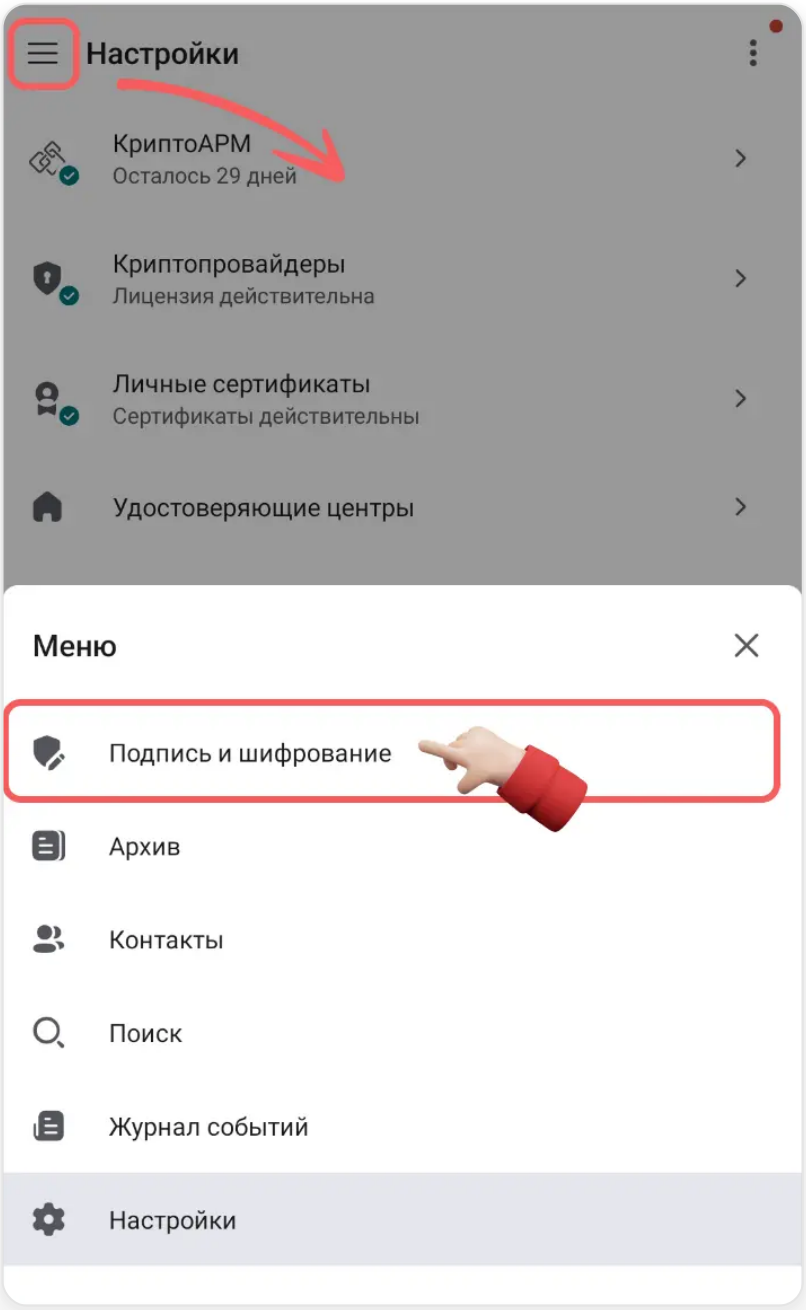
Как снять подпись с документа в КриптоАРМ Подпись и шифрование

- Снятие подписи с документа
- Возможные ошибки
- Инструкции по теме

Снятие подписи с документа

Шаг 1. Запуск мастера

1. Вызовите главное меню по кнопке , размещенной в верхнем левом углу окна приложения.
2. Выберите пункт **Подпись и шифрование**.



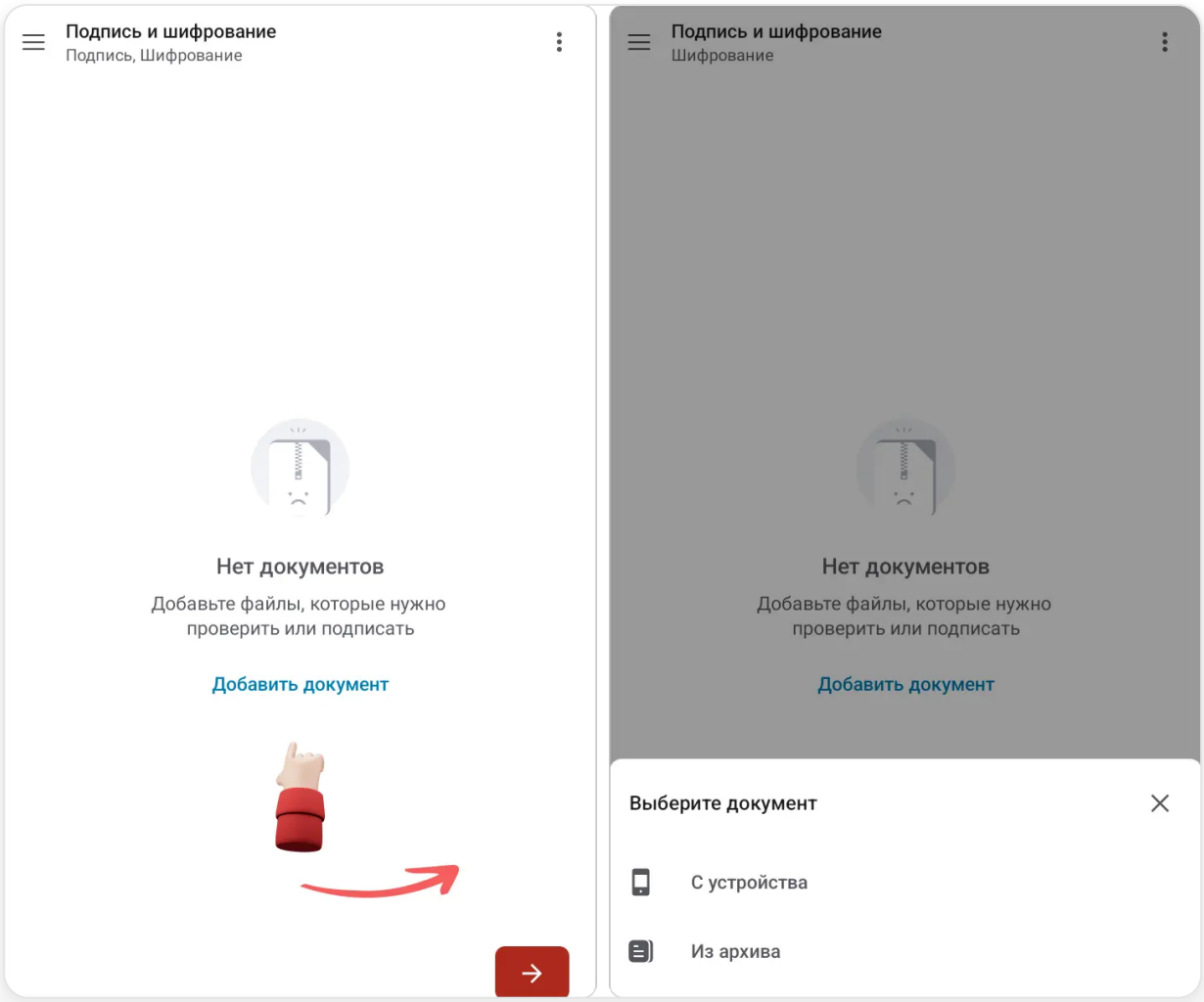
💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

Шаг 2. Добавление документов

Из мастера

1. В окне **Подпись и шифрование** нажмите на кнопку **Добавить документ**.
2. В появившемся меню выберите:
    - **С устройства** — для выбора файлов, сохраненных на устройстве,

- **Из архива** — для выбора файлов, сохраненных в разделе **Архив**.



Из сторонних приложений

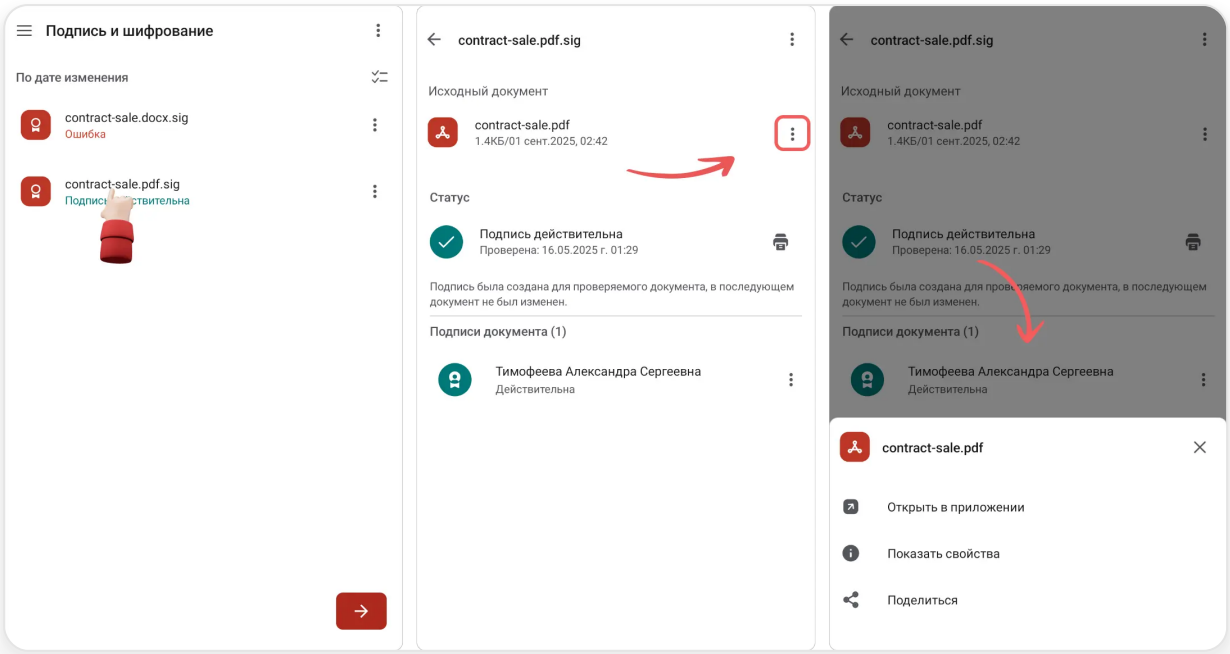
1. Выберите файлы в любом стороннем приложении.
2. Нажмите **Открыть с помощью** и выберите **КриптоАРМ**.

> 💡 **Совет**: Ненужный файл можно удалить из списка через меню **Еще** → **Удалить**.

Шаг 3. Результаты

1. После добавления документов запустится автоматическое расшифрование (если есть) и проверка подписи.
2. На панели с документом отобразится статус подписи. Подробнее про проверку подписи читайте в инструкции.
3. Нажмите на панель с подписанным файлом, либо вызовите меню действий с файлом по кнопке **Еще** ⋮ и выберите действие **Открыть**.

4. Откроется окно, в котором будет выведен общий статус подписи, список подписей и исходный документ.
5. В блоке **Исходный документ** будет отображён файл без подписи.



> 💡 **Совет**: Чтобы увидеть доступные действия с исходным документом, нажмите кнопку **Еще** ⋮.

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана. Просмотр подробной информации доступен в разделе **Журнал событий**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Рекомендуемые действия
Не найден подписанный документ. Невозможно проверить подпись	Добавьте в мастер исходный файл, для которого была сделана отсоединенная подпись. Или укажите путь к файлу в окне просмотра информации о подписи.

Инструкции по теме

- Как расшифровать документ
- Как проверить подпись документа
- Как зашифровать документ
- Как подписать документ

Открыть статью на сайте

Как расшифровывать документы в КриптоАРМ Подпись и шифрование

- Перед началом работы
- Расшифрование документа
- Возможные ошибки
- Инструкции по теме

Перед началом работы

Прежде чем приступить к расшифрованию документа, убедитесь, что рабочее место готово, а все необходимые инструменты установлены.

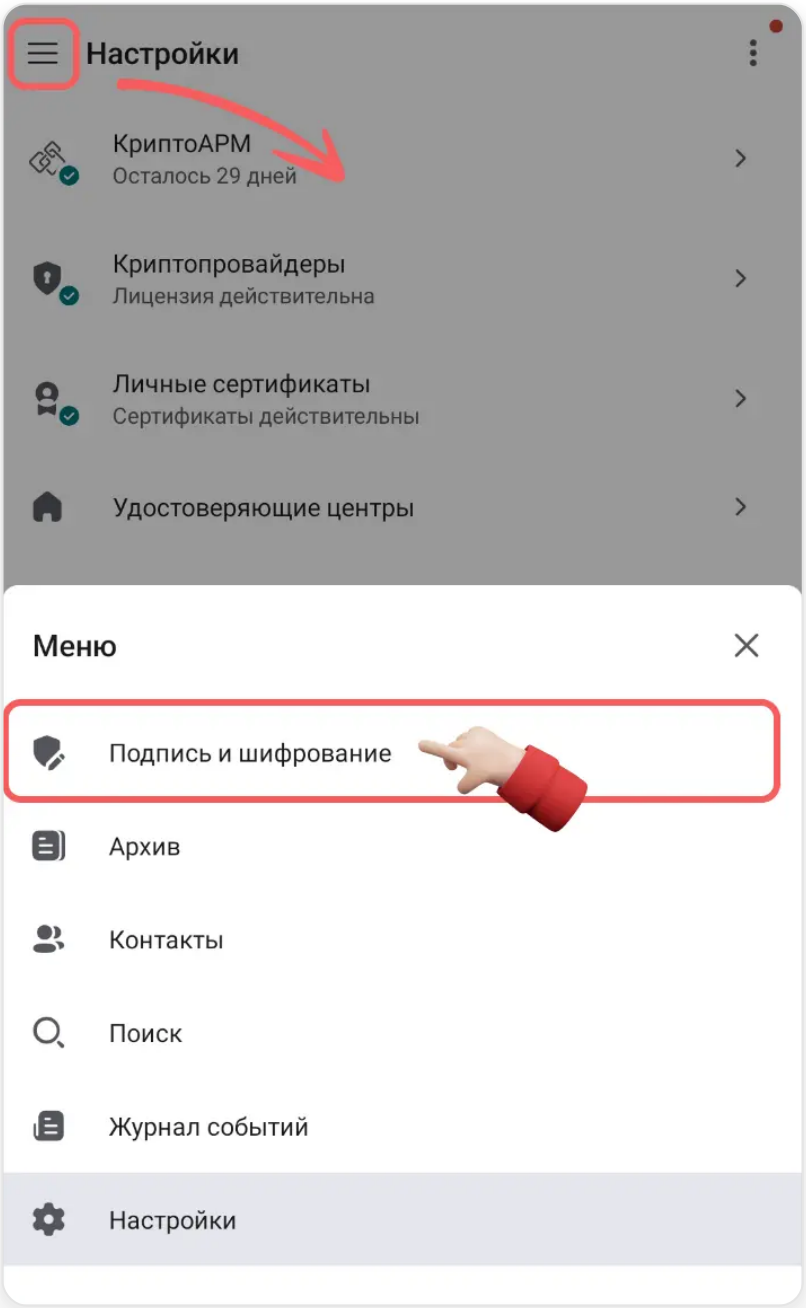
1. **Проверьте лицензии**: убедитесь в наличии действующих лицензий на КриптоАРМ и КриптоПро CSP. Без действующих лицензий расшифровать документ невозможно. Подробнее про лицензии читайте в инструкции Лицензирование.
2. **Установите личный сертификат**: в хранилище **Личные сертификаты** должен быть установлен сертификат, в адрес которого было выполнено шифрование. Подробная инструкция: Установка личного сертификата.

> 💡 **Совет**: Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

Расшифрование документа

Шаг 1. Запуск мастера

1. Вызовите главное меню по кнопке , размещенной в верхнем левом углу окна приложения.
2. Выберите пункт **Подпись и шифрование**.



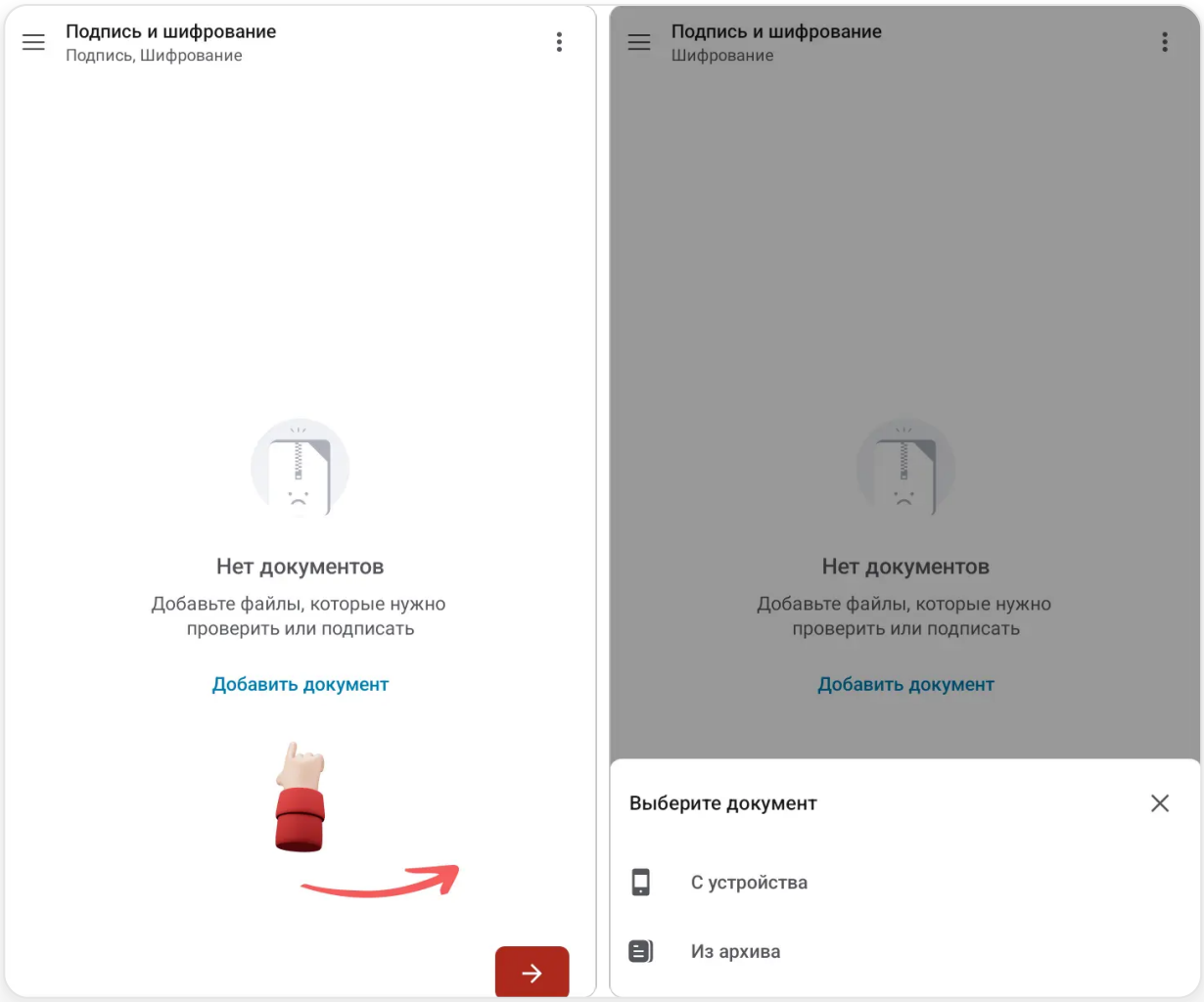
💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

Шаг 2. Добавление документов

Из мастера

1. В окне **Подпись и шифрование** нажмите на кнопку **Добавить документ**.
2. В появившемся меню выберите:
    - **С устройства** — для выбора файлов, сохраненных на устройстве,

- **Из архива** — для выбора файлов, сохраненных в разделе **Архив**.



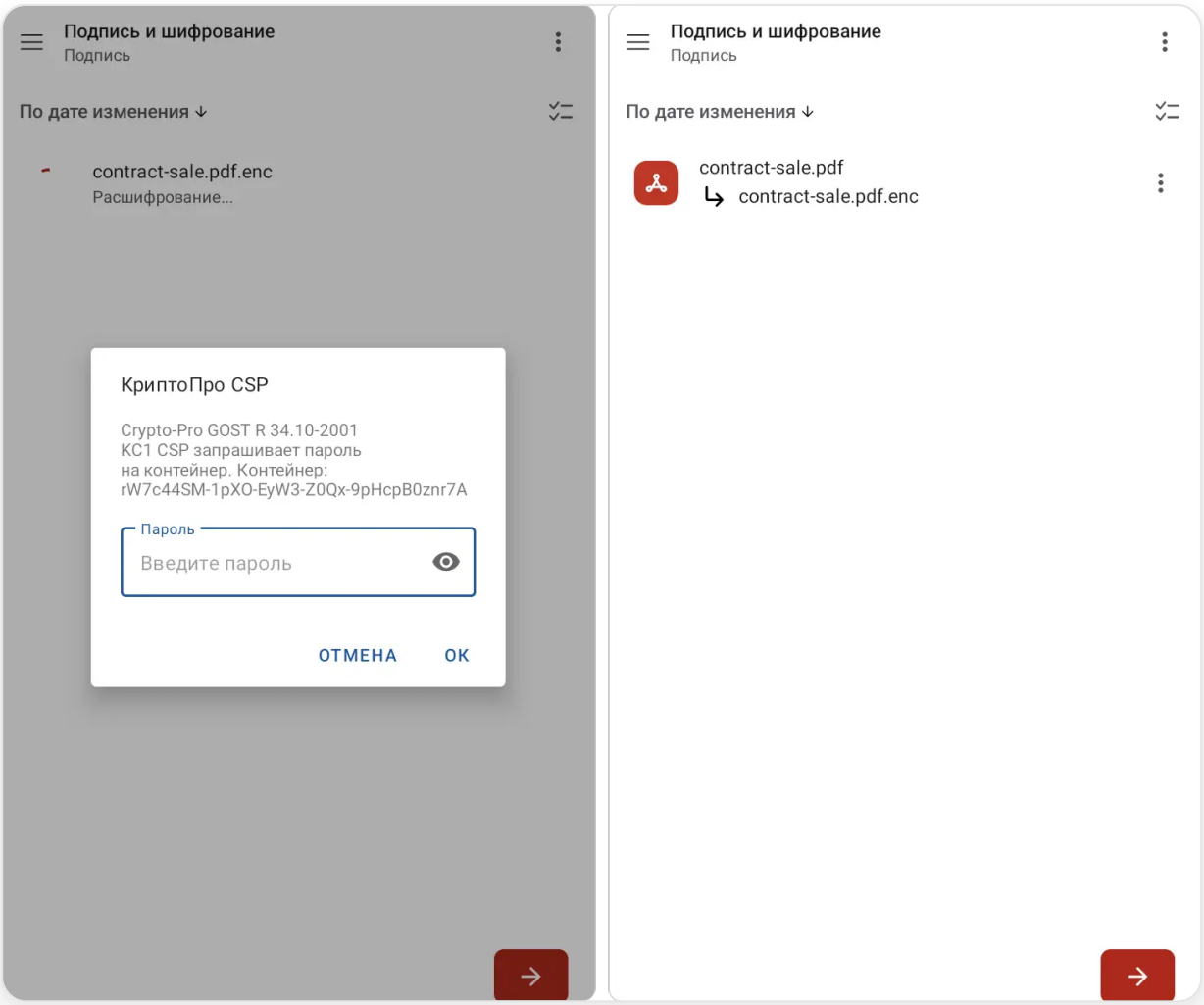
Из сторонних приложений

1. Выберите файлы в любом стороннем приложении.
2. Нажмите **Открыть с помощью** и выберите **КриптоАРМ**.

> 💡 **Совет**: Ненужный файл можно удалить из списка через меню **Еще** → **Удалить**.

Шаг 3. Результаты

1. После добавления документов запустится автоматическое расшифрование и проверка подписи (если есть).
2. При необходимости укажите пароль на контейнер с личным сертификатом.



После завершения операции в списке отобразится расшифрованный файл.

> 💡 **Совет**: Чтобы увидеть доступные действия с расшифрованным документом, нажмите кнопку **Еще** ⋮ .

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана.

Просмотр подробной информации доступен в разделе **Журнал событий**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

Ошибка	Описание	Рекомендуемые действия
Невозможно просмотреть содержимое зашифрованного файла	Не обнаружен сертификат расшифрования	Убедитесь в наличии сертификата для расшифрования в хранилище **Личные сертификаты**
Произошла ошибка	Введен неверный пароль для доступа к закрытому ключу	Добавьте файл повторно и укажите верный пароль на контейнер
Отсутствует лицензия на приложение КриптоАРМ	Истек срок действия или не активирована лицензия КриптоАРМ	1. Приобретите лицензию КриптоАРМ 2. Установите лицензию в настройках приложения
Произошла ошибка	Не обнаружена действующая лицензия криптопровайдера КриптоПро CSP	1. Приобретите лицензию КриптоПро CSP 2.Установите лицензию в настройках приложения.

Инструкции по теме

- Как проверить подпись документа
- Как снять подпись с документа
- Как зашифровать документ
- Как подписать документ

Открыть статью на сайте

Как управлять документами в КриптоАРМ Подпись и шифрование

- Для чего нужна папка «Архив»?
- Доступные действия
- Инструкции по теме

Для чего нужна папка «Архив»?

Папка **Архив** предназначена для безопасного и удобного хранения подписанных, зашифрованных и других важных документов.

Какие файлы можно хранить в «Архиве»?

- Подписанные файлы,
- Зашифрованные файлы,
- Машиночитаемые доверенности,
- Другие резервные копии важных документов.

Основные функции

- Помогает избежать потери документов,
- Быстрый доступ к ранее обработанным документам,
- Использование документов без повторной загрузки.

Автосохранение документов в «Архив»

Чтобы включить автосохранение результатов операций, активируйте опцию **Сохранить в «Архив»** в профиле подписи. Все файлы, созданные при работе с этим профилем, будут автоматически сохраняться в указанную папку раздела **Архива**.

Особенности работы:

1. При создании отсоединенной подписи в **Архив** сохраняется:
    - Файл подписи,
    - Копия исходного документа.
2. Промежуточные файлы операций не сохраняются.
3. В профиле подписи можно настроить действия при соподписи документов из **Архива**.

Доступные действия

> 💡 **Совет**: Чтобы совершить действие сразу с несколькими документами или папками выберите **Выбрать все** в меню, которое доступно по кнопке **Еще** . В списке появятся флажки. Отметьте нужные документы или папки и выберите необходимое действие.

Просмотр документа

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий по кнопке **Еще** , размещенной на панели с файлом.
3. В открывшемся меню действий выберите действие **Открыть**.

   В зависимости от настроек устройства произойдет одно из двух:

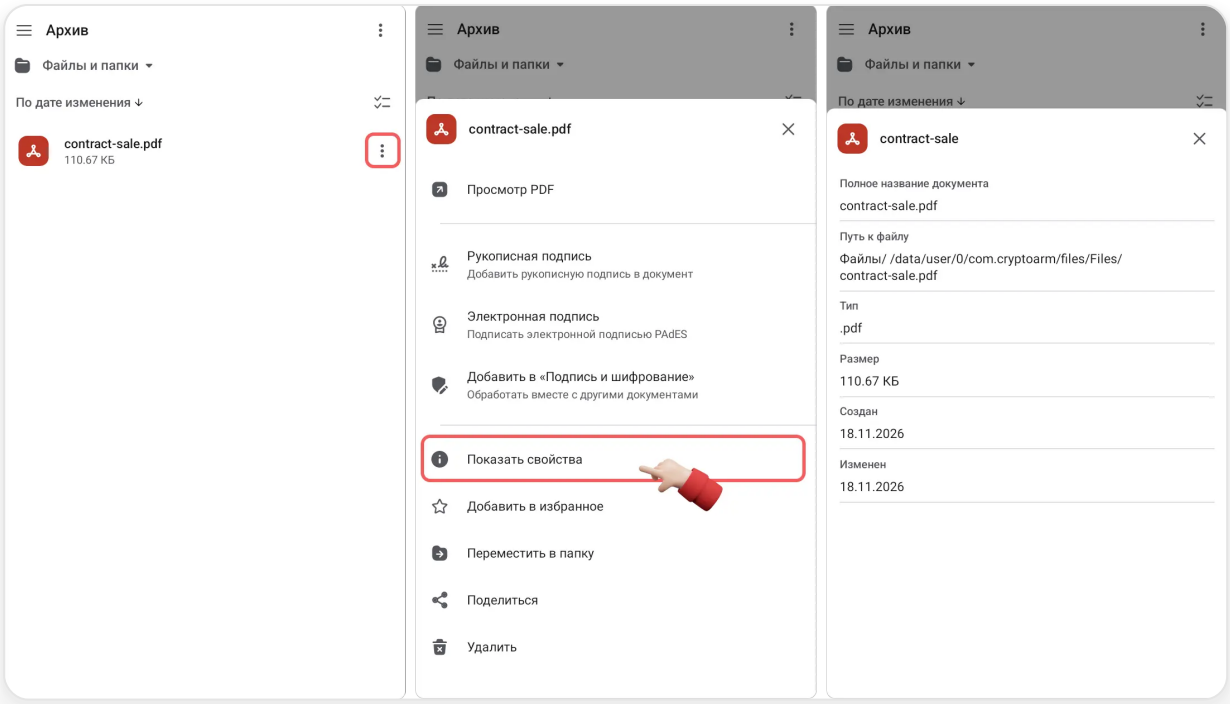
   - появится список приложений, поддерживающих открытие файла, — выберите нужное;
   - файл сразу откроется в приложении, установленном на устройстве по умолчанию для данного типа файлов.

> 📌 **Примечание:** PDF-файлы можно просматривать непосредственно в просмотрщике **КриптоАРМ Подпись и шифрование**.

Дальнейшие действия зависят от выбранного приложения. Чтобы вернуться в **КриптоАРМ Подпись и шифрование**, воспользуйтесь системной навигацией устройства.

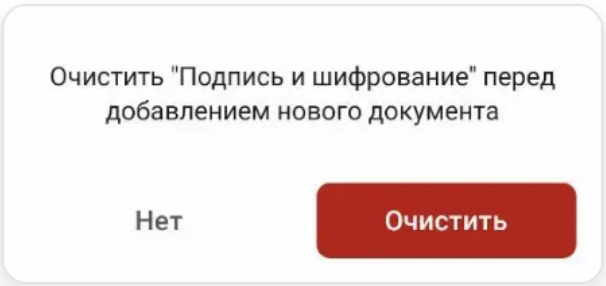
Просмотр свойств

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий с документом.
3. В открывшемся меню действий выберите действие **Показать свойства**.
4. Откроется окно со свойствами файла.



Добавление в мастер

1. Перейдите в раздел **Архив**.
2. Нажмите кнопку **Еще** на панели с файлом и выберите действие. В зависимости от типа файла доступны следующие варианты:
   - **Рукописная подпись** — добавить изображение рукописной подписи;
   - **Электронная подпись** — подписать документ по стандарту PAdES в мастере **Подпись и защита PDF**;
   - **Добавить в «Подпись и шифрование»** — обработать файл вместе с другими документами.
3. Если в мастере **Подпись и шифрование** уже есть документы, выберите, нужно ли очистить список перед добавлением нового документа.



Работа с избранным

Избранные документы — это те документы, которые вы считаете важными или часто используете и хотите иметь быстрый доступ к ним.

Добавление в избранное

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий с документом.
3. В появившемся меню выберите действие **Добавить в избранное**.

Документ будет помечен как «Избранный». На документе появится иконка — звездочка .
Документ станет доступен в специальной группе **Избранные**.

> 🔍 Подробнее про группы читайте в инструкции Группировка документов.

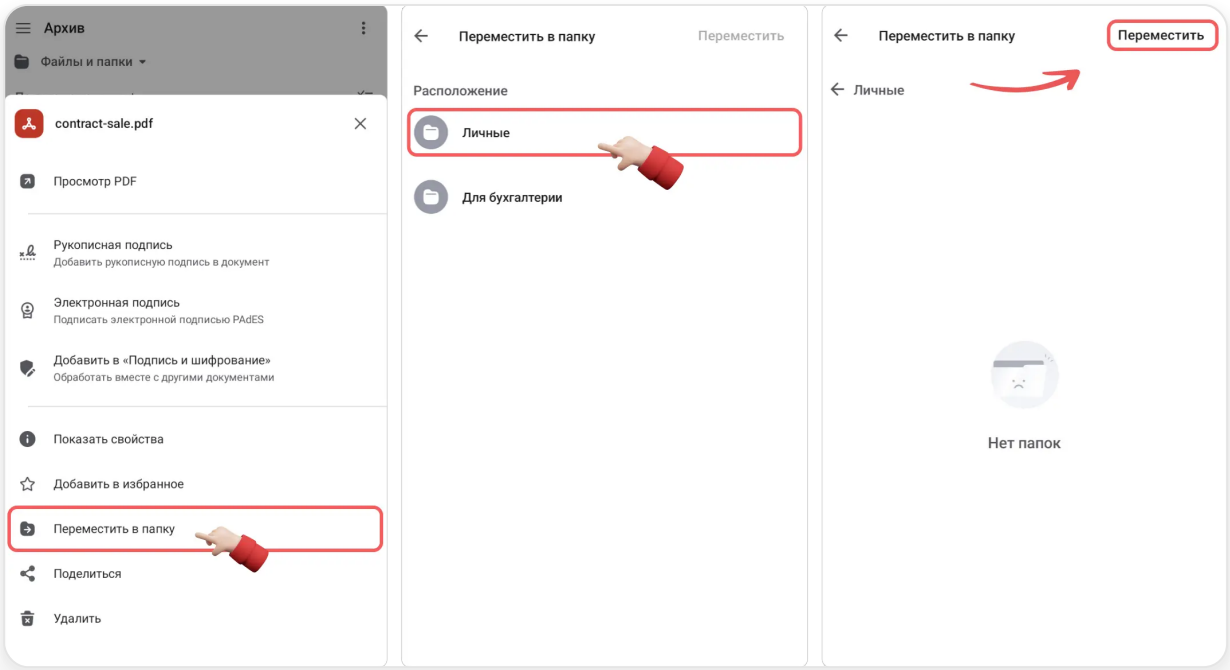
Удаление из избранного

1. Откройте раздел **Архив**.
2. Вызовите меню действий с документом.
3. В появившемся меню выберите действие **Удалить из избранного**.

Документ будет удален из «Избранных».

Перемещение документа

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий с документом.
3. В появившемся меню выберите действие **Переместить в папку**.
4. В открывшемся окне выберите папку и нажмите **Переместить**.



Поделиться документом

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий, которое открывается по кнопке **Еще** , размещенной на панели с документом в списке.
3. В появившемся меню выберите действие **Поделиться**.
4. Откроется системное окно со списком приложений.
5. Выберите приложения для отправки или сохранения документа.

Удаление документа

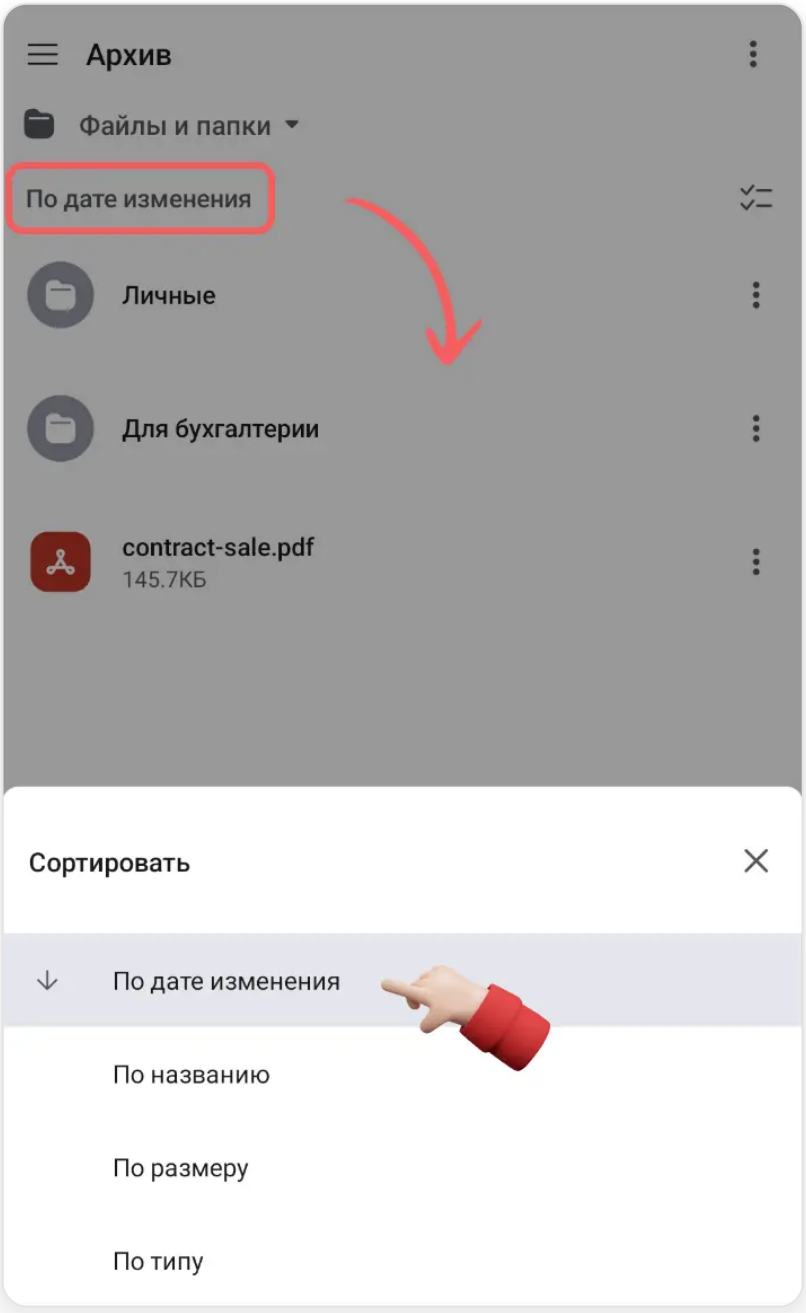
> 🚨 **Примечание**: Документы удаляются без возможности восстановления.

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий с документом.
3. В появившемся меню выберите действие **Удалить**.
4. Подтвердите действие в модальном окне.

После удаления документа будет отображено уведомление об успешном выполнении операции. Документ пропадет из списка.

Сортировка документов

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий **Сортировка**.



3. Настройте тип сортировки.
4. Настройте порядок сортировки. Чтобы изменить порядок сортировки, нажмите на панель с выбранным типом сортировки.

Изменения применяются автоматически и не требуют дополнительного сохранения.

Инструкции по теме

- Группировка документов в папке «Архив»

Открыть статью на сайте

Группировка документов в КриптоАРМ Подпись и шифрование

- Общая информация
- Создание папки
- Действия с папками
- Инструкции по теме

Общая информация

Группировка документов в папки позволяет организовать файлы и упростить их поиск. В приложении поддерживается многоуровневая вложенность папок.

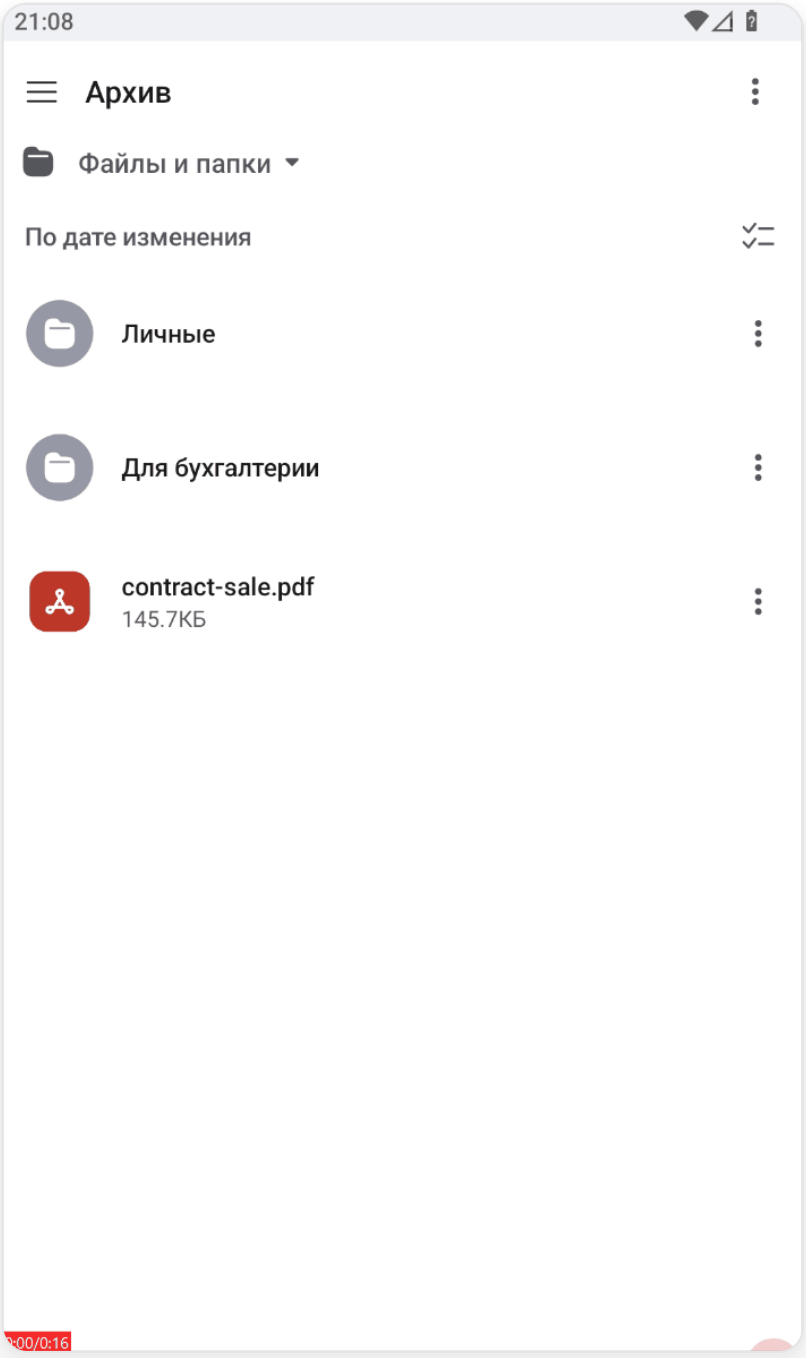
После установки в приложении доступны следующие папки:

- **Все документы** - специальная папка, в которой отображаются документы из всех папок.
- **Избранные** - специальная папка, в которой отображаются все документы, отмеченные как избранные.
- **Файлы и папки** - корневая папка, в которой можно создавать собственные папки и подпапки.

Создание папки

> 💡 **Совет**: В приложении можно создавать несколько уровней вложенности папок. Для этого используйте символ `/` в названии. Например, если указать `Проекты/2025`, будут созданы две папки: `Проекты` и вложенная в нее `2025`.

1. Откройте раздел **Архив**.
2. Перейдите в окно **Создать группу** одним из способов:
   - Откройте меню **Действия** по кнопке **Еще** и выберите действие **Создать** → **Создать папку**.
   - Откройте окно со списком папок и нажмите на кнопку **Создать папку** .
3. Укажите название группы и ее расположение.
4. Нажмите **Сохранить**.

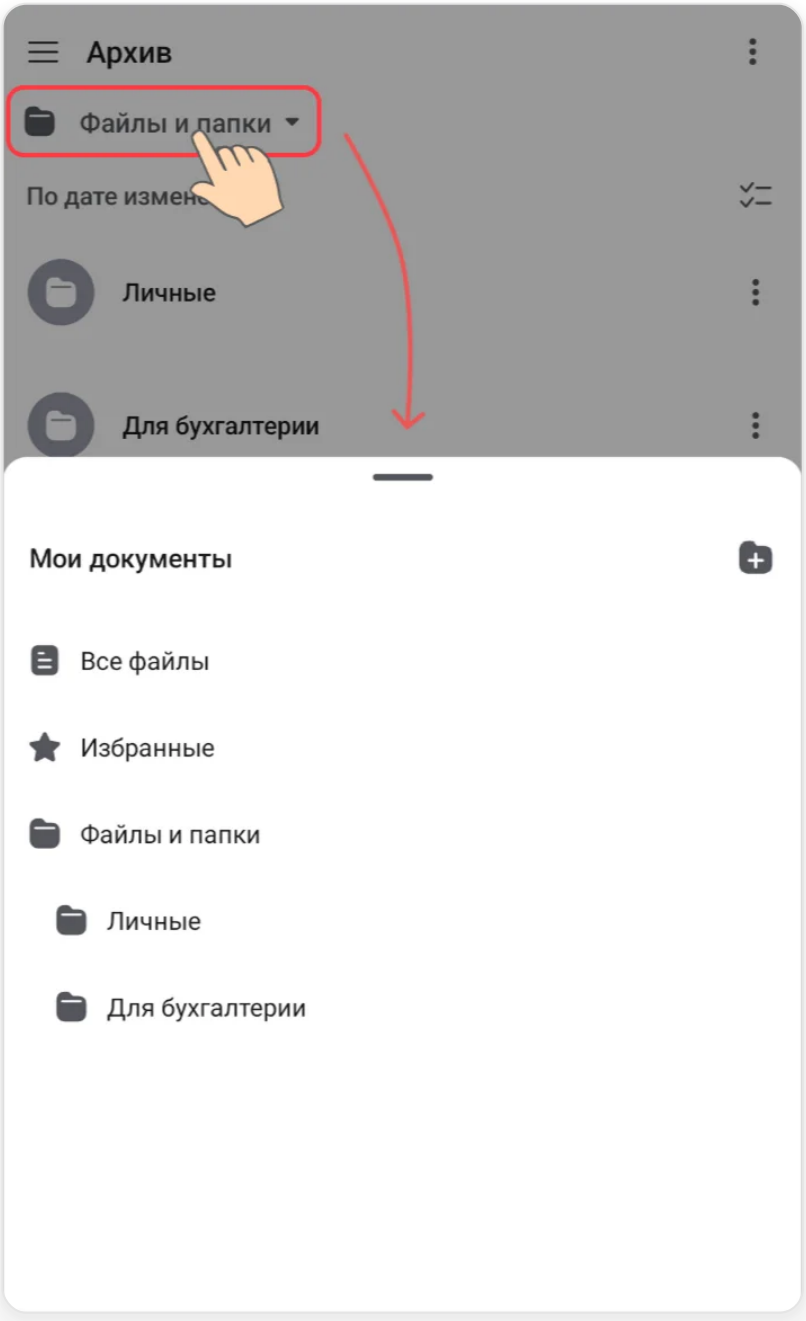


Действия с папками

> 💡 **Совет**: Чтобы совершить действие сразу с несколькими документами или папками, нажмите **Выбрать все** в меню по кнопке **Еще** ⋮, отметьте нужные документы и выберите необходимое действие.

1. Открытие списка папок

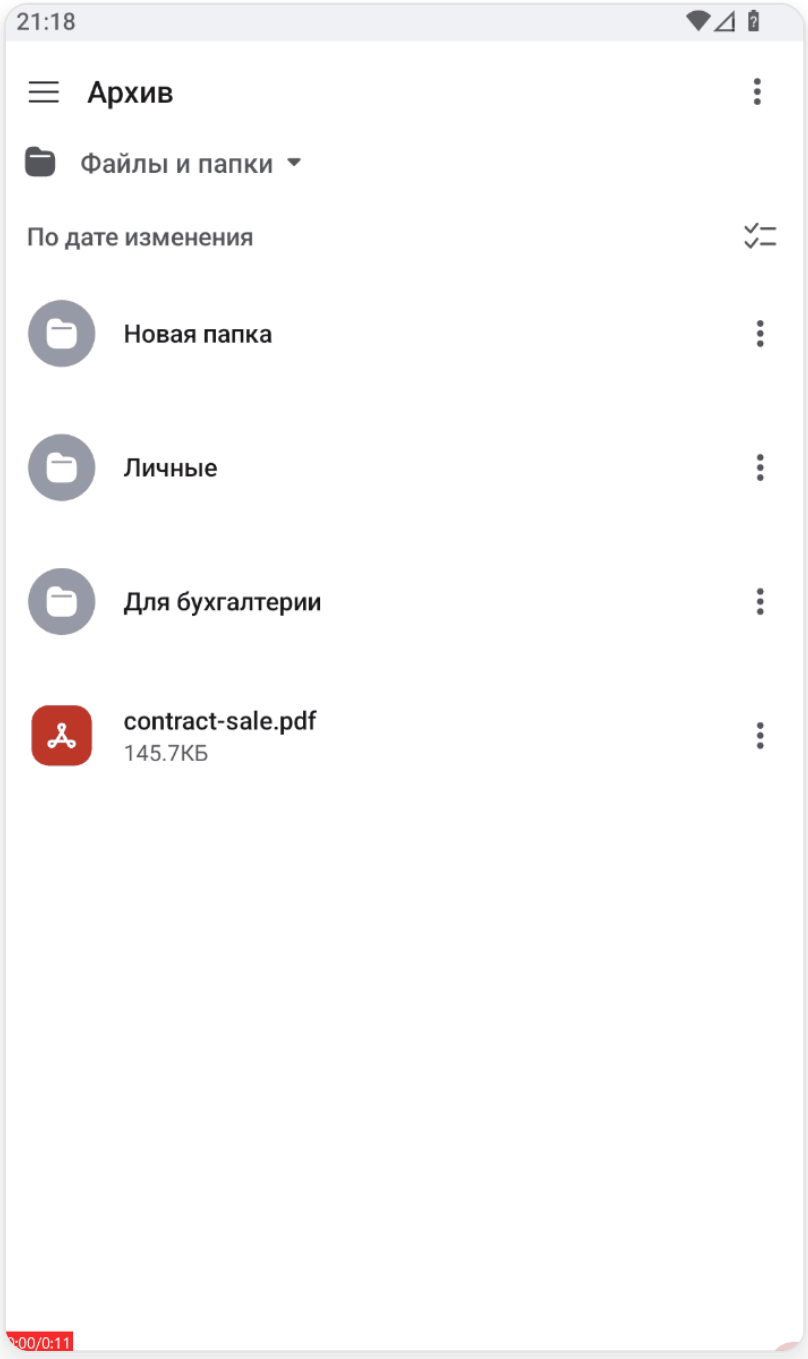
1. Откройте раздел **Архив**.
2. Нажмите на кнопку с названием активной папки.
3. Откроется окно со списком папок, созданных в приложении.



2. Перемещение папки

1. Откройте раздел **Архив**.
2. Вызовите меню действий по кнопке **Еще** , размещенной на панели с папкой.
3. В появившемся меню выберите действие **Переместить в папку**.

4. В открывшемся окне выберите папку и нажмите **Переместить**.

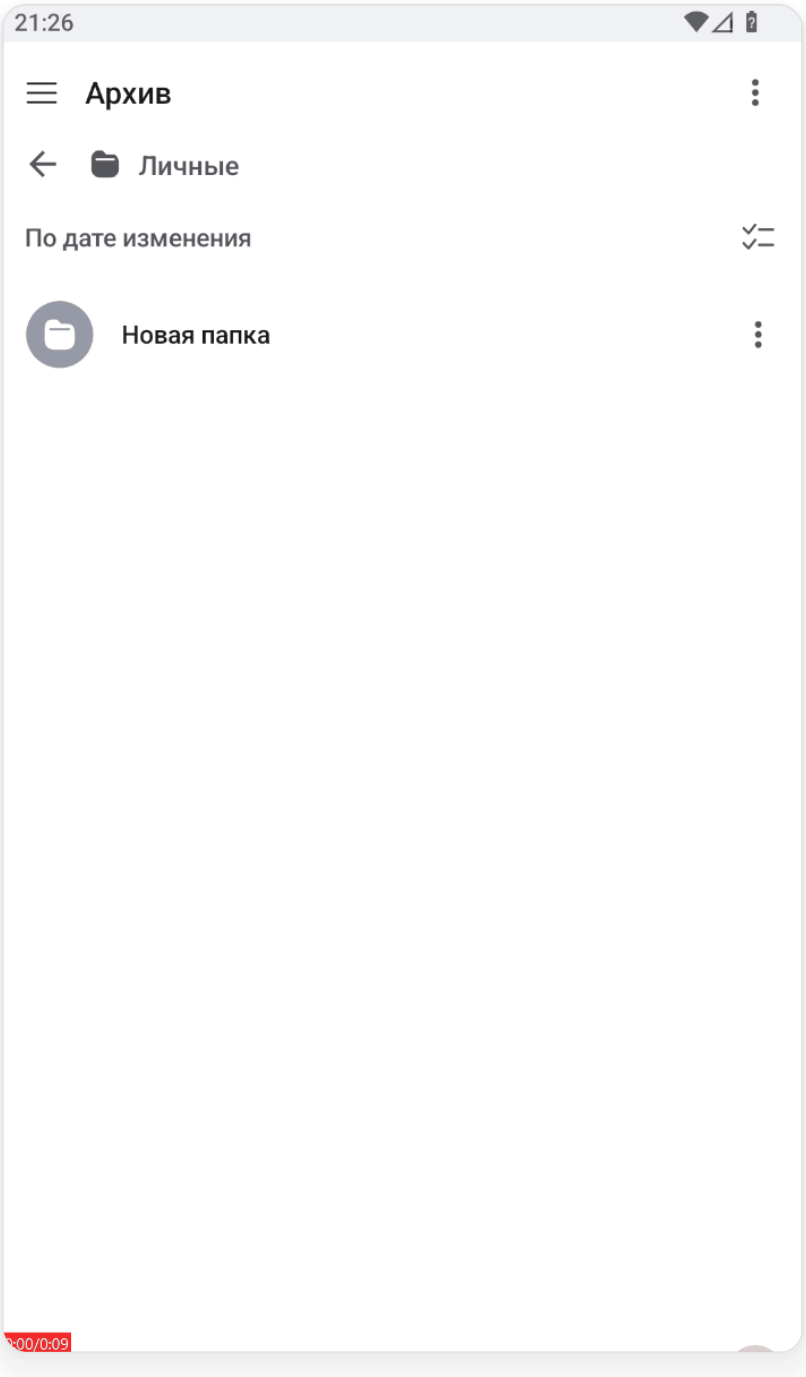


3. Удаление папки

> 🚨 **Примечание**: Удаление папки означает безвозвратное удаление всей информации, связанной с этой папкой. Это включает в себя удаление всех документов папки и ее подпапок. После удаления папки восстановить информацию невозможно.

1. Откройте раздел **Архив**.

2. Вызовите меню действий по кнопке **Еще** , размещенной на панели с папкой.
3. В появившемся меню выберите действие **Удалить**.
4. Подтвердите действие в модальном окне.



После удаления папки будет отображено уведомление об успешном выполнении операции. Папка пропадет из списка.

Инструкции по теме

- Действия с документами в папке «Архив»

Открыть статью на сайте

Работа с облачными папками в КриптоАРМ Подпись и шифрование

Раздел **Документы** предназначен для работы с документами, которые хранятся во внешних информационных системах и доступны через подключенные сетевые профили.

Доступ к облачным папкам осуществляется через сетевой профиль, в котором сохранены параметры подключения к информационной системе.

В приложении документы из облака распределяются по папкам **Входящие**, **Исходящие** и пользовательским папкам.

В отличие от **Архива**, облачные папки не являются самостоятельным локальным хранилищем. Их содержимое синхронизируется с внешней информационной системой. При этом приложение может сохранять локальные копии документов, необходимые для работы с ними.

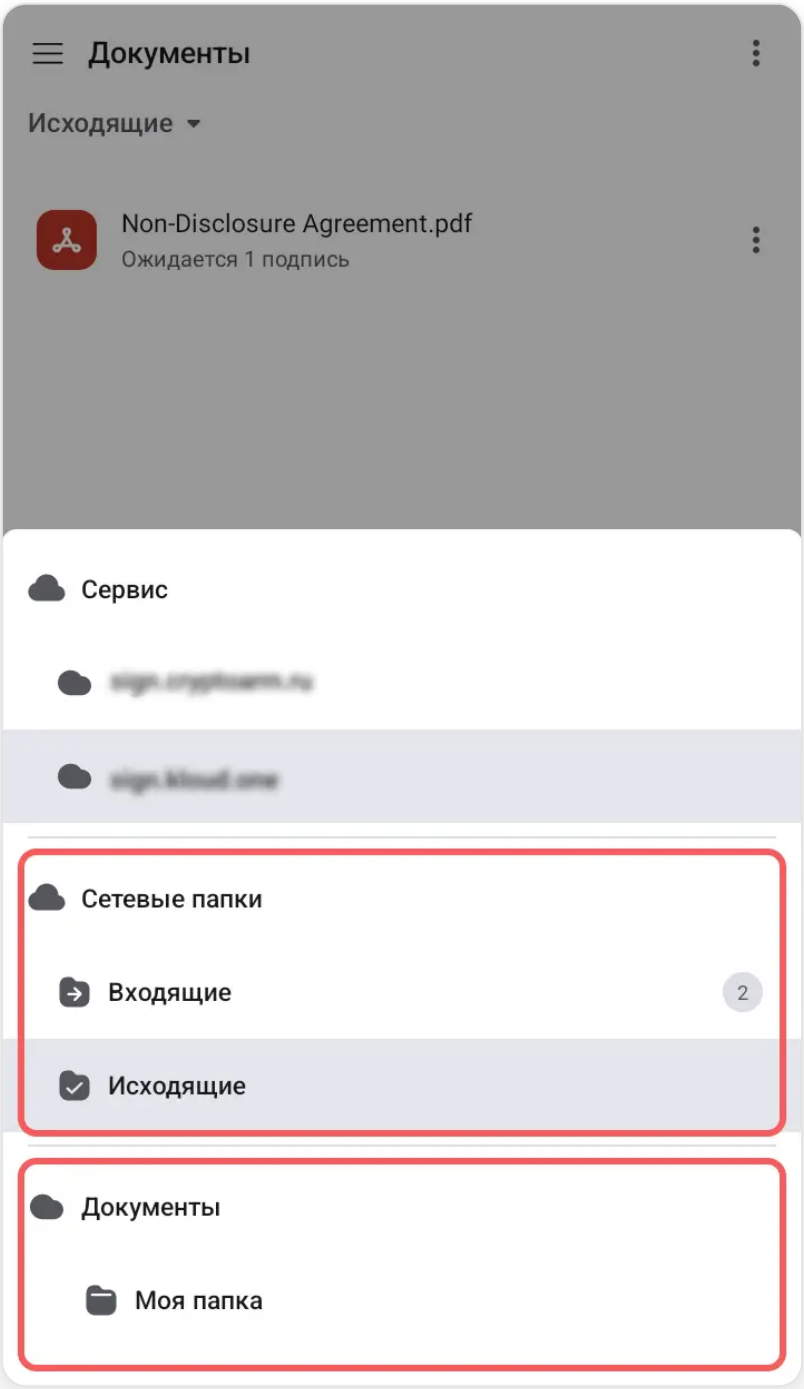
> ⚠️ **Примечание:** Для работы с облачными папками и обмена данными с информационной системой требуется подключение к сети.

Навигация по облачным папкам

Документы в облачном хранилище распределены по сетевым профилям и папкам:

- **Входящие** — документы, которые другие пользователи информационной системы направили вам на подпись.
- **Исходящие** — документы, которые вы направили на подпись другим пользователям информационной системы.
- **Пользовательские папки** — папки, созданные вами в информационной системе.

Пользовательские папки отображаются в боковом меню рядом с папками **Входящие** и **Исходящие**.



Папка «Входящие»

В папке **«Входящие»** отображаются документы, которые другие пользователи информационной системы направили вам на подпись.

Документы сгруппированы по пакетам. Чтобы просмотреть файлы, входящие в пакет:

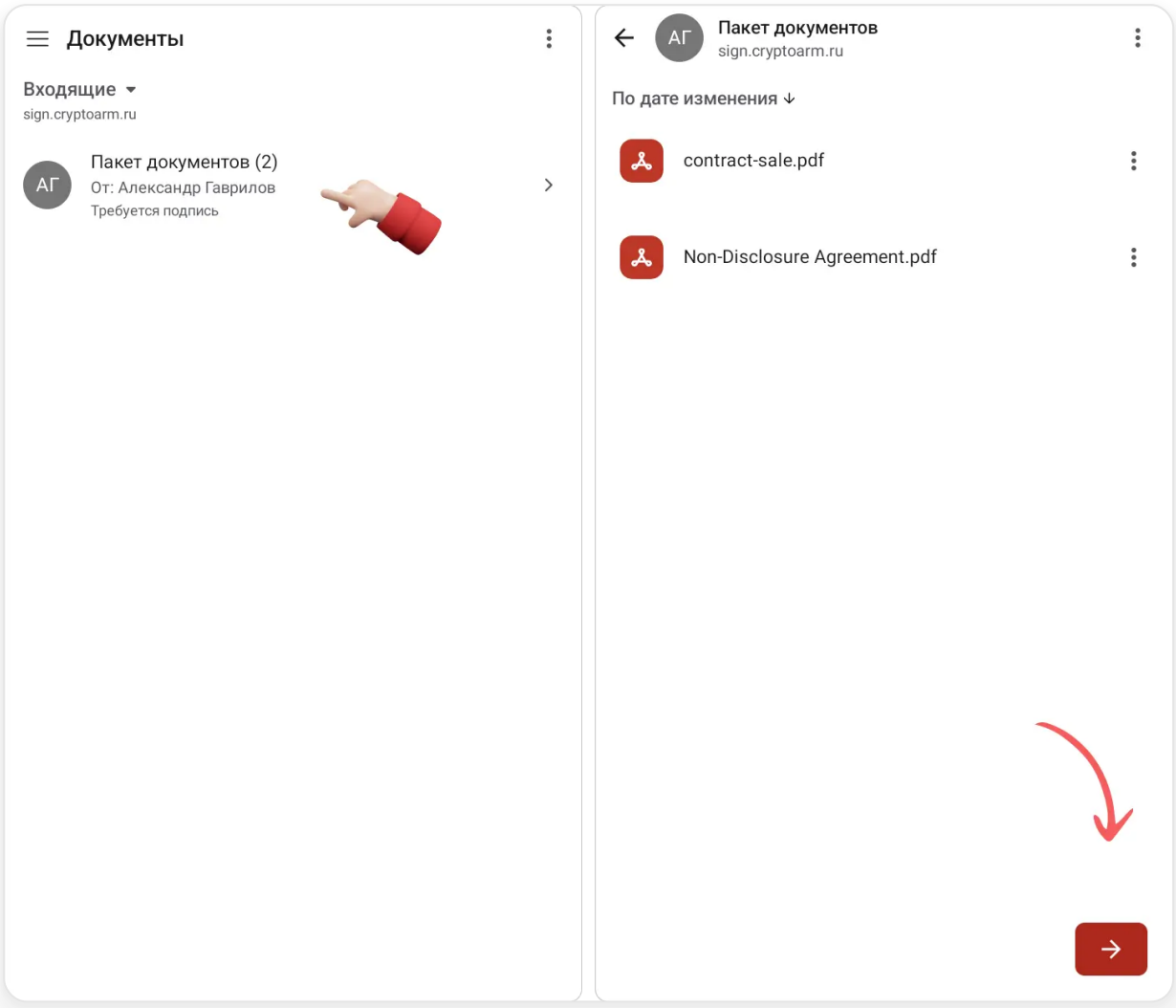
1. Откройте папку **«Входящие»**.
2. Нажмите на панель с нужным пакетом.

3. В открывшемся списке выберите файл для просмотра.

Подписание документа

Чтобы подписать документ:

1. Откройте нужный файл из списка документов пакета.



2. Нажмите **Подписать** в нижней части экрана.

3. Дождитесь завершения создания электронной подписи и ее выгрузки в облако.

Параметры создания подписи задаются в настройках сетевого профиля.

В отличие от документов из пользовательских папок, подпись для документов из папки **Входящие** автоматически выгружается в информационную систему и прикрепляется к исходному документу.

После завершения подписания:

- файл электронной подписи прикрепляется к исходному документу в облачной папке;
- подписанный документ исчезает из папки **«Входящие»**;

- статус документа для отправителя изменяется.

> ⚠️ **Примечание:** Для выгрузки электронной подписи в информационную систему требуется подключение к сети.

Просмотр списка подписантов

Чтобы посмотреть, кому документ был направлен на подпись:

1. Вызовите меню действий с нужным файлом.
2. Выберите **Показать подписантов**.

Откроется окно со списком пользователей, которым документ был направлен на подпись через информационную систему.

Папка «Исходящие»

В папке **Исходящие** отображаются документы, которые вы направили на подпись другим пользователям информационной системы.

> ⚠️ **Примечание:** В текущей версии **КриптоАРМ Подпись и шифрование** отправить документ на подпись непосредственно из приложения нельзя. Сначала направьте документ на подпись через интерфейс информационной системы. После этого он появится в папке **Исходящие**.

Просмотр списка подписантов и статусов подписания

Чтобы посмотреть, кому направлен документ и кто уже поставил подпись:

1. Перейдите в раздел **Документы** и откройте папку **Исходящие**.
2. Вызовите меню действий с нужным файлом.
3. Выберите **Показать подписантов**.

Откроется список пользователей, которым был направлен документ. Для каждого подписанта отображаются имя и дата подписания, если подпись уже создана. Если пользователь еще не подписал документ, вместо даты отображается статус **Ожидается подпись**.

> 💡 **Совет:** После того как подписант поставит подпись, статус документа в папке **Исходящие** обновится автоматически.

Инструкции по теме

- Действия с документами в папке «Архив»
- Группировка документов в папке «Архив»

Открыть статью на сайте

Как создать контакт в КриптоАРМ Подпись и шифрование

- Добавление нового контакта
- Описание полей контакта
- Инструкции по теме

Добавление нового контакта

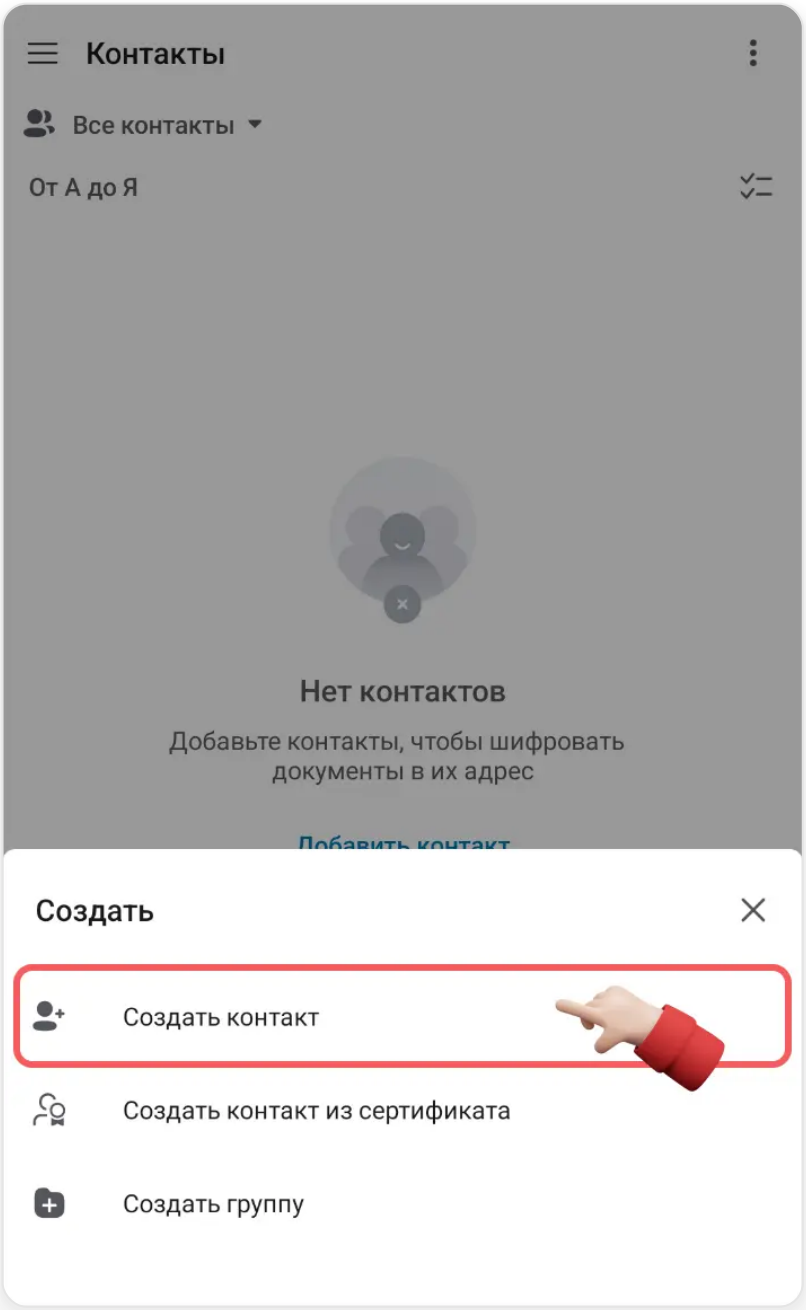
В КриптоАРМ можно создать контакт с расширенным профилем, который будет включать:

- Личные данные (ФИО, должность, компания),
- Различные контактные данные (телефоны, email, адреса),
- Фотографию,
- Сертификаты.

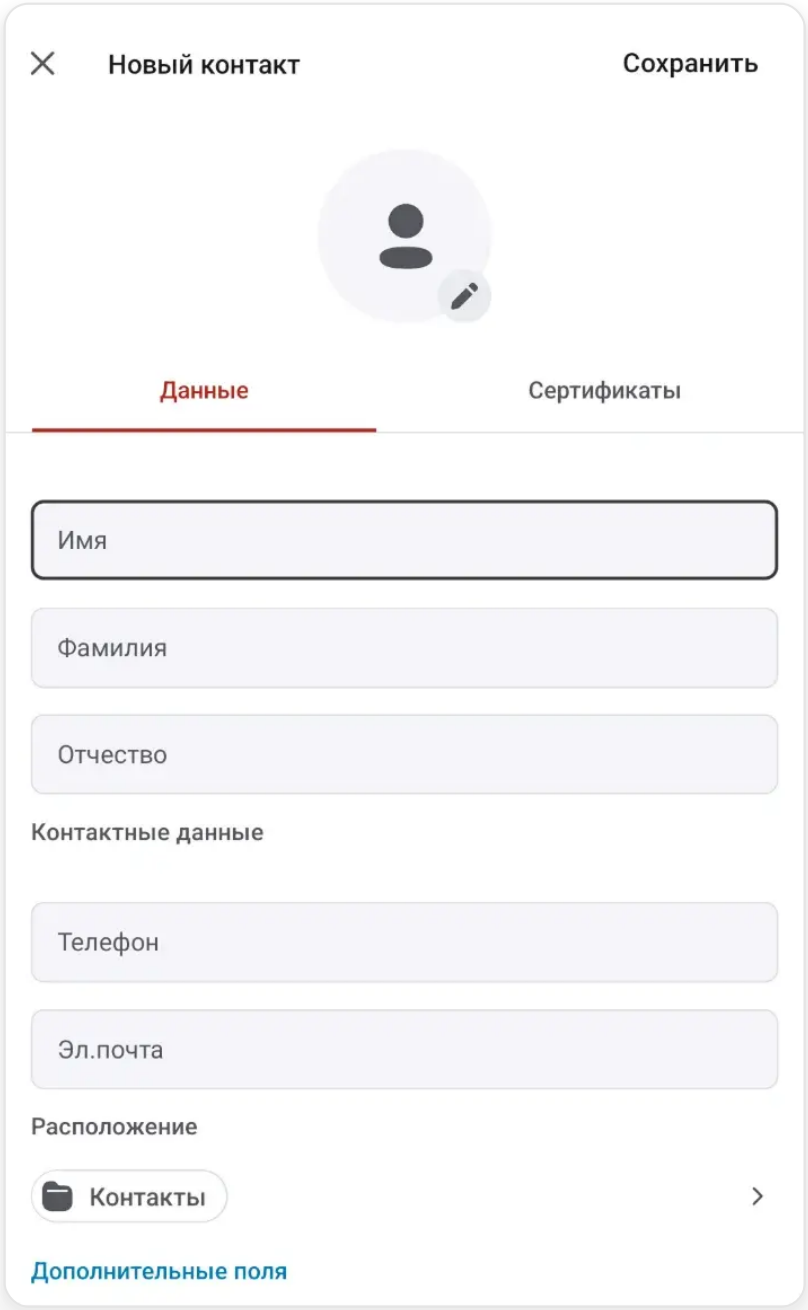
> 💡 **Совет**: Сертификаты используются для шифрования файлов в адрес контакта.

1. Стандартный способ

1. Откройте раздел **Контакты**.
2. Вызовите меню действий **Создать** одним из способов:
    - Нажмите на кнопку **Добавить контакт** в центре окна, если в приложении отсутствуют контакты,
    - Вызовите меню действий по кнопке **Еще** и выберите действие **Создать**.
3. В появившемся меню выберите действие **Создать контакт**.



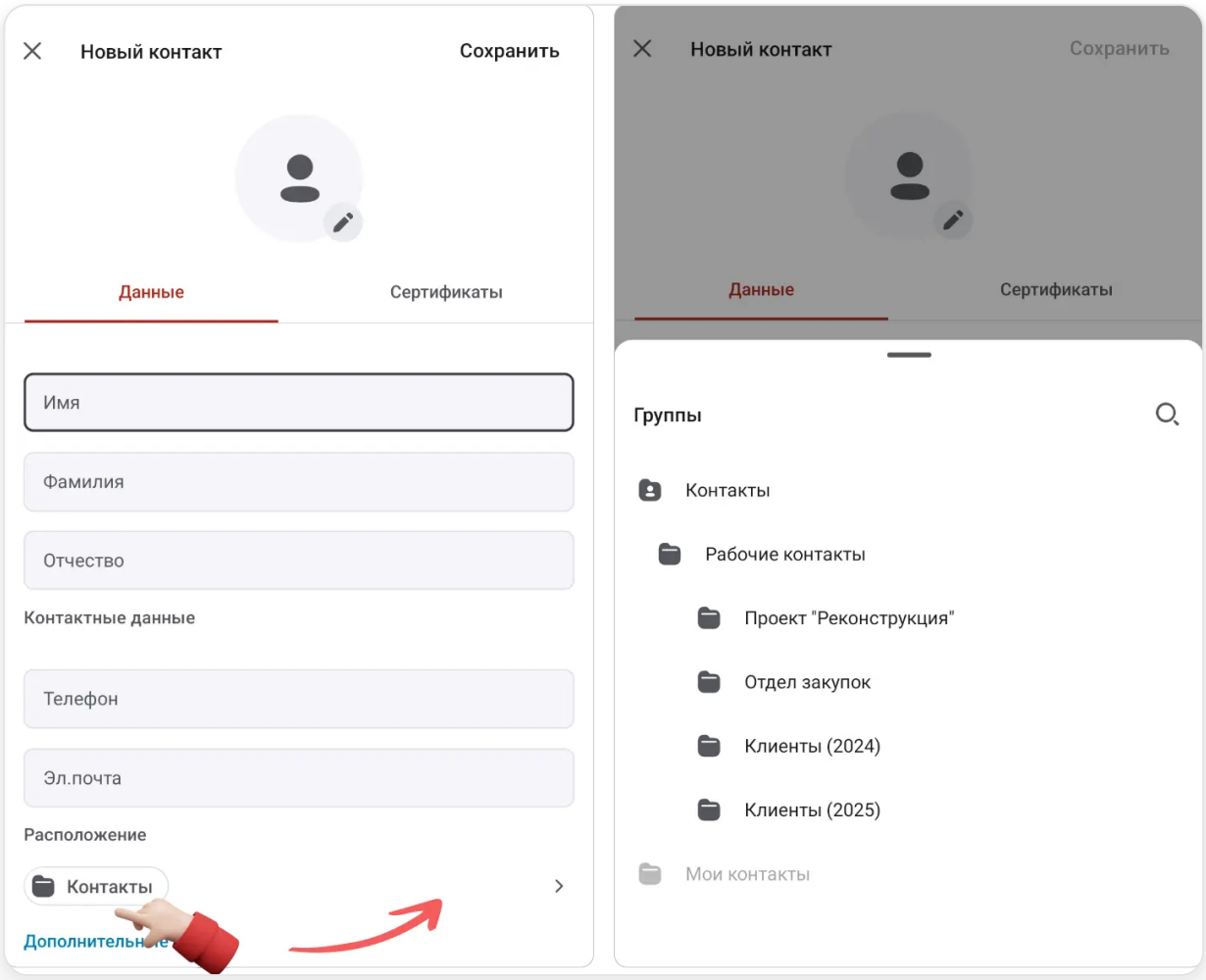
4. Откроется форма создания контакта.



5. При необходимости добавьте к контакту фото. Для этого нажмите на кнопку и выберите фото в системном окне файлового менеджера.

6. Заполните сведения о контакте на вкладке **Данные**.

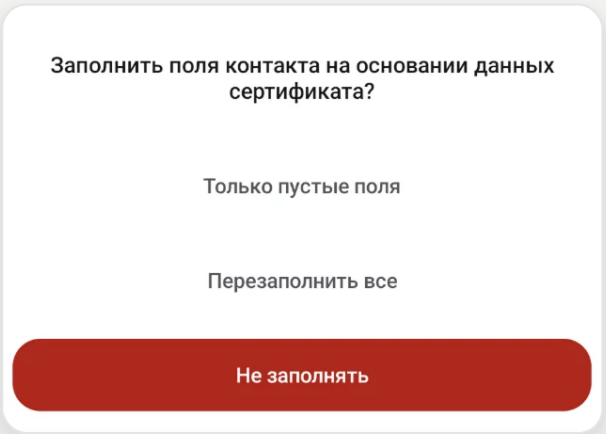
7. Выберите группу для создания контакта. По умолчанию контакт будет добавлен в активную группу. Чтобы изменить группу, нажмите на её название в разделе **Расположение** и выберите нужную группу.



8. Добавьте электронный сертификат на вкладке **Сертификаты**.

🔍 Подробнее читайте в инструкции Добавление сертификата.

💡 **Совет**: При выборе сертификата доступно заполнение полей контакта на основании данных сертификата.



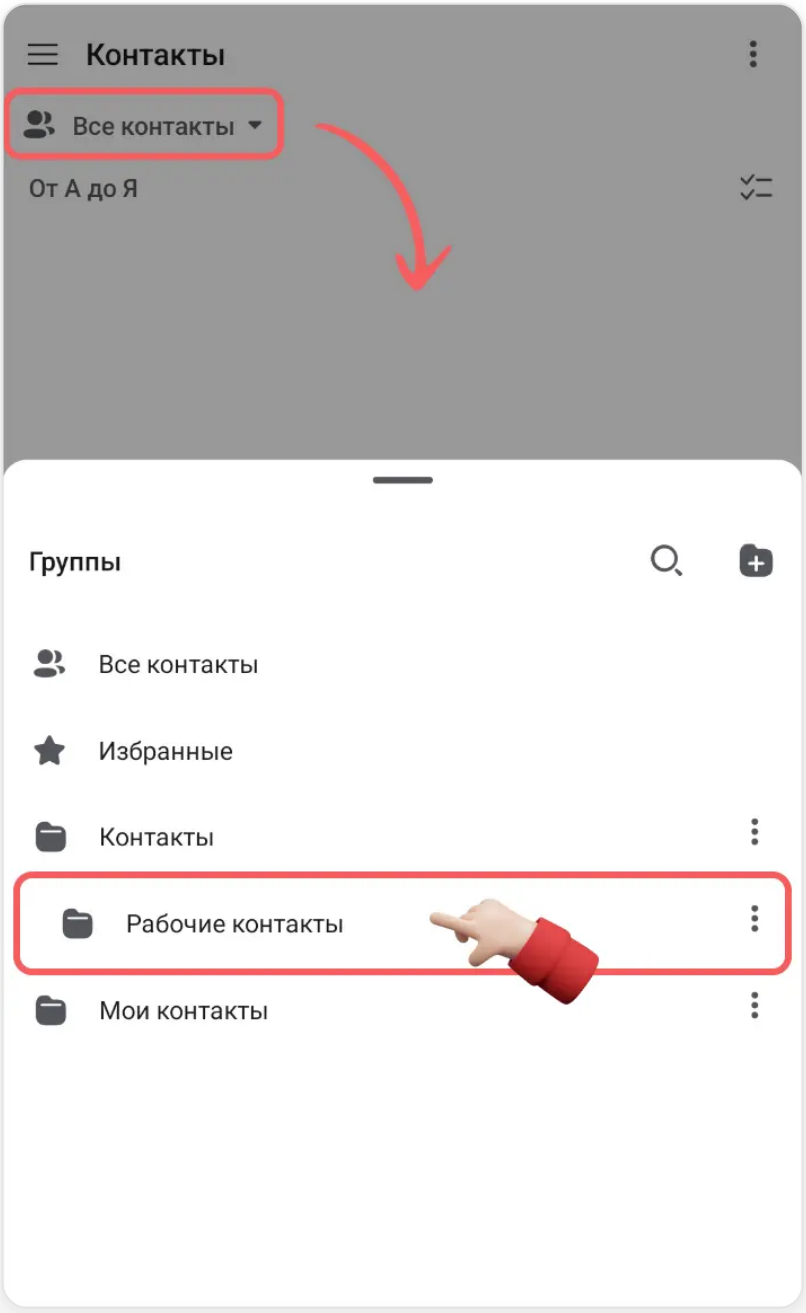
9. Нажмите на **Сохранить**.

При успешном создании контакт будет сохранен в указанную группу.

2. Создание из сертификата

> 💡 Прежде чем приступить к созданию контакта, убедитесь, что в памяти устройства сохранен файл с сертификатом с расширением `.cer`/`.crt`.

1. Откройте раздел **Контакты**.
2. Перейдите в группу, в которой необходимо создать контакт. Для этого нажмите на кнопку **Все контакты** в верхней части окна и в появившемся меню нажмите на название необходимой группы.



⚠️ **Примечание**: По умолчанию контакт будет добавлен в активную группу.

3. Вызовите меню действий **Создать** одним из способов:
   - Нажмите на кнопку **Добавить контакт** в центре окна, если в приложении отсутствуют контакты,
   - Вызовите меню действий по кнопке **Еще** ⋮ и выберите действие **Создать**.
4. В появившемся меню выберите действие **Создать контакт из сертификата**.
5. Откроется окно файлового менеджера.

6. Выберите в окне один или несколько файлов с расширением `.cer`/`.crt`
7. Запустится автоматический процесс создания контактов.

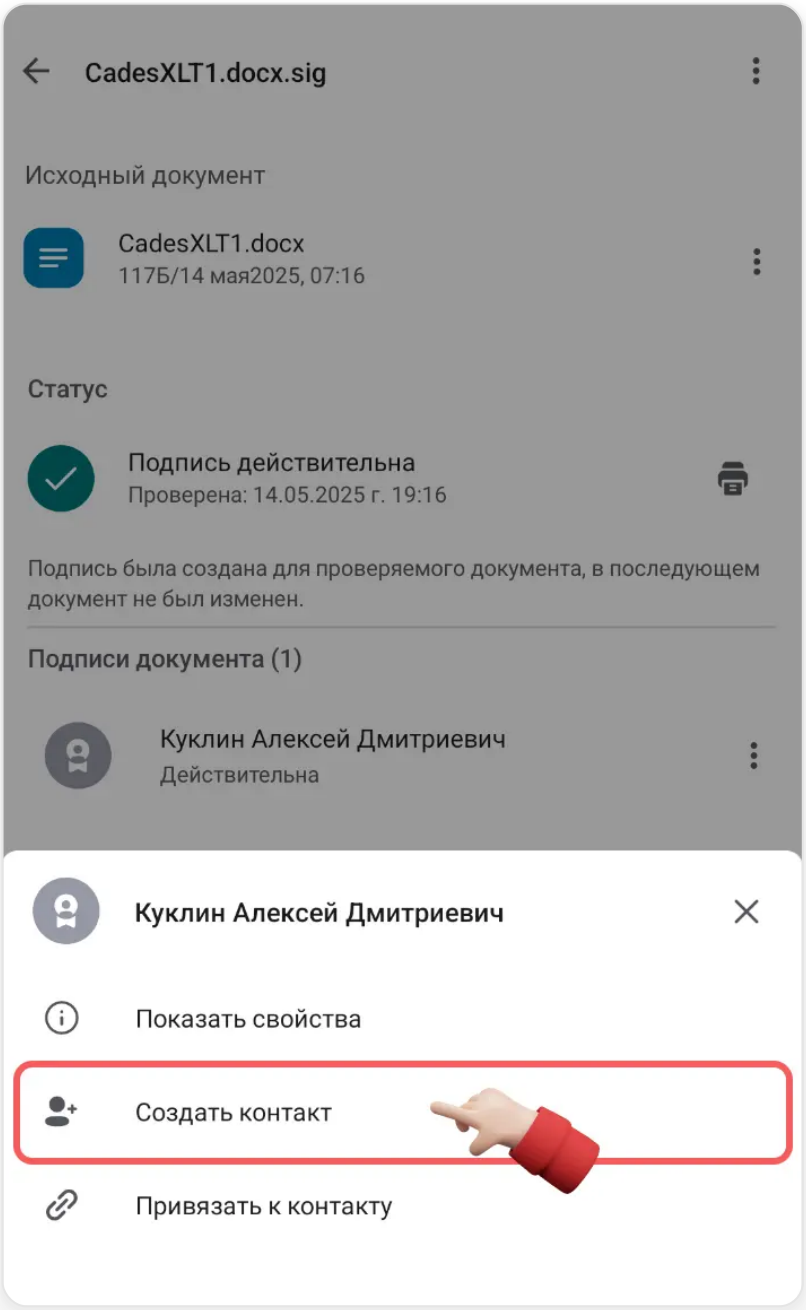
При успешном создании будет отображено уведомление о количестве созданных контактов.

Контакты будут сохранены в указанную группу.

3. Создание при проверке подписи документа

При проверке подписи документа доступно создание контакта для лица, подписавшего документ.

1. Перейдите в **Подпись и шифрование**.
2. Добавьте подписанный документ. Для этого нажмите на кнопку **Еще** в верхней части экрана и в появившемся меню действий выберите действие **Добавить документ**.
3. Нажмите на панель с документом.
4. Откроются сведения о подписи.
5. В блоке **Подписи документа** для любой из подписей вызовите меню действий по кнопке **Еще** , размещенной на панели с подписью.
6. Выберите действие **Создать контакт**.



7. Откроется форма создания контакта с данными, заполненными на основании сертификата подписи.

8. При необходимости внесите изменения в данные.
9. Выберите группу для создания контакта. По умолчанию контакт будет добавлен в активную группу. Чтобы изменить группу, нажмите на её название в разделе **Расположение** и выберите нужную группу.
10. Нажмите **Сохранить**.

При успешном создании контакт будет сохранен в указанную группу.

Описание полей контакта

Раздел	Поле	Обязательное	Описание
Имя и фото	Фото	Нет	Аватар контакта (макс. 2MB). Рекомендуемый размер: 200x200 px
	Фамилия	Нет	-
	Имя	Да	-
	Отчество	Нет	-
Контактные данные	Номер телефона	Нет	Формат: +7 (XXX) XXX-XX-XX. Поддержка международных номеров
	Адрес электронной почты	Нет	Проверка на корректность формата (user@domain.com)
Дополнительно	Дата рождения	Нет	Формат: ДД.ММ.ГГГГ. Возможность выбора из календаря
	Адрес	Нет	Многострочное поле: страна, город, улица, дом, индекс
	Организация	Нет	Полное или краткое наименование
	Должность	Нет	-
	Профессия	Нет	-
	Преффикс	Нет	Например: "Д-р", "Проф."
	Суффикс	Нет	Например: "Jr", "PhD"
	Обращение	Нет	Произвольная форма обращения ("Уважаемый Алексей Петрович")
	Пол	Нет	Варианты: • Не указано • Мужской • Женский
	Язык	Нет	В формате ISO 639-1 (ru, en, de)

Раздел	Поле	Обязательное	Описание
	Часовой пояс	Нет	Формат: UTC±XX:XX (например, UTC+03:00)
	Веб-сайт	Нет	Автоматическая проверка формата (https://example.com)
	Широта	Нет	Формат: от -90.000000 до +90.000000
	Долгота	Нет	Формат: от -180.000000 до +180.000000
	Примечание	Нет	Многострочное поле для дополнительной информации
Сертификат	Привязанные сертификаты	Нет	Сертификат из файла `.cer/.crt` или из раздела **Сертификаты**

Инструкции по теме

- Действия с контактами
- Управление сертификатами контакта
- Как поделиться контактом
- Группы контактов

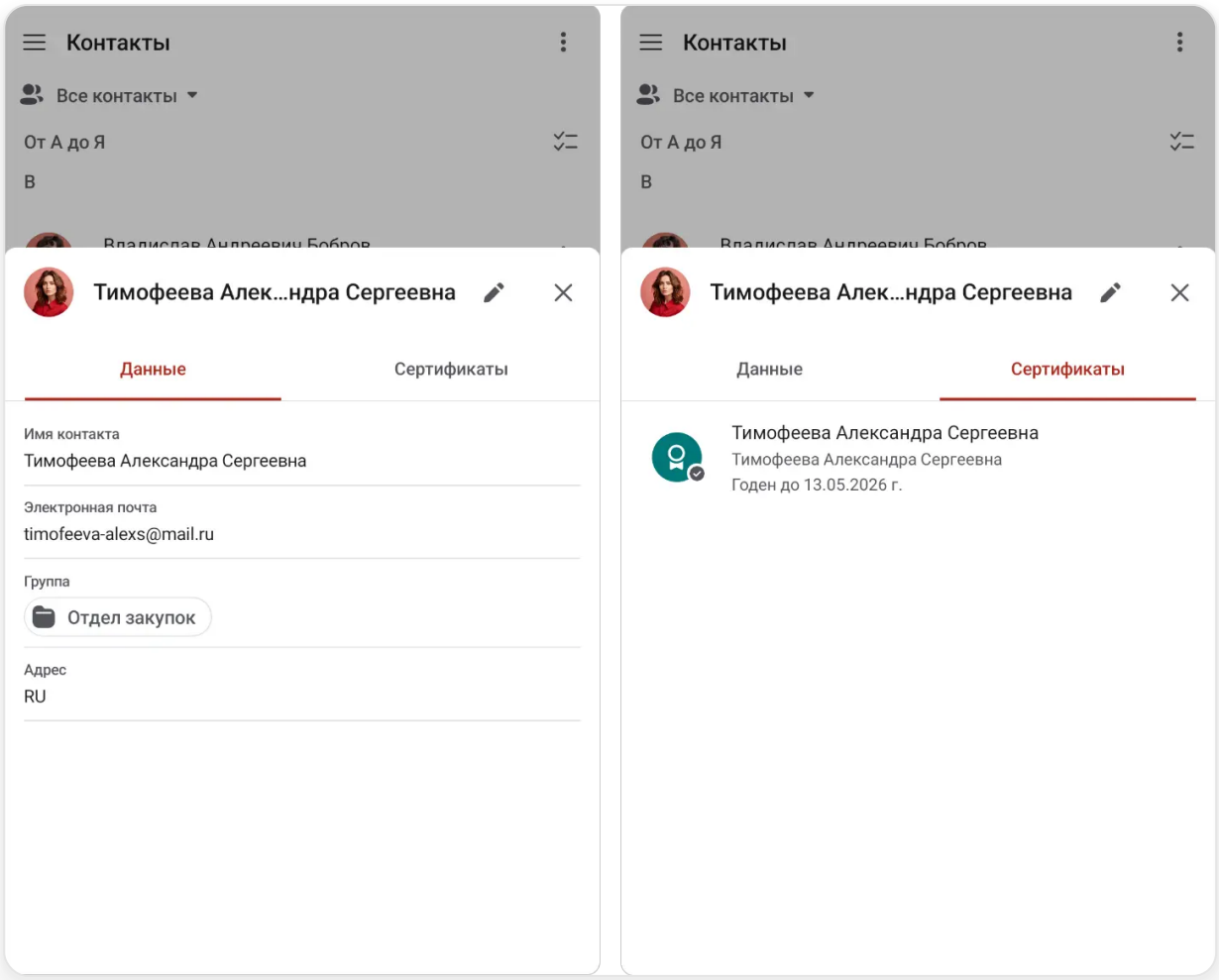
Открыть статью на сайте

Управление контактами в КриптоАРМ Подпись и шифрование

- 1. Просмотр сведений о контакте
- 2. Редактирование контакта
- 3. Работа с «Избранными»
- 4. Перемещение контакта
- 5. Сортировка и настройка отображения
- 6. Удаление контакта
- Инструкции по теме

1. Просмотр сведений о контакте

1. Перейдите в раздел **Контакты**.
2. Нажмите на панель с контактом, сведения о котором необходимо просмотреть.
3. Откроется окно со сведениями о контакте.
    - На вкладке **Данные** отображаются все сведения о контакте, указанные при его создании.
    - На вкладке **Сертификаты** отображается список сертификатов, привязанных к контакту.



2. Редактирование контакта

> 💡 **Совет**: Чтобы совершить действие сразу с несколькими контактами, нажмите **Выбрать все** в меню по кнопке **Еще** ⋮, отметьте нужные контакты и выберите необходимое действие.

Редактирование данных контакта

1. Откройте форму редактирования контакта одним из способов:
   - Нажмите на кнопку **Изменить контакт** ✎ в форме просмотра контакта,
   - Выберите действие **Изменить контакт** в меню **Действия**, которое вызывается по кнопке **Еще** ⋮, размещенной на панели с контактом в списке.
2. Внесите изменения в данные контакта.

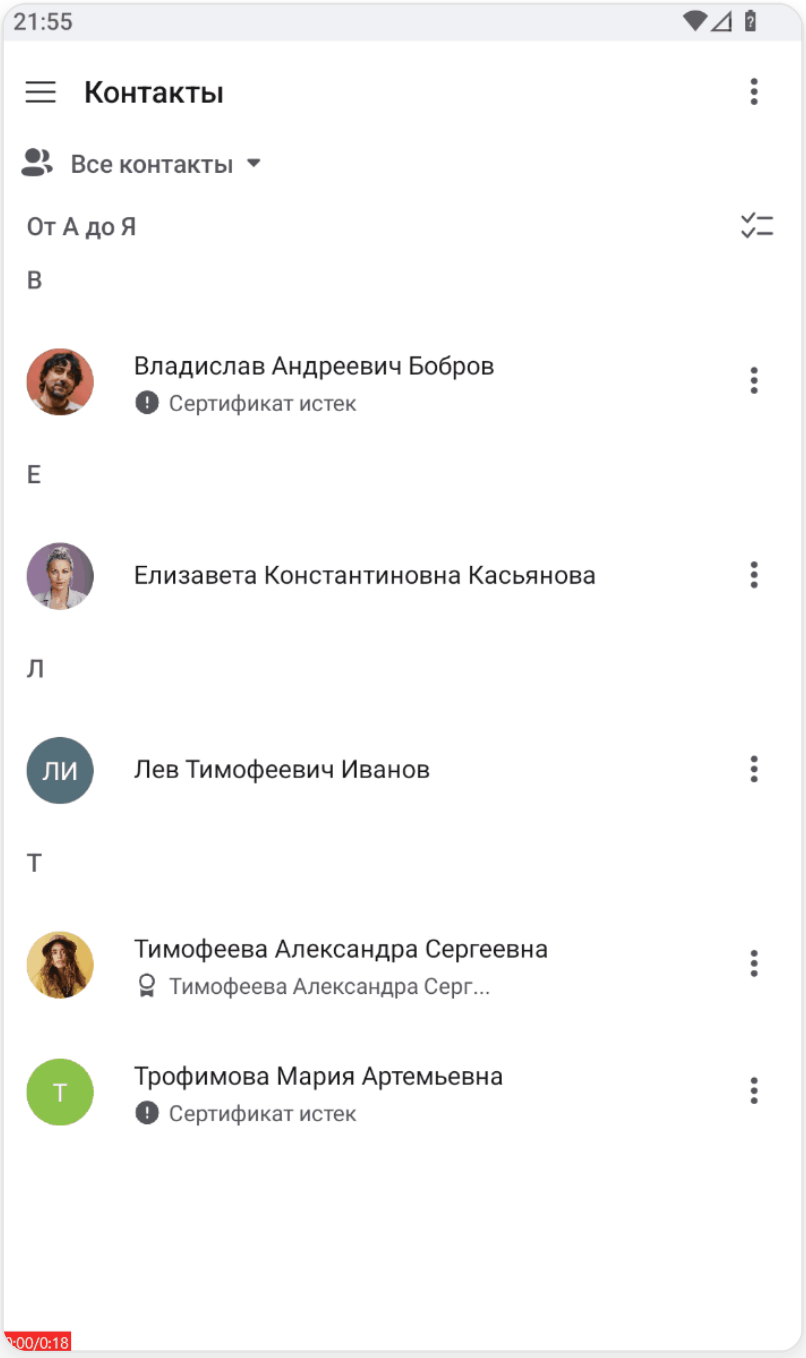
3. Внесите изменения в сертификаты. Подробнее читайте в инструкции Управление сертификатами контакта.
4. Нажмите **Сохранить**.

Редактирование фото

Если у контакта нет фотографии, можно добавить новую, либо заменить уже существующую. Доступна загрузка фото из файла. Загруженное фото контакта можно удалить.

Загрузка фото

1. Откройте форму редактирования контакта одним из способов:
   - Нажмите на кнопку **Изменить контакт**  в форме просмотра контакта,
   - Выберите действие **Изменить контакт** в меню **Действия**, которое вызывается по кнопке **Еще** , размещенной на панели с контактом в списке.
2. Нажмите на круг с фотографией.
3. В появившемся меню выберите действие **Загрузить фото**.
4. Откроется окно файлового менеджера.
5. Выберите новую фотографию.
6. Откроется редактор фото. Для выбранной фотографии можно настроить область, которая будет отображаться в качестве изображения контакта. Чтобы настроить её размер, потяните за уголок рамки. Рамку можно переместить, чтобы выбрать другую область. Удерживайте нажатие внутри рамки и перемещайте её. Нажмите **Готово** после того, как настроите фото.
7. Нажмите **Сохранить** в форме редактирования контакта.



Удаление фото контакта

1. Откройте форму редактирования контакта одним из способов:
   - Нажмите на кнопку **Изменить контакт** в форме просмотра контакта,
   - Выберите действие **Изменить контакт** в меню **Действия**, которое вызывается по кнопке **Еще** , размещенной на панели с контактом в списке.
2. Нажмите на круг с фотографией.
3. В появившемся меню выберите действие **Удалить фото**.
4. Фотография контакта будет заменена на монограмму из букв.

5. Нажмите **Сохранить** в форме редактирования контакта.

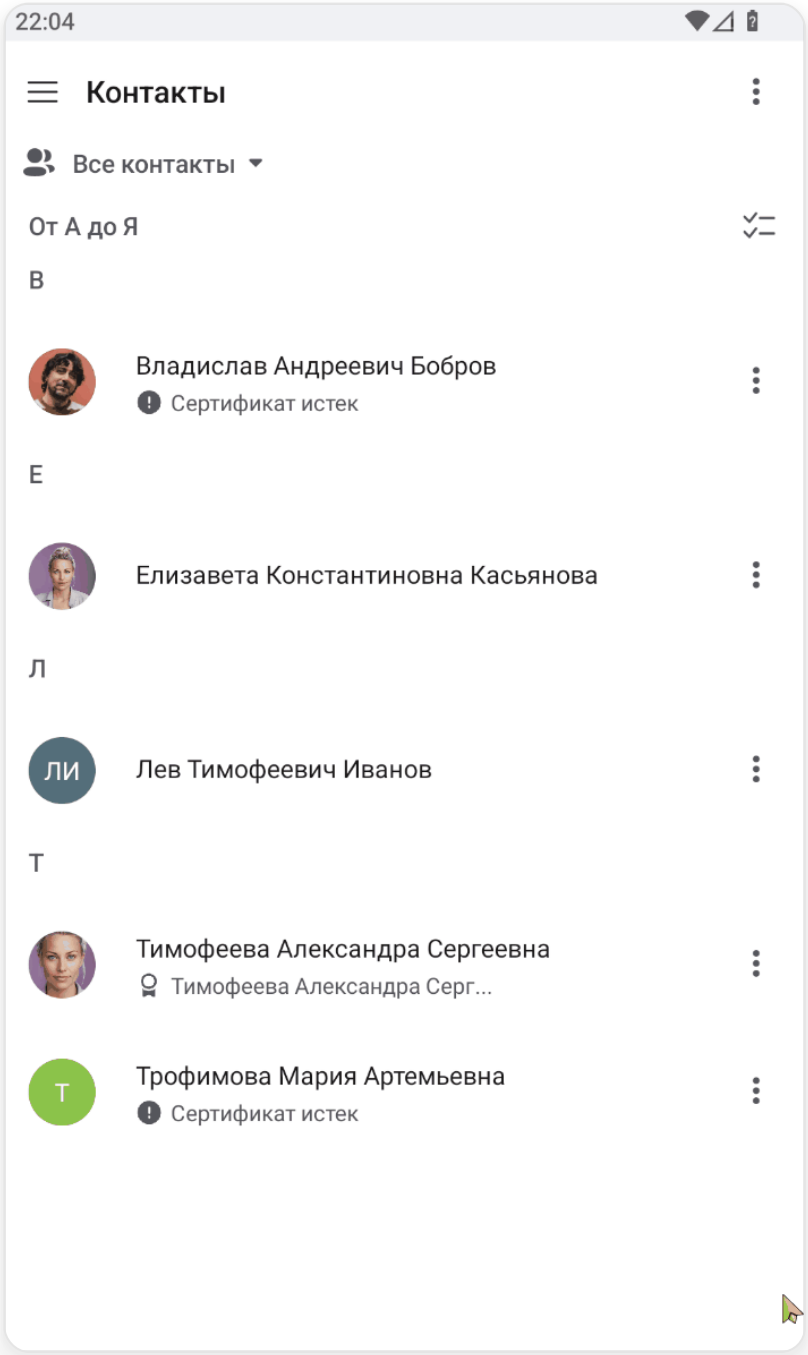
---

3. Работа с «Избранными»

Избранные контакты — это те контакты, которые вы считаете важными или часто используете и хотите иметь быстрый доступ к ним.

Добавление в «Избранные»

1. Откройте раздел **Контакты**.
2. Вызовите меню **Действия**, которое доступно по кнопке **Еще** , размещенной на панели с контактом в списке.
3. В появившемся меню выберите действие **Сделать избранным**.



Контакт будет помечен как «Избранный». На фотографии контакта появится иконка — звёздочка ✪. Контакт станет доступен в специальной группе **Избранные**.

> 🔍 Подробнее про группы читайте в инструкции Группировка пользователей.

Групповое добавление

1. Откройте раздел **Контакты**.

2. Отметьте флажками контакты одним из способов:
   - Выберите **Выбрать все** в меню **Действия**, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**. В списке контактов отобразятся флажки. Установите флажки напротив тех контактов, которые необходимо добавить в «Избранные».
   - Нажмите на панель с контактом и удерживайте ее. Выберите другие контакты.
3. Выберите **Сделать избранным** в меню действий, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**.

Контакты будет помечены как «Избранные» и станут доступны в специальной группе «Избранные». На фотографии контактов появится иконка — звёздочка .

Удаление из «Избранных»

Если вы больше не используете контакт и хотите освободить место в списке избранных контактов, вы можете удалить контакт из избранного.

1. Откройте раздел **Контакты**.
2. Вызовите меню **Действия**, которое доступно по кнопке **Еще** , размещенной на панели с контактом в списке.
3. В появившемся меню выберите действие **Удалить из избранных**.

Контакт будет удален из «Избранных».

Групповое удаление из «Избранных»

1. Откройте раздел **Контакты**.
2. Отметьте флажками контакты одним из способов:
   - Выберите **Выбрать все** в меню **Действия**, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**. В списке контактов отобразятся флажки. Установите флажки напротив тех контактов, которые необходимо удалить из «Избранных».
   - Нажмите на панель с контактом и удерживайте ее. Выберите другие контакты.
3. Выберите **Удалить из избранных** в меню действий, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**.

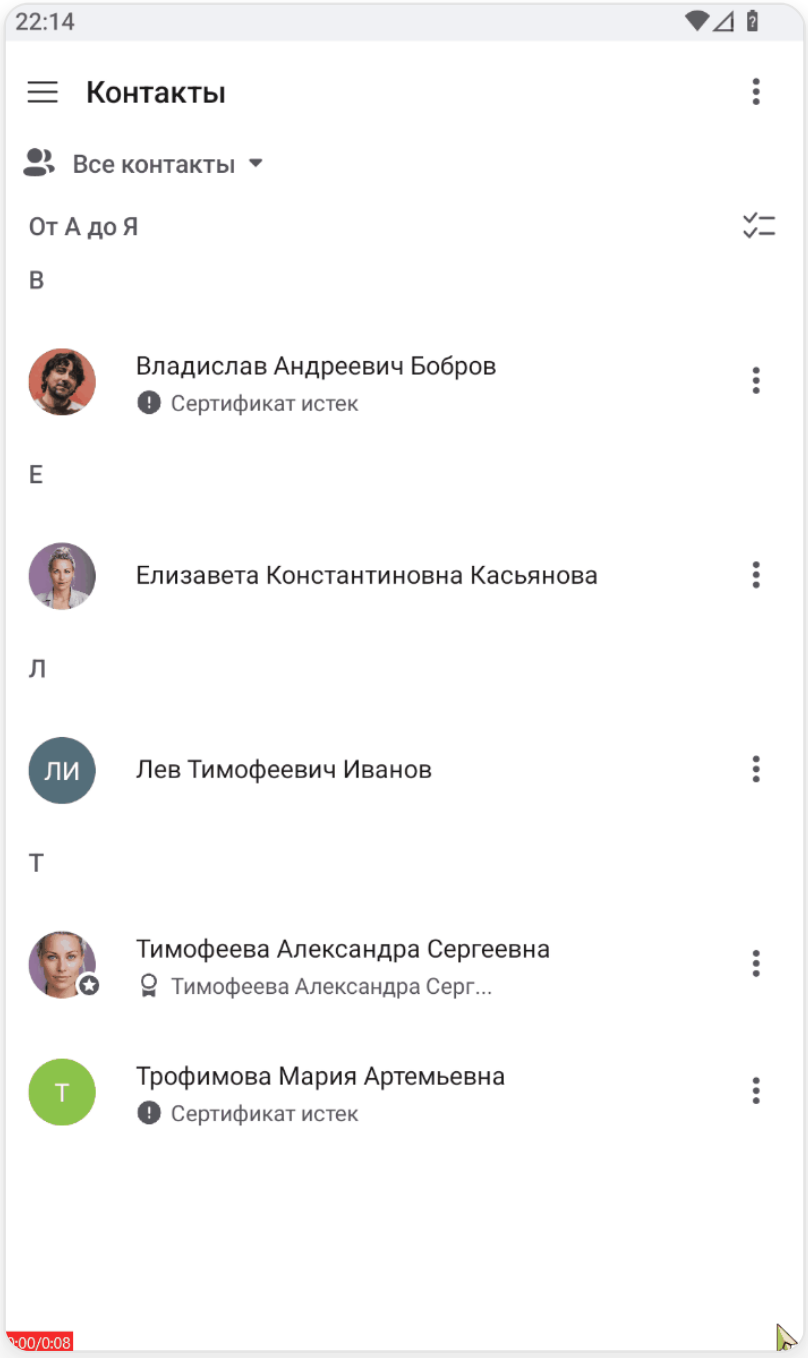
Контакты будут удалены из «Избранных».

4. Перемещение контакта

Перемещение контактов между группами позволяет упорядочить контакты по разным категориям.

Перемещение контакта

1. Перейдите в раздел **Контакты**.
2. Вызовите меню действий, которое доступно по кнопке **Еще** , размещенной на панели с контактом в списке.
3. В появившемся меню выберите действие **Переместить**.
4. В открывшемся окне **Группы** выберите группу, в которую хотите переместить контакт.



После завершения перемещения контакта будет отображено уведомление об успешном выполнении операции.

Групповое перемещение

1. Перейдите в раздел **Контакты**.

2. Отметьте флажками контакты одним из способов:
   - Выберите **Выбрать все** в меню **Действия**, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**. В списке контактов отобразятся флажки. Установите флажки напротив тех контактов, которые необходимо переместить.
   - Нажмите на панель с контактом и удерживайте ее. Выберите другие контакты.
3. Выберите **Переместить** в меню действий, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**.
4. В открывшемся окне **Группы** выберите группу, в которую хотите переместить контакты.

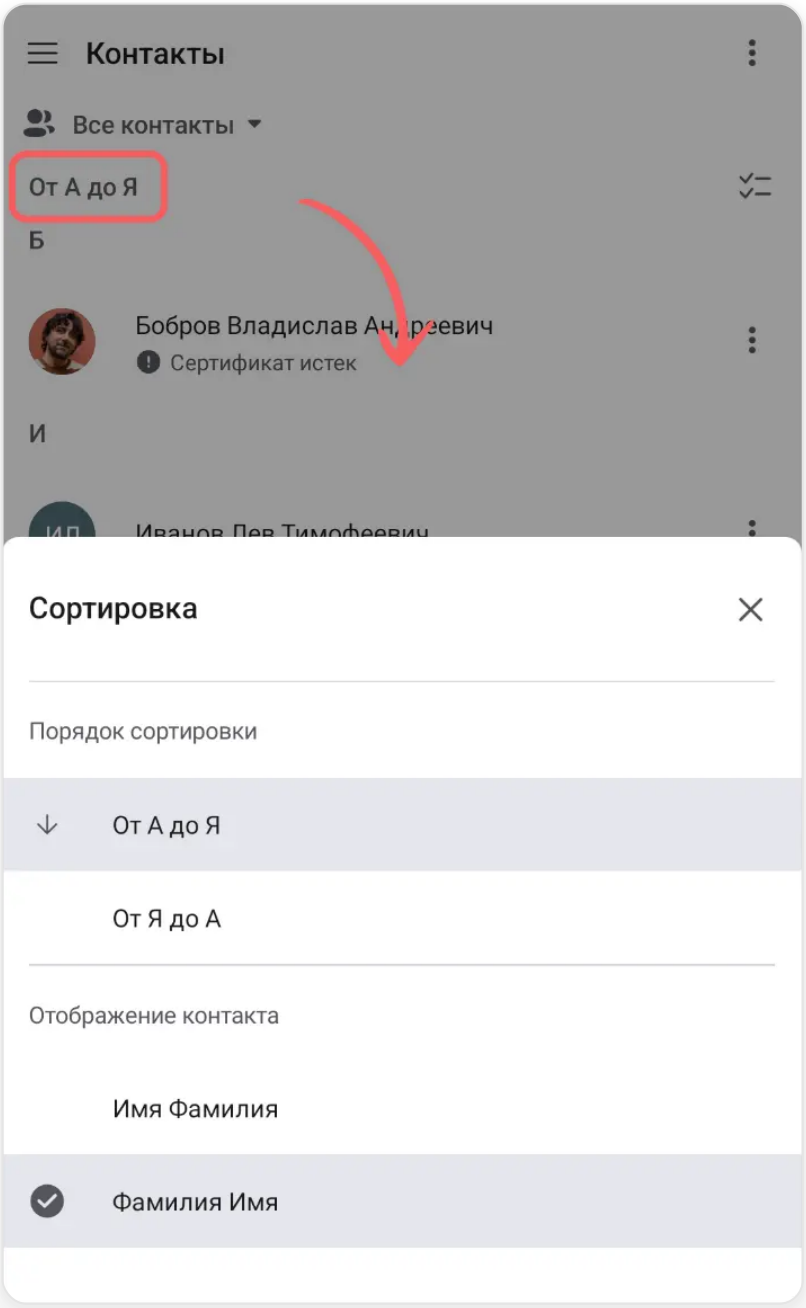
После завершения перемещения контактов будет отображено уведомление об успешном выполнении операции.

---

5. Сортировка и настройка отображения

Чтобы настроить сортировку и отображение контактов в списке:

1. Перейдите в раздел **Контакты**.
2. Вызовите меню действий **Сортировка**.



3. Настройте порядок сортировки:
    - От А до Я
    - От Я до А
4. Настройте отображение контактов:
    - Имя+Фамилия
    - Фамилия+Имя

Изменения применяются автоматически и не требуют дополнительного сохранения.

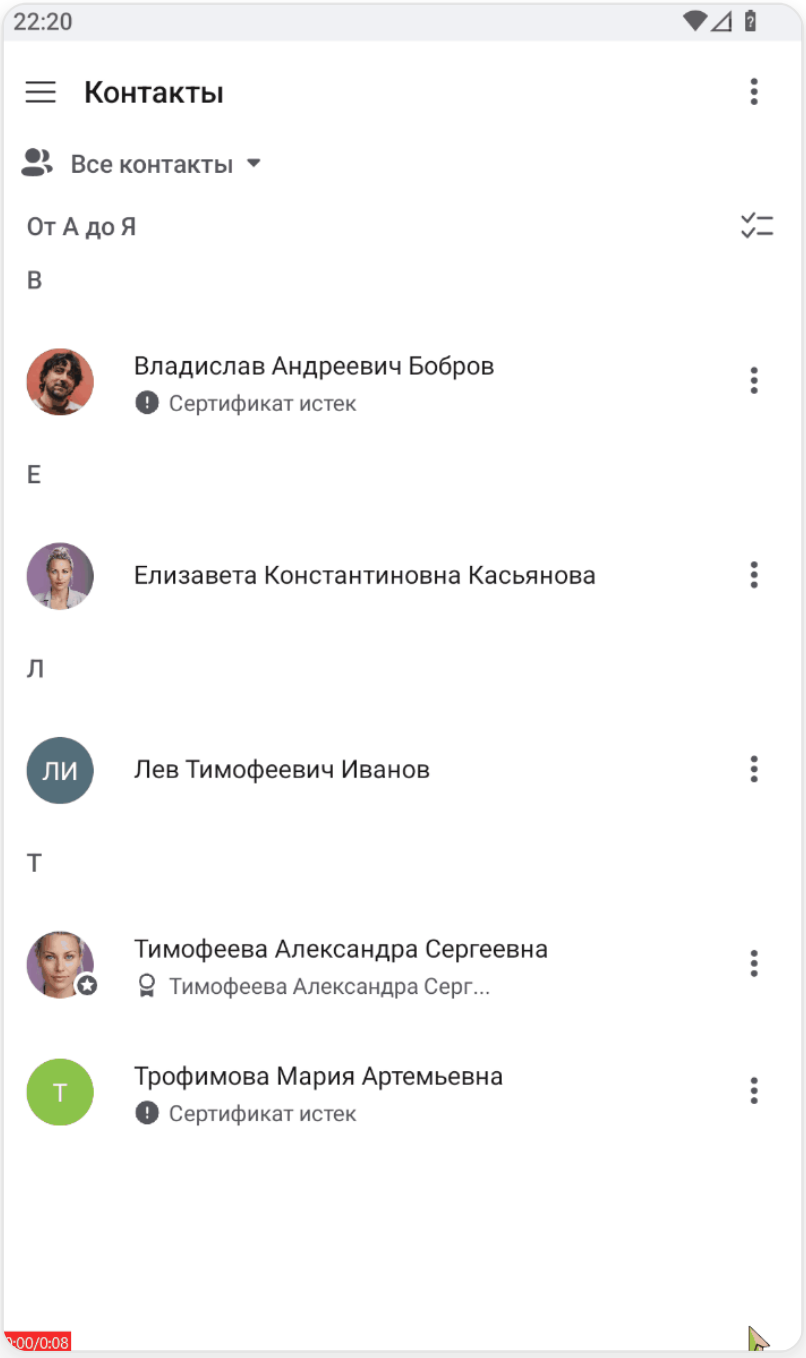
6. Удаление контакта

> ⚠️ **Примечание**: Сертификаты, привязанные к контакту из файла, не сохраняются в разделе «Настройки» → «Сертификаты других пользователей» и при удалении контакта будут удалены вместе с ним.

Удаление контакта

> 🚨 Контакты удаляются без возможности восстановления.

1. Перейдите в раздел **Контакты**.
2. Вызовите меню действий, которое доступно по кнопке **Еще** , размещенной на панели с контактом в списке контактов.
3. В появившемся меню выберите действие **Удалить**.
4. Подтвердите действие в модальном окне.



После удаления контакта будет отображено уведомление об успешном выполнении операции. Контакт пропадет из списка.

Групповое удаление

1. Перейдите в раздел **Контакты**.

2. Отметьте флажками контакты одним из способов:
   - Выберите **Выбрать все** в меню **Действия**, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**. В списке контактов отобразятся флажки. Установите флажки напротив тех контактов, которые необходимо переместить.
   - Нажмите на панель с контактом и удерживайте ее. Выберите другие контакты.
3. Выберите **Удалить** в меню действий, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**.
4. Подтвердите действие в модальном окне.

После удаления контактов будет отображено уведомление об успешном выполнении операции. Контакты пропадут из списка.

Инструкции по теме

- Как создать контакт
- Управление сертификатами контакта
- Как поделиться контактом
- Группы контактов

Открыть статью на сайте

Управление сертификатами контакта в КриптоАРМ Подпись и шифрование

- Добавление сертификата
- Просмотр сведений о сертификате контакта
- Установка сертификата по умолчанию
- Экспорт сертификата контакта
- Удаление сертификата контакта
- Инструкции по теме

Добавление сертификата

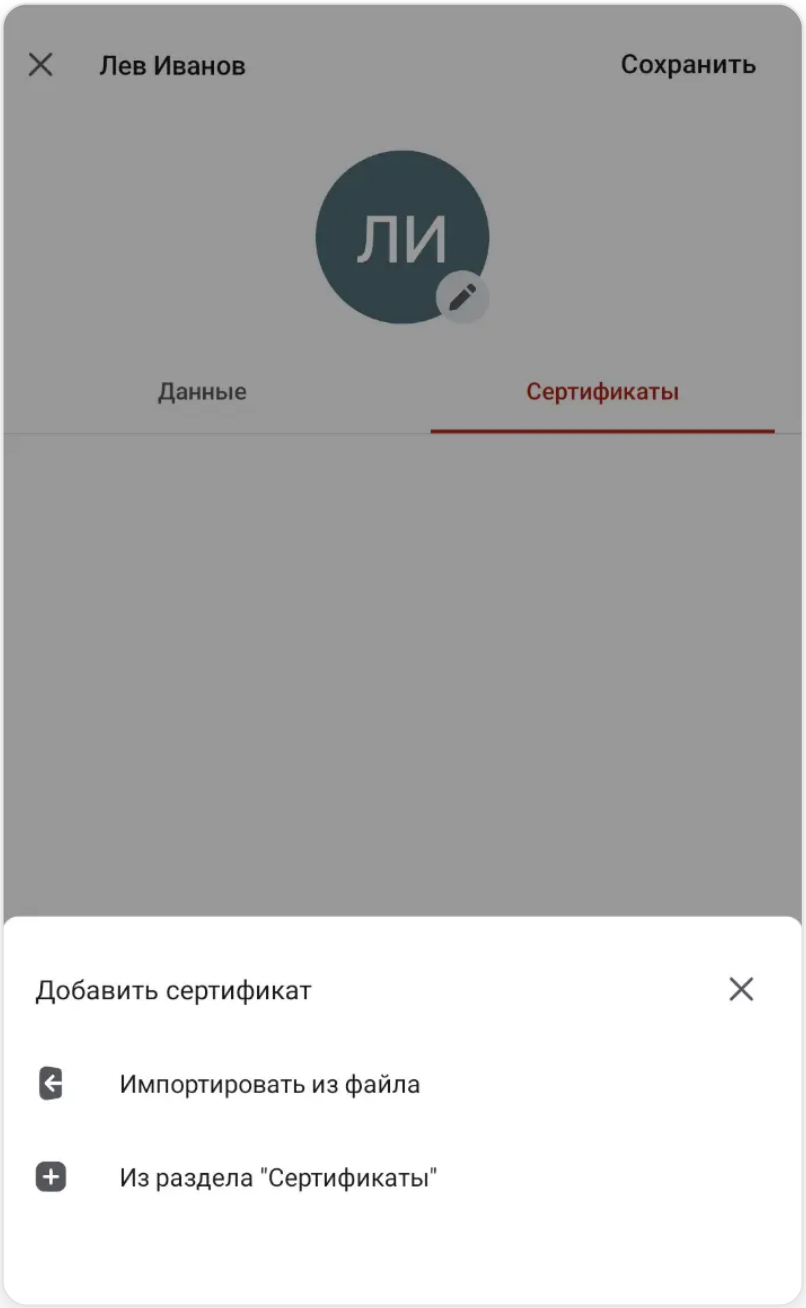
Для организации зашифрованного обмена документами с контактом необходимо привязать его сертификат.

> 💡 **Совет**: Регулярно обновляйте сертификаты при их перевыпуске. Для массовой привязки используйте функцию импорта контактов.

Способы привязки сертификата

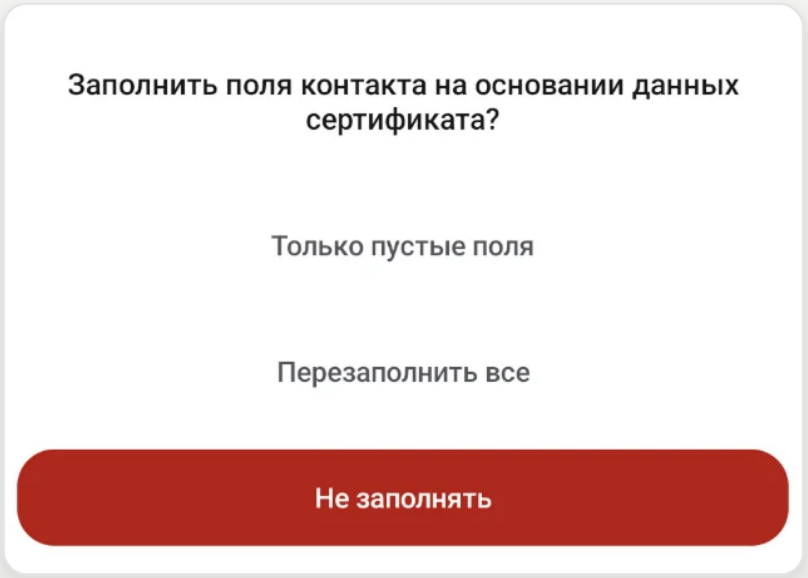
1. Стандартный способ

1. Откройте форму редактирования контакта одним из способов:
    - Нажмите на кнопку **Изменить контакт** в форме просмотра контакта,
    - Выберите действие **Изменить контакт** в меню **Действия**, которое вызывается по кнопке **Еще** , размещенной на панели с контактом в списке.
2. Перейдите на вкладку **Сертификаты**.
3. Вызовите меню по кнопке **Добавить сертификат**.



4. Выберите один из способов добавления сертификата:
    - Импортировать из файла,
    - Из **Сертификаты других пользователей** раздела **Настройки**.

> 💡 **Совет**: При выборе сертификата, доступно заполнение полей контакта на основании данных сертификата.



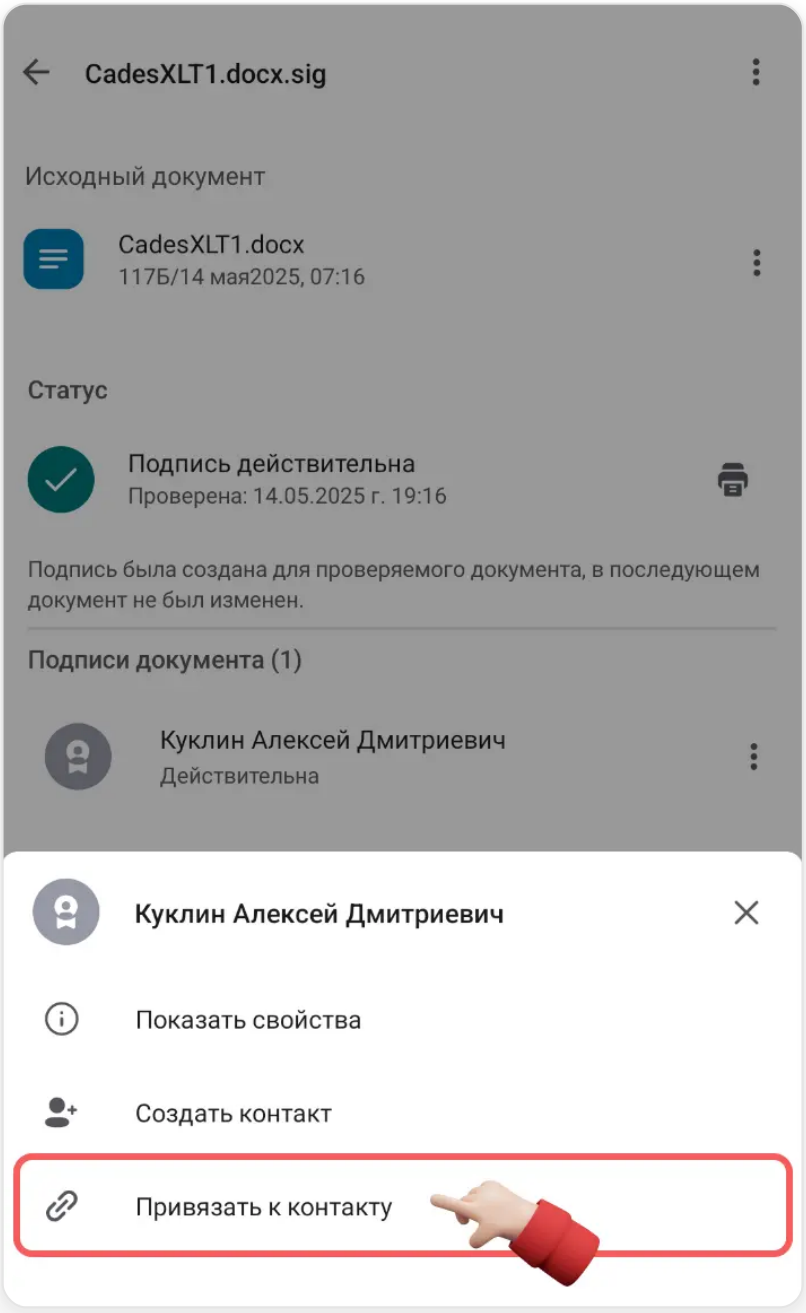
5. После выбора сертификата нажмите **Сохранить** в форме редактирования контакта.

> ⚠️ **Примечание**: Сертификаты, привязанные к контакту из файла, **не сохраняются** в разделе «Настройки» → «Сертификаты других пользователей» и при удалении контакта будут удалены вместе с ним.

2. Добавление при проверке подписи документа

Сертификат подписи, который использовался для подписания документа, можно привязать к уже существующему контакту.

1. Перейдите в раздел **Документы**.
2. Откройте сведения о подписи для любого подписанного документа.
3. В блоке **Подписи документа** для любой из подписей вызовите меню с действиями по кнопке **Еще**.
4. Выберите действие **Привязать к контакту**.



5. В открывшемся окне укажите контакт, к которому необходимо привязать сертификат. Для выбора доступен один или несколько контактов или групп.
6. Нажмите **Выбрать**.

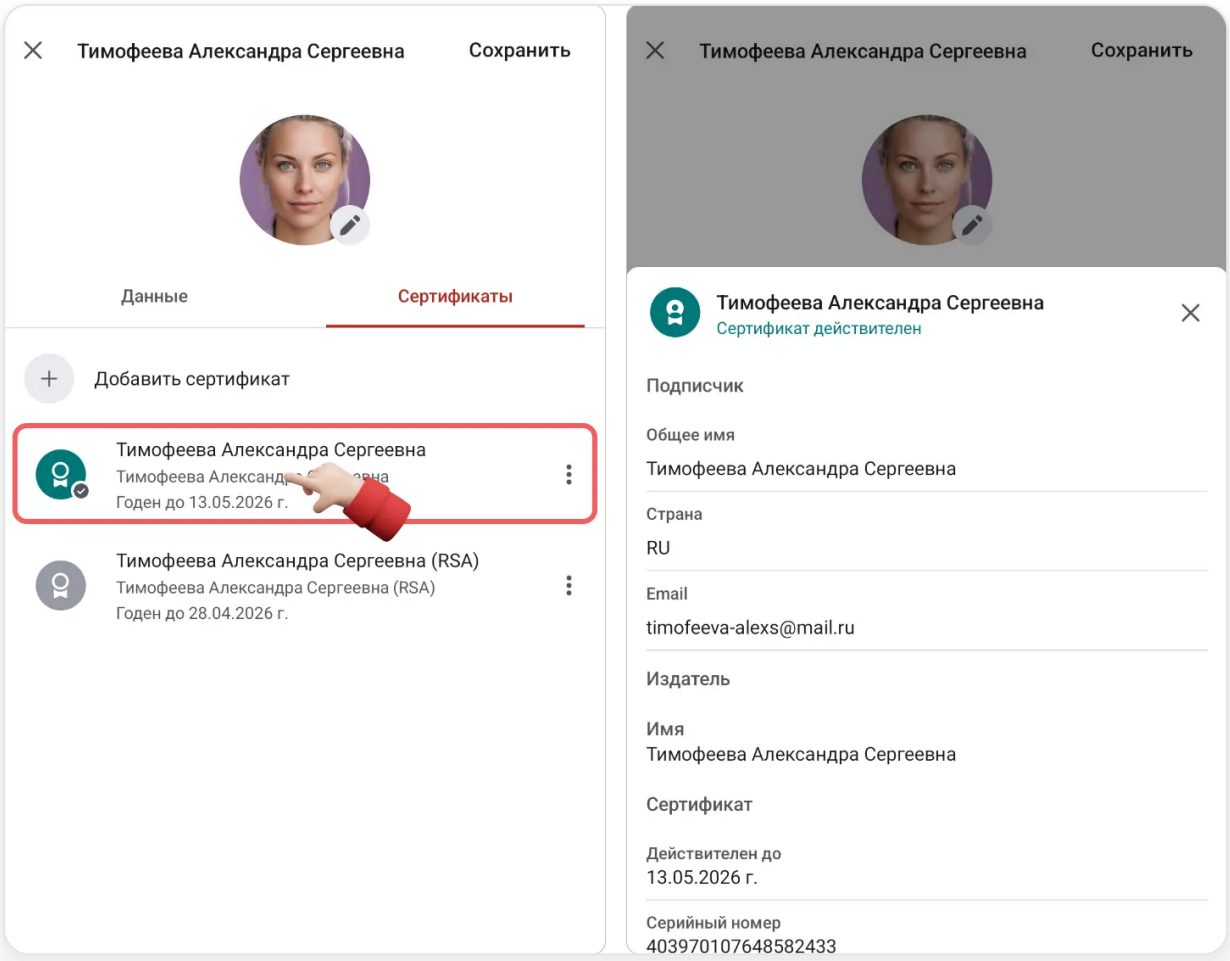
Просмотр сведений о сертификате контакта

При просмотре или редактировании контакта можно просмотреть сведения о сертификате, который к нему привязан.

1. Перейдите на вкладку **Сертификаты** в форме просмотра или редактирования контакта.

2. Нажмите на панель с сертификатом, сведения о котором необходимо просмотреть. Либо вызовите меню с действиями по кнопке **Еще** , размещенной на панели с сертификатом, и выберите **Свойства сертификата**.

3. Откроется окно со сведениями о сертификате.



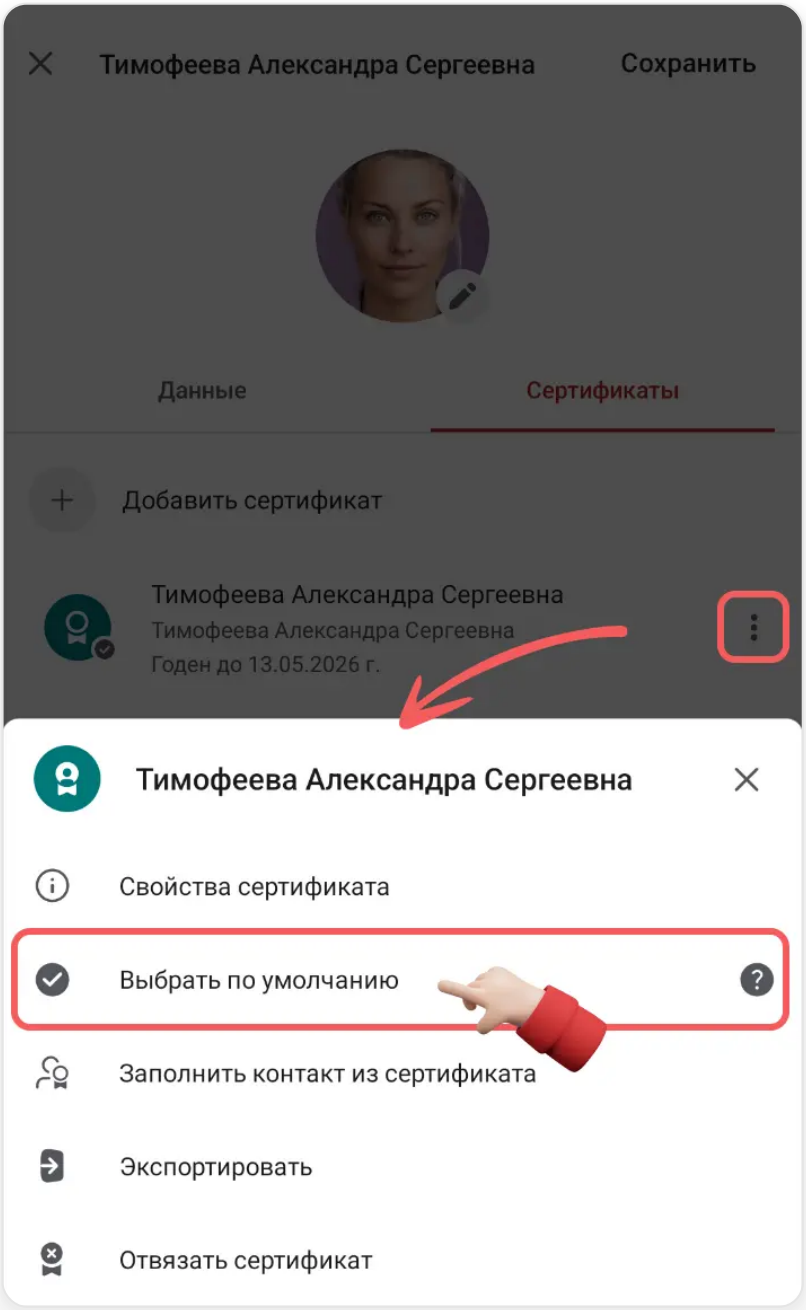
Установка сертификата по умолчанию

Если к контакту привязано несколько сертификатов, один из них можно выбрать в качестве основного (по умолчанию). При шифровании этот сертификат будет автоматически использоваться в качестве сертификата шифрования контакта.

> 💡 **Совет**: Сертификатом по умолчанию устанавливается первый сертификат, привязанный к контакту. Если вы добавляете несколько сертификатов с разными статусами, то по умолчанию устанавливается первый действительный сертификат.

Чтобы установить сертификат по умолчанию:

1. Откройте форму редактирования контакта одним из способов:
   - Нажмите на кнопку **Изменить контакт** в форме просмотра контакта,
   - Выберите действие **Изменить контакт** в меню **Действия**, которое вызывается по кнопке **Еще** , размещенной на панели с контактом в списке.
2. Перейдите на вкладку **Сертификаты**.
3. Вызовите меню по кнопке **Еще** , размещенной на панели с сертификатом, который необходимо установить по умолчанию.
4. В появившемся меню выберите действие **Задать по умолчанию**.
5. На панели с сертификатом появится дополнительная иконка в виде галки .
6. Нажмите **Сохранить** в форме редактирования контакта.



Экспорт сертификата контакта

> 💡 **Совет**: Если необходимо сохранить сертификат контакта или поделиться им с кем-то еще, можно воспользоваться функцией экспорта сертификата.

1. Откройте форму редактирования контакта одним из способов:
    - Нажмите на кнопку **Изменить контакт** в форме просмотра контакта,

- Выберите действие **Изменить контакт** в меню **Действия**, которое вызывается по кнопке **Еще** , размещенной на панели с контактом в списке.

2. Перейдите на вкладку **Сертификаты**.
3. Вызовите меню по кнопке **Еще** , размещенной на панели с сертификатом, который необходимо экспортировать.
4. В появившемся меню выберите действие **Экспортировать**.
5. Укажите место сохранения или приложение для отправки файла с сертификатом.

Удаление сертификата контакта

1. Откройте форму редактирования контакта одним из способов:
   - Нажмите на кнопку **Изменить контакт**  в форме просмотра контакта,
   - Выберите действие **Изменить контакт** в меню **Действия**, которое вызывается по кнопке **Еще** , размещенной на панели с контактом в списке.
2. Перейдите на вкладку **Сертификаты**.
3. Вызовите меню по кнопке **Еще** , размещенной на панели с сертификатом, который необходимо удалить.
4. В появившемся меню выберите действие **Удалить**.
5. Сертификат пропадет из списка сертификатов контакта.
6. Нажмите **Сохранить** в форме редактирования контакта.

Инструкции по теме

- Как создать контакт
- Действия с контактом
- Как поделиться контактом
- Группы контактов

Открыть статью на сайте

Управление группами контактов в КриптоАРМ Подпись и шифрование

- Общая информация
- Создание группы контактов
- Действия с группами
- Инструкции по теме

Общая информация

Группы предназначены для упрощения работы с контактами. Они позволяют объединять несколько контактов в один список на основе общих характеристик. Это удобно для быстрого поиска нужных контактов, а также для шифрования документов, адресованных конкретной группе.

После установки в приложении доступны следующие группы:

- **Все контакты** — специальная группа, в которой отображаются контакты из всех групп.
- **Контакты** — корневая группа, в которой можно создавать собственные группы и подгруппы.
- **Избранные** — специальная группа, в которой отображаются все контакты, отмеченные как избранные.
- **Мои контакты** — группа, предназначенная для персональных контактов. Подробнее в инструкции Мои контакты

Создание группы контактов

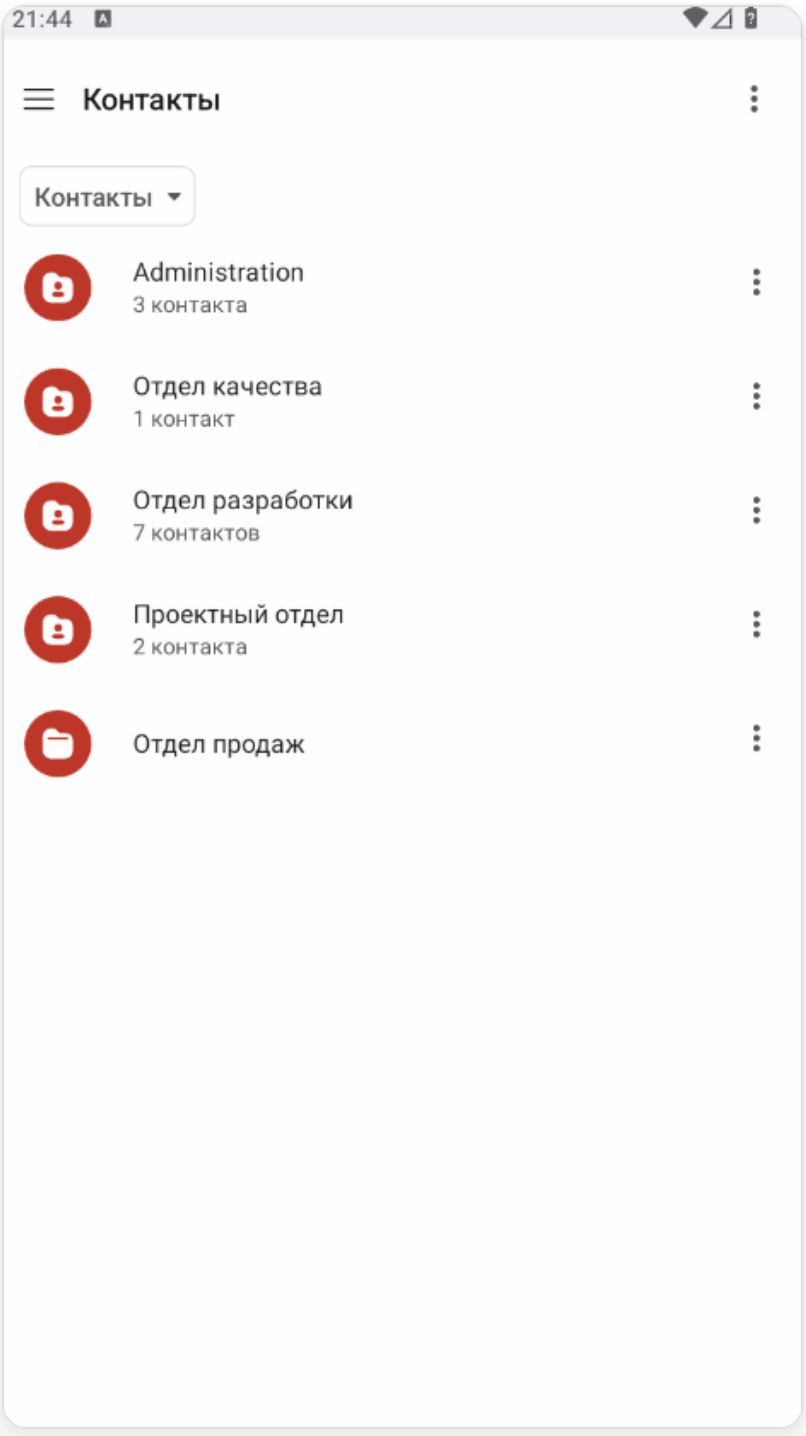
> 💡 **Совет**: В приложении можно создавать несколько уровней вложенности групп.

Чтобы создать группу:

1. Откройте раздел **Контакты**.
2. Перейдите в окно **Создать группу** одним из способов:
   - Откройте меню по кнопке **Еще** и выберите действие **Создать** → **Создать группу**,
   - Откройте окно со списком групп и нажмите на кнопку **Создать группу** .
3. Укажите название группы и ее расположение.

> 💡 **Совет**: По умолчанию группа будет создана в корневой папке «Контакты».

4. Нажмите **Сохранить**.

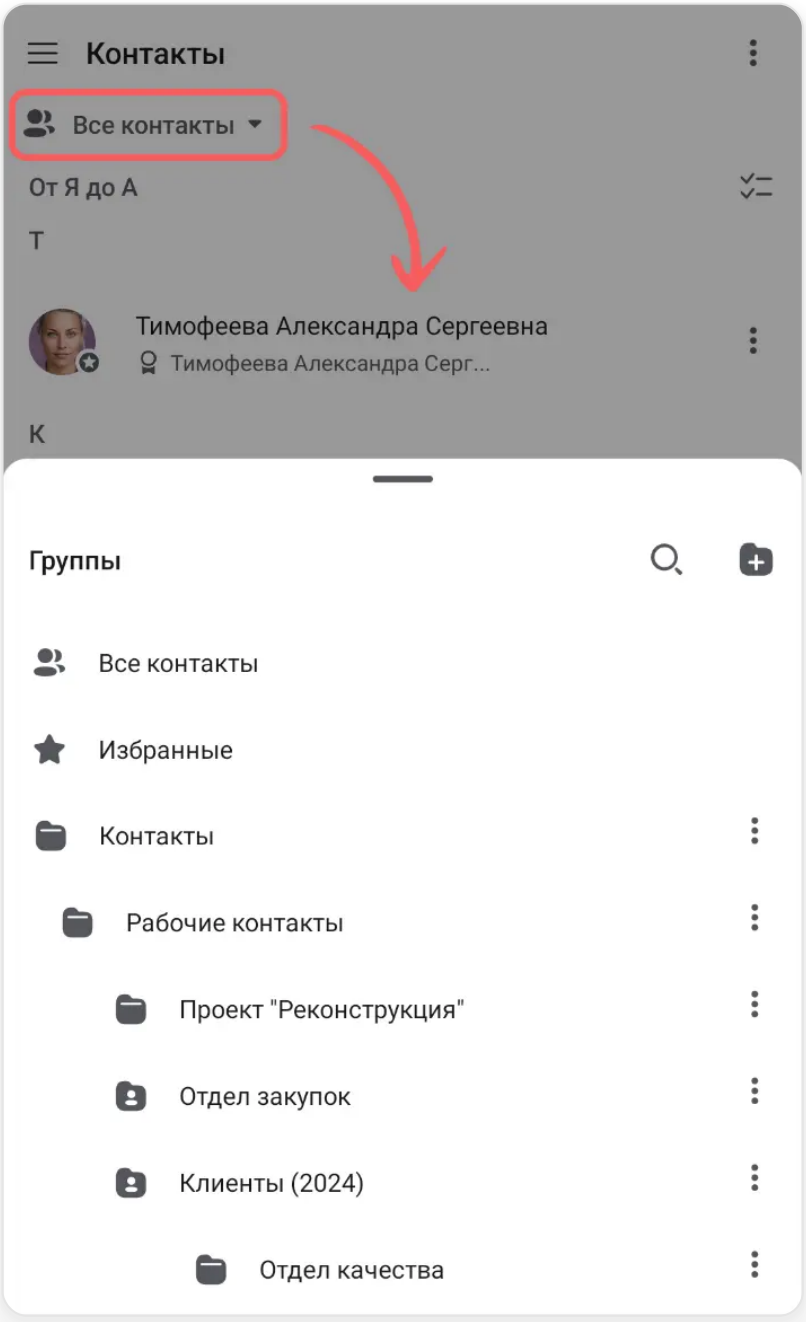


Действия с группами

> 💡 **Совет**: Чтобы совершить действие сразу с несколькими группами, нажмите **Выбрать все** в меню по кнопке **Еще** , отметьте нужные группы и выберите необходимое действие.

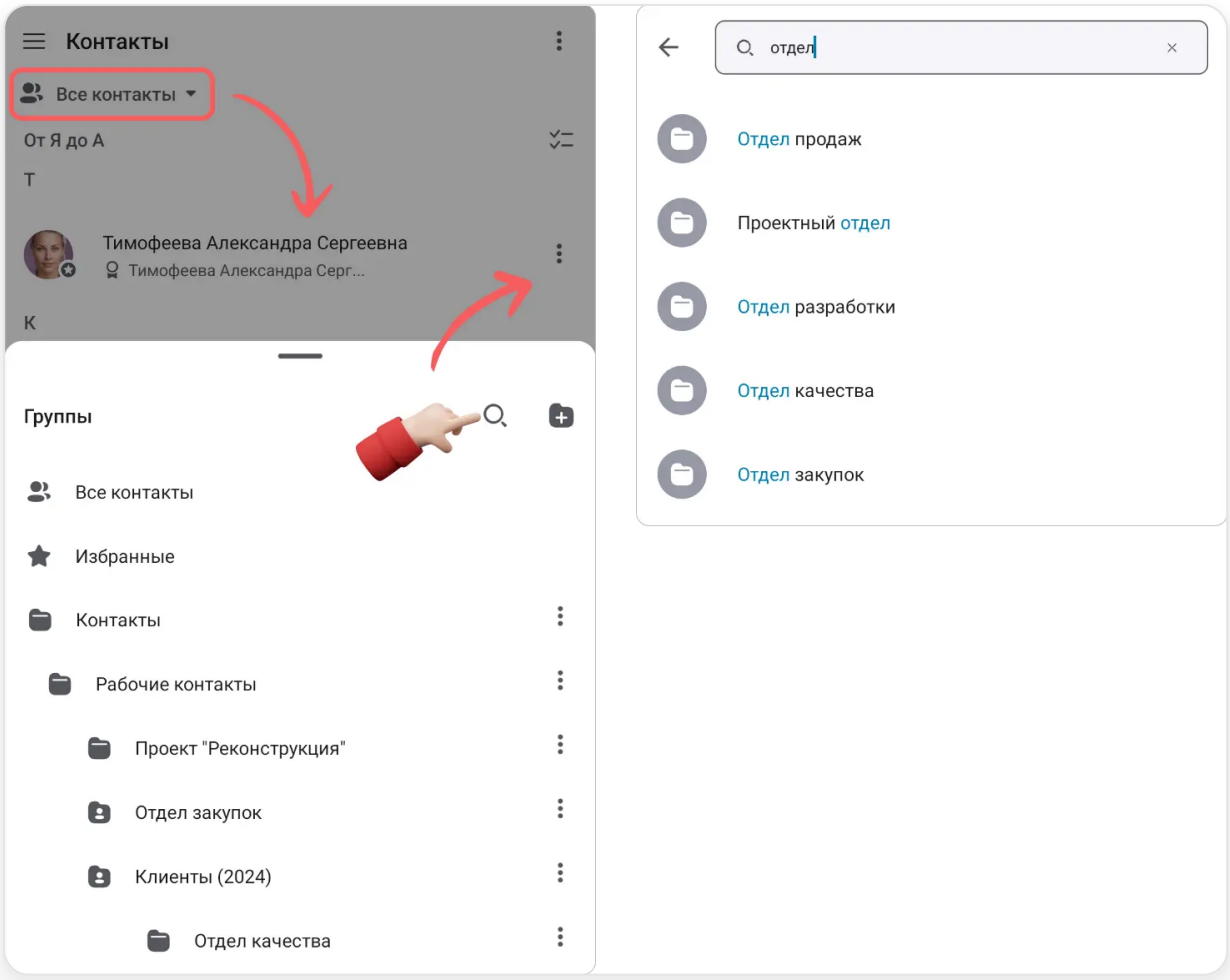
1. Открытие списка групп

1. Перейдите в раздел **Контакты**.
2. Нажмите на кнопку с названием активной группы.
3. Откроется окно со списком групп, созданных в приложении.



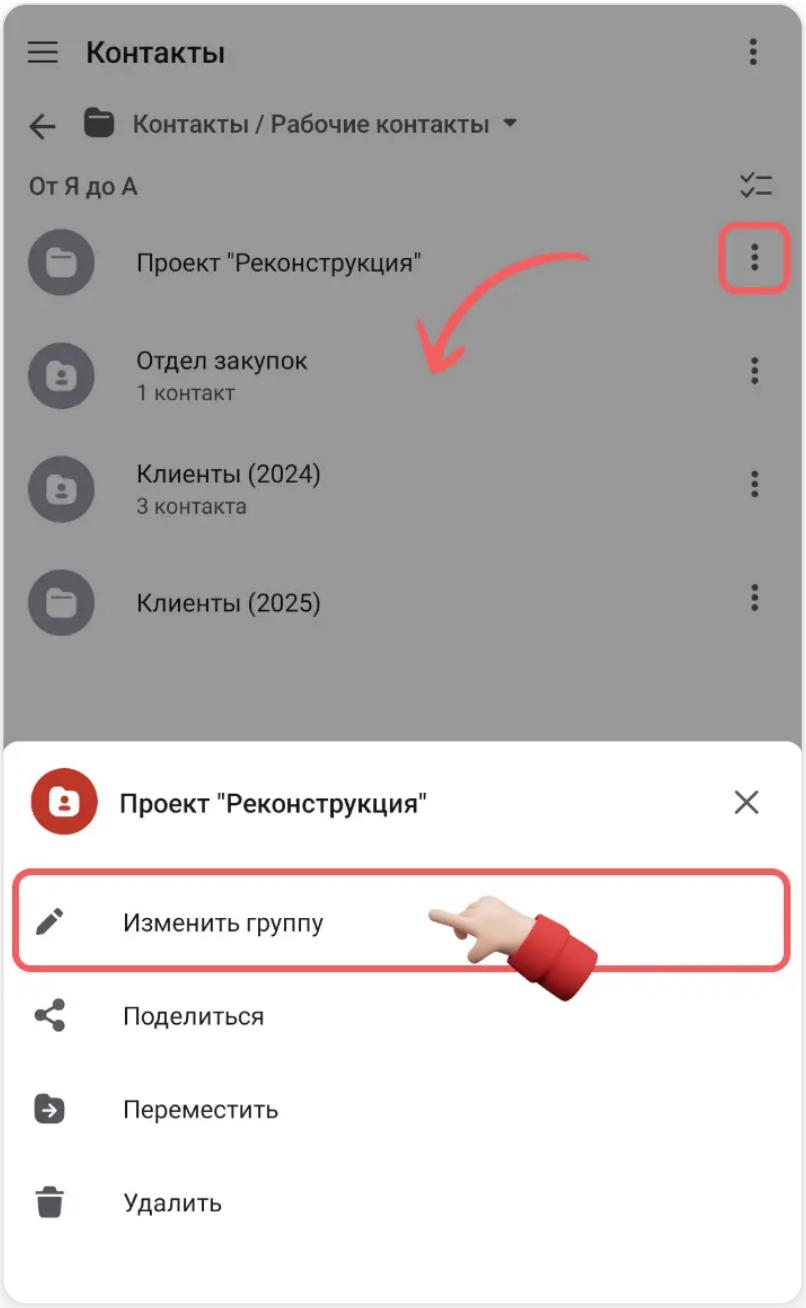
2. Поиск по группам

1. Откройте список групп в разделе **Контакты**.
2. Нажмите на кнопку **Поиск** .
3. Откроется окно поиска.
4. Введите поисковую фразу и дождитесь результатов.



3. Редактирование группы

1. Откройте раздел **Контакты**.
2. Вызовите меню действий по кнопке **Еще** ⋮ для группы, которую необходимо отредактировать.
3. В появившемся меню выберите действие **Изменить группу**.



4. Откроется форма редактирования группы.

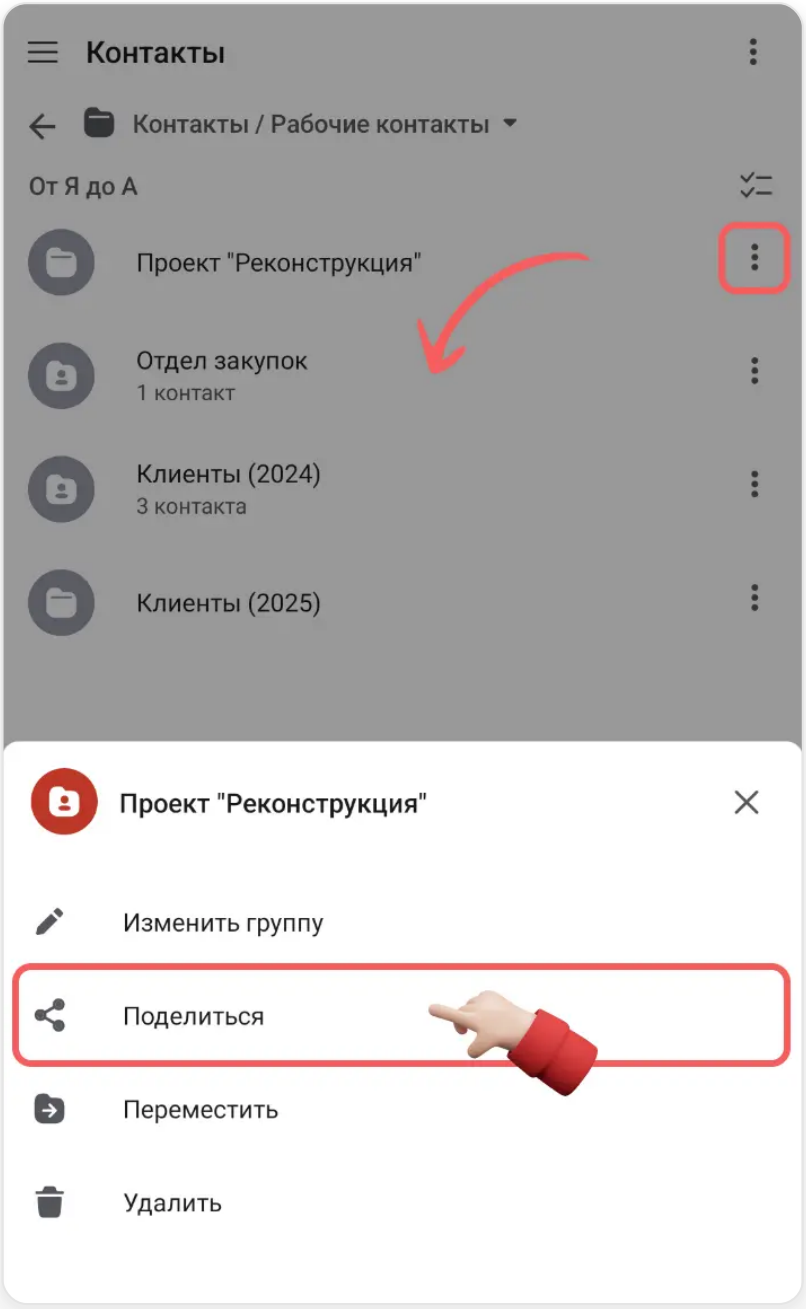
5. Внесите необходимые изменения.
6. Нажмите **Сохранить**.

5. Экспорт группы

В приложении поддерживается экспорт контактов в виде файла vCard.

> 🔍 Подробнее читайте в инструкции Импорт и экспорт контактов.

1. Откройте раздел **Контакты**.
2. Вызовите меню действий по кнопке **Еще** ⋮ для группы, которой необходимо поделиться.
3. В появившемся меню выберите действие **Поделиться**.



4. Откроется системное окно со списком приложений.
5. Выберите приложения для отправки или сохранения файла.

> 💡 При экспорте групп с контактами в файл будет сохранена их структура.

6. Перемещение группы

1. Откройте раздел **Контакты**.
2. Вызовите меню действий по кнопке **Еще** ⋮ для группы, которую необходимо переместить.
3. В появившемся меню выберите действие **Переместить**.
4. Откроется окно со списком групп.
5. Выберите группу, в которую необходимо переместить выбранную группу.

После завершения перемещения будет отображено уведомление об успешном выполнении операции.

7. Удаление группы

Удаление группы контактов означает безвозвратное удаление всей информации, связанной с этой группой. Это включает в себя удаление всех контактов и подгрупп, которые были добавлены в группу, а также удаление самой группы. После удаления группы восстановить информацию невозможно.

> ⚠️ **Примечание**: Если к контакту были привязаны сертификаты из файла, то при удалении контакта они не сохранятся в разделе «Настройки» → «Сертификаты других пользователей» и будут удалены вместе с контактом.

Чтобы удалить группу:

1. Откройте раздел **Контакты**.
2. Вызовите меню действий по кнопке **Еще** ⋮ для группы, которую необходимо удалить.
3. В появившемся меню выберите действие **Удалить**.
4. Подтвердите действие в модальном окне.

После удаления группы будет отображено уведомление об успешном выполнении операции. Группа пропадет из списка.

Инструкции по теме

- Как создать контакт
- Действия с контактом
- Управление сертификатами контакта

Открыть статью на сайте

Импорт и экспорт контактов в КриптоАРМ Подпись и шифрование

- Общая информация
- Импорт контактов
- Экспорт контактов
- Описание реквизитов контакта vCard
- Инструкции по теме

Общая информация

Приложение поддерживает формат **vCard** (Virtual Contact File) — международный стандарт для обмена электронными визитными карточками.

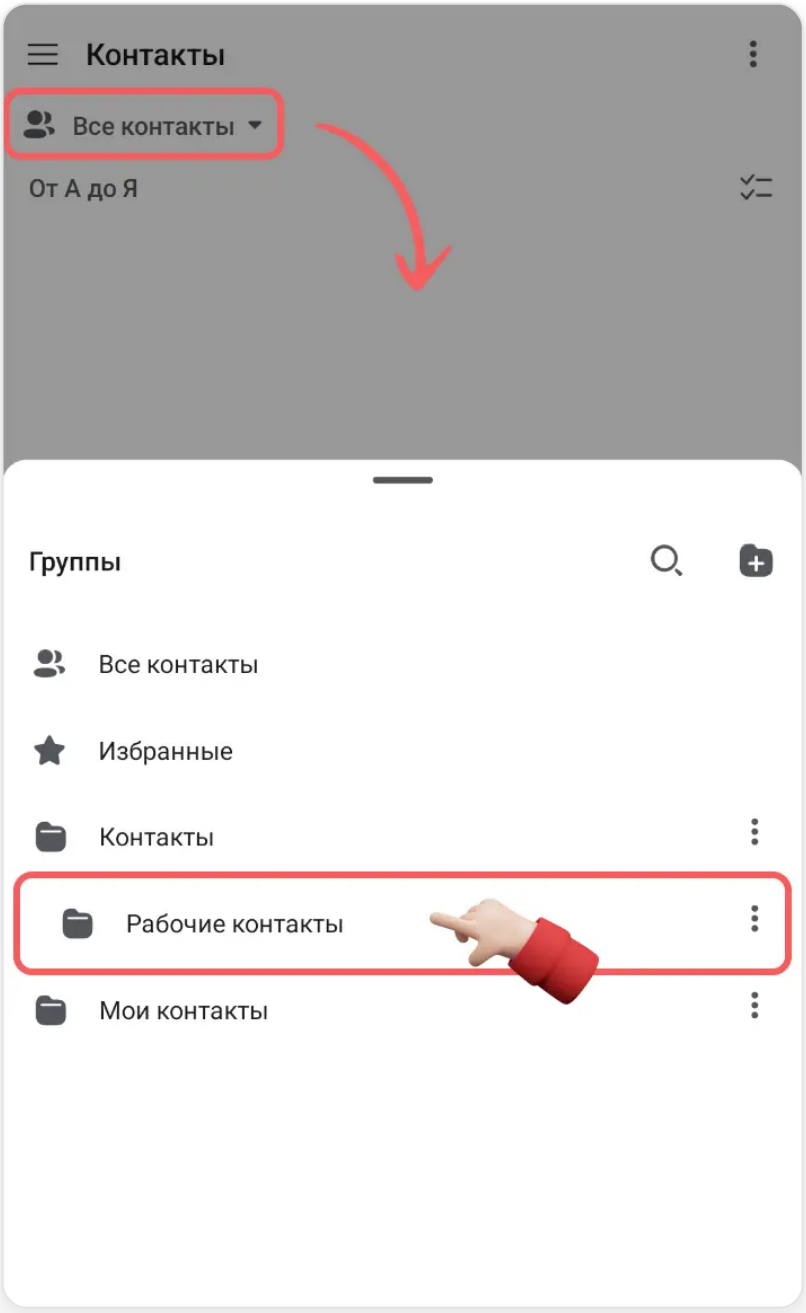
vCard позволяет хранить:

- Контактную информацию (ФИО, телефоны, email)
- Демографические данные (дата рождения, адрес)
- Мультимедийные элементы (фотографии, логотипы)
- Сертификаты

Импорт контактов

> 💡 **Совет**: Если vCard содержит контактные данные нескольких лиц, каждый контакт будет импортирован в виде отдельной записи.

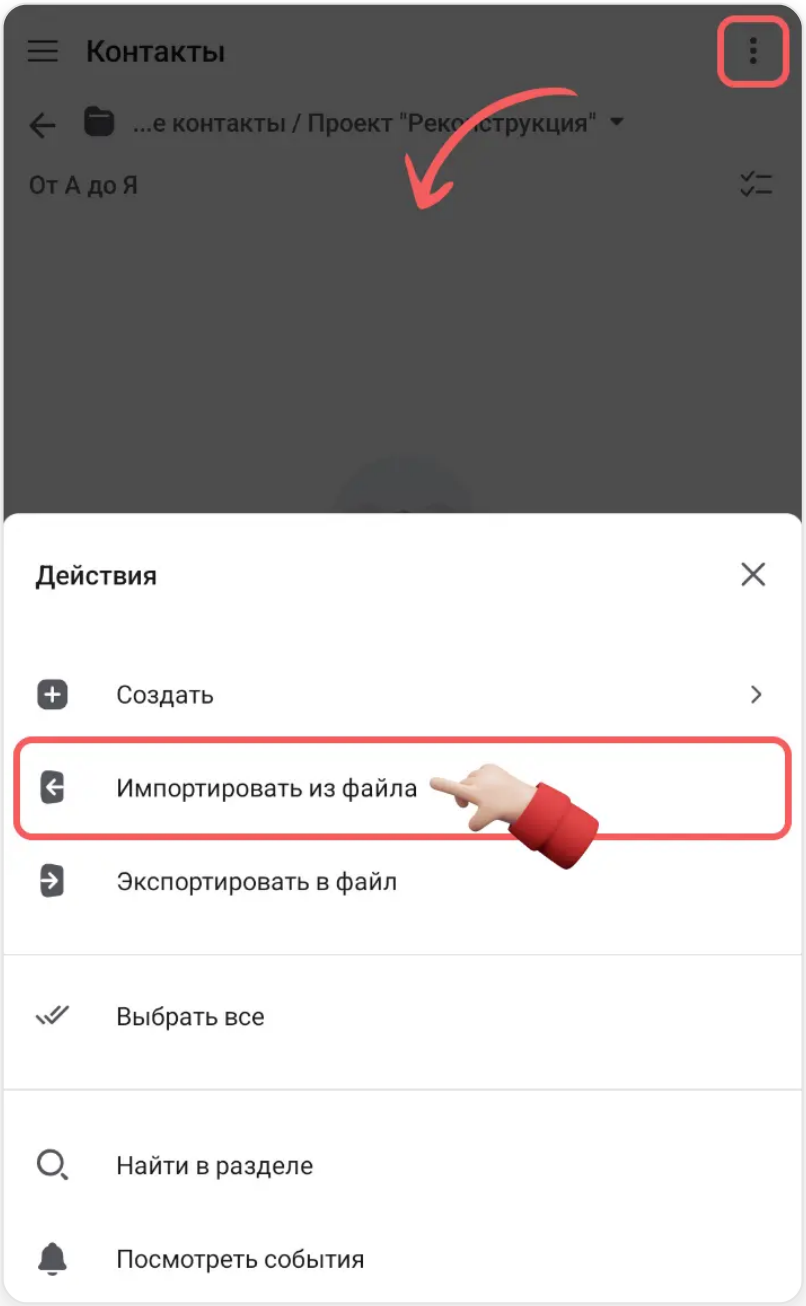
1. Откройте раздел **Контакты**.
2. Перейдите в группу, в которую необходимо импортировать контакты. Для этого нажмите на кнопку **Все контакты** в верхней части окна и в появившемся меню нажмите на название необходимой группы.



⚠️ **Примечание**: По умолчанию контакты будут импортированы в активную группу.

3. Вызовите меню **Действия** по кнопке **Еще** , размещенной в верхнем правом углу экрана.

4. В появившемся меню выберите действие **Импортировать из файла**.



5. Откроется системное окно файлового менеджера.
6. Выберите файл vCard (файл формата `.vcf`).

> ⚠️ **Примечание**: При импорте файла vCard, содержащего группы с контактами, в указанной папке будет создана структура групп и контактов в соответствии с файлом.

7. Будет запущен процесс импорта. В нижней части экрана будет выведено уведомление с прогрессом.

Дождитесь окончания операции.

Возможные ошибки

Уведомления об ошибках отображаются в нижней части экрана.

Для просмотра подробной информации нажмите **Просмотреть события** в меню **Действия**.

> 🔍 Подробнее об оповещениях читайте в инструкции Журнал событий.

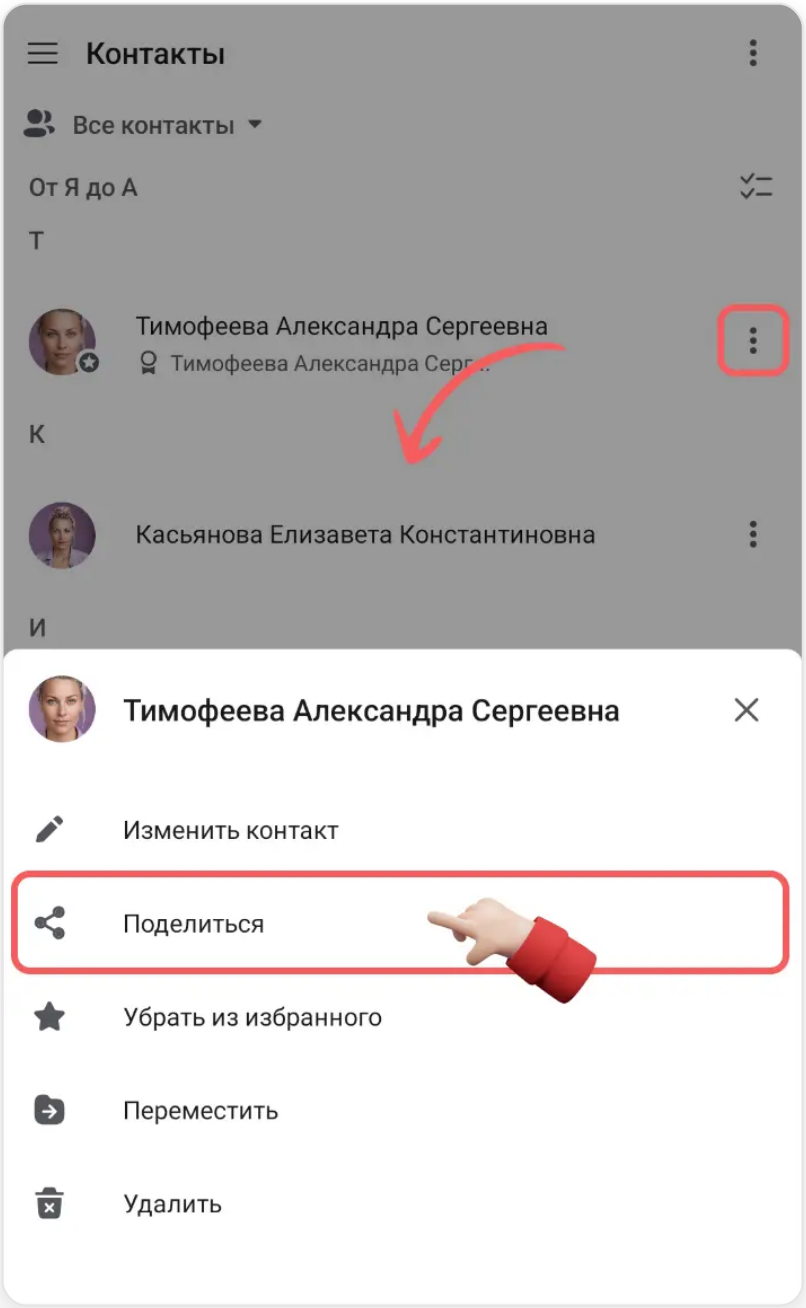
Ошибка	Описание	Рекомендуемые действия
Не удалось импортировать контакты	Возможно, файл пустой или поврежден	Проверьте содержимое файла и повторите импорт

Экспорт контактов

Поделиться контактом

> 💡 **Совет**: Вы можете экспортировать отдельные контакты, группы или всю адресную книгу.

1. Перейдите в раздел **Контакты**.
2. Вызовите меню действий, которое открывается по кнопке **Еще** , размещенной на панели с контактом в списке контактов.
3. В появившемся меню выберите действие **Поделиться**.



4. Откроется системное окно со списком приложений.

5. Выберите приложения для отправки или сохранения контакта.

Групповая отправка

1. Перейдите в раздел **Контакты**.

2. Отметьте флажками контакты одним из способов:
   - Выберите **Выбрать все** в меню **Действия**, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**. В списке контактов отобразятся флажки. Установите флажки напротив тех контактов, которые необходимо добавить в «Избранные».
   - Нажмите на панель с контактом и удерживайте ее. Выберите другие контакты.
3. Выберите **Поделиться** в меню действий, которое доступно по кнопке **Еще** , расположенной в верхнем правом углу раздела **Контакты**.
4. Откроется системное окно со списком приложений.
5. Выберите приложения для отправки или сохранения контакта.

Экспорт всей адресной книги

Экспорт адресной книги позволяет сохранить все контакты. Это полезно, если нужно перенести данные на новое устройство, поделиться ими или сделать резервную копию на случай потери или поломки телефона.

1. Откройте раздел **Контакты**.
2. Вызовите меню **Действия** по кнопке **Еще** , размещенной в верхнем правом углу экрана.
3. В появившемся меню выберите действие **Экспортировать в файл**.
4. Откроется системное окно со списком приложений.
5. Выберите приложения для отправки или сохранения файла.

Описание реквизитов контакта vCard

Реквизиты контакта	Тип	Реквизиты контакта (vCard)	Семантика	Пример
Версия	Текст	VERSION	Должен идти сразу после BEGIN	`VERSION:3.0`
Имя, фамилия, отчество в одну строку	Текст	FN	Полное имя в виде единой строки	`FN:к.м.н., пр. Nikita0503`
Имя, фамилия, отчество, префикс, суффикс	Текст	N	Структурированное представление имени (фамилия;имя;отчество;префиксы;суффиксы)	`N:Иванов;Иван;Иванович`
Обращение	Текст	NICKNAME	Никнейм	`NICKNAME:Nikita0503`

Реквизиты контакта	Тип	Реквизиты контакта (vCard)	Семантика	Пример
Аватар контакта	Текст	PHOTO	Изображение в binary формате	`PHOTO;ENCODING=b;TYPE=JPEG:MIICajCCAdOg...`
Дата рождения	Текст	BDAY	Формат: ГГГГ-ММ-ДД или с временной зоной	`BDAY:1970-12-31`
Адрес	Текст	ADR	Структурированные компоненты адреса (через ;)	`ADR;TYPE=work:;;ул. Ленина 1;Москва;;101000;Россия`
Пол	Текст	GENDER	Мужской/Женский/Не выбран	`GENDER:M`
Телефон	Число	TEL	Номер с указанием типа (work, home, cell)	`TEL;TYPE=work,cell:+7-999-123-4567`
Адрес электронной почты	Текст	EMAIL	Адрес с указанием типа (internet, x400)	`EMAIL;TYPE=INTERNET:ivanov@example.com`
Часовой пояс	Текст	TZ	Смещение или текстовое описание	`TZ:+03:00`
Широта и долгота	Число	GEO	Формат: широта,долгота	`GEO:55.7558,37.6176`
Должность	Текст	TITLE	Официальное наименование позиции	`TITLE:Директор по развитию`
Профессия	Текст	ROLE	Стандартизированное описание деятельности	`ROLE:Программист`
Логотип организации	Текст	LOGO	Изображение логотипа в binary формате	`LOGO;VALUE=uri:http://example.com/logo.webp`
Организация	Текст	ORG	Название и подразделения (через ;)	`ORG:ООО "Рога и Копыта";Отдел продаж`
Язык	Текст	LANG	Предпочитаемый язык контакта	`LANG:ru`
Примечание	Текст	NOTE	Произвольные комментарии	-

Реквизиты контакта	Тип	Реквизиты контакта (vCard)	Семантика	Пример
Идентификатор	Число	UID	Глобально уникальный ID	-
Сайт	Текст	URL	Веб-адрес	`URL:http://company.com`
Сертификат	Текст	KEY	Открытый ключ в кодировке BASE-64	`KEY;ENCODING=b:MIICajCCAdOgAwIBAgICBEU...`

Инструкции по теме

- Как создать контакт
- Действия с контактом
- Управление сертификатами контакта
- Группы контактов

Открыть статью на сайте

Личный контакт в КриптоАРМ Подпись и шифрование

- О группе «Мои контакты»
- Создание личного контакта
- Инструкции по теме

О группе «Мои контакты»

Группа «**Мои контакты**» — это место для хранения и управления вашими личными контактами. К каждому контакту можно привязать личный электронный сертификат. Это удобно для быстрого поиска и использования контактов для шифрования и других операций.

Личный контакт сохраняет все функции обычного контакта, но привязан к вашему сертификату.

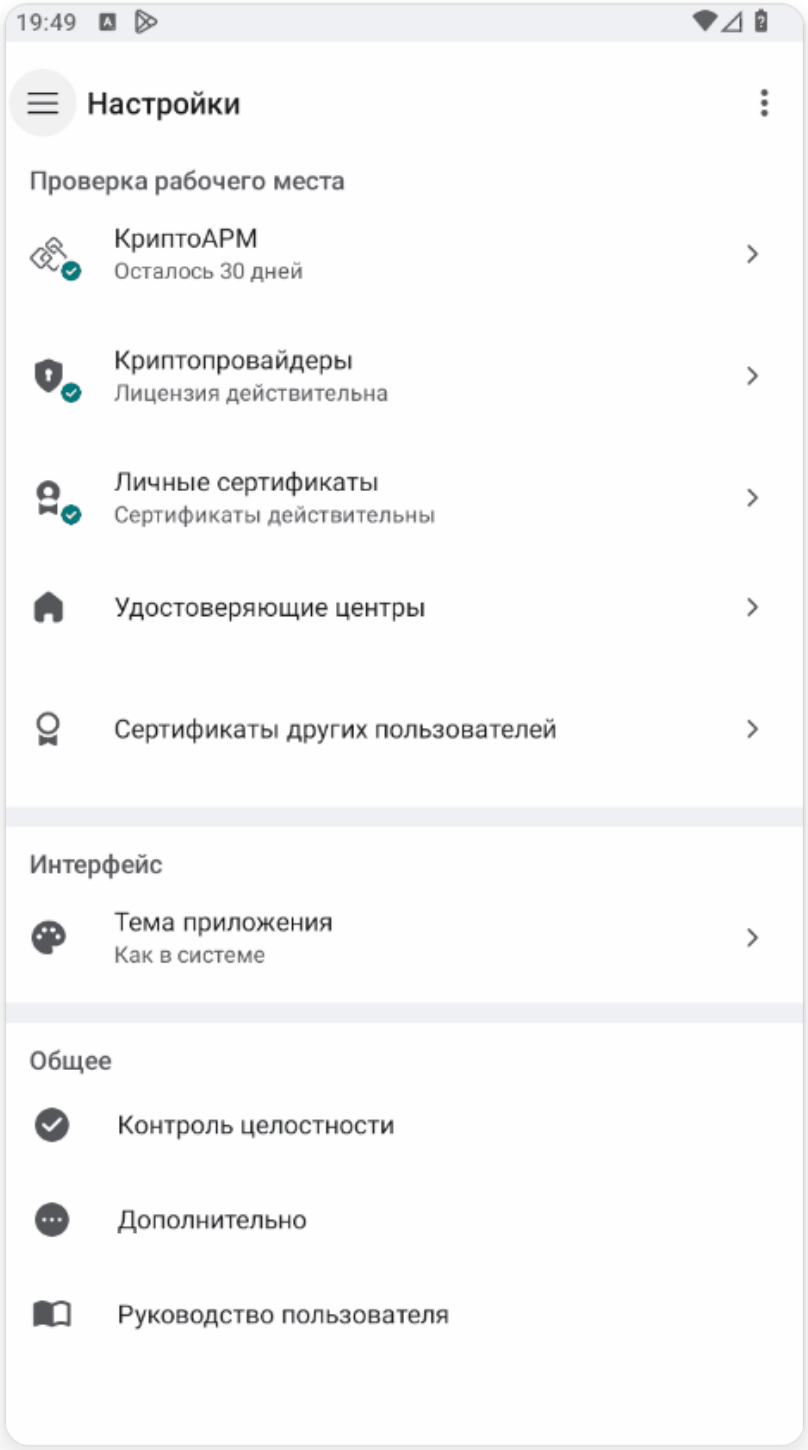
Для чего нужен «Мой контакт»

- **Шифрование в свой адрес**: Личный контакт позволяет быстро зашифровать документы для себя, используя привязанный личный сертификат.
- **Удобный обмен контактами**: Вы можете легко делиться своим контактом с другими пользователями, предоставляя данные и сертификат для безопасного обмена файлами.
- **Быстрый доступ**: Контакт автоматически содержит сведения из вашего электронного сертификата, что упрощает использование и поиск.

Создание личного контакта

> 💡 **Совет**: Перед созданием контакта убедитесь в том, что в приложении установлен личный сертификат. Подробнее про установку читайте в инструкции Установка личного сертификата.

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Нажмите на кнопку **Еще** ⋮, размещенную на панели с сертификатом, для которого необходимо создать «Мой контакт».
3. В появившемся меню действий выберите действие **Создать контакт**.



В группе «Мои контакты» будет создан персональный контакт с привязанным личным сертификатом. Данные контакта будут заполнены на основе данных электронного сертификата.

> 💡 **Совет**: С личным контактом доступны те же действия, что и с другими контактами. Подробнее читайте в инструкции Действия с контактами.

Инструкции по теме

- Группы контактов
- Действия с контактами
- Управление сертификатами контакта
- Как поделиться контактом

Открыть статью на сайте

Глобальный поиск в КриптоАРМ Подпись и шифрование

- Общие сведения
- Запуск поиска
- Действия с результатами поиска
- Инструкции по теме

Общие сведения

Глобальный поиск — это инструмент, позволяющий быстро и эффективно находить любые данные, независимо от того, где они находятся: в разделе **Настройки**, **Архив** или **Контакты**.

Как работает поиск

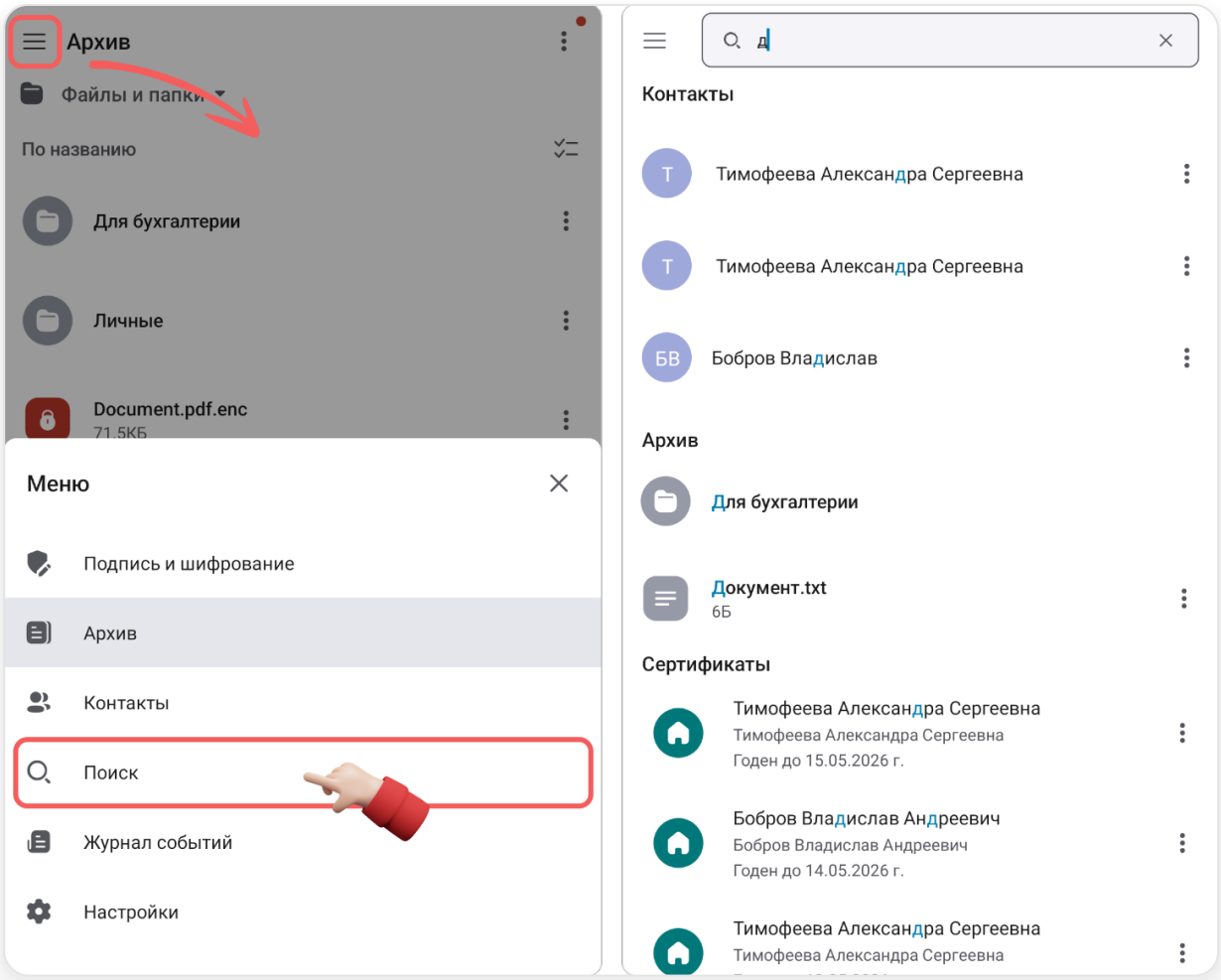
- **По названию**: поиск по совпадению в наименовании элемента
- **По расширению документов**
- **Рекурсивный**: охватывает все вложенные каталоги и группы
- **Ограничения**: не учитывает метаданные (дату, автора и др.)

> 💡 **Совет**: Чтобы найти все **подписанные документы**, введите в строку поиска расширение подписи — `.sig`.

Запуск поиска

1. Глобальный поиск

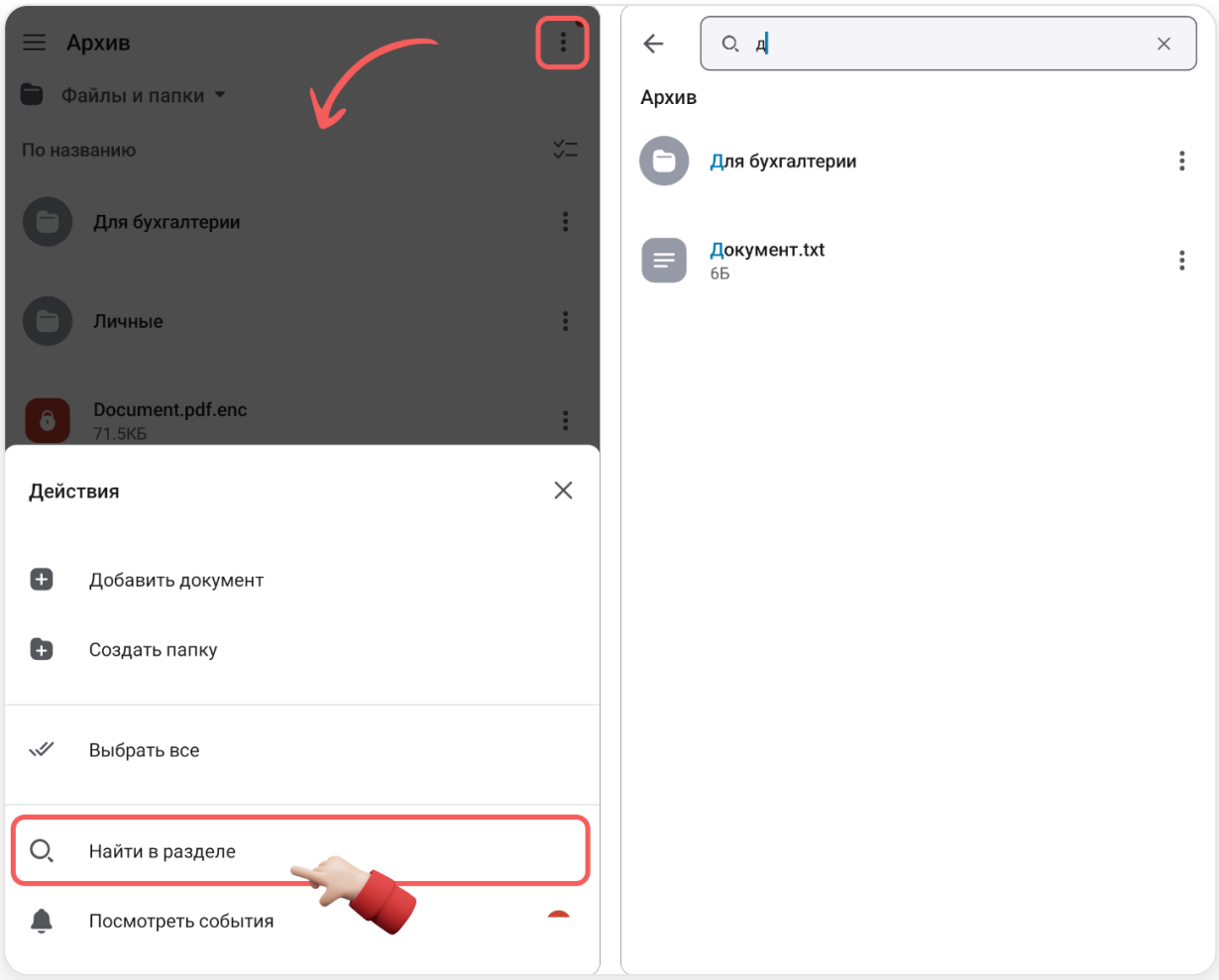
1. Вызовите главное меню по кнопке ☰, размещенной в верхнем части окна приложения.
2. Выберите пункт **Поиск**.



3. Введите поисковый запрос в поле **Поиск**.

2. Поиск по разделам

1. Перейдите в раздел **Архив** или **Контакты**.
2. Вызовите меню действий по кнопке **Еще**, размещенной в верхней части окна приложения.
3. Выберите действие **Поиск по разделу**.



4. Введите поисковый запрос в поле **Поиск**.

Действия с результатами поиска

Тип элемента	Доступные действия
Документы	Полный набор действий как в разделе Архив
Контакты	Все действия из раздела Контакты
Сертификаты	Стандартные операции как в разделе **Настройки**
Папки/Группы	Только переход по нажатию (редактирование недоступно)

> ⚠️ **Важно**: Для работы с группами и папками перейдите в раздел, которому они принадлежат.

Инструкции по теме

- Журнал событий
- Часто задаваемые вопросы
- Глоссарий

Открыть статью на сайте

Журнал событий КриптоАРМ Подпись и шифрование

- Назначение и доступ
- Уровни событий
- Работа с записями журнала
- Инструкции по теме

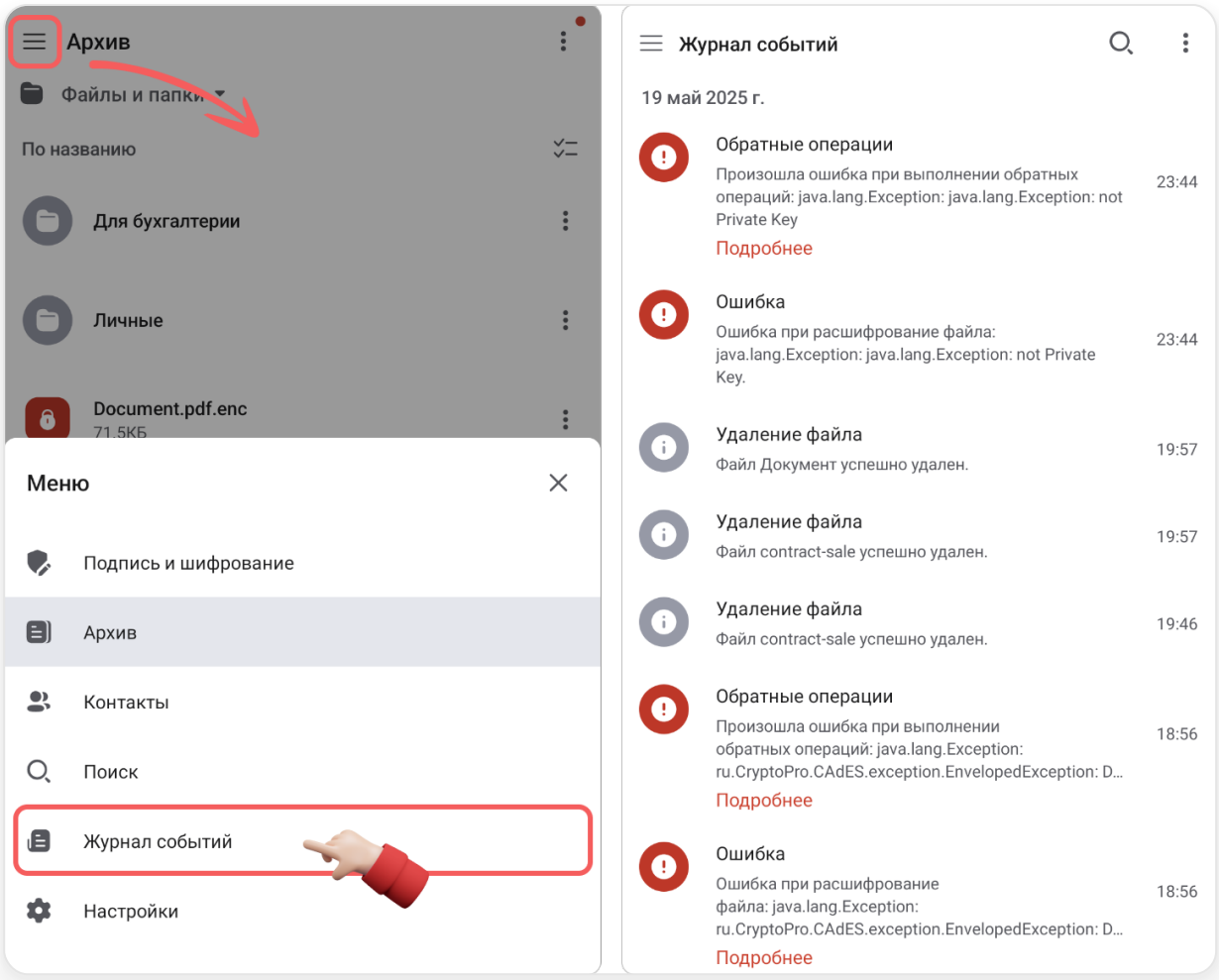
Назначение и доступ

Журнал событий фиксирует все значимые действия и ошибки в приложении, предоставляя:

- Детальную информацию о выполненных операциях
- Диагностические данные для устранения неполадок
- Историю работы для аудита и анализа

Чтобы открыть журнал:

1. Вызовите главное меню по кнопке , размещенной в верхнем части окна приложения.
2. Выберите пункт **Журнал событий**.



Уровни событий

Журнал поддерживает несколько уровней логирования:

Уровень	Описание	Примеры
Все	Полная история событий	-
Информация	Стандартные действия	Подписание документа, экспорт данных
Ошибки	Критические проблемы	Сбои при выполнении операций
Предупреждения	Потенциальные проблемы	Отсутствие лицензии, неполные данные

Работа с записями журнала

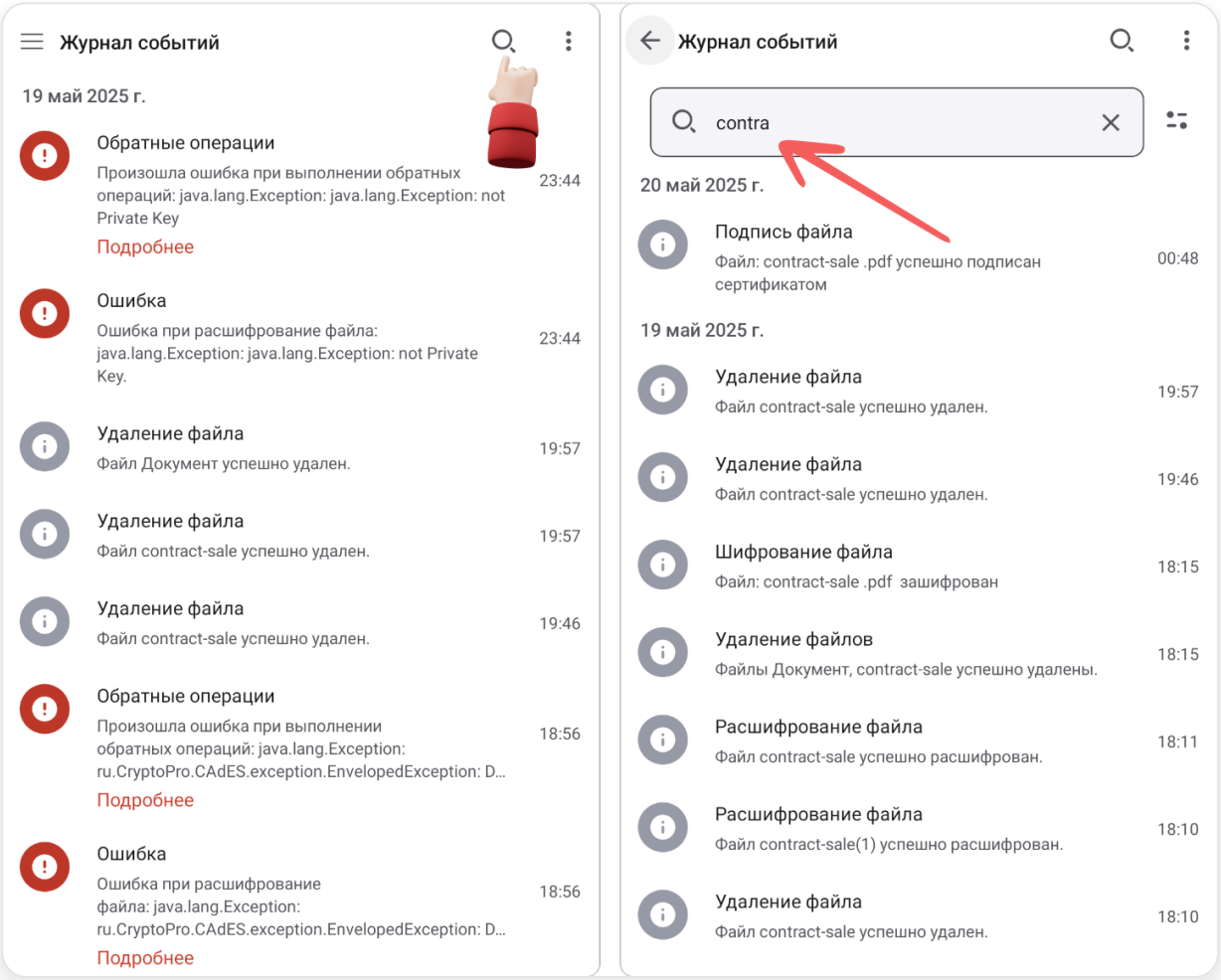
1. Просмотр события

1. Перейдите в **Журнал событий**.
2. Нажмите на панель с событием, которое хотите просмотреть.
3. Откроется окно с подробными сведениями о событии.

2. Поиск и фильтрация

Быстрый поиск

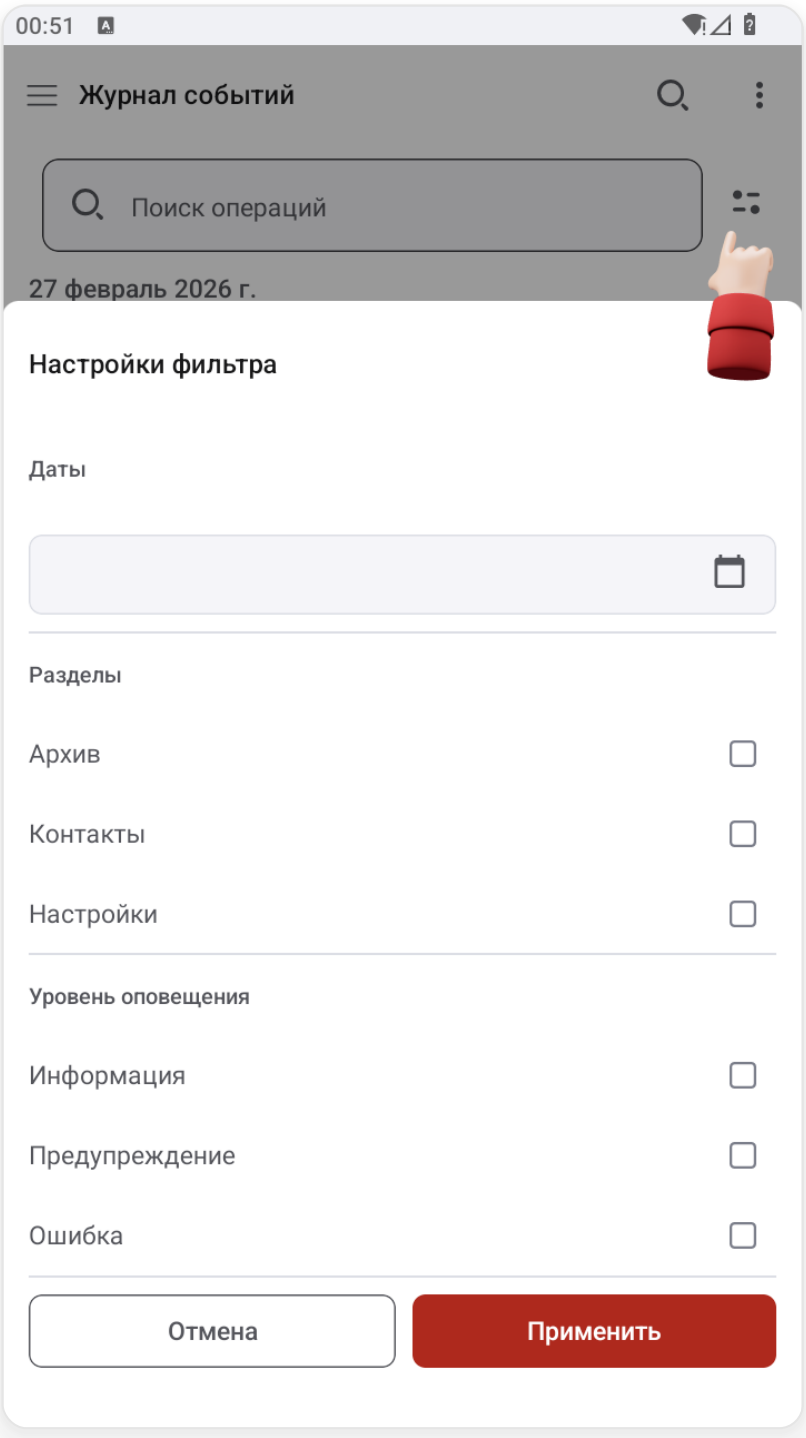
1. Перейдите в **Журнал событий**.
2. Нажмите кнопку **Поиск** , размещенную на верхней панели.
3. Над списком событий отобразится поле для ввода поисковой фразы.
4. Введите текст (поддерживается частичное совпадение).



Расширенная фильтрация

1. Перейдите в **Журнал событий**.

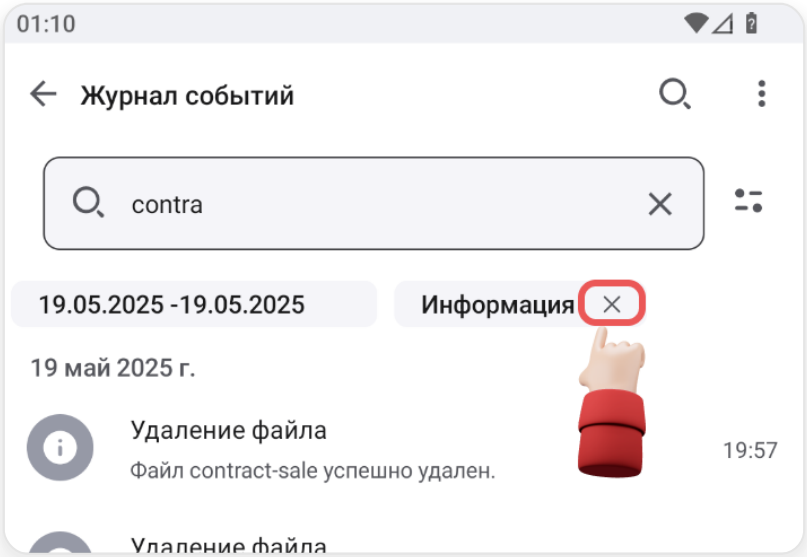
2. Нажмите кнопку **Поиск** , размещенную на верхней панели.
3. Над списком событий отобразится поле для ввода поисковой фразы.
4. Нажмите на кнопку **Настройки** , размещенную справа от поля.



5. В появившемся окне **Настройки фильтра** укажите:
   - **Период** (дата начала и окончания)
   - **Раздел** приложения
   - **Уровень оповещения**

6. Нажмите кнопку **Применить**.

Чтобы сбросить фильтр, нажмите на кнопку **Отмена** на соответствующем чипсете.



3. Экспорт данных

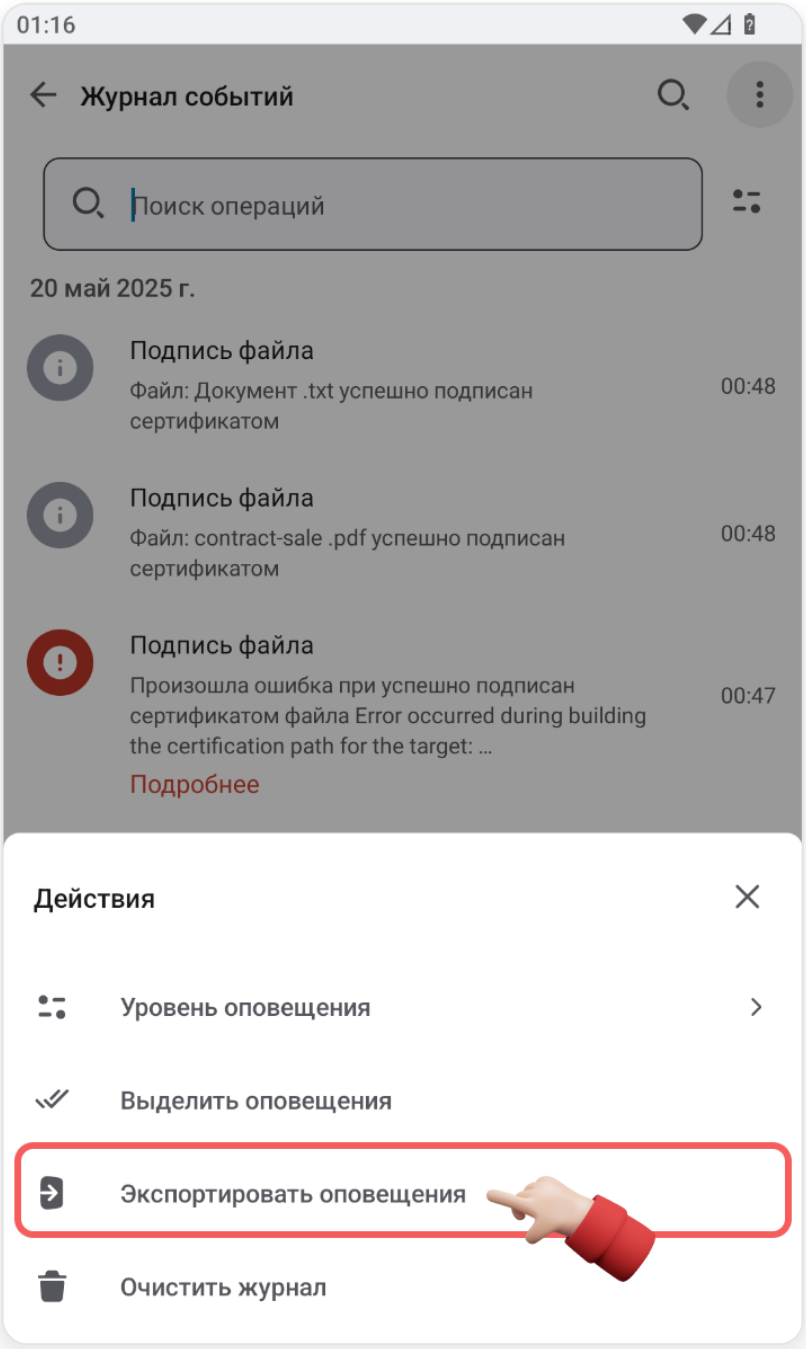
Журнал событий можно выгрузить в текстовый файл.

Для каждого события в файл будет записана следующая информация:

- ID - номер события,
- Title - заголовок события,
- Description - описание события,
- Type - уровень логирования,
- Chapter - раздел, в котором возникло событие,
- Date - дата возникновения события.

Полный экспорт журнала

1. Перейдите в **Журнал событий**.
2. Вызовите меню **Действия** по кнопке **Еще**, размещенной в верхней части окна.
3. Выберите действие **Экспортировать оповещения**.
4. Выберите приложения для отправки или сохранения файла.



Экспорт выбранных событий

1. Перейдите в **Журнал событий**.
2. Вызовите меню **Действия** по кнопке **Еще**, размещенной в верхней части окна в **Журнале событий**.
3. Выберите действие **Выделить оповещения**.
4. Отметьте флажками события, которые необходимо экспортировать.
5. На появившейся панели действий в нижней части экрана выберите необходимое действие:
    - **Сохранить** для сохранения **Журнала** в папке приложения.
    - **Отправить** для отправки **Журнала** в другое приложение.

4. Очистка журнала

> ⚠️ **Примечание**: После очистки восстановить данные невозможно.

1. Перейдите в **Журнал событий**.
2. Вызовите меню **Действия** по кнопке **Еще**, размещенной в верхней части окна в **Журнале событий**.
3. Выберите действие **Очистить журнал**.
4. Подтвердите действие в модальном окне.

Все события, зафиксированные в Журнале, будут удалены.

Инструкции по теме

- Глобальный поиск
- Часто задаваемые вопросы
- Глоссарий

Открыть статью на сайте

Часто задаваемые вопросы

О продукте

- Возможности КриптоАРМ
- Поддерживаемые криптопровайдеры
- Поддерживаемые ключевые носители

Начало работы

- Скачивание КриптоАРМ
- Установка сертификата из файла .pfx
- Установка сертификата через QR-код
- Установка сертификата с защищённого носителя
- Создание запроса на сертификат
- Генерация самоподписанного сертификата
- Получение квалифицированной электронной подписи
- Импорт корневого или промежуточного сертификата
- Импорт сертификата другого пользователя

Проверка рабочего места

- Запуск проверки рабочего места
- Скачивание или отправка отчета о системе

Лицензирование

- Активация лицензионного ключа КриптоАРМ
- Активация лицензионного ключа КриптоПро CSP

Подпись и шифрование

- Создание подписи
- Шифрование файлов

Проверка и расшифрование

- Расшифровка файлов
- Проверка подписи файла
- Удаление подписи с файла

Контакты

- Добавление нового контакта
- Создание контакта из сертификата
- Создание контакта при проверке подписи
- Импорт контакта из файла vCard
- Добавление сертификата к контакту
- Настройка сертификата по умолчанию
- Отправка контакта другому пользователю
- Создание группы контактов
- Отправка группы контактов
- Экспорт всех контактов

Открыть статью на сайте

Глоссарий

Сертификаты

Сертификат электронной подписи

Электронный документ, который подтверждает владение ключом электронной подписи

Сертификат усиленной квалифицированной электронной подписи (УКЭП)

Выпускает только аккредитованный удостоверяющий центр. Документ, подписанный УКЭП, действителен для любой организации или ведомства.

Самоподписанный сертификат

Сертификат, изданный самим пользователем, без обращения к Удостоверяющему центру.

Открытый ключ электронной подписи

Ключ проверки электронной подписи. Содержит содержит уникальный код, с помощью которого можно проверить подлинность электронной подписи. Сертификат открытого ключа содержит сведения о подписанте (ФИО, СНИЛС и др.), об удостоверяющем центре, который выдал ЭП и срок действия ключа.

Закрытый ключ электронной подписи

Секретный уникальный набор символов, который также формируется криптопровайдером. Закрытый ключ необходим для формирования электронной подписи и хранится в зашифрованном виде, как правило, на носителе (токене). Доступ к закрытому ключу имеет только владелец.

Запрос на сертификат

Электронный документ, который содержит информацию для получения сертификата электронной подписи в Удостоверяющем центре

Ключевой контейнер

Способ хранения закрытых ключей. Кроме ключей, он содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т.п. Физическое представление ключевого контейнера зависит от типа ключевого носителя: флешка, жёсткий диск, смарт-карты, реестр.

Статус сертификата электронной подписи

Информация о действительности сертификата

Удостоверяющий центр (УЦ)

Доверенная организация, которая имеет право выпускать сертификаты электронной подписи (ЭП) юридическим и физическим лицам

Корневой сертификат

Цифровой документ, в котором содержится информация об удостоверяющем центре. Корневые сертификаты выдаются только организациям и могут иметь разный уровень. В Российской Федерации главный корневой сертификат принадлежит Министерству цифрового развития. На основе этого сертификата Минцифры РФ выдаёт удостоверяющим центрам собственные сертификаты, подписывая их своим корневым сертификатом.

Промежуточный сертификат

Сертификат, выданный удостоверяющим центрам

Сертификат другого пользователя

Сертификат, принадлежащий другому пользователю. Предназначен для шифрования документов в его адрес.

Список отзыва сертификатов

Список сертификатов, которые удостоверяющий центр пометил как отозванные.

Цепочка сертификации или цепочка доверия

Иерархическая коллекция сертификатов. Для квалифицированных сертификатов ЭП, как правило, состоит из 3 звеньев. Верхнее звено - корневой сертификат. Среднее звено - сертификат удостоверяющего центра. Конечное звено - сертификат пользователя.

Сервис DSS

Сервис электронной подписи. Предназначен для шифрования и расшифрования электронных документов, формирования запросов на создание и управление сертификатами ключей проверки электронной подписи, создания и проверки электронной подписи различного формата криптографических сообщений.

Подпись и шифрование

Электронная подпись (ЭП)

Информация в электронно-цифровой форме для определения и подтверждения личности автора подписи

Усиленная неквалифицированная электронная подпись (УНЭП)

Цифровой аналог собственноручной подписи. Применяется, если стороны заключили соглашение об этом или так указано в законе. В таких случаях документы, подписанные от руки или с помощью УНЭП, имеют равную юридическую силу.

Усиленная квалифицированная электронная подпись (УКЭП)

Цифровой аналог собственноручной подписи. Ей можно подписывать любые документы без предварительной договорённости с другой стороной.

Профили подписи в КриптоАРМ

Заранее подготовленные наборы настроек, которые можно применять для выполнения подписи, архивирования и шифрования.

Алгоритмы подписи

Криптографические алгоритмы, которые используются для создания электронной цифровой подписи

Алгоритмы шифрования

Криптографические алгоритмы, которые используются для шифрования файлов

Криптопровайдер

Провайдер криптографических услуг, криптопровайдер специализированный программный модуль или набор модулей, предоставляющих средства шифрования и дешифрования данных, цифровой подписи, а также генерации и хранения ключей.

Присоединенная подпись

Подпись, в процессе создания которой формируется специальный контейнер, в котором находятся как подписываемый документ, так и файл подписи.

Отсоединенная подпись

Файл подписи формируется и хранится отдельно от подписываемого документа.

Стандарт подписи CAdES-BES (Basic Electronic Signature)

Основной и простейший формат электронной подписи, описываемый в стандарте CAdES. Он обеспечивает базовую проверку подлинности данных и защиту их целостности

Стандарт подписи CAdES-T (Timestamp)

Формат электронной подписи, в которую автоматически добавляется штамп времени на подпись.

Стандарт подписи CAdES-X Long Type 1

Формат электронной подписи, включающий дополнительные атрибуты certificate-values и revocation-values, которые представляют собой полные данные сертификатов и списки отзыва сертификатов. А также штампы времени на подпись и ссылки на сертификаты и списки отзыва сертификатов.

Стандарт подписи CAdES-A (Archival)

Формат электронной подписи, сформированный на основе CAdES-X Long Type 1 или Type 2 путём добавления одного или нескольких атрибутов archive-time-stamp, представляющих собой архивные штампы времени.

Машиночитаемая доверенность

Аналог бумажной доверенности в электронном виде. Она создаётся в формате XML, который позволяет компьютеру прочитать её содержание и подтвердить личность того, кто подписал документ

vCard

Текстовый формат для обмена электронными визитными карточками. В карточке может содержаться имя, номера телефонов, адрес электронной почты, адрес проживания, дата рождения, фотография, сертификат и другие данные контакта.

Открыть статью на сайте

- КриптоАРМ Mobile
- КриптоАРМ
- электронная подпись
- шифрование данных author: Команда date: 2026-05-50 updated: 2025-05-05

КриптоАРМ Mobile

КриптоАРМ Mobile — приложение для электронной подписи и шифрования на мобильных устройствах.

КриптоАРМ Mobile может использоваться для безопасного хранения и передачи электронных документов в системах корпоративной защищенной мобильности. Поддерживает алгоритмы ГОСТ Р 34.10-2012, ГОСТ 34.12-2018. Приложение КриптоАРМ представлено под платформы Android и Аврора.

КриптоАРМ Mobile для IOS (версия 1.2)

Документация

Инструкции по установке

КриптоАРМ Mobile для Android (версия 1.2)

Документация

Инструкции по установке

КриптоАРМ Mobile для Аврора (версия 1.0)

Документация

Инструкции по установке

Функциональные возможности

- **Работа с документами**
  - работа с результатами выполнения операций с документами
  - хранение копии документов, полученных в результате выполнения операций
  - переход в мастер прямых (подпись и шифрование) и обратных (проверка подписи и расшифрование) операций
- **Электронная подпись**
  - электронная подпись и проверка подписи произвольных файлов на поддерживаемых платформах
  - добавление электронной подписи (функция создания соподписи) на поддерживаемых платформах
  - создание присоединенной и отсоединенной электронной подписи
  - создание подписи со штампом времени на подпись и подписываемые данные
  - создание усовершенствованной подписи
  - подпись сертификатом DSS
- **Шифрование/расшифрование**
  - шифрование и расшифрование файлов на поддерживаемых платформах
  - удаление исходных файлов после шифрования
  - шифрование по стандарту PKCS#7/CMS
  - расшифрование сертификатом DSS
- **Управление контактами**
  - создание локальных контактов
  - добавление сертификата к контакту
  - импорт контактов из каталога LDAP
  - шифрование документов в адрес контактов
- **Архивирование**
  - архивирование файлов перед шифрованием
- **Управление сертификатами и ключами**
  - отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых - криптопровайдеров
  - проверка корректности выбранного сертификата с построением цепочки доверия и скачиванием актуального списка отзыва
  - хранение закрытых ключей на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.), ESMART (ISBC) при условии использования криптопровайдера КриптоПро CSP
  - создание запросов на сертификат
  - импорт сертификатов с привязкой к закрытому ключу
  - экспорт сертификатов

- удаление сертификатов
- импорт сертификатов из DSS

- **Журнал событий и уведомления**
  - отображение списка событий по уровням детализации
  - просмотр уведомлений о событиях