Цифровые технологии

КриптоАРМ Mobile · Android

Документация продукта

Релиз v1.0

> Архивная документация. Актуальный релиз: v1.2

Исходная документация на CryptoARM.ru

Редакция от 26.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Общие сведения

О продукте ... 4

Функциональность ... 6

Лицензирование ... 8

Начало работы

Установка и первый запуск ... 9

Проверка рабочего места ... 14

Установка лицензий ... 21

Настройки

Личные сертификаты и запросы

Установка личного сертификата ... 25

Создание самоподписанного сертификата ... 35

Создание запроса ... 40

Просмотр и проверка статуса сертификата ... 49

Экспорт личного сертификата ... 53

Удаление сертификата ... 60

Сертификаты удостоверяющих центров и списки отзыва

Установка корневого и промежуточного сертификатов ... 63

Установка списка отзыва ... 67

Сертификаты других пользователей

Установка сертификатов других пользователей ... 71

Экспорт и удаление сертификата другого пользователя ... 75

Профили подписи

Управление профилями ... 78

Описание полей профиля ... 86

Прочие настройки

Настройка интерфейса ... 90

Общие настройки ... 93

Подпись и шифрование

Подпись документов ... 98

Добавление соподписи ... 108

Шифрование документов ... 120

Проверка и расшифрование

Проверка подписи ... 128

Снятие подписи ... 134

Расшифрование ... 139

Архив

Действия с документами ... 144

Группировка документов ... 151

Контакты

Создание контакта ... 158

Действия с контактами ... 168

Управление сертификатами контакта ... 182

Группы контактов ... 190

Импорт и экспорт контактов ... 199

Мои контакты ... 207

Поиск

Глобальный поиск ... 210

Журнал

Журнал событий ... 214

FAQ

Часто задаваемые вопросы ... 223

Глоссарий ... 225

Открыть статью на сайте

О продукте

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.

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 локальных 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, 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" и выше;
- Поддержка 3G, 4G, LTE рекомендуется;
- Фото-камера 8МП и выше;
- Наличие функции USB-host.

Открыть статью на сайте

Функциональность

Возможности	
Электронная подпись	Электронная подпись произвольных файлов размером до 50 Мб. Размер файла не может быть больше, чем свободная оперативная память.
	Создание присоединенной и отсоединенной электронной подписи
	Поддержка стандарта электронной подписи ГОСТ Р 34.10-2012, ГОСТ 34.12-2018, RSA, ECDSA
	Создание подписи со штампом времени на подпись и подписываемые данные CAdES -T
	Создание усовершенствованной подписи CAdES-X Long Type 1
	Соподпись
	Снятие электронной подписи с документа
Проверка электронной подписи	Проверка электронной подписи файлов размером до 50 Мб. Размер файла не может быть больше, чем свободная оперативная память.
Шифрование/расшифрование	Шифрование и расшифрование файлов размером до 50 Мб. Размер файла не может быть больше, чем свободная оперативная память.
	Шифрование по стандарту PKCS#7 и CMS. Поддержка ГОСТ Р 34.12-2015 (ГОСТ 34.12-2018) 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

Возможности	
	Импорт сертификатов с привязкой к закрытому ключу
	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 с контактами
	Экспорт/импорт контактов в формате vCard
	Создание личного контакта с личными сертификатами
Работа с журналом событий и уведомлениями	Отображение списка событий по уровням детализации
	Просмотр уведомлений о событиях
Работа с файлами в каталоге Архив	Сохранение результатов операций с файлами в разделе «Архив»
Поддержка тем	Поддержка и переключение тем
Проверка рабочего места	Проверка готовности приложения к работе
Проверка контроля целостности приложения	Обеспечение безопасности данных и предотвращение несанкционированного доступа к информации
Проверка флага KeyAgreement	Контроль соответствия требованиям стандарта безопасности ключей, которые используются в процессе обмена ключами

Открыть статью на сайте

Лицензирование

- Общая информация о лицензиях
- Пробная лицензия

Общая информация о лицензиях

Для выполнения криптографических операций в КриптоАРМ требуется действующая лицензия.

Доступны следующие варианты лицензий:

- **Пробная лицензия** (30 дней)
- **Годовая лицензия**
- **Бессрочная лицензия**

Приобрести лицензию КриптоАРМ можно в официальном интернет-магазине cryptoarm.ru.

> 🚨 Для криптопровайдера КриптоПро CSP потребуется приобретение отдельной лицензии. В интернет-магазине cryptoarm.ru можно приобрести годовую или бессрочную версию лицензии криптопровайдера.

Пробная лицензия

При первой установке приложения активируется ознакомительная лицензия КриптоАРМ со сроком на 30 дней и лицензия КриптоПро CSP со сроком на 90 дней.

По окончании ознакомительного периода для полнофункциональной работы приложения требуется приобретение лицензии КриптоАРМ.

> 🔐 Без лицензии в КриптоАРМ будут недоступны функции подписи и расшифрования.

Открыть статью на сайте

Установка и первый запуск

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

Где скачать КриптоАРМ

Загрузить и установить приложение **КриптоАРМ Mobile** 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 Mobile** 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

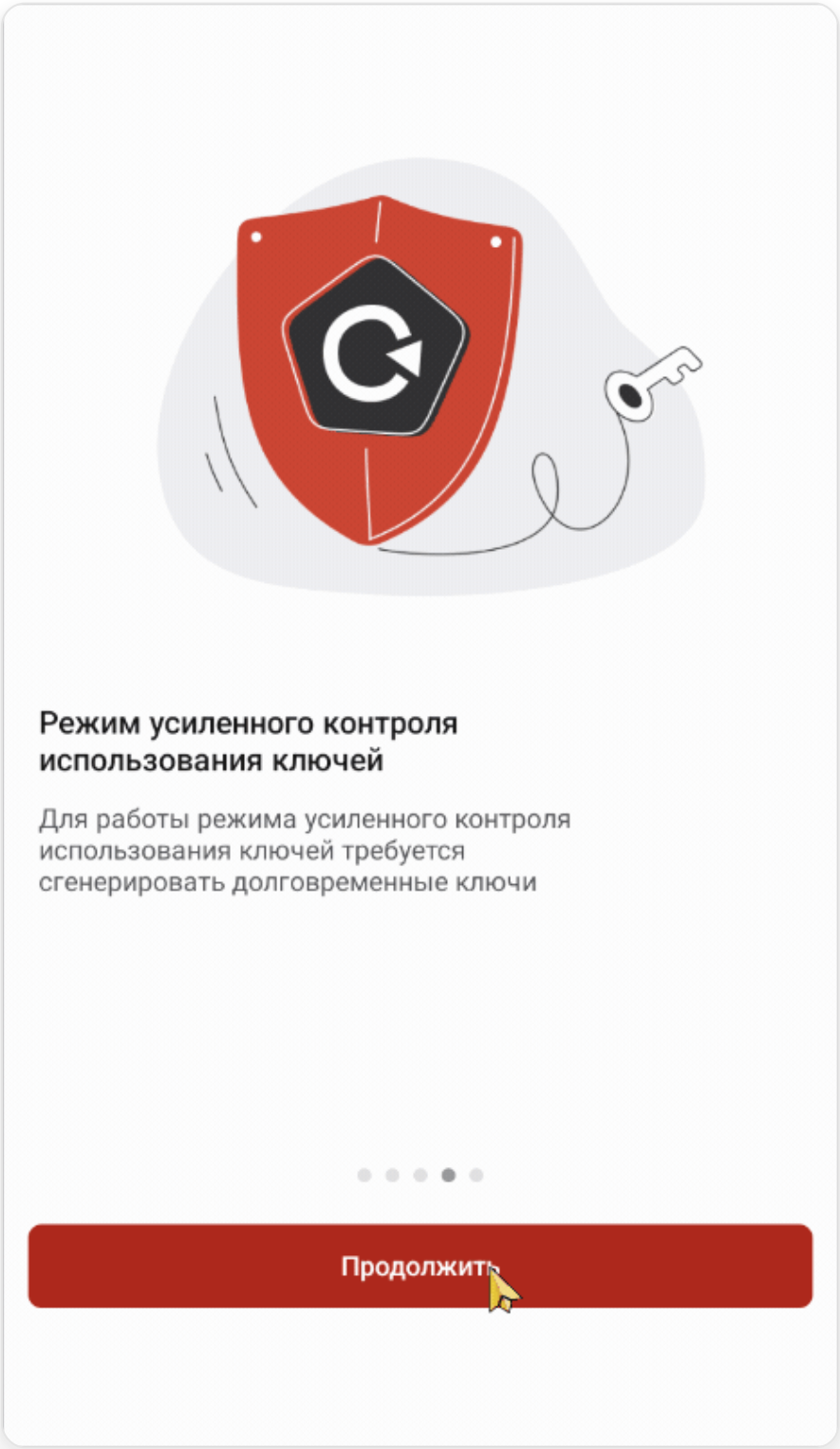
Что это такое?

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

Проверка рабочего места

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

Зачем нужна проверка

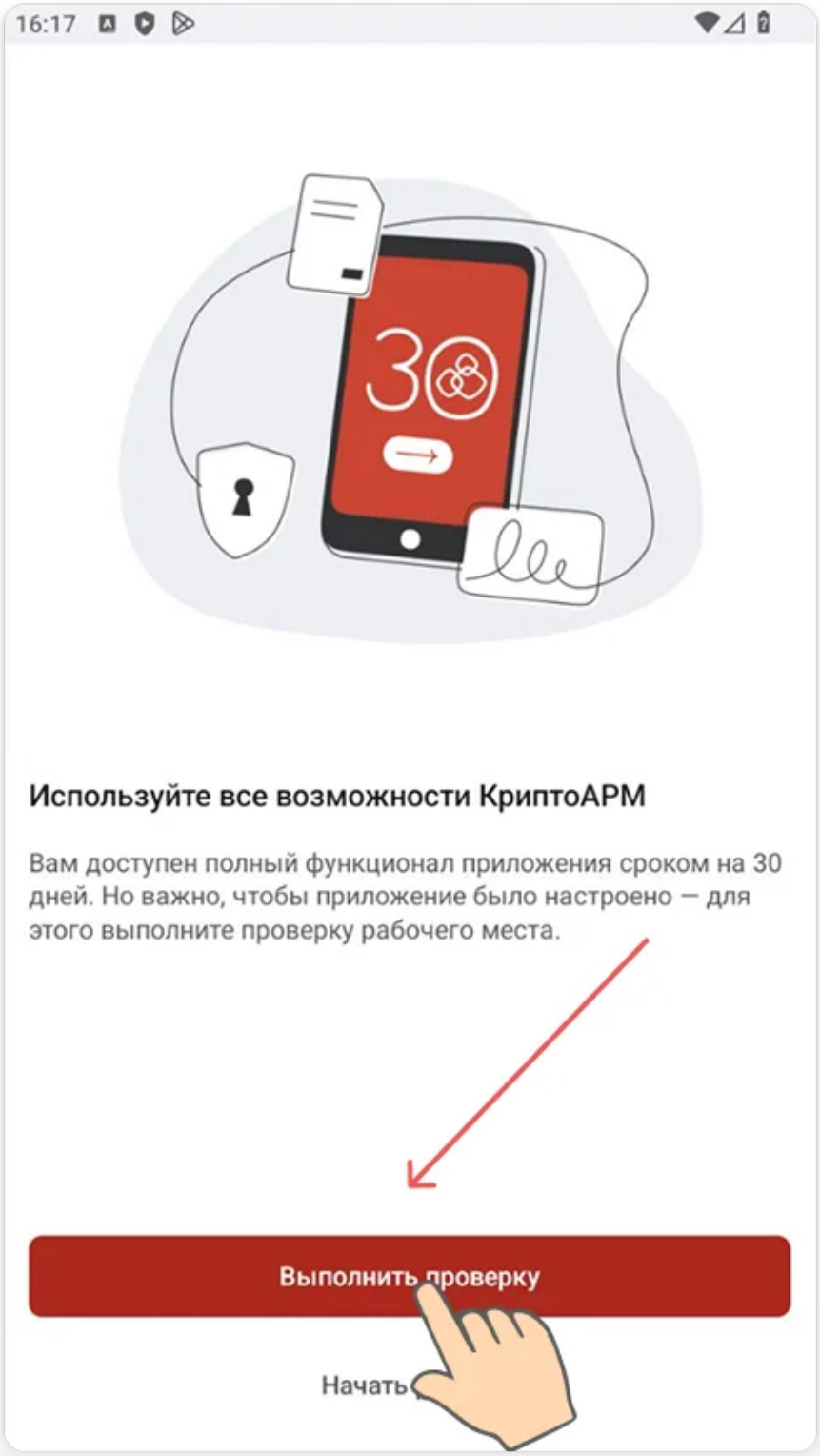
Проверка рабочего места — это инструмент, который помогает убедиться, что все компоненты для работы с электронной подписью установлены и готовы к использованию.

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.

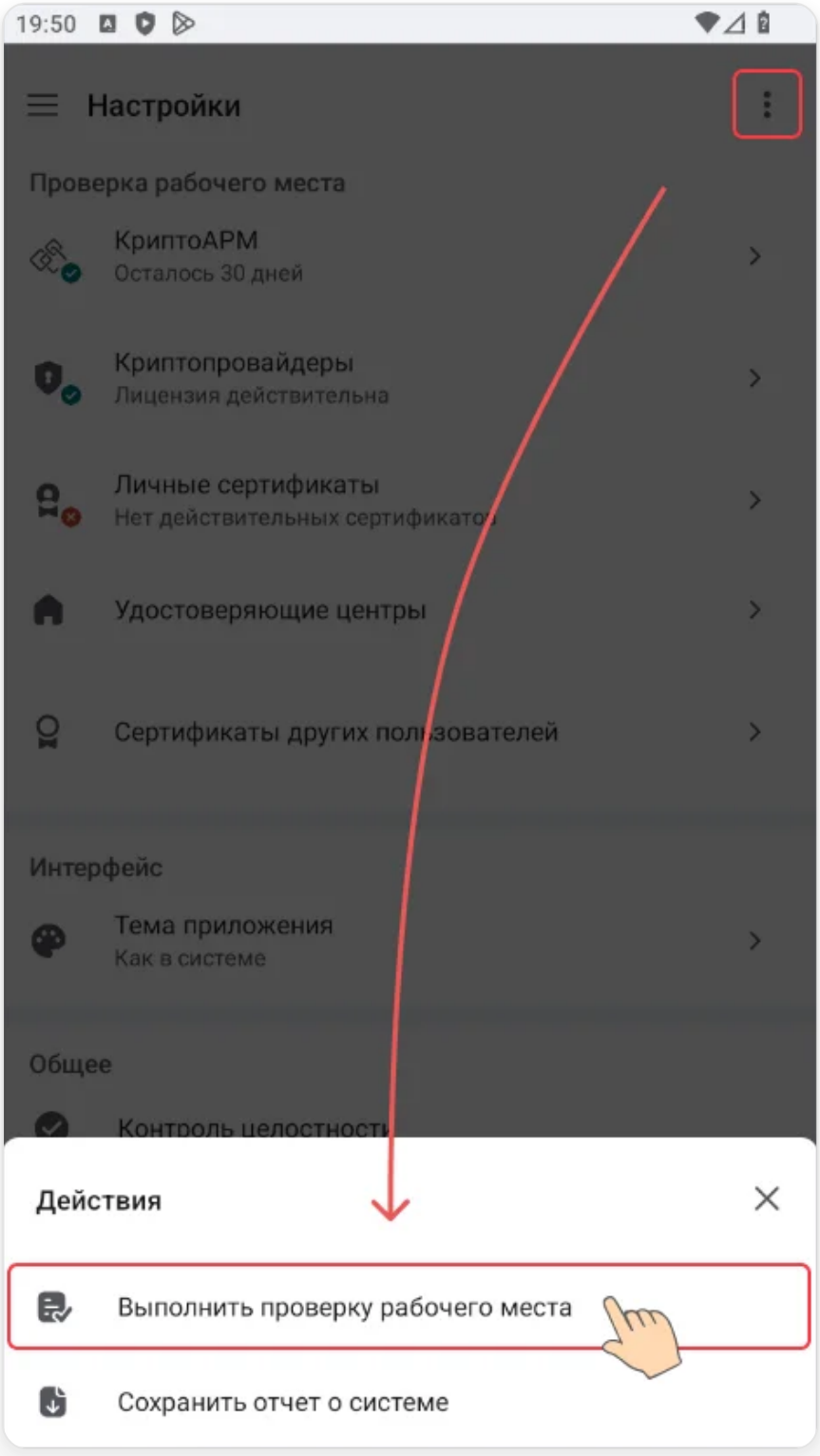


Ручной запуск

В дальнейшем проверку можно запустить самостоятельно:

1. Перейдите в раздел **Настройки**.
2. Нажмите кнопку **Еще** ⋮ и выберите пункт **Действия**.

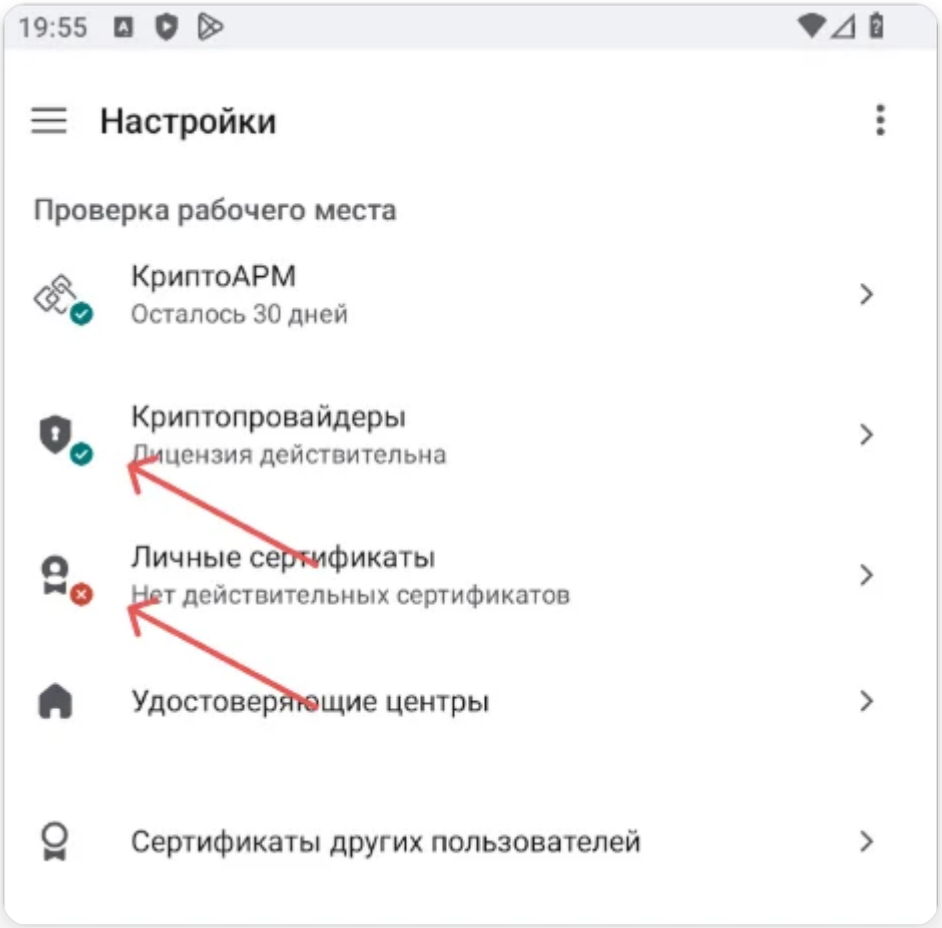
3. Выберите **Выполнить проверку рабочего места**.



Результаты проверки

Результаты проверки отображается в виде индикатора с пояснением:

1. ✅ Зеленый - компонент готов к работе
2. ❌ 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

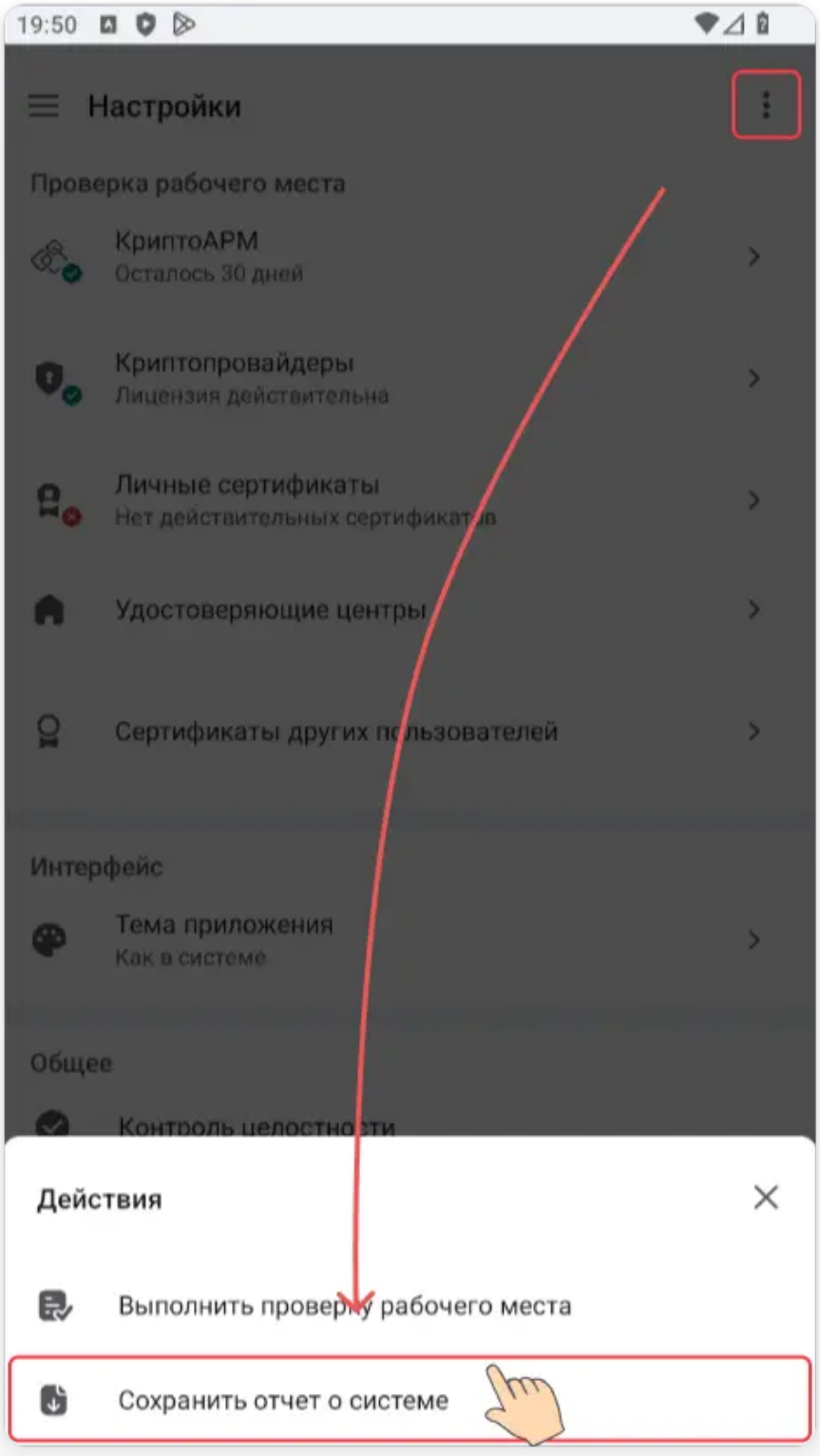
При необходимости можно сохранить подробный системный отчет.

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

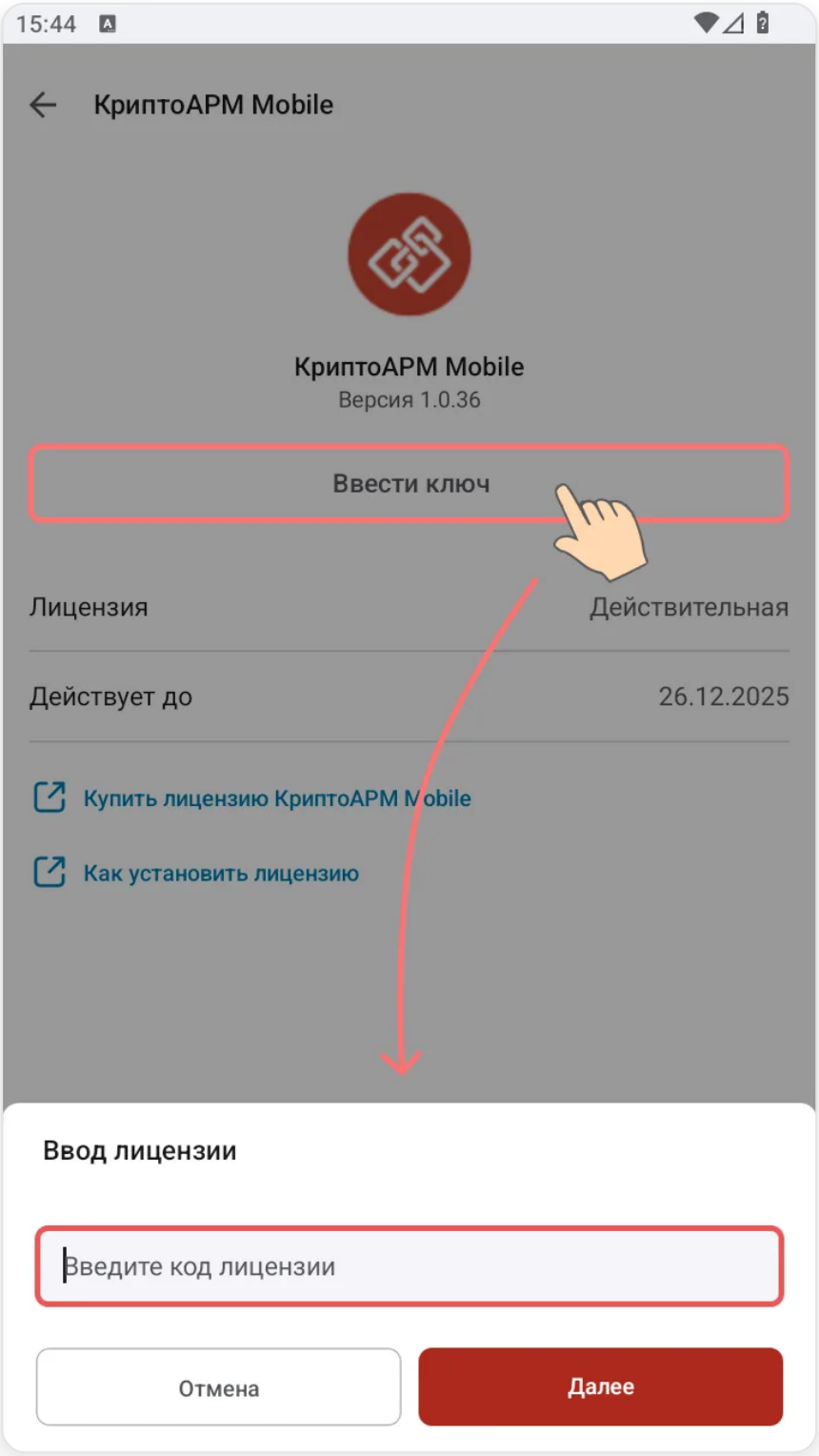
- Как установить личный сертификат
- Как импортировать корневой или промежуточный сертификат

Открыть статью на сайте

Установка лицензий

Установка лицензионного ключа КриптоАРМ

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

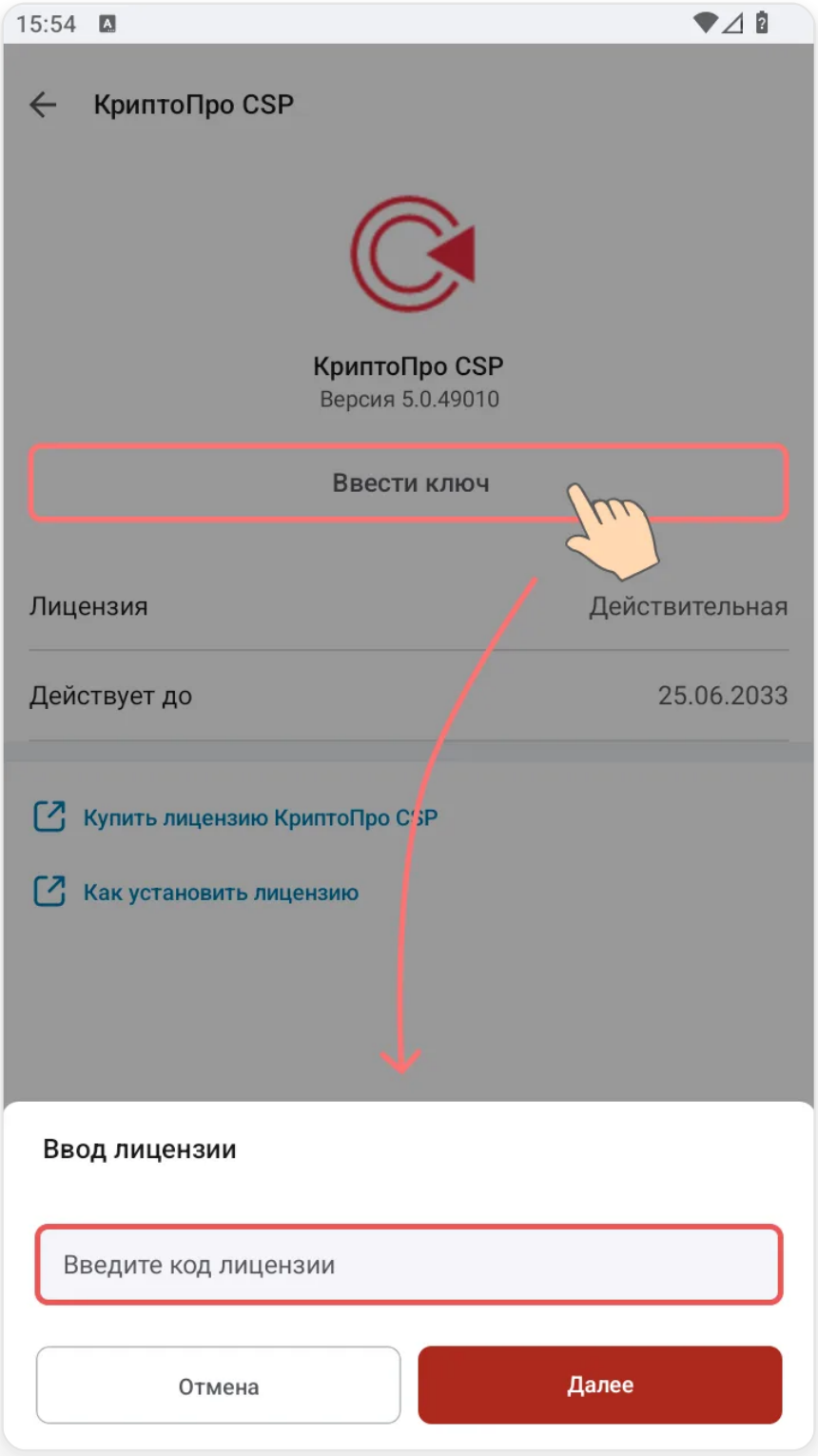


Дождитесь окончания активации лицензии.

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

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

Установка личного сертификата

- Перед началом работы
- Установка с защищённого носителя Рутокен
- Установка сертификата из файла .pfx
- Установка сертификата с помощью QR-кода
- Возможные ошибки

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 защищённого 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 неё.

Требования к устройству

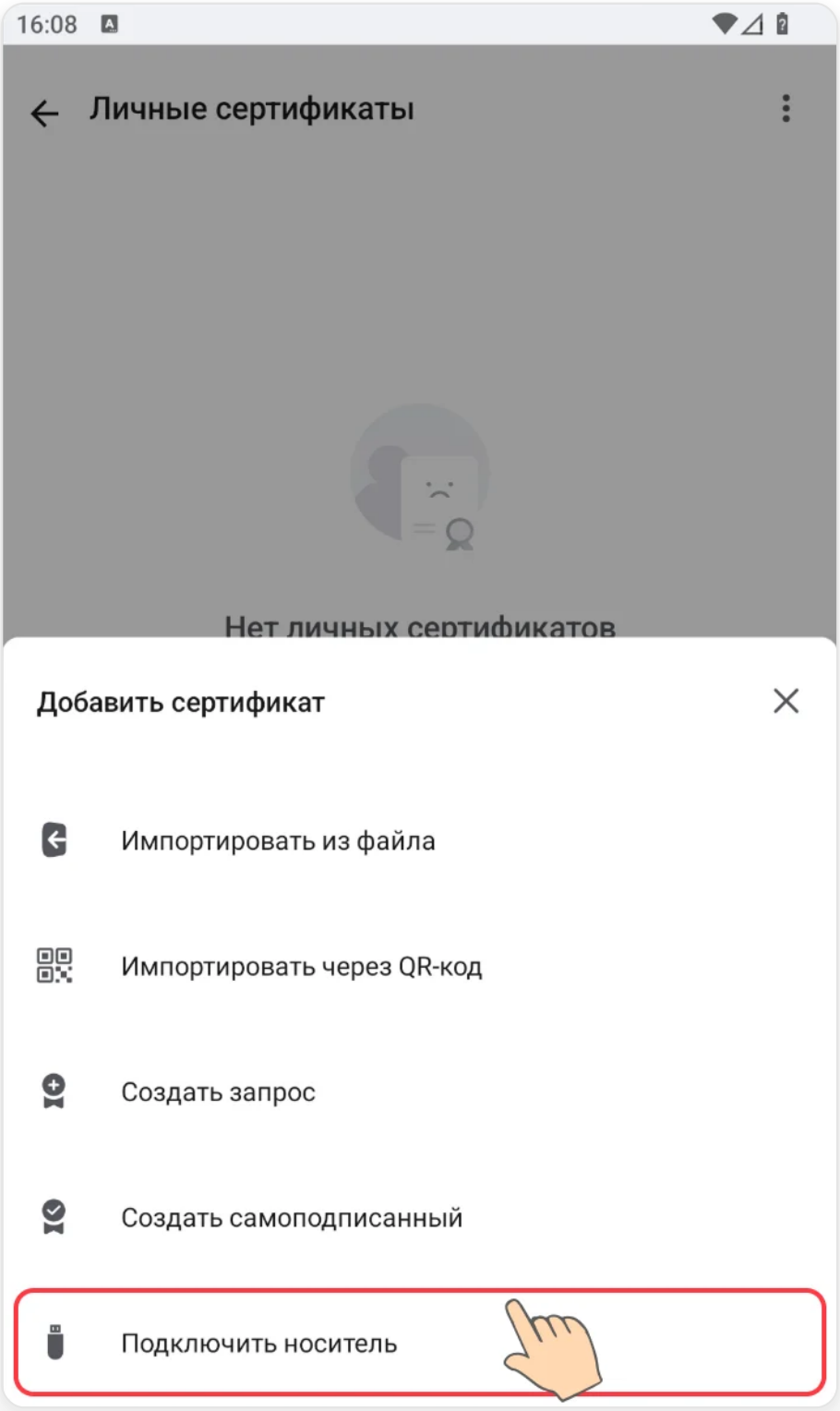
- Устройство должно поддерживать функцию **USB-OTG** для работы с USB-токенами.

- На некоторых моделях (Tecno, OPPO) OTG нужно включить в настройках. Подробнее — на Портале документации Рутокен.

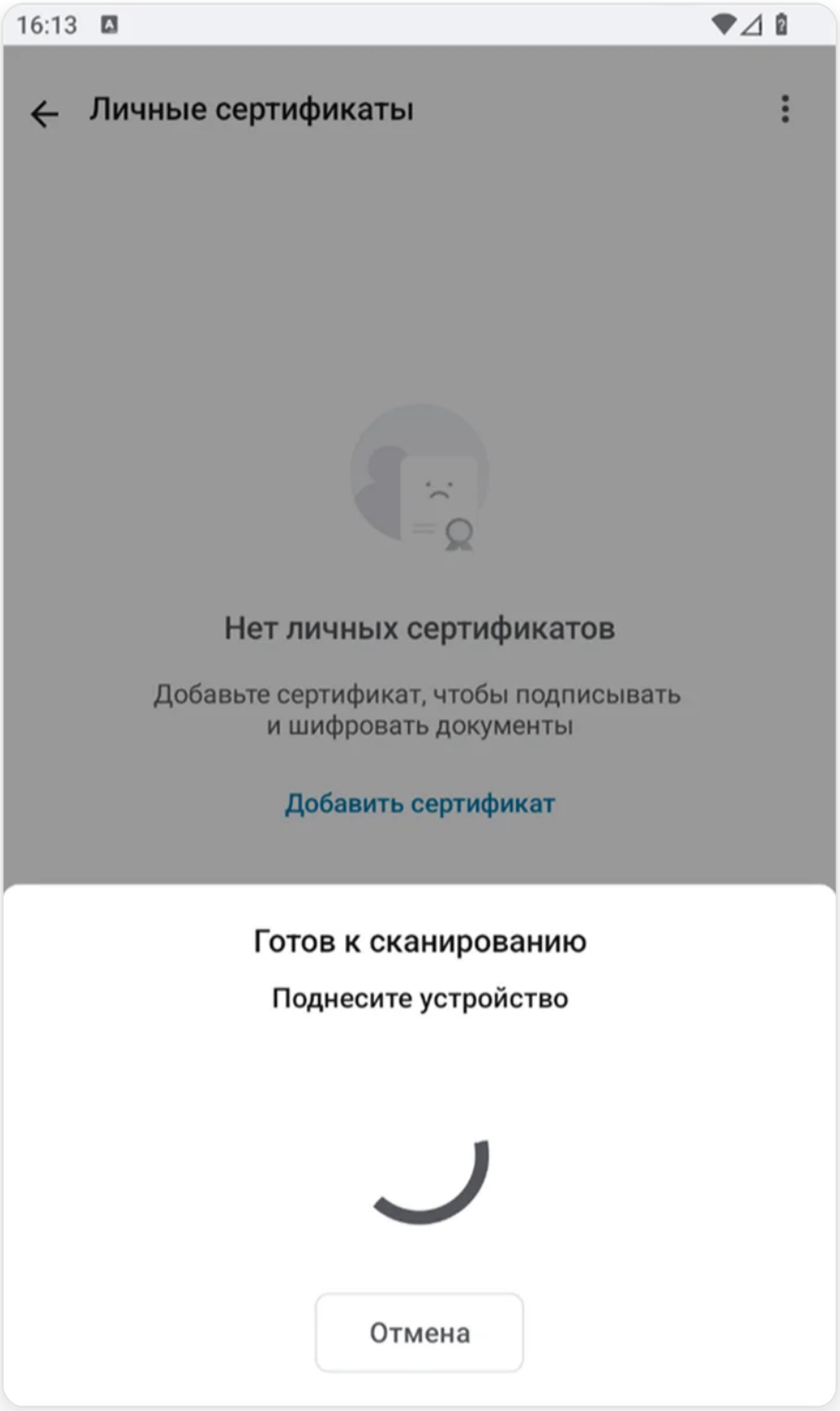
> 📌 **OTG** – это технология, связывающая два устройства без дополнительного USB-хоста, благодаря ей телефон может считывать данные со съемного носителя и передавать данные на другое устройство.

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.



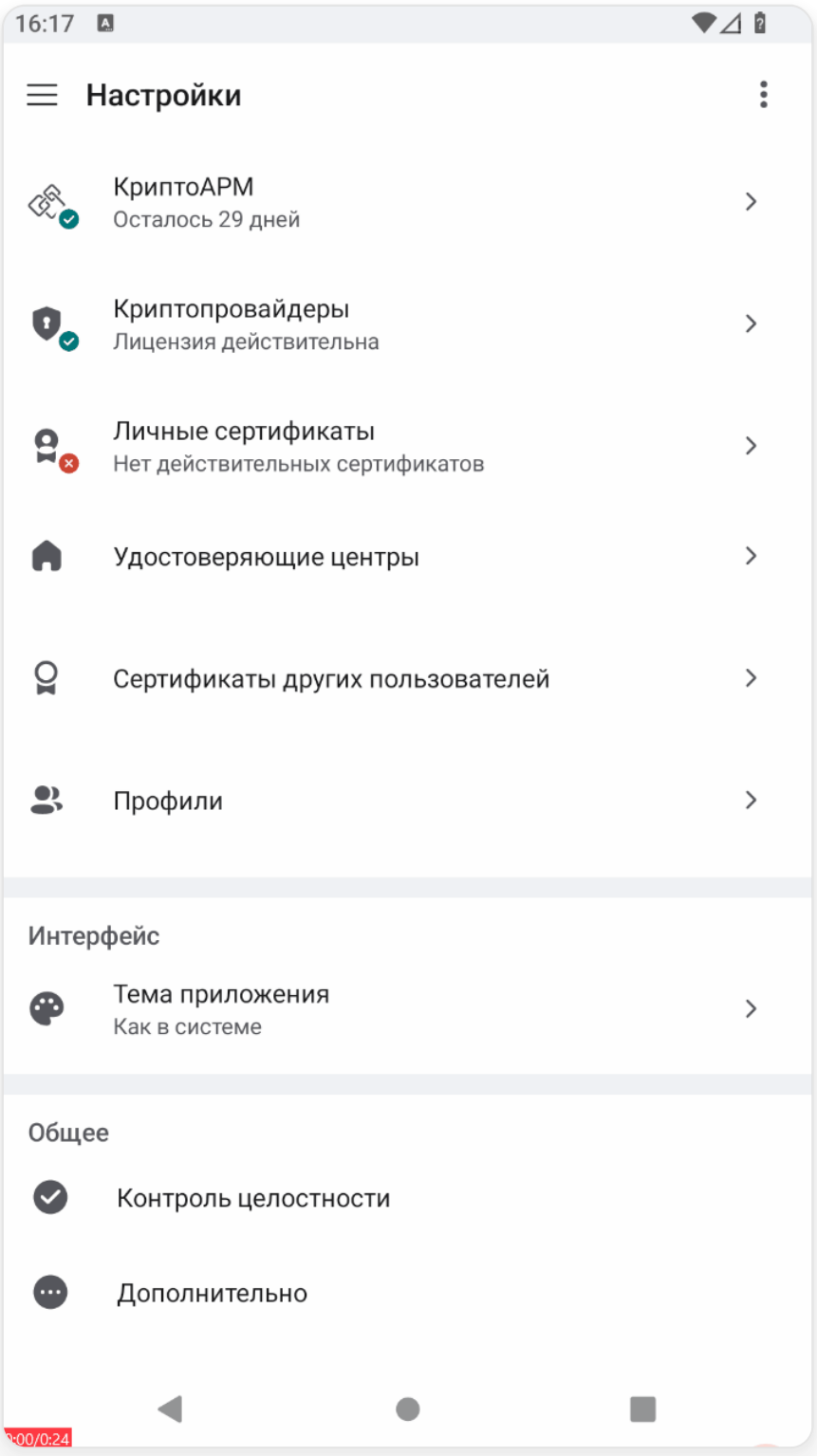
5. Подключите или поднесите носитель к устройству.
   - **Type-C** → вставьте напрямую,
   - **USB** → используйте переходник Type-C–USB,
   - **NFC-карта** → включите NFC и поднесите карту.
6. Откроется окно с обнаруженными сертификатами.

7. Выберите нужный сертификат из списка.
8. Нажмите **Установить**.

Установка сертификата из файла .pfx

> 💡 Перед установкой убедитесь, что файл `.pfx` сохранён 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.

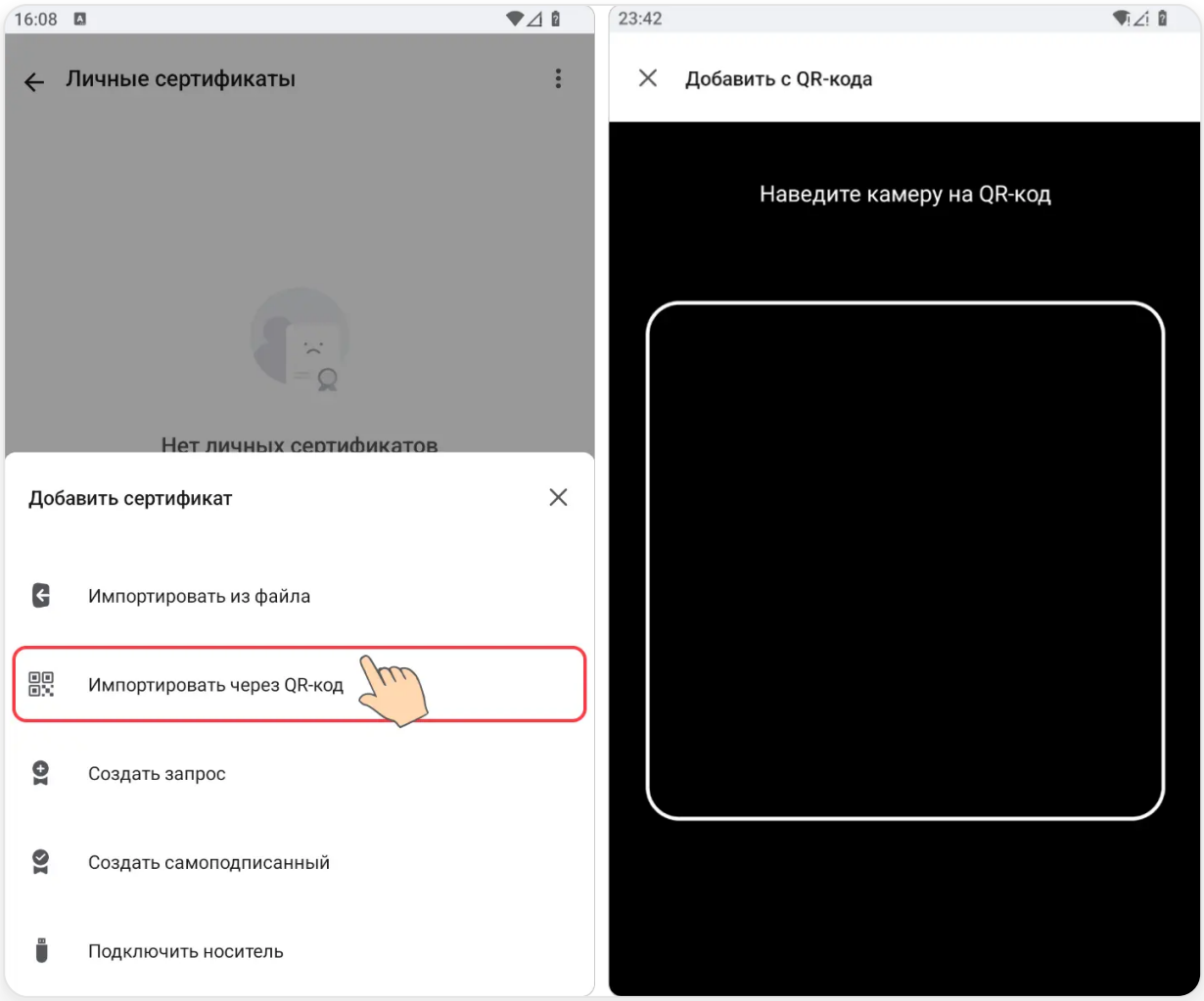


После успешного импорта сертификат отобразится в списке и появится сообщение **Сертификат успешно добавлен**.

Установка сертификата с помощью QR-кода

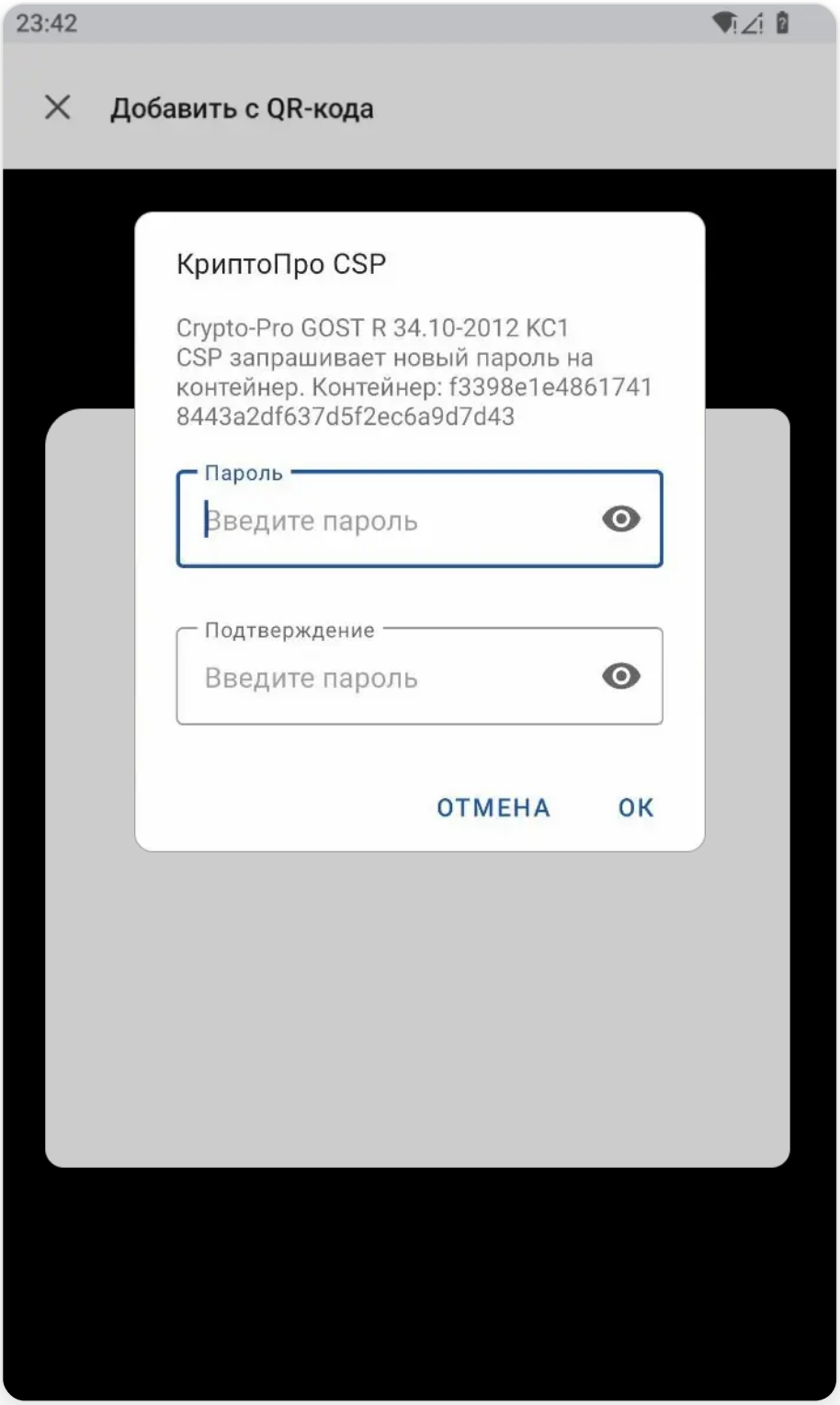
> 💡 Как создать QR-код с помощью КриптоПро CSP смотрите в нашей видеоинструкции.
>
> 🚨 **Условие**: Сертификат подписи должен быть экспортируемым, иначе ключ не получится перенести.

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

Создание самоподписанного сертификата

- Что такое самоподписанный сертификат?
- Как создать самоподписанный сертификат

Что такое самоподписанный сертификат?

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

Особенности

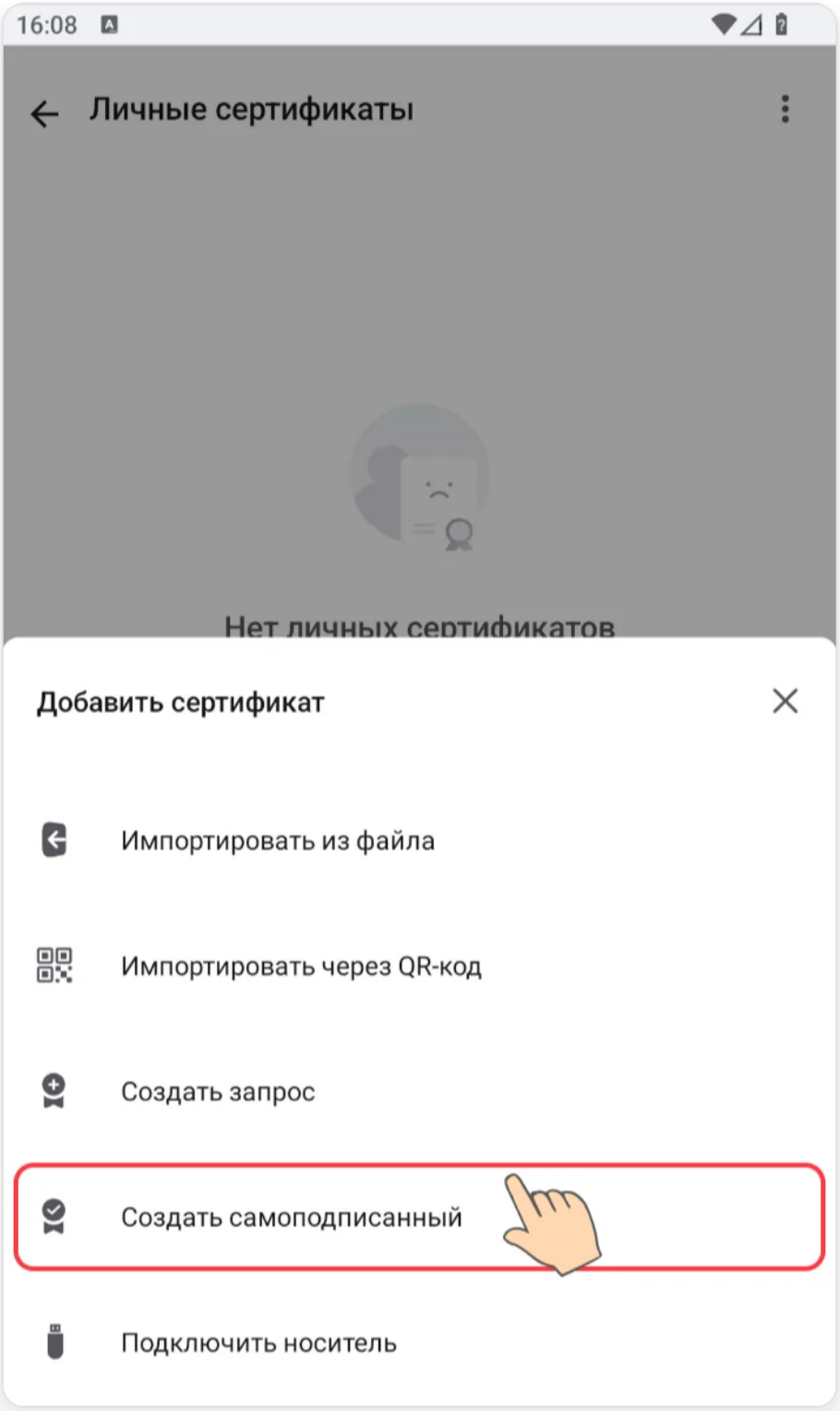
- Совмещает функции личного сертификата и корневого сертификата.
- Подходит только для личного или внутреннего использования, например, для тестирования или обмена документами внутри доверенной группы.

❌ Не подходит для официального документооборота:

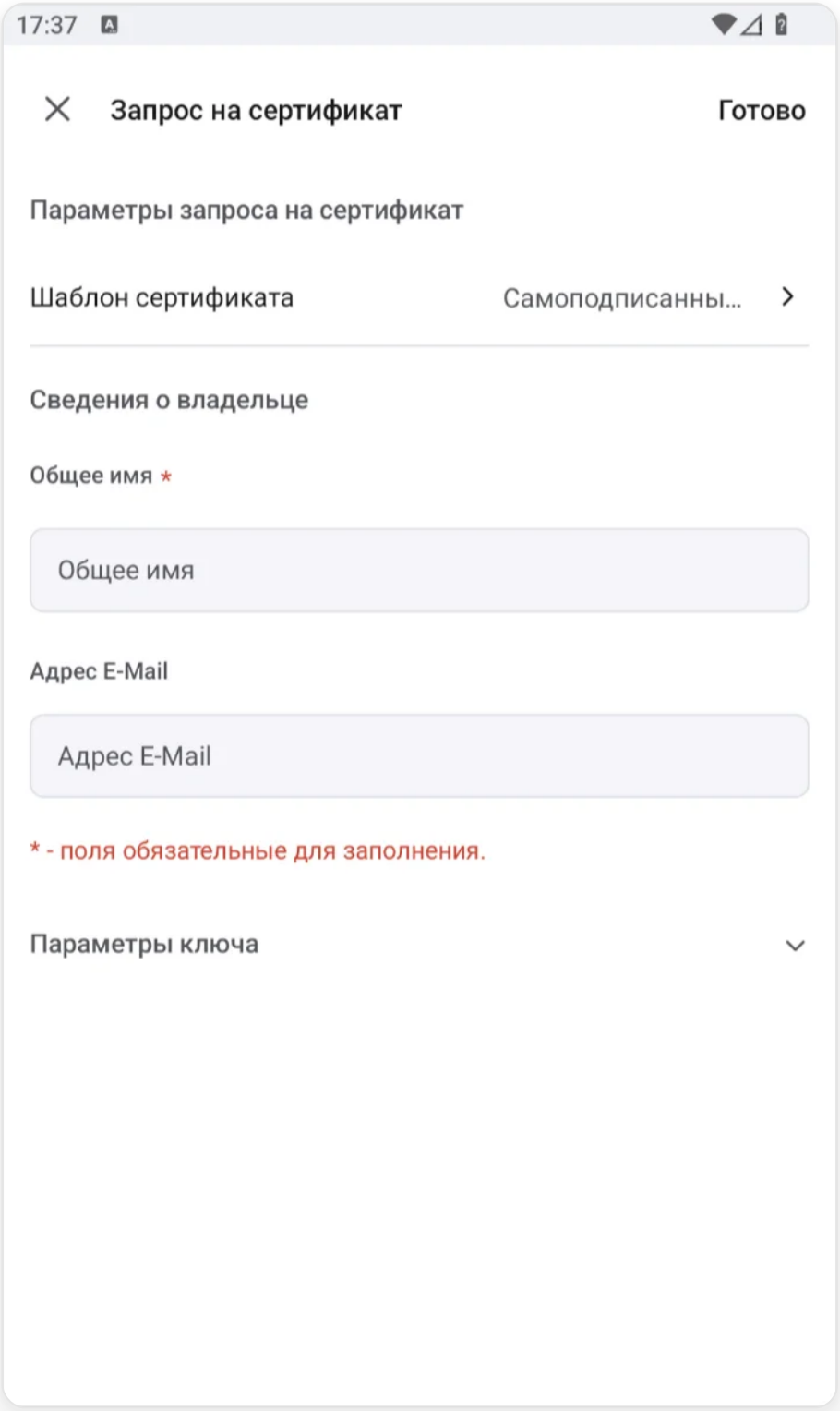
- **Нет независимой проверки** — сертификат создан вами, и сторонние организации не могут проверить его подлинность.
- **Нет юридической силы** — государственные порталы, банки и официальные системы требуют сертификаты, выданные доверенными Удостоверяющими центрами.
- **Риск подделки** — любой может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

Как создать самоподписанный сертификат

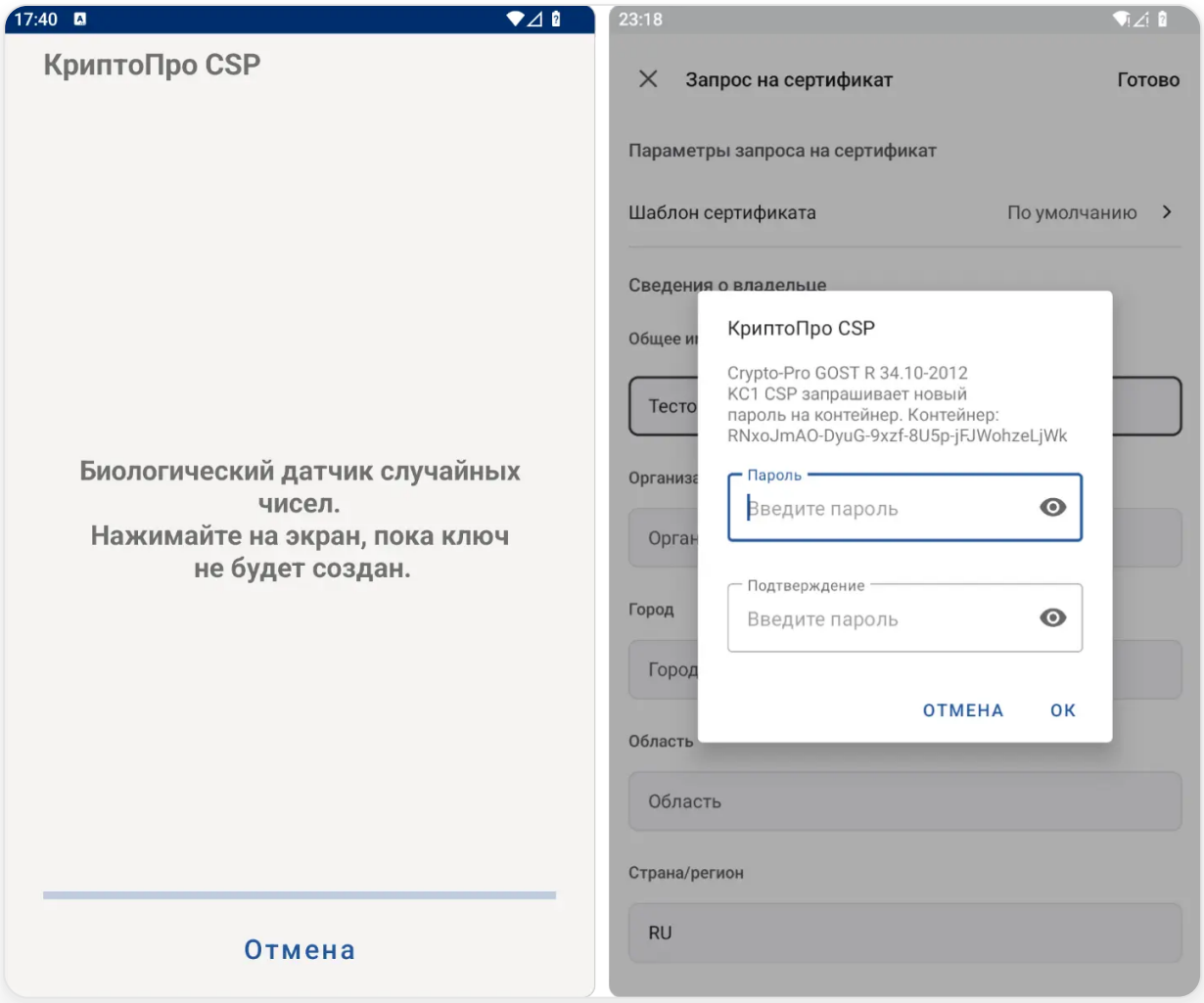
1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий **Добавить сертификат** одним из способов:
    - Нажмите на кнопку **Добавить сертификат** в центре окна, если в приложении отсутствуют личные сертификаты.
    - Вызовите меню по кнопке **Еще** ⋮ и выберите действие **Добавить сертификат**.
3. Выберите действие **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 на контейнер. Поле можно оставить пустым.



После этого сертификат будет создан и установлен.

> ⚠️ **Важно:** чтобы статус самоподписанного сертификата определялся правильно, 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

Создание запроса

- 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

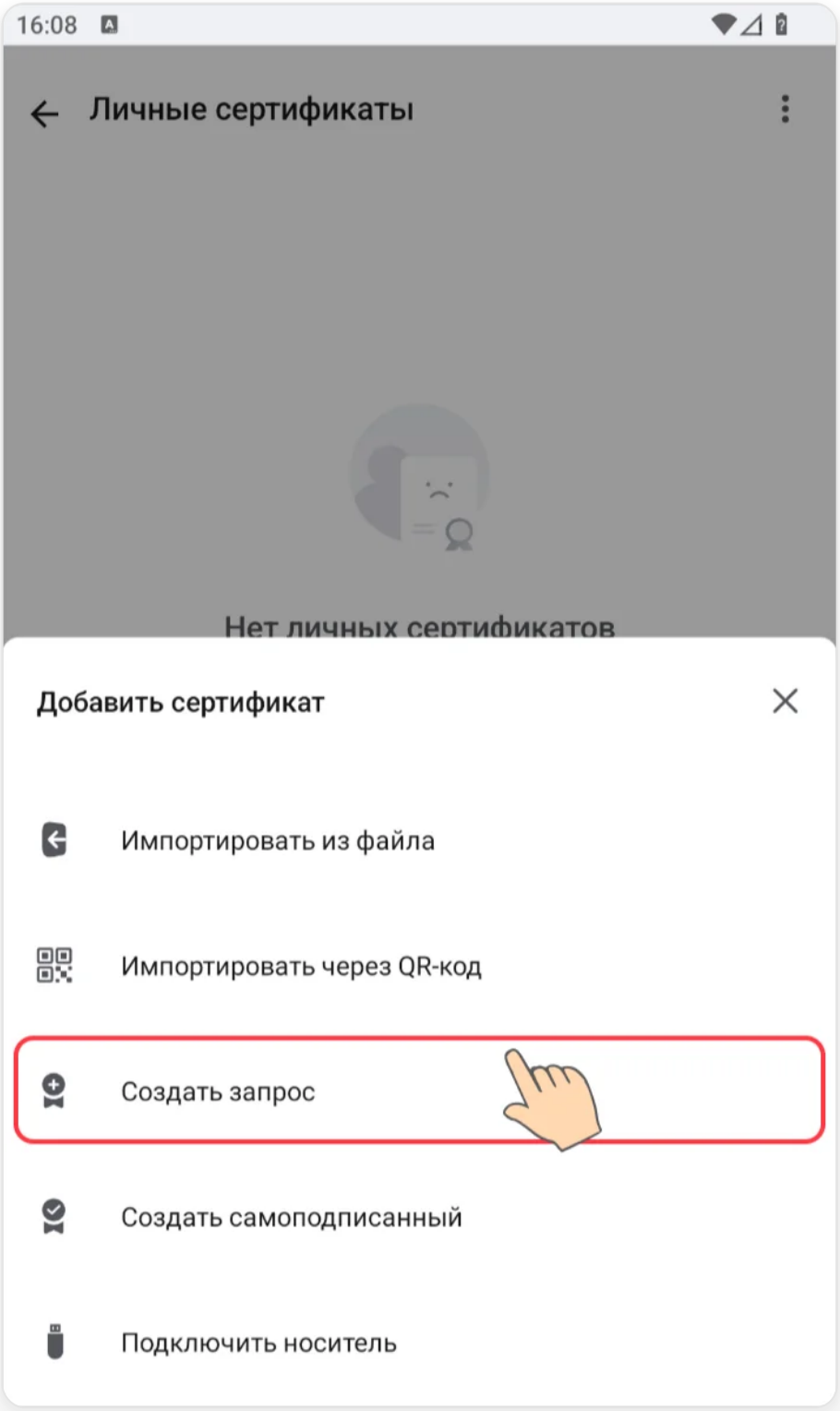
1. **Сведения о владельце**
    - ФИО, должность, организация и контактная информация.
    - Эти данные будут указаны в самом сертификате.
2. **Параметры ключевой пары**
    - Тип и длина ключа,
    - Назначение ключа,
    - Возможность экспорта ключа для переноса на другие устройства.
3. **Технические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

Как используется запрос

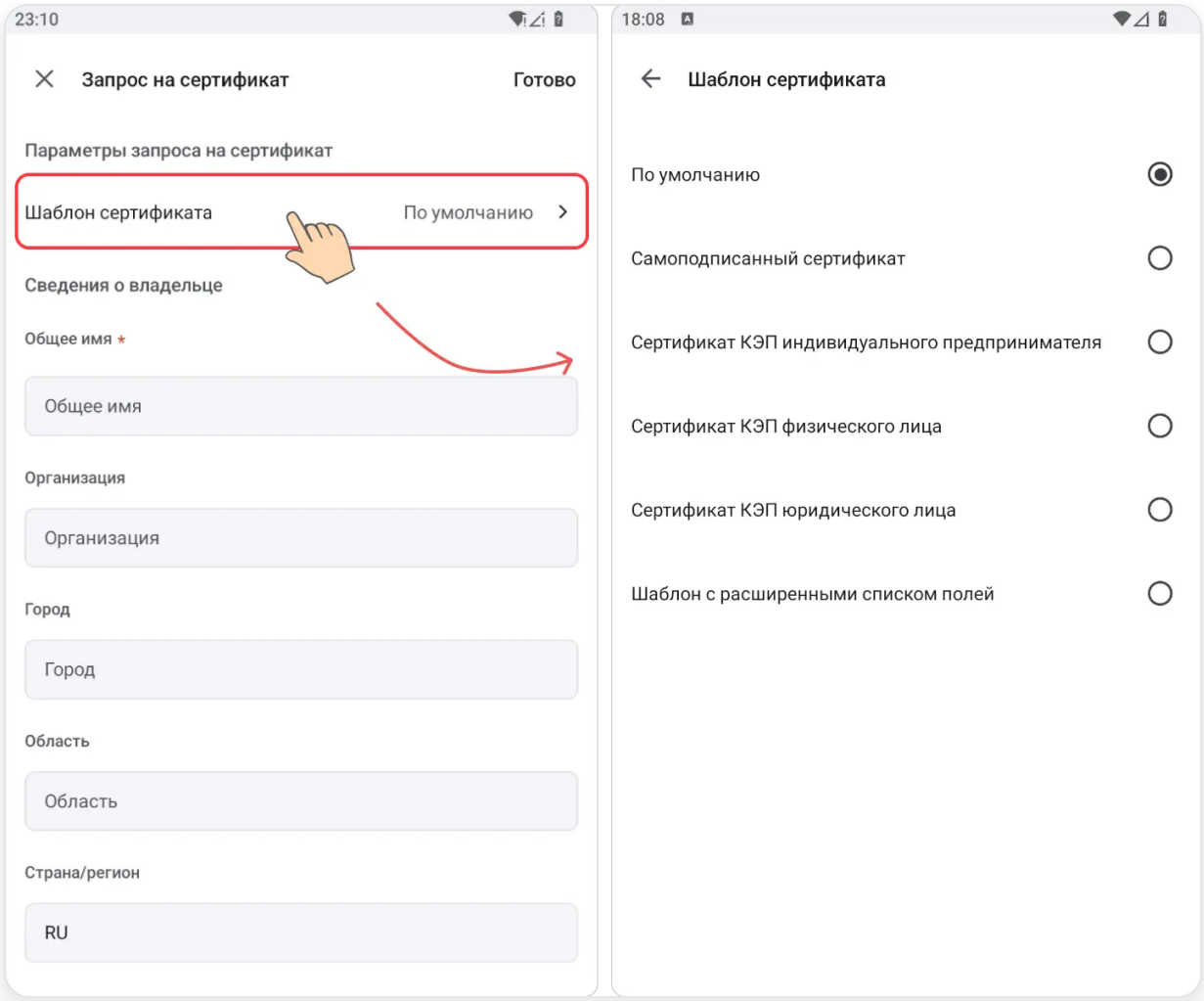
- После создания файла запроса его отправляют в Удостоверяющий центр.
- Удостоверяющий центр проверяет предоставленные данные и создаёт сертификат, который соответствует указанным параметрам.
- После получения сертификата его импортируют в приложение, и он становится готовым для подписания и шифрования документов.

Как создать запрос на сертификат

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий **Добавить сертификат** одним из способов:
   - Нажмите 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 **Создать запрос**.



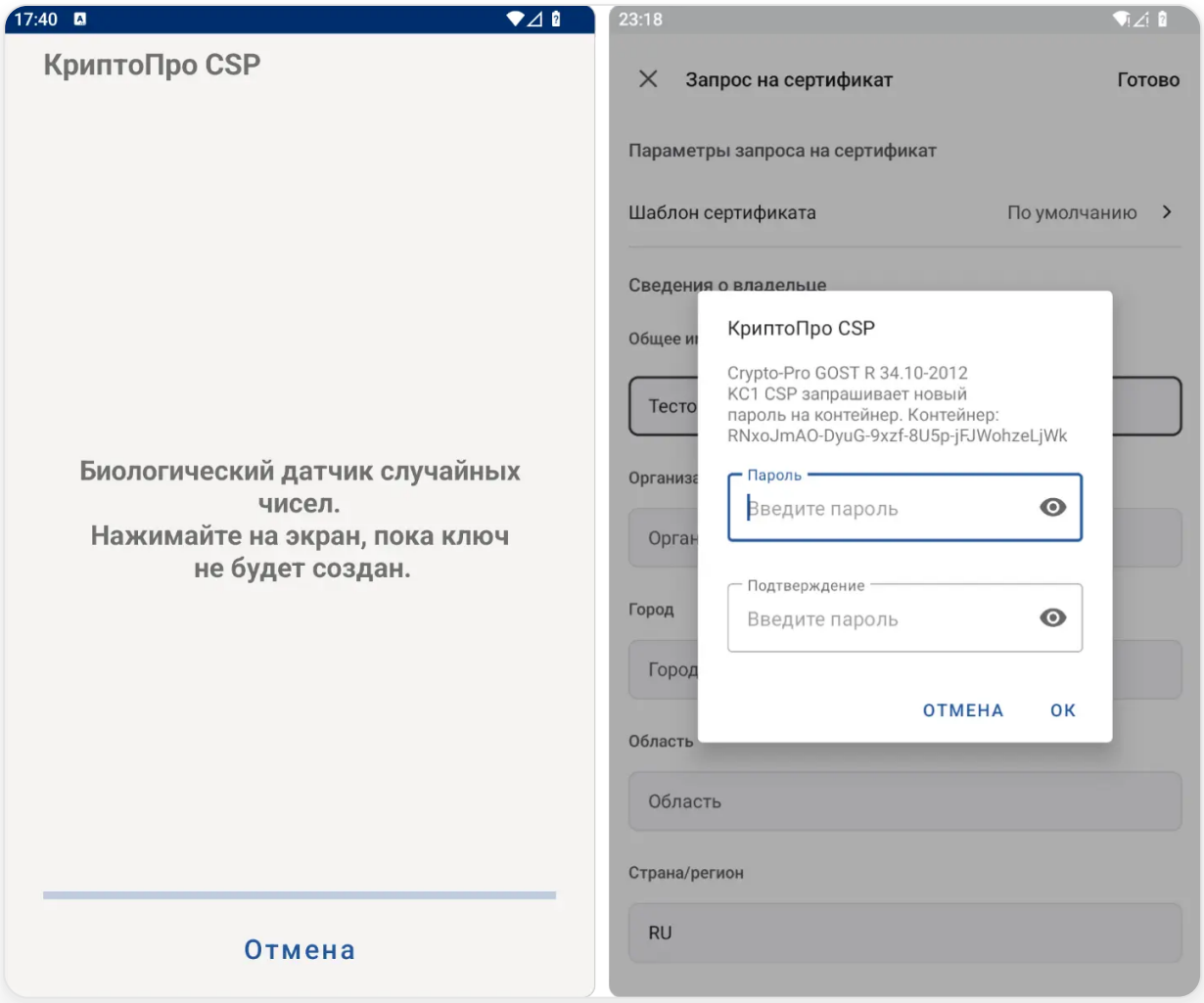
4. Откроется форма создания запроса.



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 перечислен 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 на контейнер. Поле можно оставить пустым.



На основе указанных данных будет сформирован запрос на сертификат.

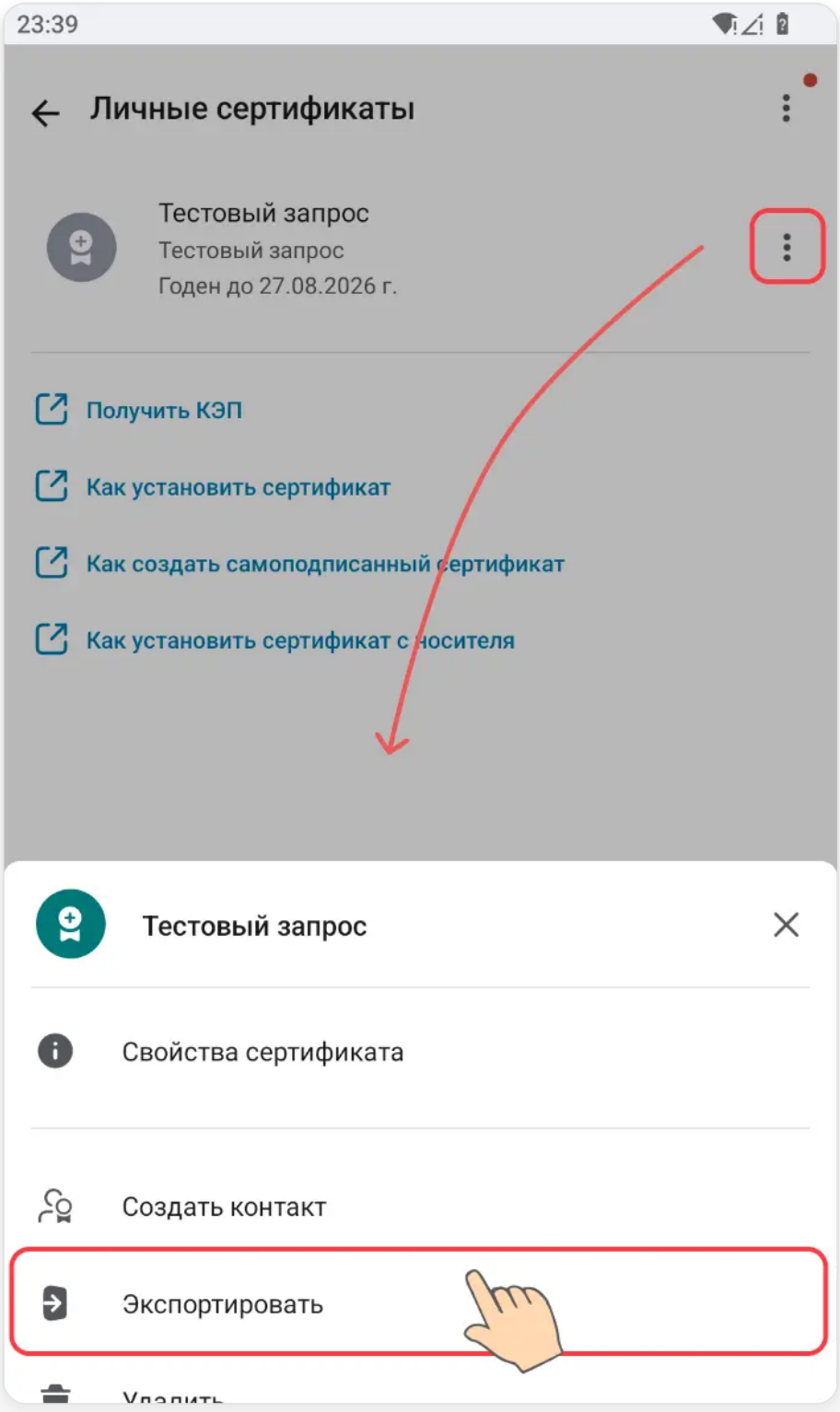
Дальнейшие действия после создания запроса

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** , размещенной на панели с запросом.
3. Выберите действие **Экспортировать**.



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

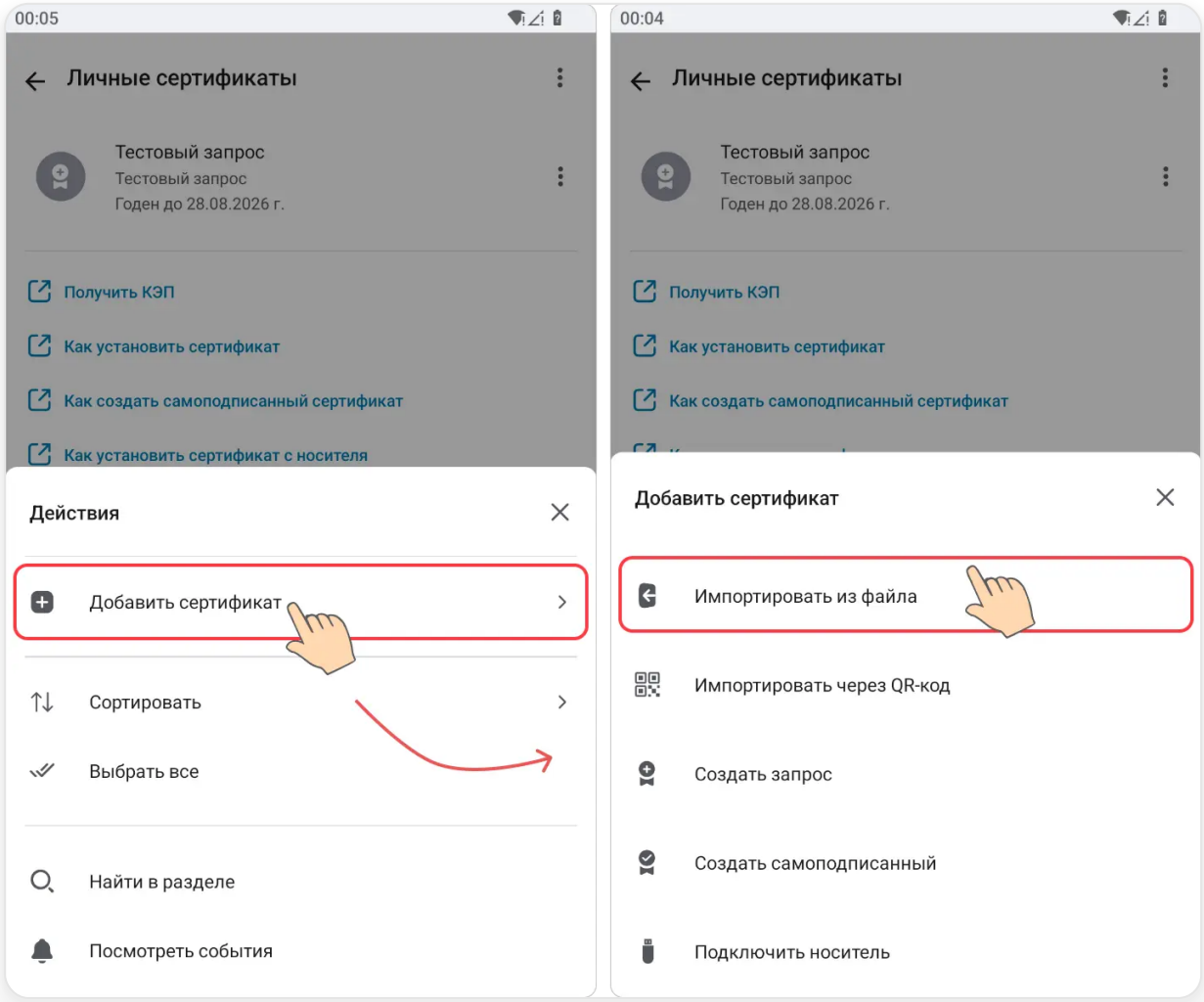
После этих действий файл запроса готов для передачи в УЦ.

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 готов к использованию.

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

Описание настроек запроса

Параметры ключа

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Алгоритм	`ГОСТ Р 34.10-2012 256 бит`	Алгоритм подписи	- `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 сертификат вместе с закрытым ключом 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)		✅	✅

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

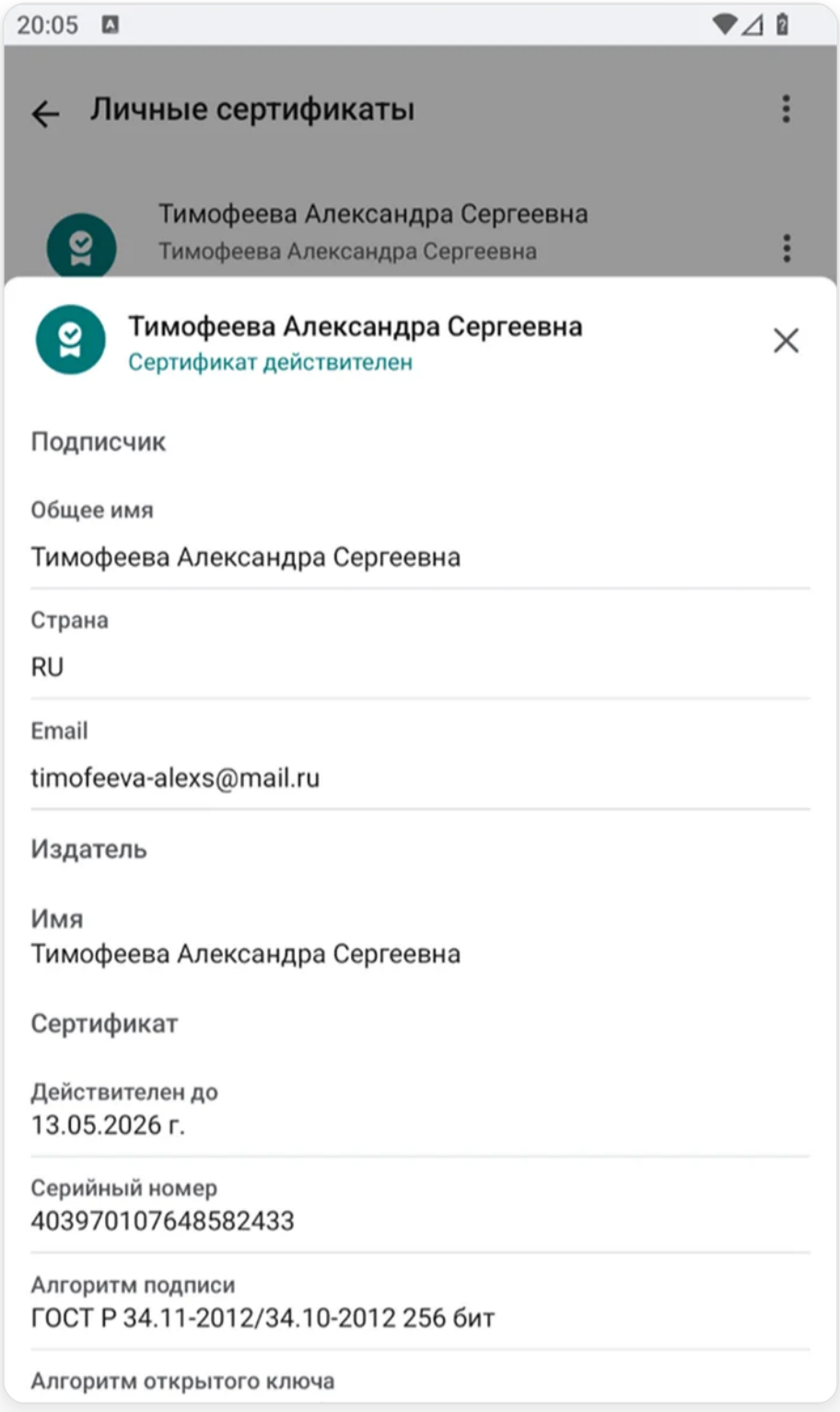
Открыть статью на сайте

Просмотр и проверка статуса сертификата

- Просмотр сведений о сертификате
- Проверка статуса сертификата

Просмотр сведений о сертификате

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



Проверка статуса сертификата

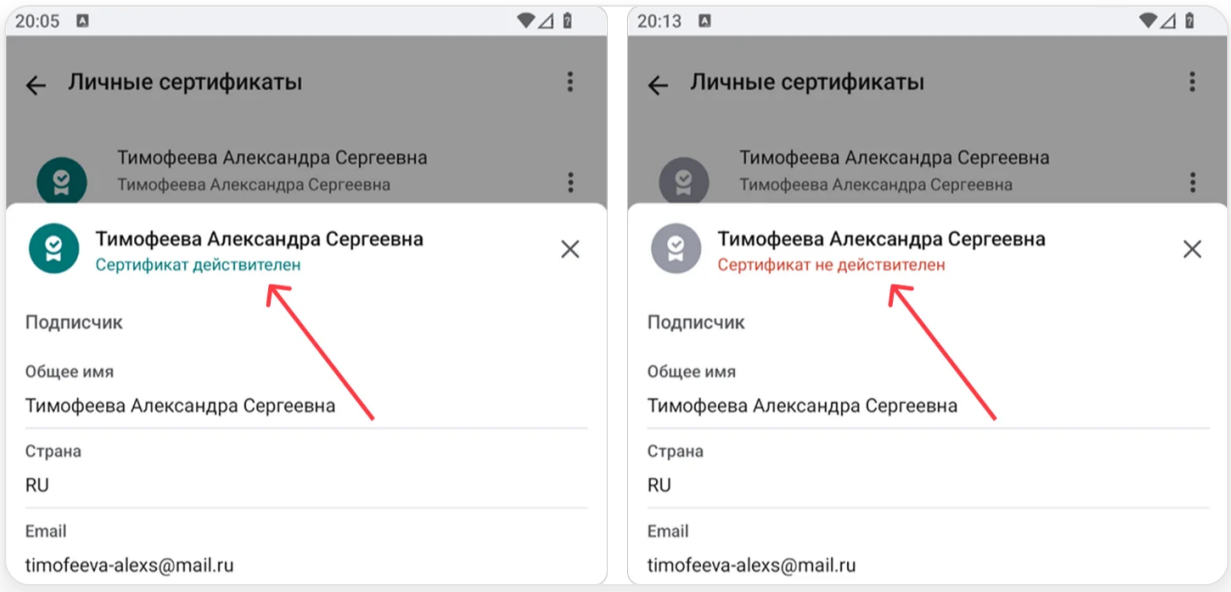
Статус сертификата проверяется по следующим параметрам:

Критерий проверки	Что означает	Почему это важно
Срок действия	Проверка временного периода валидности	Гарантирует, что сертификат не просрочен
Подпись УЦ	Верификация цифровой подписи выпустившего центра	Подтверждает подлинность сертификата
Цепочка доверия	Построение полной цепочки до корневого сертификата	Обеспечивает доверие к сертификату
Статус отзыва	Проверка по актуальным спискам CRL	Исключает использование отозванных сертификатов

Возможные статусы сертификата

В приложении возможны 2 статуса сертификата:

1. **Действительный** (● зелёный индикатор) - когда:
    - Подпись Удостоверяющего центра корректна.
    - Срок действия сертификата не истек.
    - Сертификат используется для тех целей, для которых был создан.
    - Сертификат не отозван и его действие не приостановлено.
2. **Недействительный** (● серый индикатор) - если не выполняется хотя бы одно условие.



Распространенные проблемы с сертификатами

Причины недействительности сертификатов:

Проблема	Можно исправить?	Что делать
Срок действия истёк	❌ Нет	Оформите новый сертификат
Сертификат отозван	❌ Нет	Оформите новый сертификат
Неполная цепочка доверия	✅ Да	Установите недостающие корневые/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

Экспорт личного сертификата

- Основные принципы экспорта
- Экспорт без закрытого ключа
- Экспорт с закрытым ключом

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.

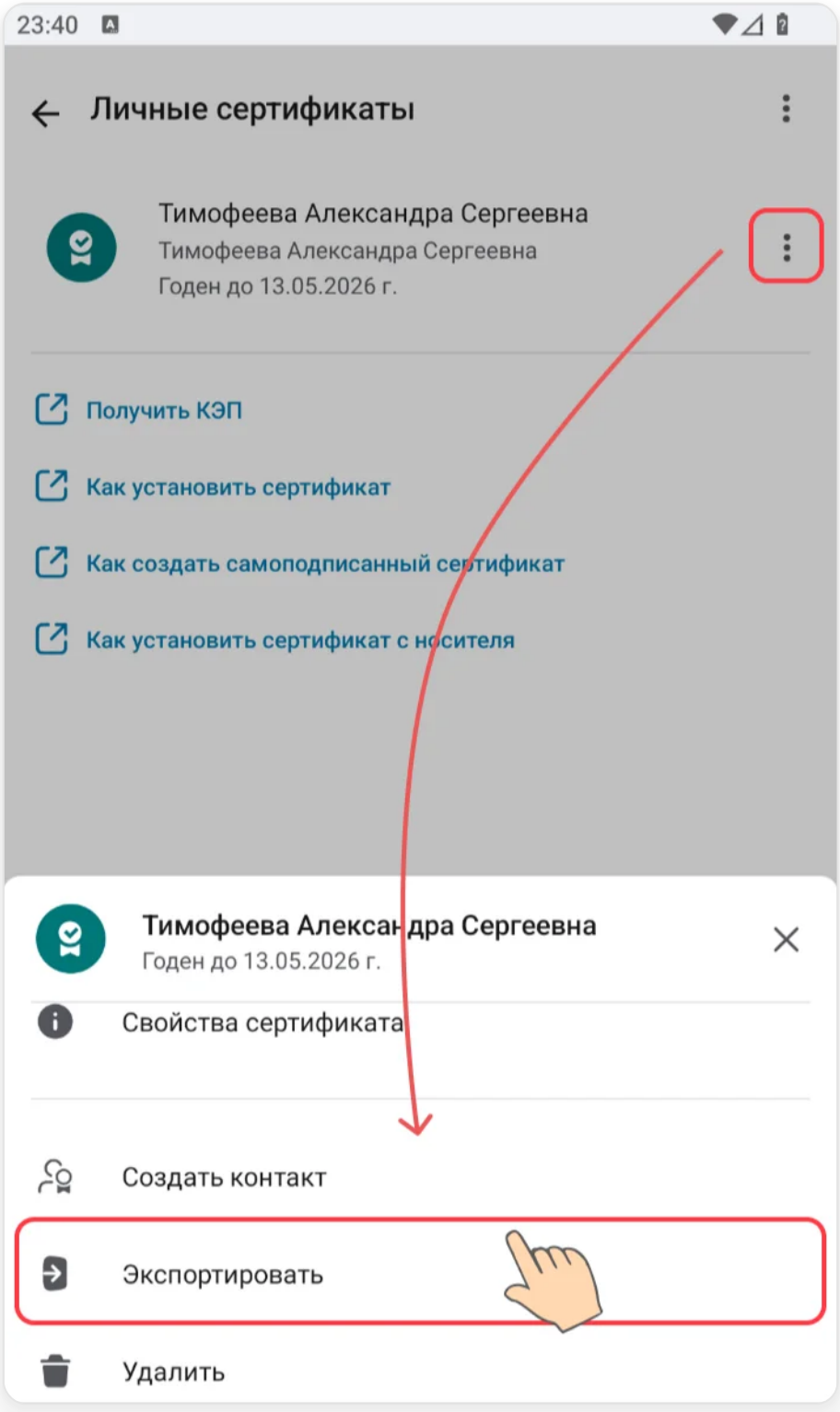
Сравнение способов экспорта

Параметр	Без закрытого ключа	С закрытым ключом
Назначение	Передача сертификата другим людям или системам	Перенос сертификата на другое устройство, резервное копирование
Можно использовать для	Проверки подписи, шифрования данных для вас	Подписи и расшифровки на другом устройстве
Безопасность		

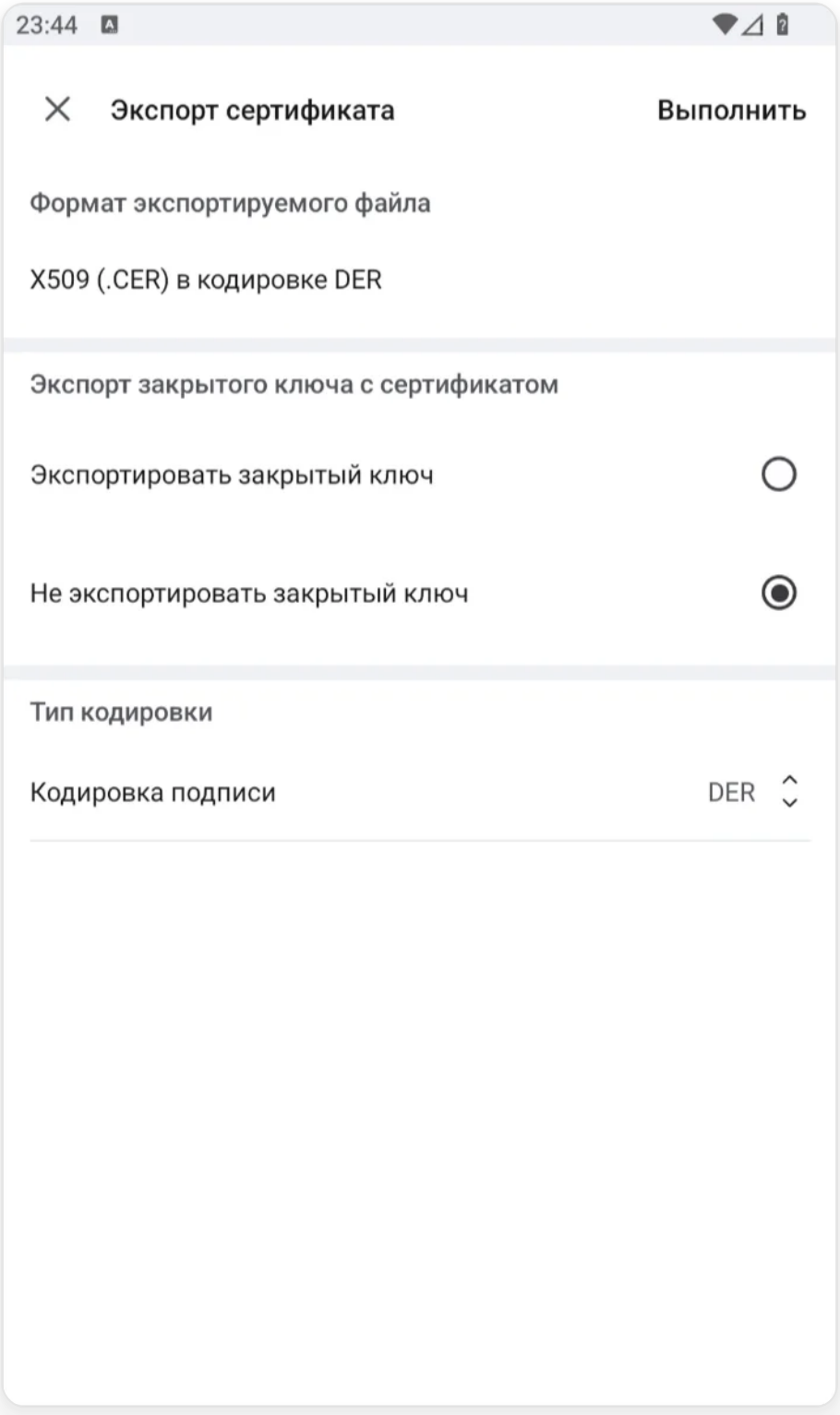
Параметр	Без закрытого ключа	С закрытым ключом
	Безопасно, т.к. закрытый ключ остаётся у вас	Опасно при неправильном хранении: возможна компрометация ключа
Кому можно передавать	Любому получателю, кому нужно знать ваш открытый ключ	Только самому себе (для переноса) или доверенным лицам под вашу ответственность
Формат файла	`.cer`	`.pfx` (пароль обязателен)

Экспорт без закрытого ключа

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



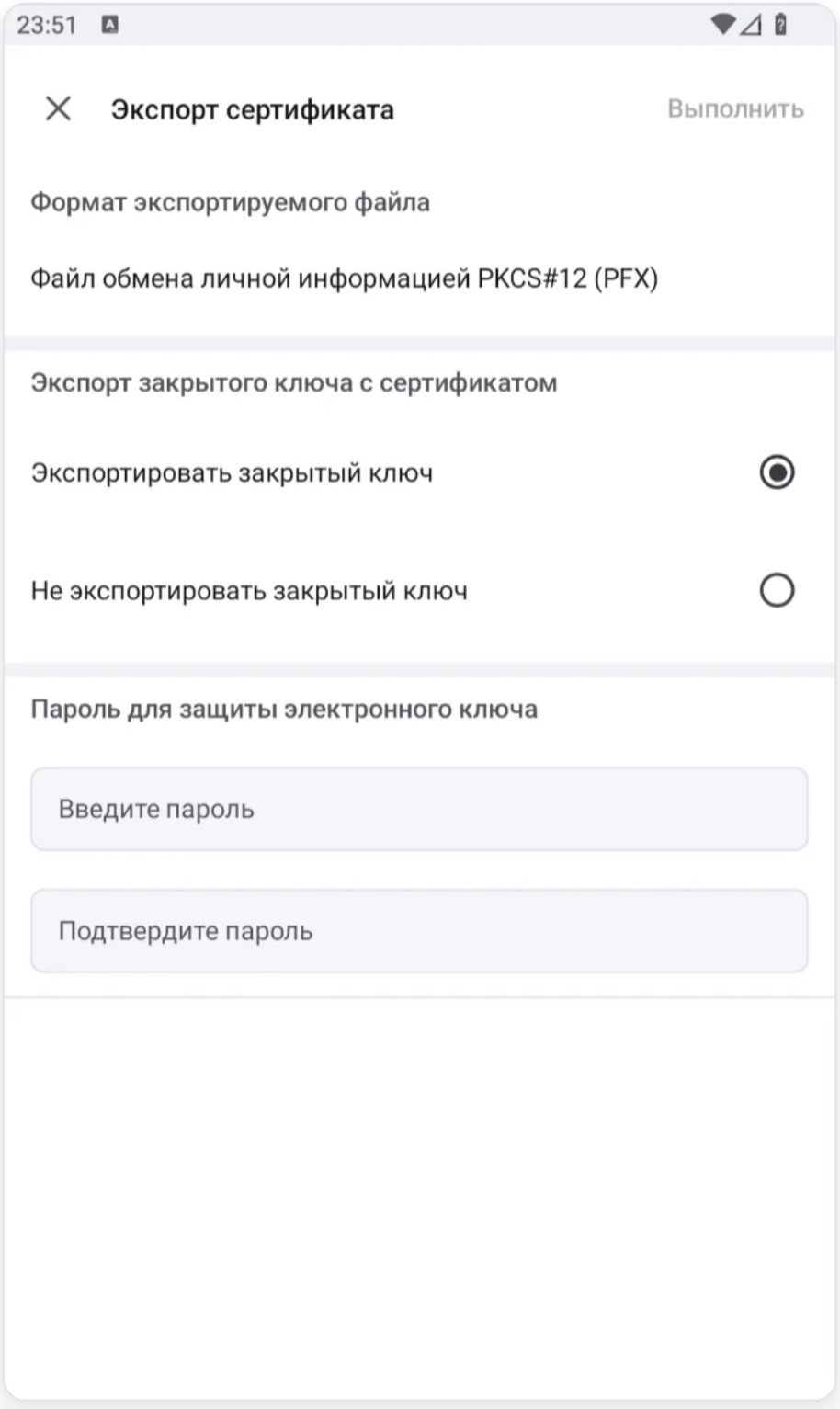
4. Откроется окно **Экспорт сертификата**:
    - Выберите опцию **Не экспортировать закрытый ключ**.
    - Укажите **Тип кодировки**.



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

Экспорт с закрытым ключом

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Вызовите меню действий по кнопке **Еще** , размещенной на панели 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 на **Выполнить**.
6. В появившемся окне укажите место для сохранения сертификата или выберите приложение для 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

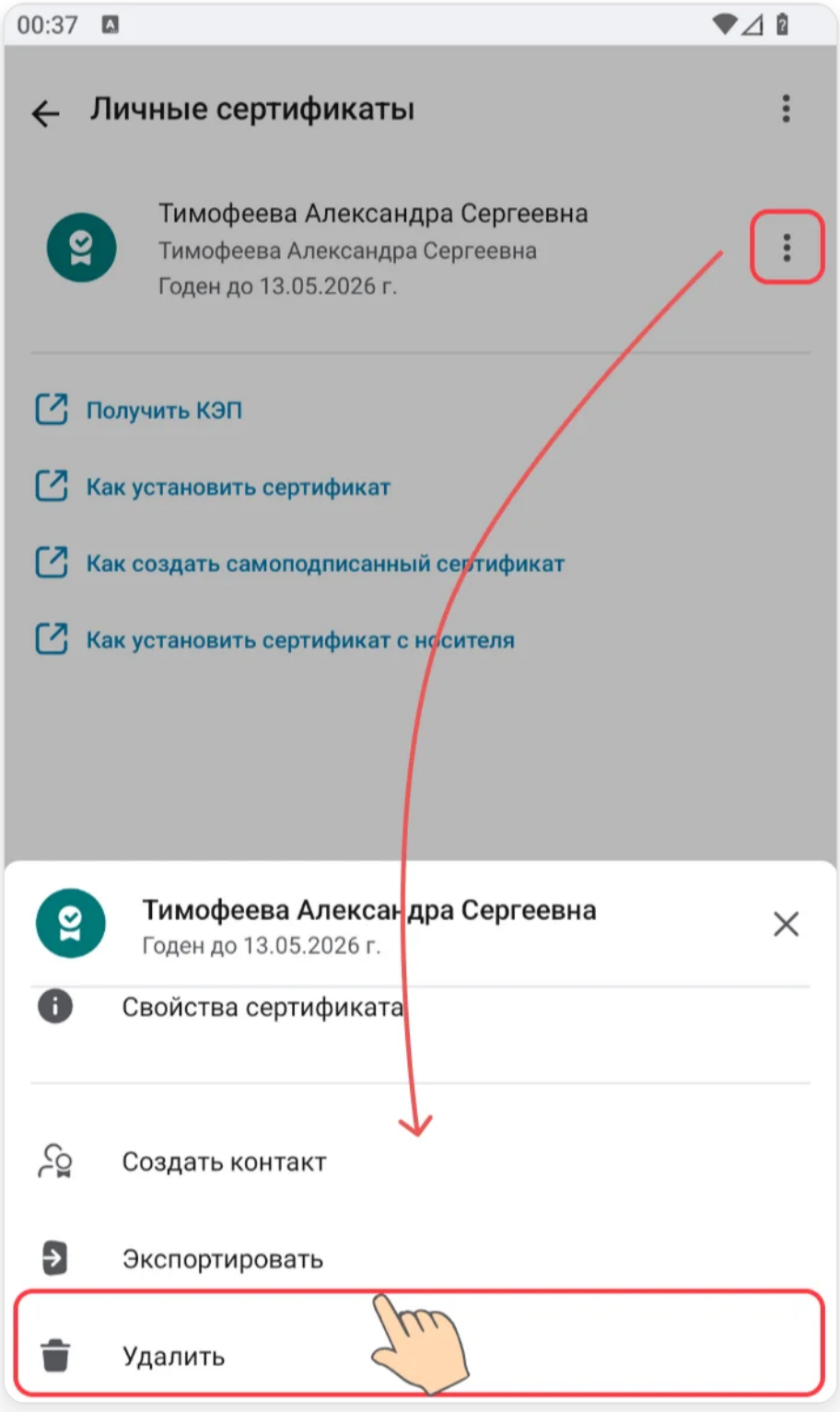
Удаление сертификата

> 💡 **Совет**: Если срок действия вашего сертификата истёк или вы создали дубликат уже существующего в приложении сертификата, вы можете его удалить.

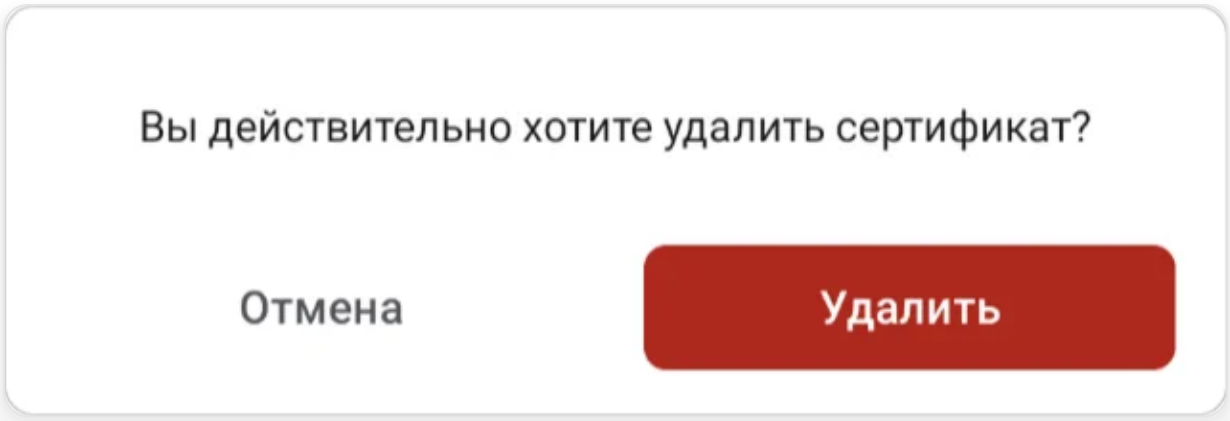
Удаление одного сертификата

Чтобы удалить сертификат:

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



4. Подтвердите действие в модальном окне.



После этого сертификат будет удалён из хранилища.

Групповое удаление

Чтобы удалить несколько сертификатов одновременно:

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. Отметьте флажками сертификаты одним из 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 на панель с сертификатом и удерживайте ее. Напротив панели с сертификатом отобразится флажок. Отметьте флажками другие сертификаты.
3. Вызовите меню действий по кнопке **Еще** и выберите действие **Удалить**.
4. Подтвердите действие 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

Установка корневого и промежуточного сертификатов

- Основные понятия
- Импорт корневого или промежуточного сертификата
- Возможные ошибки

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 главный корневой сертификат принадлежит **Минцифры РФ**.
- Минцифры подписывает корневым сертификатом сертификаты удостоверяющих центров — они называются **промежуточными**.
- На основе промежуточных сертификатов УЦ выпускает **пользовательские сертификаты** (ваши личные или сертификаты других лиц).

Таким образом, проверка подлинности сертификата всегда строится **снизу вверх**: 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

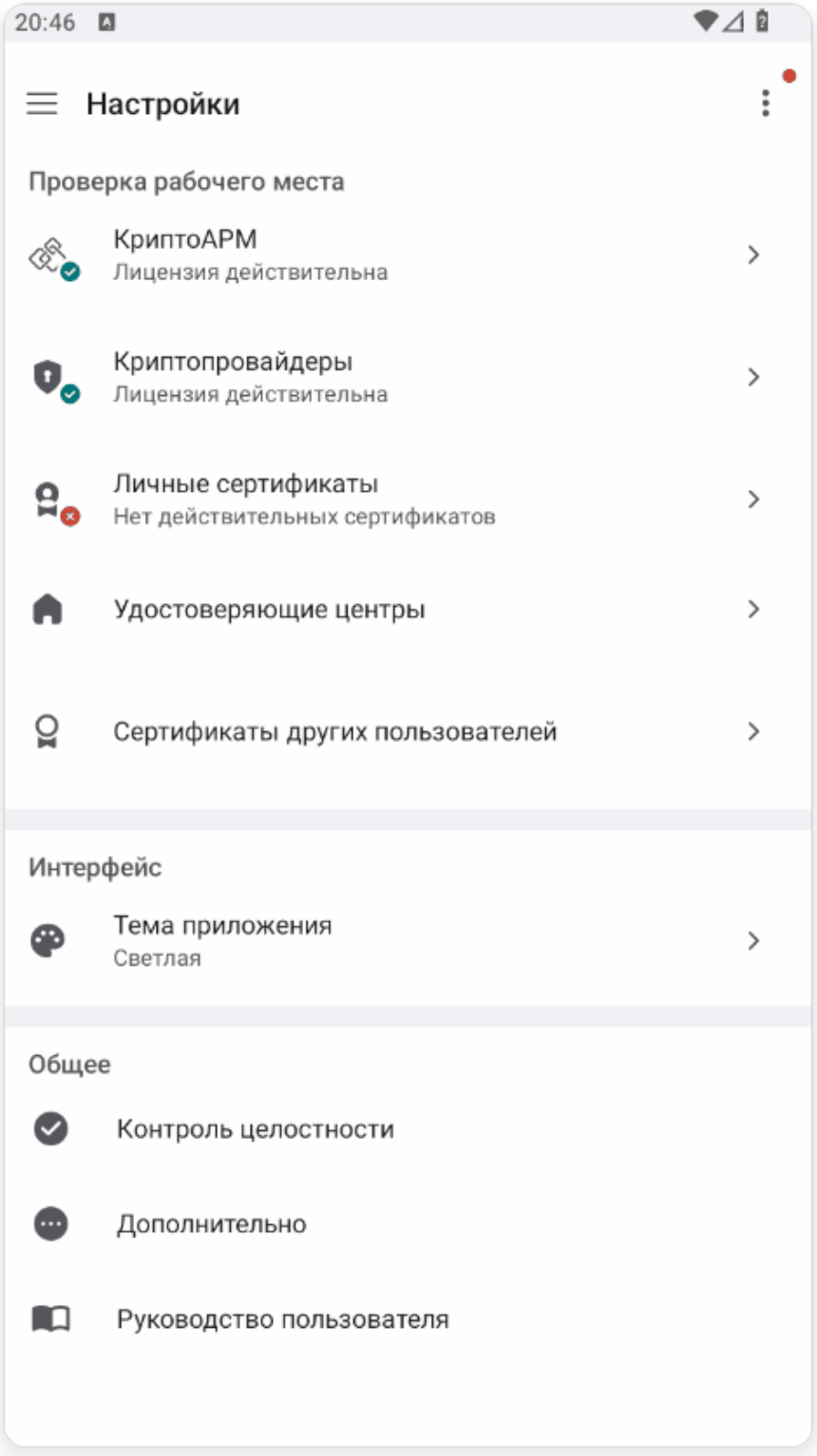
- **На официальном сайте удостоверяющих центров**: обычно в разделе «Поддержка» или «Загрузки» доступны актуальные корневые и промежуточные сертификаты, а также списки отзыва.

> ⚠️ 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 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 `.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 повреждён, не полностью скачан или содержит неподдерживаемые 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

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

Установка списка отзыва

- Основные понятия
- Импорт списка отзыва

Основные понятия

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

Использование СОС необходимо для проверки актуальности сертификатов и исключения компрометированных ключей из доверенной среды.

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. **Из личного сертификата**: в свойствах сертификата есть поле **CRL Distribution Point (CDP)**. По указанной там ссылке (`http://...`) можно скачать актуальный СОС.

> ⚠️ Списки отзыва имеют ограниченный срок действия. По его истечении необходимо скачать и установить обновлённую версию.

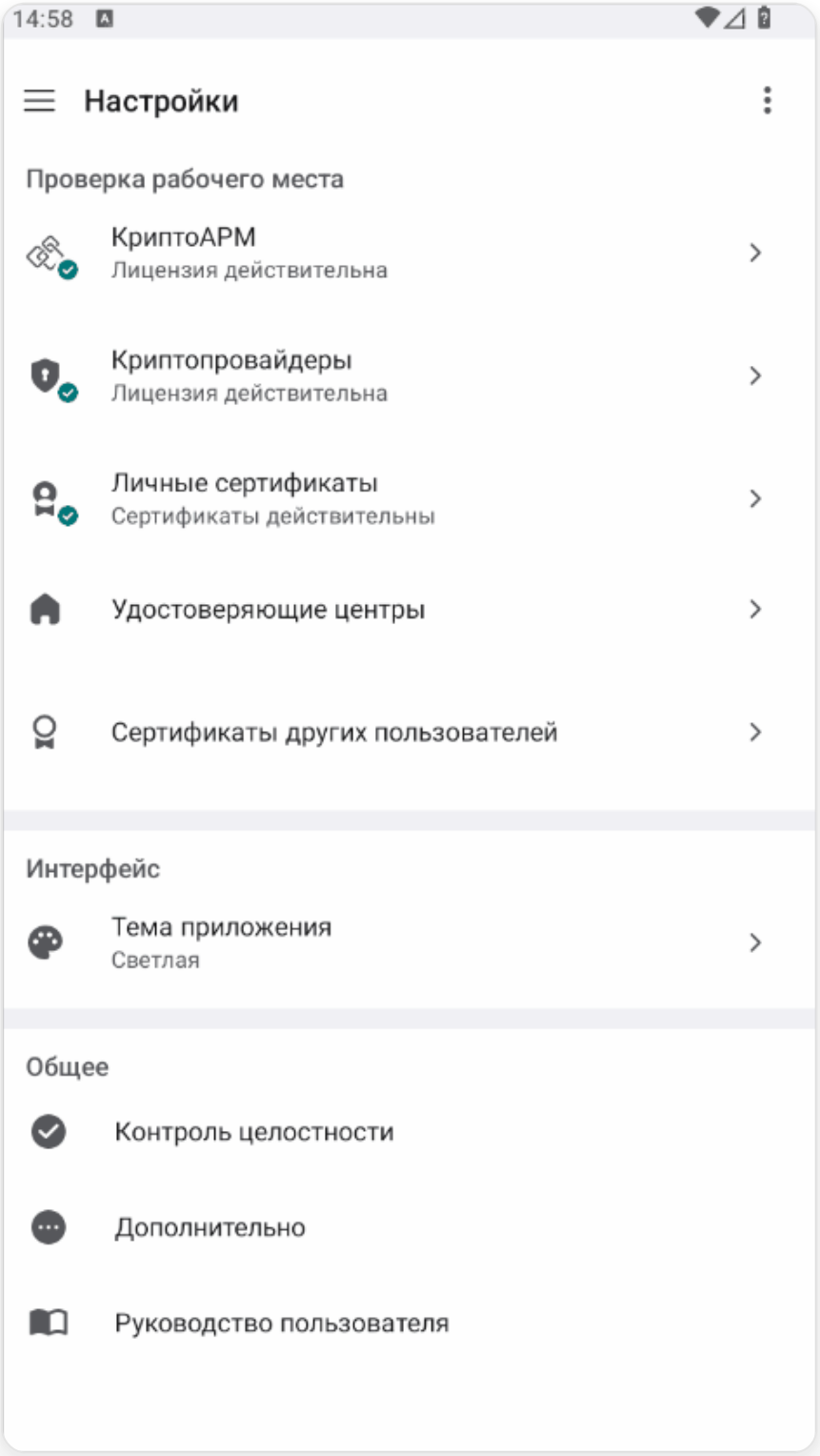
> ⚠️ Всегда скачивайте списки отзыва только с официальных сайтов УЦ.

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 действий **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 заново 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

Установка сертификатов других пользователей

- Импорт сертификата другого пользователя
- Возможные ошибки

Зачем нужны сертификаты других пользователей

Сертификаты других пользователей нужны для безопасного обмена зашифрованными документами.

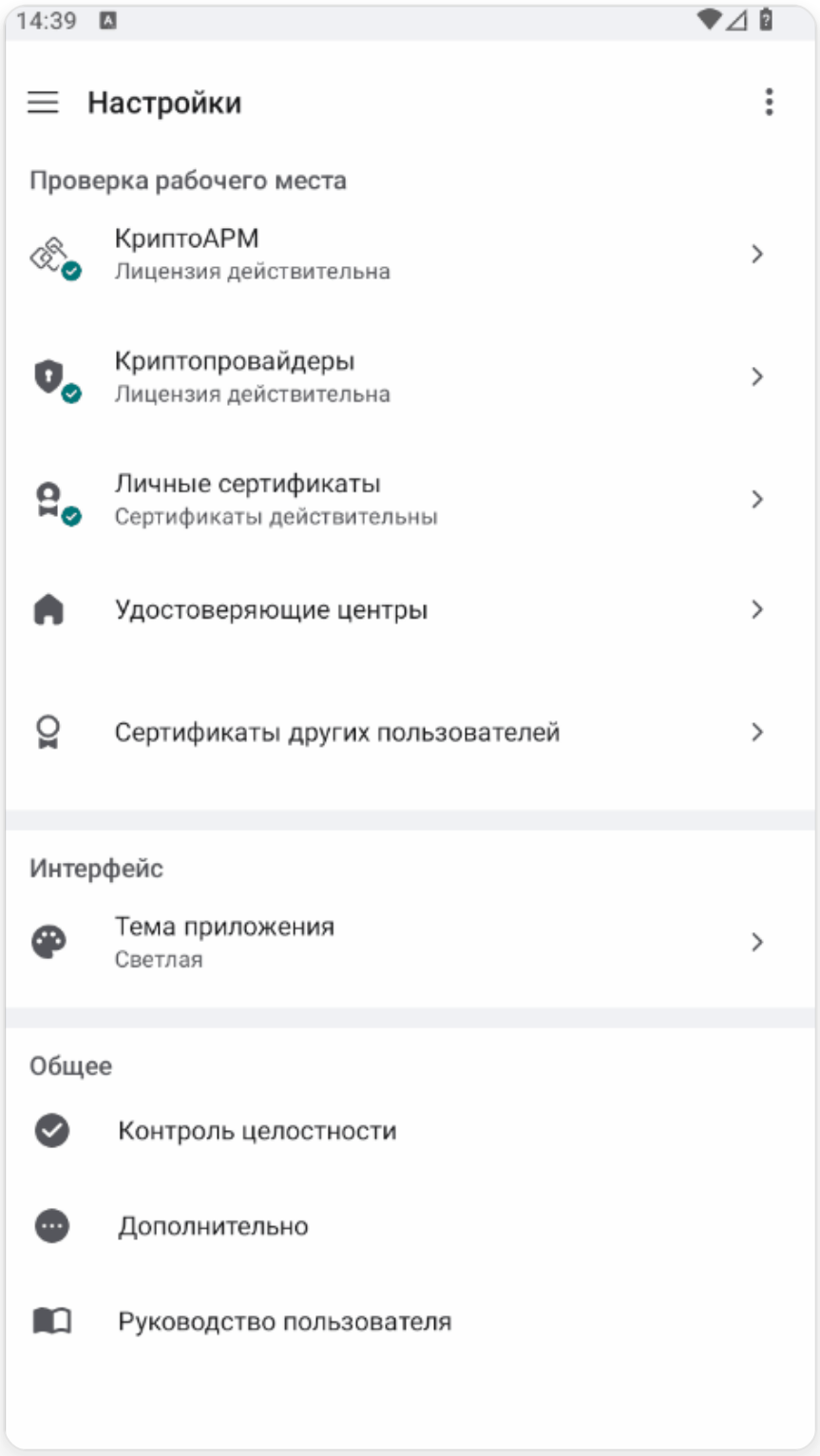
Когда вы хотите переслать коллеге или партнёру конфиденциальную информацию (например, договор, отчёт или персональные данные), документ шифруется с использованием открытого ключа получателя, который хранится в его сертификате.

> 💡 **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 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 `.cer`.



Дождитесь окончания импорта.

После успешного импорта сертификат отобразится в списке.

Возможные ошибки

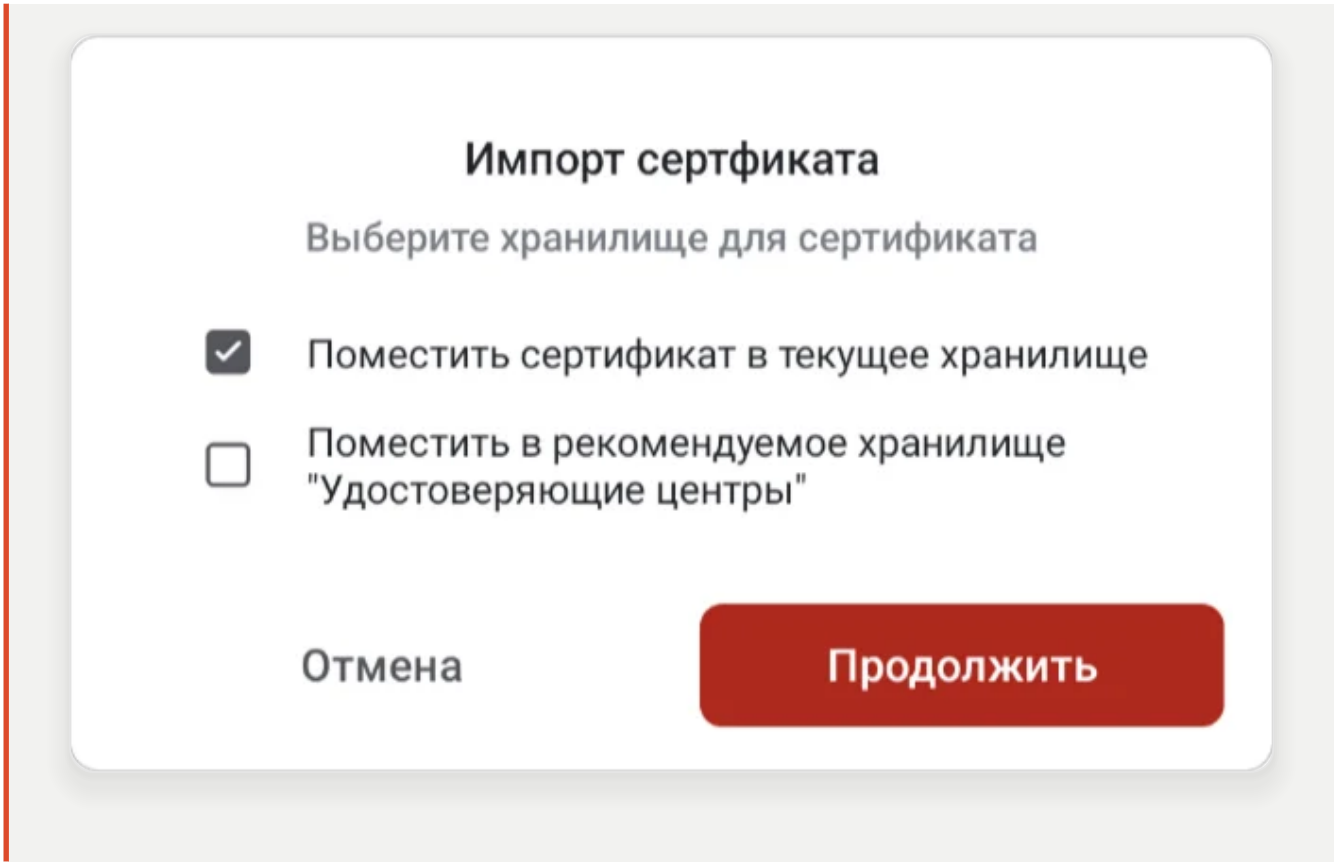
Уведомления об ошибках отображаются в нижней части экрана.

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

Экспорт и удаление сертификата другого пользователя

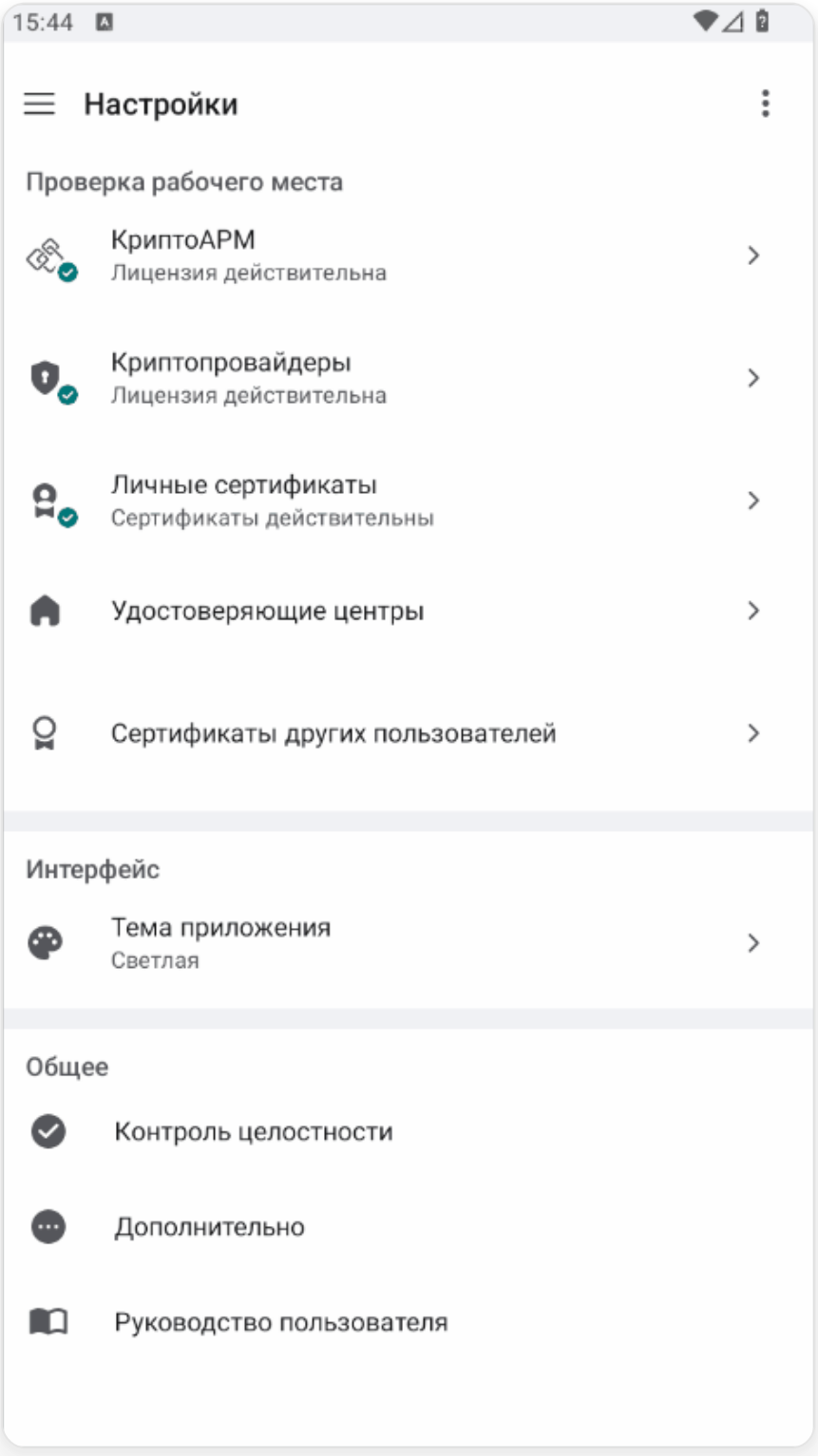
- Экспорт сертификата другого пользователя
- Удаление сертификата другого пользователя

Экспорт сертификата другого пользователя

> ⚠️ **Примечание**: Сертификаты других пользователей, 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 на **Выполнить** в правом верхнем углу.



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

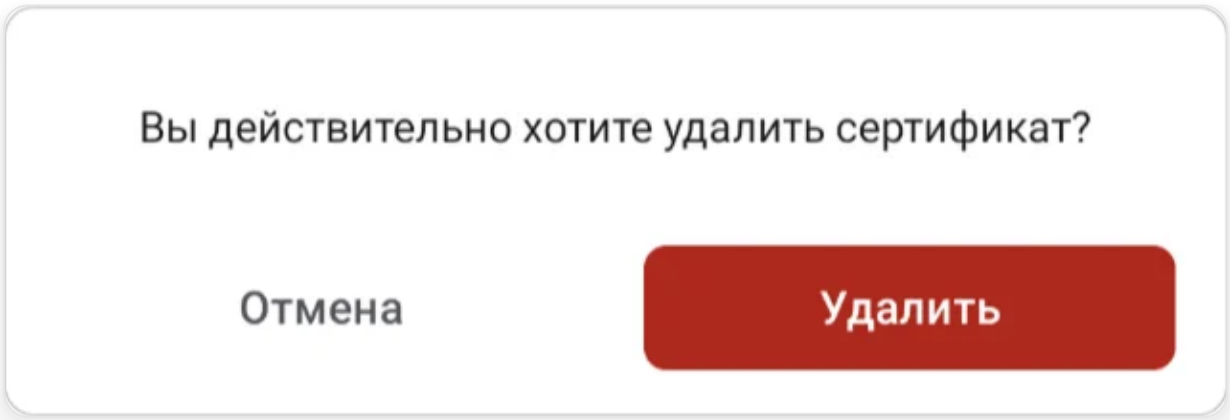
Удаление сертификата другого пользователя

Если срок действия сертификата истёк 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

- О профилях подписи
- Создание профиля подписи
- Установка профиля по умолчанию
- Изменение настроек профиля
- Импорт профиля подписи
- Экспорт профиля подписи
- Удаление профиля

О профилях подписи

Профили подписи — это готовые наборы настроек, которые можно применять для выполнения подписи, архивирования и шифрования.

> 🔍 Про настройки профиля читайте в инструкции Описание настроек профиля.

Советы по работе:

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

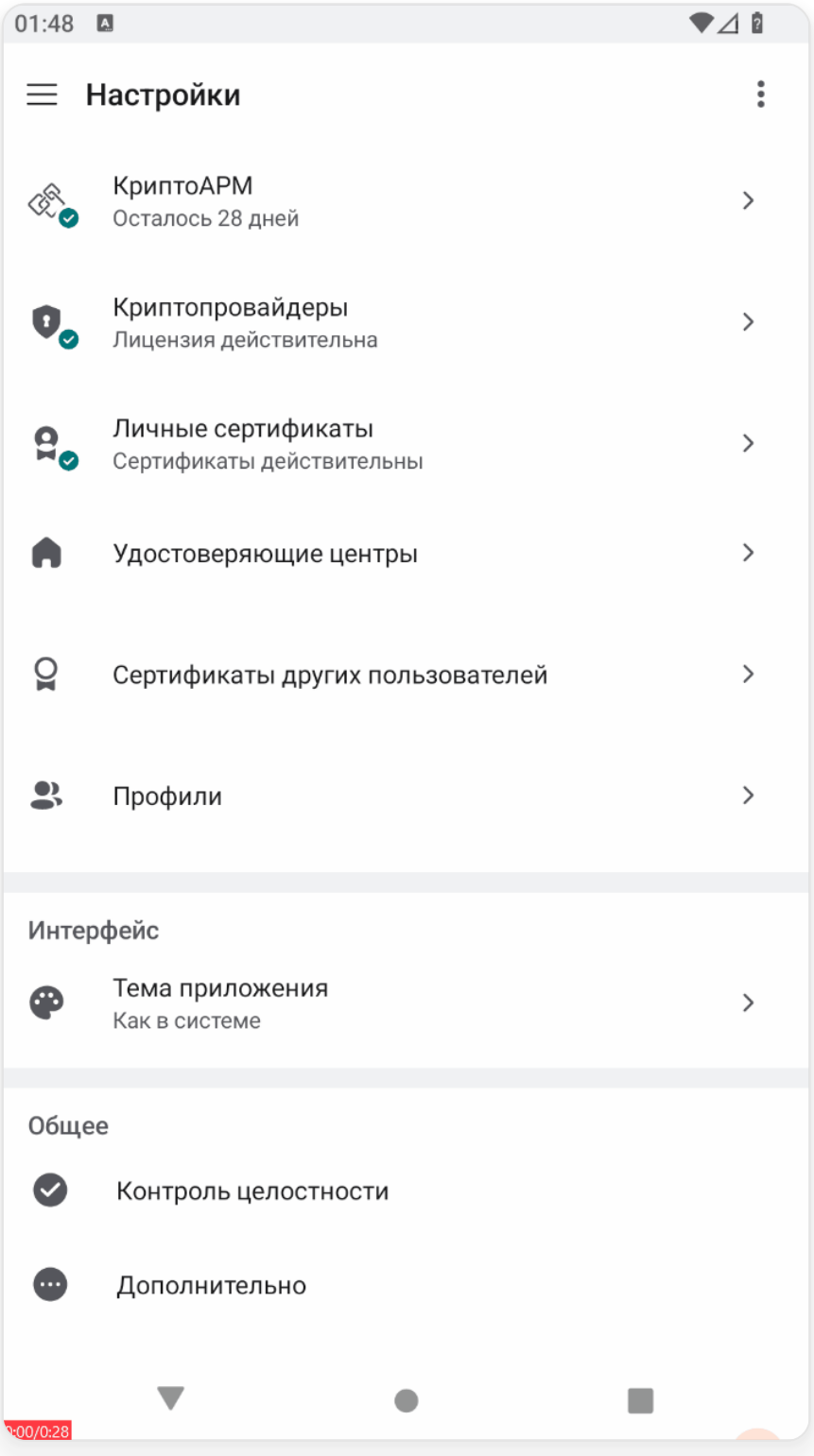
> ⚠️ **Примечание**: При установке приложения автоматически создается профиль подписи с активными операциями «Подпись» и «Шифрование».

Создание профиля подписи

Чтобы создать профиль:

1. Перейдите в раздел **Настройки** → **Профили**.
2. Откроется окно со списком профилей, созданных в приложении.
3. Вызовите меню действий по кнопке **Еще** ⋮ и выберите действие **Создать**.
4. Откроется окно **Новый профиль**.
5. Укажите настройки профиля.

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



6. Нажмите **Сохранить**.

Если создание профиля пройдет успешно, появится уведомление: **Профиль создан**.

Новый профиль отобразится в окне **Профили**.

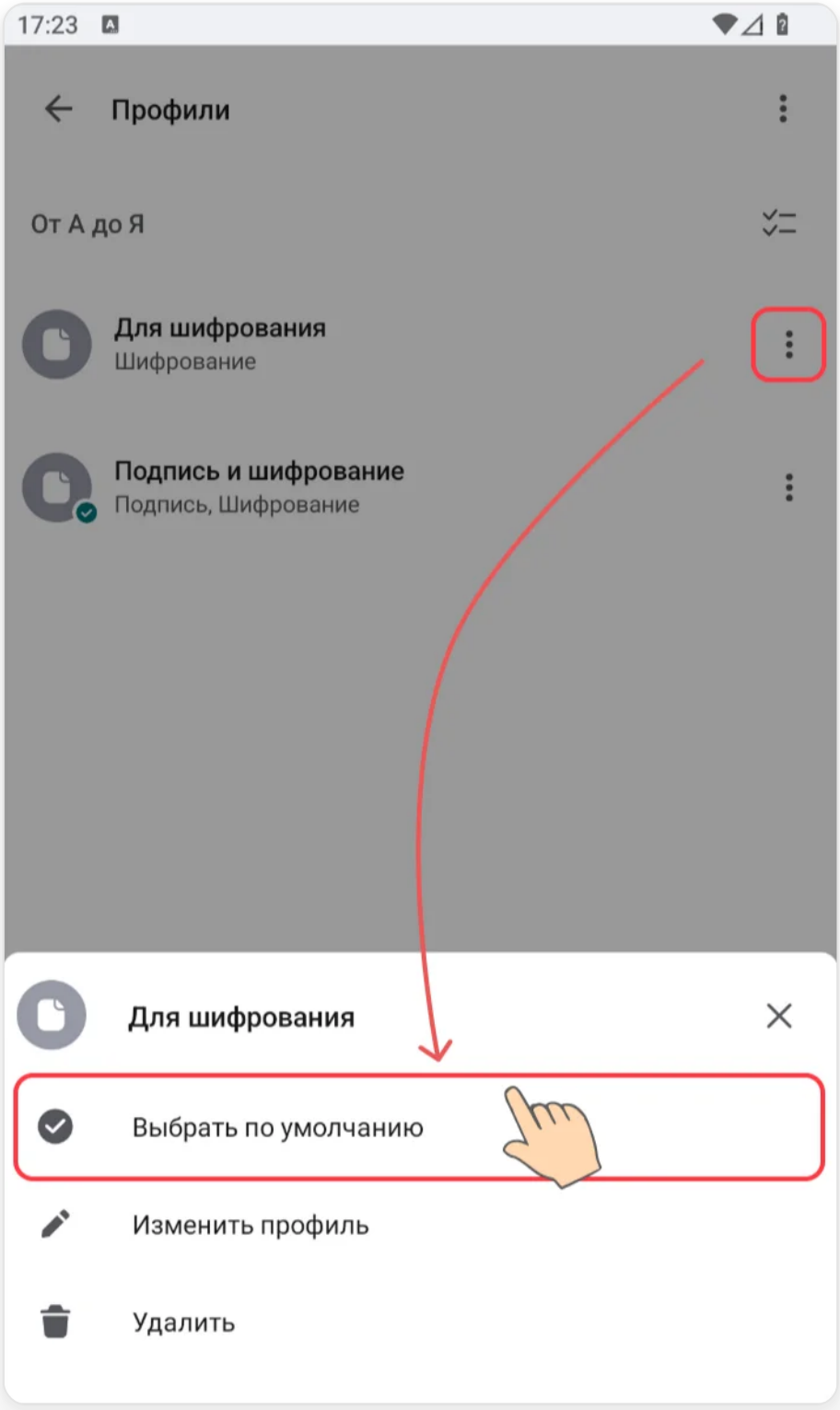
> 💡 **Совет**: Чтобы автоматически использовать профиль при выполнении операций, установите его в качестве профиля по умолчанию.

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. Вызовите меню действий с профилем одним из способов:
   - Нажмите на панель с профилем.
   - 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 про настройки читайте в инструкции Описание полей 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.

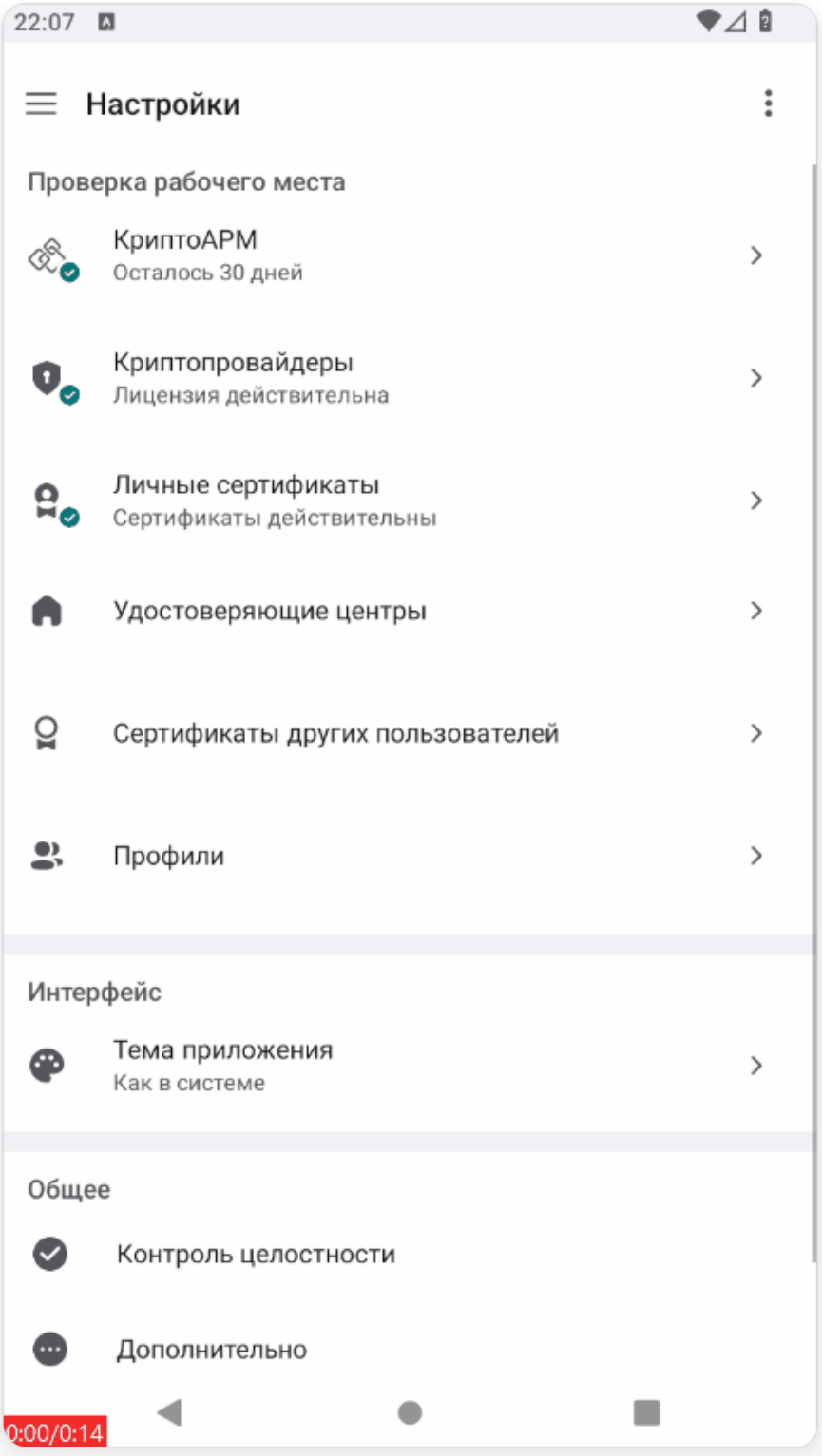
1. Экспорт профиля в файл

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 на панель с профилем и удерживайте ее. Напротив панели с профилем отобразится 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.


22:07
Настройки
Проверка рабочего места
КриптоАРМ
Осталось 30 дней
Криптопровайдеры
Лицензия действительна
Личные сертификаты
Сертификаты действительны
Удостоверяющие центры
Сертификаты других пользователей
Профили
Интерфейс
Тема приложения
Как в системе
Общее
Контроль целостности
Дополнительно
0:00/0:14

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 успешного 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 полей профиля
- Как установить личный сертификат
- Как создать самоподписанный сертификат
- Как импортировать корневой или промежуточный сертификат

Открыть статью на сайте

Описание полей профиля

- 1. Операции
- 2. Сохранение результатов
- 3. Настройки подписи
- 4. Настройки шифрования

1. Операции

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Выбор операций	Множественный выбор (переключатели)	`Подпись`	Определяет набор действий, применяемых к документу	`Подпись`, `Архивирование`, `Шифрование`

2. Сохранение результатов

Название настройки	Тип	Значение по умолчанию	Описание	Дополнительные значения
Сохранить в «Архив»	Переключатель (On/Off)	`Off`	Включает сохранение результатов в специальную папку приложения	`On` / `Off`
Место сохранения	-	Каталог `Файлы и папки`	Папка для сохранения результатов	-

3. Настройки подписи

Сертификат подписи

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
		-		

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Сертификат подписи	Поле для выбора сертификата		Личный сертификат, который будет использоваться для подписи документов.	Сертификат из хранилища **Личные**

Параметры подписи

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Стандарт подписи	Выпадающий список	`CAdES-BES`	Выбор стандарта электронной подписи.	- `CAdES-BES` (классическая подпись), - `CAdES-T` (со штампом времени), - `CAdES-X Long Type 1` (усовершенствованная)
Вид подписи	Выпадающий список	`Присоединенная`	Выбор формата хранения подписи относительно документа.	- `Присоединенная` (подпись и документ в одном файле), - `Отсоединенная` (подпись хранится отдельно)
Кодировка подписи	Выпадающий список	`DER`	Определяет способ кодирования данных подписи.	- `DER` (стандартная бинарная кодировка), - `BASE-64` (текстовая кодировка)
Формат файла подписи	Выпадающий список	`.sig`	Расширение файла, в который сохраняется подпись.	- `.sig`, - `.p7s`, - `.sgn`, - `.sign`, - `.bin`
Действия при соподписи	Выпадающий список	`Добавлять в исходный документ`	Действие, которое будет применяться к подписанному документу,	- `Добавлять в исходный документ`, - `Добавлять в копию исходного документа`

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
			добавленному в мастер из раздела «Архив».	

Настройки для стандартов со штампами

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Служба штампов времени (TSP)	Текстовое поле	-	Адрес службы штампов времени. Адрес службы можно узнать у поставщика услуги. Услуги службы штампов времени могут предоставлять удостоверяющие центры.	Формат адреса: `<https>://<сервер>[:порт][/путь]`
Служба онлайн статусов (OCSP)	Текстовое поле	-	Адрес службы онлайн-статусов. Данное поле **необязательно** для заполнения, чаще всего адрес прописан в сертификате подписи.	Формат адреса: `<https>://<сервер>[:порт][/путь]`

Машиночитаемая доверенность (МЧД)

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Машиночитаемая доверенность	Переключатель (On/Off)	`Off`	Добавление МЧД к пакету документов.	`On` / `Off`
Файл МЧД	Файл (.xml)	-	Выберите XML-файл доверенности, который будет прикреплён к документам.	-
Файл подписи доверителя	Файл (.sig)	-		-

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
			Выберите подпись доверителя для файла МЧД.	

4. Настройки шифрования

Получатели (Сертификаты шифрования)

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Сертификаты шифрования	Поле для выбора сертификатов	-	Сертификаты, которые будут использоваться при шифровании	- Сертификаты из хранилищ **Личные** и **Других пользователей**, - Контакты с сертификатами

Параметры шифрования

Название настройки	Тип	Значение по умолчанию	Описание	Допустимые значения
Алгоритм шифрования	Выпадающий список	`ГОСТ Р 34.12-2015 Магма`	Определяет алгоритм, используемый для шифрования данных	`ГОСТ 28147-89` (устаревший), `ГОСТ Р 34.12-2015 Магма` (актуальный), `ГОСТ Р 34.12-2015 Кузнечик` (256-битный)
Кодировка файлов	Выпадающий список	`DER`	Задает способ представления зашифрованных данных	`DER`, `BASE-64`

Инструкции по теме

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

Открыть статью на сайте

Настройка интерфейса

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.

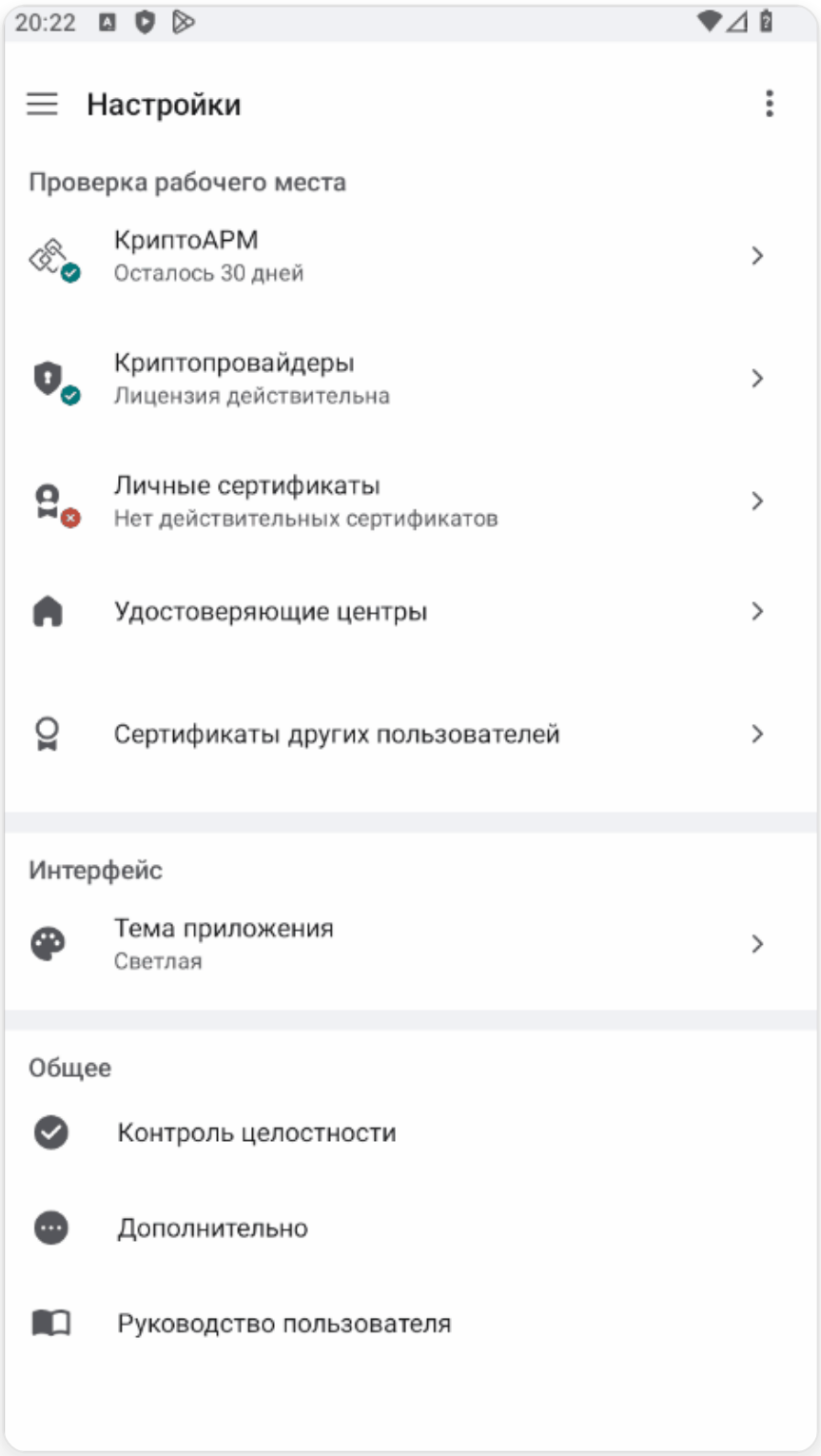
Изменение темы приложения

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

Общие настройки

- Контроль целостности приложения
- Проверка атрибута KeyAgreement
- Портал документации

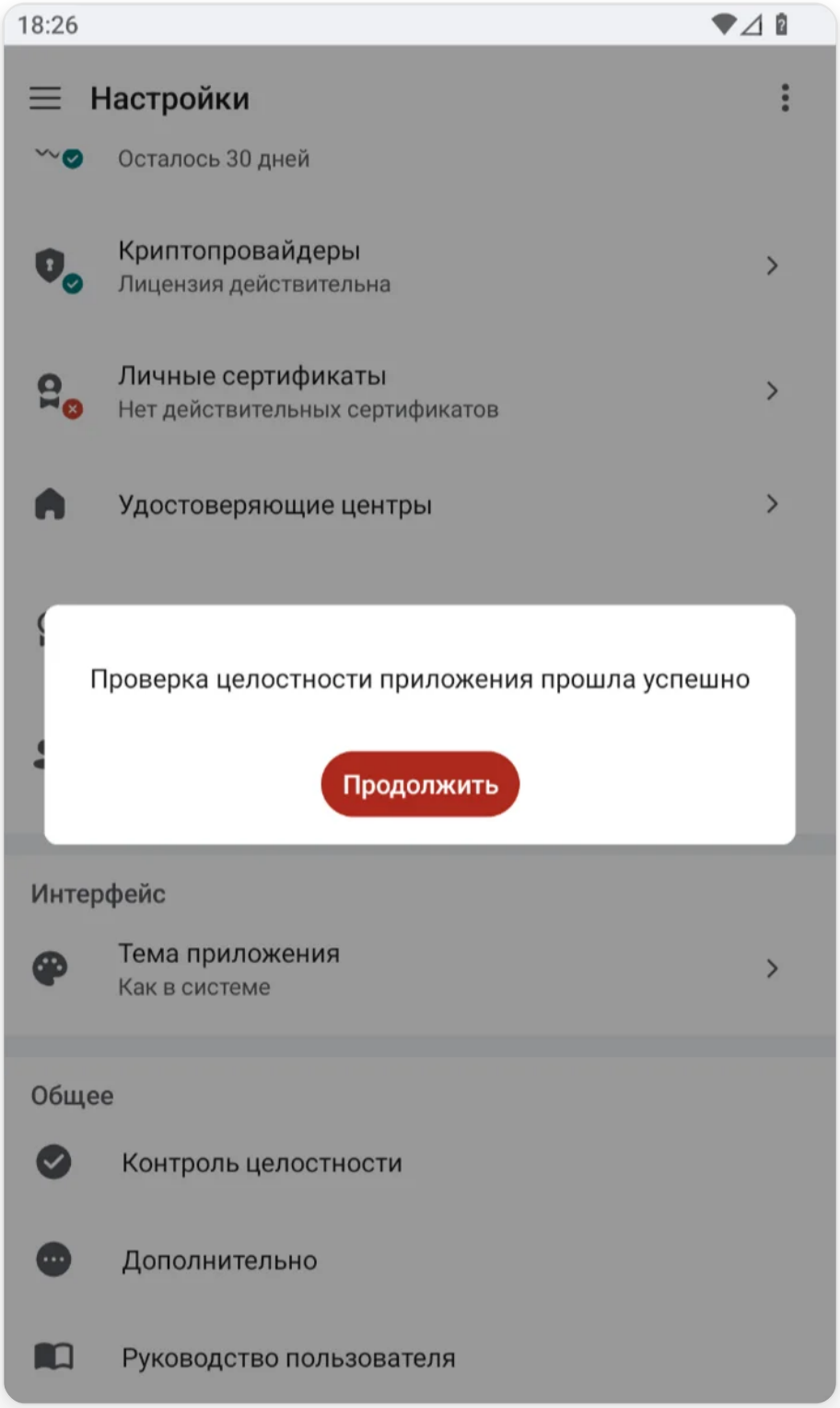
Контроль целостности приложения

> 💡 **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.


18:26
Настройки
Осталось 30 дней
Криптопровайдеры
Лицензия действительна
Личные сертификаты
Нет действительных сертификатов
Удостоверяющие центры
Проверка целостности приложения прошла успешно
Продолжить
Интерфейс
Тема приложения
Как в системе
Общее
Контроль целостности
Дополнительно
Руководство пользователя

Проверка атрибута KeyAgreement

Зачем нужна проверка

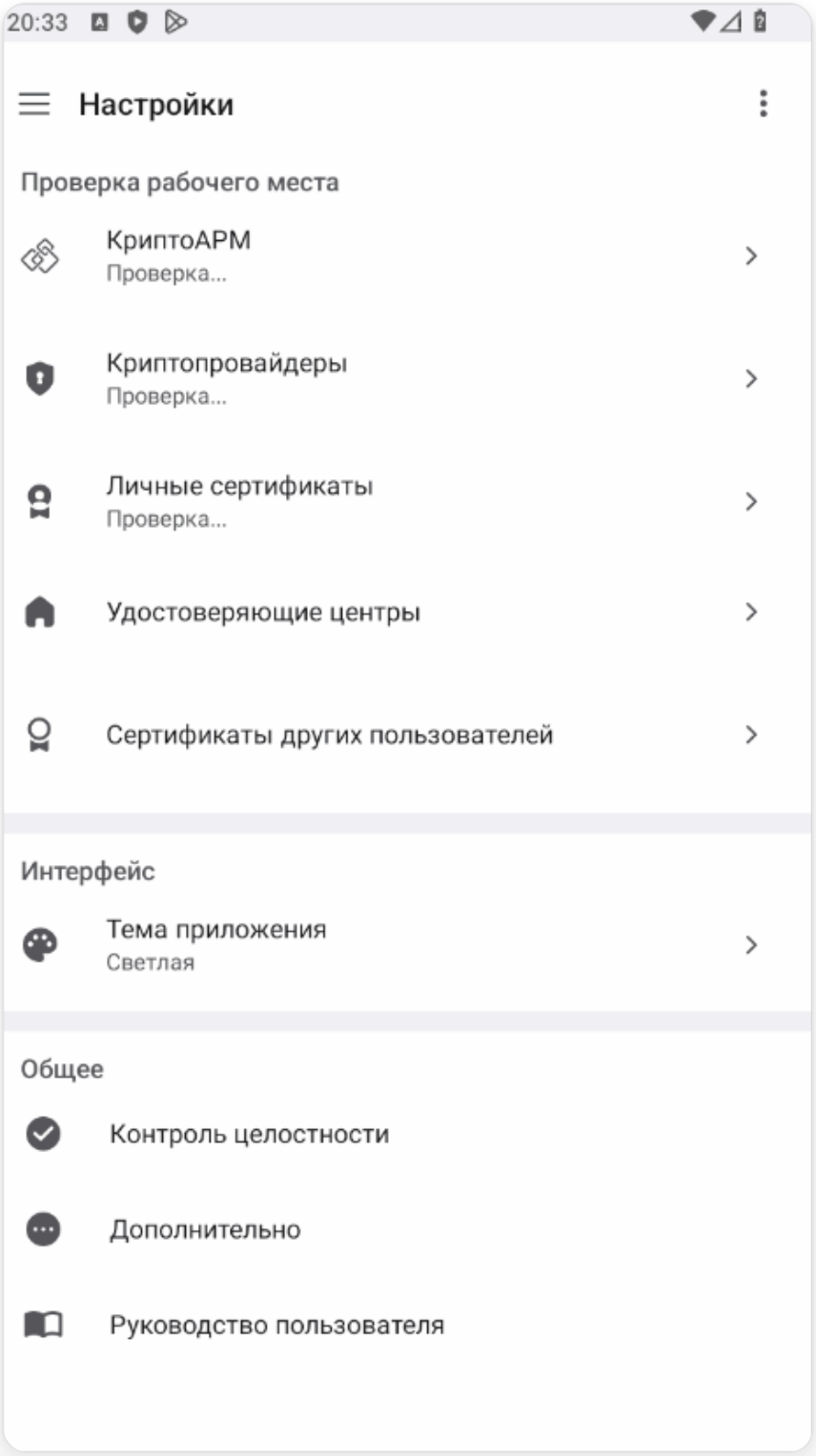
Атрибут **KeyAgreement** (согласование ключей) в расширении **keyUsage** указывает, что сертификат можно использовать для безопасного обмена ключами при шифровании.

- 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

Подпись документов

- О подписи
- Как подписать документы
- Возможные ошибки

О подписи

В **КриптоАРМ** можно создавать электронные подписи документов по стандартам CAdES. Электронная подпись гарантирует подлинность документа и защищает его от изменений.

Поддерживаемые стандарты

- **CAdES-BES** - базовая подпись без меток времени,
- **CAdES-T** - подпись со штампом времени (TSP) для фиксации момента подписания,
- **CAdES-X Long Type 1** - для создания усовершенствованной подписи с архивными штампами времени и полными доказательствами валидации и цепочки сертификатов.

Типы подписи

Подпись может быть добавлена в файл как присоединенная или отсоединенная.

- При **присоединенной подписи** документ и подпись хранятся в одном файле. Для подписанного документа создается новый файл расширением (например, `.sig` или `.p7s`). Что делает невозможным открытие файла без снятия подписи с помощью специализированного приложения. Основное преимущество такого варианта — удобство хранения и передачи.
- **Отсоединенная подпись** сохраняется в отдельном файле (например, с расширением `.sig` или `.p7s`). Исходный документ остается неизменным и доступным для просмотра.

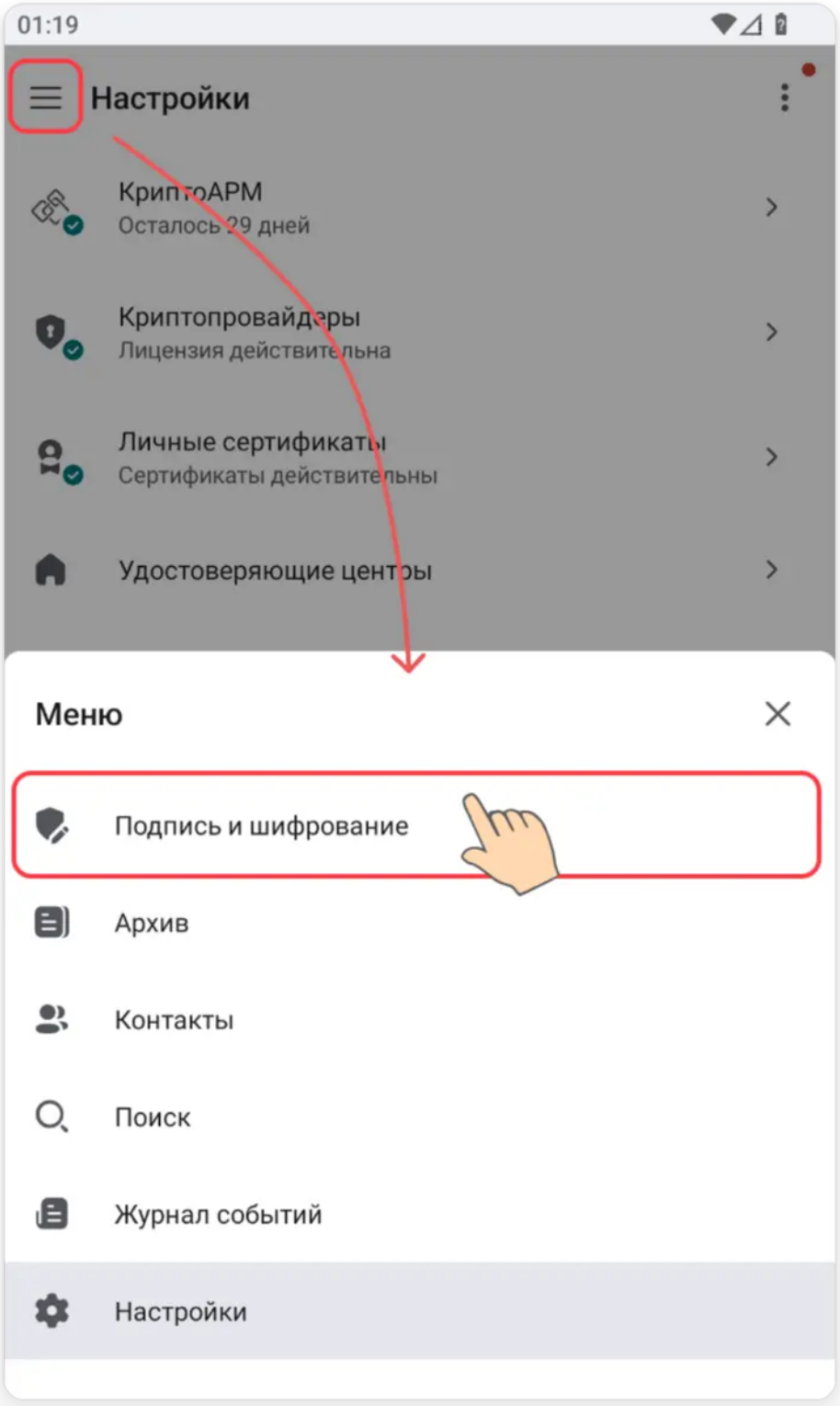
Как подписать документы

> 💡 **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 , размещенной в верхнем левом углу окна приложения.

2. Выберите пункт **Подпись и шифрование**.

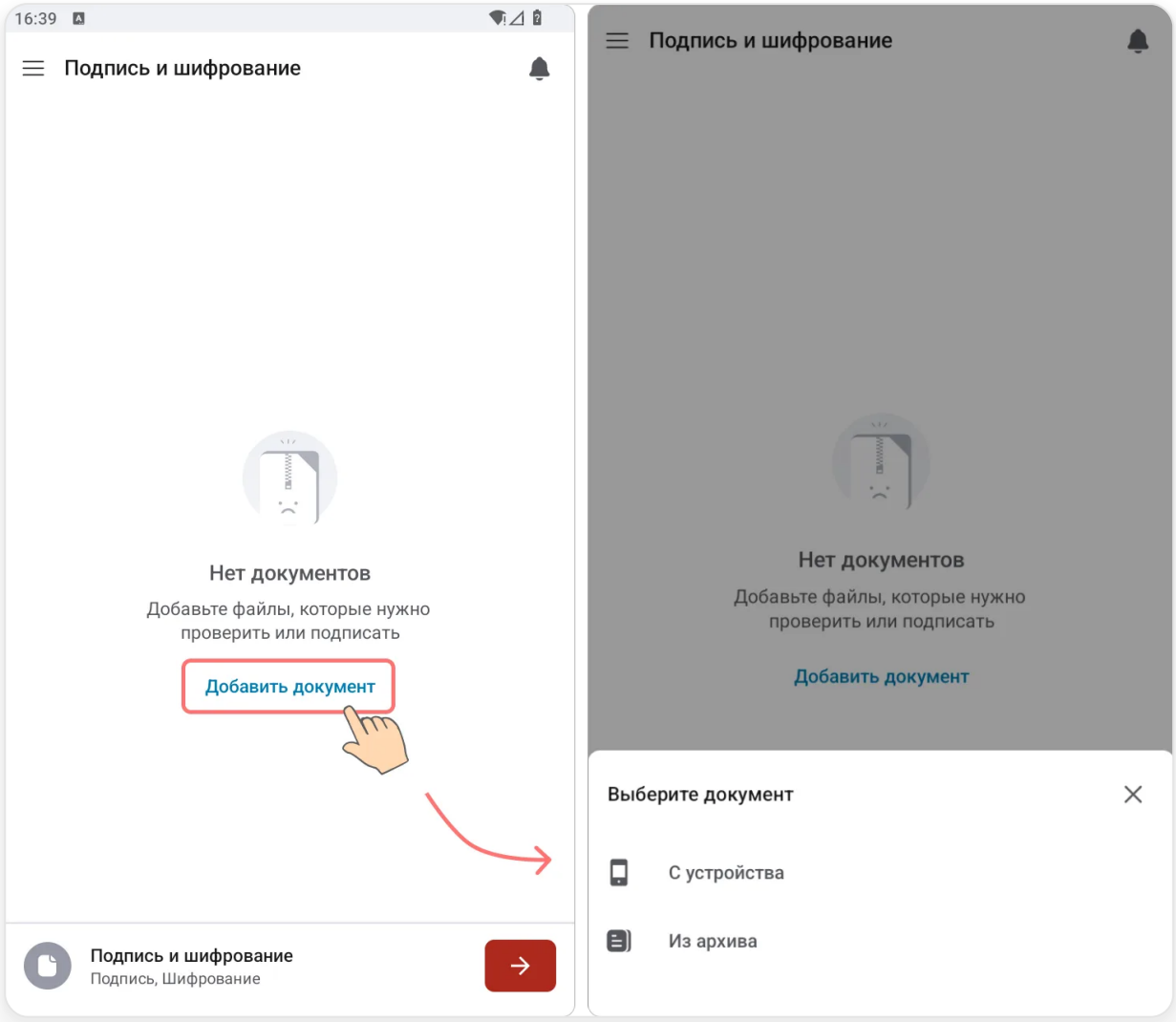


> 💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов.

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**.

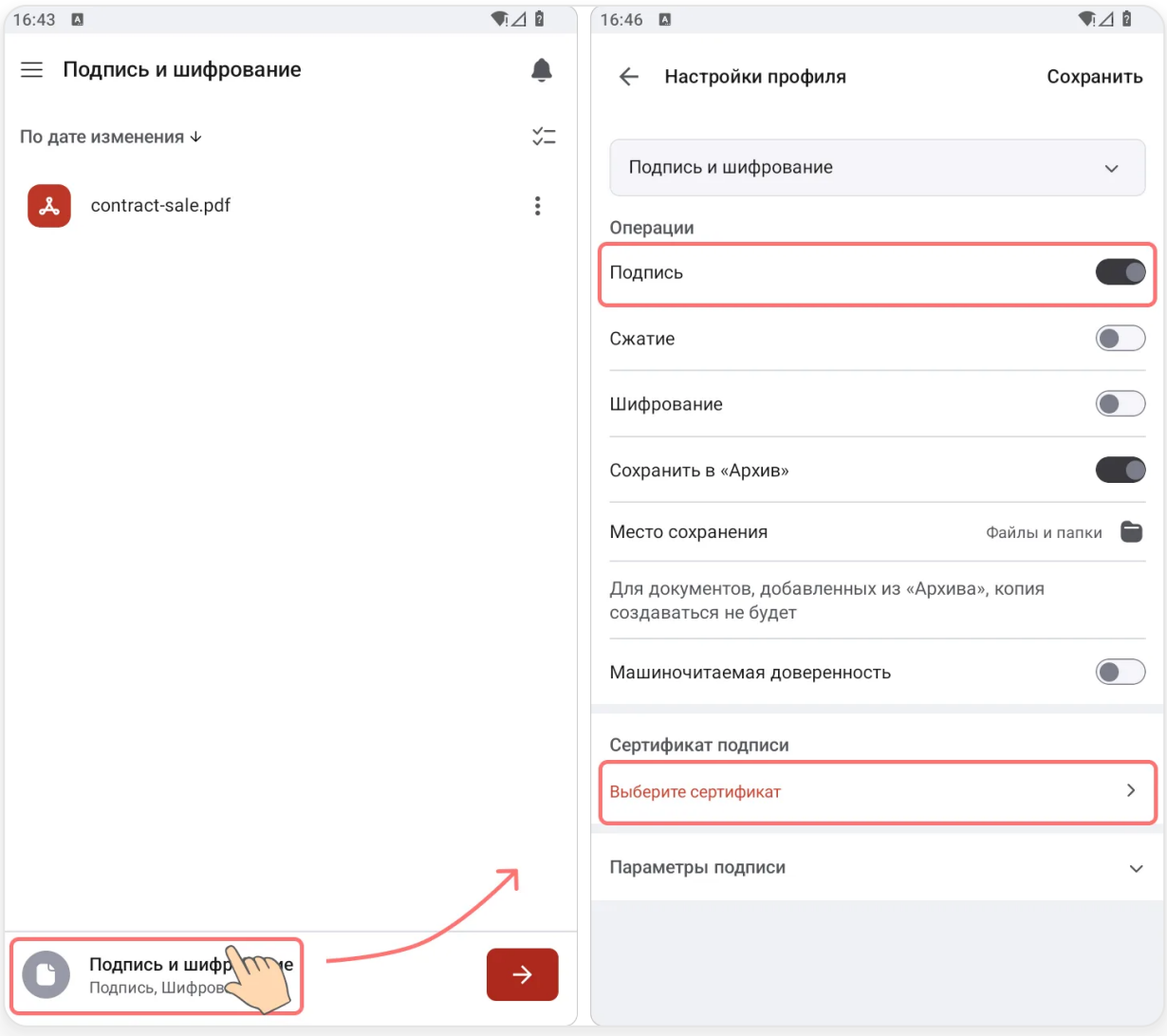
Шаг 3. Настройка параметров подписи

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:
   - Выберите **Подпись** в блоке **Операции**.
   - Выберите **сертификат подписи**. Для этого нажмите на соответствующую панель и в открывшемся окне укажите один из личных сертификатов.



Дополнительно можно:

- указать машиночитаемую доверенность (МЧД),
- включить сохранение копии подписанных файлов с помощью настройки **Сохранить в «Архив»**,
- выбрать стандарт и тип подписи.

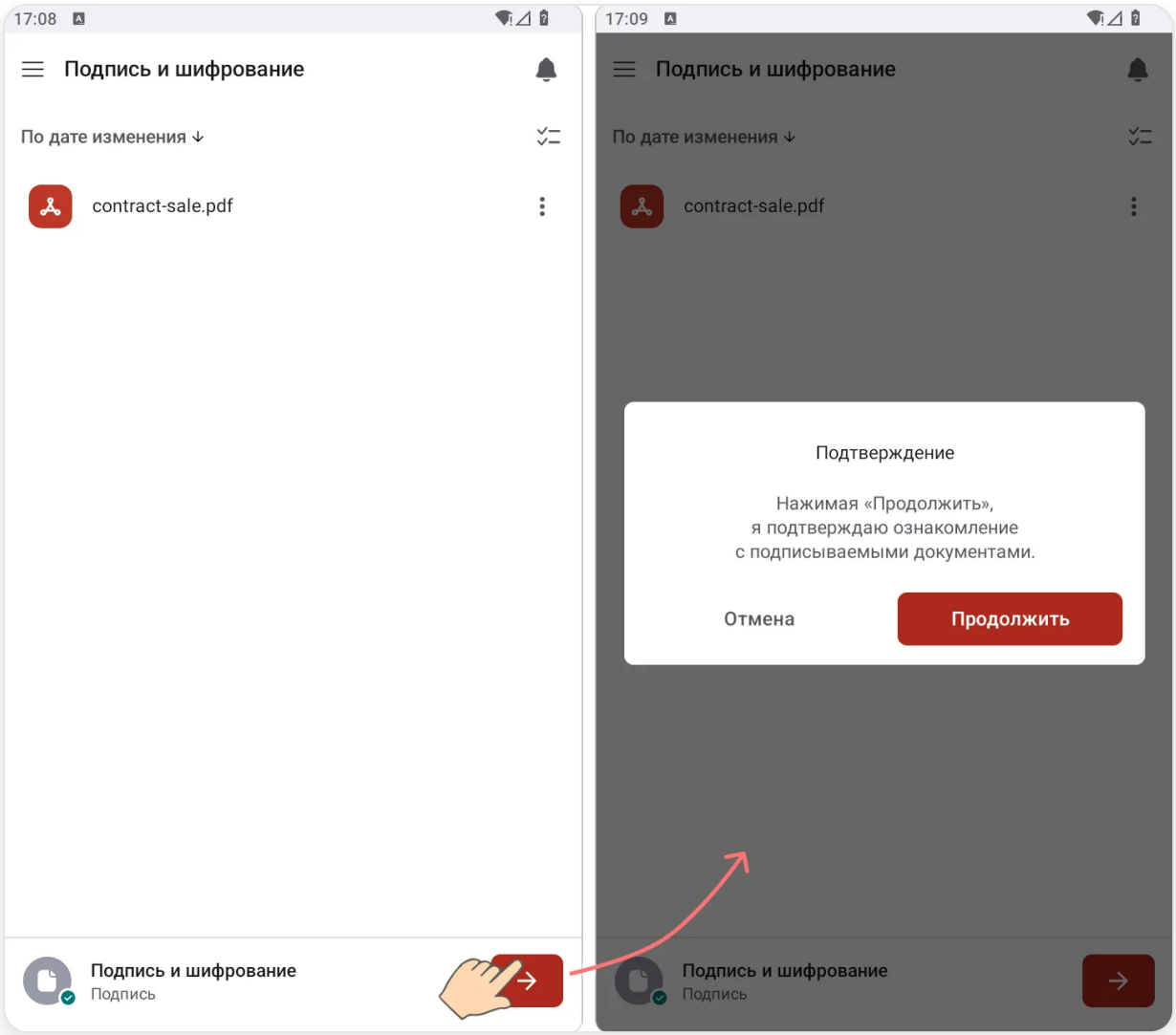
> 💡 **Совет**: Чтобы поставить подпись со штампами, выберите стандарт подписи **CAdES-X Long Type 1** или **CAdES-T** и укажите настройки служб штампов времени. Про описание настроек читайте в инструкции Настройки для стандартов со штампами.

3. Сохраните настройки профиля.

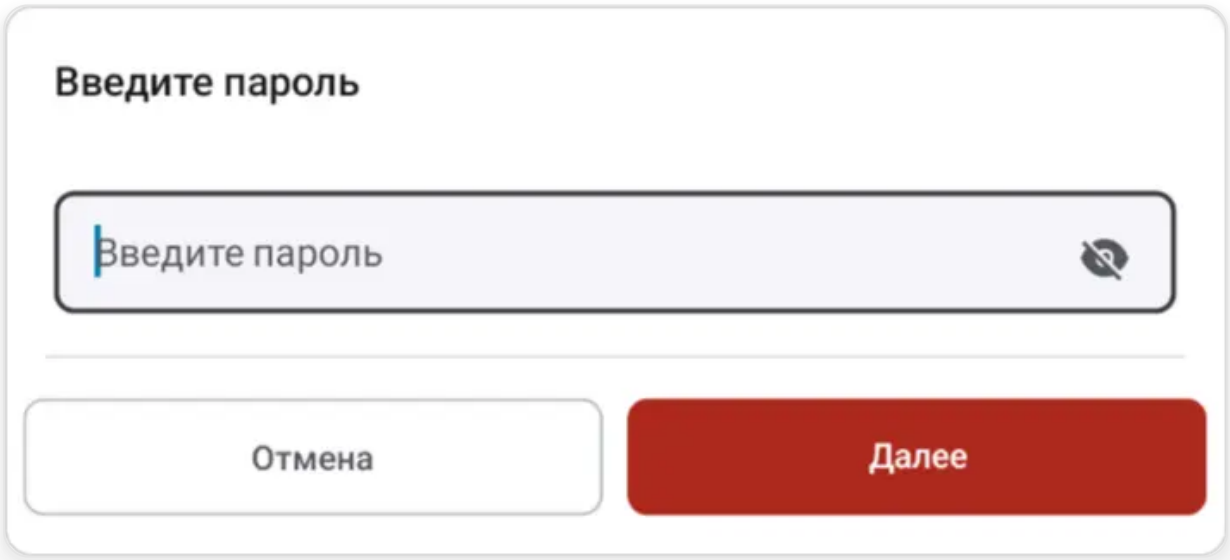
> 💡 **Совет**: Чтобы переключить профиль, нажмите кнопку рядом с его названием и выберите нужный профиль из выпадающего списка.

Шаг 4. Подтверждение и выполнение операции

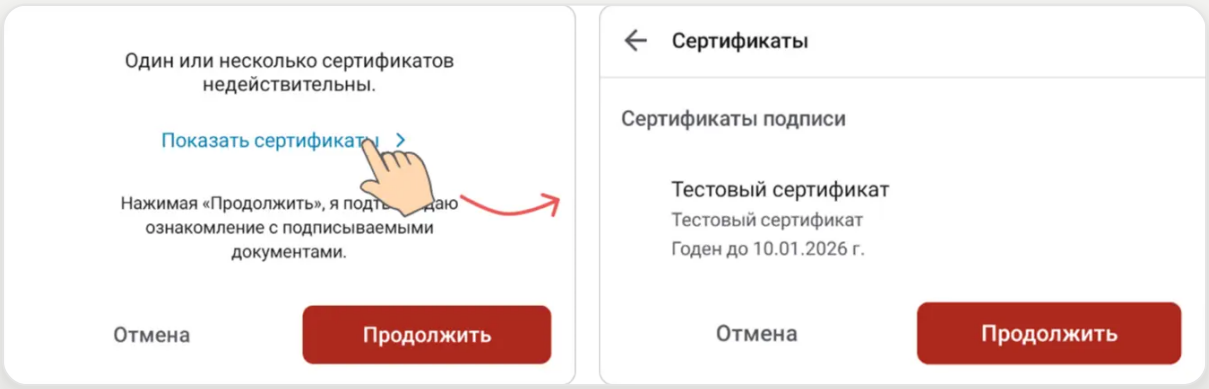
1. Нажмите кнопку **Выполнить** в нижней части окна **Подпись и шифрование**.
2. В окне подтверждения нажмите **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.



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



🚨 Если сертификат недействителен, будет показано предупреждение. Подпись всё равно будет выполнена, но её юридическая значимость может быть оспорена.

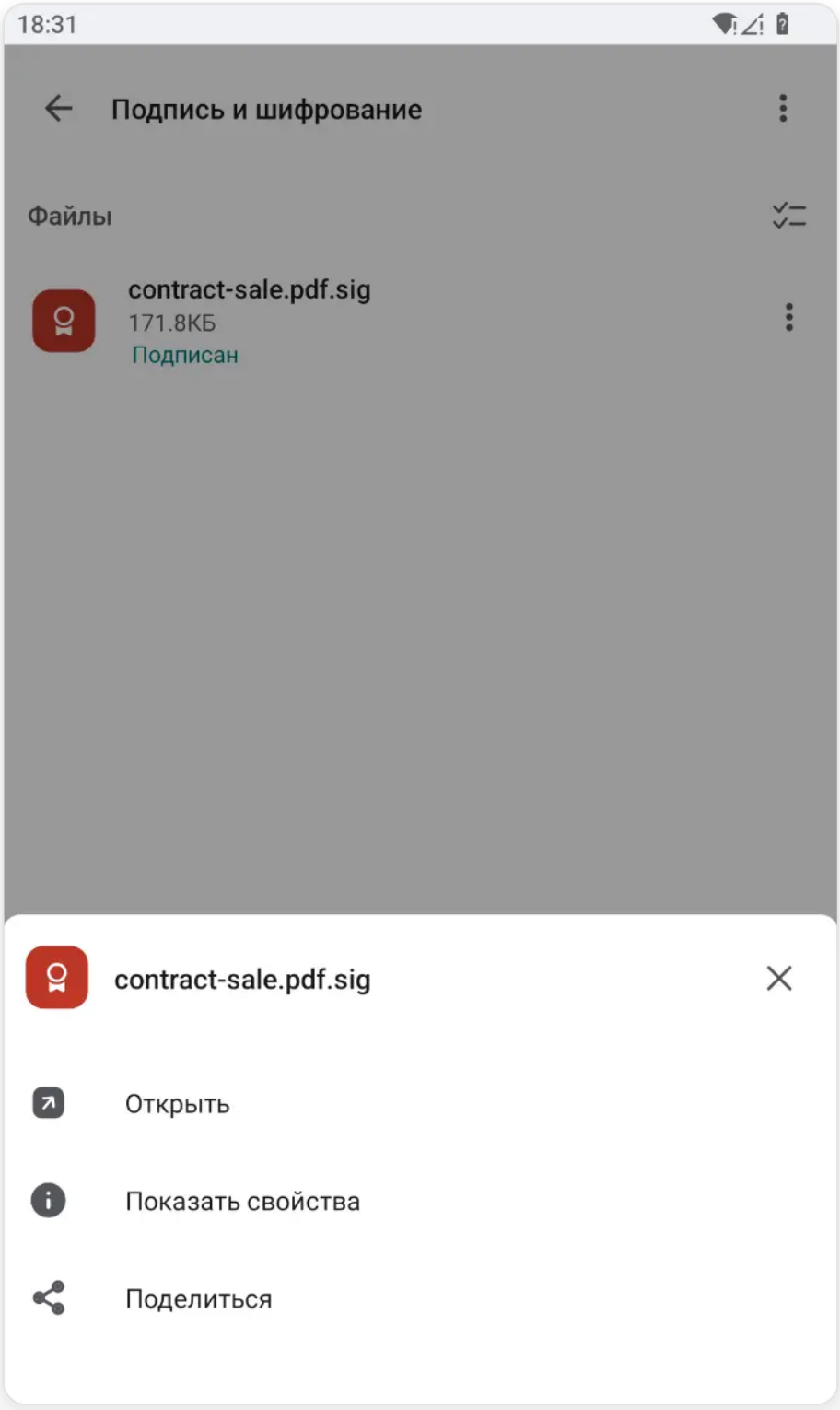


Шаг 5. Результат

Выполнение операции занимает определенное время и зависит от их объема 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 отсоединённая подпись, то в раздел «Документы» помимо файла подписи сохранится копия исходного файла.



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

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
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
Произошла ошибка	Введен неверный пароль для доступа к закрытому ключу	Указан неверный 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.
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	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

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

Добавление соподписи

- Что такое соподпись?
- Как добавить соподпись

Что такое соподпись?

Соподпись - это процесс добавления дополнительной электронной подписи к документу, который уже содержит одну или несколько подписей.

Соподпись может потребоваться в следующих случаях:

- Коллективное утверждение документа;
- Многоэтапное согласование между отделами;
- Подтверждение документа несколькими ответственными лицами.

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

- **Присоединённая подпись**: если исходный документ содержит присоединённую подпись, рекомендуется делать соподпись также **присоединённой**, чтобы все подписи хранились в одном файле.
- **Отсоединённая подпись**: если исходный документ содержит отсоединённую подпись, соподпись лучше делать **отсоединённой**, чтобы сохранить согласованную схему хранения подписей.

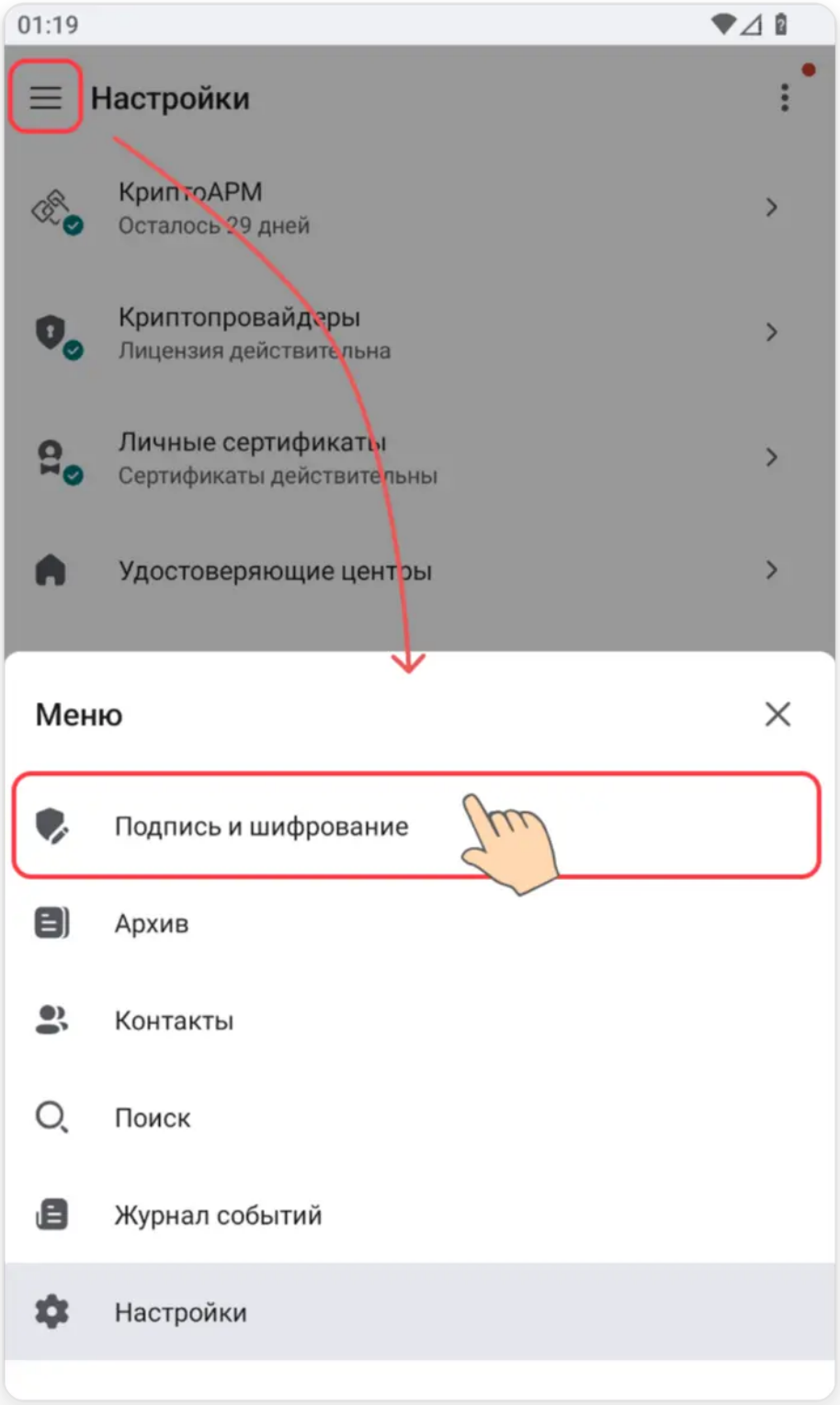
> ⚠️ Несоблюдение согласованного типа подписи может привести к путанице при проверке и хранении документа.

Как добавить соподпись

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

Шаг 1. Запуск мастера

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

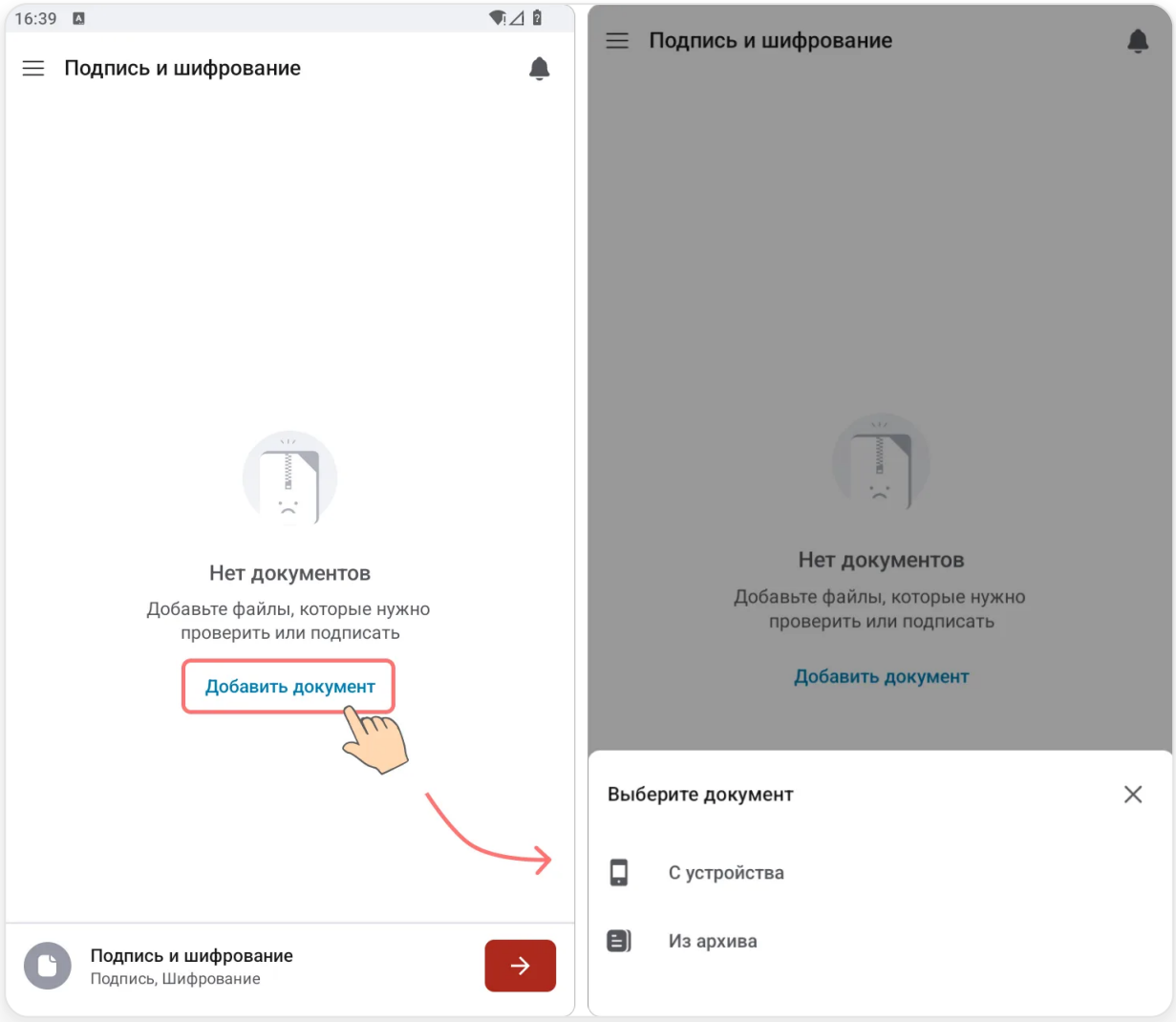


💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

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. Проверка подписей

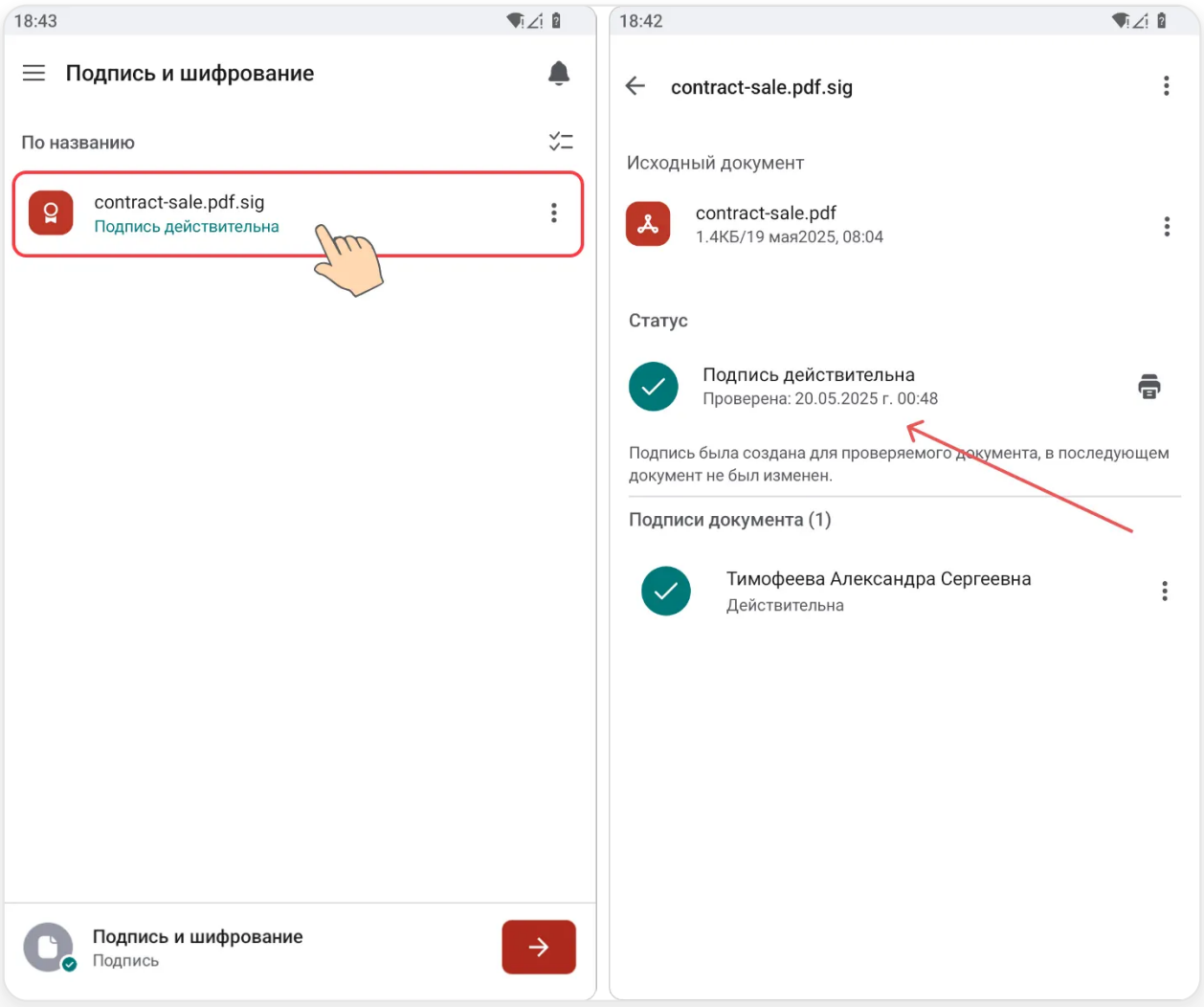
Проверьте валидность всех существующих подписей и убедитесь, что документ не изменялся после последнего подписания.

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 её не удалось проверить.

> 💡 **Совет**: 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.



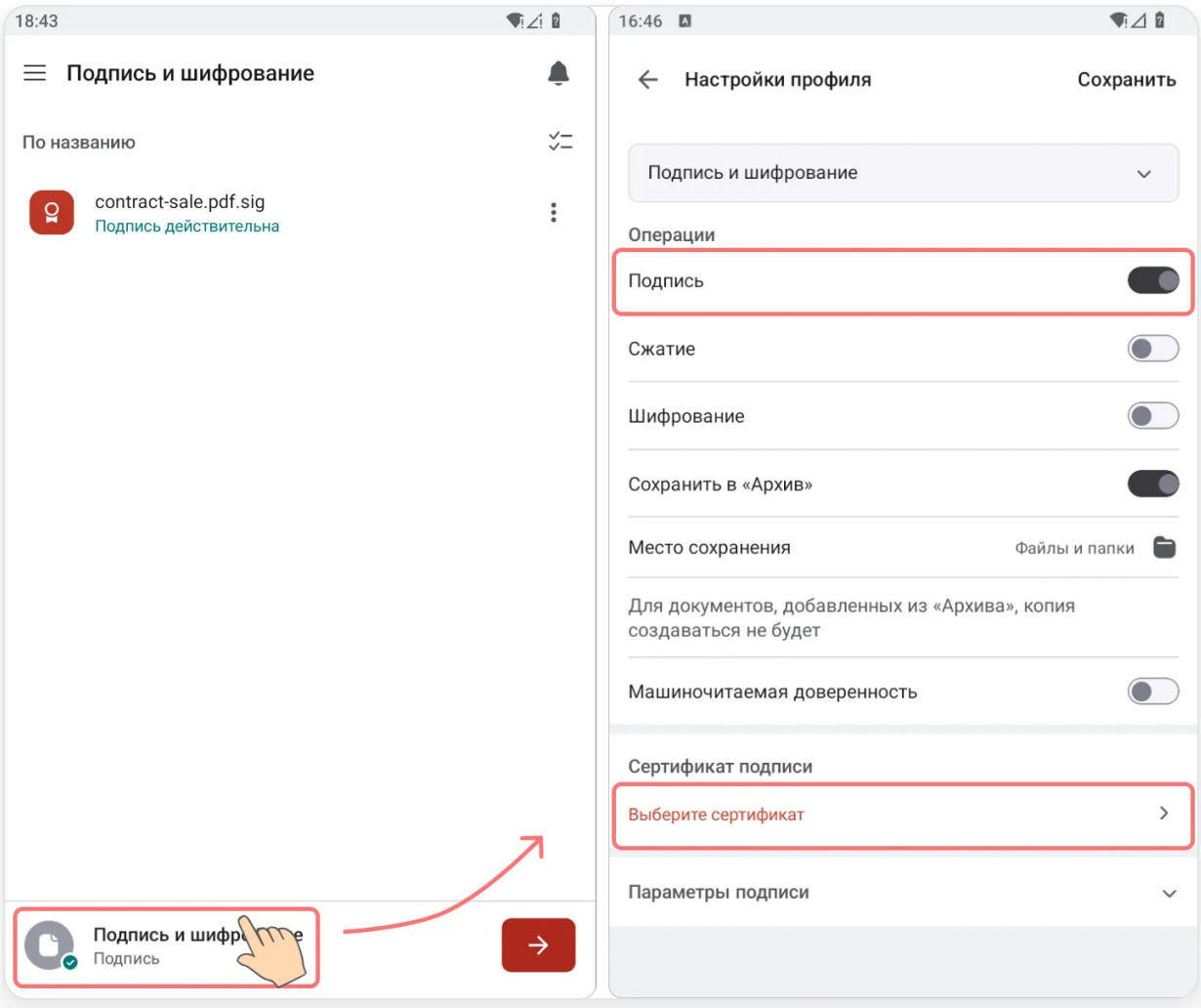
Шаг 4. Настройка параметров подписи

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:
   - Выберите **Подпись** в блоке **Операции**.
   - Выберите **сертификат подписи**. Для этого нажмите на соответствующую панель и в открывшемся окне укажите один из личных сертификатов.



Дополнительно можно:

- указать машиночитаемую доверенность (МЧД),
- включить сохранение копии подписанных файлов с помощью настройки **Сохранить в «Архив»**,
- выбрать стандарт и тип подписи.
- выбрать способ соподписи документов из **Архива**: в исходный файл или его копию.

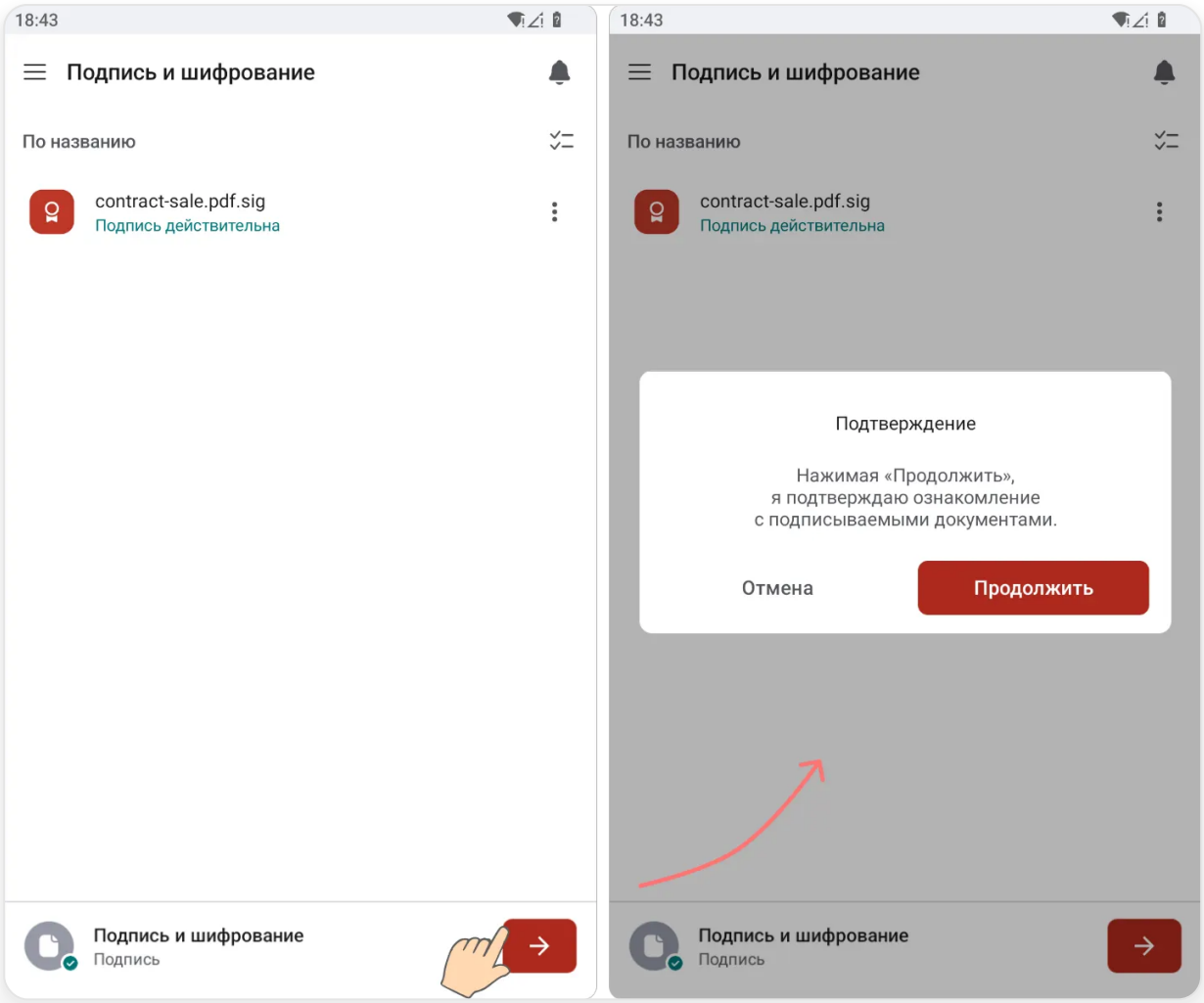
> 💡 **Совет**: Чтобы поставить подпись со штампами, выберите стандарт подписи **CAdES-X Long Type 1** или **CAdES-T** и укажите настройки служб штампов времени. Про описание настроек читайте в инструкции Настройки для стандартов со штампами.

3. Сохраните настройки профиля.

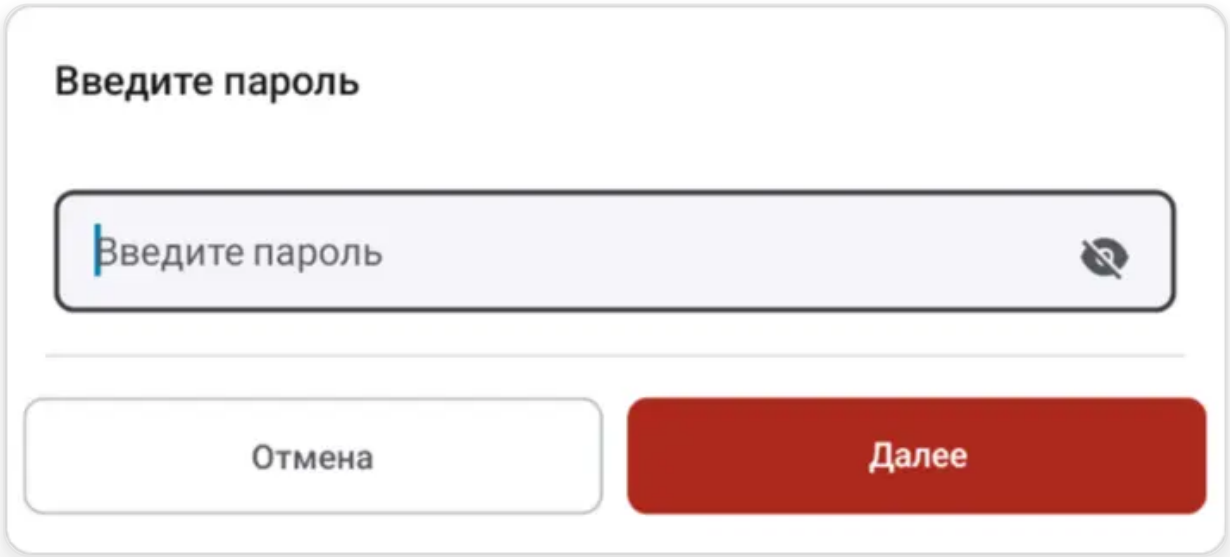
> 💡 **Совет**: Чтобы переключить профиль, нажмите кнопку рядом с его названием и выберите нужный профиль из выпадающего списка.

Шаг 5. Подтверждение и выполнение операции

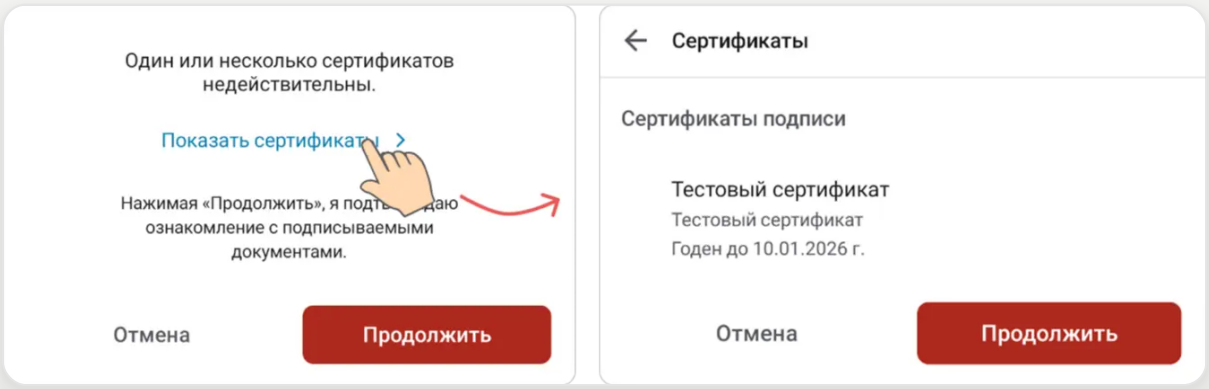
1. Нажмите кнопку **Выполнить** в нижней части окна **Подпись и шифрование**.
2. В окне подтверждения нажмите **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.



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



🚨 Если сертификат недействителен, будет показано предупреждение. Подпись всё равно будет выполнена, но её юридическая значимость может быть оспорена.

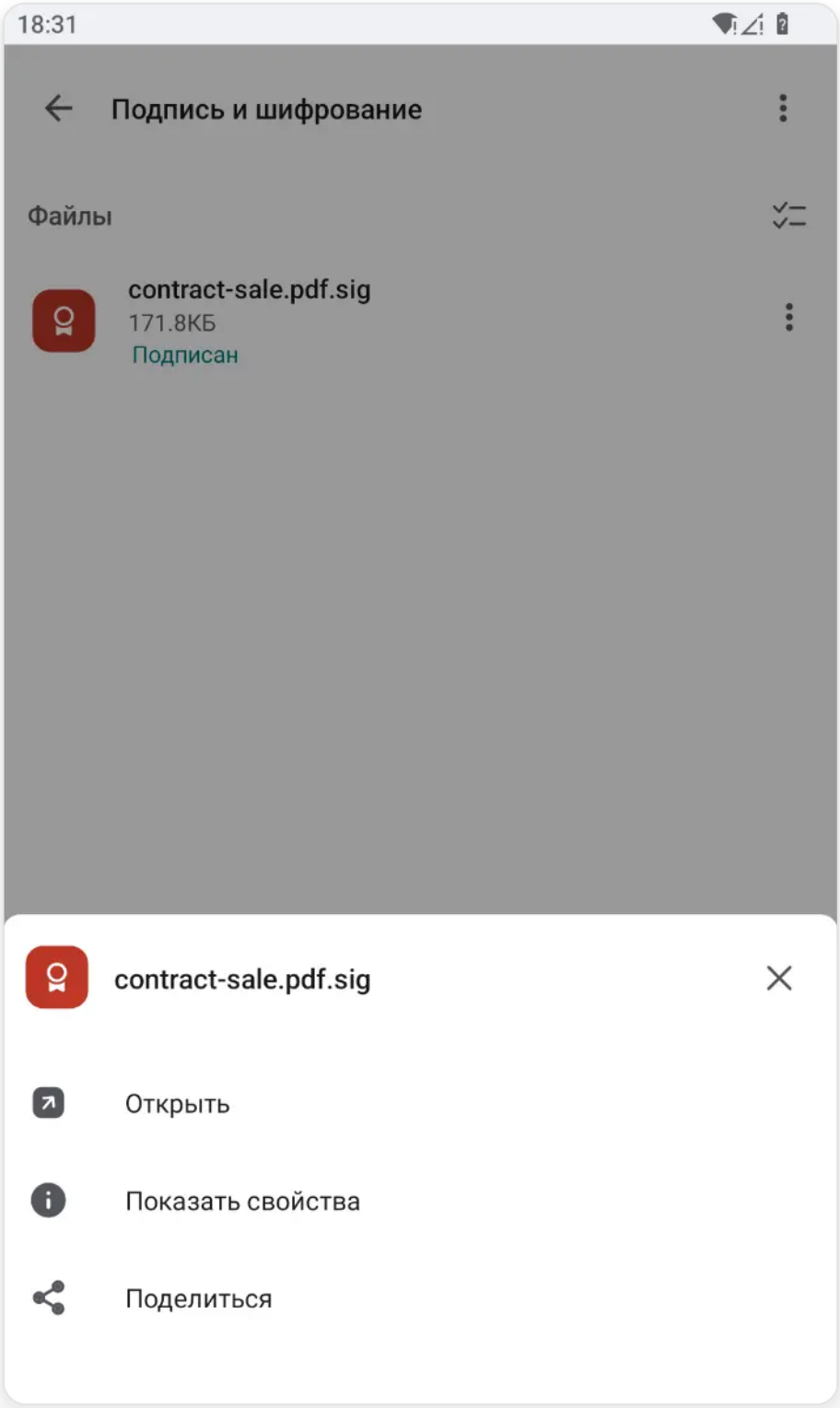


Шаг 6. Результат

Выполнение операции занимает определенное время и зависит от их объема 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 отсоединённая подпись, то в раздел «Документы» помимо файла подписи сохранится копия исходного файла.



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

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
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
Произошла ошибка	Введен неверный пароль для доступа к закрытому ключу	Указан неверный 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.
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	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

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

Шифрование документов

- О шифровании
- Как зашифровать документы
- Возможные ошибки

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.

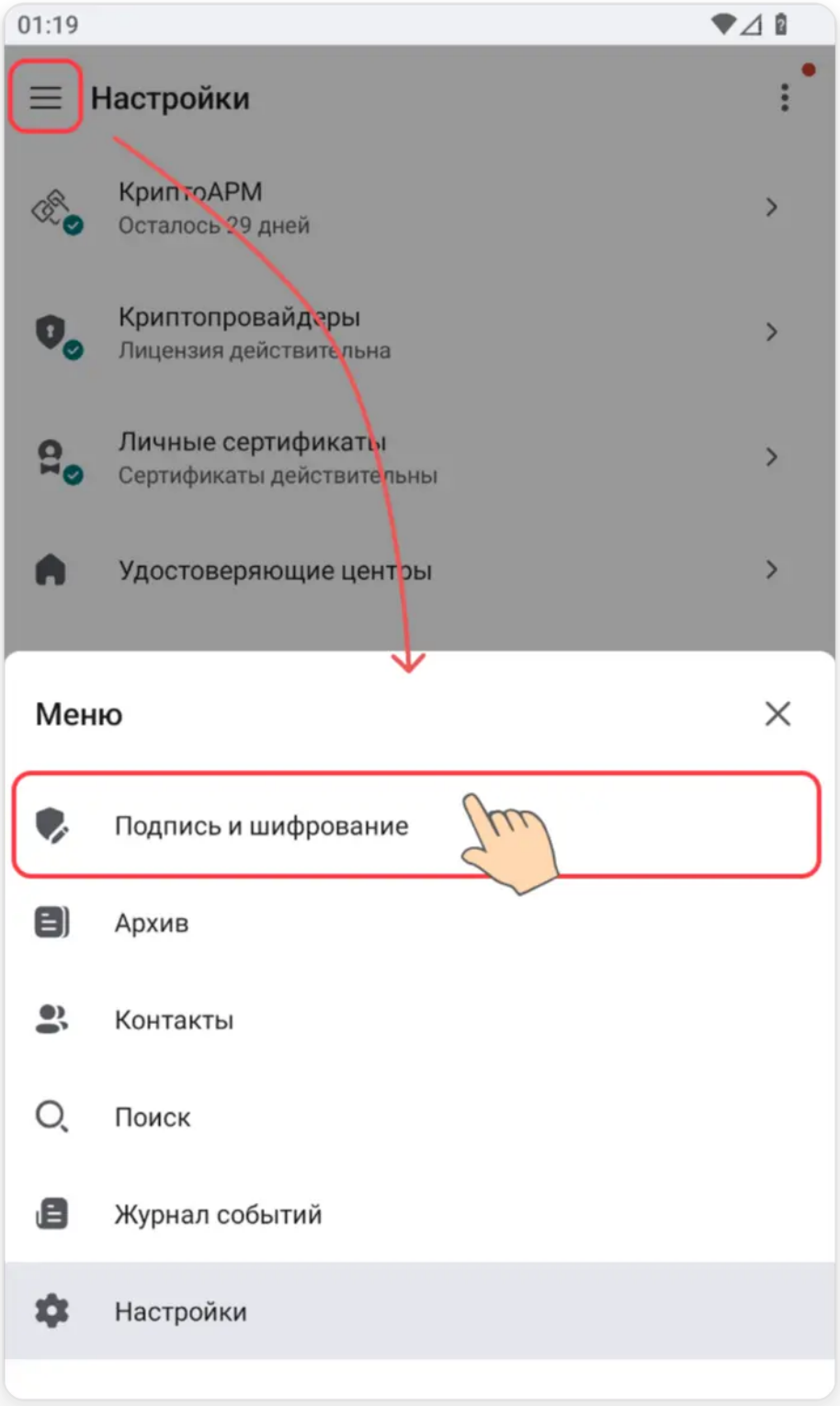
4. Настройки безопасности
   - Убедитесь, что используемые алгоритмы шифрования соответствуют внутренним требованиям организации.
   - Если получатели используют разные криптопровайдеры, проверьте совместимость сертификатов перед шифрованием.

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**.

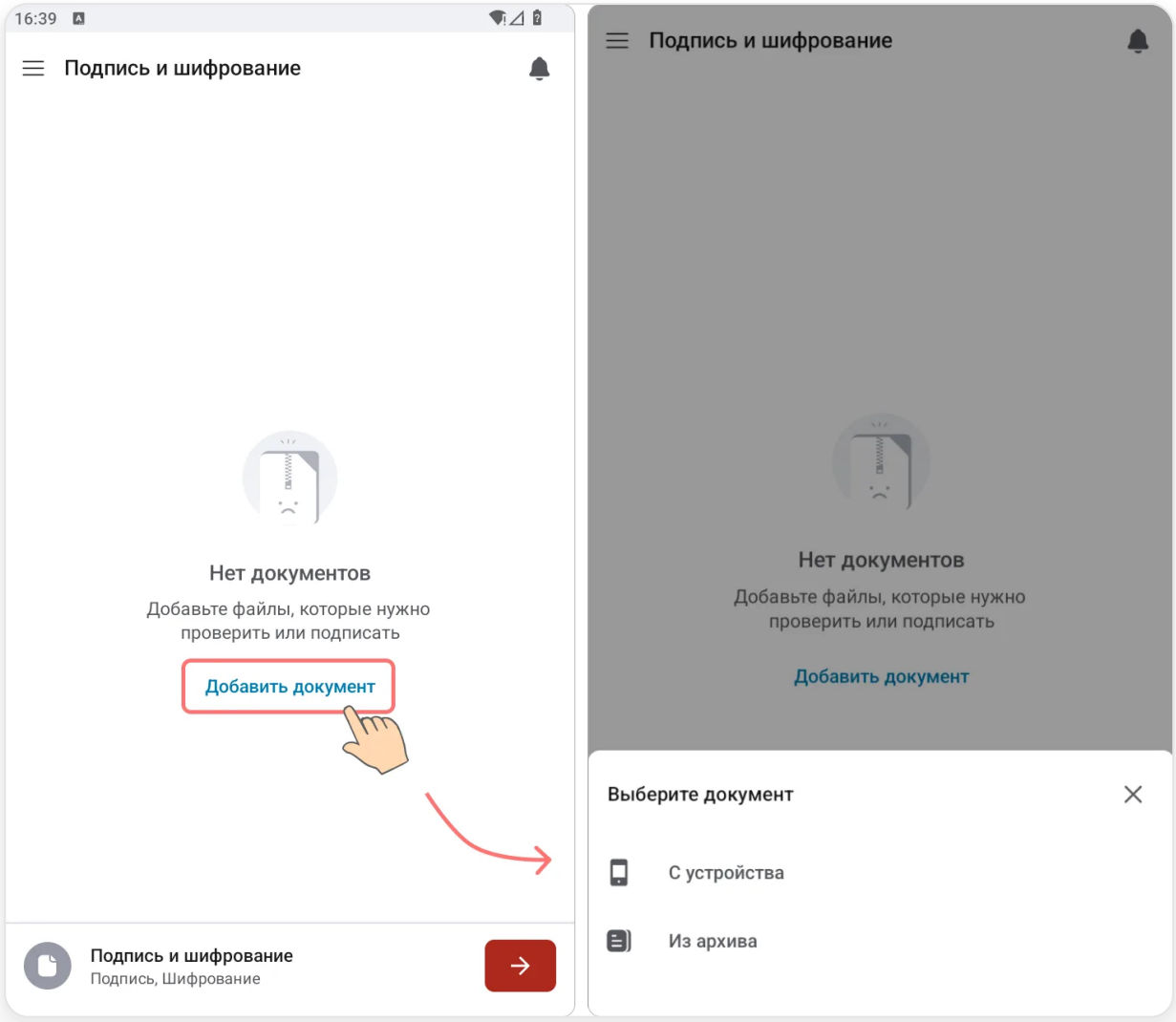


💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

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.

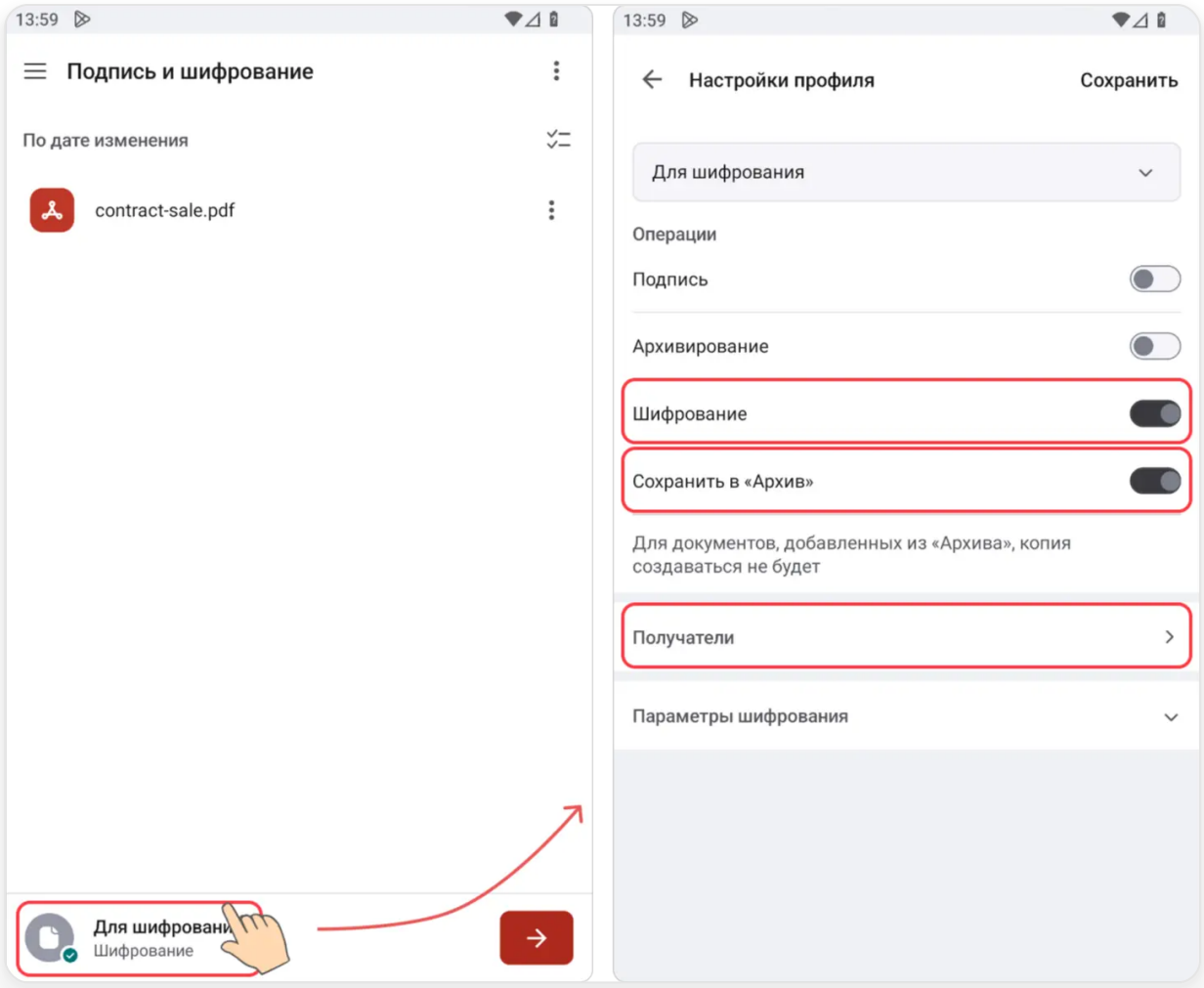
> 💡 **Профиль** — это сохранённый набор настроек подписи. Используя профили, вы можете быстро переключаться между разными сценариями. Подробнее про профили читайте в инструкции Управление профилями.

Чтобы изменить настройки профиля:

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

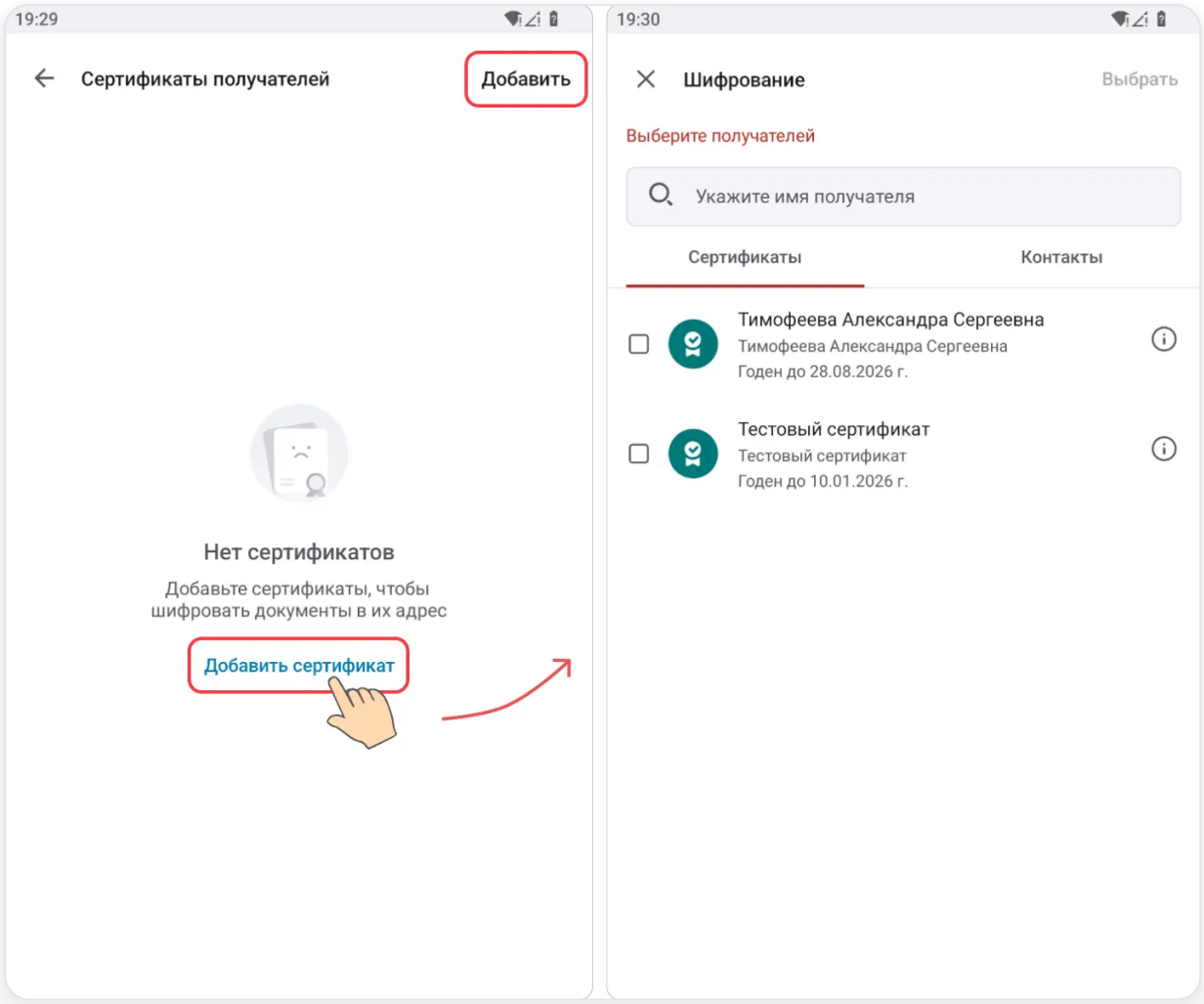
    > 💡 **Совет**: Для создания одного зашифрованного архива включите **Архивирование** — все файлы будут помещены в архив и зашифрованы.

    - 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

Проверка подписи

- О проверке подписи
- Проверка подписи документа
- Проверка подписи документа с соподписями
- Распространенные проблемы
- Печать отчета о проверке подписи
- Возможные ошибки

О проверке подписи

Проверка подписи документа — это процесс, который подтверждает подлинность электронной подписи, использованной для подписания документа. Это крайне важно для того, чтобы документ обладал юридической силой и был достоверным.

Успешная проверка подписи подтверждает авторство документа и гарантирует, что после его подписания в текст не вносились никакие изменения.

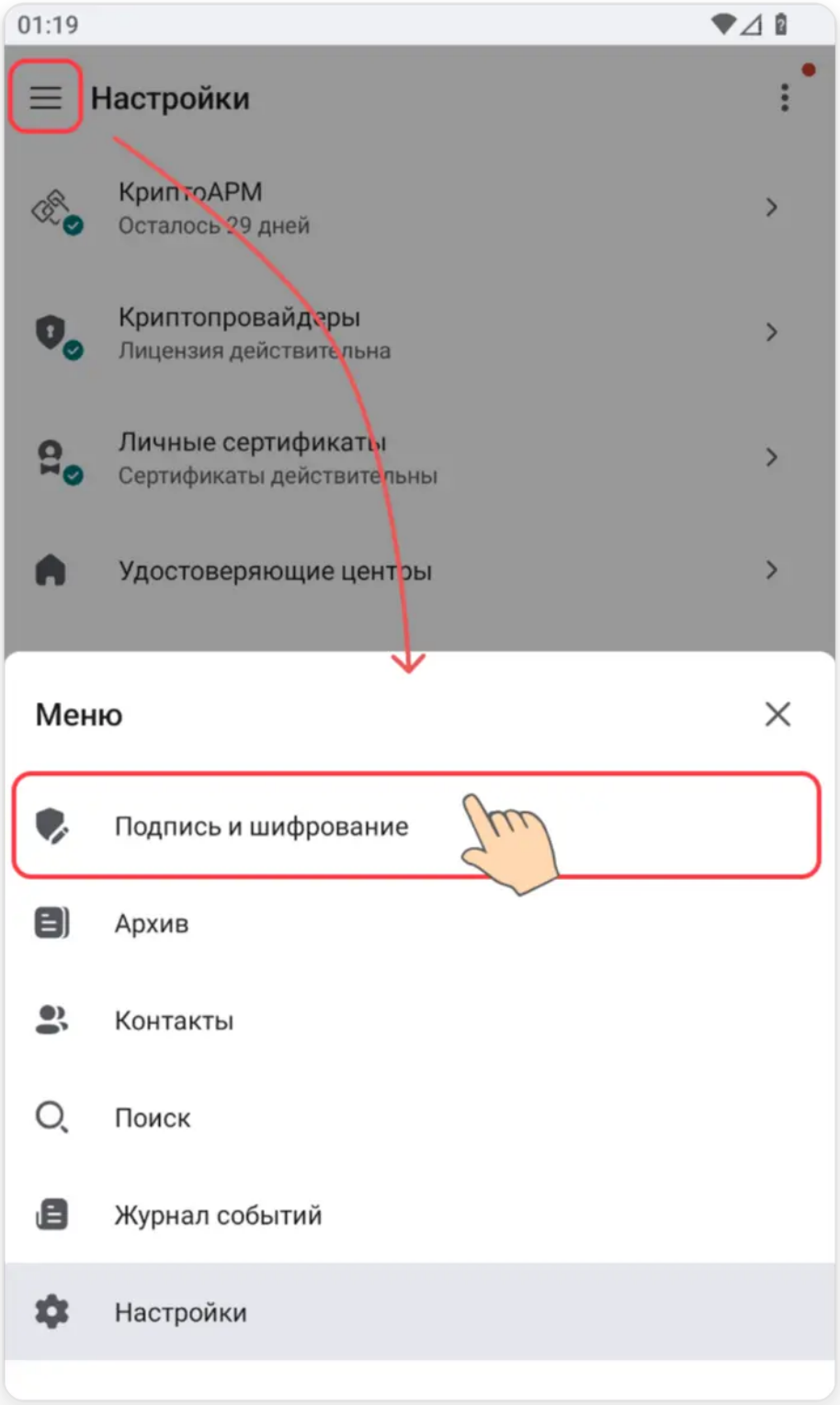
В КриптоАРМ поддерживается проверка подписи для файлов с расширением `.sig`, `.p7s`, `.sgn`, `.sign`, `.bin` с ГОСТ алгоритмами.

> 💡 **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 , размещенной в верхнем левом углу окна приложения.
2. Выберите пункт **Подпись и шифрование**.

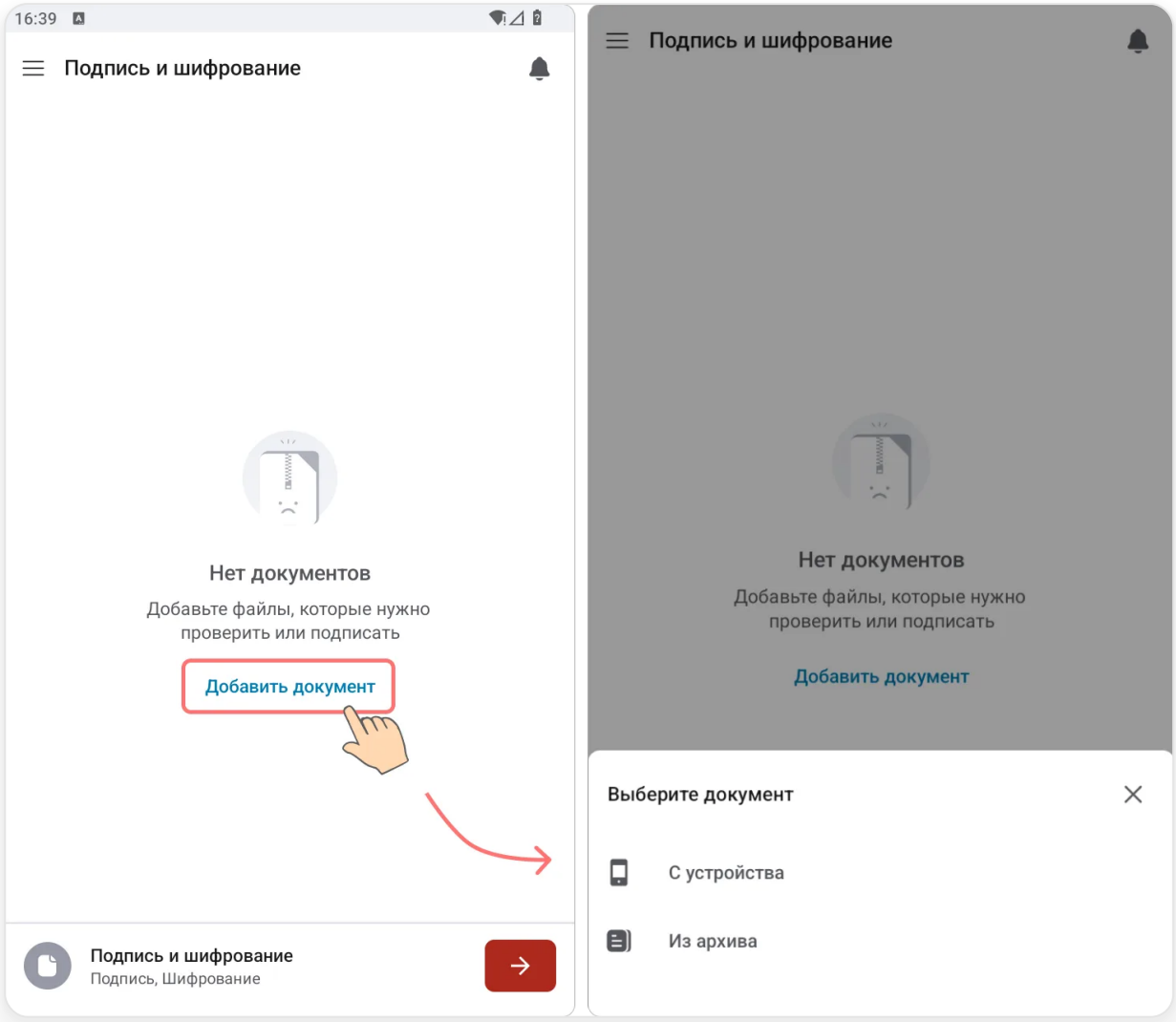


💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

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**.

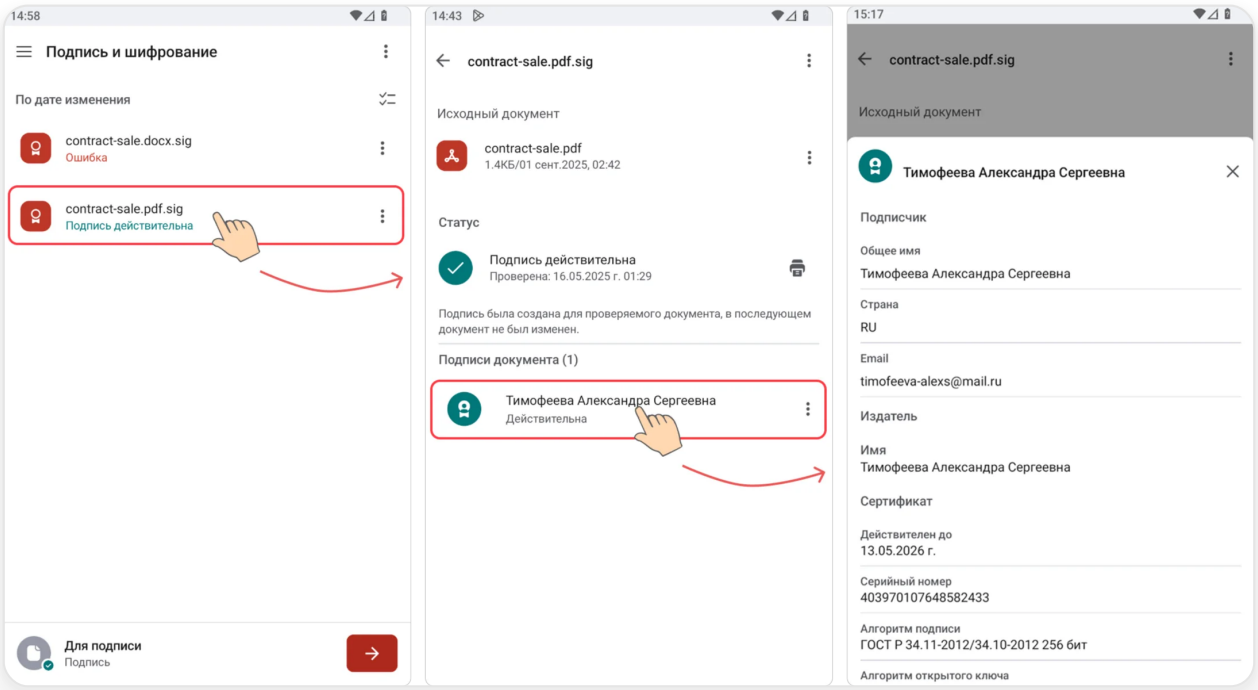
Шаг 3. Результаты проверки

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 её не удалось проверить.

> 💡 **Совет**: 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.

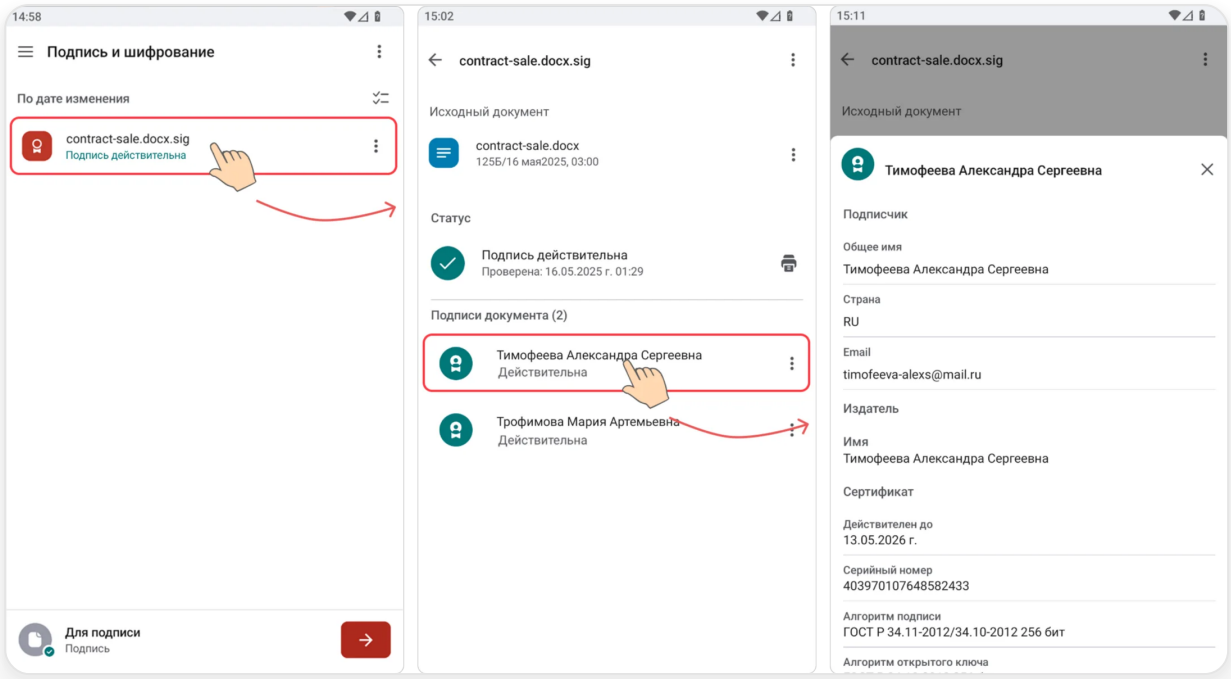


Проверка подписи документа с соподписями

> 🚨 **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 истёк или сертификат отозван	❌ Невозможно исправить	Запросите новый документ, подписанный действующим сертификатом
Документ изменён 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

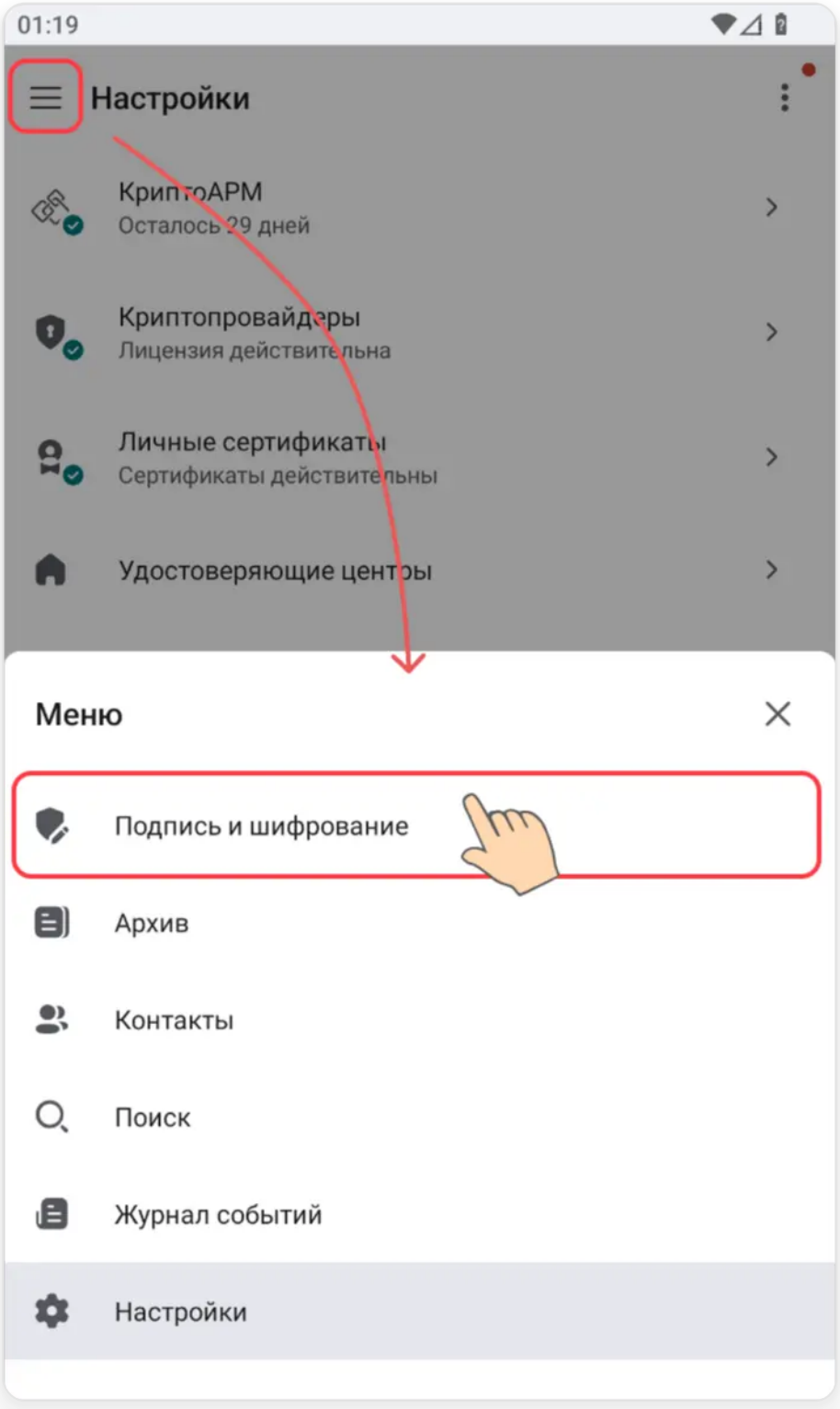
Снятие подписи

- Снятие подписи с документа
- Возможные ошибки

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**.

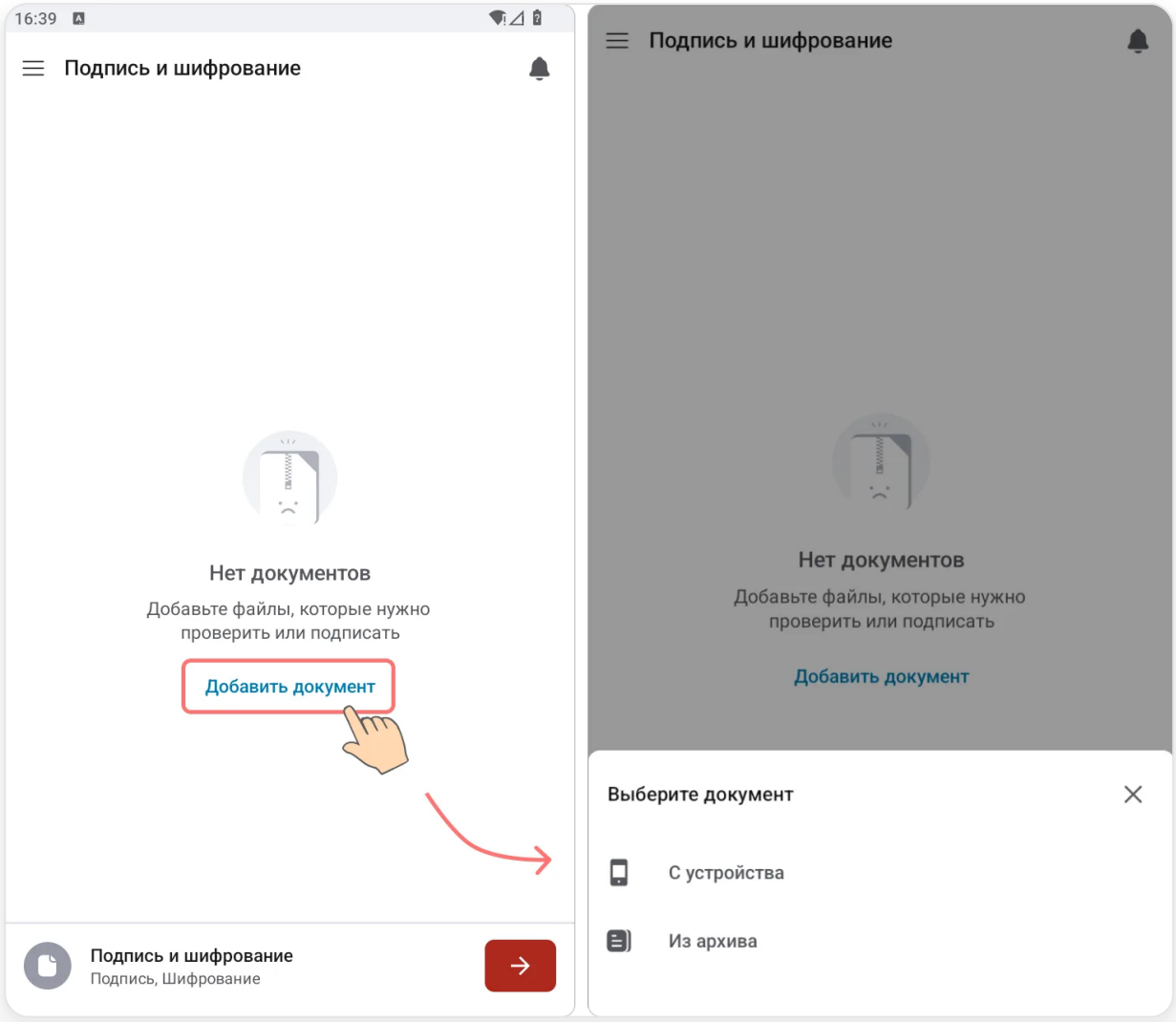


💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

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**.



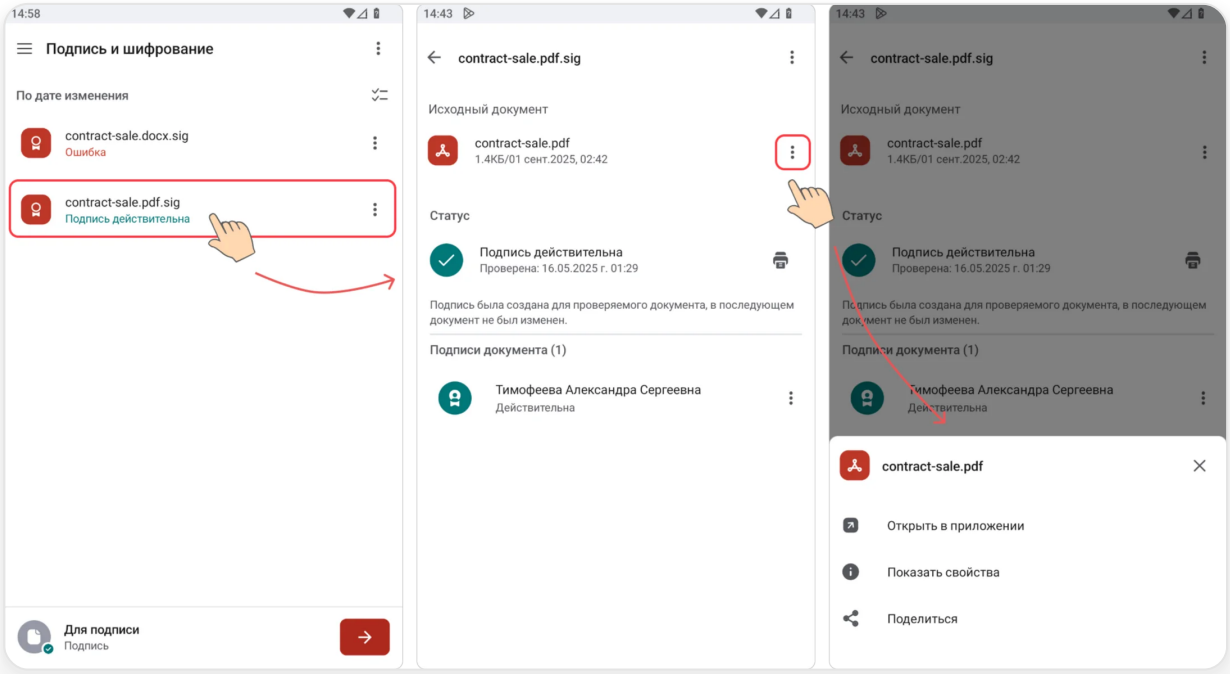
Из сторонних приложений

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

Расшифрование документов

- 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.

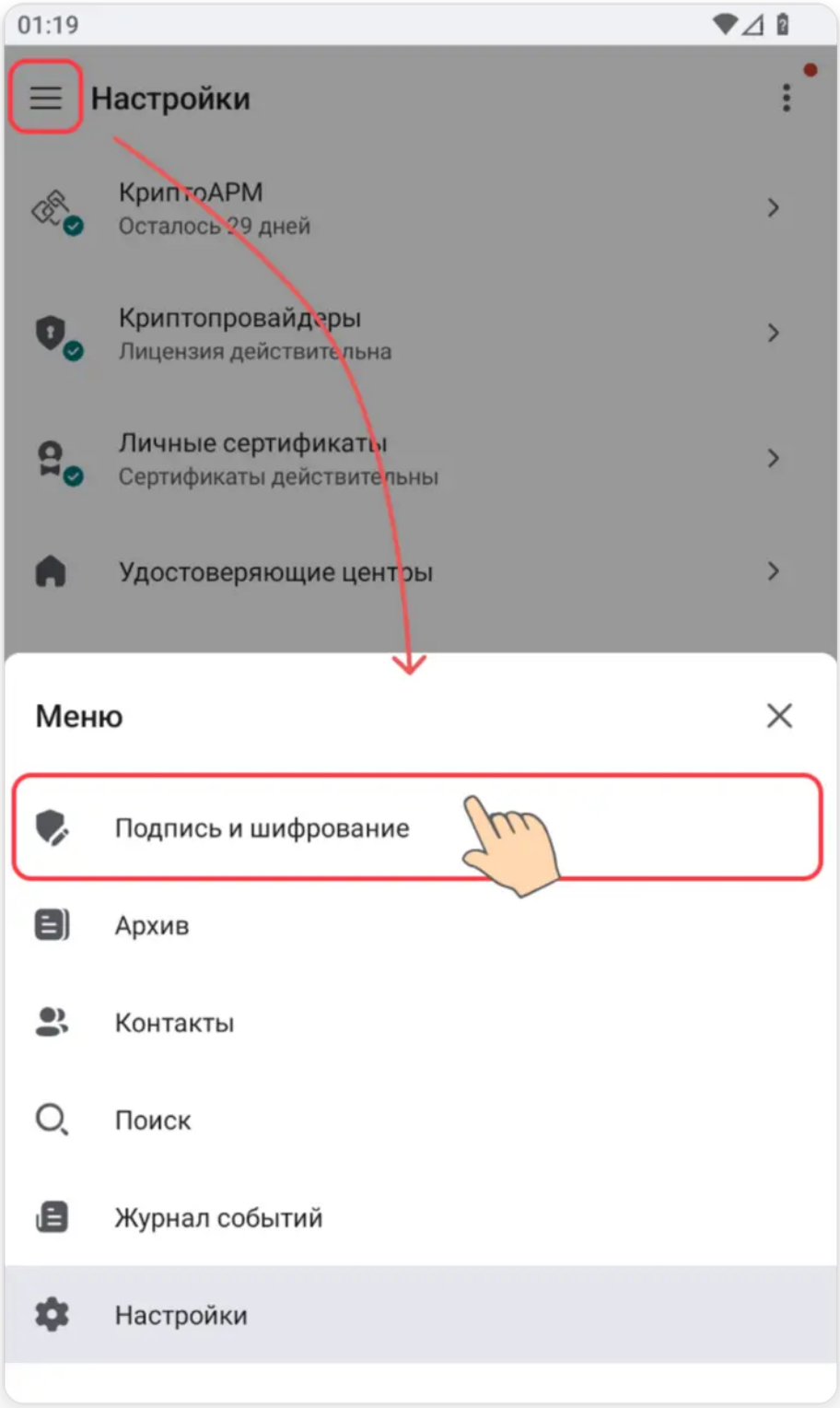
1. **Проверьте лицензии**: убедитесь в наличии действующих лицензий на КриптоАРМ и КриптоПро CSP. Без действующих лицензий расшифровать документ невозможно. Подробнее про лицензии читайте в инструкции Лицензирование.
2. **Установите личный сертификат**: в хранилище **Личные сертификаты** должен быть 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**.

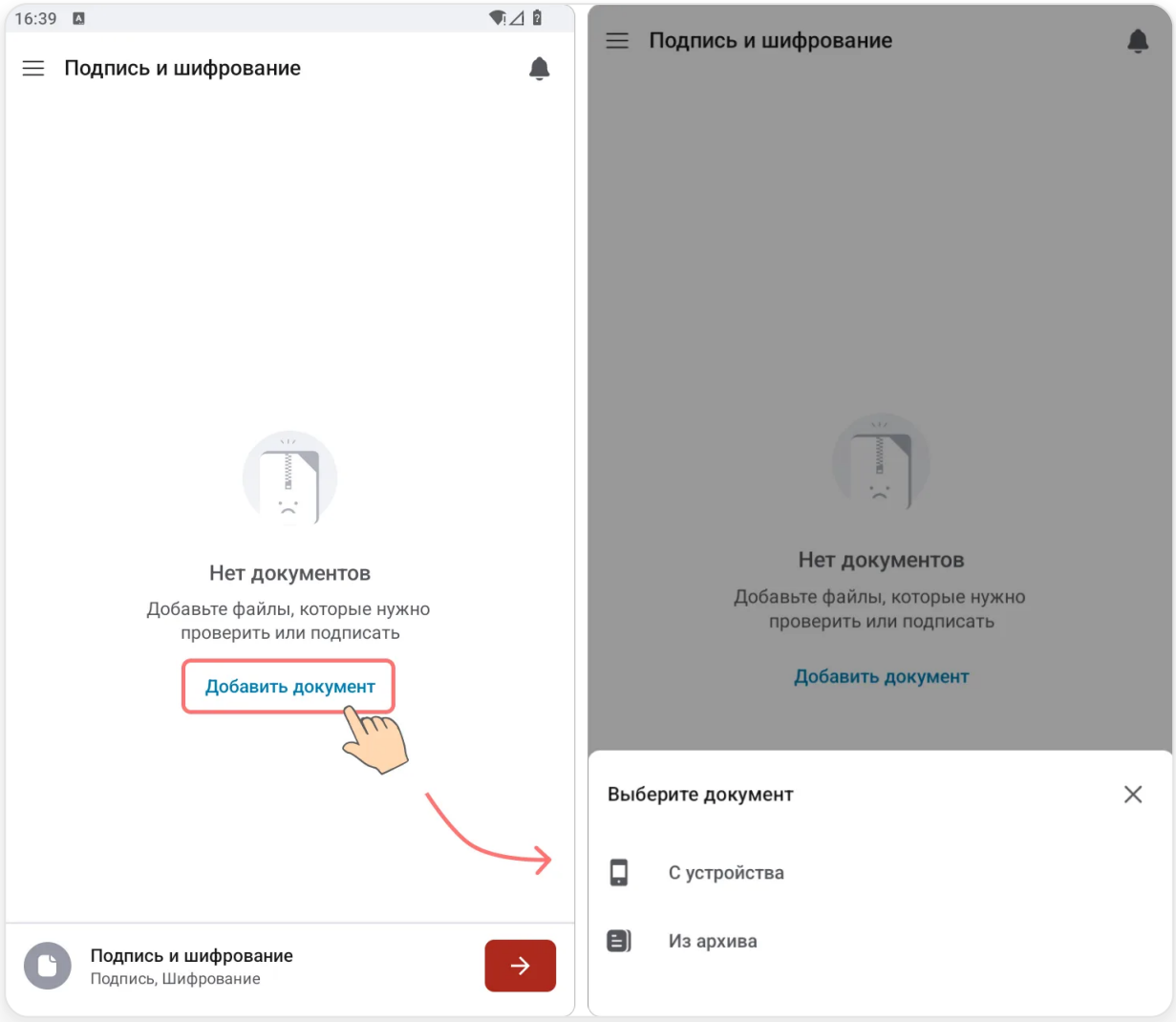


💡 **Совет**: Перейти в мастер можно из раздела **Архив** с помощью действия **Открыть** для одного или нескольких файлов, либо с помощью действия **Добавить документ**.

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**.



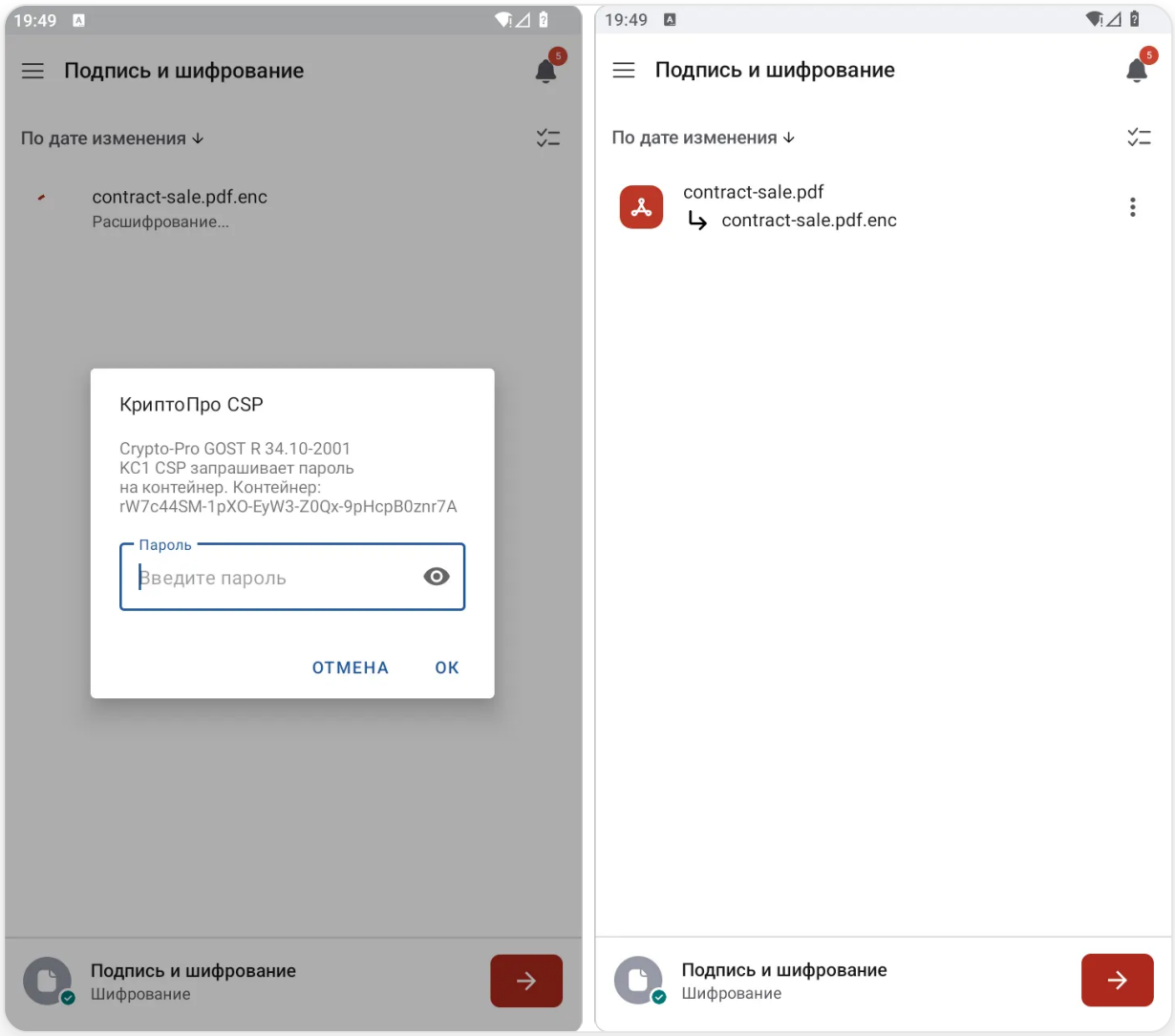
Из сторонних приложений

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

Действия с документами

- Для чего нужна папка «Архив»?
- Доступные действия

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:

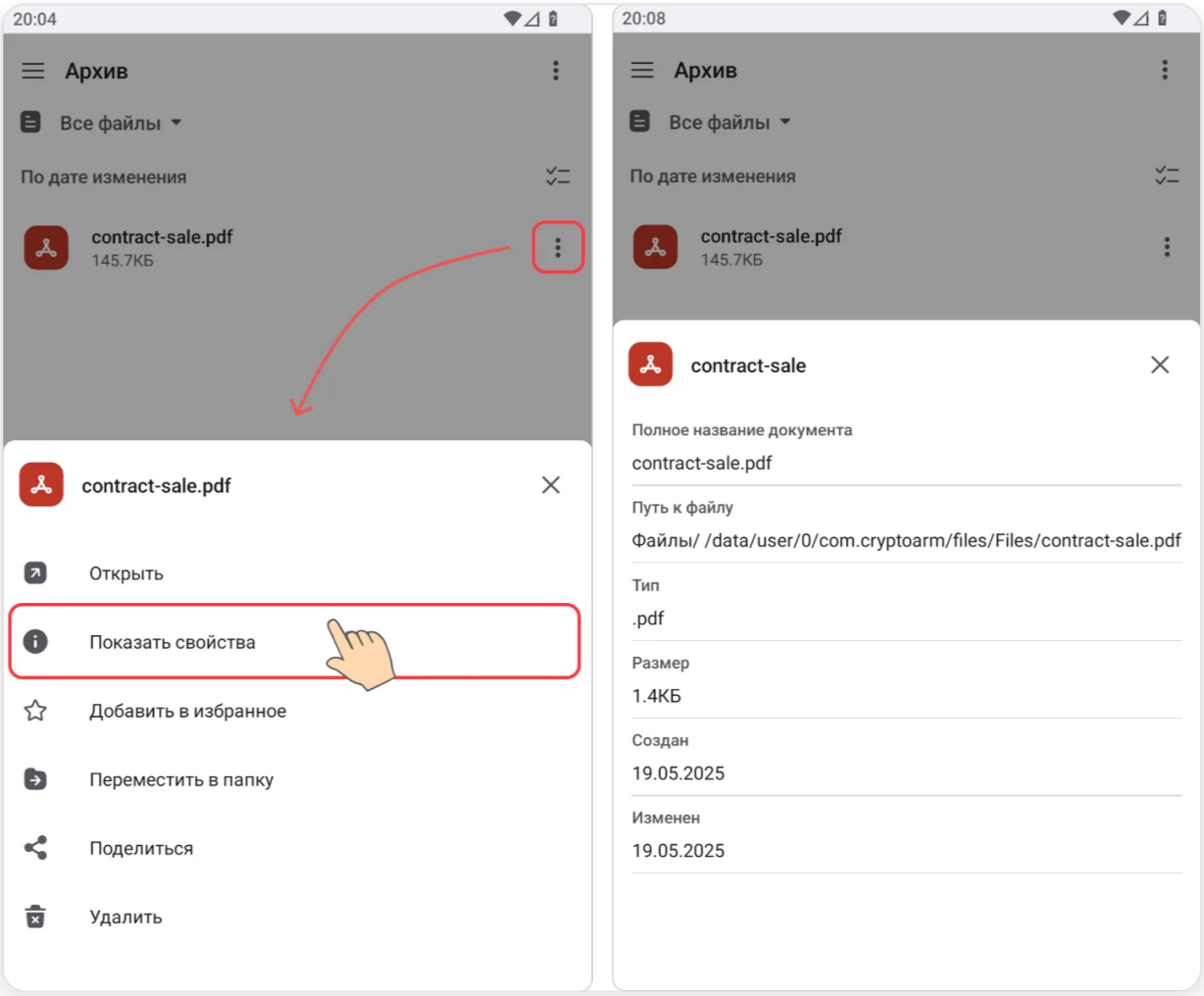
1. При создании отсоединённой подписи в **Архив** сохраняется:
    - Файл подписи,
    - Копия исходного документа.
2. Промежуточные файлы операций не сохраняются.
3. В профиле подписи можно настроить действия при соподписи документов из **Архива**.

Доступные действия

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

Просмотр свойств

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий по кнопке **Еще** , размещенной на панели с файлом.
3. В открывшемся меню действий выберите действие **Показать свойства**.
4. Откроется окно со свойствами файла.

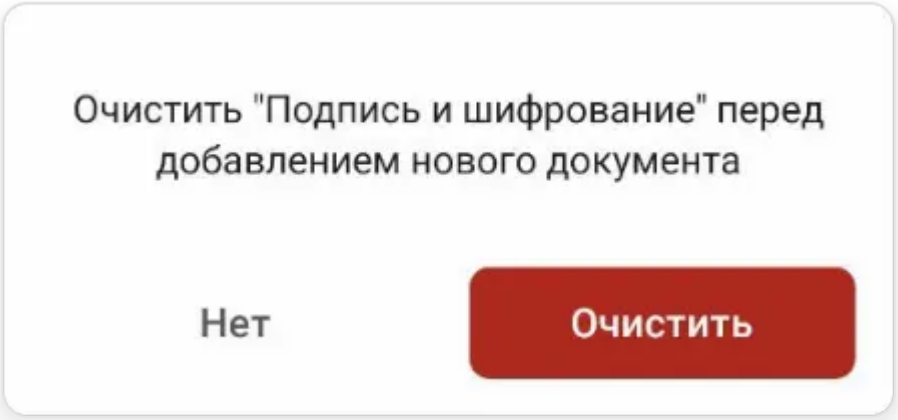


> 💡 **Совет**:

> Чтобы открыть документ, добавьте его в мастер **Подписи и шифрование** и выберите **Открыть в приложении** из меню действий по кнопке **Еще** ⋮.
> Для документов с присоединенной подписью откройте окно с информацией о подписи и выберите **Открыть в приложении** для исходного документа.

Добавление в мастер

1. Перейдите в раздел **Архив**.
2. Выполните одно из следующих действий:
   - Нажмите на панель с файлом.
   - Нажмите на кнопку **Еще** ⋮, расположенную на панели с файлом, и выберите действие **Открыть**.
3. Если в мастере уже есть документы, выберите, нужно ли очистить список перед добавлением нового документа.



4. Файл откроется в мастере **Подпись и шифрование**.

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, которое доступно по кнопке **Еще** ⋮, размещенной на панели с документом.
3. В появившемся меню выберите действие **Добавить в избранное**.

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

> 🔍 Подробнее про группы читайте в инструкции Группировка документов.

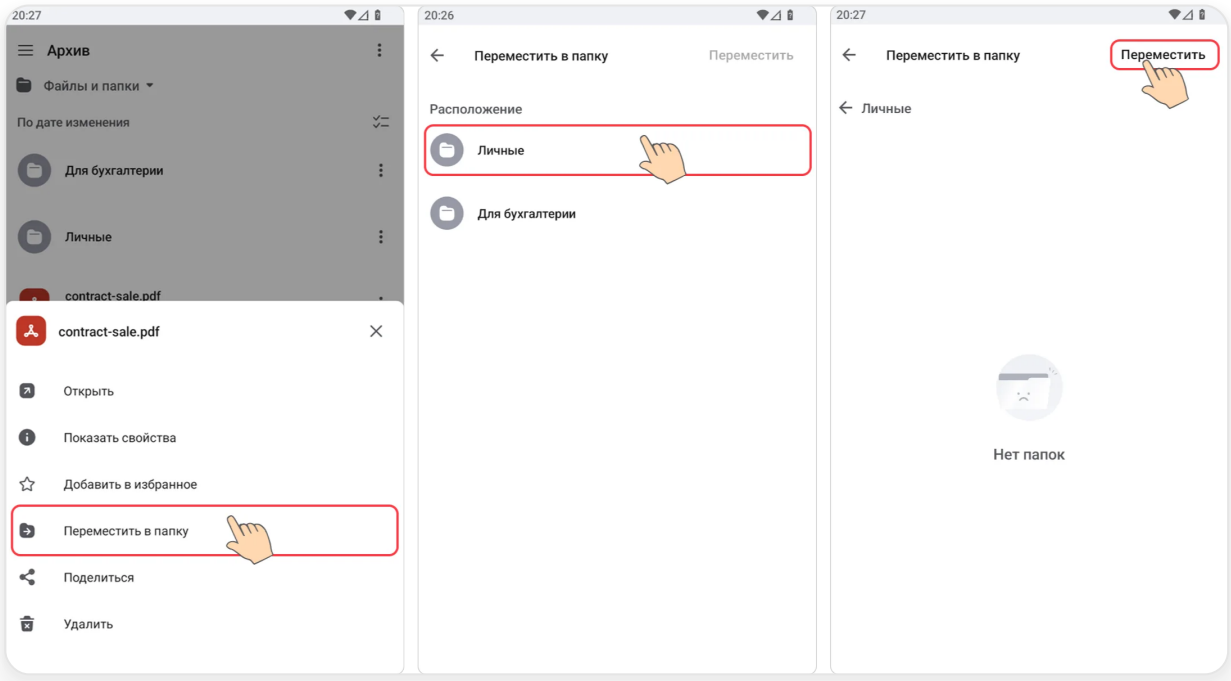
Удаление из избранного

1. Откройте раздел **Архив**.
2. Вызовите меню **Действия**, которое доступно по кнопке **Еще** , размещенной на панели с документом в списке.
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, которое доступно по кнопке **Еще** , размещенной на панели с документов в списке.
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

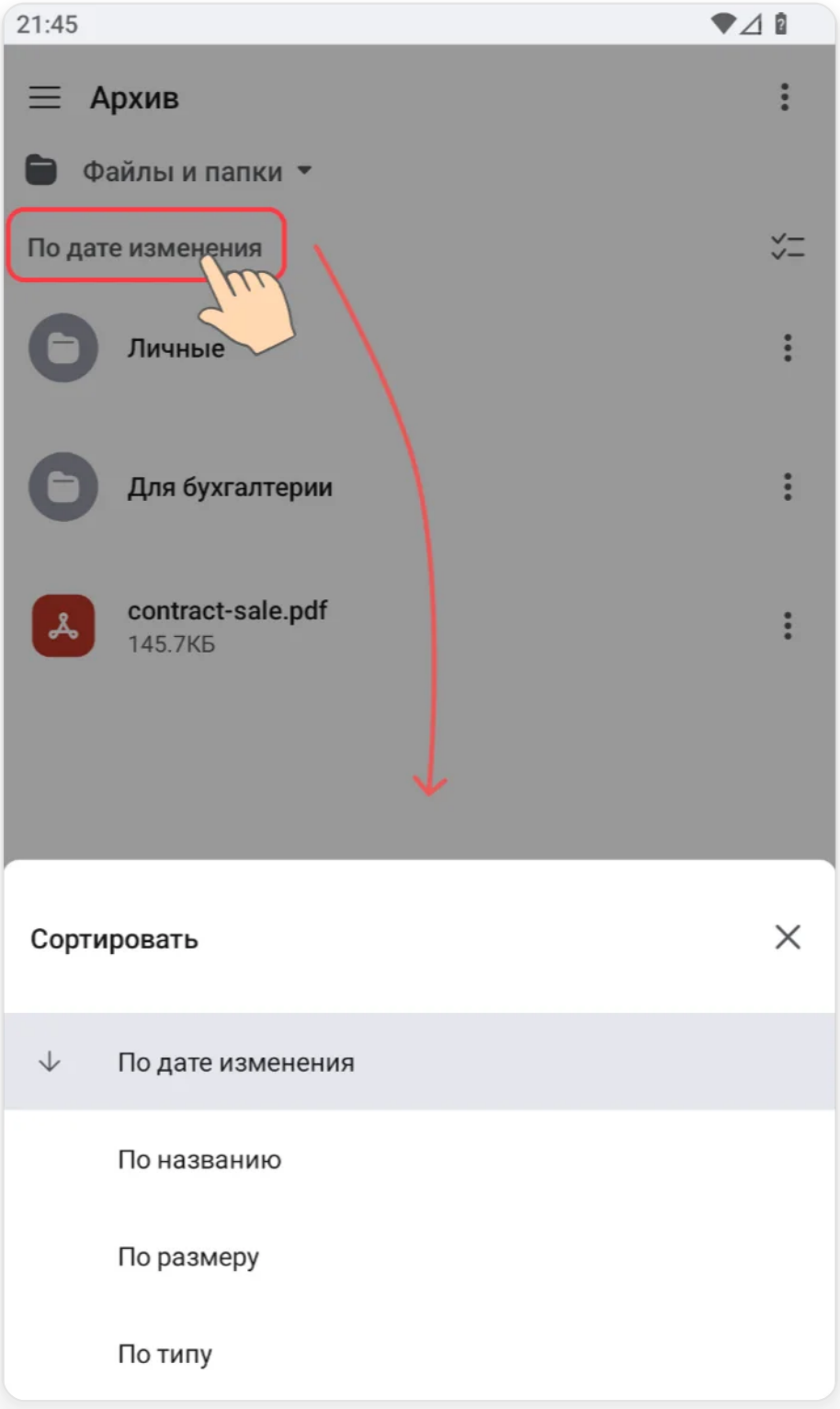
> 🚨 **Примечание**: Документы удаляются без возможности восстановления.

1. Перейдите в раздел **Архив**.
2. Вызовите меню действий, которое доступно по кнопке **Еще** , размещенной на панели с документом в списке.
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

Открыть статью на сайте

Группировка документов

- Общая информация
- Создание папки
- Действия с папками

Общая информация

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

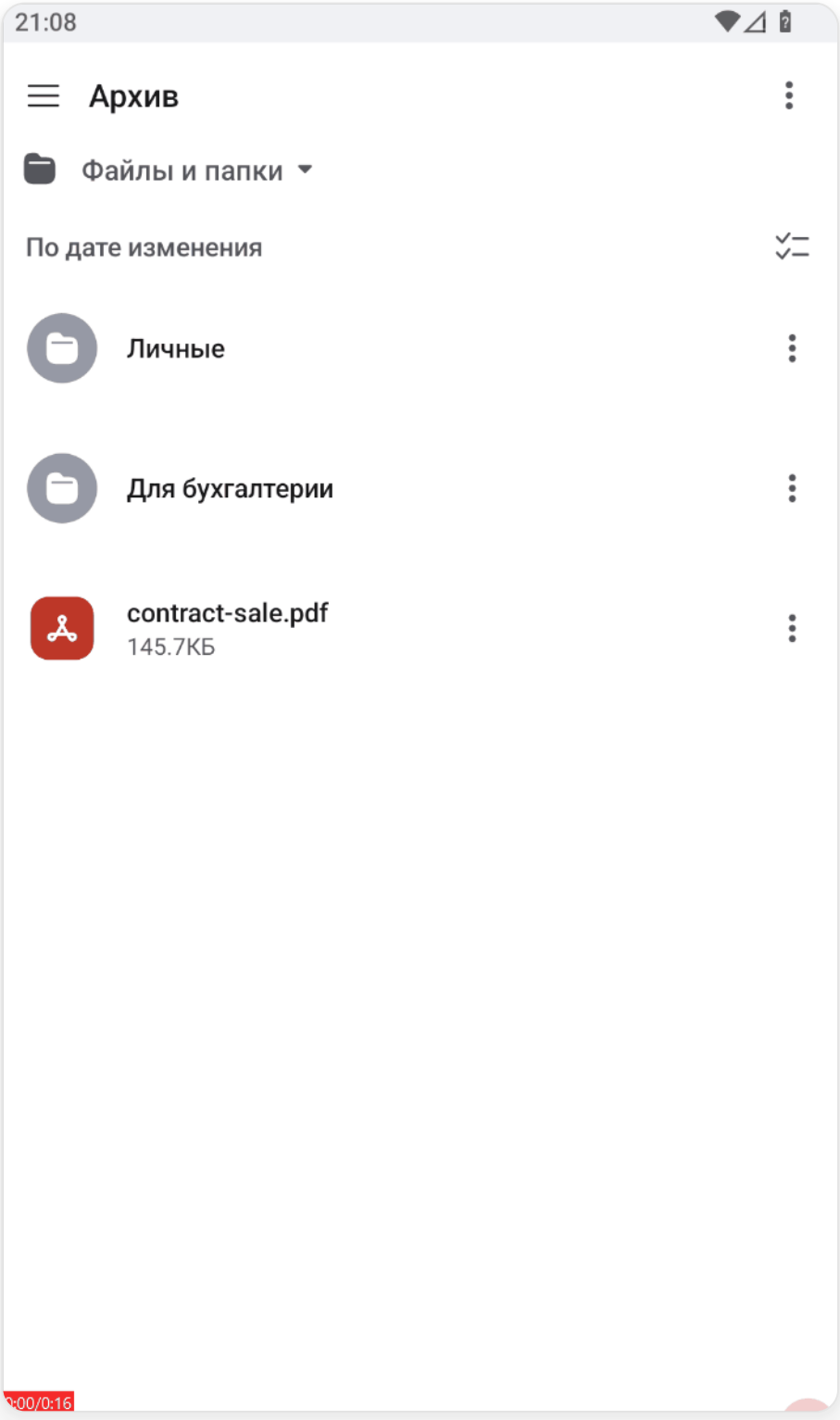
После установки в приложении доступны следующие папки:

- **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 неё `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**.

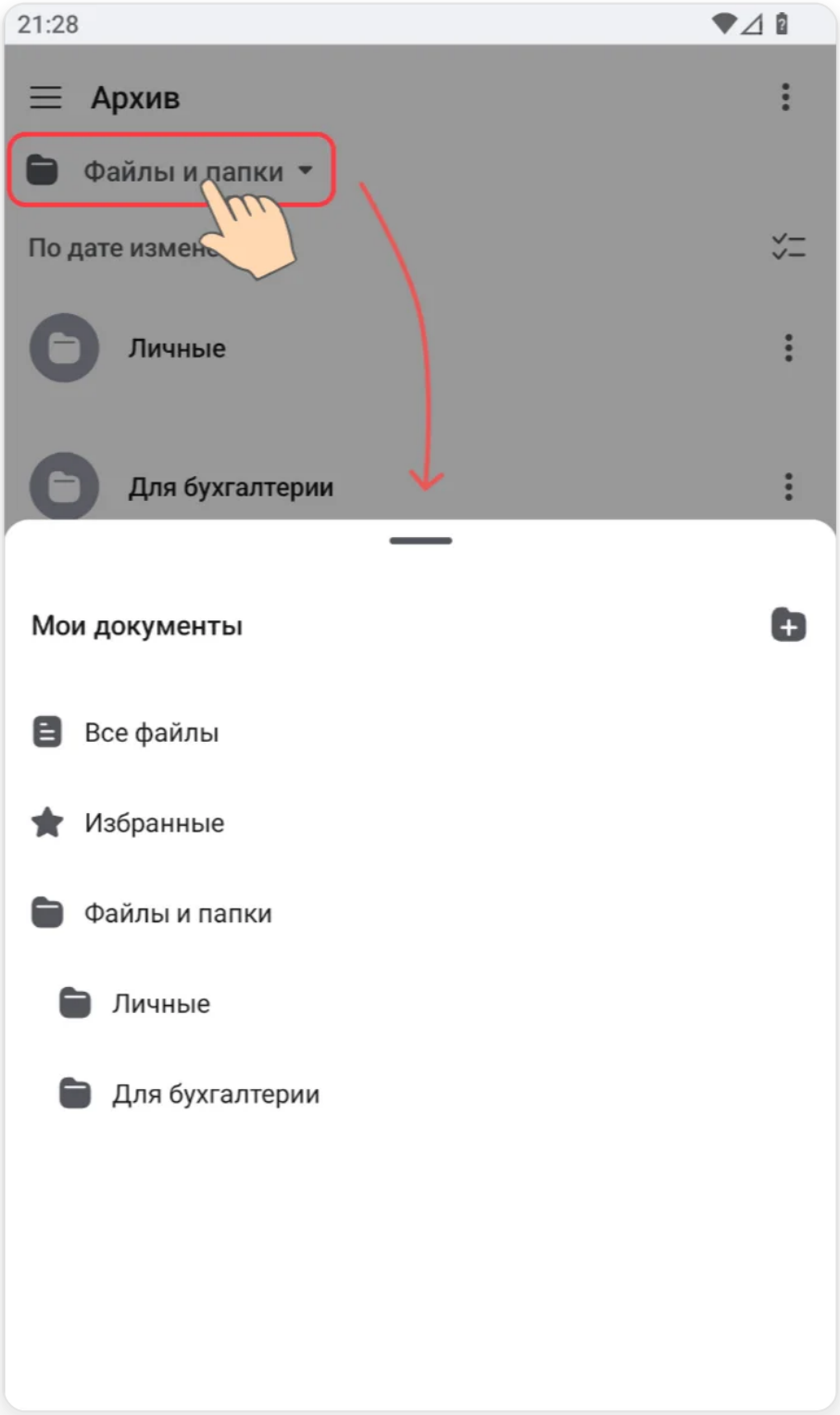

21:08
Архив
Файлы и папки
По дате изменения
Личные
Для бухгалтерии
contract-sale.pdf
145.7КБ
0:00/0:16

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.

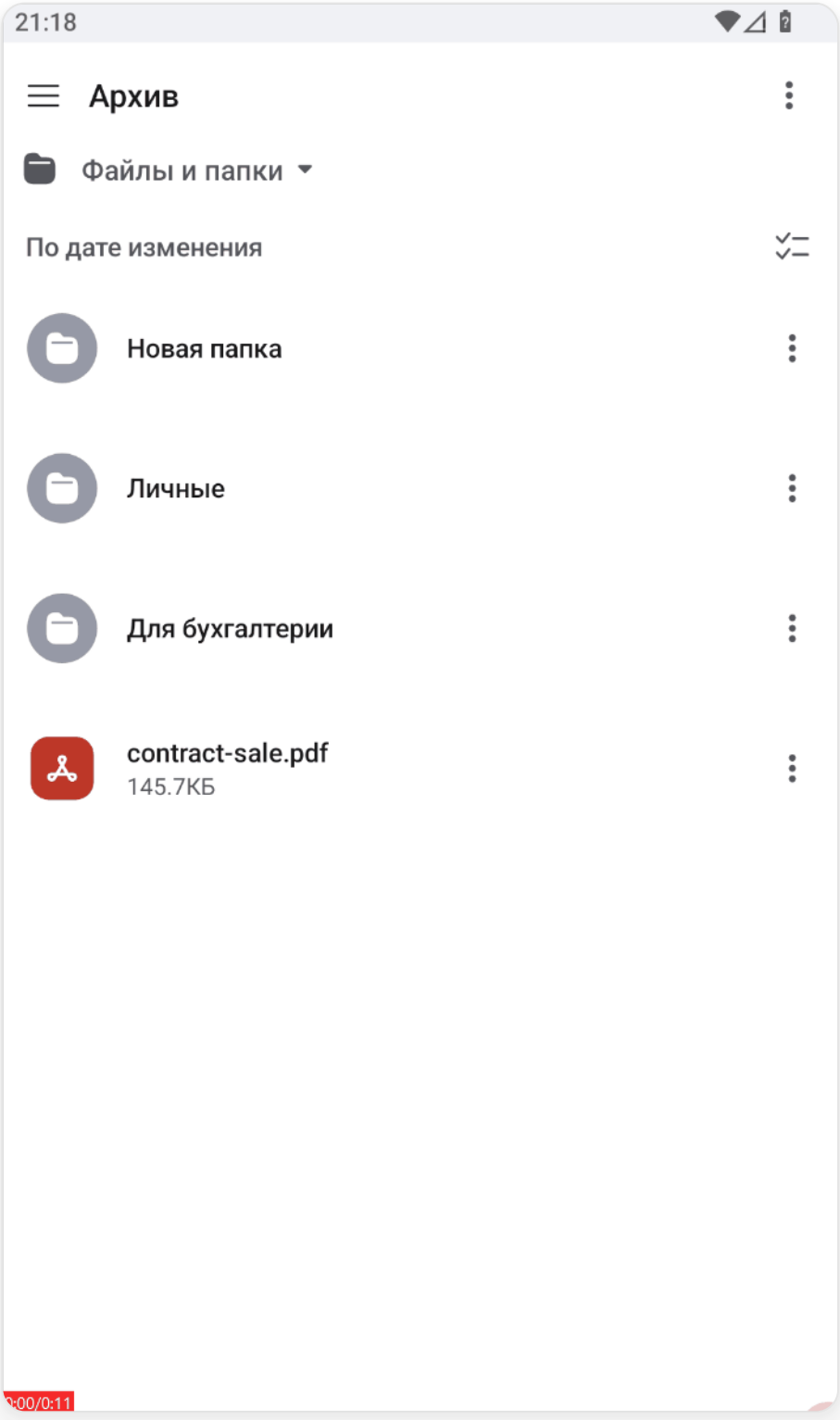
1. Открытие списка папок

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



2. Перемещение папки

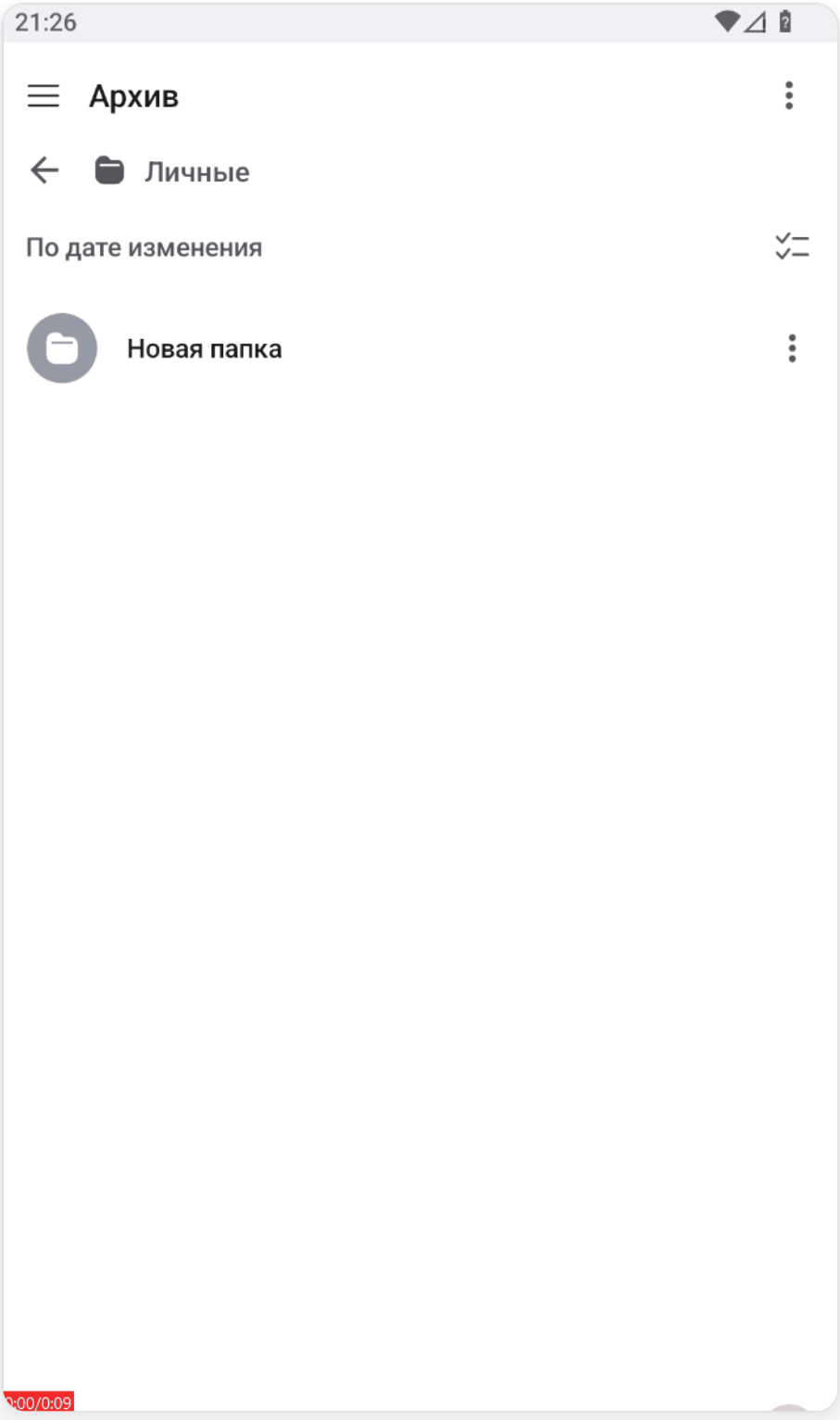
1. Откройте раздел **Архив**.
2. Вызовите меню действий по кнопке **Еще** , размещенной на панели с папкой.
3. В появившемся меню выберите действие **Переместить в папку**.
4. В открывшемся окне выберите папку и нажмите **Переместить**.


21:18
Архив
Файлы и папки
По дате изменения
Новая папка
Личные
Для бухгалтерии
contract-sale.pdf
145.7КБ

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

Открыть статью на сайте

Создание контакта

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

Добавление нового контакта

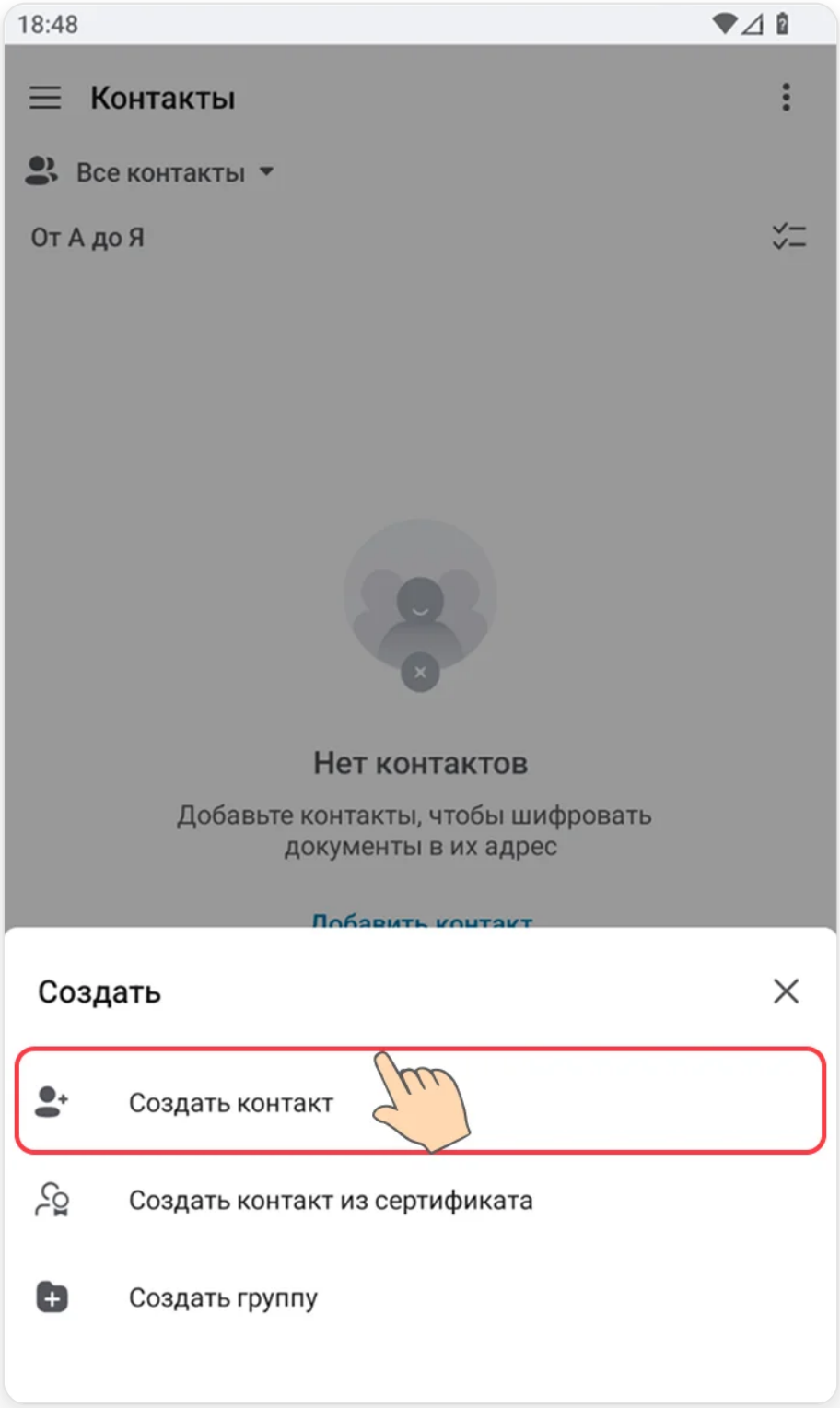
В КриптоАРМ можно создать контакт с расширенным профилем, который будет включать:

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

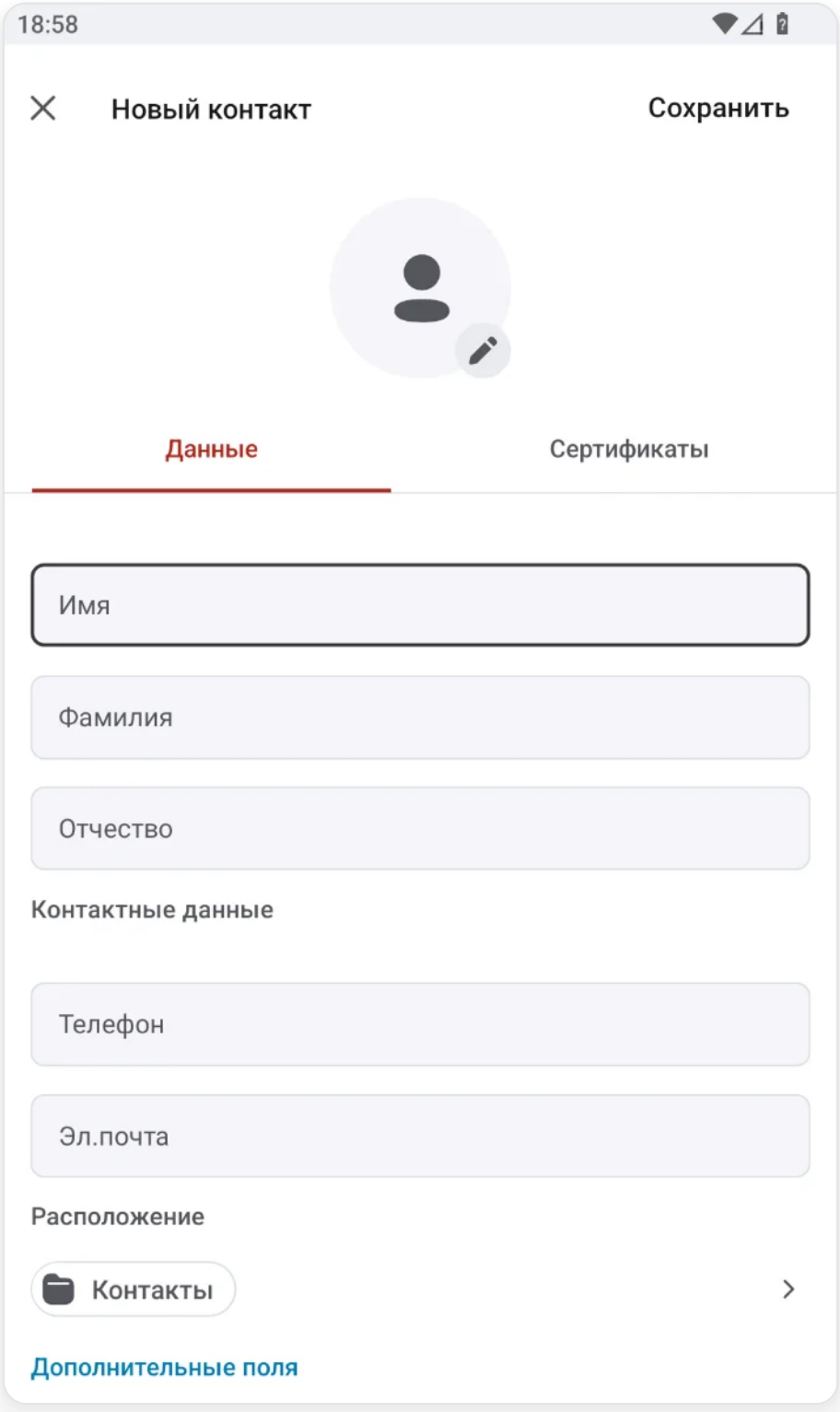
> 💡 **Совет**: Сертификаты используются для шифрования файлов в адрес контакта.

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**.



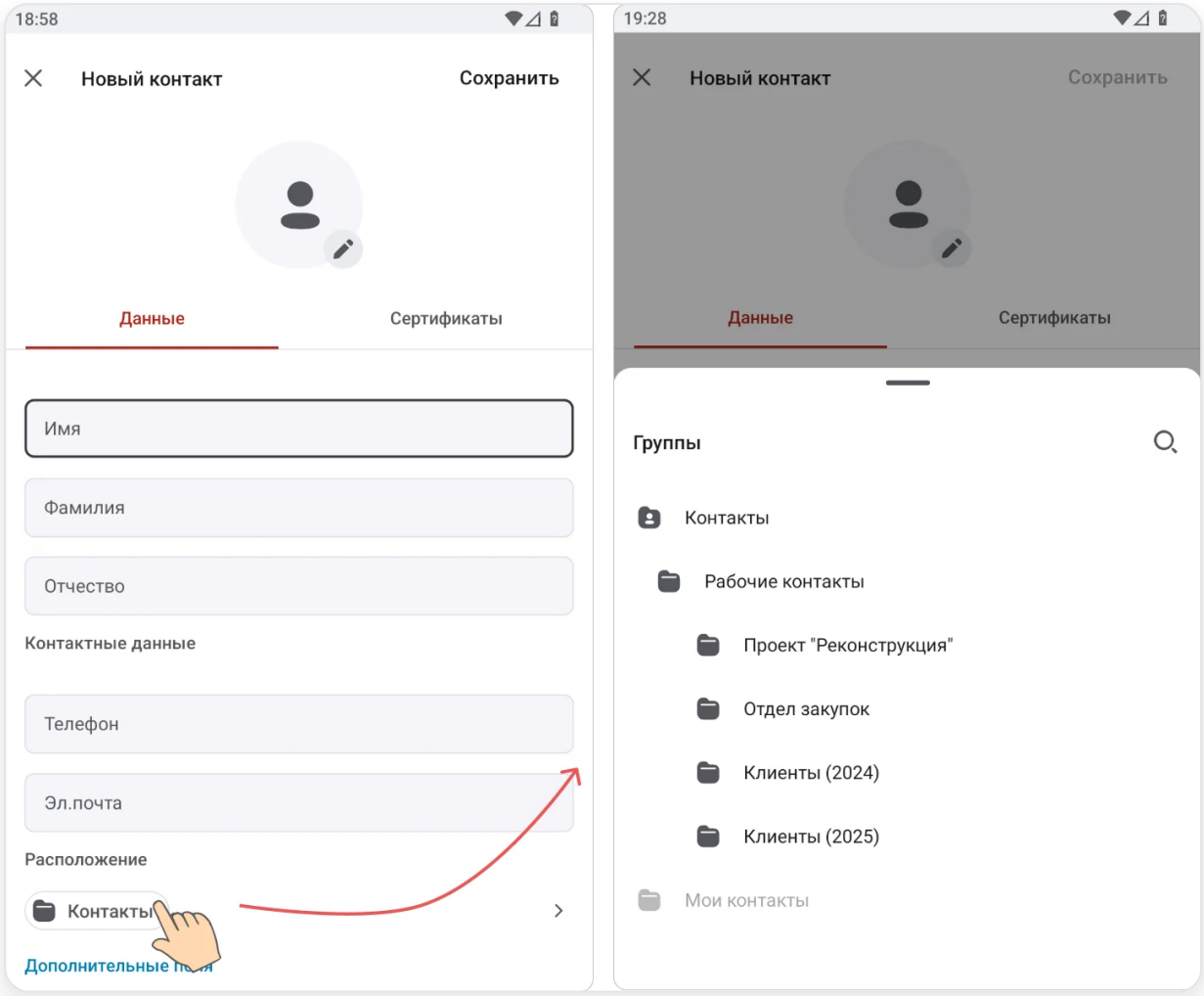
4. Откроется форма создания контакта.



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

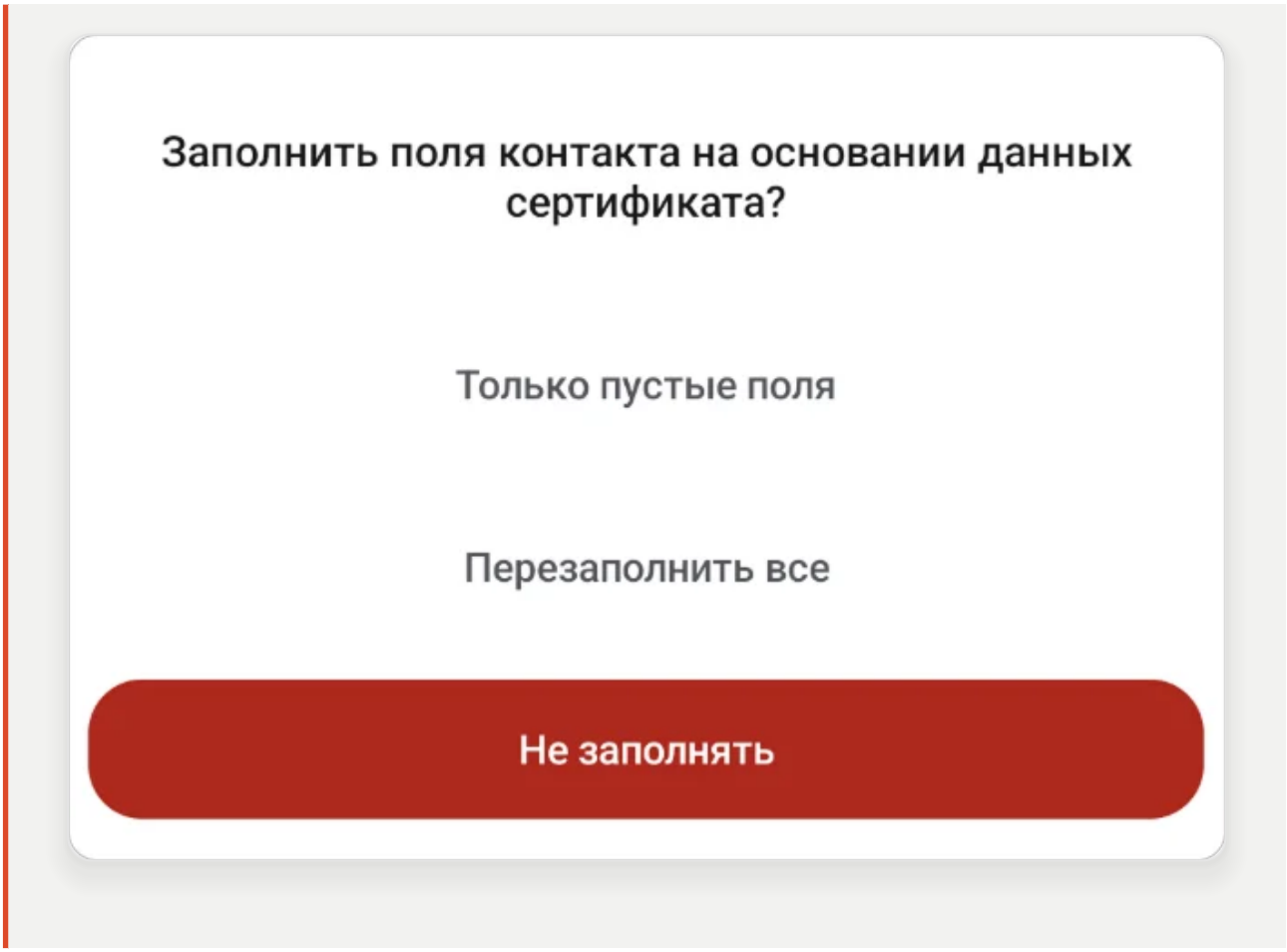
6. Заполните сведения о контакте на вкладке **Данные**.

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.



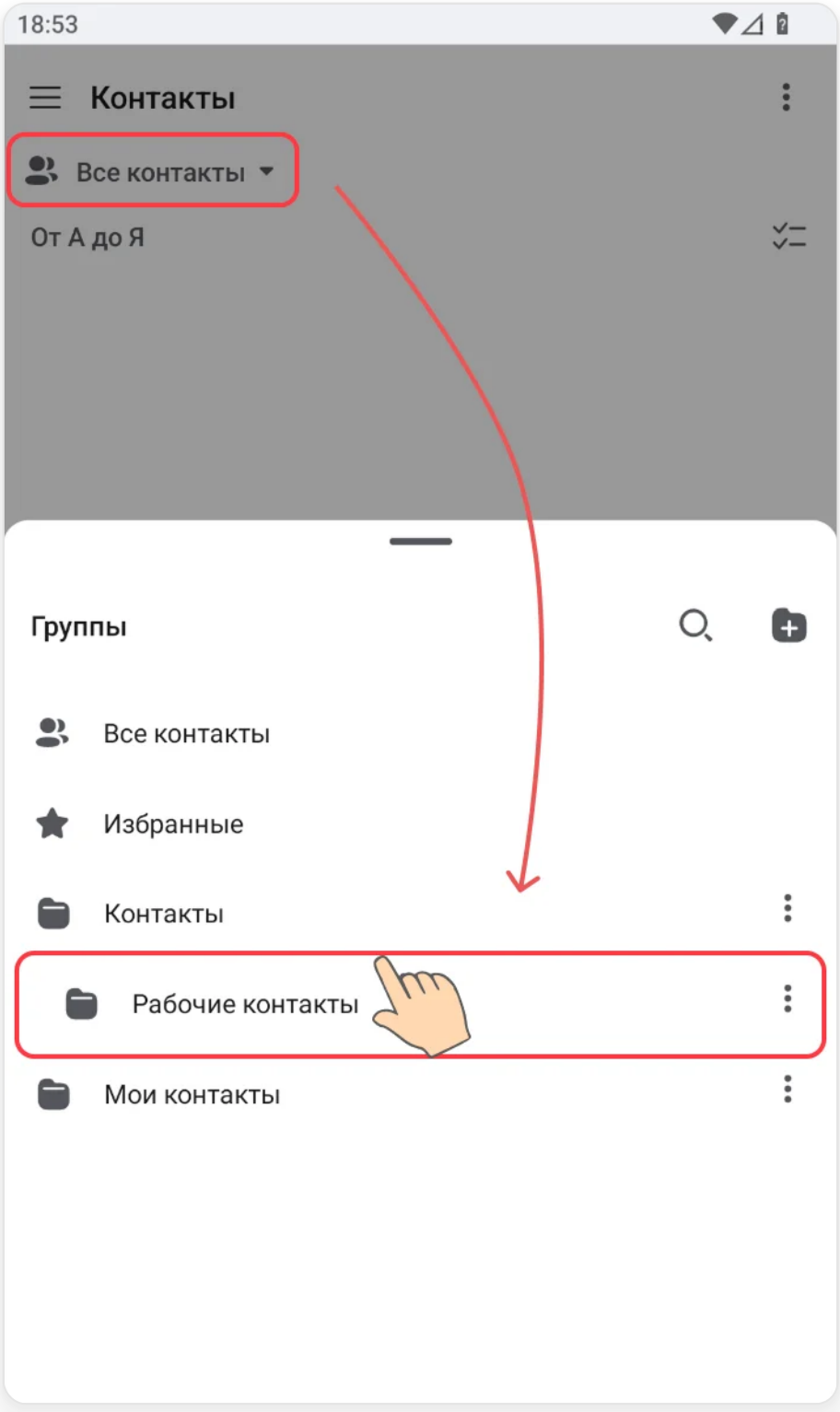
9. Нажмите на **Сохранить**.

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.

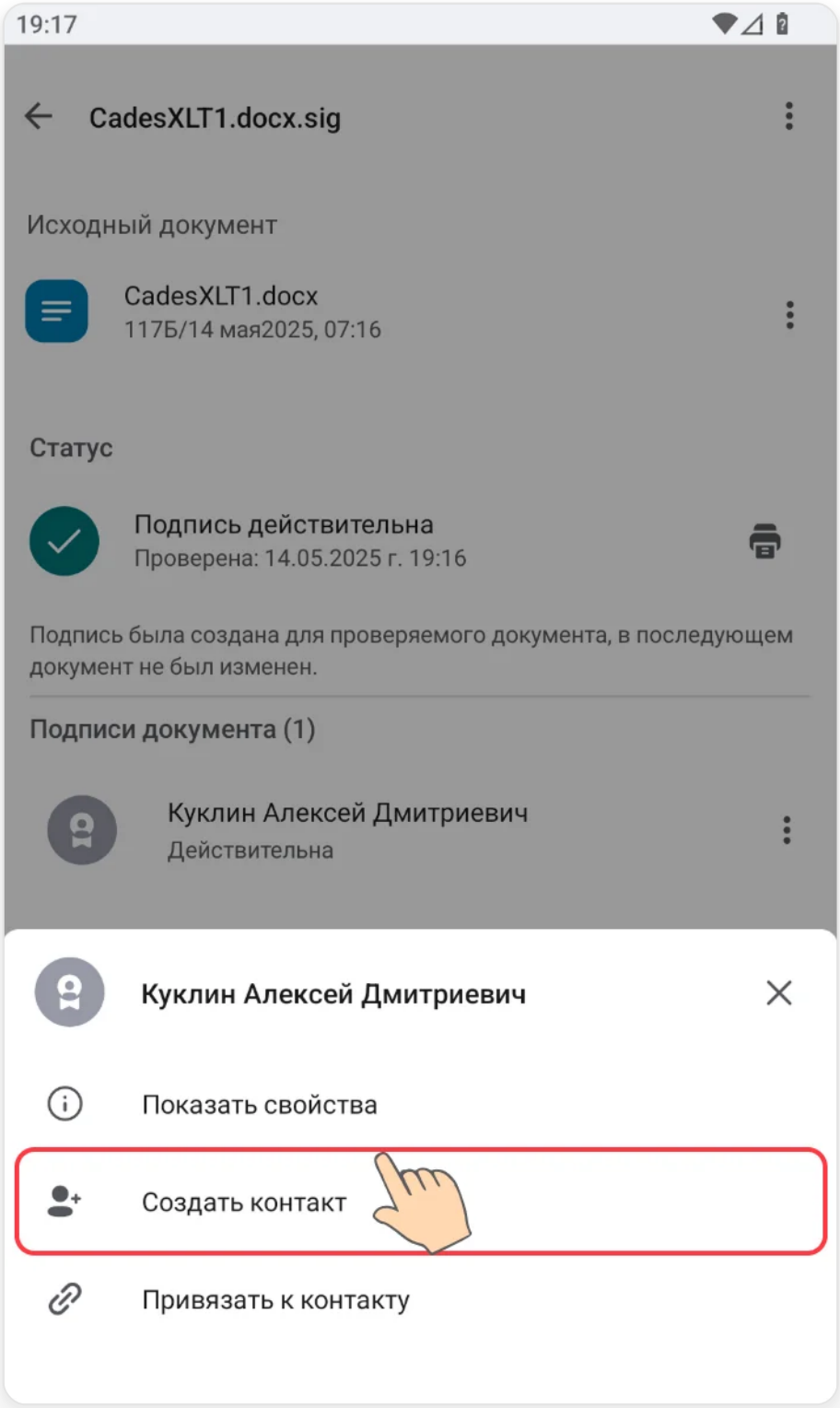
Контакты будут сохранены в указанную группу.

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	

Раздел	Поле	Обязательное	Описание
			Варианты: • Не указано • Мужской • Женский
	Язык	Нет	В формате ISO 639-1 (ru, en, de)
	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

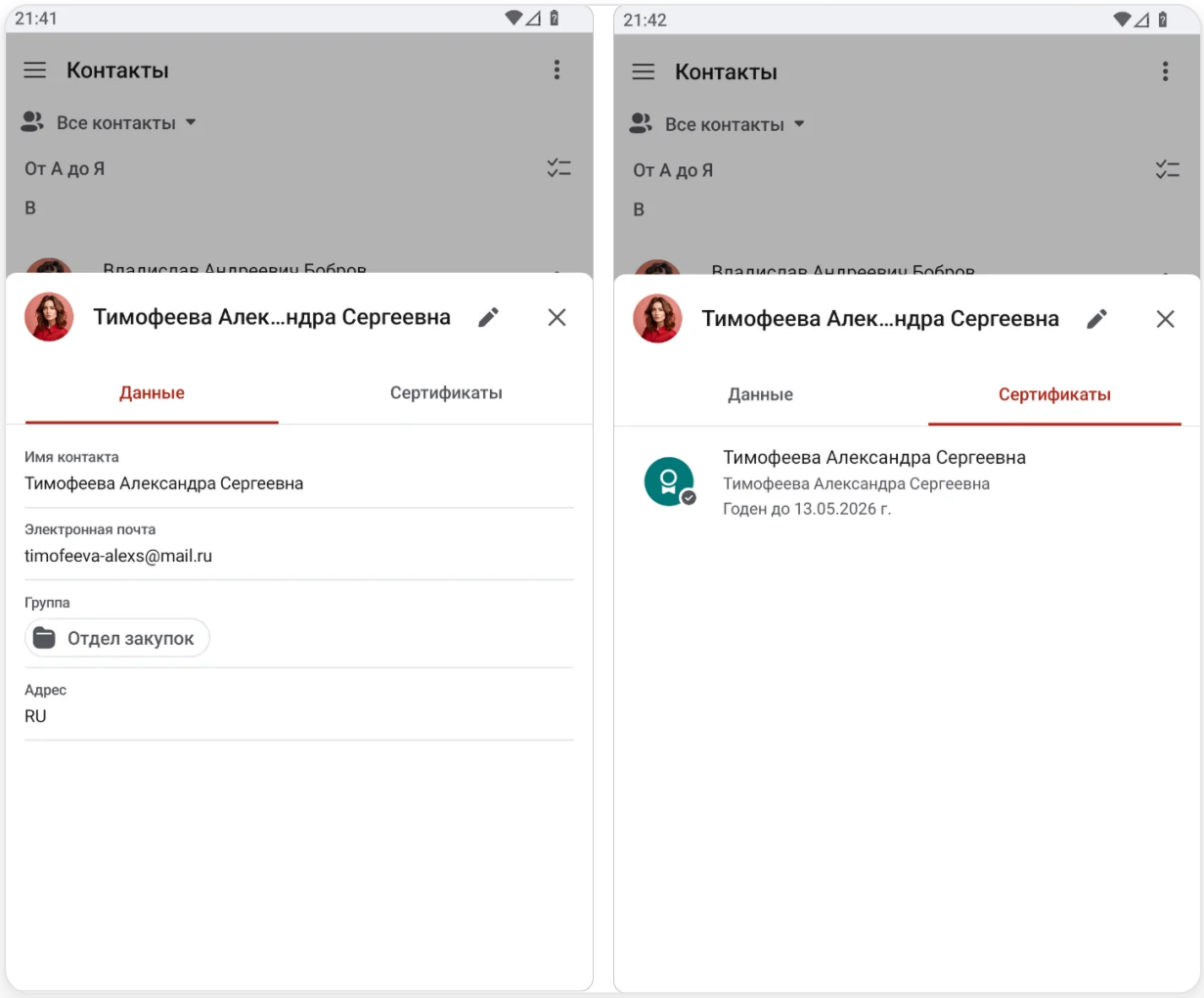
Открыть статью на сайте

Действия с контактами

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

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.

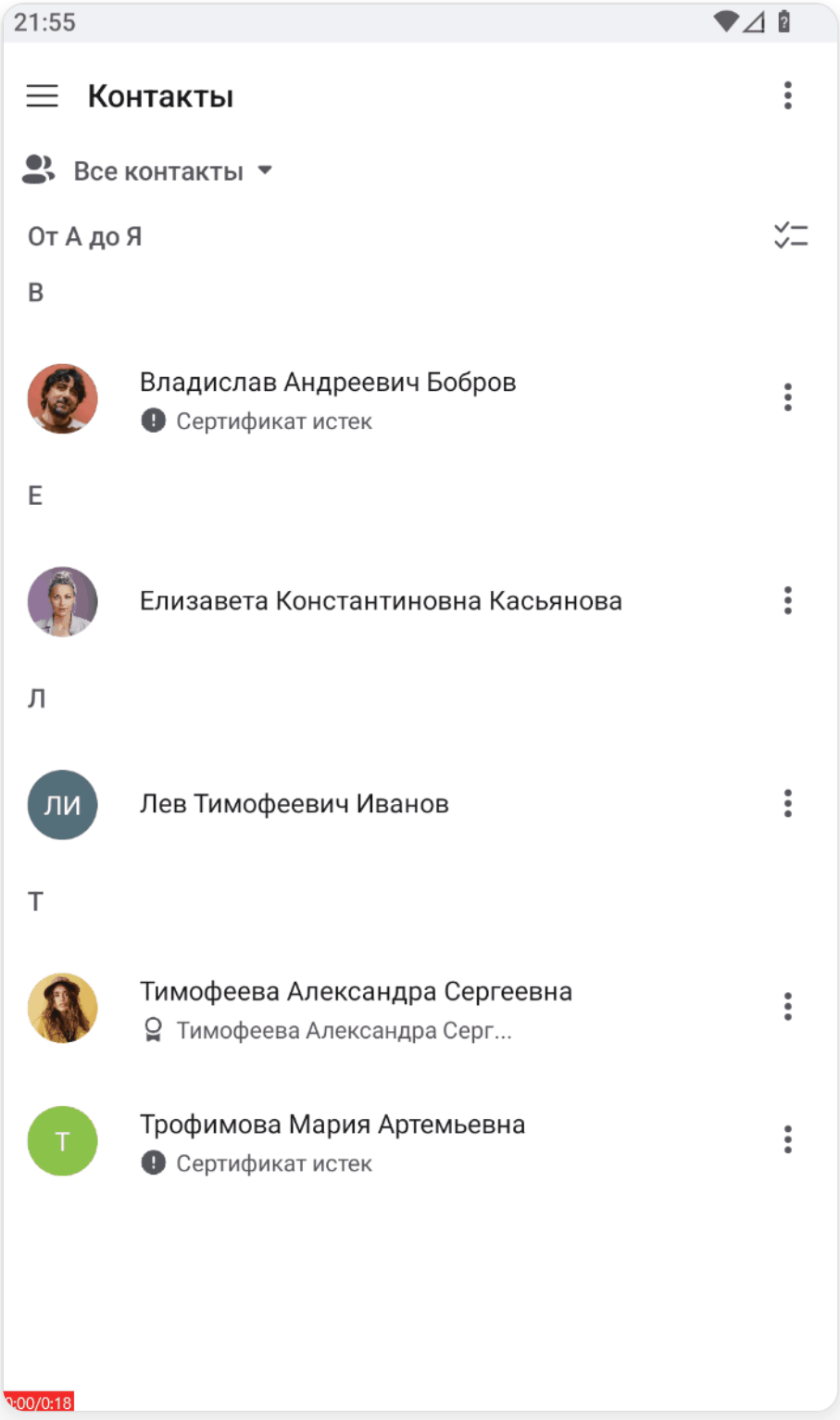
3. Внесите изменения в сертификаты. Подробнее читайте в инструкции Управление сертификатами контакта.
4. Нажмите **Сохранить**.

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.

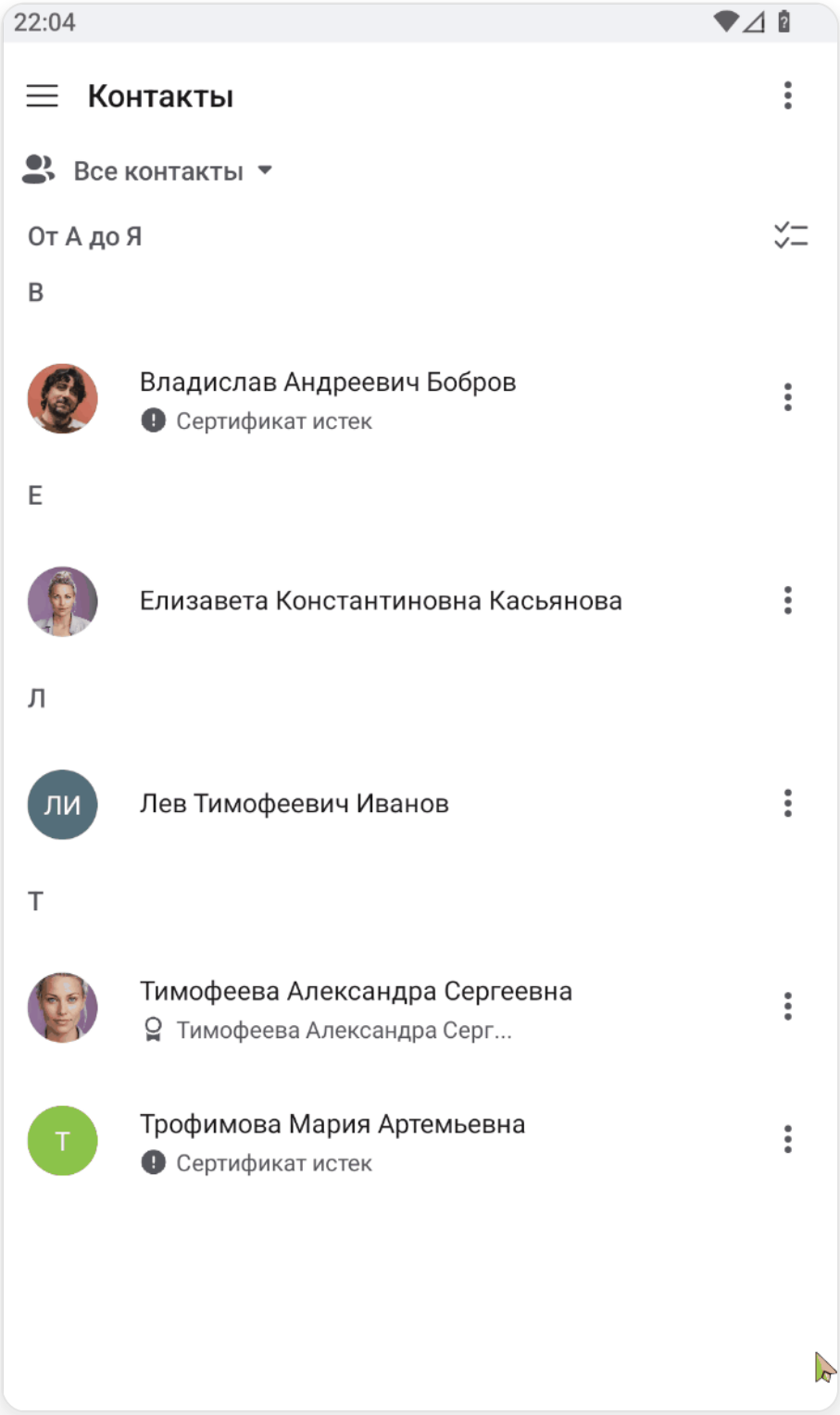
---

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**.

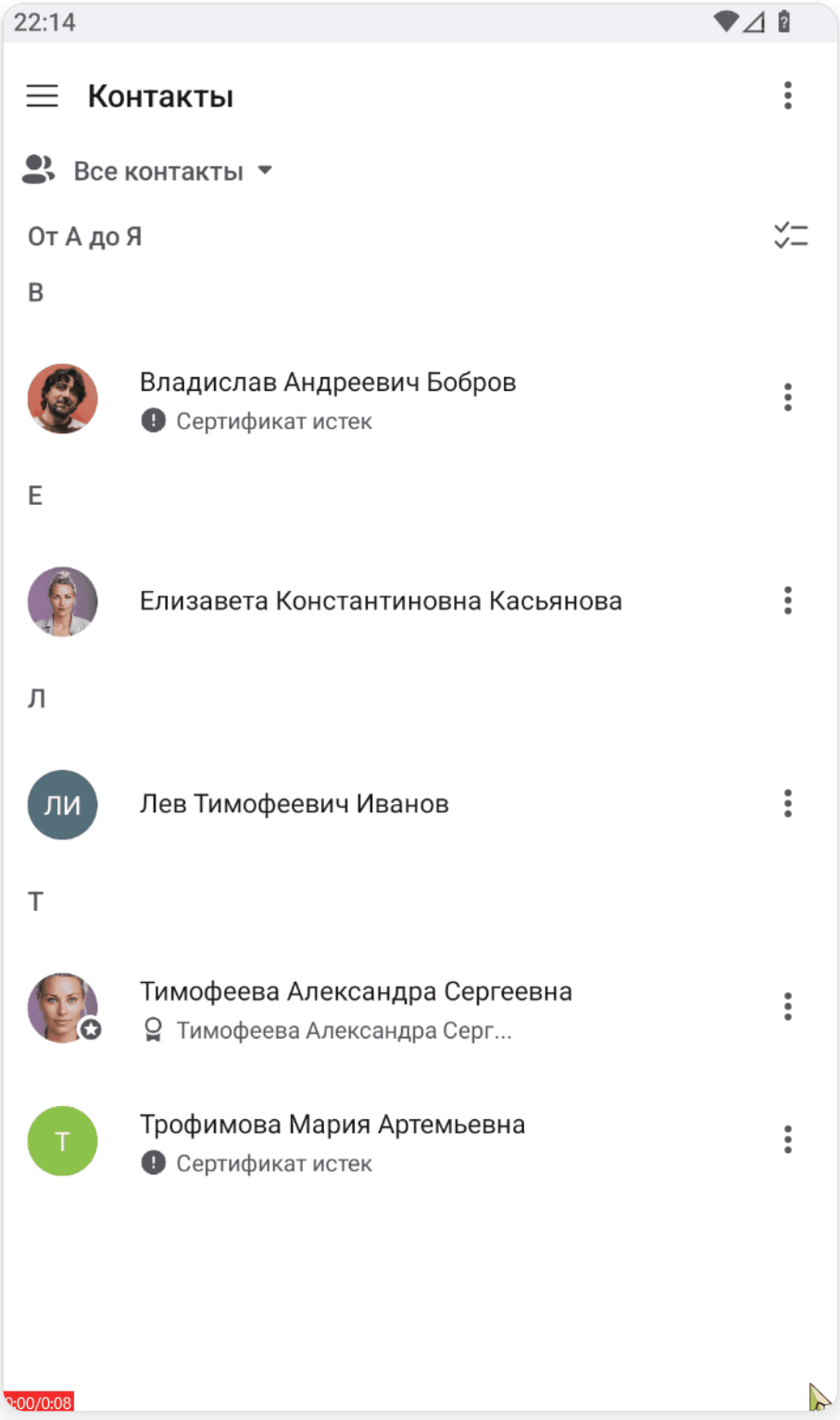
Контакты будут удалены из «Избранных».

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.

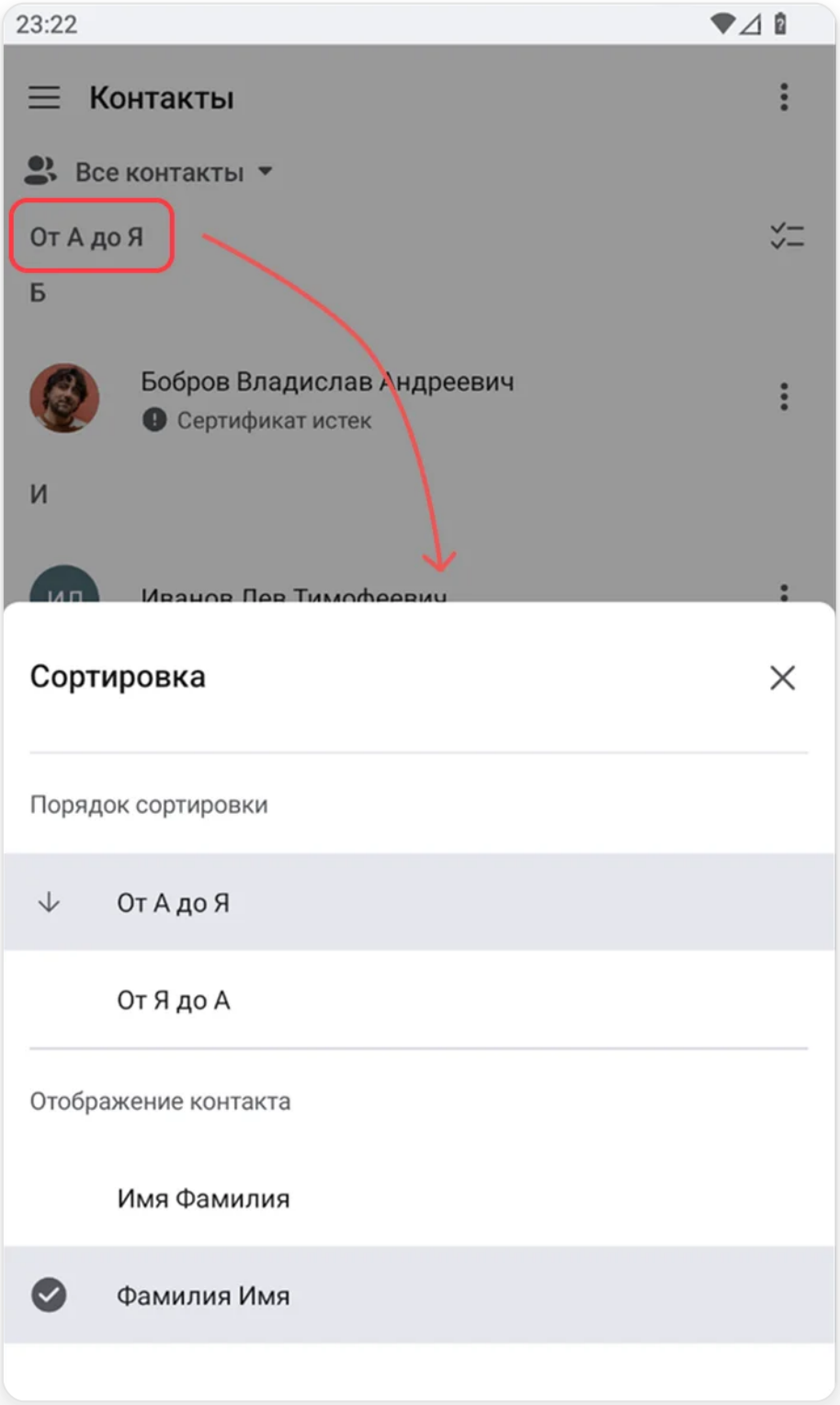
После завершения перемещения контактов будет отображено уведомление об успешном выполнении операции.

---

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.

---

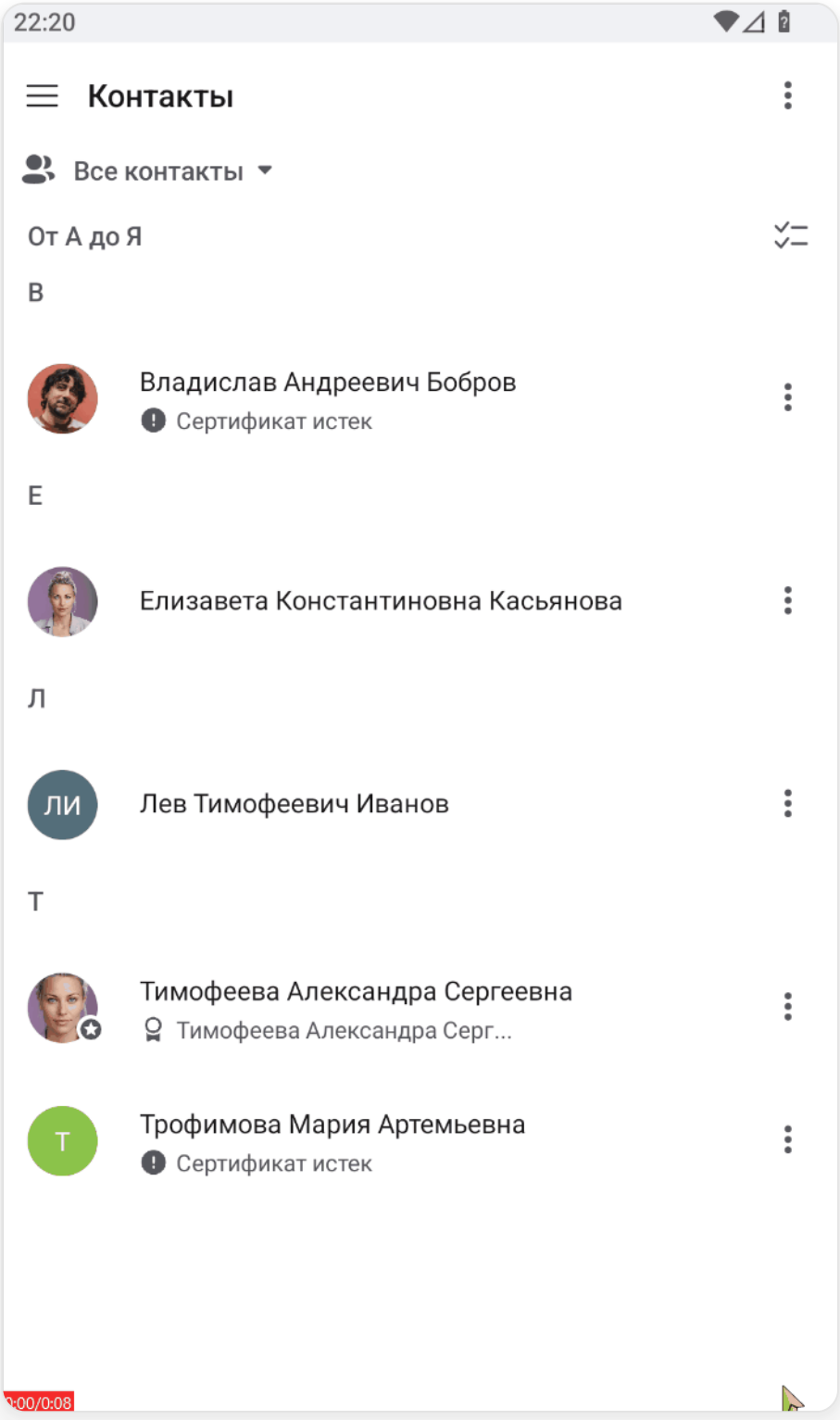
6. Удаление контакта

> ⚠️ **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

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

Добавление сертификата

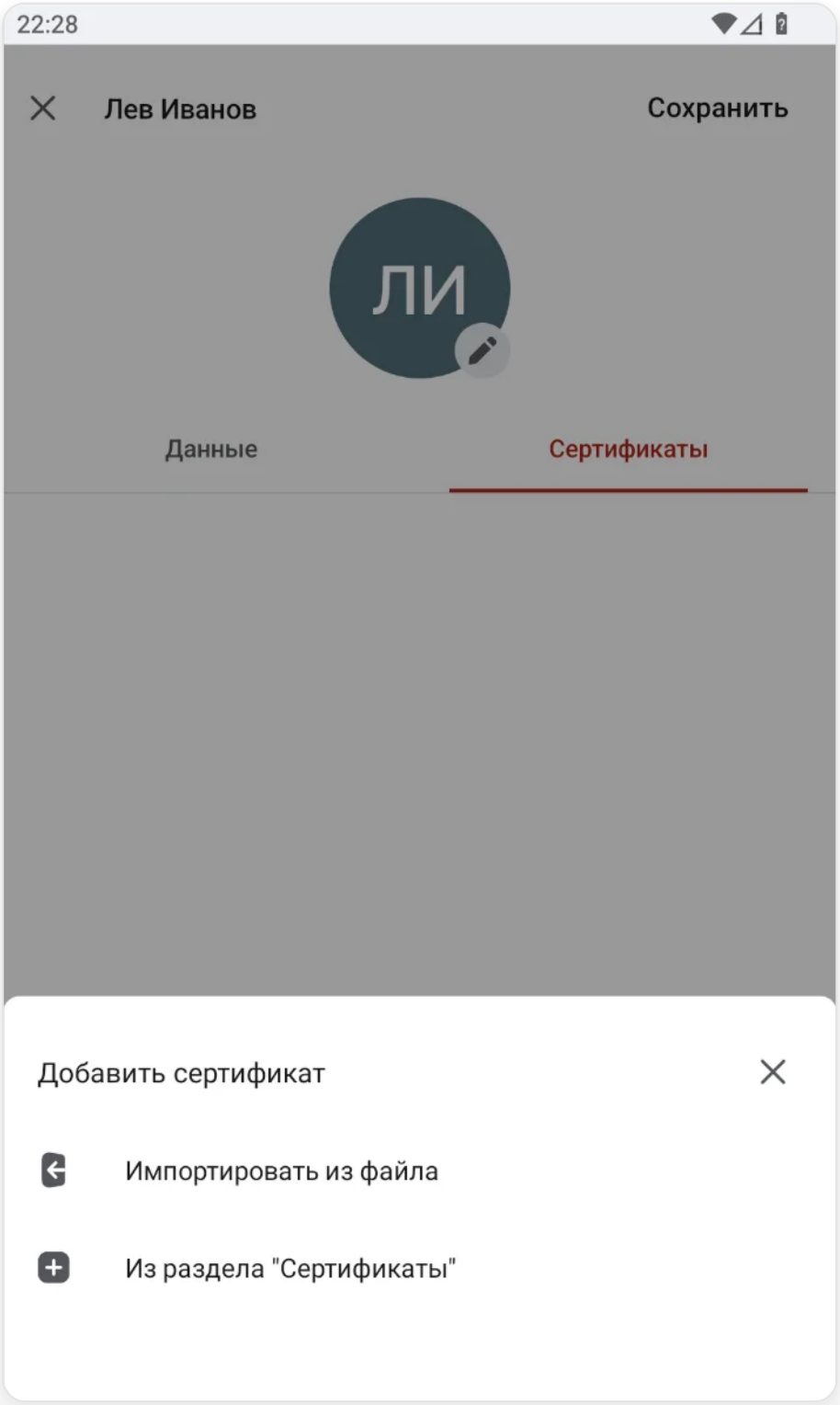
Для организации зашифрованного обмена документами с контактом необходимо привязать его сертификат.

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

Способы привязки сертификата

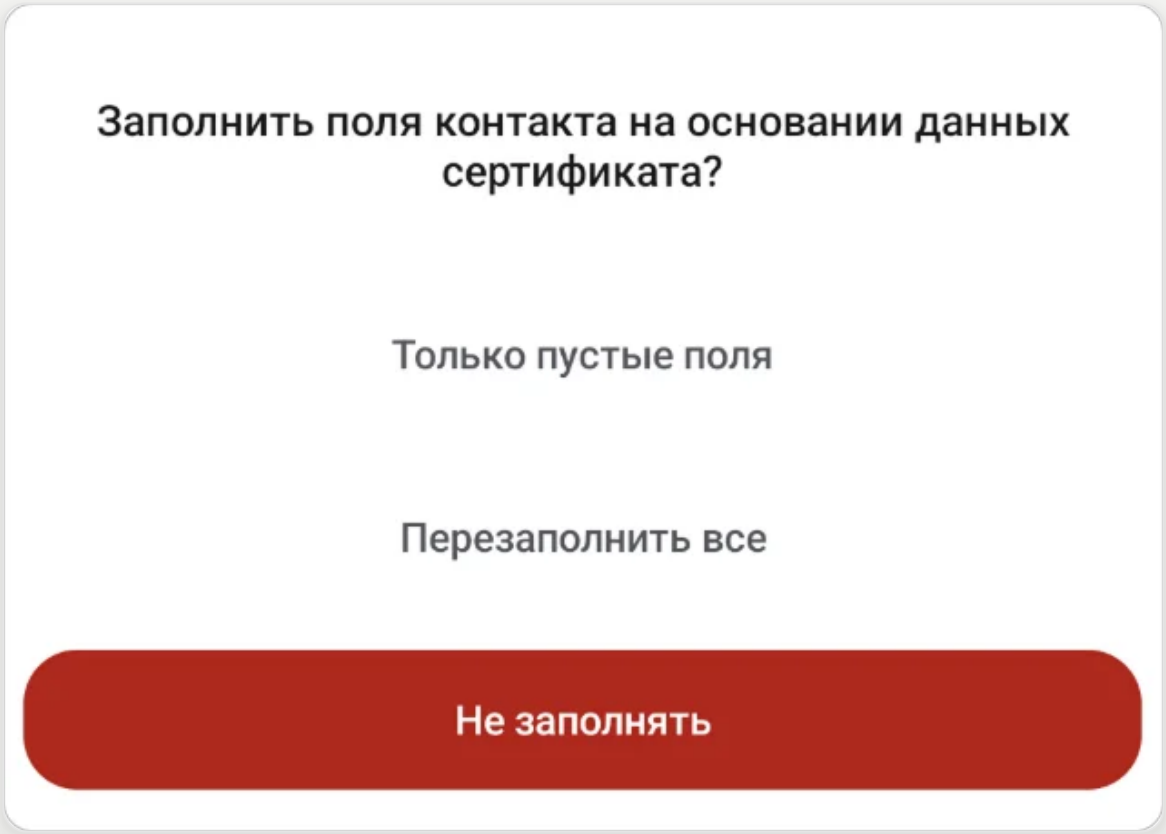
1. Стандартный способ

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.



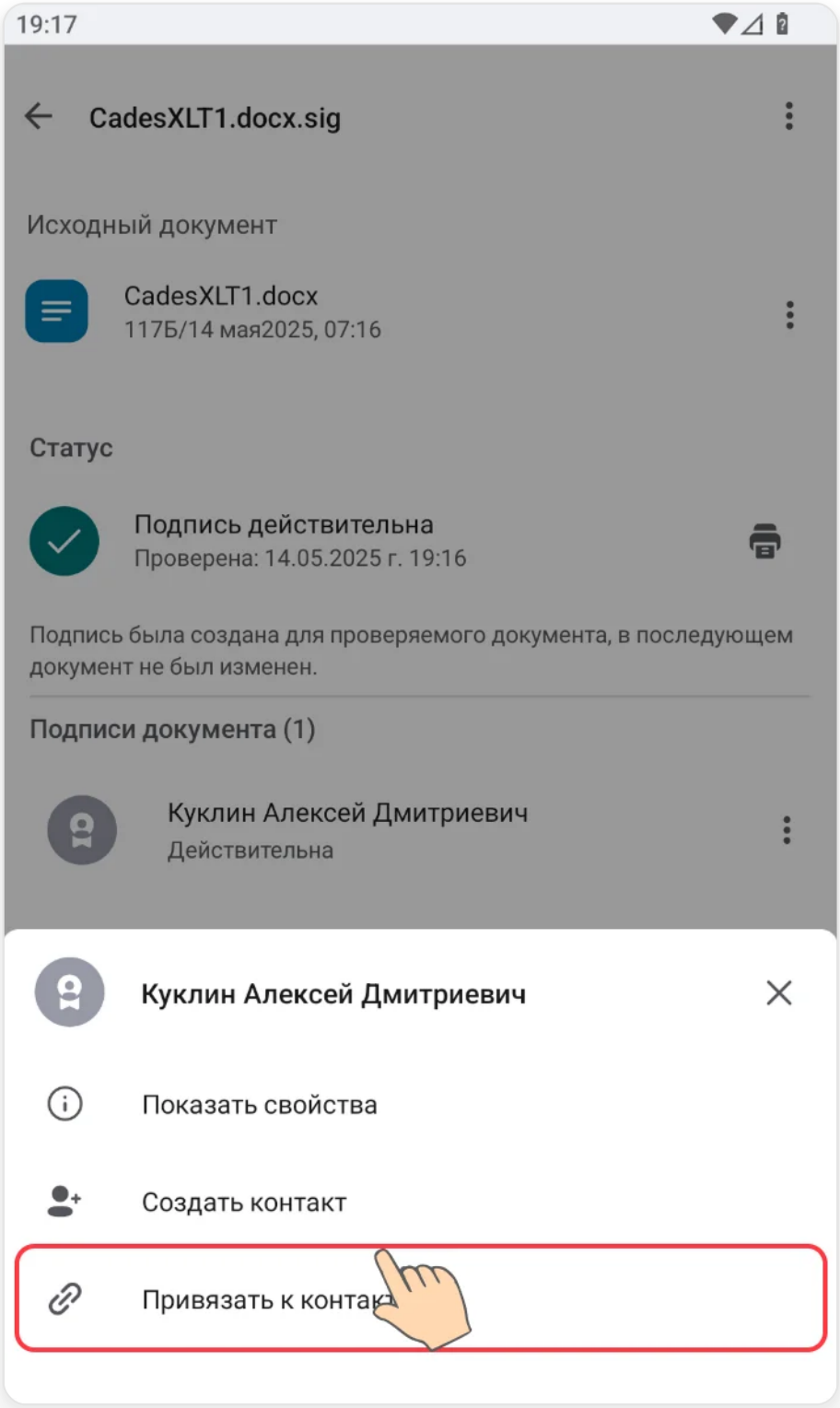
5. После выбора сертификата нажмите **Сохранить** в форме редактирования контакта.

> ⚠️ **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**.



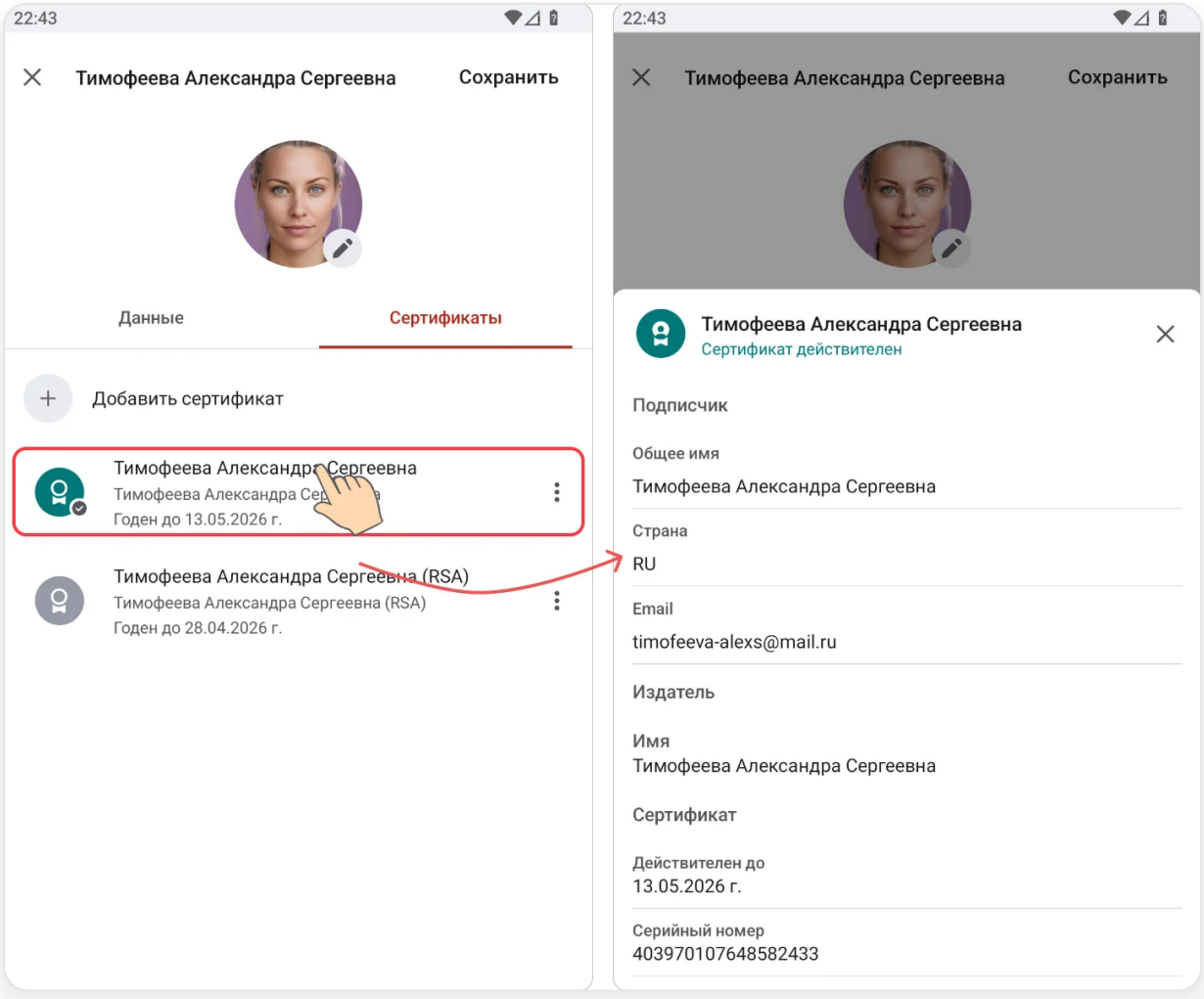
5. В открывшемся окне укажите контакт, к которому необходимо привязать сертификат. Для выбора доступен один или несколько контактов или групп.

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.



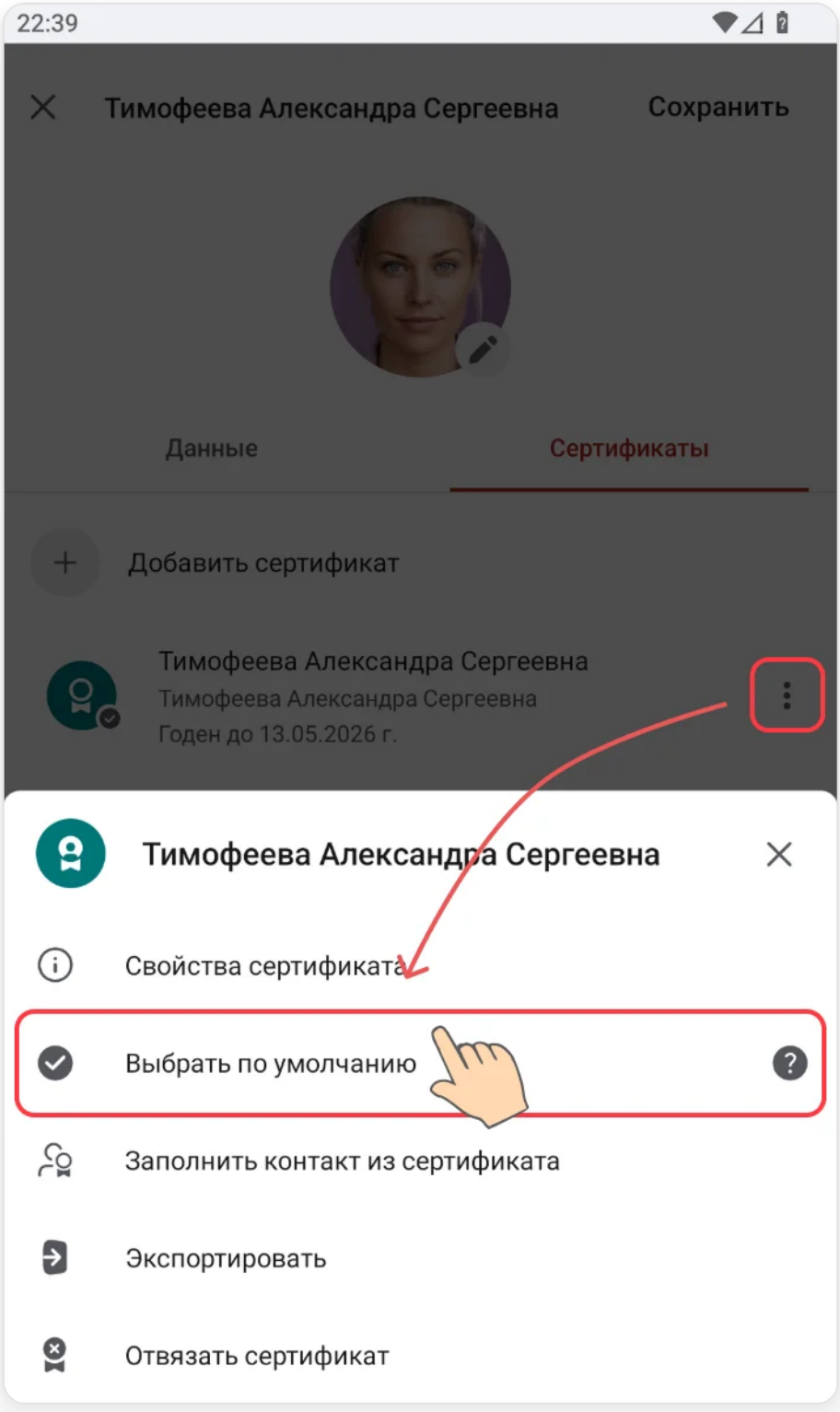
Установка сертификата по умолчанию

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.


22:39
Тимофеева Александра Сергеевна
Сохранить
Данные
Сертификаты
Добавить сертификат
Тимофеева Александра Сергеевна
Тимофеева Александра Сергеевна
Годен до 13.05.2026 г.
Тимофеева Александра Сергеевна
Свойства сертификата
Выбрать по умолчанию
Заполнить контакт из сертификата
Экспортировать
Отвязать сертификат

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

Группы контактов

- Общая информация
- Создание группы контактов
- Действия с группами

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

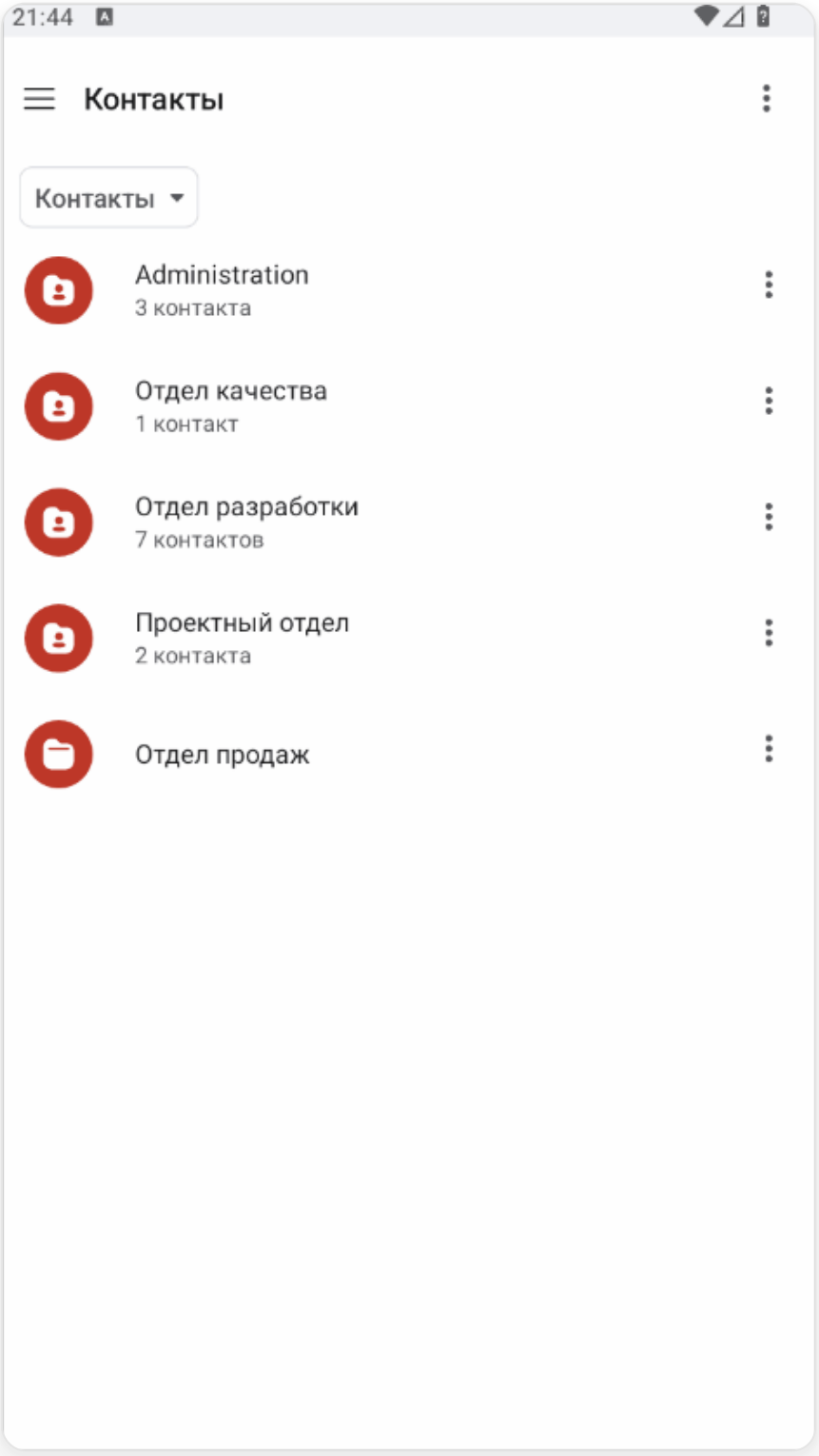
> 💡 **Совет**: В приложении можно создавать несколько уровней вложенности групп.

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**.

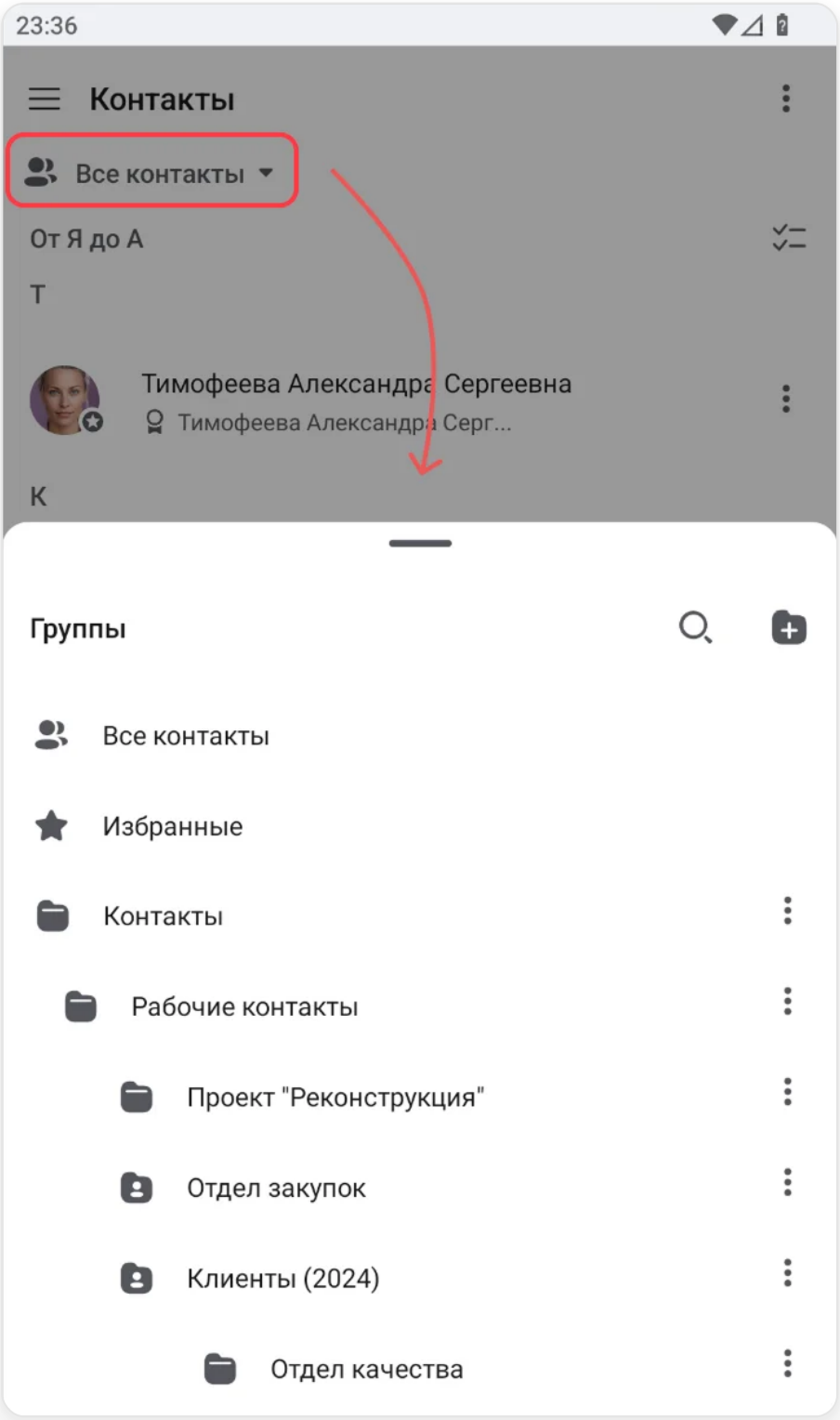


Действия с группами

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

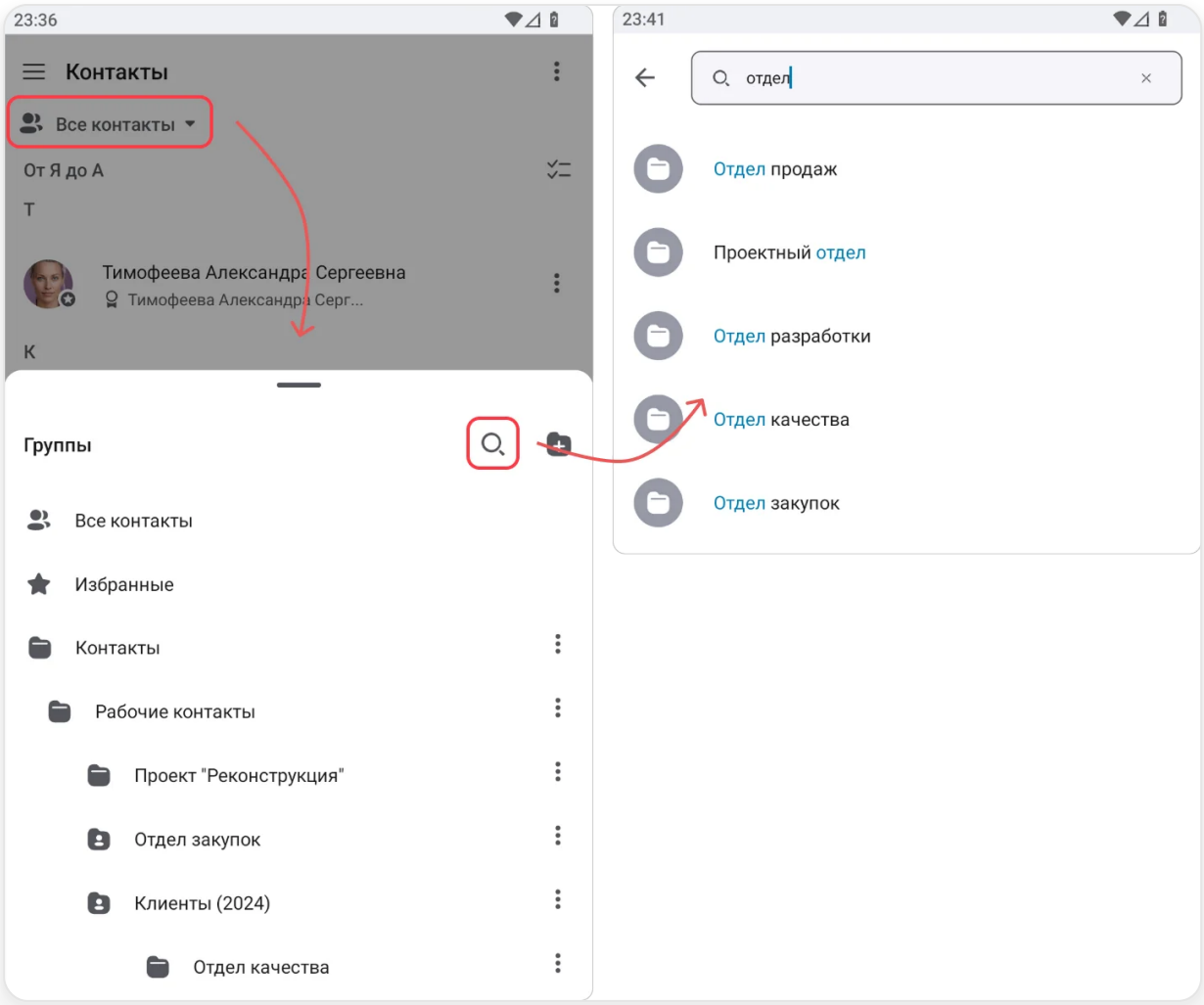
1. Открытие списка групп

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



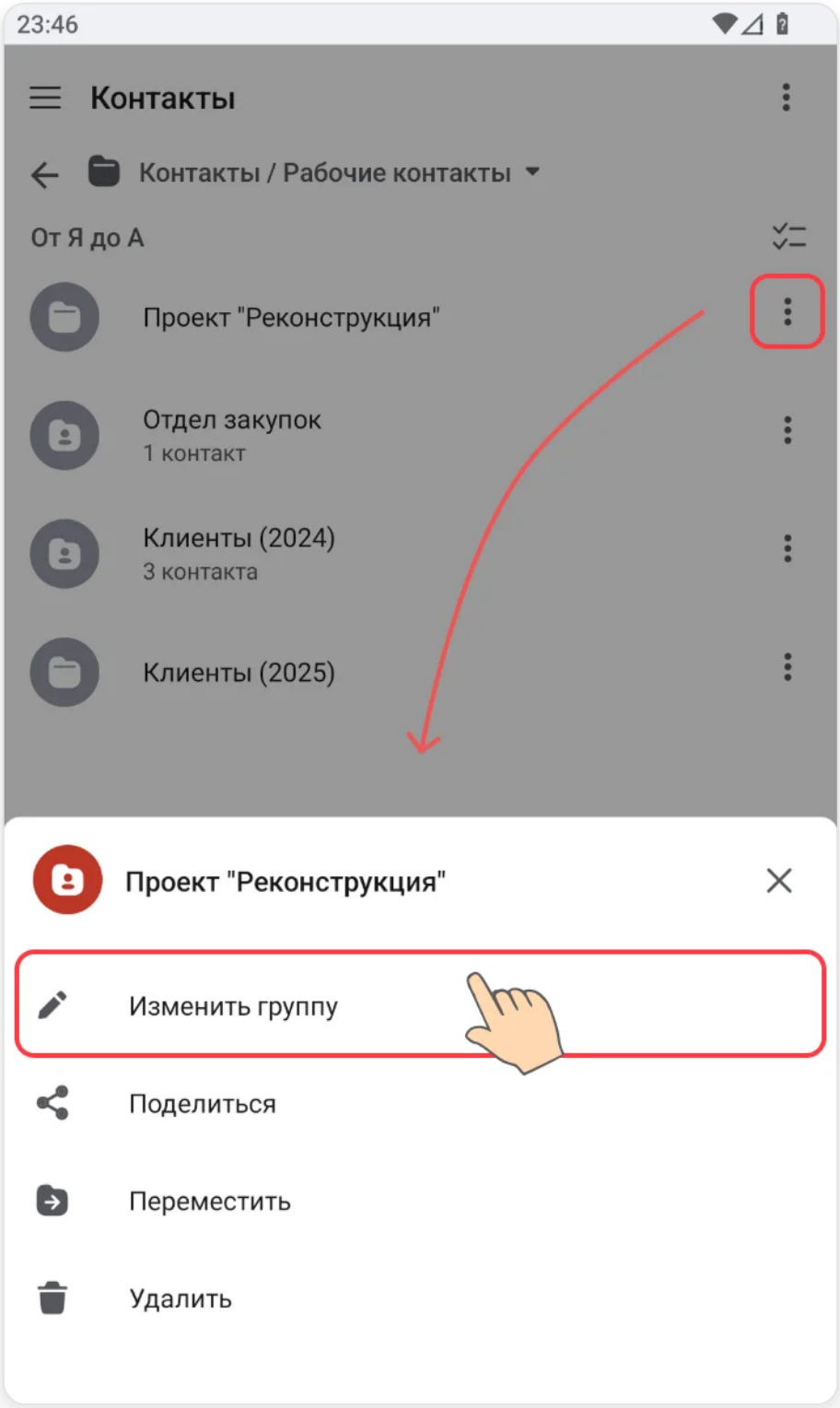
2. Поиск по группам

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.

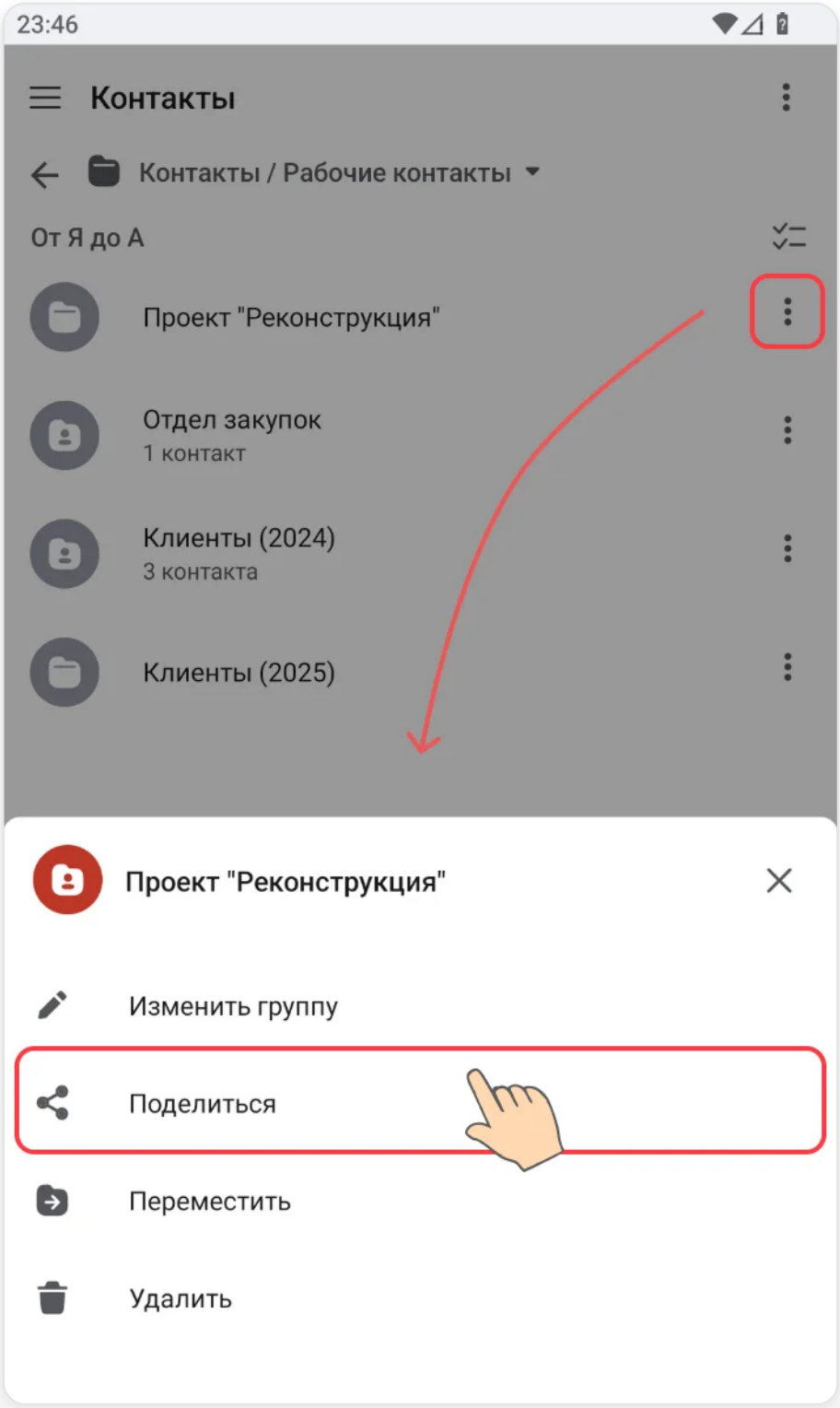
5. Внесите необходимые изменения.
6. Нажмите **Сохранить**.

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

- Общая информация
- Импорт контактов
- Экспорт контактов
- Описание реквизитов контакта vCard

Общая информация

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

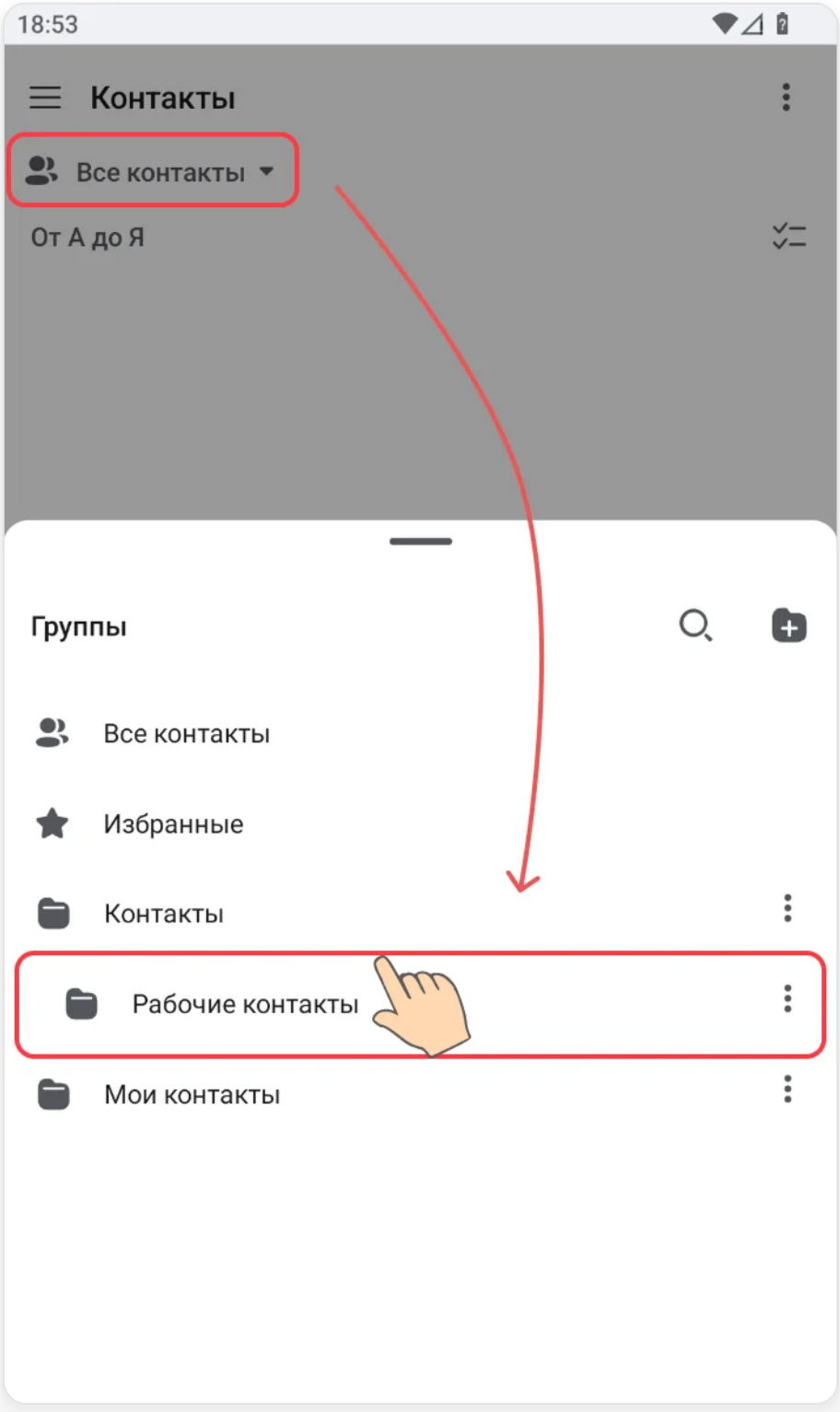
vCard позволяет хранить:

- 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.

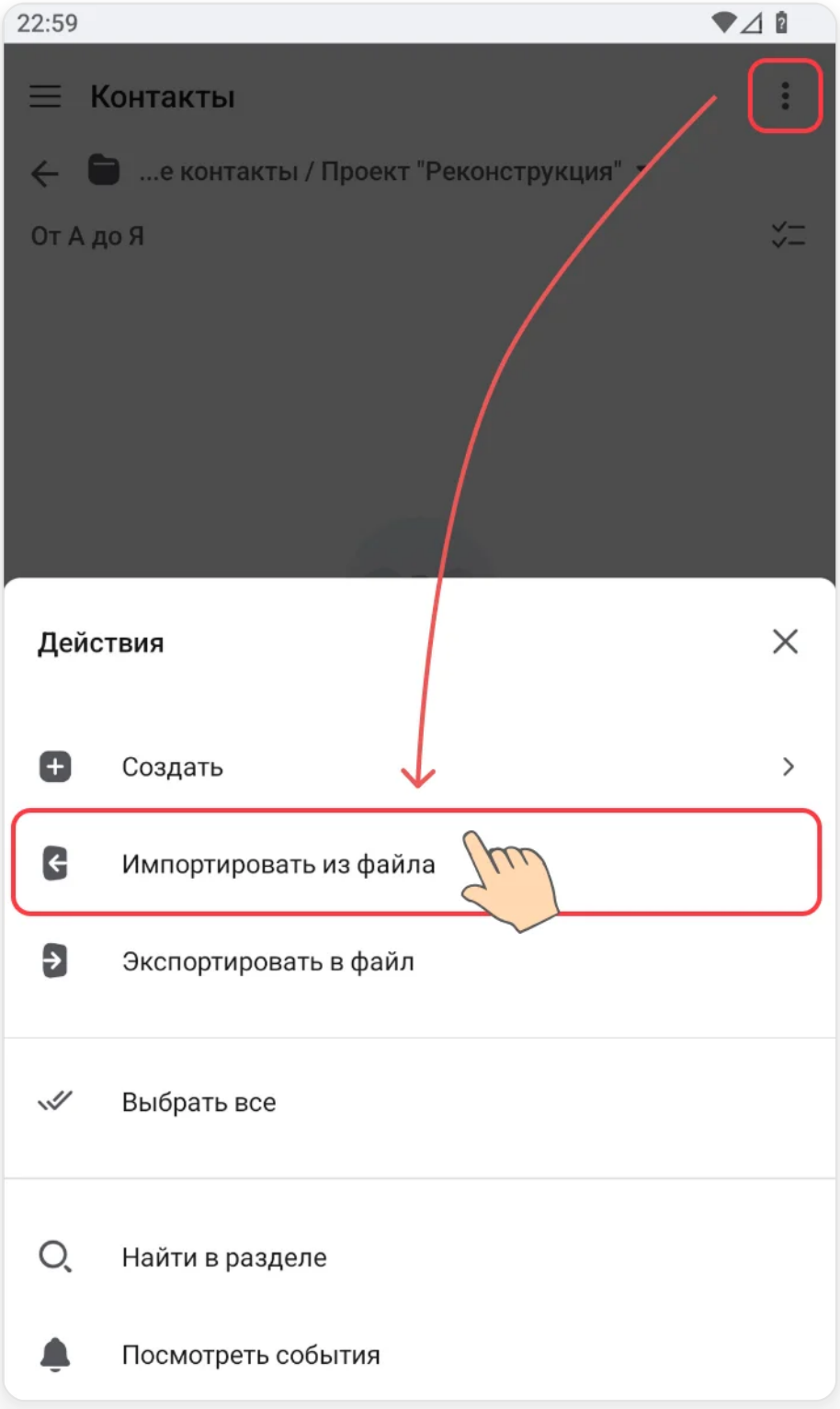
1. Откройте раздел **Контакты**.
2. Перейдите в группу, в которую необходимо импортировать контакты. Для этого нажмите на кнопку **Все контакты** в верхней части окна и в появившемся меню нажмите на название необходимой группы.



⚠️ **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.

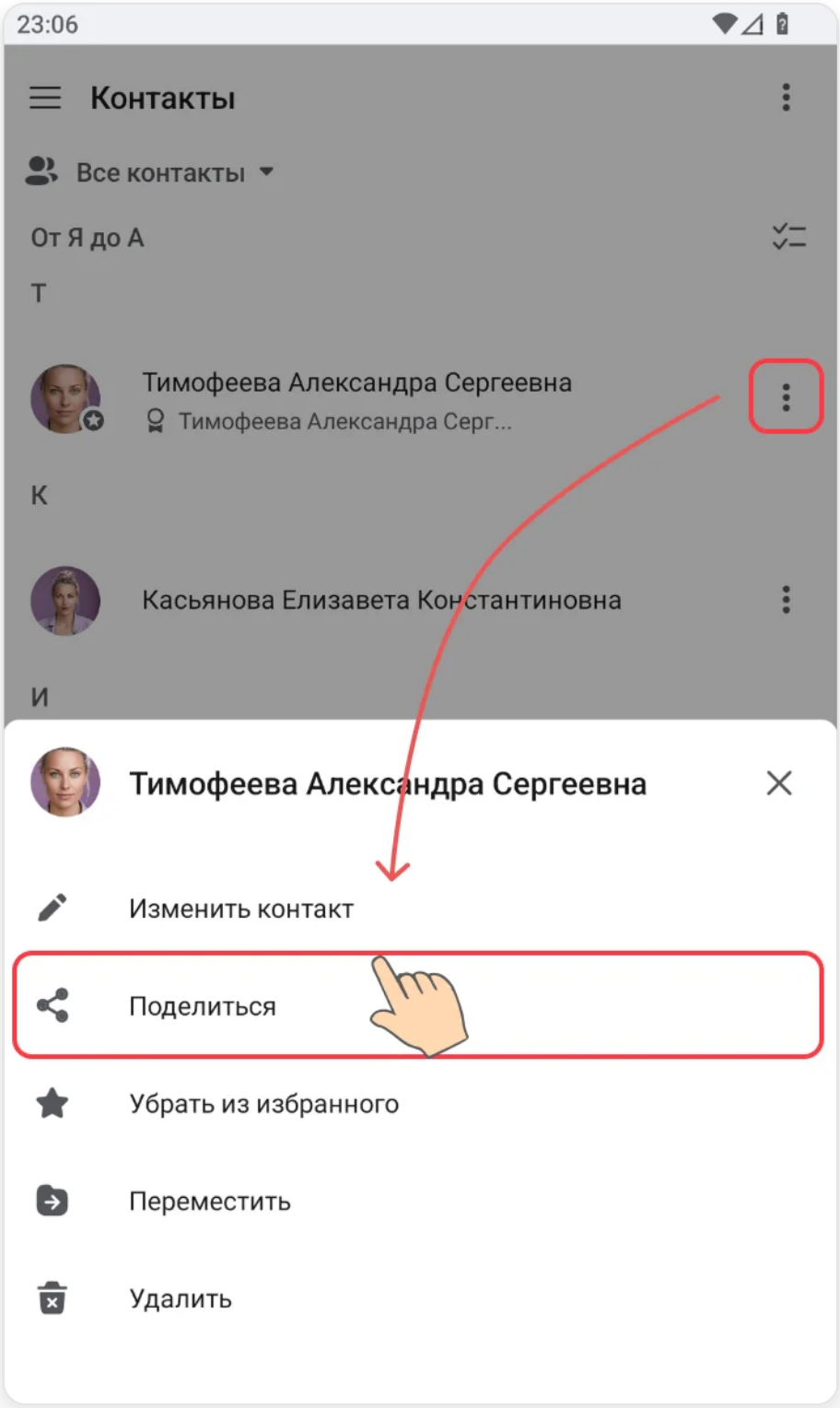
Ошибка	Описание	Рекомендуемые действия
Не удалось импортировать контакты	Возможно, файл пустой или повежден	Проверьте содержимое файла и повторите импорт

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

Мои контакты

- О группе «Мои контакты»
- Создание личного контакта

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.

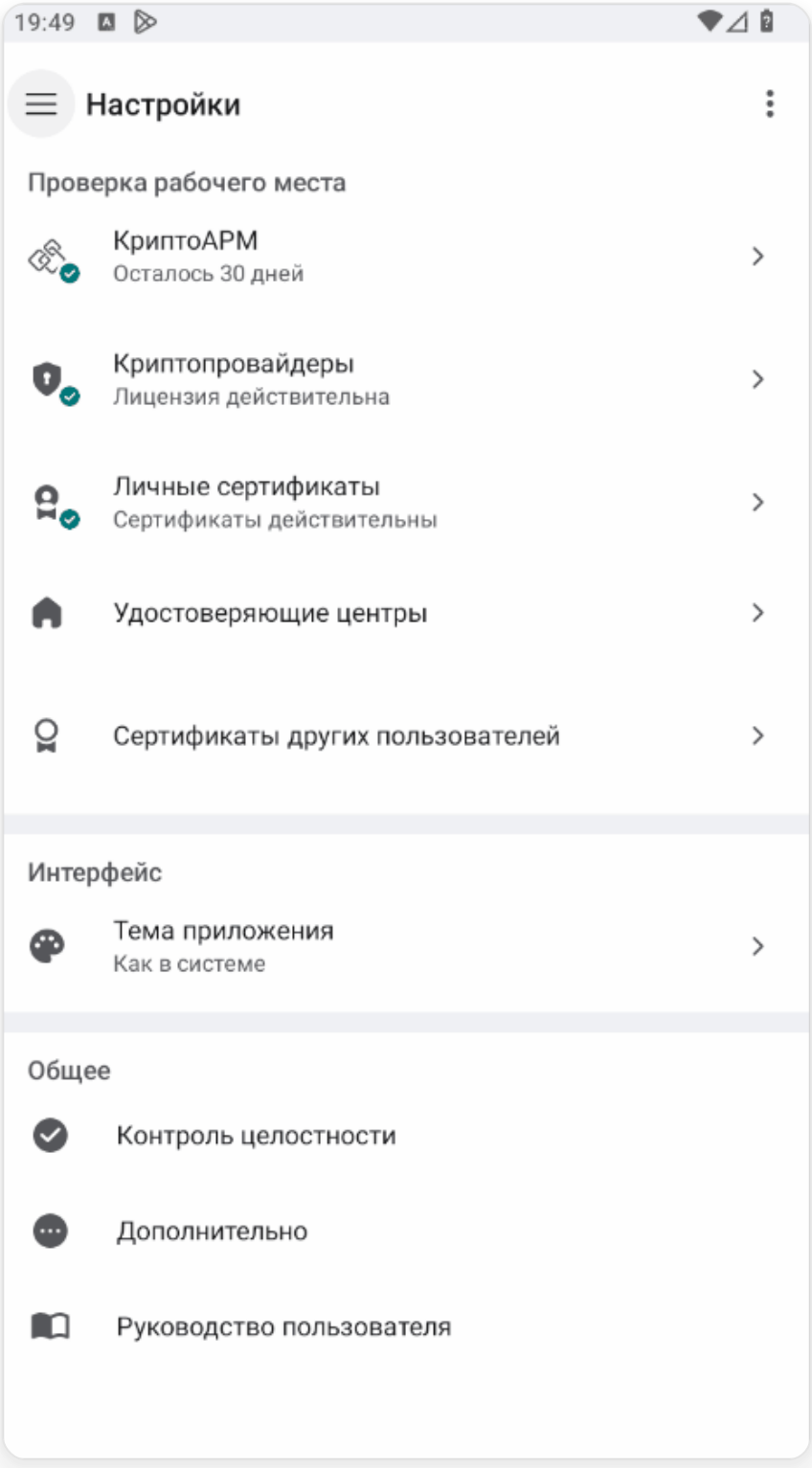
Для чего нужен «Мой контакт»

- **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

- Общие сведения
- Запуск поиска
- Действия с результатами поиска

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

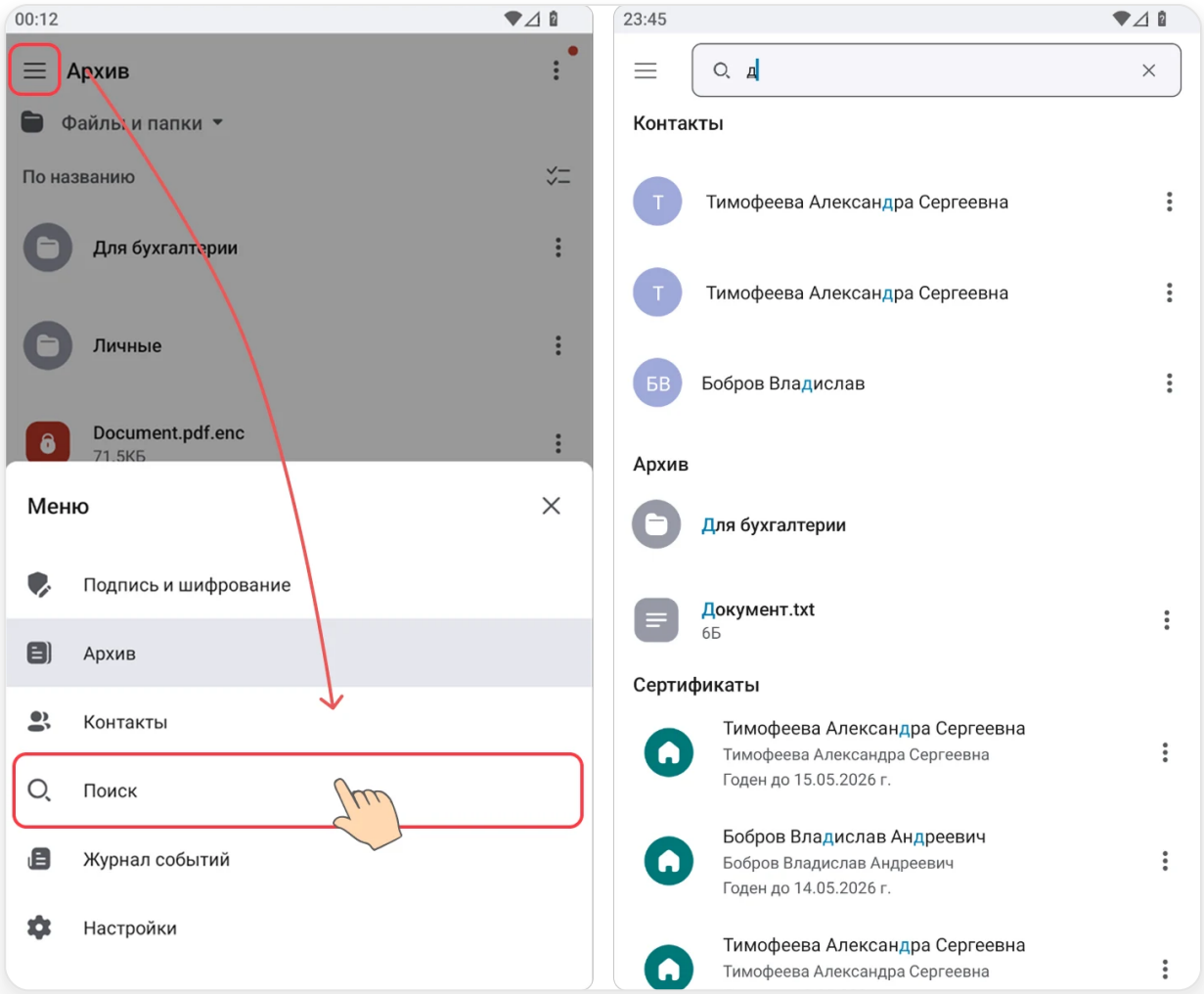
- **По названию**: поиск по совпадению в наименовании элемента
- **По расширению документов**
- **Рекурсивный**: охватывает все вложенные каталоги и группы
- **Ограничения**: не учитывает метаданные (дату, автора и др.)

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

Запуск поиска

1. Глобальный поиск

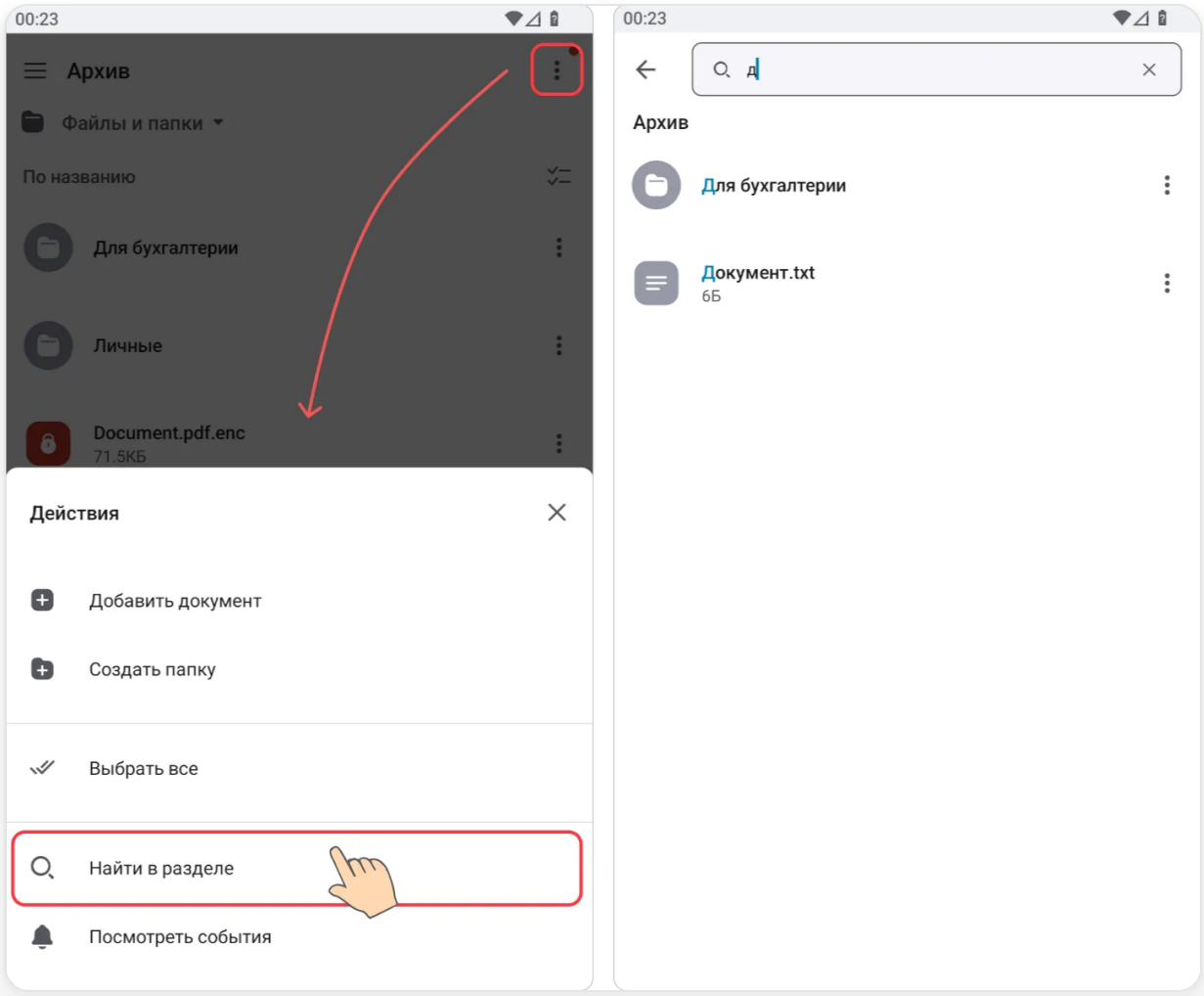
1. Вызовите главное меню по кнопке , размещенной в верхнем части окна приложения.
2. Выберите пункт **Поиск**.



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

- Назначение и доступ
- Уровни событий
- Работа с записями журнала

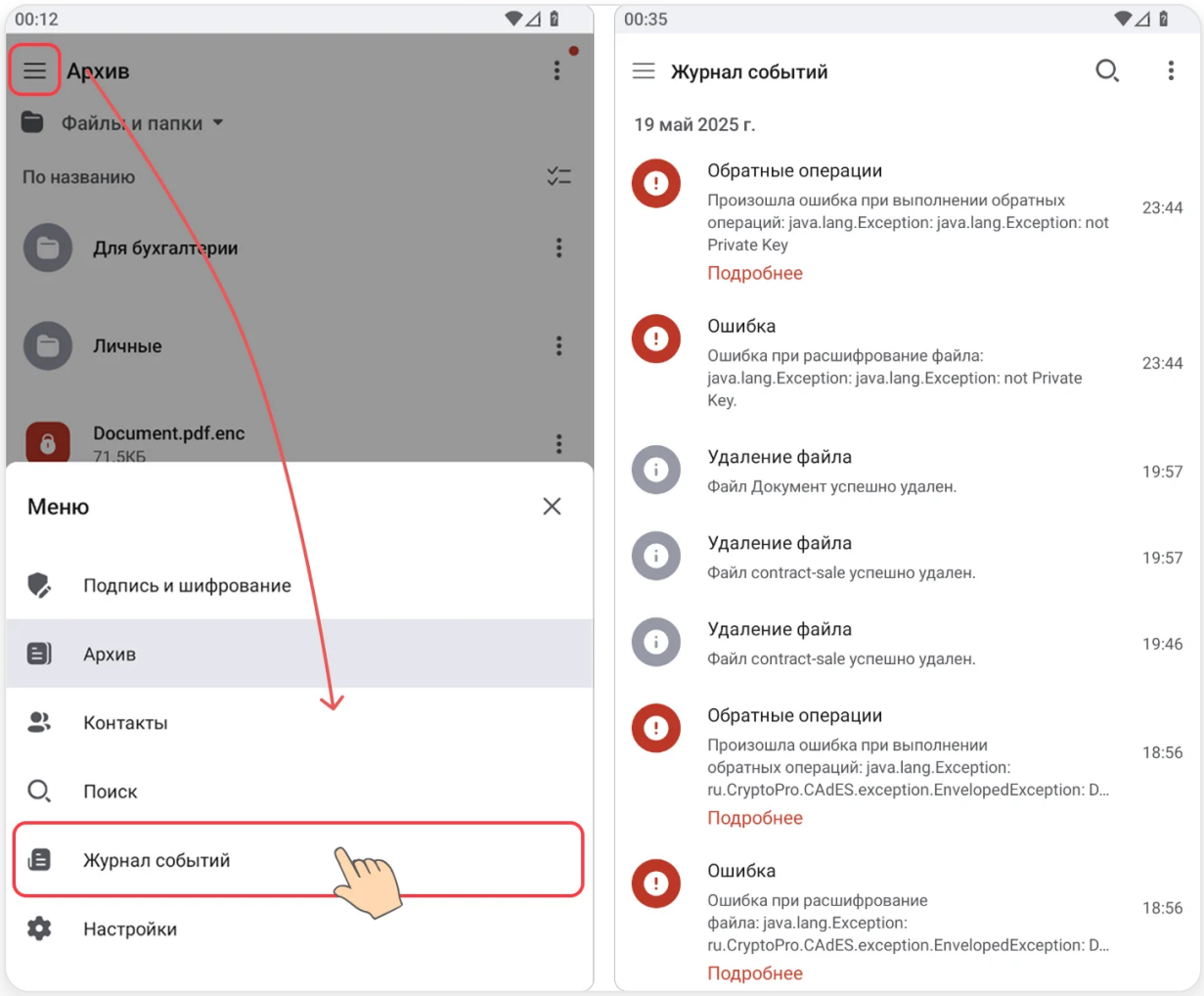
Назначение и доступ

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

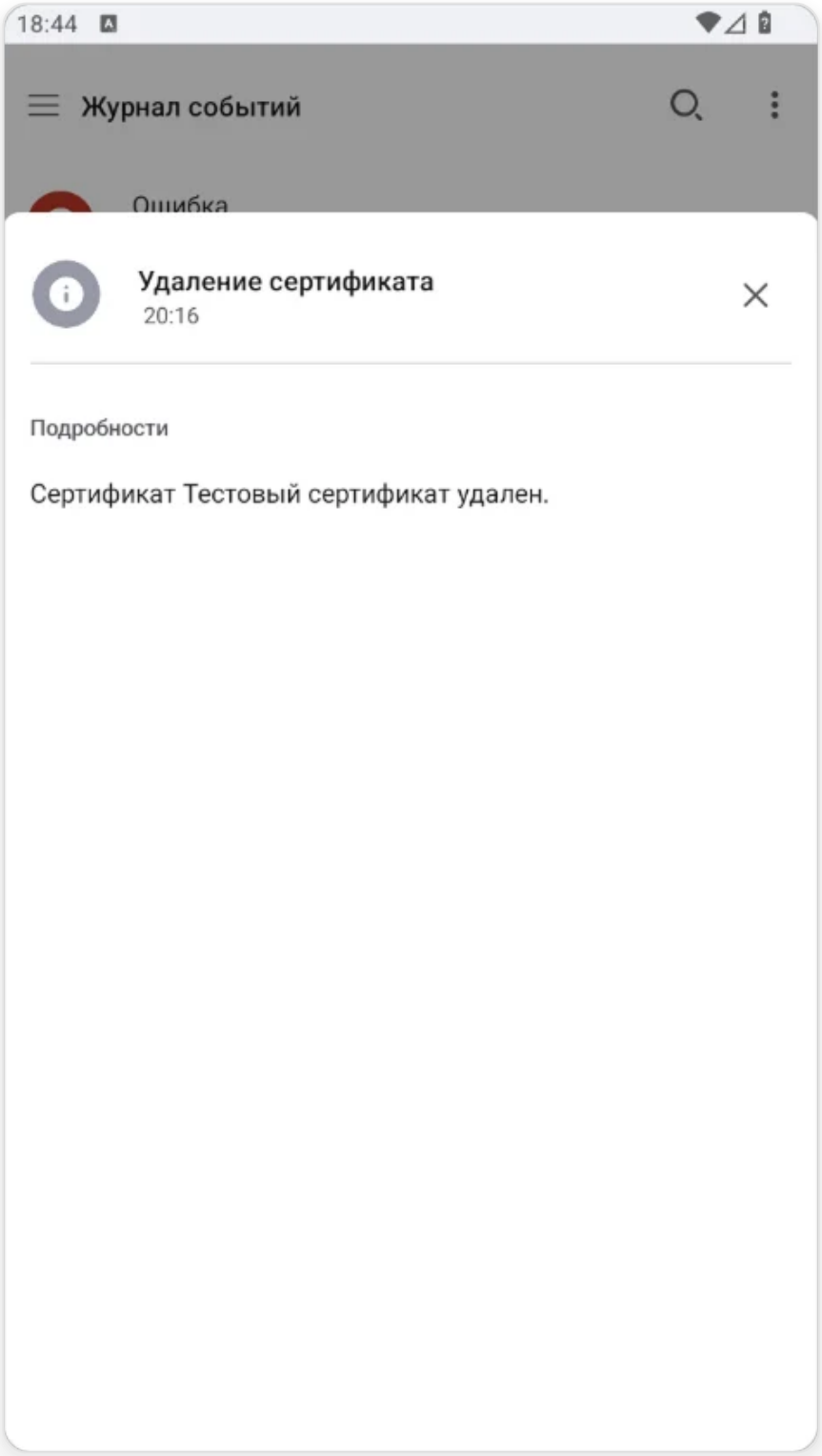
Журнал поддерживает несколько уровней логирования:

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.

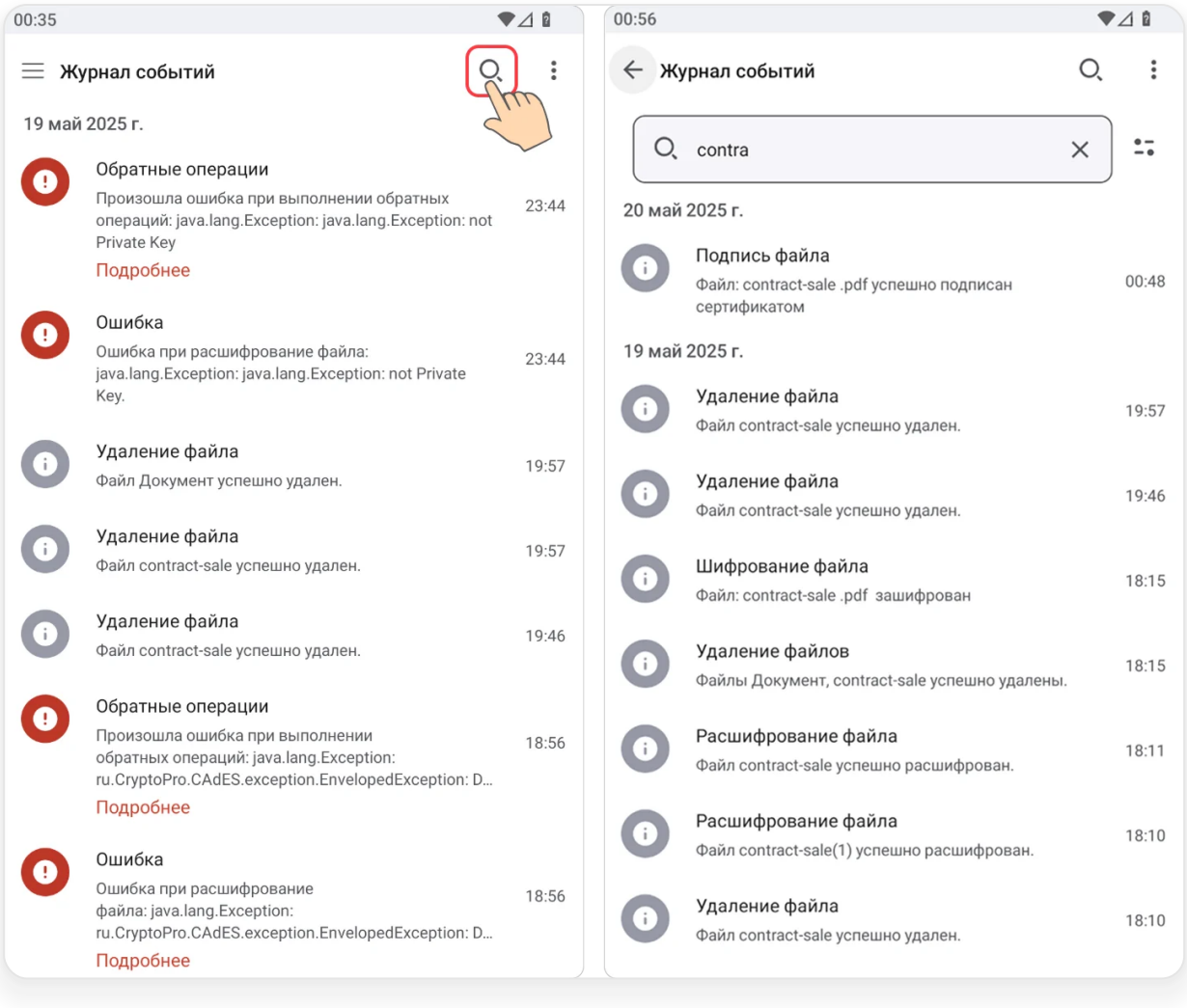


2. Поиск и фильтрация

Быстрый поиск

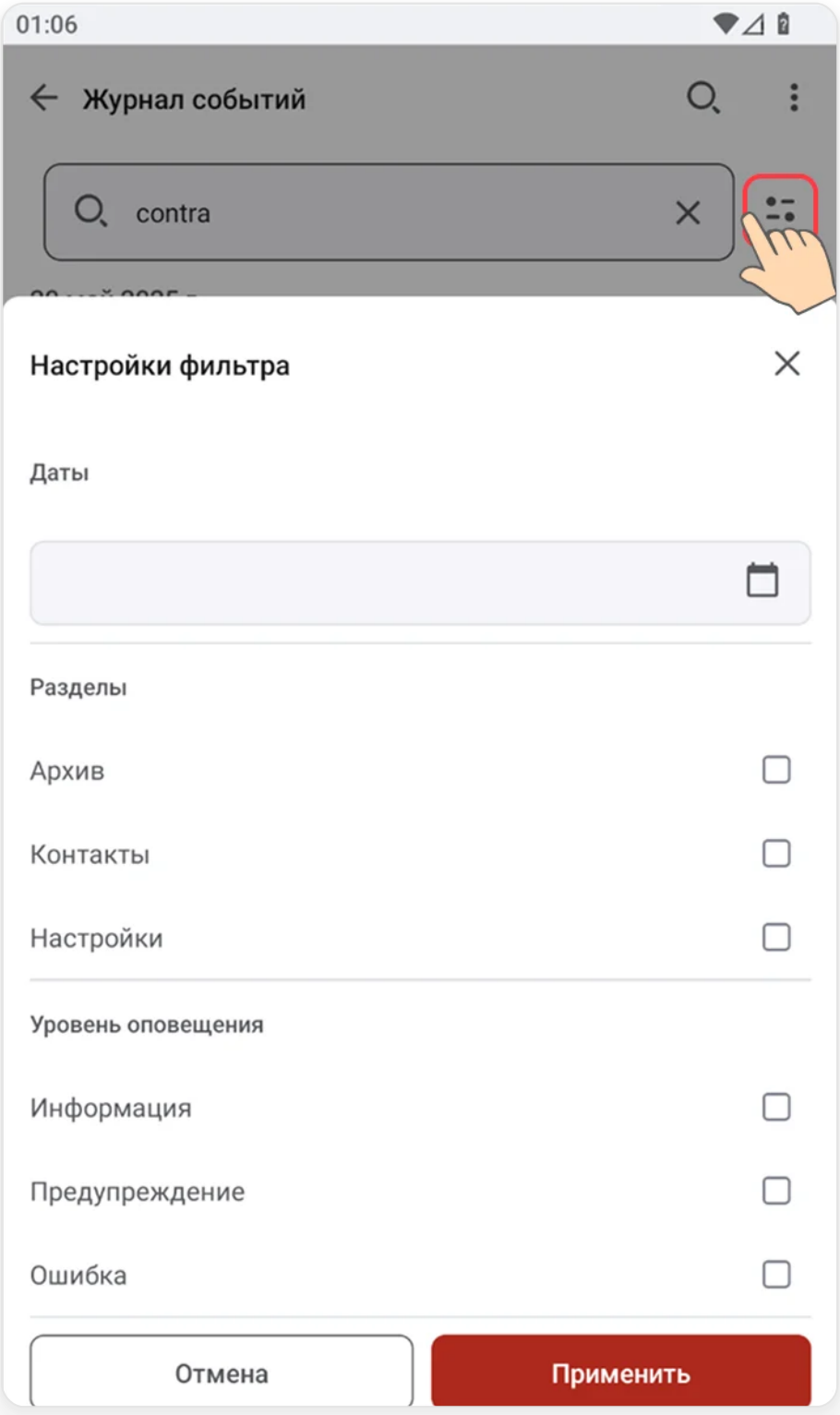
1. Перейдите в **Журнал событий**.
2. Нажмите кнопку **Поиск** , размещенную на верхней панели.
3. Над списком событий отобразится поле для ввода поисковой фразы.

4. Введите текст (поддерживается частичное совпадение).



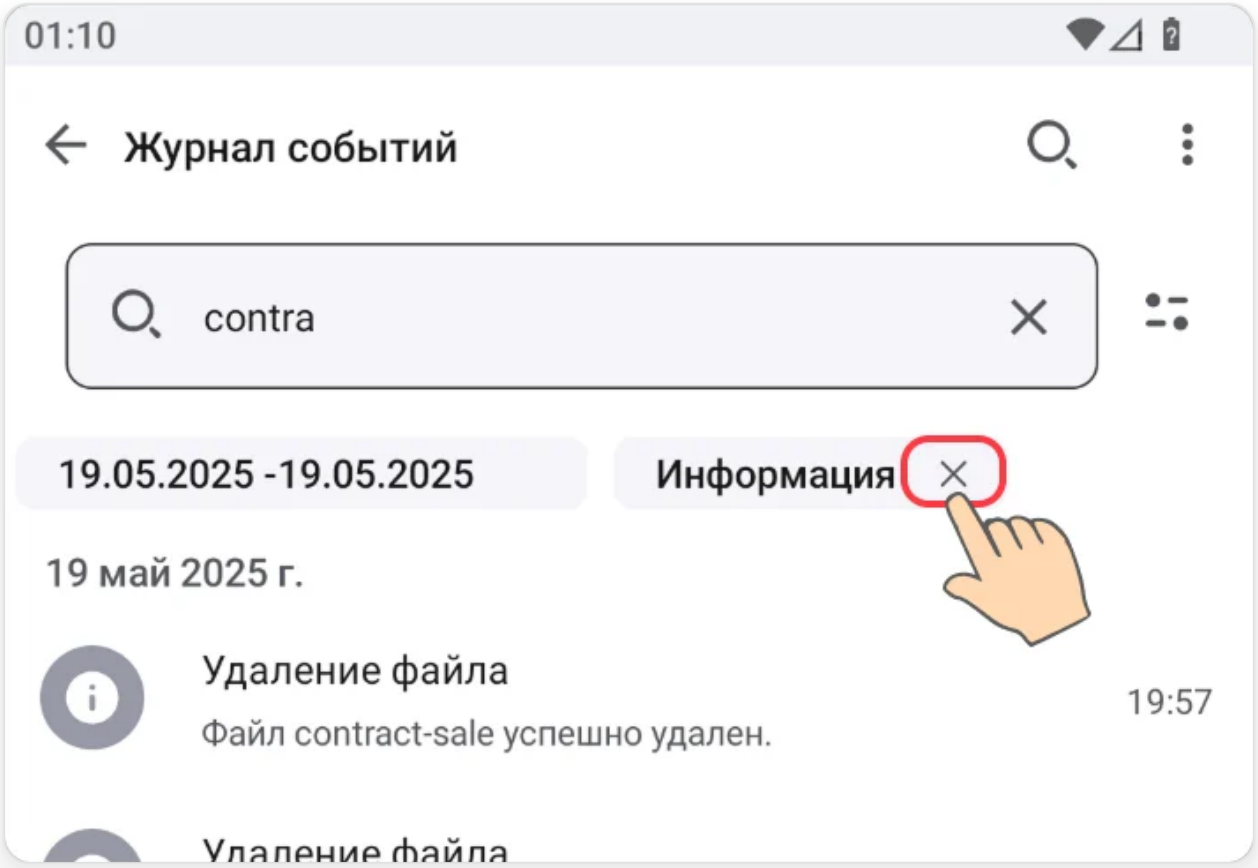
Расширенная фильтрация

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

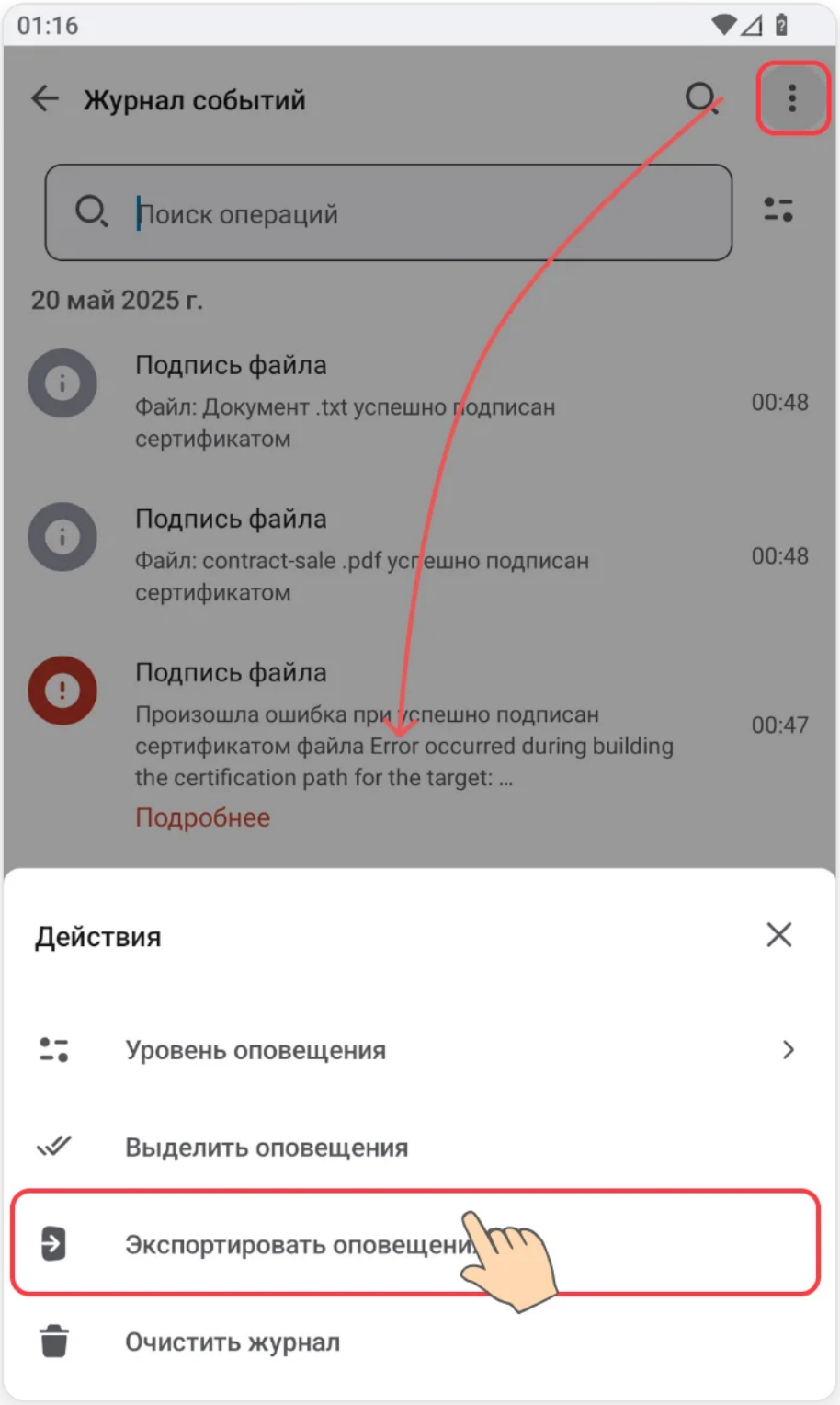
Журнал событий можно выгрузить в текстовый файл.

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.