Цифровые технологии

КриптоАРМ Защищенная почта

Документация продукта

Релиз v7.2

Архивная документация. Актуальный релиз: v7.3

Исходная документация на CryptoARM.ru

Редакция от 26.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

КриптоАРМ 7 — защищённая почта и электронная подпись 4

Общие сведения

- О продукте 6
- Поддерживаемые криптопровайдеры 12
- Глоссарий 14

Установка

- Установка на Windows 21
- Установка на Linux 33
- Установка на macOS 48
- Активация лицензии 58

Начало работы

- Быстрый старт 64
- Общие настройки 66
- Уведомления и журнал событий 70
- Проверка обновлений 76

Почта

- Подключение почтового аккаунта 80
- Подключение аккаунта Mail.ru 88
- Подключение аккаунта Yandex 91
- Подключение аккаунта Gmail 94
- Подключение аккаунта Outlook 97
- Подключение аккаунта iCloud 100
- Подключение аккаунта Rambler 103
- Почтовые настройки 106
- Создание нового письма 120
- Работа с письмами 135
- Автоматизация почты 157
- Работа с расширениями .eml, .p7s, .p7m 168

Документы

- Обзор операций и выбор мастера 171

Профиль подписи ... 176
Подпись и шифрование ... 189
Проверка и расшифрование ... 204
Подпись и защита PDF ... 215
Настройки подписи и шифрования ... 230
Управление документами ... 247
Выполнение операций в командной строке ... 255

Сертификаты

Управление сертификатами ... 266
Установка сертификатов ... 273
Создание запроса и самоподписанного сертификата ... 287
Экспорт и удаление сертификатов ... 297
Действия с ключевыми контейнерами ... 304

Контакты

Работа с контактами ... 308
Адресные книги ... 324

API

Описание API КриптоАРМ ... 335
Команда signAndEncrypt ... 342
Команда certificates ... 361
Команда certrequests ... 372
Команда diagnostics ... 381
Команда startView ... 390
Команда mail ... 395
Команда saveDocuments ... 402
Команда authorize ... 407
Команда mtlsAuthorization ... 413

Открыть статью на сайте

title: КриптоАРМ 7 — защищённая почта и электронная подпись description: КриптоАРМ 7 — программа для шифрования, подписи и обмена защищёнными письмами. Узнайте возможности и начните использовать уже сегодня. keywords: - КриптоАРМ 7 - КриптоАРМ - электронная подпись - шифрование данных - защищённая почта author: Команда date: 2026-05-50 updated: 2025-05-05

КриптоАРМ 7

КриптоАРМ — отечественная программа, сочетающая в себе функции почтового клиента и программы для подписания и шифрования информации.

- Работает на Windows, macOS, Linux (в том числе российские ОС).
- Совместим с криптопровайдером СКЗИ «КриптоПро CSP» 5.0 R2 и выше.

Позволяет организовать юридически значимый электронный документооборот по e-mail и передавать конфиденциальную информацию в зашифрованном виде по Интернету.

КриптоАРМ версии 7 — почтовый клиент с возможностью обмена защищёнными письмами и работы с документами, который включает в себя следующую функциональность:

- обмен подписанными и зашифрованными письмами;
- работа с документами, подпись и проверка подписи, шифрование и расшифрование;
- создание единого пакета документов с приложенной машиночитаемой доверенностью;
- встроенная подпись для PDF-документов с визуализацией электронной подписи и сертификацией файла для защиты от изменений;
- предустановленная лицензия для ознакомительного использования, которая активируется при первом запуске программы и действует в течение 30 дней;
- интеграция в информационные системы с помощью API и SDK.

КриптоАРМ 7 похож по интерфейсу и функциональности на **КриптоАРМ ГОСТ 3** и включает в себя все новые возможности.

> **Важно:** приобретённые ранее лицензии на ПО **КриптоАРМ ГОСТ версии 3 Защищённая почта** не подойдут для работы с **КриптоАРМ версии 7**.

По истечении срока действия годовой и ознакомительной лицензии на **КриптоАРМ** вы можете использовать его в качестве бесплатного почтового клиента и обмениваться письмами без функций подписи, шифрования и расшифрования писем и документов.

Сертифицированные версии КриптоАРМ

Линейка сертифицированных продуктов **КриптоАРМ** включает в себя **КриптоАРМ ГОСТ версии 3** и **версии 2.5**:

- **КриптоАРМ ГОСТ 3** сертифицирован с КриптоПро CSP версии 5.0 R3 — защищённый почтовый клиент и работа с электронными документами в одном окне;
- **КриптоАРМ ГОСТ 2.5** сертифицирован с КриптоПро CSP версии 5.0 R2 — работа с электронными документами (подпись и проверка подписи, шифрование и расшифрование).

Открыть статью на сайте

КриптоАРМ — приложение для электронной подписи и защиты документов

КриптоАРМ — это кроссплатформенное программное обеспечение для создания и проверки электронной подписи, шифрования файлов и безопасного обмена электронными документами.

КриптоАРМ предназначен для юридически значимого электронного документооборота между организациями, государственными органами и частными лицами, а также для защиты конфиденциальных данных.

Содержание:

- Основные возможности КриптоАРМ
- Совместимость и условия эксплуатации
- Лицензирование
- Системные требования
- Поддерживаемые операционные системы
- Смотрите также

Основные возможности КриптоАРМ

КриптоАРМ предоставляет полный набор инструментов для работы с электронной подписью, сертификатами, шифрованием данных и защищённой электронной почтой.

Электронная подпись

- создание электронной подписи произвольных файлов;
- проверка электронной подписи;
- создание присоединённой и отсоединённой электронной подписи;
- создание соподписей;
- поддержка стандартов электронной подписи CAdES-BES, CAdES-T, CAdES-X Long Type 1, CAdES-A;
- формирование отчётов о проверке электронной подписи в формате PDF;
- снятие и объединение электронных подписей.

Подпись документов формата PDF

- подписание и сертификация документов формата PDF;
- поддержка стандартов PAdES-BES, PAdES-T, PAdES-X Long Type 1, PAdES-A;
- разметка областей размещения подписей и подписантов;

- добавление текстовых и графических элементов;
- преобразование документов в форматы PDF/A-2b и PDF/A-3b.

Шифрование и расшифрование данных

- шифрование и расшифрование файлов;
- поддержка стандарта PKCS#7;
- шифрование данных для одного или нескольких получателей;
- шифрование данных по сертификатам контактов;
- автоматическое удаление исходных файлов после шифрования (при настройке).

Архивирование данных

- архивирование файлов перед выполнением операций шифрования;
- разархивирование файлов из формата ZIP.

Управление контактами

- создание, редактирование, удаление и восстановление локальных контактов;
- импорт контактов из LDAP-каталогов;
- поддержка формата vCard и протокола CardDAV;
- группировка, поиск и сортировка контактов;
- поиск дубликатов и объединение записей;
- отправка зашифрованных и подписанных сообщений в адрес контактов и групп.

Управление сертификатами и ключами

- отображение сертификатов и связанных с ними закрытых ключей;
- проверка корректности сертификатов с построением цепочки доверия;
- создание запросов на сертификаты;
- импорт, экспорт и удаление сертификатов;
- формирование отчётов о действительности сертификатов;
- работа с аппаратными ключевыми носителями при использовании поддерживаемых криптопровайдеров.

Защищённая электронная почта

- подключение почтовых аккаунтов по протоколам SMTP(S), IMAP(S), POP3;
- поддержка почтовых серверов Microsoft Exchange и CommuniGate;
- получение, отправка, хранение и удаление электронных сообщений;
- подпись и шифрование электронных писем;
- автоматическая проверка подписи и расшифрование входящих сообщений;
- локальное и зашифрованное хранение почтовых данных.

Журналирование и уведомления

- ведение журнала событий;

- просмотр, фильтрация и сортировка событий;
- экспорт журналов в файл формата .log;
- печать и передача журналов.

Совместимость и условия эксплуатации

Поддерживаемые криптопровайдеры

КриптоАРМ поддерживает два типа криптопровайдеров, каждый из которых предназначен для работы с определёнными криптографическими стандартами:

1. **Встроенная библиотека OpenSSL (версии 1.1.1)**
    - реализует криптографические операции по международным стандартам: RSA, ECDSA, AES и др.;
    - не поддерживает российские криптографические алгоритмы ГОСТ;
2. **КриптоПро CSP (версии 5.0 и выше)** — обеспечивает выполнение криптографических операций с использованием российских алгоритмов ГОСТ (ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ 28147-89 и др.) и необходим для:
    - работы с сертификатами, выданными по российским стандартам ГОСТ;
    - создания электронной подписи, отвечающей требованиям законодательства РФ;
    - использования аппаратных ключевых носителей.

Поддерживаемые ключевые носители

При использовании криптопровайдера КриптоПро CSP поддерживается работа с аппаратными ключевыми носителями:

- РУТОКЕН ЭЦП 3.0 (ФОРМ-ФАКТОРЫ УКАЗАНЫ В ФОРМУЛЯРЕ НА РУТОКЕН ЭЦП 3.0);
- JaCarta,
- ESMART,
- ФОРОС,
- АНГАРА.

Актуальный список поддерживаемых носителей приведён в формуляре криптопровайдера КриптоПро CSP.

Лицензирование

Общая информация о лицензиях

Для выполнения криптографических операций с алгоритмами ГОСТ требуется лицензия.

Доступны следующие варианты лицензии:

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

Пробная лицензия

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

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

Лицензия на рабочее место

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

Особенности:

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

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

- КриптоАРМ версии Подпись и шифрование, годовая
- КриптоАРМ версии Защищенная почта, годовая
- КриптоАРМ версии Подпись и шифрование, бессрочная
- КриптоАРМ версии Защищенная почта, бессрочная

Лицензия пользователя информационной системы

Лицензия на пользователя информационной системы предназначена для работы с КриптоАРМ, который интегрирован с внешней системой через API.

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

Особенности:

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

Расширенная лицензия

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

Как работает расширенная функция:

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

Приобрести лицензии можно в официальном интернет-магазине kloud.one.

- Лицензия на одного пользователя информационной системы, расширенная, на 12 месяцев
- Лицензия на одного пользователя информационной системы, на 12 месяцев

Системные требования

Минимальные и рекомендуемые системные требования приведены в таблице ниже.

Компонент	Минимальная конфигурация	Рекомендуемая конфигурация
Процессор	x86-64, 1.0 ГГц	x86-64, 2.0 ГГц+
ОЗУ	2 ГБ	4 ГБ+
Дисковое пространство	500 МБ	5 ГБ+
Дисплей	1024×768	1920×1080+

Поддерживаемые операционные системы

Клиентские операционные системы

- Windows 10, 11
- Astra Linux Special Edition 1.7, 1.8
- Альт Рабочая станция 10, 11
- Альт СП релиз 10
- АльтерОС 2025
- РЕД ОС 7.3, 8
- РОСА «ХРОМ»
- ОС «Атлант»
- МСВСфера АРМ
- ОС ОН "ОСнова"
- Ubuntu 20.04, 22.04

- macOS 11–15, 26 (Big Sur, Monterey, Ventura, Sonoma, Sequoia, Tahoe)

Серверные операционные системы

- Windows Server 2016, 2019
- Альт Сервер 10, 11
- Astra Linux Server
- Ubuntu Server 20.04, 22.04
- CentOS 8
- РОСА Хром Сервер
- РЕД ОС «Сервер»
- МСВСфера Сервер
- ОС ОН "ОСнова"

Смотрите также

- Поддерживаемые криптопровайдеры — обзор поддерживаемых криптопровайдеров в КриптоАРМ.
- Установка на Windows — руководство по установке КриптоАРМ на Windows.
- Установка на Linux — руководство по установке КриптоАРМ на Linux.
- Установка на macOS — руководство по установке КриптоАРМ на macOS.

Открыть статью на сайте

Поддерживаемые криптопровайдеры в КриптоАРМ

В приложении КриптоАРМ реализована поддержка как российских стандартов ГОСТ через КриптоПро CSP, так и международных алгоритмов через встроенную библиотеку OpenSSL. Эта статья поможет разобраться в их отличиях и выбрать нужный для ваших задач.

Содержание:

- Что такое криптопровайдер
- Особенности в российском сегменте
- Поддерживаемые криптопровайдеры в КриптоАРМ
- Инструкции по установке КриптоПро CSP

Что такое криптопровайдер

Криптопровайдер (CSP — Cryptography Service Provider) — это специализированный программный модуль, интегрируемый в операционную систему, который обеспечивает выполнение криптографических операций и управление криптографической инфраструктурой.

Криптопровайдер выполняет ключевые функции:

- Генерация и хранение криптографических ключей
- Создание и проверка электронной подписи (ЭП)
- Шифрование и расшифрование данных
- Обеспечение целостности и подлинности информации
- Работа с аппаратными ключевыми носителями (токены, смарт-карты)

Принцип работы криптопровайдера

Криптопровайдер выступает посредником между:

1. **Операционной системой**, предоставляющей интерфейсы безопасности;
2. **Пользовательскими приложениями**, которым необходима защита данных и электронная подпись;
3. **Аппаратными средствами**, такими как токены и смарт-карты.

Приложения обращаются к CSP через стандартизированные API, что позволяет унифицировать работу с различными криптопровайдерами и аппаратными устройствами.

Особенности в российском сегменте

В России использование встроенных криптопровайдеров Windows **не допускается** для работы с государственными органами и юридически значимыми документами, так как они **не сертифицированы ФСБ России** как средства криптографической защиты информации, соответствующие российским криптографическим стандартам ГОСТ. Сертификация обязательна для СКЗИ, используемых в государственных системах и для работы с юридически значимыми документами.

При работе с государственными органами или в ситуациях, требующих применения сертифицированных СКЗИ, необходимо использовать решения, прошедшие сертификацию ФСБ России и поддерживающие российские криптоалгоритмы (ГОСТ Р 34.10-2012 для электронной подписи, ГОСТ Р 34.11-2012 для хеширования, ГОСТ 28147-89 для шифрования и др.).

Для работы с российскими алгоритмами ГОСТ в приложении КриптоАРМ используется **КриптоПро CSP** — криптопровайдер СКЗИ, разработанный компанией «КриптоПро».

Поддерживаемые криптопровайдеры в КриптоАРМ

В приложении КриптоАРМ реализована поддержка двух типов криптопровайдеров:

- **Российские алгоритмы ГОСТ** — через криптопровайдер **КриптоПро CSP**, который обеспечивает создание квалифицированной электронной подписи, работу с сертификатами ГОСТ и аппаратными ключевыми носителями.
- **Международные алгоритмы** — через встроенную библиотеку **OpenSSL**, используемую для криптографических операций по международным стандартам.

> 🔍 Более подробная информация о поддерживаемых криптопровайдерах, их возможностях и совместимых ключевых носителях доступна в основной статье: КриптоАРМ — приложение для защиты ваших файлов.

Инструкции по установке КриптоПро CSP

Выберите вашу операционную систему:

- Windows
- macOS
- Linux

Открыть статью на сайте

Глоссарий терминов КриптоАРМ

- Сертификаты
- Подпись и шифрование
- Почта

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.

Сертификация PDF документа

Позволяет защитить PDF документ от изменений путем его подписания электронной подписью, с указанием типа изменений, разрешенных для документа.

Конвертация PDF документа

При конвертации PDF документа происходит удаление скриптов, форм и прочих элементов, влияющих на безопасность и целостность документа.

Формат подписи CadES

Стандарт электронной подписи, представляющий собой расширенную версию стандарта электронной подписи CMS. Эту электронную подпись можно прикрепить к любому типу файла : текстовым файлам (.doc, .docx), электронным таблицам (.xls, .xlsx), изображениям (.jpg, .png, .gif) и PDF-файлам.

Формат подписи PadES

Формат, при котором подпись встраивается в PDF-документ. «Встроенная» подпись позволяет подписывать электронные документы без изменения формата файла и без создания отдельного файла подписи, как это происходит при использовании присоединенной и отсоединенной подписи соответственно. Подпись встраивается в электронный документ, и получатель может проверить документ на действительность электронной подписи.

Видимая подпись PDF документа

«Встроенная» подпись, которая отображается на странице документа в виде штампа.

Невидимая подпись PDF документа

«Встроенная» подпись, которая визуально на страницах не видна.

Область для штампа подписи в PDF документе

Область на странице PDF документа, размеченная для видимой подписи.

Произвольная область в PDF документе

Область для графического изображения или текста. В области можно разместить свой комментарий, статус или отметку о конфиденциальности документа.

Почта

Адрес электронной почты

Название электронного почтового ящика, который может получать (и отправлять) электронные письма в сети (например, в интернете или в локальной сети, не подключённой к интернету).

Почтовый сервер

Это программа, работающая у интернет-провайдеров и на крупных сайтах и используемая для передачи почты. Обычно пользователи не взаимодействуют с почтовыми серверами напрямую: электронная почта отправляется с помощью почтового клиента на почтовый сервер, который доставляет её в почтовый клиент получателя.

Почтовый клиент

Это программа (например, на компьютере или мобильном устройстве), которая используется для чтения и отправки электронных сообщений.

IMAP

Протокол, который используется для получения сообщений электронной почты с сервера. IMAP позволяет почтовым программам получать доступ не только к новым сообщениям, но и к папкам на сервере. Действия синхронизируются между несколькими почтовыми программами, подключёнными через IMAP.

POP

Протокол, который используется для получения сообщений электронной почты с сервера. В отличие от IMAP, POP позволяет почтовому клиенту загружать только последние сообщения, которыми можно управлять в клиенте и на устройстве.

SMTP

Протокол, который используется для передачи электронной почты. Он определяет формат сообщений и процедуру их передачи через Интернет от отправителя к получателю с помощью почтовых серверов.

S/MIME

Стандарт для шифрования и подписи электронных писем с помощью открытого ключа.

SSL

Протокол, который обеспечивает безопасное соединение между клиентом и сервером.

Логин (имя пользователя)

Имя почтового ящика — комбинация из букв и цифр, которая, как правило, находится в адресе перед именем домена.

Пароль

Набор символов, предназначенный для подтверждения личности.

Скрытая копия

Копия электронного письма, отправленного получателю, адрес электронной почты которого не указан (в качестве получателя) в сообщении

Копия

Копия электронного письма, отправленного получателю, адрес электронной почты которого указан в поле заголовка «Копия».

Тело письма

Основная часть электронного письма, которая содержит текст, изображения и другие данные (например, прикреплённые файлы).

LDAP

Протокол быстрого доступа к каталогам. Он позволяет получать и принимать через сеть данные из каталогов с иерархической структурой.

ALD Pro

Служба каталога для Linux, программный комплекс централизованного управления компьютерами с помощью групповых политик, а также прикладными сервисами для ИТ-инфраструктур организаций различного масштаба. Комплекс создан «Группой Астра».

CardDAV

Протокол адресной книги, предназначенный для предоставления пользователям доступа к данным на сервере.

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.

Gravatar

Сервис компании Automattic, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.

Открыть статью на сайте

Пошаговая установка КриптоАРМ на Windows

В этом разделе мы расскажем, как установить КриптоАРМ на ОС Windows. Вы узнаете, как подготовить систему, установить КриптоАРМ и КриптоПро CSP, а также где найти инструкции по активации лицензий.

Содержание:

- Подготовка к установке
- Установка КриптоАРМ
- Установка КриптоПро CSP
- Активация лицензий
- Удаление КриптоАРМ
- Смотрите также

Подготовка к установке

Перед установкой

1. **Проверьте наличие прав администратора**. Для установки КриптоАРМ и связанных компонентов требуются права администратора. Убедитесь, что у вас есть соответствующие привилегии на компьютере.

2. **Установите Microsoft Visual C++ 2015-2022 Redistributable**. Этот пакет позволяет Windows запускать программы, созданные с помощью Visual C++. На 64-битной системе установите x86 и x64 версии.

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте установочный файл КриптоАРМ с официальных источников:

- Официальный сайт КриптоАРМ
- Сайт компании-разработчика Trusted.ru

Дистрибутив КриптоПро CSP (при использовании ГОСТ-алгоритмов)

> ⚠️ **Примечание**: КриптоАРМ можно использовать без установки КриптоПро CSP, если ваши сценарии работы не требуют выполнения криптографических операций с алгоритмами ГОСТ.

Скачайте дистрибутив КриптоПро CSP с официального сайта компании ООО «КРИПТО-ПРО» или используйте компакт-диск.

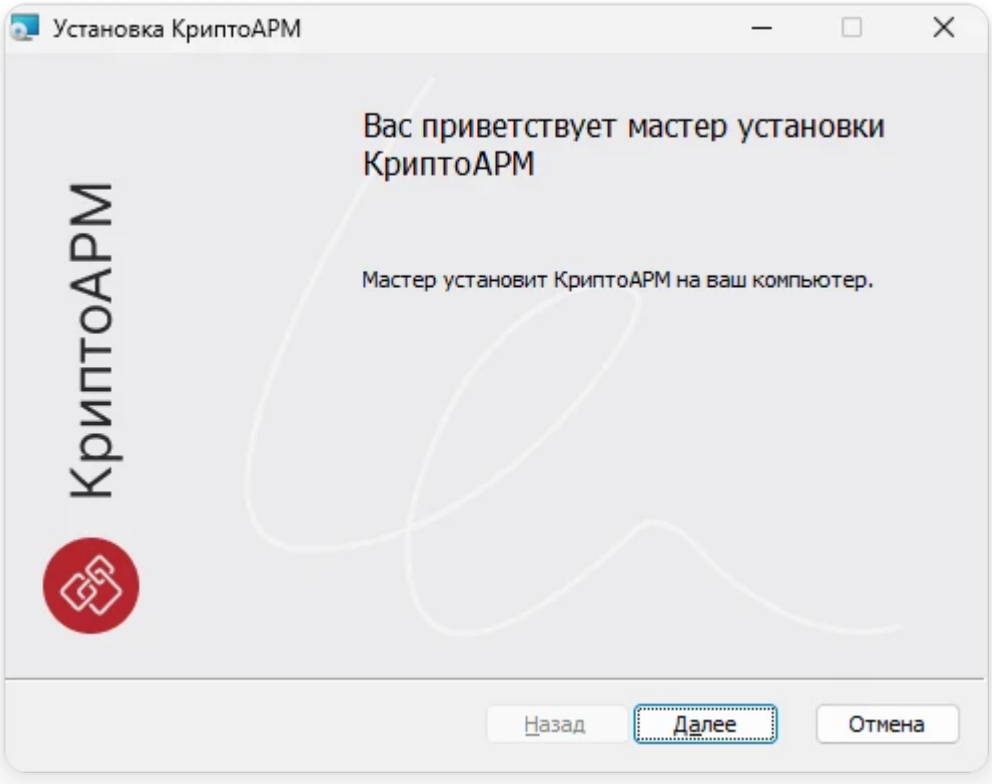
Чтобы загрузить дистрибутив КриптоПро CSP из официального источника:

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

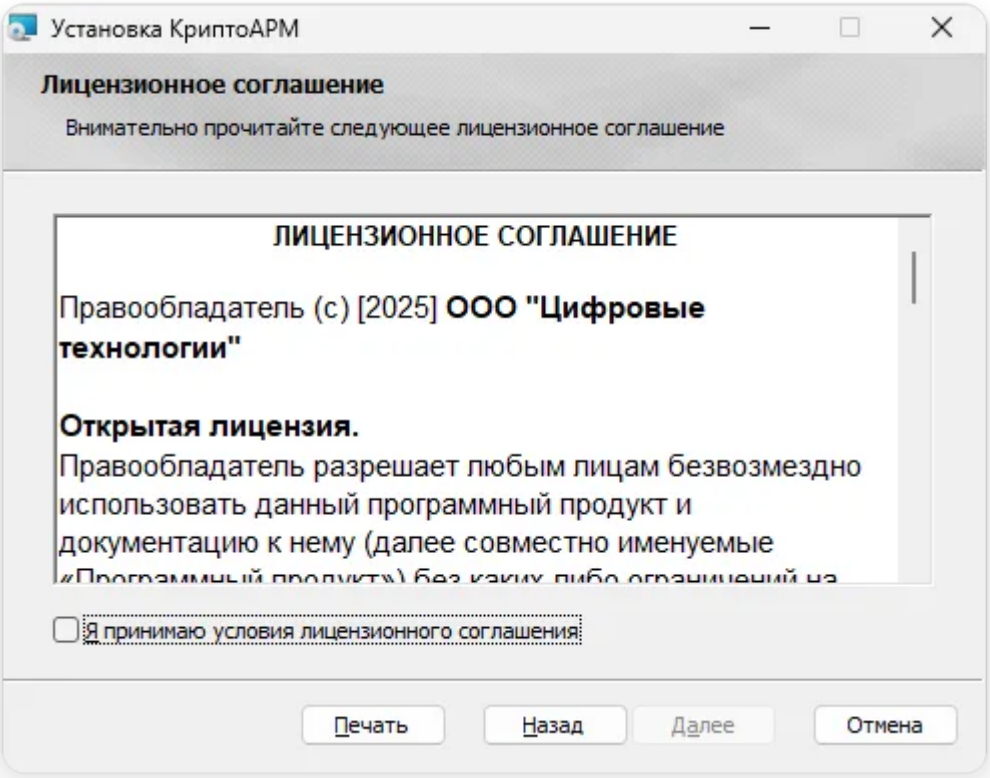
> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше

Установка КриптоАРМ

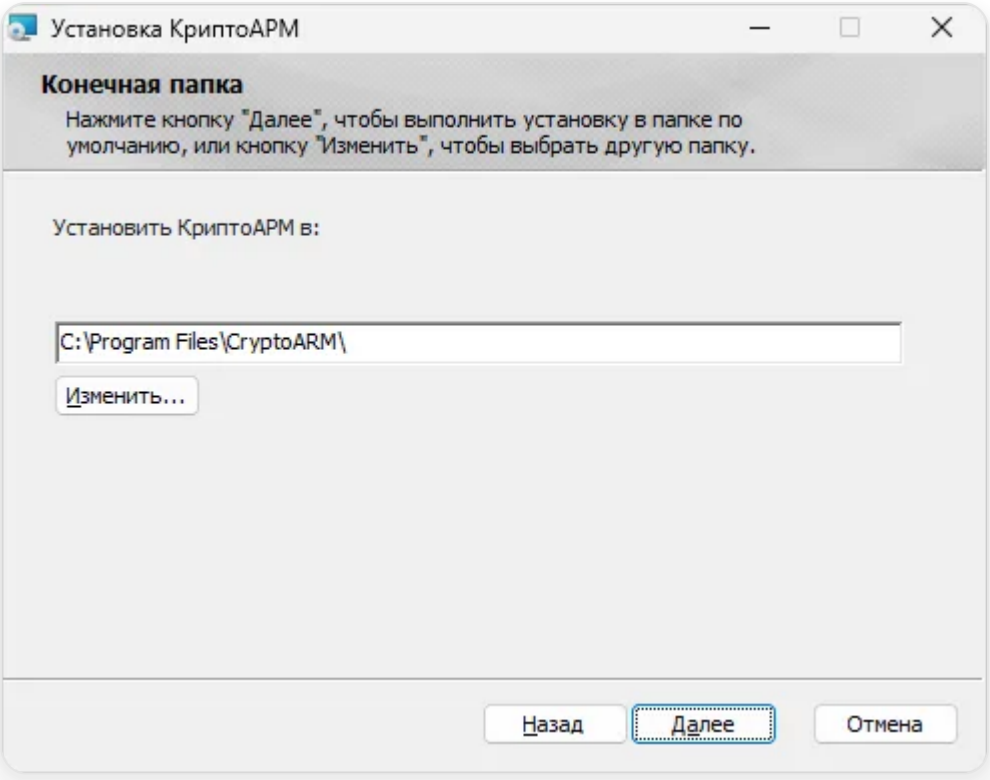
1. Запустите установочный файл КриптоАРМ.
2. Откроется мастер установки. Нажмите **Далее**.



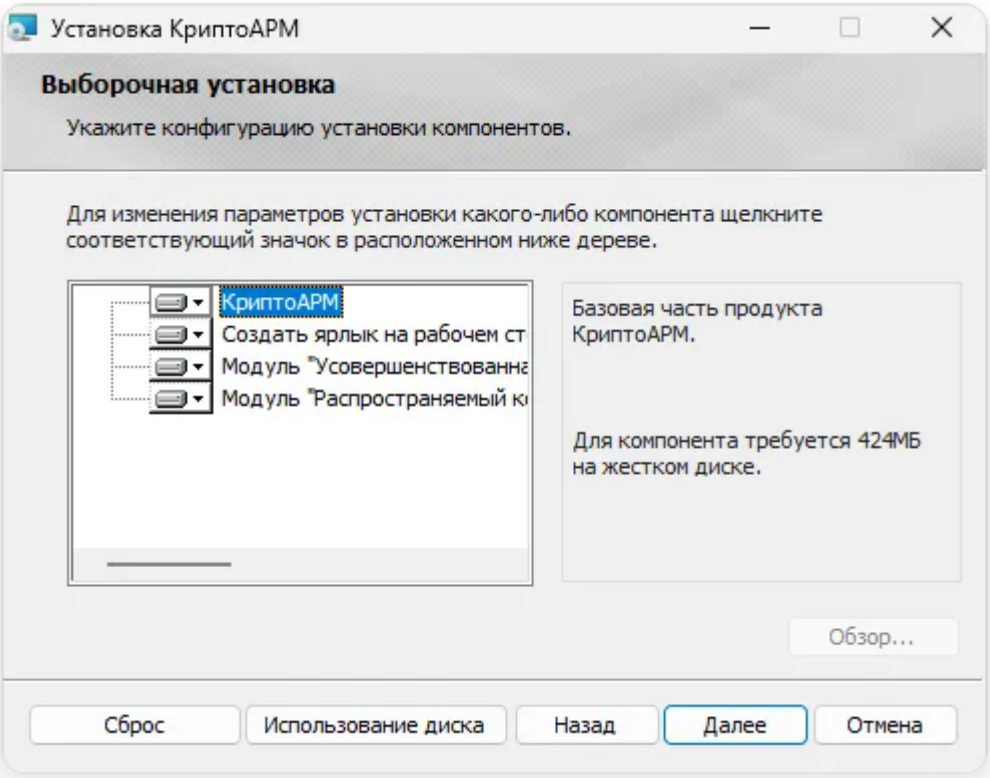
3. Ознакомьтесь с условиями лицензионного соглашения. Если вы согласны со всеми пунктами, нажмите **Принять**, затем нажмите **Далее**.



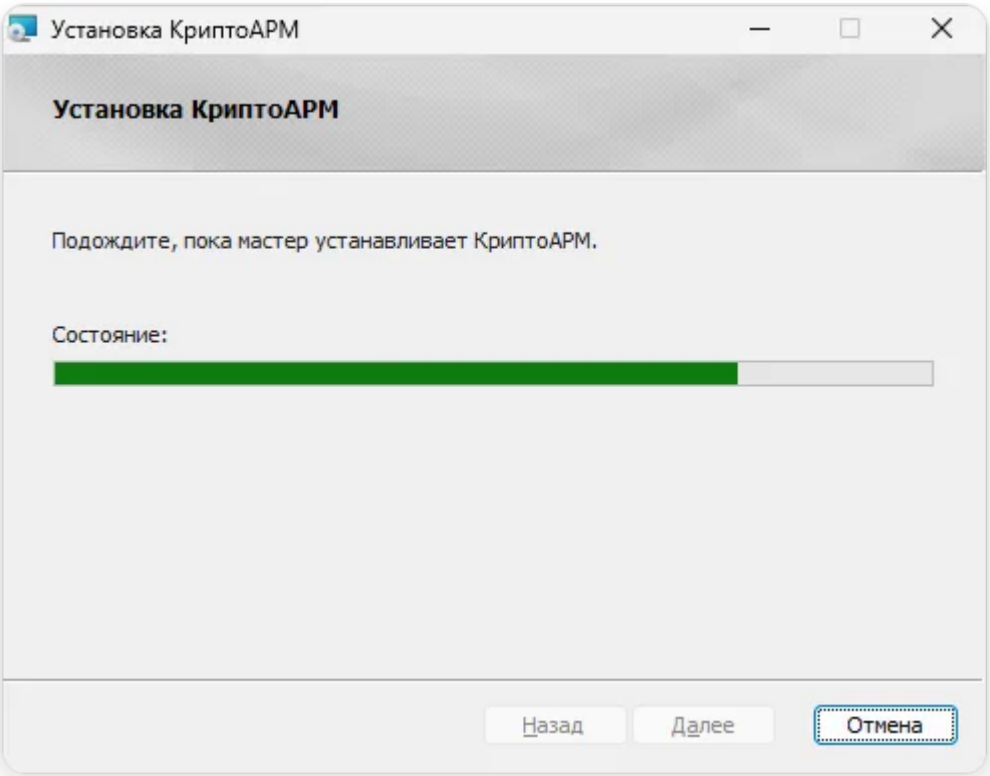
4. Выберите каталог для установки приложения. По умолчанию приложение устанавливается в каталог `%ProgramFiles%\CryptoARM\`.



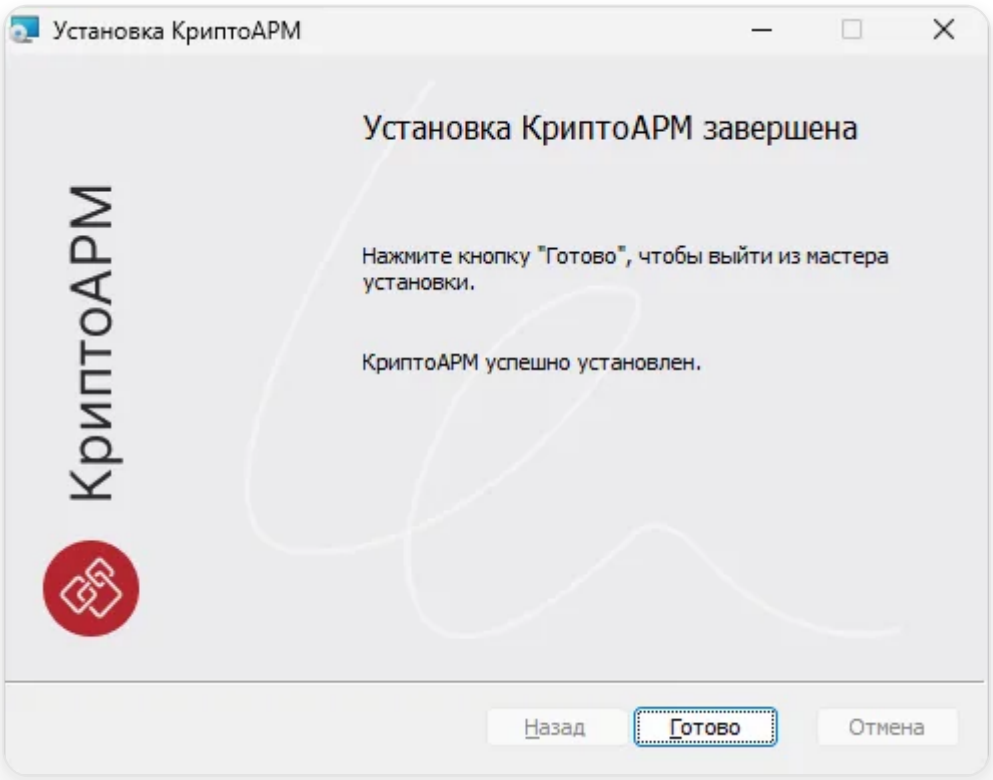
5. При необходимости выберите компоненты и запустите установку.



6. Дождитесь окончания установки.



Закройте окно установки по кнопке **Готово**.

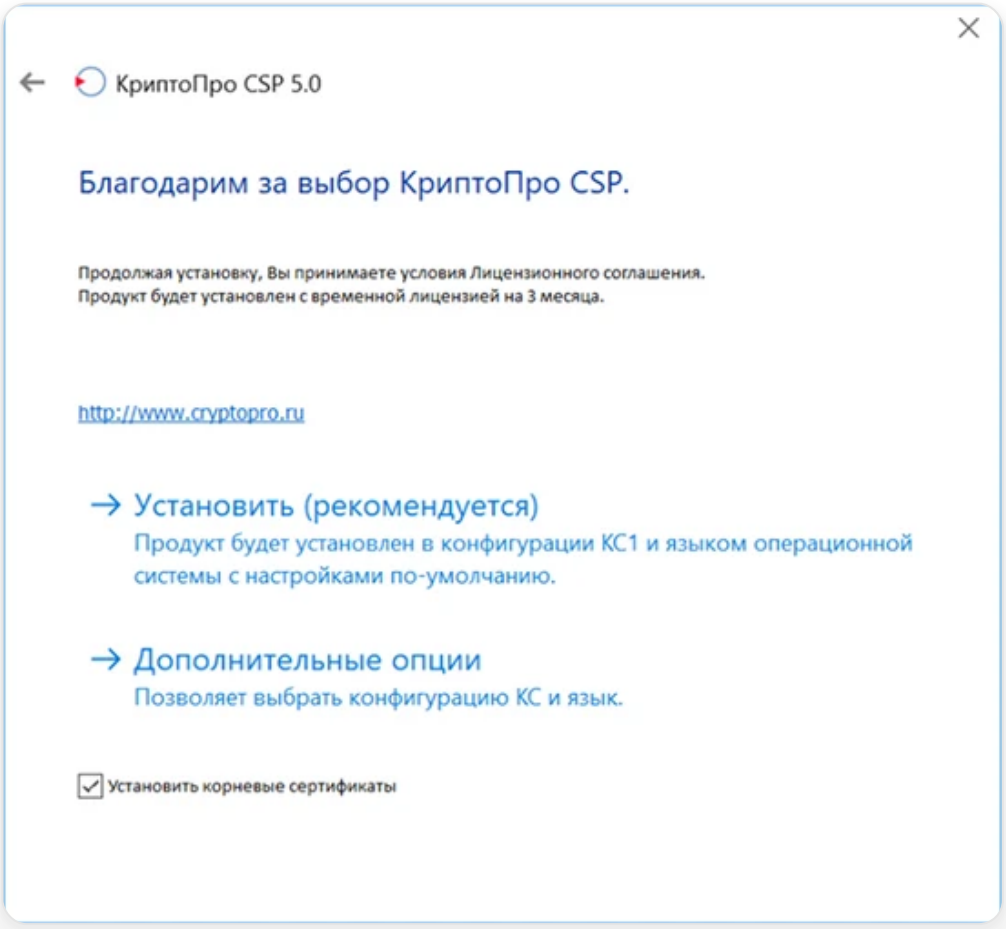


Установка КриптоПро CSP

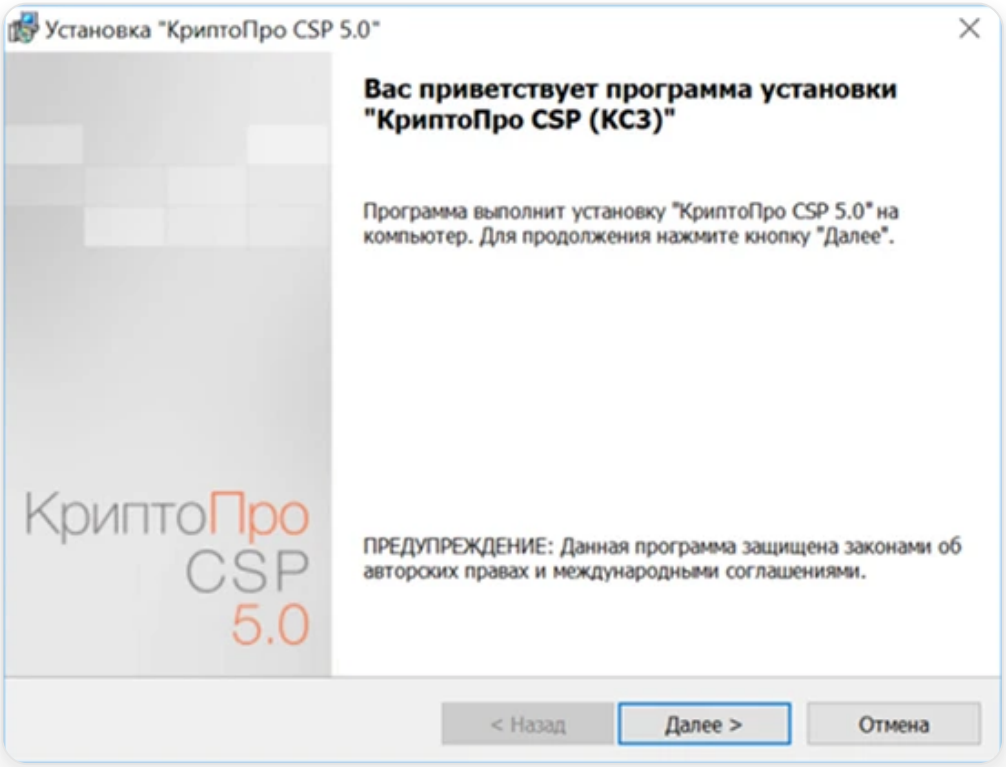
1. Запустите скачанный дистрибутив КриптоПро CSP. Если используется компакт-диск, в стартовом меню диска выберите систему и язык установки.



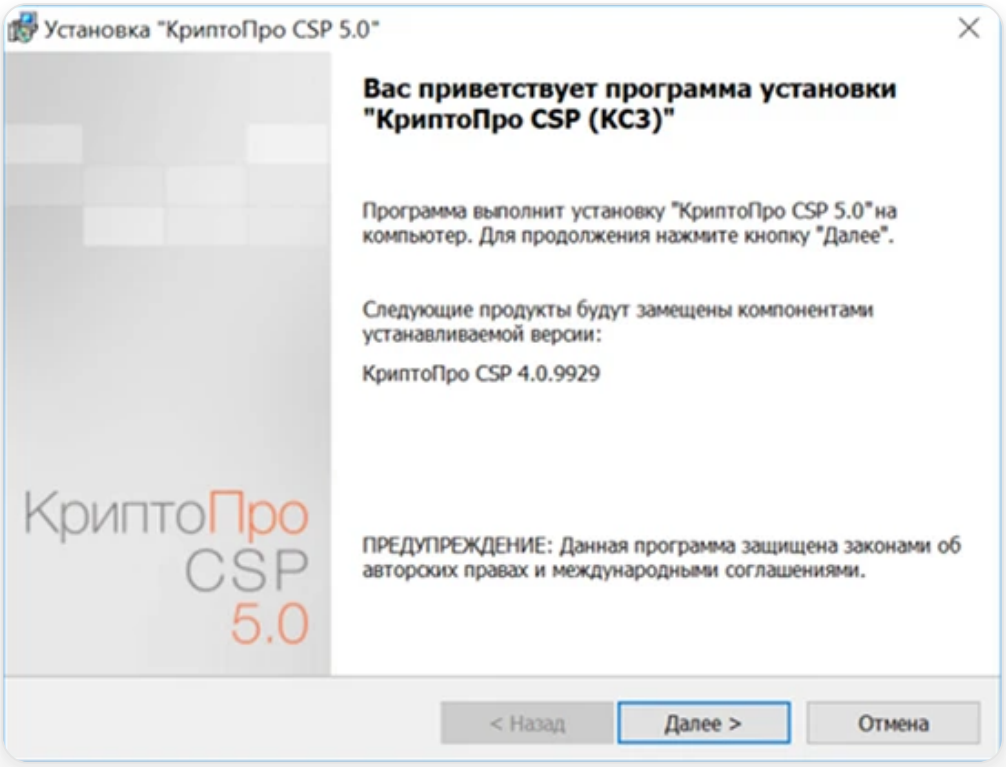
2. Откроется приветственное окно мастера установки КриптоПро CSP. Для изменения уровня класса защиты или языка установки нажмите кнопку **Дополнительные опции**.



3. Последующая установка производится в соответствии с сообщениями, выдаваемыми программой установки. В процессе установки будет предложено зарегистрировать дополнительные считыватели ключевой информации, дополнительные датчики случайных чисел или настроить криптопровайдер на использование дополнительной защиты. Для продолжения установки нажмите **Далее**.

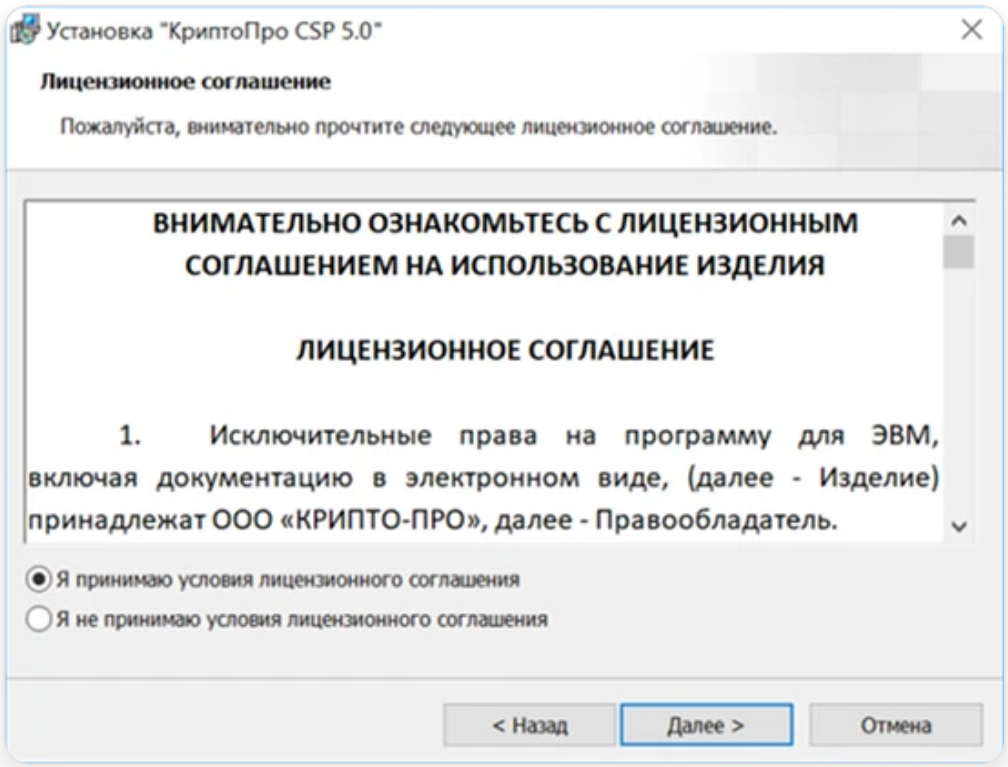


4. Если в системе была установлена более ранняя версия КриптоПро CSP, то в окне установки появится информация о текущей версии. Для продолжения установки нажмите **Далее**.

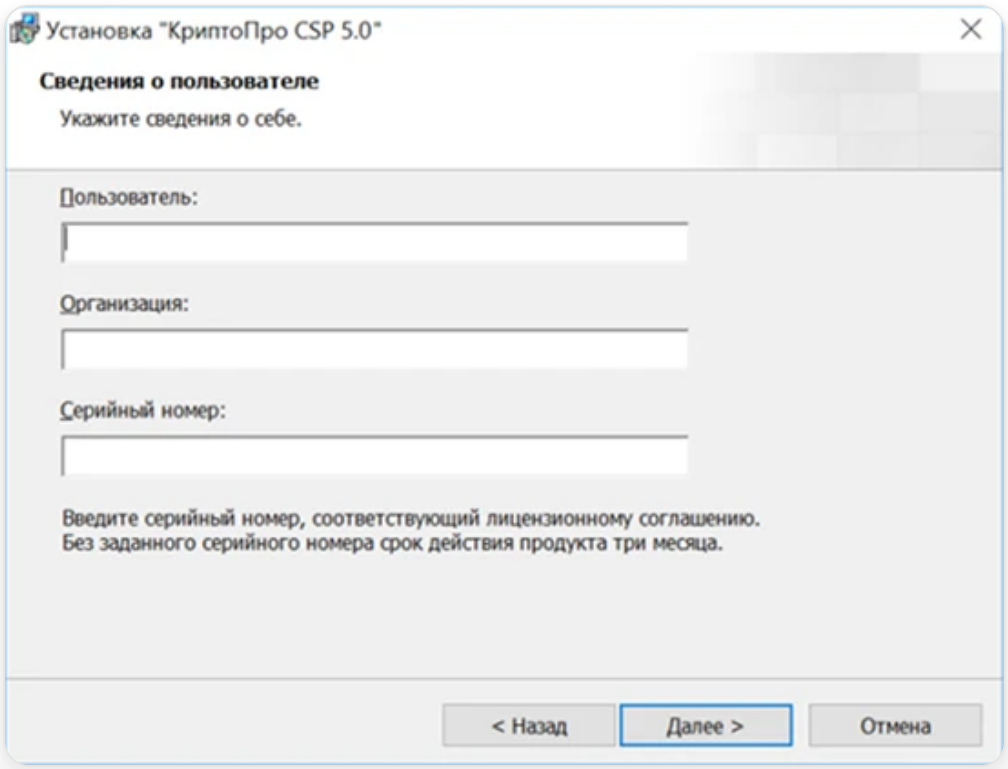


5. Внимательно ознакомьтесь с лицензионным соглашением.

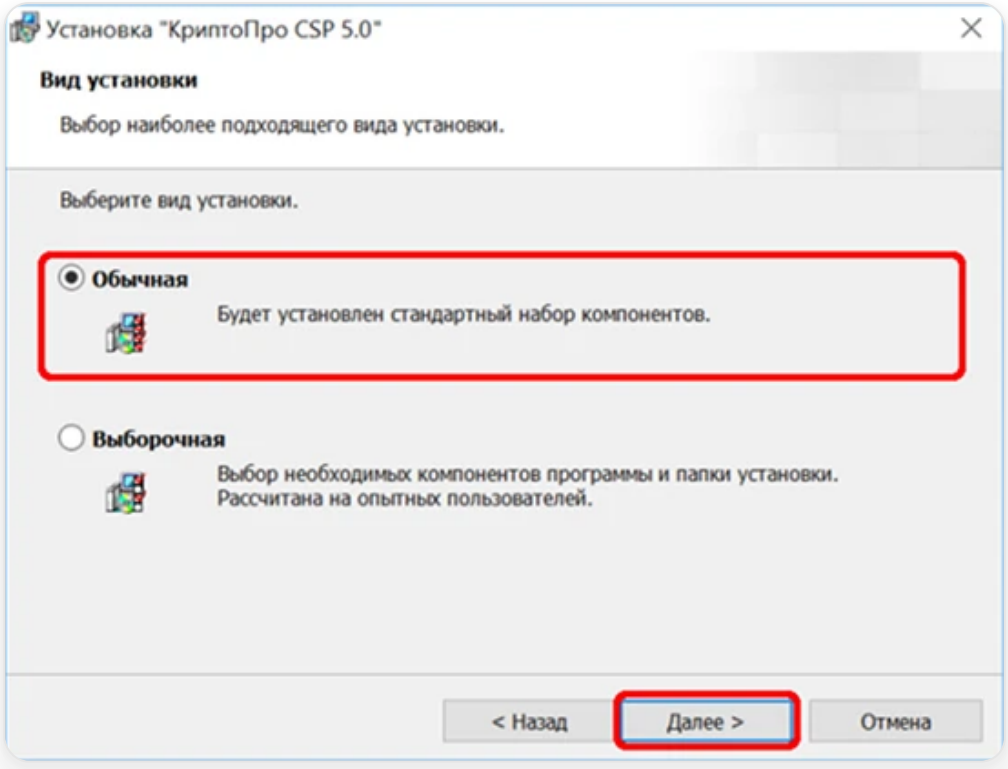
Выберите опцию **Я принимаю условия лицензионного соглашения** и нажмите **Далее** для продолжения установки.



6. В окне сведений о пользователе можно ввести данные о пользователе, организации и серийный номер лицензии. Эти данные можно вести позже в процессе работы с программой. Для продолжения установки нажмите **Далее**.

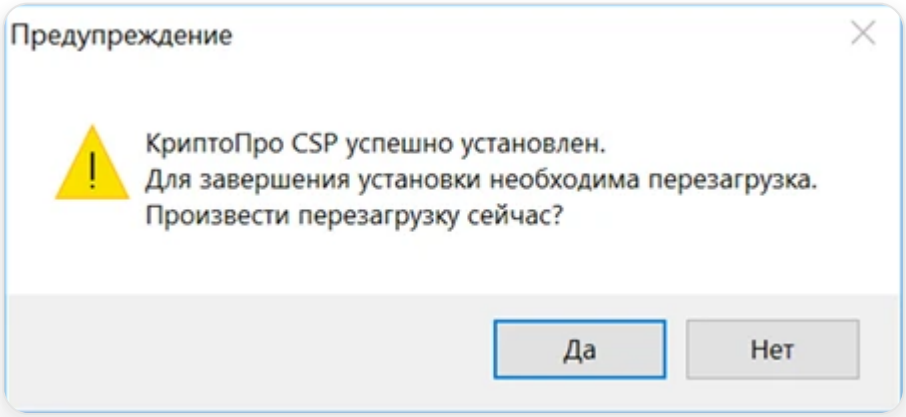


7. Выберите тип установки — **Обычная** (стандартный набор компонентов) и нажмите **Далее**.



8. Дождитесь окончания установки.

9. После успешной установки криптопровайдера выполните перезагрузку системы.



Активация лицензий

Для выполнения криптографических операций с алгоритмами ГОСТ необходимо активировать лицензию «КриптоАРМ версии Про».

Инструкции по активации лицензий:

- Активация лицензии КриптоАРМ — подробное руководство по установке лицензии КриптоАРМ.
- Активация лицензии КриптоПро CSP — только при использовании CSP. Содержит руководство по установке лицензии КриптоПро через интерфейс КриптоАРМ.

При первом запуске КриптоАРМ автоматически активируется **30-дневная пробная лицензия**, которая позволяет полностью ознакомиться со всеми возможностями приложения и протестировать работу криптографических операций с российскими алгоритмами ГОСТ.

При первой установке криптопровайдера КриптоПро CSP может быть активирована ознакомительная лицензия (обычно сроком до 90 дней).

> 💡 Пробный период КриптоАРМ и ознакомительная лицензия КриптоПро CSP действуют независимо друг от друга.

Удаление КриптоАРМ

Через стандартный интерфейс Windows

1. Откройте **Панель управления** → **Программы и компоненты** (или **Приложения и возможности** в Windows 10/11).
2. Найдите в списке **КриптоАРМ**.

3. Нажмите на программу правой кнопкой мыши и выберите **Удалить** или **Удалить/Изменить**.
4. В открывшемся окне мастера удаления нажмите **Далее**, затем подтвердите удаление.
5. Дождитесь завершения процесса и закройте мастер.

> 💡 После удаления ярлык приложения исчезнет из меню **Пуск**, а файлы программы будут удалены из каталога установки (по умолчанию `%ProgramFiles%\CryptoARM\`).

Очистка остаточных файлов

После стандартного удаления могут оставаться папки с файлами приложения:

- `%ProgramFiles%\CryptoARM\`
- `%AppData%\CryptoARM`
- `%ProgramData%\CryptoARM`

Удалите их вручную, если необходимо полностью очистить систему.

> 💡 Будьте осторожны при удалении файлов в `%AppData%` и `%ProgramData%` — убедитесь, что удаляете только папки, связанные с КриптоАРМ.

Смотрите также

- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.
- Быстрый старт — инструкция по первому запуску и базовой настройке КриптоАРМ.

Открыть статью на сайте

Пошаговая установка КриптоАРМ на Linux

В этом разделе мы расскажем, как установить КриптоАРМ КриптоАРМ на ОС Linux (RPM и DEB). Вы узнаете, как подготовить систему, установить КриптоАРМ и КриптоПро CSP, а также где найти инструкции по активации лицензий.

Содержание:

- Подготовка к установке
- Установка КриптоАРМ
- Установка КриптоПро CSP
- Активация лицензий
- Удаление КриптоАРМ
- Смотрите также

Подготовка к установке

Перед установкой

1. **Права администратора**

   Проверьте наличие прав суперпользователя (`root`) или возможности использовать `sudo`. Для установки КриптоАРМ и связанных компонентов требуются соответствующие привилегии на компьютере.

2. **Библиотека** `libsasl2`

   Для работы приложения требуется библиотека `libsasl2`. Если установлена только версия `libsasl2.so.3`, создайте символическую ссылку на `libsasl2.so.2`:

```
apt-get install libsasl2
ln -s /lib64/libsasl2.so.3.0.0 /lib64/libsasl2.so.2
```

Это обеспечит совместимость приложения с библиотекой.

1. **Дополнительные зависимости для Ubuntu 20.04**

   На Ubuntu 20.04 необходимо установить следующие пакеты:

```
sudo apt install libtidy-dev
sudo apt install libctemplate-dev
```

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте установочный файл КриптоАРМ с официальных источников:

- Официальный сайт КриптоАРМ
- Сайт компании-разработчика Trusted.ru

Дистрибутив КриптоПро CSP (при использовании ГОСТ-алгоритмов)

> ⚠️ **Примечание**: КриптоАРМ можно использовать без установки КриптоПро CSP, если ваши сценарии работы не требуют выполнения криптографических операций с алгоритмами ГОСТ.

Скачайте дистрибутив КриптоПро CSP с официального сайта компании ООО «КРИПТО-ПРО» или используйте компакт-диск.

Чтобы загрузить дистрибутив КриптоПро CSP из официального источника:

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше

Для создания подписей со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP. Дистрибутив КриптоПро CSP не содержит пакетов TSP и OCSP. Эти модули доступны в составе КриптоПро ЭЦП SDK для macOS, который необходимо скачать отдельно.

Установка КриптоАРМ

Установка RPM-пакета

Через терминал

1. Откройте терминал.

2. Выполните команду для установки пакета:
   - Если вы находитесь в той же папке, что и пакет:

```
apt-get install имя_пакета.rpm # ALT Linux, Astra Linux CE, RedOS
dnf install имя_пакета.rpm     # ROSA
```

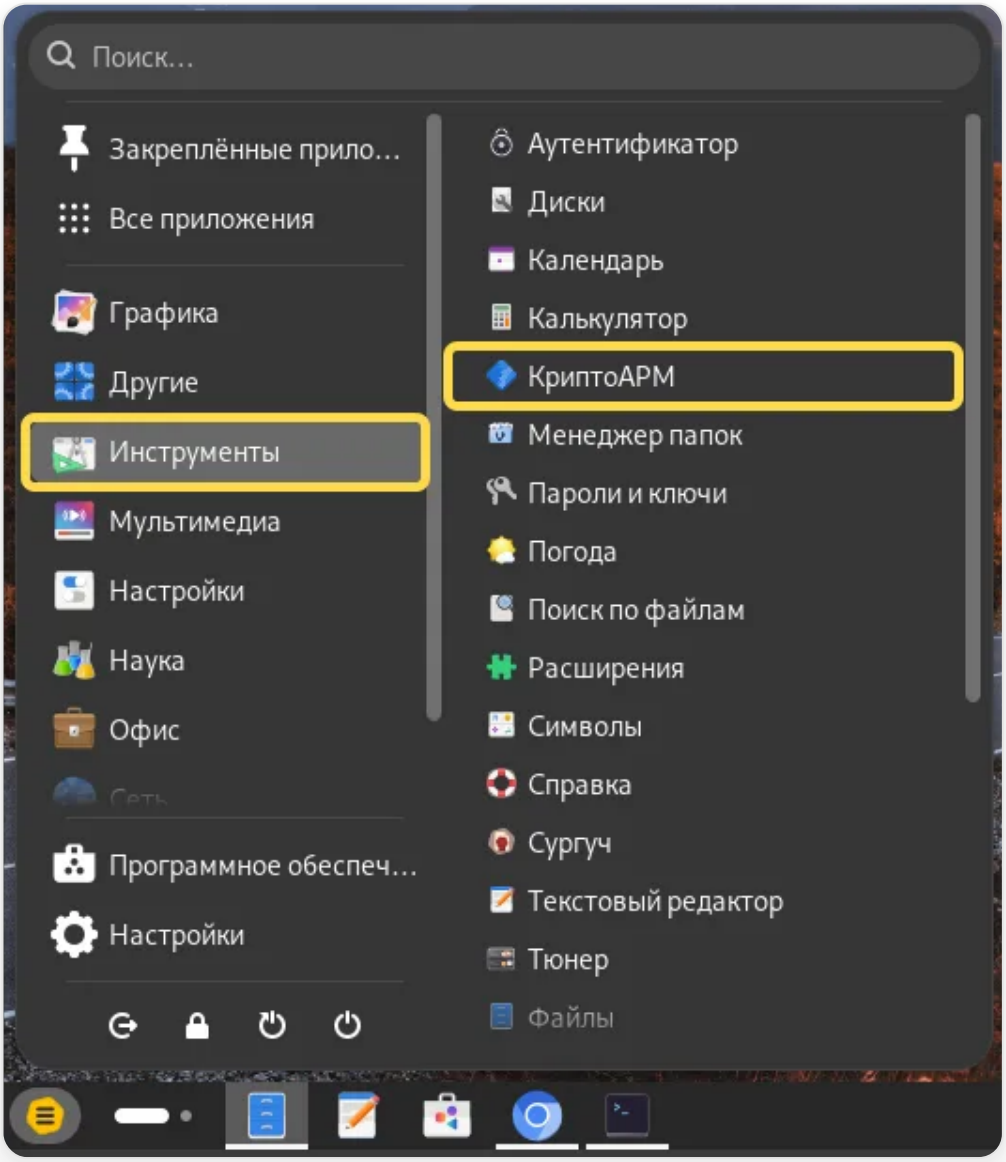
   - Если пакет находится в другой папке:

```
apt-get install /{путь_до_файла}/имя_пакета.rpm
```

3. Дождитесь окончания установки.

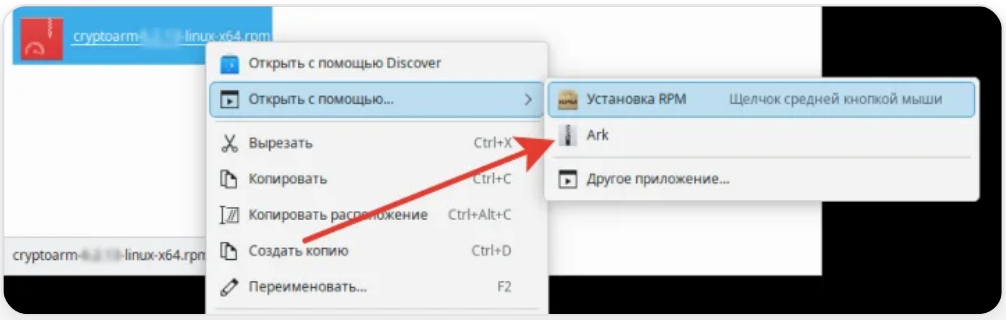
> 📌 По умолчанию приложение устанавливается в каталог `/opt/cryptoarm/`.

После установки приложение автоматически появляется в меню системы. Например, в **Альт Рабочая станция** приложение можно найти в разделе **Инструменты**.

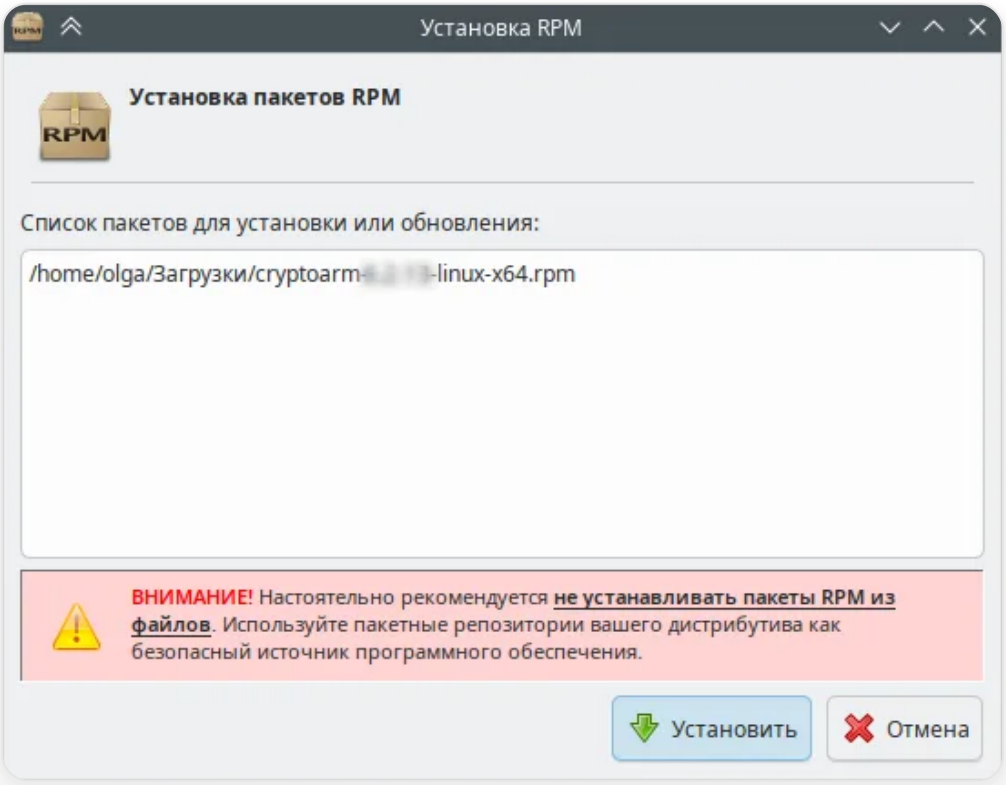


Через графический интерфейс

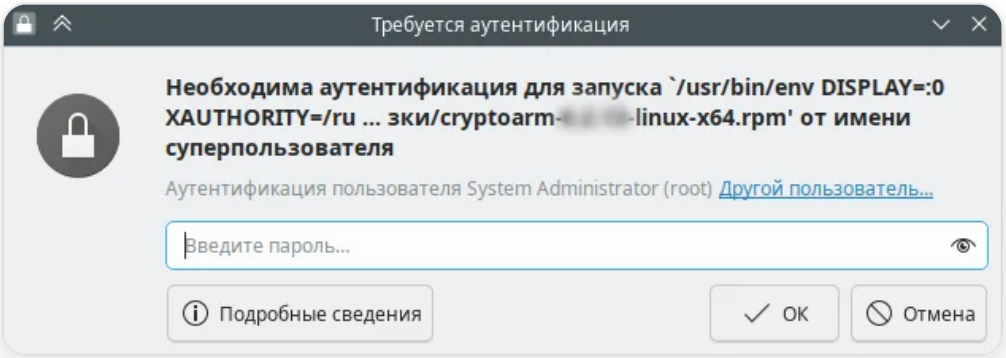
1. Откройте установочный файл `.rpm` через установщик пакетов.



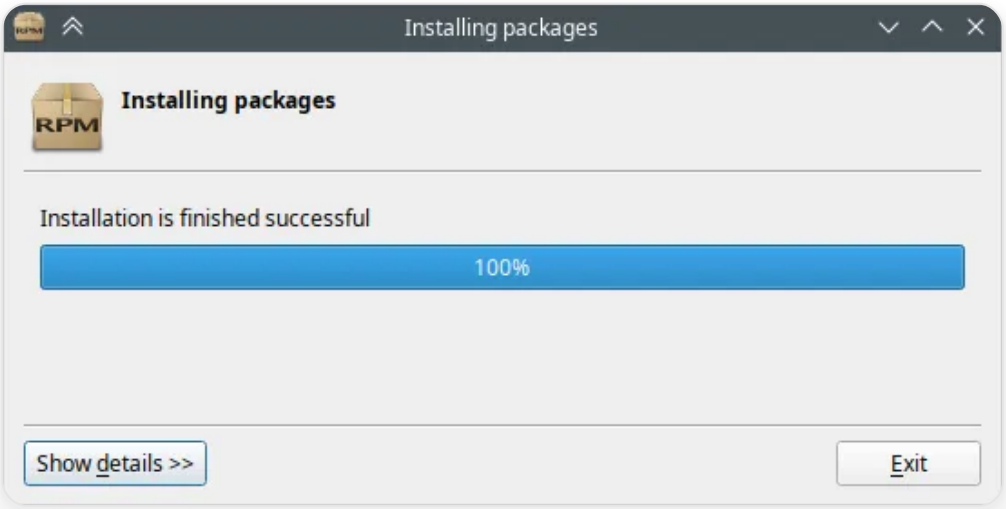
2. Нажмите на кнопку **Установить**.



3. При необходимости укажите пароль системного администратора.



4. Дождитесь окончания установки.



Установка DEB-пакета

Через терминал

1. Откройте терминал.
2. Выполните команду для установки пакета:
   - Если вы находитесь в той же папке, что и пакет:

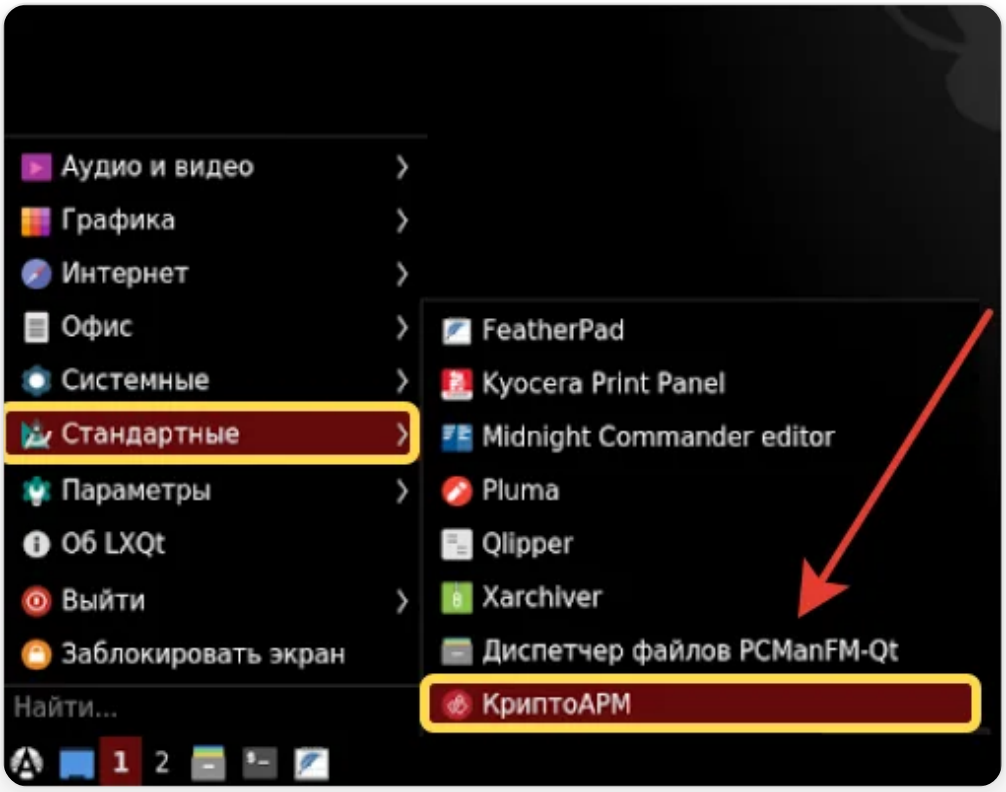
     ```
     sudo dpkg -i имя_пакета.deb
     ```

   - Если пакет находится в другой папке:

     ```
     sudo dpkg -i /{путь_до_файла}/имя_пакета.deb
     ```

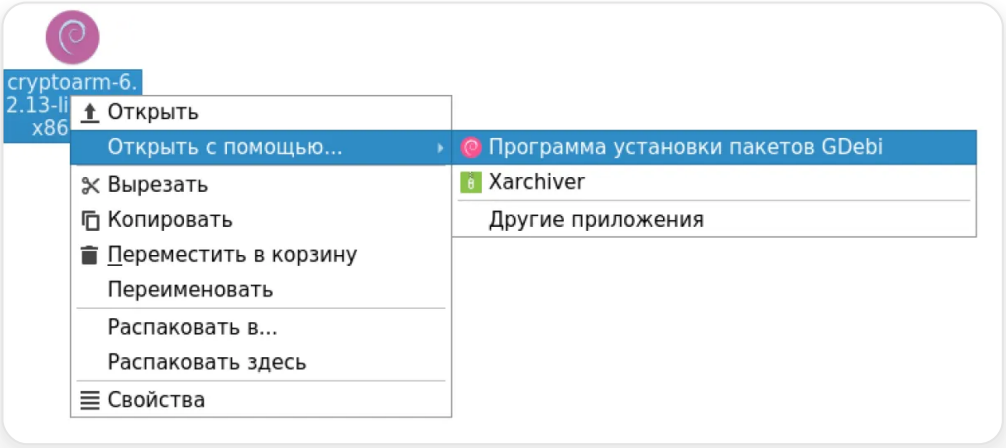
3. Дождитесь окончания установки.

   После установки приложение автоматически появляется в меню системы. Например, в ОС **Атлант** приложение можно найти в разделе **Стандартные**.

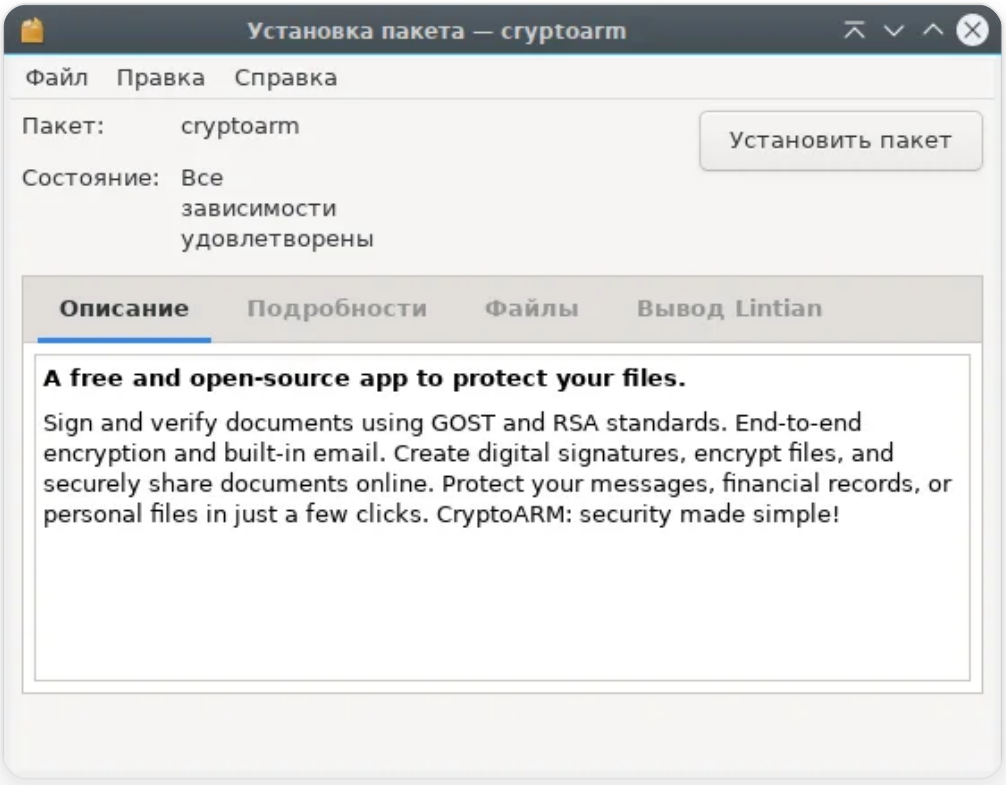


Через графический интерфейс

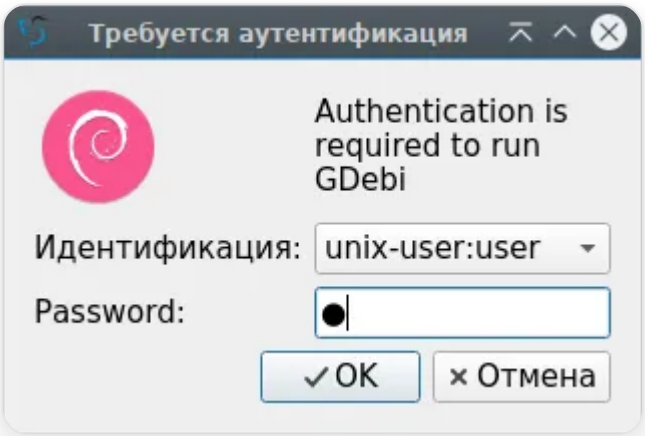
1. Дважды кликните на файл `.deb` или откройте его через установщик пакетов.



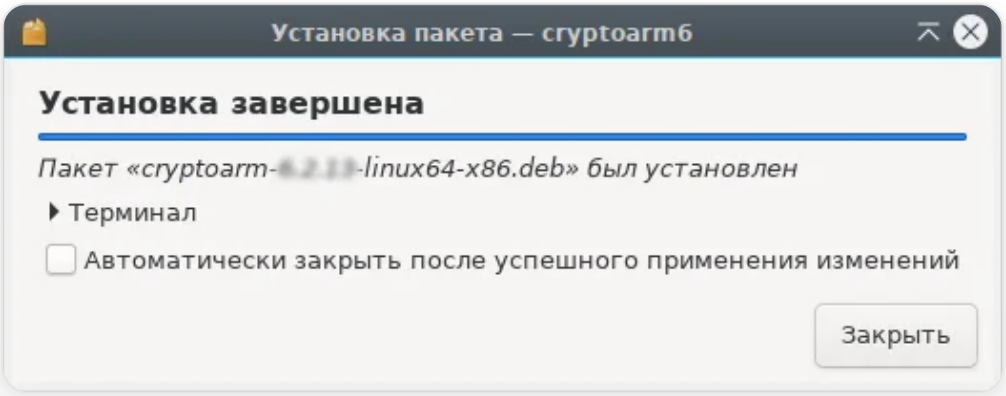
2. Нажмите на кнопку **Установить пакет**.



3. При необходимости укажите пароль системного администратора.



4. Дождитесь окончания установки.



Для завершения установки нажмите кнопку **Закрыть**.

Установка КриптоПро CSP

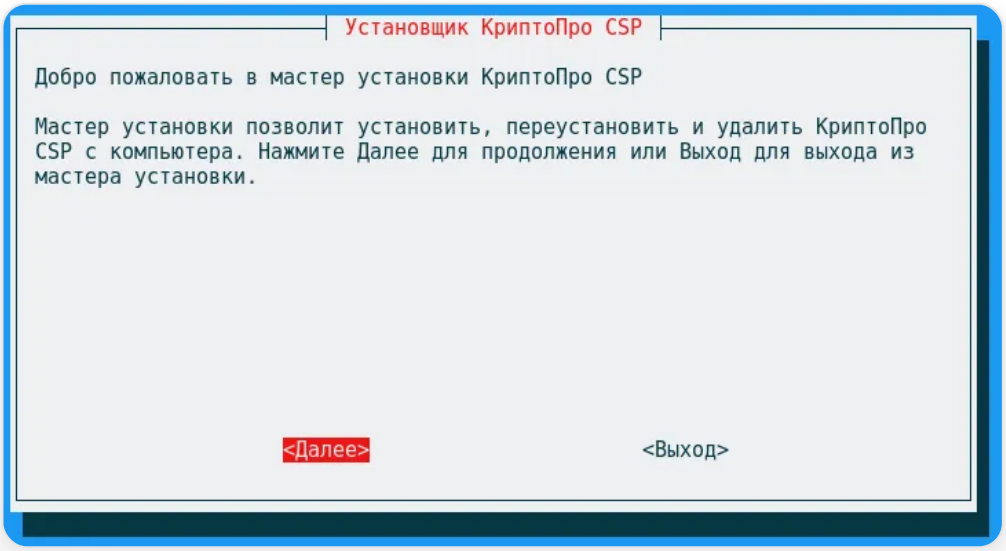
1. Если дистрибутив скачан в формате `.tgz`, его необходимо распаковать. Сделать это можно двумя способами — через графический интерфейс или в терминале.
   - Найдите архив в файловом менеджере и нажмите на него правой кнопкой мыши. Выберите пункт **Распаковать в эту папку**/**Извлечь здесь**.
   - Выполните команду в терминале:

```
tar -xzf имя_пакета.tgz # Распаковка в текущую директорию
tar -xzf имя_пакета.tgz -C  /{путь_до_файла}/ # Распаковка в указанную директорию
```

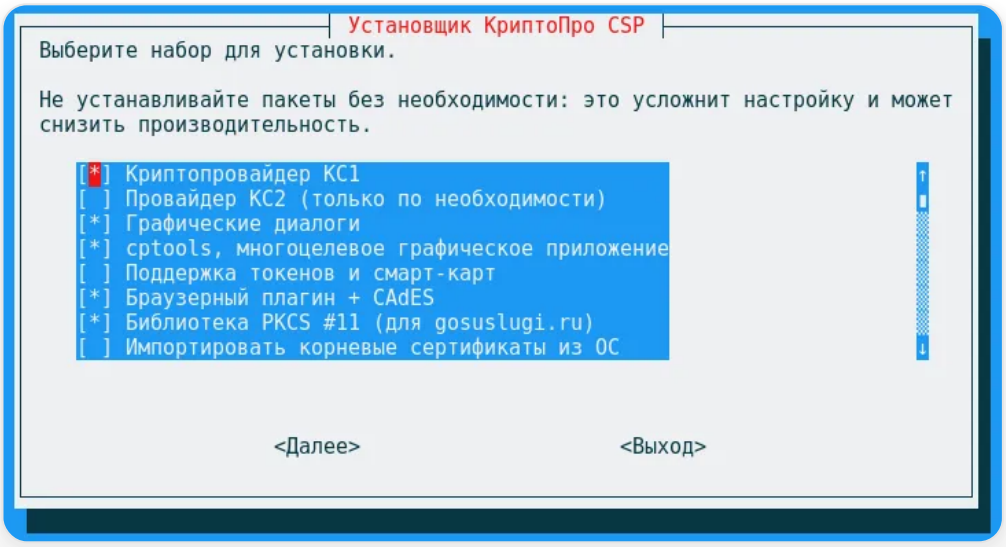
2. Запустите установщик по команде:

```
/{путь_до_файла}/install_gui.sh # Запуск графического установщика
/{путь_до_файла}/install.sh # Без графического установщика
```

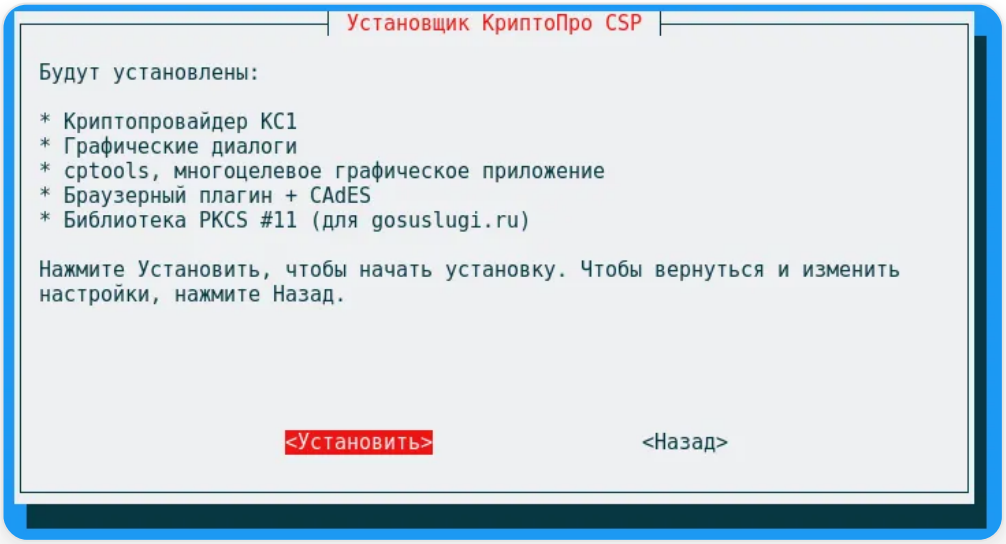
3. Если запущена графическая установка, нажмите **Далее** в открывшемся окне.



4. Выберите все дополнительные пакеты, кроме «Провайдер КС2», и снова нажмите **Далее**.



5. Подтвердите установку и дождитесь её окончания.



6. Закройте установщик.

> 📌 По умолчанию CSP устанавливается в `/opt/cprocsp/`.

Установка пакета для графического интерфейса ввода пароля

Для работы с контейнерами закрытых ключей требуется ввод пароля.

Установите пакет для графического интерфейса диалога ввода пароля, запустив в терминале команду:

```
sudo dpkg -i /<путь_до_файла>/cprocsp-rdr-gui-<...>.deb
```

Установка пакетов для работы с ключевыми носителями

> ⚠️ **Примечание**: Для работы с ключевыми ностителями в deb-based системе должны быть установлены: библиотека `libccid` не ниже 1.3.11, пакеты `pcscd` и `libpcsclite1`.

1. Установите пакеты и драйвера для работы с ключевыми носителями с помощью команд в терминале:

   ```
   sudo dpkg -i <путь_до_файла>/cprocsp-rdr-pcsc-<...>.deb
   ```

2. Для ключевого носителя **Рутокен**:

   ```
   sudo dpkg -i <путь_до_файла>/cprocsp-rdr-rutoken-<...>.deb
   ```

```
sudo dpkg -i <путь_до_файла>/ifd-rutokens_<...>.deb
```

3. Для ключевого носителя **JaCarta**:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rdr-jacarta -<...>.deb
```

4. Для ключевого носителя **ESMART**:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rdr-esmart -<...>.deb
```

Установка лицензии КриптоПро CSP через терминал

> 💡 Установить лицензию можно в разделе Настройки приложения КриптоАРМ, в терминале системы или через отдельные утилиты КриптоПро.

1. Откройте терминал.
2. Введите лицензию командой:

```
sudo /opt/cprocsp/sbin/amd64/cpconfig -license -set <серийный_номер>
```

> ⚠️ **Примечание**: Серийный номер вводится с учётом регистра символов.

Установка модулей TSP и OCSP

Для создания подписи со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP:

1. Скачайте КриптоПро ЭЦП SDK 2.0.
2. Распакуйте архив.
3. Установите пакет:

```
sudo dpkg -i <путь_до_файла>/cprocsp-pki-x.x.x-amd64-cades.deb
```

> 💡 Для создания обычной подписи без штампа времени установка этих модулей не обязательна.

Установка лицензии на модули TSP и OCSP через терминал

> 💡 Установить лицензию можно в разделе Настройки приложения КриптоАРМ, в терминале системы или через отдельные утилиты КриптоПро.

1. Откройте терминал.
2. Введите лицензию на модуль TSP командой:

```
sudo /opt/cprocsp/bin/amd64/tsputil license -s <серийный_номер>
```

3. Введите лицензию на модуль OCSP командой:

```
sudo /opt/cprocsp/bin/amd64/ocsputil license -s <серийный_номер>
```

> ⚠️ **Примечание**: Серийный номер следует вводить с соблюдением регистра символов.

Настройки для работы с КриптоПро CSP 4

1. Установите пакет cprocsp-rsa из дистрибутива КриптоПро:

```
sudo dpkg -i <путь_до_файла>/cprocsp-rsa-<...>.deb
```

2. Скачайте скрипт.
3. В терминале введите команду:

```
chmod u+x <путь к скрипту>/script.sh  # Делаем скрипт исполняемым
```

4. Далее введите команду:

```
sudo bash <путь к скрипту>/script.sh # Запуск скрипта с правами администратора
```

В результате выполнения команды должно выйти сообщение «Operations done».

Активация лицензий

Для выполнения криптографических операций с алгоритмами ГОСТ необходимо активировать лицензию «КриптоАРМ версии Про».

Инструкции по активации лицензий:

- Активация лицензии КриптоАРМ — подробное руководство по установке лицензии КриптоАРМ.
- Активация лицензии КриптоПро CSP — только при использовании CSP. Содержит руководство по установке лицензии КриптоПро через интерфейс КриптоАРМ.

При первом запуске КриптоАРМ автоматически активируется **30-дневная пробная лицензия**, которая позволяет полностью ознакомиться со всеми возможностями приложения и протестировать работу криптографических операций с российскими алгоритмами ГОСТ.

При первой установке криптопровайдера КриптоПро CSP может быть активирована ознакомительная лицензия (обычно сроком до 90 дней).

> 💡 Пробный период КриптоАРМ и ознакомительная лицензия КриптоПро CSP действуют независимо друг от друга.

Удаление КриптоАРМ

RPM-пакеты

1. Откройте терминал и переключитесь на `root` при необходимости:

   ```
   su -
   ```

2. Выполните команду:

   Удаление только приложения:

   ```
   rpm -e имя_пакета
   ```

   Удаление вместе с зависимостями (если установлено через `apt-get`):

   ```
   apt-get remove имя_пакета
   ```

После выполнения команды приложение будет удалено из системы.

DEB-пакеты

1. Откройте терминал.
2. Выполните команду:

   Удаление приложения:

```
sudo dpkg -r имя_пакета
```

Полное удаление с настройками:

```
sudo dpkg -P имя_пакета
```

После выполнения команды приложение будет удалено из системы.

Смотрите также

- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.
- Быстрый старт — инструкция по первому запуску и базовой настройке КриптоАРМ.

Открыть статью на сайте

Пошаговая установка КриптоАРМ на macOS

В этом разделе мы расскажем, как установить КриптоАРМ КриптоАРМ на ОС macOS. Вы узнаете, как подготовить систему, установить КриптоАРМ и КриптоПро CSP, а также где найти инструкции по активации лицензий.

Инструкция актуальна для КриптоАРМ версии 6.x на macOS 11–15 и выше.

Содержание:

- Скачивание установочных файлов
- Установка КриптоАРМ
- Установка КриптоПро CSP
- Активация лицензий
- Меню приложения КриптоАРМ на macOS
- Удаление КриптоАРМ
- Смотрите также

Скачивание установочных файлов

Дистрибутив КриптоАРМ

Скачайте установочный файл КриптоАРМ с официальных источников:

- Официальный сайт КриптоАРМ
- Сайт компании-разработчика Trusted.ru

Дистрибутив приложения поставляется в упакованном виде в формате `.dmg` и представляет собой образ диска, содержащий пакет установки **cryptoarm-x.x.x-x64.pkg,** описание приложения, каталог со скриптами удаления приложения.

Дистрибутив КриптоПро CSP (при использовании ГОСТ-алгоритмов)

> ⚠️ **Примечание**: КриптоАРМ можно использовать без установки КриптоПро CSP, если ваши сценарии работы не требуют выполнения криптографических операций с алгоритмами ГОСТ.

Скачайте дистрибутив КриптоПро CSP с официального сайта компании ООО «КРИПТО-ПРО» или используйте компакт-диск.

Чтобы загрузить дистрибутив КриптоПро CSP из официального источника:

1. Перейдите на официальный сайт КриптоПро.
2. Пройдите регистрацию или авторизацию.
3. Откроется страница продукта КриптоПро CSP.
4. Нажмите **Скачать**.
5. Ознакомьтесь и согласитесь с лицензионным соглашением.
6. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

> ⚠️ **Требования к версии**: КриптоАРМ поддерживает КриптоПро CSP версии 5.0 и выше

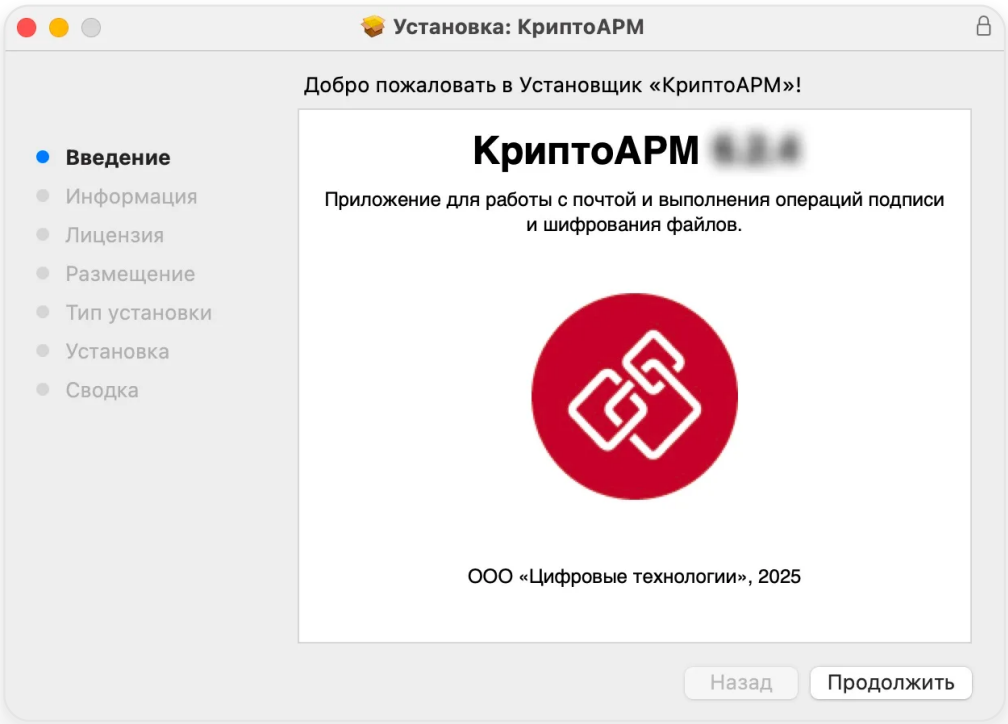
Для создания подписей со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP. Дистрибутив КриптоПро CSP не содержит пакетов TSP и OCSP. Эти модули доступны в составе КриптоПро ЭЦП SDK для macOS, который необходимо скачать отдельно.

Установка КриптоАРМ

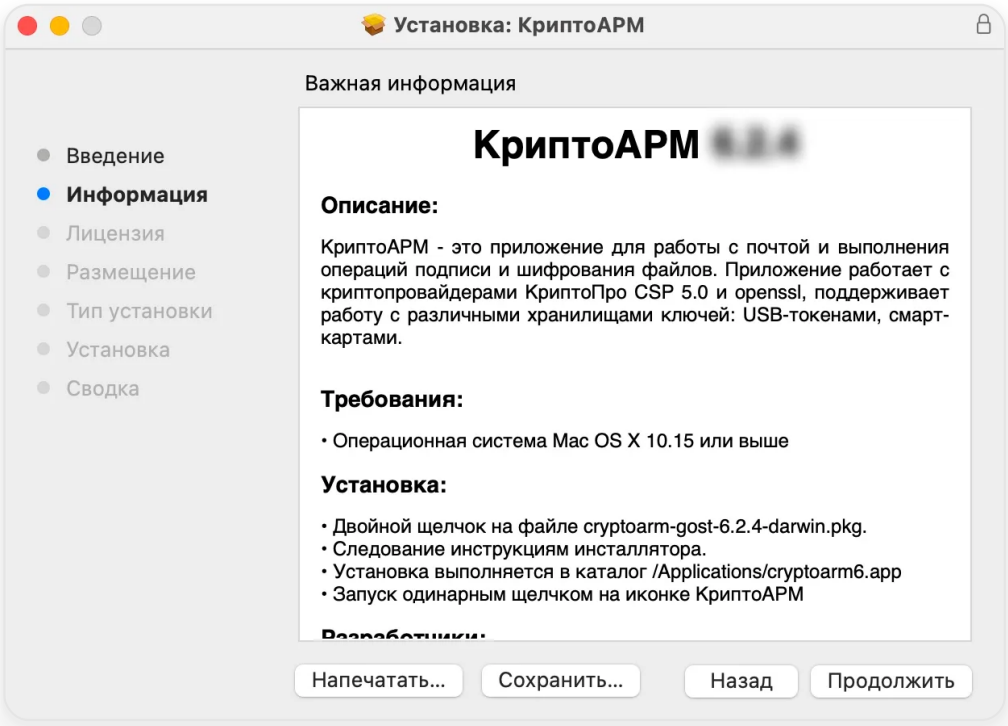
1. Для установки пакета через графический интерфейс откройте образ диска с дистрибутивом `.dmg`.

   Установочный пакет для приложения может поставляться вне образа диска. В таком случае нужно сразу запустить файл `.pkg`.

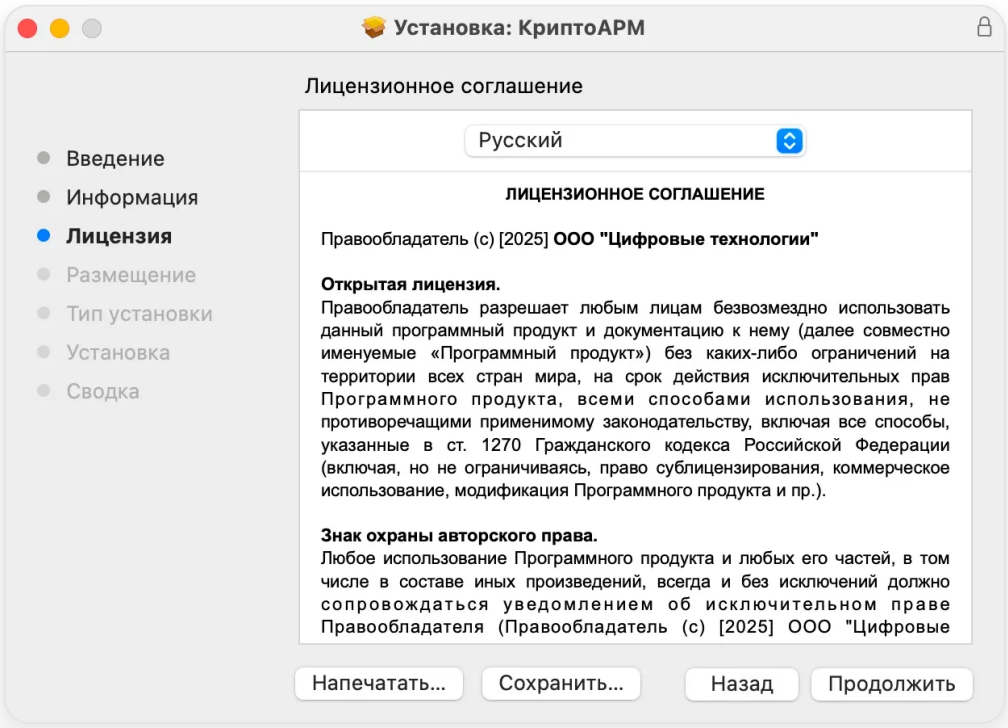
2. Откроется мастер установки. Нажмите **Продолжить**.



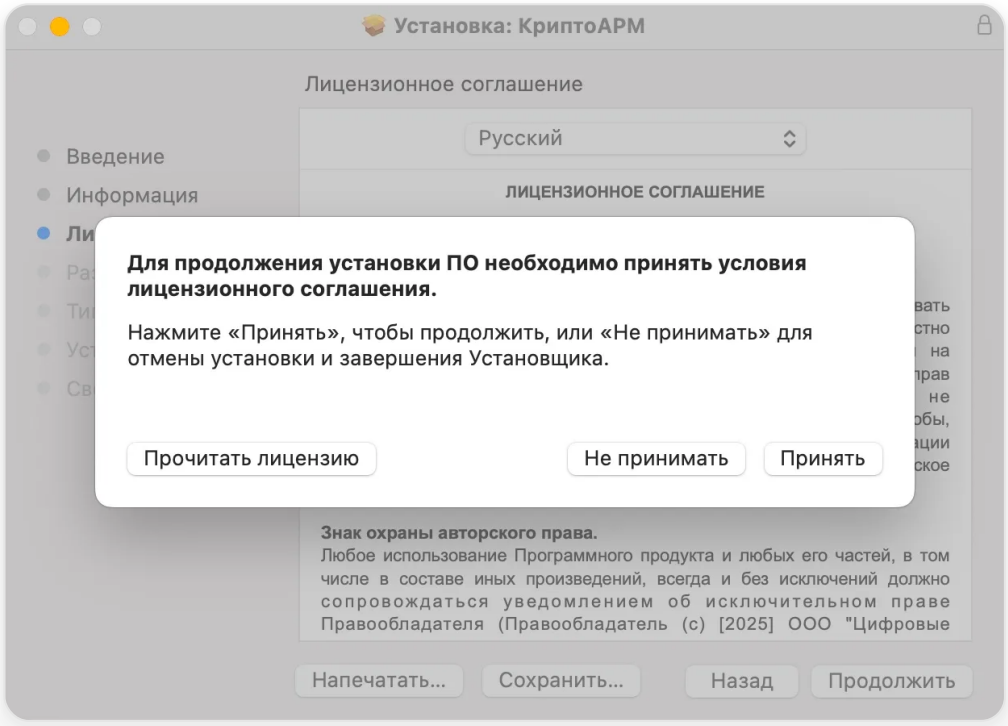
3. Откроется окно с описанием программы. Нажмите **Продолжить**.



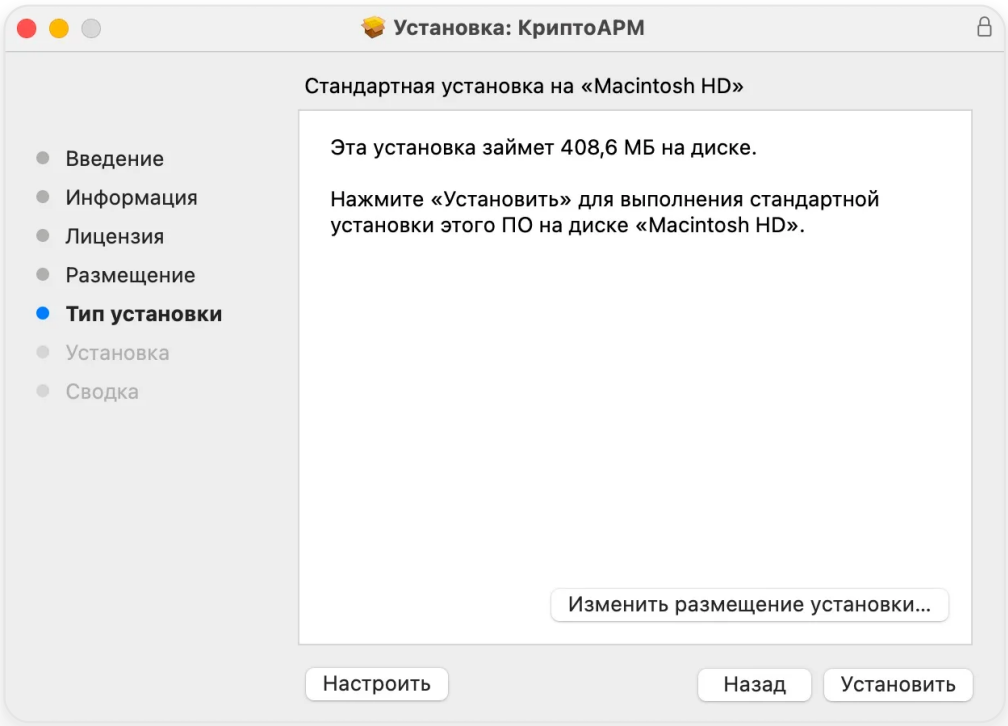
4. Ознакомьтесь с условиями лицензионного соглашения и нажмите **Продолжить**.



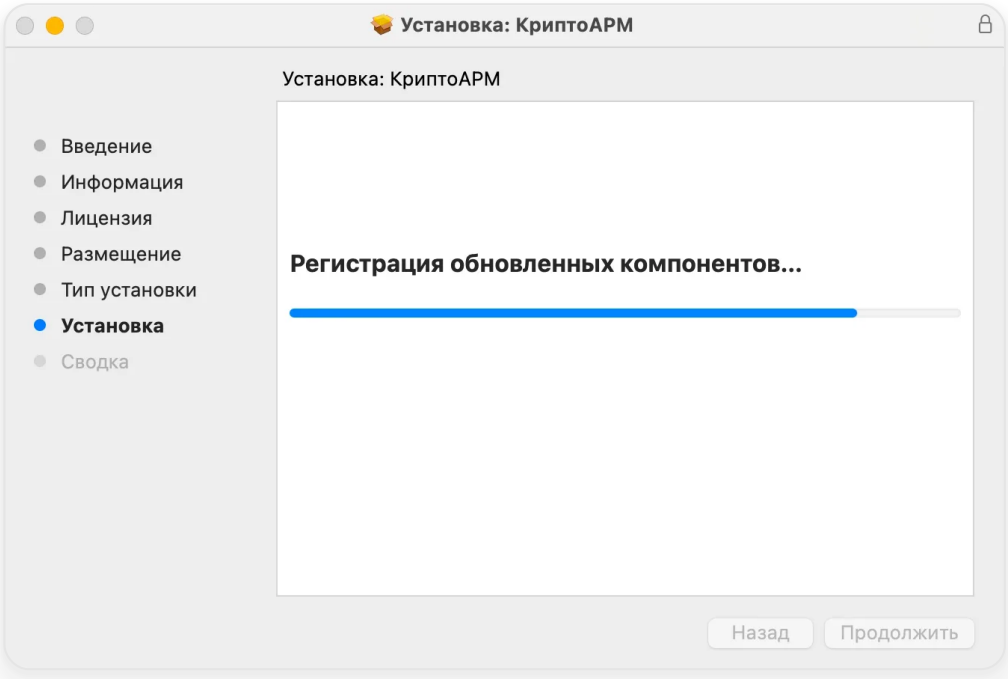
Примите условия лицензионного соглашения по кнопке **Принять**. По кнопке **Не принимать** произойдет отмена установки.



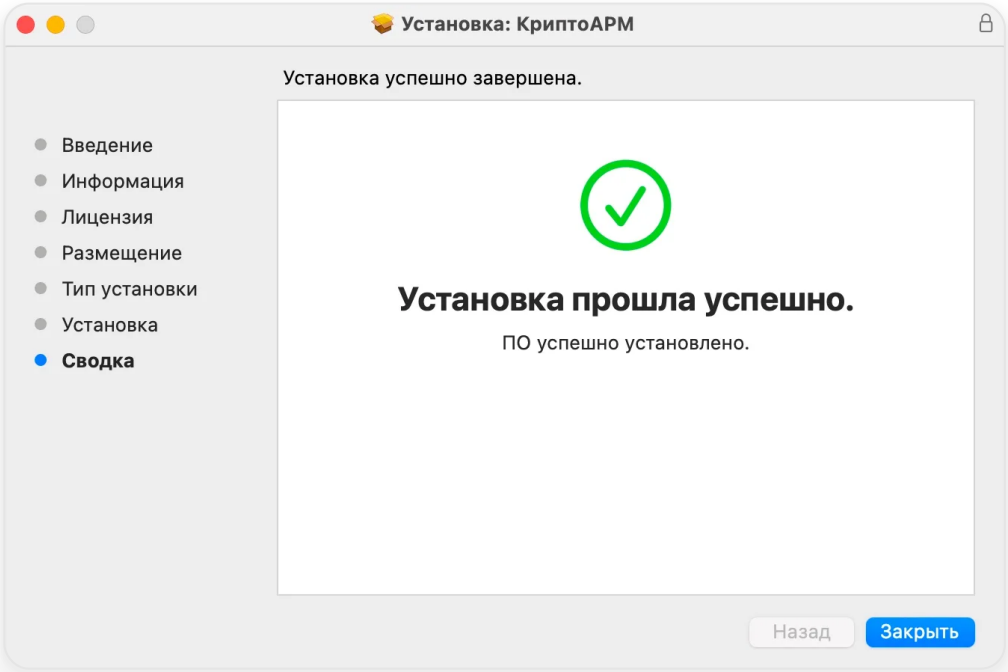
5. На последнем шаге мастера нажмите **Установить**.



Дождитесь окончания установки.



6. Закройте окно установки.



После установки программы в **Launchpad** появится ярлык приложения.

В каталоге **Applications** (Программы) будут созданы подкаталоги приложения.

Установка КриптоПро CSP

1. Распакуйте загруженный дистрибутив `.tgz`.
2. Откройте образ диска `.dmg` двойным кликом.
3. Запустите установочный пакет `.pkg` двойным кликом.
4. Если появится предупреждение «Программа загружена из интернета», выберите **Открыть**.
5. Нажмите **Продолжить**, ознакомьтесь с лицензией и примите условия.
6. Выберите все необходимые пакеты и нажмите **Продолжить → Установить**.
7. После завершения закройте мастер установки.

> 📌 По умолчанию CSP устанавливается в `/Applications/CryptoPro_ECP.app`. Если вы выбрали другой каталог, используйте его в последующих командах терминала.

Установка модулей TSP и OCSP

Для создания подписей со штампом времени или усовершенствованной подписи необходимо установить библиотеки поддержки модулей TSP и OCSP:

1. Скачайте КриптоПро ЭЦП SDK 2.0.
2. Установите пакет `.pkg`, следуя шагам установщика.

> 💡 Для создания обычной подписи без штампа времени установка этих модулей не обязательна.

Активация лицензий на модули TSP и OCSP через терминал

> 💡 Рекомендуемый способ активации лицензий — через интерфейс КриптоАРМ (раздел Настройки). Использование терминала рекомендуется только в случаях, когда графический интерфейс недоступен или невозможно выполнить стандартную активацию.

1. Откройте терминал и введи команды.

   Если вы используете стандартный путь установки (`/Applications/CryptoPro_ECP.app`), команды будут:

   ```
   sudo /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license -s XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
   sudo /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license -s XXXXX-XXXXX-XXXXX-XXXXX-XXXXX
   ```

   - Замените серийный номер на ваш приобретённый.
   - Если CSP установлен в другой каталог, замените путь на соответствующий.

2. После ввода команды система попросит пароль пользователя macOS.

3. Проверьте статус лицензий по команде:

   ```
   /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license
   /Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license
   ```

Активация лицензий

Для выполнения криптографических операций с алгоритмами ГОСТ необходимо активировать лицензию «КриптоАРМ версии Про».

Инструкции по активации лицензий:

- Активация лицензии КриптоАРМ — подробное руководство по установке лицензии в КриптоАРМ.
- Активация лицензии КриптоПро CSP — только при использовании CSP. Содержит руководство по установке лицензии КриптоПро через интерфейс КриптоАРМ.

При первом запуске КриптоАРМ автоматически активируется **30-дневная пробная лицензия**, которая позволяет полностью ознакомиться со всеми возможностями приложения и протестировать работу криптографических операций с российскими алгоритмами ГОСТ.

При первой установке криптопровайдера КриптоПро CSP может быть активирована ознакомительная лицензия (обычно сроком до 90 дней).

> 💡 Пробный период КриптоАРМ и ознакомительная лицензия КриптоПро CSP действуют независимо друг от друга.

Меню приложения КриптоАРМ на macOS

Приложение КриптоАРМ в macOS имеет стандартное меню, расположенное в верхней части экрана. В зависимости от активного окна, доступны различные пункты.

1. **Меню приложения**

   Содержит общие команды для управления программой:

   - **О программе** – информация о версии КриптоАРМ.
   - **Настройки... (⌘,)** – открывает параметры приложения.
   - **Скрыть КриптоАРМ (⌘H)** – временно убирает окно программы.
   - **Скрыть остальные (⌥⌘H)** – скрывает все приложения, кроме КриптоАРМ.
   - **Выход (⌘Q)** – завершает работу программы.

2. **Меню «Окно»**

Управление открытыми окнами в приложении:

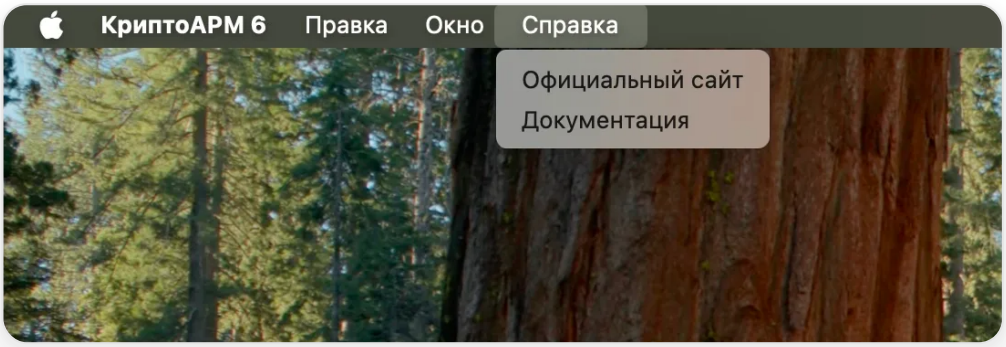
Пункт меню	Горячая клавиша	Описание
Свернуть (⌘M)	`⌘ + M`	Сворачивает текущее окно в Dock.
Развернуть	–	Переводит окно в полноэкранный режим (если поддерживается).
Закрыть (⌘W)	`⌘ + W`	Закрывает текущее окно (не завершает программу).
На передний план	–	Переключает на активное окно КриптоАРМ, если открыто несколько.

```
<img src="../images/install-mac-10.webp" alt="Меню с действиями над окном приложения КриптоАРМ
на macOS" style="max-width:500px; width:100%">
```

1. **Меню «Справка»**

   Доступ к официальной документации и поддержке:

Пункт	Описание
Официальный сайт	Открывает сайт КриптоАРМ в браузере.
Документация	Открывает руководство пользователя.



Удаление КриптоАРМ

Закрытие приложения

1. Перед удалением убедитесь, что КриптоАРМ не запущен.
2. Закройте все окна программы.
3. Для гарантированного завершения работы откройте **Activity Monitor (Мониторинг системы)** и убедитесь, что процессы `CryptoARM` отсутствуют. Если есть – завершите их.

Удаление приложения

1. Откройте каталог **Программы (Applications)**.
2. Найдите папку или ярлык **CryptoARM**.
3. Перетащите её в **Корзину (Trash)**.

> 💡 Если установлен дистрибутив в формате `.dmg`, удалять нужно установленное приложение, а не сам образ диска.

Удаление файлов конфигурации и данных пользователя

Для полной очистки системы рекомендуется удалить оставшиеся настройки и данные:

1. Откройте **Finder** → **Перейти** → **Перейти к папке...** (или `Shift+Cmd+G`).
2. Введите следующие пути и удалите соответствующие папки:

- `~/Library/Application Support/CryptoARM`
- `~/Library/Preferences/ru.cryptoarm.*.plist`
- `~/Library/Logs/CryptoARM`

> ⚠️ Будьте внимательны: удаляйте только файлы, относящиеся к КриптоАРМ.
>
> 💡 **Совет:** Если вы планируете повторную установку КриптоАРМ или CSP, убедитесь, что удалены все остаточные файлы и перезагрузите систему, чтобы избежать конфликтов старых настроек.

Смотрите также

- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.
- Быстрый старт — инструкция по первому запуску и базовой настройке КриптоАРМ.

Открыть статью на сайте

Инструкция по активации лицензий КриптоАРМ и КриптоПро CSP

В этой инструкции вы узнаете, как активировать лицензии на **КриптоАРМ** и **КриптоПро CSP**, а также на дополнительные модули **TSP Client** и **OCSP Client** через интерфейс приложения КриптоАРМ.

Инструкция подходит для рабочих мест, на которых КриптоАРМ используется как основной инструмент управления криптографическими компонентами.

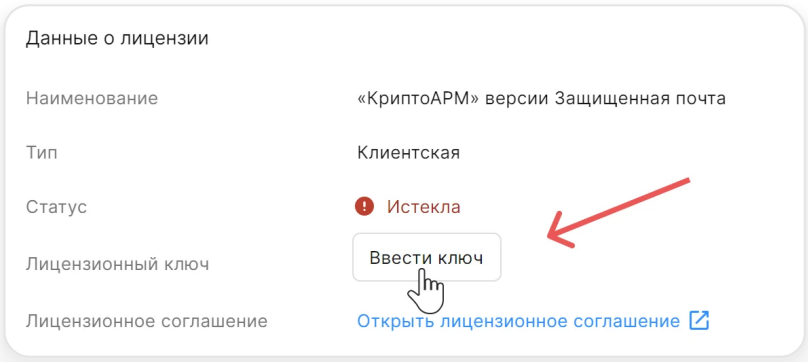
Содержание:

- Лицензия КриптоАРМ
- Лицензия КриптоПро CSP
- Проверка статуса лицензии
- Смотрите также

Лицензия КриптоАРМ

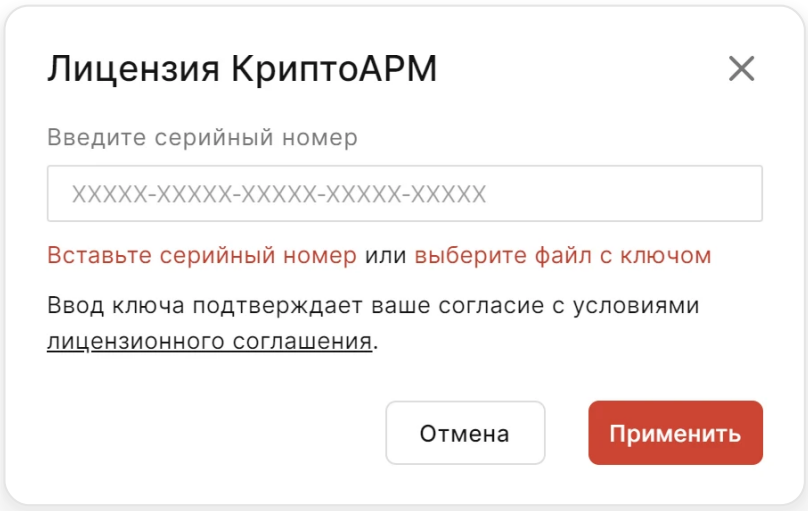
Активация лицензии КриптоАРМ

1. Перейдите в раздел **Настройки** → вкладка **О программе**.
2. В блоке **Данные о лицензии** нажмите **Ввести ключ**.



3. Вставьте скопированный ключ из буфера или укажите путь к файлу с ним.

> ⚠️ **Примечание**: Приложение принимает лицензию, введённую без символа «-». Это удобно, если копируете лицензию из письма или документа, где дефисы отсутствуют.



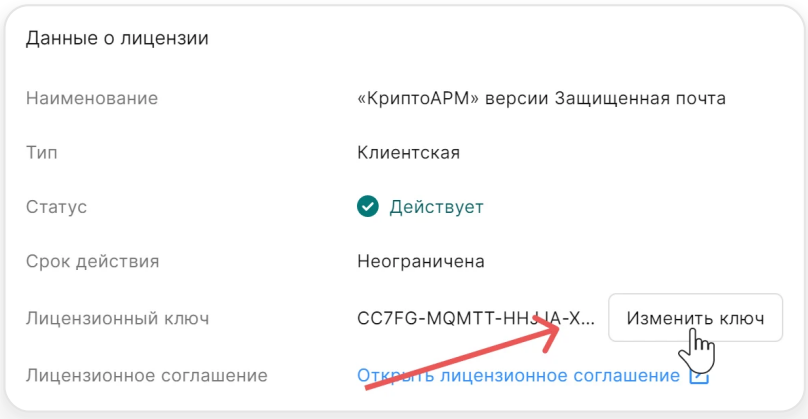
4. Нажмите **Применить** и дождитесь завершения активации.

Если активация лицензии прошла успешно, её статус будет обновлён автоматически.

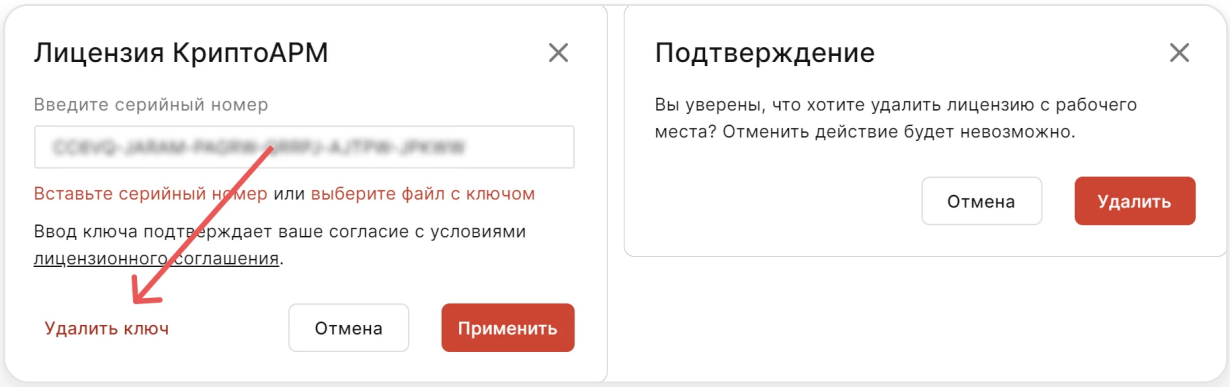
> ⚠️ **Важно**: Лицензионные ключи от предыдущих версий КриптоАРМ не поддерживаются в текущей версии продукта. Для продолжения работы скачайте соответствующий дистрибутив на сайте cryptoarm.ru или приобретите обновление лицензии в интернет-магазине.

Перенос лицензии КриптоАРМ на другое устройство

1. Перейдите в раздел **Настройки** → вкладка **О программе**.
2. В блоке **Данные о лицензии** нажмите нажмите **Изменить ключ**.



3. При необходимости скопируйте ключ в открывшемся окне.
4. Нажмите **Удалить ключ** и подтвердите действие.



После удаления ключа с текущего устройства вы можете активировать лицензию на новом, следуя инструкции по активации.

Лицензия КриптоПро CSP

В данной инструкции описан способ активации лицензии КриптоПро CSP через интерфейс КриптоАРМ — это самый простой вариант, не требующий перехода в отдельные утилиты КриптоПро.

Обратите внимание, что лицензию КриптоПро CSP также можно активировать:

- через **Инструменты КриптоПро** (графический интерфейс, если он установлен);
- через **терминал (командную строку)** — актуально в первую очередь для Linux.

Подробные инструкции по активации лицензии через терминал:

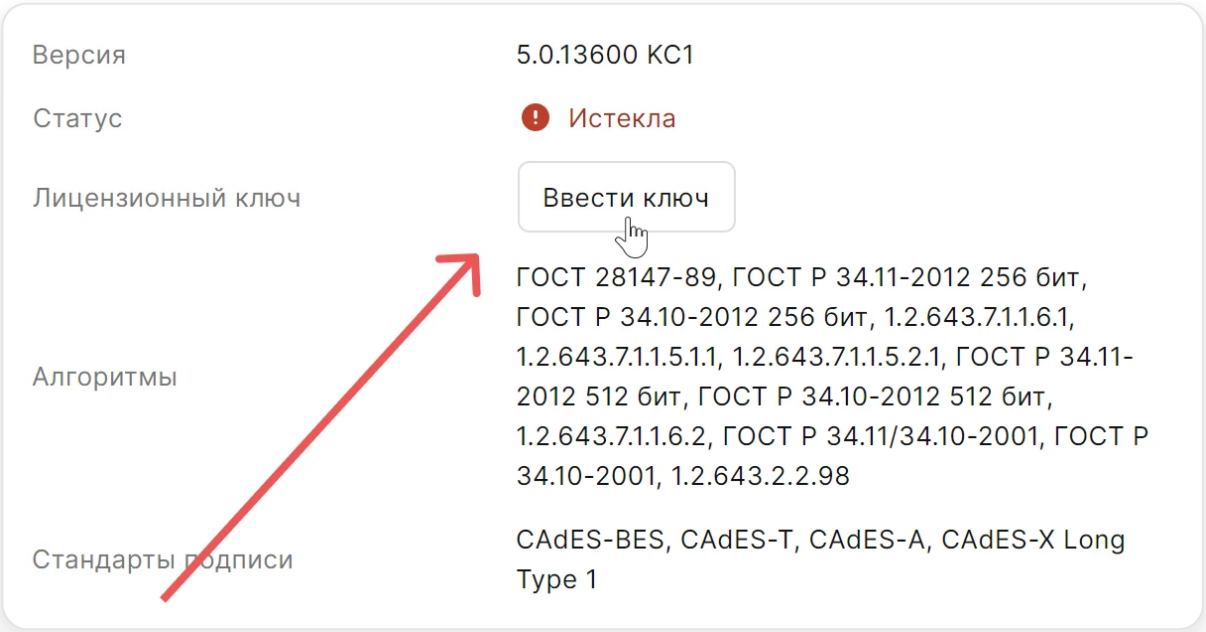
- Активация лицензии КриптоПро CSP в Linux через терминал
- Активация лицензий на модули TSP и OCSP в Linux через терминал
- Активация лицензий на модули TSP и OCSP в macOS через терминал

> 💡 Рекомендуется использовать активацию через КриптоАРМ, если нет необходимости выполнять настройку вручную или работать в среде без графического интерфейса.

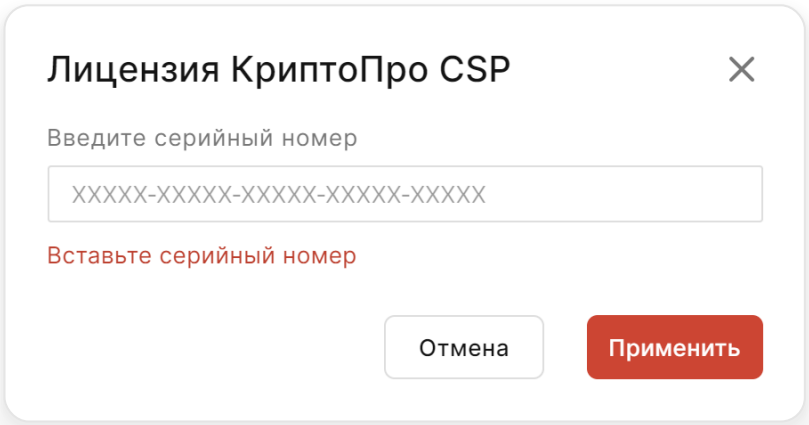
Активация лицензии КриптоПро CSP

1. Перейдите в раздел **Настройки** → вкладка **Криптопровайдеры** → провайдер **КриптоПро CSP**.

2. В блоке **Лицензия** нажмите **Ввести ключ**.



3. В открывшемся окне введите лицензионный ключ.



4. Нажмите **Применить** и дождитесь завершения активации.

Если активация лицензии прошла успешно, её статус будет обновлён автоматически.

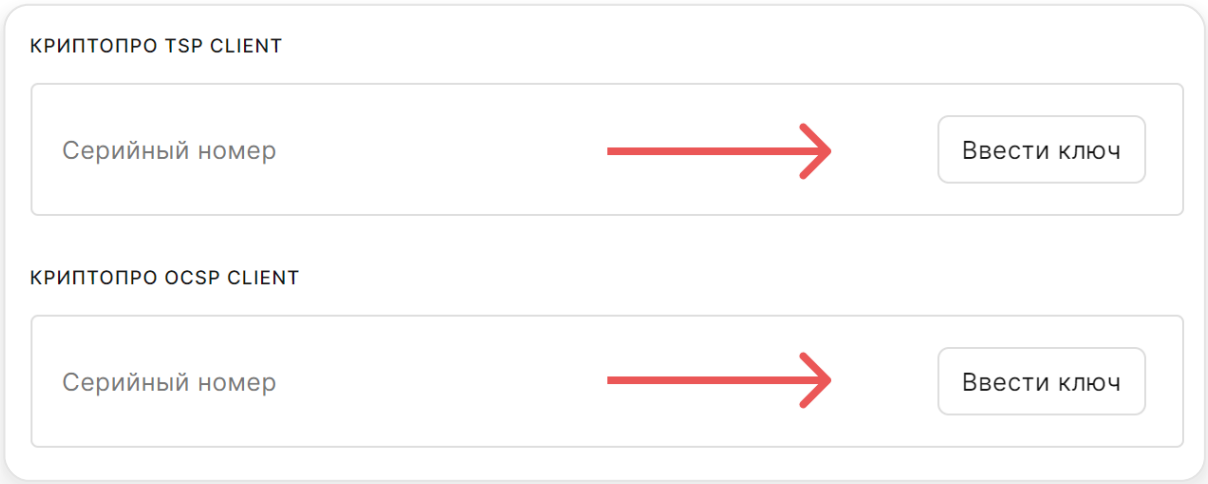
Активация лицензии на модули TSP и OCSP

> 💡 Модули **КриптоПро TSP Client** и **КриптоПро OCSP Client** лицензируются отдельно и активируются аналогично лицензии КриптоПро CSP.

1. Перейдите в раздел **Настройки**.
2. При необходимости запустите проверку для юрисдикции **Российская Федерация**.
3. Нажмите на панель **Криптопровайдеры** в блоке **Проверка рабочего места**.
4. Откроется окно со списком провайдеров.

5. Выберите **КриптоПро CSP**.
6. Откроется окно со сведениями о лицензиях криптопровайдера КриптоПро CSP, модулей КриптоПро TSP Client и КриптоПро OCSP Client.

7. Нажмите на кнопку **Ввести ключ** в блоке **КриптоПро TSP Client** или **КриптоПро OCSP Client**.



8. В открывшемся окне введите лицензионный ключ.

9. Нажмите **Применить** и дождитесь завершения активации.

Проверка статуса лицензии

КриптоАРМ

1. Перейдите в **Настройки** → **О программе**.

2. В блоке **Данные о лицензии** найдите статус:

Статус	Значение	Действие
✅ Действует	Лицензия активна	Все функции доступны
⚠️ Отсутствует	Лицензия отсутствует или истекла	Введите новый ключ

КриптоПро CSP и модули

1. Перейдите в **Настройки** → **Крипторовайдеры**.
2. Выберите **КриптоПро CSP**.

3. В блоке **Лицензия** найдите статус:

Статус	Значение	Действие
✅ Действует	Лицензия активна	Все функции доступны
⚠️ Отсутствует	Лицензия отсутствует или истекла	Введите новый ключ

> ⚠️ **Обратите внимание**: В Windows информация о статусе лицензий модулей КриптоПро TSP Client и КриптоПро OCSP Client не отображается в интерфейсе КриптоАРМ. Это является особенностью работы платформы и не влияет на функционирование модулей.

Смотрите также

- Быстрый старт — инструкция по первому запуску и базовой настройке КриптоАРМ.
- Общие настройки — инструкция по настройке приложения КриптоАРМ.
- Установка сертификатов — руководство по установке сертификатов в КриптоАРМ.

Открыть статью на сайте

Начало работы в КриптоАРМ

Это пошаговое руководство поможет вам быстро подготовить КриптоАРМ к работе. Вы узнаете, как настроить защищённую почту и адресные книги, управлять сертификатами и документами. Всё необходимое для старта собрано в одном месте, чтобы вы могли сразу приступить к работе.

Содержание:

- Общие подготовительные шаги
- Сценарий 1: Настройка защищённой почты
- Сценарий 2: Настройка для работы с документами
- Смотрите также

Общие подготовительные шаги

Некоторые действия универсальны и необходимы для любого сценария.

Добавьте сертификат подписи

Сертификат используется для создания электронной подписи.

- Установите личный сертификат
- Создайте самоподписанный сертификат

Добавьте контакты с сертификатами

Для шифрования документов и отправки защищённых писем добавьте контакты получателей с сертификатами:

- Добавьте контакт вручную
- Добавьте готовый список контактов vCard
- Добавьте контакты из LDAP-каталога
- Добавьте контакты из адресной книги CardDAV
- Импортируйте сертификаты контактов
- Привяжите сертификаты к контактам

Сценарий 1: Настройка защищённой почты

Если вы планируете отправлять и получать подписанные и зашифрованные письма, выполните следующие шаги:

Шаг 1. Добавьте почтовый аккаунт

- Добавьте почтового ящика

Шаг 2. Настройте отправку защищенной почты

- Настройте автоматическую подпись и шифрование писем
- Настройте алгоритм шифрования писем
- Привяжите сертификат к почтовому аккаунту
- Привяжите сертификаты к контактам

Шаг 3. Дополнительные настройки

- Настройте подпись с контактными данными
- Настройте правила сортировки писем
- Изучите общие настройки почты

Готово! Теперь вы можете отправлять и получать защищённые письма.

Сценарий 2: Настройка для работы с документами

Если вам нужно подписывать, шифровать и проверять файлы на компьютере:

Шаг 1. Создайте профиль подписи

Профиль содержит готовый набор настроек, которые можно применять для выполнения подписи, архивирования и шифрования.

- Создайте и настройте профиль подписи

Шаг 2. Привяжите сертификаты к контактам

Для отправки зашифрованных документов конкретным получателям привяжите их сертификаты к контактами.

- Привяжите сертификаты к контактам

Готово! Теперь вы можете работать с документами в разделе «Документы».

Смотрите также

- Общие настройки — инструкция по настройке приложения КриптоАРМ.
- Установка сертификатов — руководство по установке сертификатов в КриптоАРМ.
- Подключение почтового аккаунта — инструкция по подключению почтовых ящиков в КриптоАРМ.

Открыть статью на сайте

Общие настройки КриптоАРМ

В этом разделе вы узнаете, как настроить КриптоАРМ под свои задачи: выбрать раздел при запуске, проверить версию программы, оставить отзыв, открыть документацию и управлять проверкой сертификатов через KeyAgreement.

Содержание:

- Стартовый раздел
- Настройка темы
- Сворачивание в трей при закрытии окна
- Ограничение использования сертификатов по атрибуту KeyAgreement
- Смотрите также

Стартовый раздел

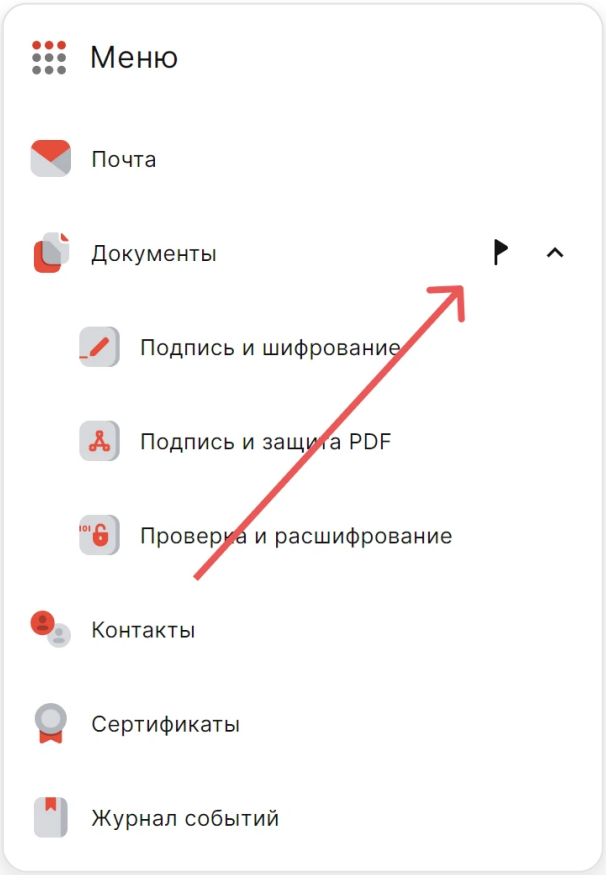
Вы можете выбрать раздел, который будет открываться при запуске приложения.

Способ 1: через раздел **Настройки**

1. Откройте раздел **Настройки** → вкладка **Интерфейс**.
2. Выберите необходимый раздел в настройке **Раздел при запуске**.

Способ 2: через меню приложения

1. Нажмите кнопку **Меню** в верхнем левом углу окна.
2. Наведите курсор мыши на раздел, который должен открываться при запуске приложения.
3. Нажмите на кнопку **Показывать при запуске**.

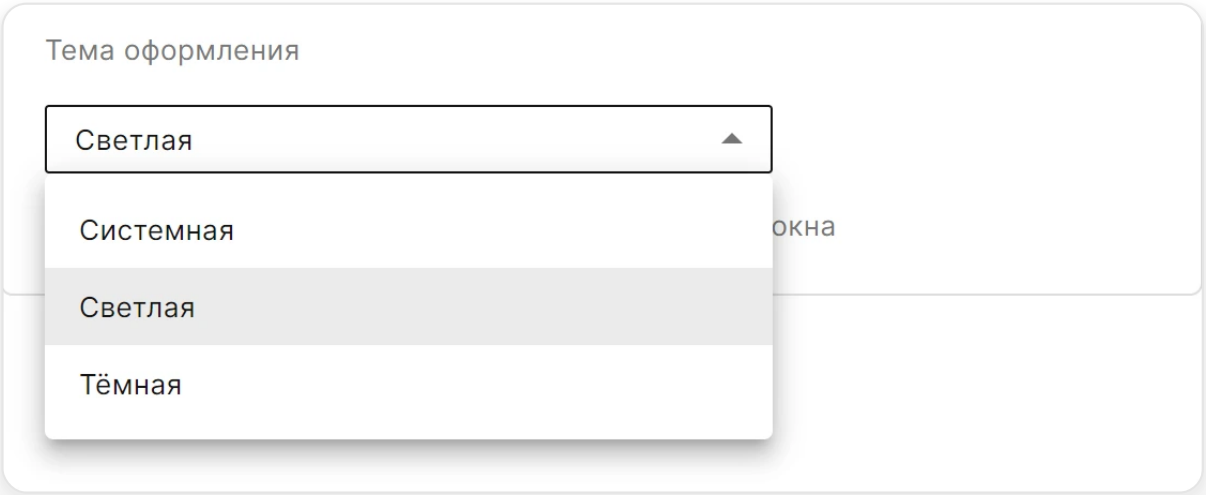


Выбранный раздел будет открываться автоматически при следующем запуске приложения.

Настройка темы

Чтобы настроить тему приложения:

1. Откройте раздел **Настройки** → вкладка **Интерфейс**.
2. Выберите один из доступных вариантов темы:
   - 🌞 **Светлая** — классическое светлое оформление
   - 🌙 **Темная** — для комфортной работы в темное время суток
   - ⚙️ **Системная** — автоматически следует за настройками вашей ОС

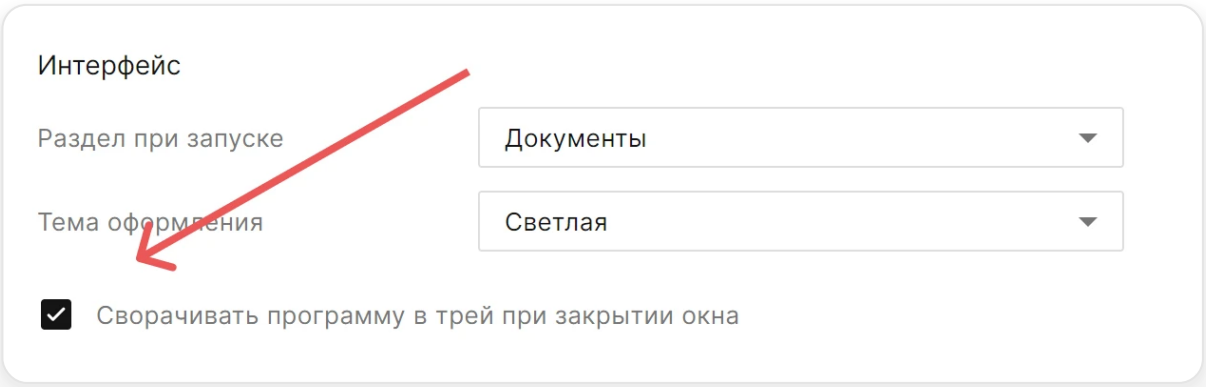


Сворачивание в трей при закрытии окна

Чтобы настроить сворачивание окна приложения в трей при закрытии:

1. Откройте раздел **Настройки** → **Интерфейс**.
2. Установите флажок **Сворачивать программу в трей при закрытии окна**

   После включения этой опции нажатие на стандартную кнопку **Закрыть** (крестик) в правом верхнем углу окна не завершит работу программы, а свернет её в область уведомлений (трей).



Как управлять программой, когда она свернута в трей:

- **Развернуть окно** — дважды кликните левой кнопкой мыши по иконке в трее или один раз кликните правой кнопкой и выберите Открыть / Восстановить.
- **Полностью выйти из программы** — кликните правой кнопкой по иконке в трее и выберите Выход (или Завершить работу).

Ограничение использования сертификатов по атрибуту KeyAgreement

Зачем нужна проверка

Атрибут **KeyAgreement** (согласование ключей) в расширении **keyUsage** сертификата указывает, что сертификат может использоваться для безопасного обмена ключами при выполнении операций шифрования.

В КриптоАРМ доступна настройка, позволяющая ограничить использование сертификатов при шифровании:

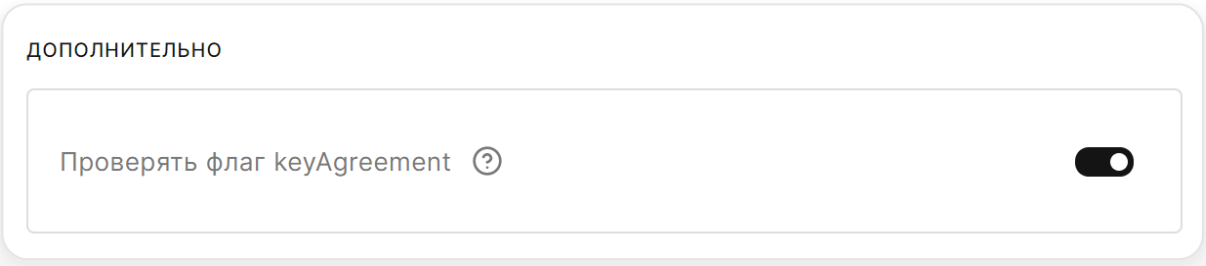
- при включённой проверке операция шифрования выполняется только для сертификатов, содержащих атрибут **KeyAgreement**;
- при отключённой проверке допускается использование сертификатов с атрибутом **keyEncipherment**, даже если атрибут **KeyAgreement** отсутствует.

По умолчанию проверка атрибута **KeyAgreement** отключена.

> ⚠️ Настройка доступна только при использовании криптопровайдера КриптоПро CSP и влияет исключительно на операции шифрования.

Включение проверки KeyAgreement

1. Перейдите в раздел **Настройки** → вкладка **Криптопровайдеры**.
2. Нажмите на панель **КриптоПро CSP**.
3. В блоке **Дополнительно** активируйте настройку **Проверять флаг keyAgreement**.



Смотрите также

- Общие настройки — инструкция по настройке приложения КриптоАРМ.
- Установка сертификатов — руководство по установке сертификатов в КриптоАРМ.
- Подключение почтового аккаунта — инструкция по подключению почтовых ящиков в КриптоАРМ.

Открыть статью на сайте

Как работать с журналом событий и уведомлениями КриптоАРМ

В этом разделе вы научитесь использовать журнал событий в КриптоАРМ: отслеживать ошибки, анализировать операции, экспортировать записи и настраивать логирование для быстрой диагностики проблем.

Содержание:

- Уведомления
- Журнал событий
- Смотрите также

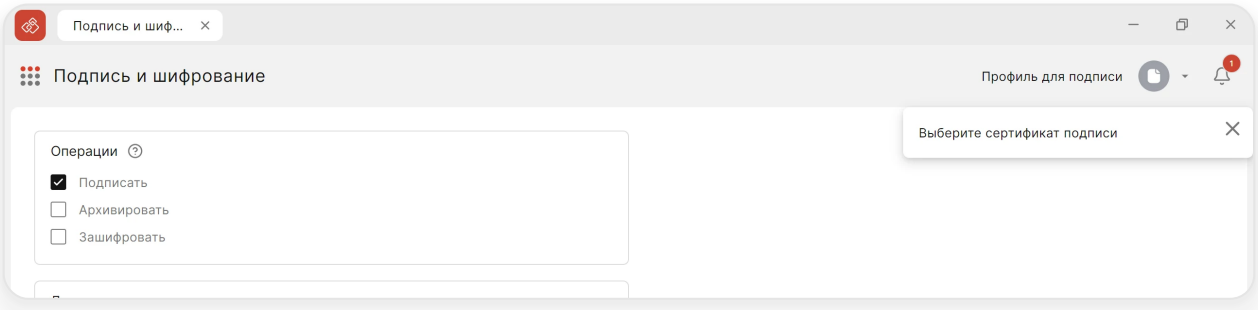
Уведомления

Приложение КриптоАРМ использует многоуровневую систему оповещений о событиях и ошибках.

Всплывающие уведомления

Всплывающие уведомления отображают краткую информацию о событиях и ошибках и автоматически скрываются через 5 секунд. Они позволяют быстро узнать о результате выполненного действия без перехода в журнал.

Пример всплывающего уведомления:



> 💡 **Совет**: Если всплывающее уведомление исчезло, вы всегда сможете найти его в **центре уведомлений**. Там вы сможете изучить подробности и, если нужно, перейти к журналу событий.

Центр уведомлений

Центр уведомлений собирает все уведомления, которые ранее появлялись во всплывающих окнах. Это позволяет вернуться к информации о событиях и ошибках, даже если всплывающее сообщение исчезло.

Как открыть центр уведомлений:

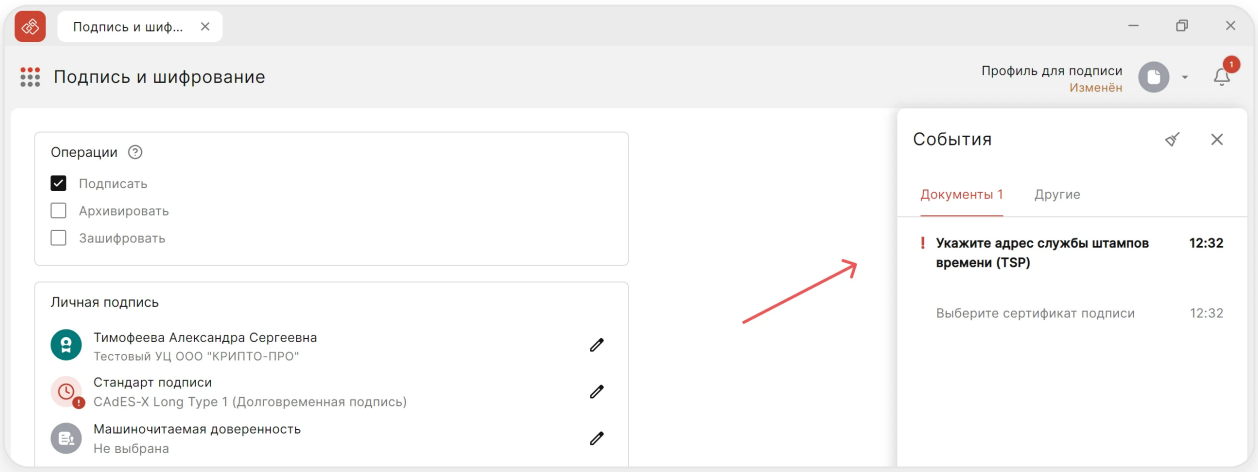
- нажатием на всплывающее уведомление;
- кликом по иконке в верхнем правом углу окна.

Структура центра уведомлений:

- **Текущая** - Уведомления, связанные с разделом приложения, в котором вы работаете в данный момент
- **Другие** - Все остальные системные уведомления, полученные в ходе работы с приложением.

Новые уведомления выделены **жирным шрифтом**

Уведомления сортируются по времени — последние события отображаются вверху списка.



Работа с уведомлениями

1. **Просмотр деталей**:
    - Нажмите на уведомление для раскрытия дополнительной информации,
    - Используйте кнопку **Перейти в журнал** для полного отчета.
2. **Очистка**:
    - Удалите все уведомления с помощью кнопки

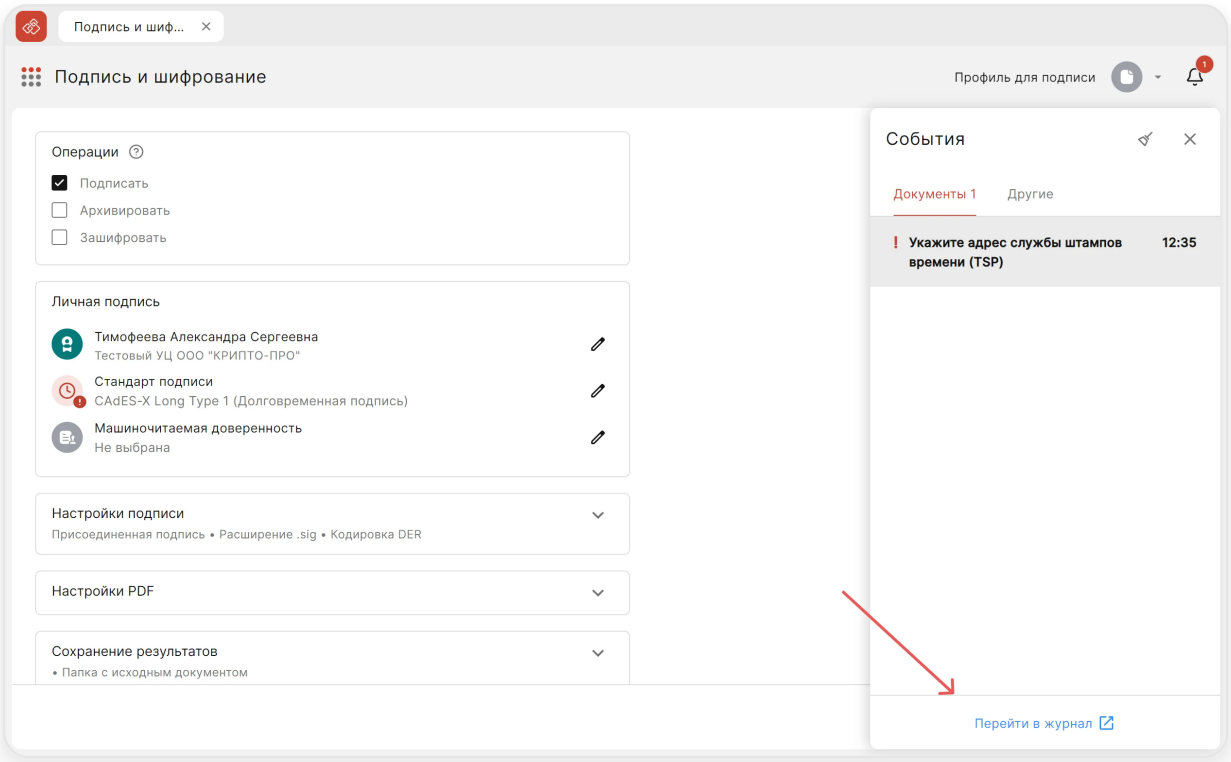
Журнал событий

Журнал событий фиксирует все значимые действия и ошибки в приложении и используется для диагностики, анализа сбоев и передачи данных в службу поддержки.

Открытие журнала

Через центр уведомлений:

1. Откройте центр уведомлений по кнопке , размещенной в верхнем правом углу окна.
2. Нажмите на **Перейти в журнал**.



Через главное меню:

1. Откройте главное меню приложения.
2. Выберите раздел **Журнал**.

Типы событий

Тип	Иконка	Описание	Примеры
Ошибка		Критические сбои	Не удалось подписать документ
Информация		Штатные операции	Успешная синхронизация

Работа с журналом

Просмотр деталей

1. Выделите запись в списке.
2. Нажмите на кнопку **Подробно** на панели действий.
3. В области справа от списка отобразится подробная информация о событии.

Копирование информации

1. Откройте детали события.
2. Нажмите **Скопировать** .
3. Данные будут сохранены в буфер обмена.

Экспорт в файл

Экспорт позволяет сохранить выбранные записи журнала в файл для анализа или передачи в службу поддержки.

1. Выделите с помощью флагов нужные события.
2. Нажмите на кнопку **Сохранить** на панели действий.
3. В файловом менеджере задайте имя и расположение файла `.log`.

Отправка по email

1. Выделите события
2. Нажмите **Отправить** на панели действий.
3. Будет создано новое письмо с вложенным файлом журнала.

Печать событий

1. Выделите с помощью флагов нужные события.
2. На верхней панели действий нажмите на кнопку **Распечатать**.

Настройки журнала

В программе можно настроить размер журнала и уровни логирования:

1. На панели действий нажмите на кнопку **Параметры журнала**.
2. Задайте параметры журнала:
    - Размер журнала (по умолчанию 2 МБ),
    - Уровень логирования.

> ⚠️ **Обратите внимание**:
> - Максимальный размер журнала — 10 МБ. При достижении максимального размера файла создается новый журнал без перезаписи старого.
> - Общие параметры, такие как имя, расположение, даты создания и изменения, недоступны для редактирования и являются информационными.

3. Нажмите на кнопку **Сохранить**.

Загрузка архивного журнала

Чтобы посмотреть события из архивного журнала:

1. На панели действий нажмите на кнопку **Загрузить архив**.
2. Укажите путь к файлу с архивным журналом.

Архивная копия открывается в новой вкладке.

Просмотр расположения файла событий

Чтобы перейти к расположению файла событий, нажмите на кнопку **Показать в папке** на панели действий.

Поиск и фильтрация

Для удобства работы с большим количеством записей в журнале предусмотрены быстрый поиск и расширенная фильтрация.

Быстрый поиск

Для фильтрации журнала используется строка поиска.

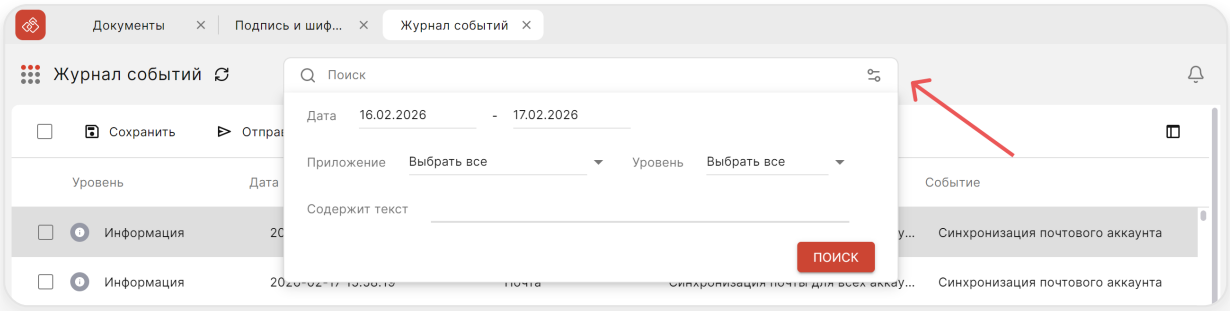
1. Установите курсор в строку поиска.
2. Введите поисковую фразу.

Поиск осуществляется по названию операции и тексту события.

Расширенная фильтрация

Для более детальной фильтрации вы можете задать параметры.

1. Нажмите на кнопку **Открыть фильтр** в строке поиска.
2. Укажите параметры:
   - **Дата** — диапазон дат;
   - **Приложение** — раздел, в котором возникло событие;
   - **Уровень логирования**;
   - **Содержит текст** — ключевые слова в сообщении.



3. Нажмите кнопку **Поиск**.

Чтобы отменить примененный фильтр, нажмите на кнопку **Отменить запрос** ✕ в строке поиска.

Смотрите также

- Общие настройки — инструкция по настройке приложения КриптоАРМ.
- Установка сертификатов — руководство по установке сертификатов в КриптоАРМ.
- Подключение почтового аккаунта — инструкция по подключению почтовых ящиков в КриптоАРМ.

Открыть статью на сайте

Как выполнить обновление КриптоАРМ

Обновления КриптоАРМ приносят не только новые функции, но и улучшают безопасность, совместимость с операционными системами и общую производительность. В этой инструкции мы расскажем как проверить наличие обновлений и установить актуальную версию приложения.

Содержание:

- Автоматическая проверка при запуске
- Ручная проверка обновлений
- Предварительные версии
- Установка обновления
- Что делать, если обновление не обнаруживается?
- Смотрите также

Автоматическая проверка при запуске

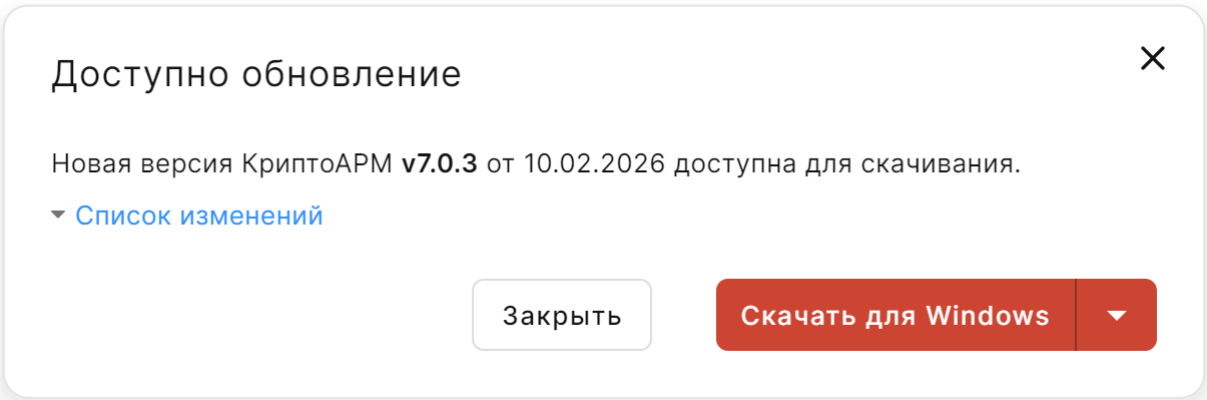
При каждом запуске программа автоматически обращается к серверу обновлений и проверяет наличие более свежей версии.

Если обновление доступно, появляется окно со следующими сведениями:

- номер новой версии;
- список изменений (новые возможности, исправленные ошибки, улучшения);
- предложение скачать установочный файл, соответствующий вашей операционной системе.

> 💡 **Примечание**: версия ОС определяется автоматически. Если вам нужен дистрибутив для другой платформы, нажмите на стрелку вниз рядом с кнопкой скачивания и выберите нужную ОС из выпадающего списка.

Пример окна:

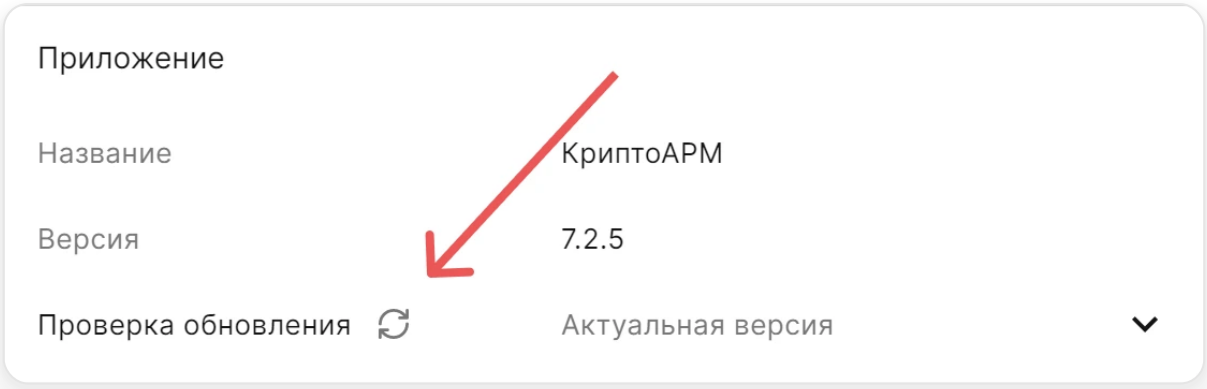


Ручная проверка обновлений

Вы можете в любой момент инициировать проверку вручную. Это полезно, если вы хотите убедиться в наличии обновлений до того, как перезапустите приложение.

Чтобы инициировать проверку вручную:

1. Откройте раздел **Настройки** → вкладка **О программе**.
2. В блоке **Приложение** нажмите на кнопку **Проверить обновления**.



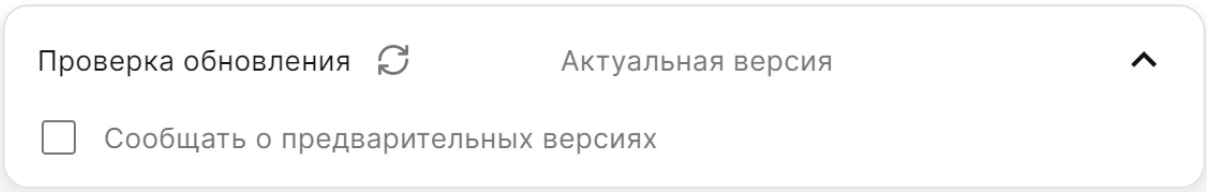
При обнаружении новой версии появится уже знакомое окно с предложением скачать дистрибутив.

Предварительные версии

В КриптоАРМ можно настроить получение предварительных версий. Такие версии содержат новые возможности, находящиеся в тестировании, и могут работать нестабильно.

Как включить уведомления о предварительных версиях

1. Откройте раздел **Настройки** → вкладка **О программе**.
2. Нажмите на кнопку напротив настройки **Проверка обновлений**.
3. Установите флажок **Сообщать о предварительных версиях**, чтобы получать уведомления о бета-версиях. Снимите флажок, чтобы получать только стабильные версии.



После изменения ветки обновлений выполните проверку обновлений вручную (см. Ручная проверка обновлений).

Установка обновления

После того как вы нажали кнопку скачивания в окне обновления, установочный файл будет загружен в стандартную папку загрузок вашей системы. Запустите его и следуйте инструкциям мастера установки.

> ⚠️ **Примечание**: перед установкой обновления рекомендуется закрыть приложение КриптоАРМ, чтобы избежать конфликтов.

Воспользуйтесь инструкцией по установке КриптоАРМ на свою платформу:

- Установка на Windows — руководство по установке КриптоАРМ на Windows.
- Установка на Linux — руководство по установке КриптоАРМ на Linux.
- Установка на macOS — руководство по установке КриптоАРМ на macOS.

> 📌 При обновлении приложения лицензия останется действующей. Повторная активация после обновления не нужна.

Что делать, если обновление не обнаруживается?

Иногда автоматическая или ручная проверка может не показывать новую версию, даже если вы знаете о её выходе.

Возможные причины и решения:

Проблема	Решение
Отсутствует подключение к интернету	Проверьте соединение и повторите попытку.
Брандмауэр или антивирус блокирует обращение к серверу обновлений	Добавьте КриптоАРМ в исключения или временно отключите защиту.
Используется прокси-сервер	Убедитесь, что в системе настроены параметры прокси.
Установлена самая свежая версия	Проверьте номер текущей версии в разделе **Настройки → КриптоАРМ → Версия**.

> 🚨 Если ни одно из решений не помогло, обратитесь в техническую поддержку: support@trusted.ru.

Смотрите также

- Общие настройки — инструкция по настройке приложения КриптоАРМ.
- Установка на Windows — руководство по установке КриптоАРМ на Windows.
- Установка на Linux — руководство по установке КриптоАРМ на Linux.
- Установка на macOS — руководство по установке КриптоАРМ на macOS.

Открыть статью на сайте

Как добавить почтовый аккаунт в КриптоАРМ

Эта инструкция поможет подключить почтовый аккаунт в КриптоАРМ. Вы узнаете, как добавить почту популярных сервисов, выбрать активный аккаунт и решить типовые проблемы подключения.

> 🔍 Подробные инструкции для конкретных почтовых сервисов: **Mail.ru** · **Yandex** · **Gmail** · **Outlook.com** · **iCloud** · **Rambler**

Содержание:

- Подключение почтового аккаунта
- Выбор активного аккаунта
- Удаление почтового аккаунта
- Смотрите также

Подключение почтового аккаунта

> 💡 В КриптоАРМ можно добавить **несколько почтовых аккаунтов** и свободно переключаться между ними.

Шаг 1. Настройки подключения

> 💡 КриптоАРМ автоматически подставляет параметры подключения для большинства популярных почтовых сервисов после ввода адреса электронной почты.

1. Откройте форму добавления аккаунта:
   - В разделе **Почта** нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
   - В разделе **Настройки** → проверка **Почтовые аккаунты** нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
   - **Адрес электронной почты**,

- **Пароль**: используйте либо основной пароль от ящика, либо специальный пароль приложения, который необходимо создать в настройках почтового сервиса.

  Инструкции по созданию паролей приложений:

Почтовый сервис	Ссылка на инструкцию
Mail.ru	🔗 help.mail.ru
Yandex	🔗 yandex.ru/support
Gmail (Google)	🔗 support.google.com
Outlook.com (Microsoft)	🔗 support.microsoft.com

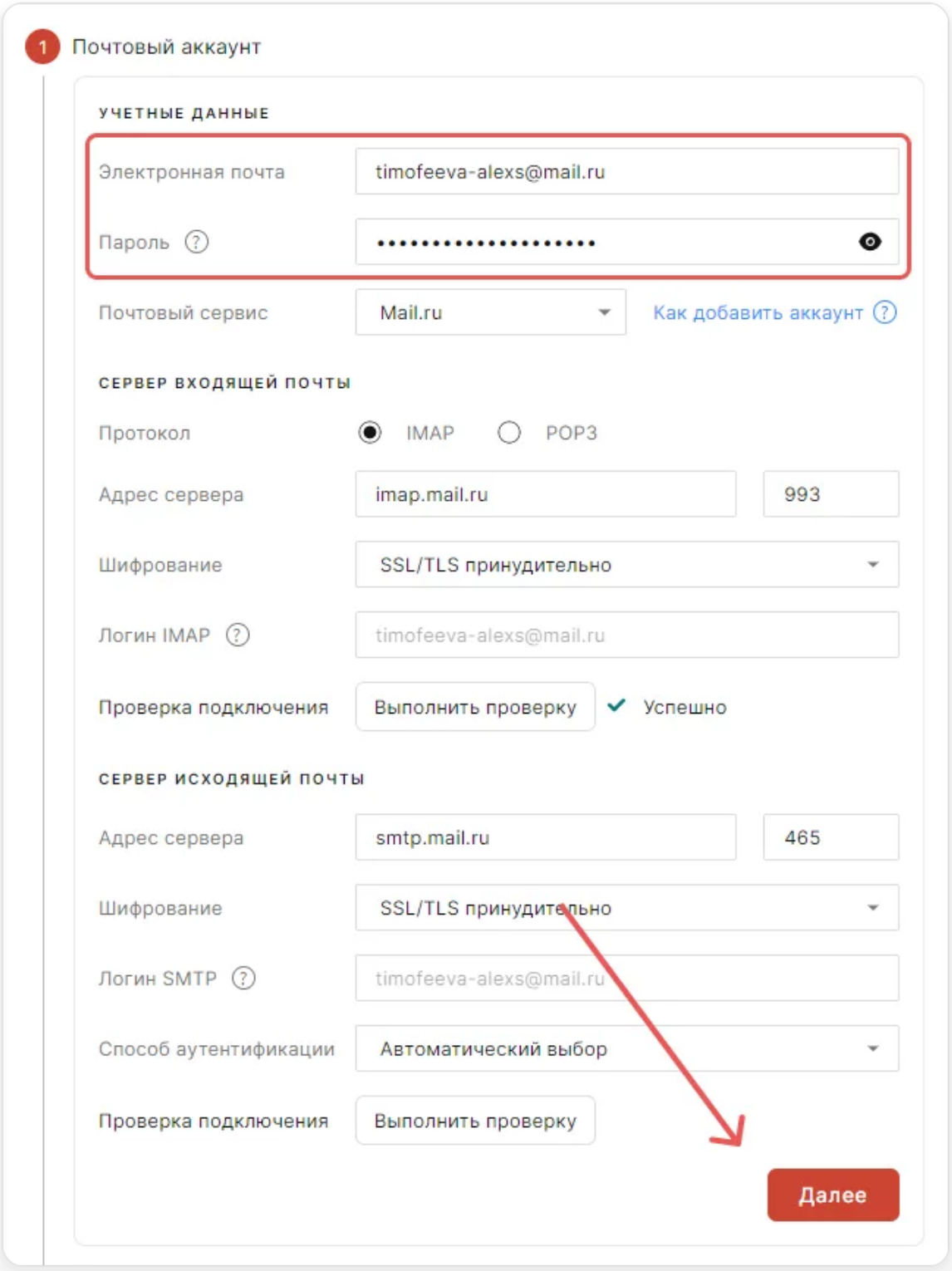
- **Почтовый сервис**,
- **Протокол подключения**,
- **Адреса серверов** входящей и исходящей почты, параметры шифрования,
- **Логин IMAP/SMTP**: логин для подключения к серверу входящей/исходящей почты. Обычно совпадает с адресом электронной почты, но на некоторых серверах может отличаться.

> 💡 **Подсказка:**
> Если поле логина оставить пустым, будет использован адрес электронной почты, указанный выше.

- **Способ аутентификации**.

  Выберите, каким образом приложение будет выполнять вход на почтовый сервер:

Способ	Назначение
Автоматический	Рекомендуемый способ
Логин	Публичные почтовые сервисы
NTLM	Корпоративная почта Microsoft
GSS-API (Kerberos)	Доменная аутентификация

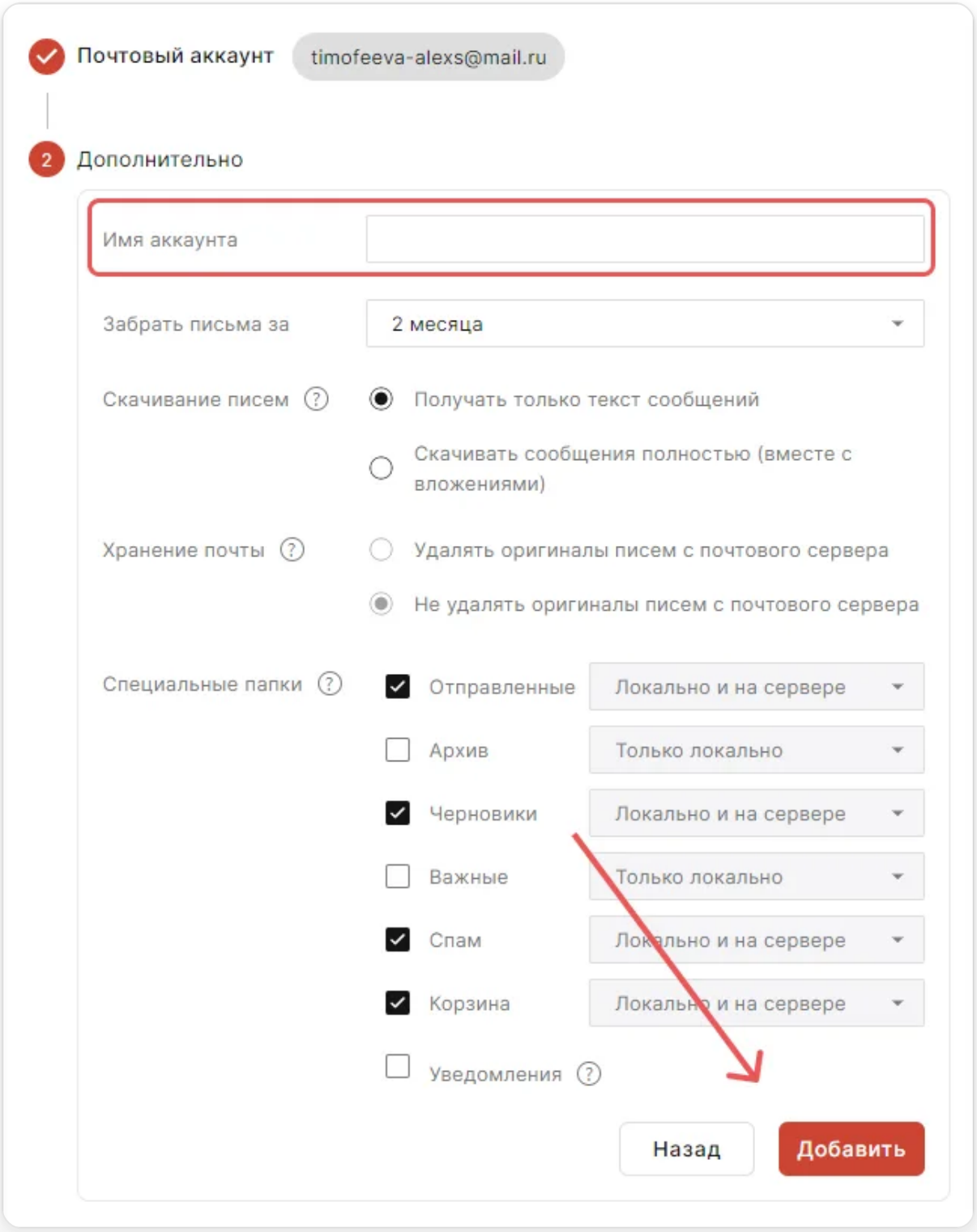


3. Нажмите на кнопку **Далее**.

> 💡 **Подсказка:**
> Нажмите **Выполнить проверку**, чтобы убедиться, что параметры подключения указаны верно. В случае ошибки приложение подскажет, что нужно исправить.

Шаг 2. Настройки почтового ящика

1. Укажите **имя аккаунта** для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.



После добавления аккаунта запустится синхронизация, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта выберите его активным.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при добавлении аккаунта:

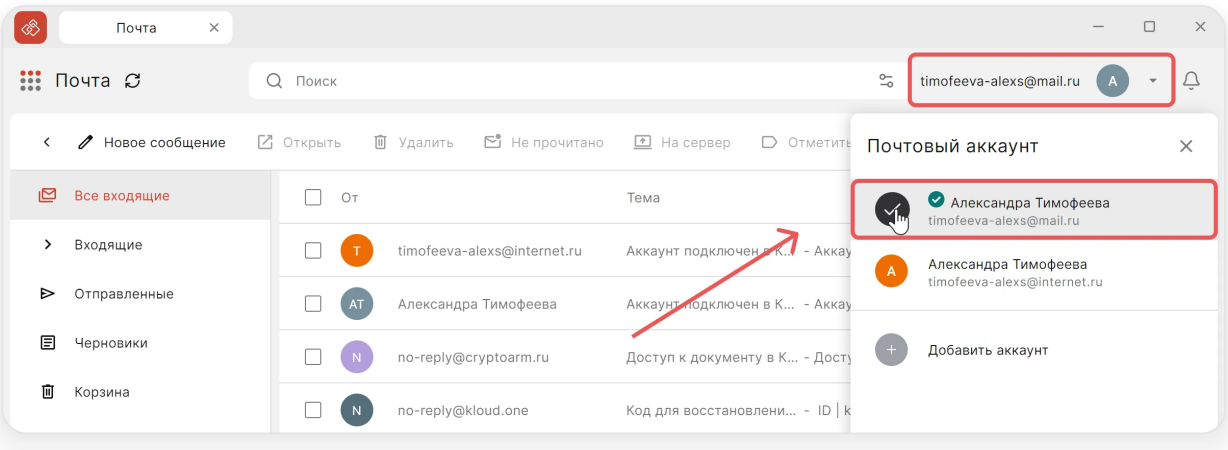
Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка аутентификации	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Выбор активного аккаунта

Выберите активный аккаунт, чтобы просматривать и управлять его письмами. В папке **Все входящие** отображаются письма всех подключенных аккаунтов, в остальных папках — только выбранного.

Как выбрать активный аккаунт

1. Перейдите в раздел **Почта**.
2. Нажмите на имя текущего активного аккаунта.



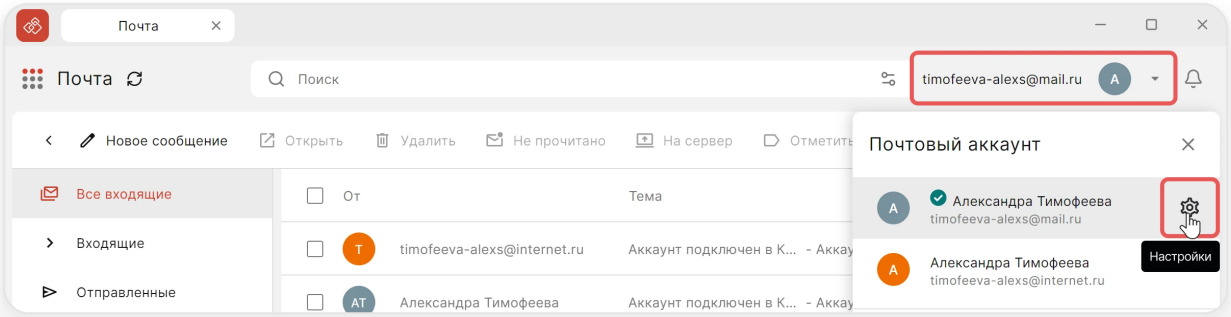
3. Кликните по аватару нужного аккаунта.

Аккаунт отмечается иконкой и становится активным.

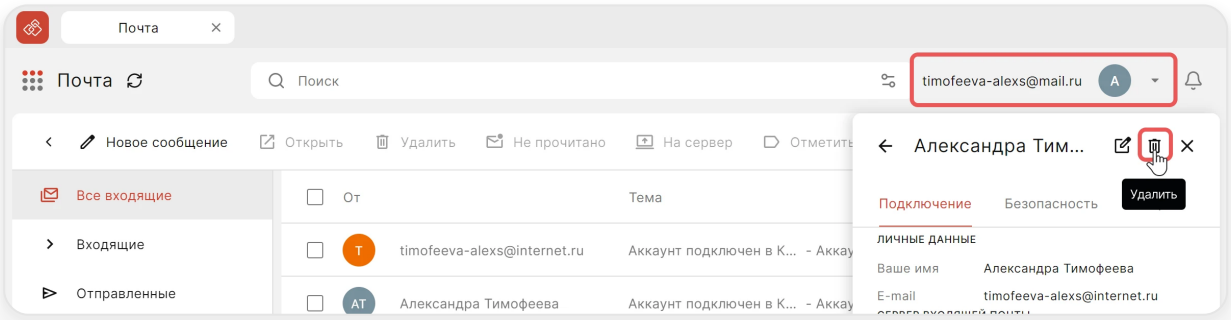
Удаление почтового аккаунта

Чтобы удалить почтовый аккаунт из приложения:

1. Перейдите в раздел **Почта**.
2. Нажмите на имя активного аккаунта.
3. Наведите курсор на аккаунт, который хотите удалить.

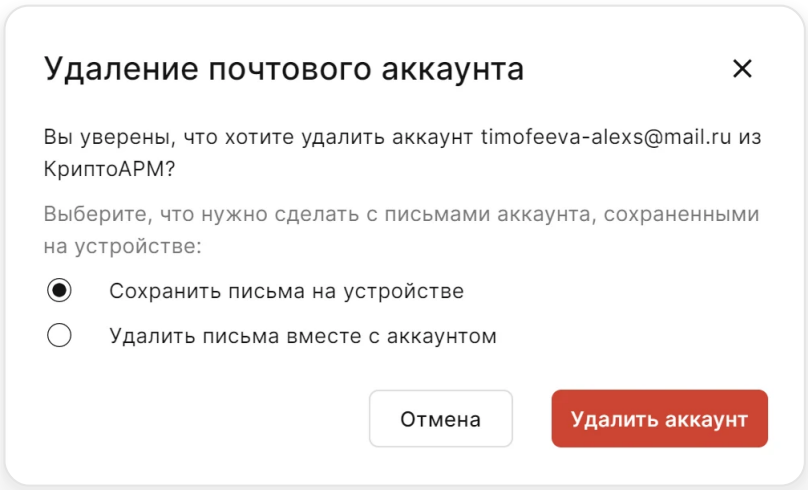


4. Нажмите всплывающую кнопку **Настройки**.
5. В открывшемся окне нажмите кнопку **Удалить** и подтвердите удаление.



Если в вашем аккаунте имеются сохраненные письма, вам необходимо выбрать, как с ними поступить:

- **Удалить письма вместе с аккаунтом** — все письма будут безвозвратно удалены.
- **Сохранить письма на устройстве** — все письма из этого аккаунта сохранятся в папке **Сохраненные письма**, а сам аккаунт будет удален из списка подключенных.



Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как подключить почту Mail.ru в КриптоАРМ

Узнайте, как добавить почту Mail.ru в КриптоАРМ, настроить отправку и получение писем, а также избежать распространённых проблем при подключении.

Содержание:

- Создание пароля приложения
- Добавление аккаунта
- Возможные ошибки
- Смотрите также

Создание пароля приложения

Перед добавлением почтового аккаунта необходимо создать специальный пароль для приложения КриптоАРМ в настройках почтового сервиса.

Для создания специального пароля воспользуйтесь официальной инструкцией на портале help.mail.ru.

Добавление аккаунта

Шаг 1. Настройки подключения

1. Откройте форму добавления аккаунта:
    - В разделе **Почта** нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - В разделе **Настройки** → проверка **Почтовые аккаунты** нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
    - **Учетные данные**: адрес электронной почты и созданный пароль приложения,
    - **Почтовый сервис**: mail.ru,
    - **Протокол подключения**,
    - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

> 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Mail.ru.

- **Способ аутентификации**: автоматический или логин.
- **Логин IMAP/SMTP**: логин для подключения к серверу входящей/исходящей почты. Если оставить поле логина пустым, приложение автоматически использует электронный адрес, указанный выше.

3. Нажмите на кнопку **Далее** для перехода на следующий шаг.

> 💡 **Подсказка:**
> Нажмите **Выполнить проверку**, чтобы убедиться, что параметры подключения указаны верно. В случае ошибки приложение подскажет, что нужно исправить.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После добавления аккаунта запустится синхронизация, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта выберите его активным.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при добавлении аккаунта:

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка аутентификации	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как подключить почту Yandex в КриптоАРМ

Узнайте, как добавить почту Yandex в КриптоАРМ, настроить отправку и получение писем, а также избежать распространённых проблем при подключении.

Содержание:

- Перед добавлением
- Добавление аккаунта
- Возможные ошибки
- Смотрите также

Перед добавлением

Перед добавлением почтового аккаунта выполните дополнительные настройки в почтовом сервисе и создайте специальный пароль для приложения КриптоАРМ.

Настройка доступа

1. Откройте раздел **Почтовые программы** в настройках **Яндекс Почты**.
2. Выберите опции **Разрешить доступ к почтовому ящику с помощью почтовых клиентов** → **С сервера imap.yandex.ru по протоколу IMAP** и **Пароли приложений и OAuth-токены**.
3. Сохраните изменения.

Создание пароля приложения

Для безопасного подключения почтового аккаунта создайте специальный пароль для приложения КриптоАРМ. Используйте официальную инструкцию на портале yandex.ru.

Добавление аккаунта

Шаг 1. Настройки подключения

1. Откройте форму добавления аккаунта:
    - В разделе **Почта** нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - В разделе **Настройки** → проверка **Почтовые аккаунты** нажмите на кнопку **Добавить аккаунт**.

2. Укажите параметры подключения:
   - **Учетные данные**: адрес электронной почты и созданный пароль приложения,
   - **Почтовый сервис**: yandex.ru,
   - **Протокол подключения**,
   - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

     > 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Яндекс.

   - **Способ аутентификации**: автоматический или логин.
   - **Логин IMAP/SMTP**: логин для подключения к серверу входящей/исходящей почты. Если оставить поле логина пустым, приложение автоматически использует электронный адрес, указанный выше.
3. Нажмите на кнопку **Далее** для перехода на следующий шаг.

> 💡 **Подсказка:**
> Нажмите **Выполнить проверку**, чтобы убедиться, что параметры подключения указаны верно. В случае ошибки приложение подскажет, что нужно исправить.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После добавления аккаунта запустится синхронизация, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта выберите его активным.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при добавлении аккаунта:

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка аутентификации	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как подключить почту Gmail в КриптоАРМ

Узнайте, как добавить почту Gmail в КриптоАРМ, настроить отправку и получение писем, а также избежать распространённых проблем при подключении.

Содержание:

- Создание пароля приложения
- Добавление аккаунта
- Возможные ошибки
- Смотрите также

Создание пароля приложения

Перед добавлением почтового аккаунта необходимо создать специальный пароль для приложения КриптоАРМ в настройках почтового сервиса.

Для создания специального пароля воспользуйтесь официальной инструкцией на портале support.google.com.

> ⚠️ **Примечание**: Для создания пароля приложения в аккаунте Google должна быть включена двухэтапная аутентификация.

Добавление аккаунта

Шаг 1. Настройки подключения

1. Откройте форму добавления аккаунта:
    - В разделе **Почта** нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - В разделе **Настройки** → проверка **Почтовые аккаунты** нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
    - **Учетные данные**: адрес электронной почты и созданный пароль приложения,
    - **Почтовый сервис**: gmail.com,

- **Протокол подключения**,
- **Адреса серверов** входящей и исходящей почты, параметры шифрования.

> 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Gmail.

- **Способ аутентификации**: автоматический или логин.
- **Логин IMAP/SMTP**: логин для подключения к серверу входящей/исходящей почты. Если оставить поле логина пустым, приложение автоматически использует электронный адрес, указанный выше.

3. Нажмите на кнопку **Далее** для перехода на следующий шаг.

> 💡 **Подсказка:**
> Нажмите **Выполнить проверку**, чтобы убедиться, что параметры подключения указаны верно. В случае ошибки приложение подскажет, что нужно исправить.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После добавления аккаунта запустится синхронизация, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта выберите его активным.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при добавлении аккаунта:

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка аутентификации	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как подключить почту Outlook в КриптоАРМ

Узнайте, как добавить почту Outlook в КриптоАРМ, настроить отправку и получение писем, а также избежать распространённых проблем при подключении.

Содержание:

- Создание пароля приложения
- Добавление аккаунта
- Возможные ошибки
- Смотрите также

Создание пароля приложения

Перед добавлением почтового аккаунта необходимо создать специальный пароль для приложения КриптоАРМ в настройках почтового сервиса.

Для создания специального пароля воспользуйтесь официальной инструкцией на портале support.microsoft.com.

Добавление аккаунта

Шаг 1. Настройки подключения

1. Откройте форму добавления аккаунта:
    - В разделе **Почта** нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - В разделе **Настройки** → проверка **Почтовые аккаунты** нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
    - **Учетные данные**: адрес электронной почты и созданный пароль приложения,
    - **Почтовый сервис**: outlook.com,
    - **Протокол подключения**,
    - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

> 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Outlook.

- **Способ аутентификации**: автоматический или логин.
- **Логин IMAP/SMTP**: логин для подключения к серверу входящей/исходящей почты. Если оставить поле логина пустым, приложение автоматически использует электронный адрес, указанный выше.

3. Нажмите на кнопку **Далее** для перехода на следующий шаг.

> 💡 **Подсказка:**
> Нажмите **Выполнить проверку**, чтобы убедиться, что параметры подключения указаны верно. В случае ошибки приложение подскажет, что нужно исправить.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После добавления аккаунта запустится синхронизация, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта выберите его активным.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при добавлении аккаунта:

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка аутентификации	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как подключить почту iCloud в КриптоАРМ

Узнайте, как добавить почту iCloud в КриптоАРМ, настроить отправку и получение писем, а также избежать распространённых проблем при подключении.

Содержание:

- Создание пароля приложения
- Добавление аккаунта
- Возможные ошибки
- Смотрите также

Создание пароля приложения

Перед добавлением почтового аккаунта необходимо создать специальный пароль для приложения КриптоАРМ в настройках почтового сервиса.

Для создания специального пароля воспользуйтесь официальной инструкцией на портале support.apple.com.

Добавление аккаунта

Шаг 1. Настройки подключения

1. Откройте форму добавления аккаунта:
    - В разделе **Почта** нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - В разделе **Настройки** → проверка **Почтовые аккаунты** нажмите на кнопку **Добавить аккаунт**.
2. Укажите параметры подключения:
    - **Учетные данные**: адрес электронной почты и созданный пароль приложения,
    - **Почтовый сервис**: icloud.com,
    - **Протокол подключения**,
    - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

> 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки ICloud.

- **Способ аутентификации**: автоматический или логин.
- **Логин IMAP/SMTP**: логин для подключения к серверу входящей/исходящей почты. Если оставить поле логина пустым, приложение автоматически использует электронный адрес, указанный выше.

3. Нажмите на кнопку **Далее** для перехода на следующий шаг.

> 💡 **Подсказка:**
> Нажмите **Выполнить проверку**, чтобы убедиться, что параметры подключения указаны верно. В случае ошибки приложение подскажет, что нужно исправить.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
   - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
   - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
   - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
   - **Не удалять оригиналы писем с почтового сервера** — письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После добавления аккаунта запустится синхронизация, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта выберите его активным.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при добавлении аккаунта:

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка аутентификации	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как подключить почту Rambler в КриптоАРМ

Узнайте, как добавить почту Rambler в КриптоАРМ, настроить отправку и получение писем, а также избежать распространённых проблем при подключении.

Содержание:

- Перед добавлением
- Добавление аккаунта
- Возможные ошибки
- Смотрите также

Перед добавлением

Перед добавлением почтового аккаунта выполните дополнительные настройки в почтовом сервисе и создайте специальный пароль для приложения КриптоАРМ.

Настройка доступа

Для корректной работы почтового аккаунта убедитесь, что доступ к ящику разрешён для внешних приложений. Подробную инструкцию по настройке доступа к почтовому ящику читайте на портале официальной документации help.rambler.ru.

Создание пароля приложения

Для безопасного подключения почтового аккаунта создайте специальный пароль для приложения КриптоАРМ. Используйте официальную инструкцию на портале help.rambler.ru.

Добавление аккаунта

Шаг 1. Настройки подключения

1. Откройте форму добавления аккаунта:
    - В разделе **Почта** нажмите на кнопку **Добавить аккаунт** в центре окна (если аккаунты еще не подключены) или в окне со списком почтовых аккаунтов.
    - В разделе **Настройки** → проверка **Почтовые аккаунты** нажмите на кнопку **Добавить аккаунт**.

2. Укажите параметры подключения:
    - **Учетные данные**: адрес электронной почты и созданный пароль приложения,
    - **Почтовый сервис**: rambler.ru,
    - **Протокол подключения**,
    - **Адреса серверов** входящей и исходящей почты, параметры шифрования.

    > 💡 Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Rambler.

    - **Способ аутентификации**: автоматический или логин.
    - **Логин IMAP/SMTP**: логин для подключения к серверу входящей/исходящей почты. Если оставить поле логина пустым, приложение автоматически использует электронный адрес, указанный выше.
3. Нажмите на кнопку **Далее** для перехода на следующий шаг.

> 💡 **Подсказка:**
> Нажмите **Выполнить проверку**, чтобы убедиться, что параметры подключения указаны верно. В случае ошибки приложение подскажет, что нужно исправить.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта для отображения в приложении.
2. Настройте период, за который необходимо загрузить письма с сервера.
3. Укажите параметры загрузки писем:
    - **Получать только текст сообщений** — ускоренная загрузка без вложений. Загрузка вложений будет запущена при открытии письма.
    - **Скачивать сообщения полностью** (вместе с вложениями) — загрузка писем со всеми вложениями.
4. Укажите настройки хранения почты:
    - **Удалять оригиналы писем с почтового сервера** — письма будут удалены с почтового сервера после загрузки на устройство.
    - **Не удалять оригиналы писем с почтового сервера** — письма останутся на сервере после загрузки на устройство.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить** для завершения.

После добавления аккаунта запустится синхронизация, которая может занять некоторое время в зависимости от объема писем.

> 💡 Для просмотра писем нового аккаунта выберите его активным.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при добавлении аккаунта:

Ошибка	Решение
Ошибка соединения	Проверьте интернет-подключение и доступность почтового сервера
Ошибка аутентификации	Убедитесь в правильности: - Адреса электронной почты и пароля - Серверных настроек - Параметров подключения

Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как настроить почту в КриптоАРМ

Эта инструкция поможет настроить почтовый аккаунт в приложении КриптоАРМ. Вы узнаете, как отправлять и получать защищённые письма, изменять настройки подключения, а также настраивать специальные папки и хранение писем.

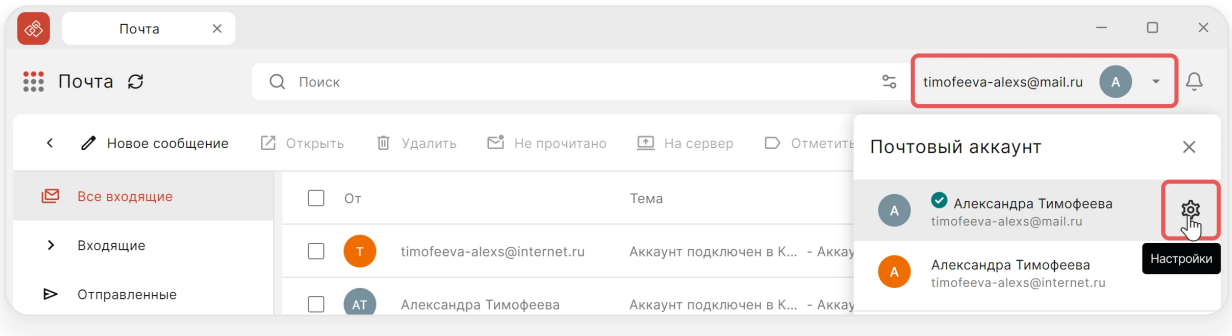
Содержание:

- Как открыть настройки почтового аккаунта
- Настройки для отправки и получения защищенной почты
- Настройки подключения
- Общие настройки
- Подписи (контактная информация)
- Смотрите также

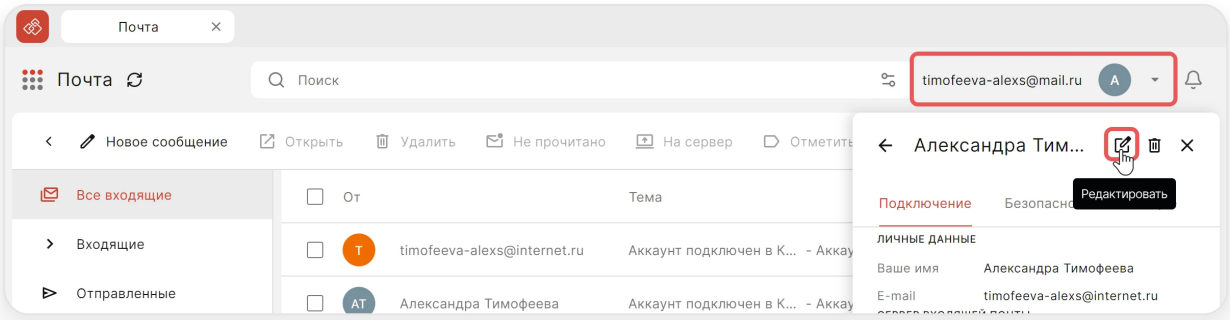
Как открыть настройки почтового аккаунта

Чтобы открыть настройки почтового аккаунта:

1. Перейдите в раздел **Почта**.
2. Нажмите на имя активного аккаунта в верхнем правом углу окна.
3. В открывшемся окне наведите курсор на аккаунт, настройки которого надо изменить.



4. Нажмите всплывающую кнопку **Настройки**.
5. Откроется окно с настройками аккаунта.
6. Нажмите кнопку **Редактировать** .



7. Откроется окно настроек почтового аккаунта со следующими вкладками:
   - Безопасность — параметры подписи и шифрования писем;
   - Подключение — параметры подключения и управление специальными папками;
   - Общие — настройки группировки писем и уведомлений;
   - Подписи — настройка контактной информации в письмах.

Настройки для отправки и получения защищенной почты

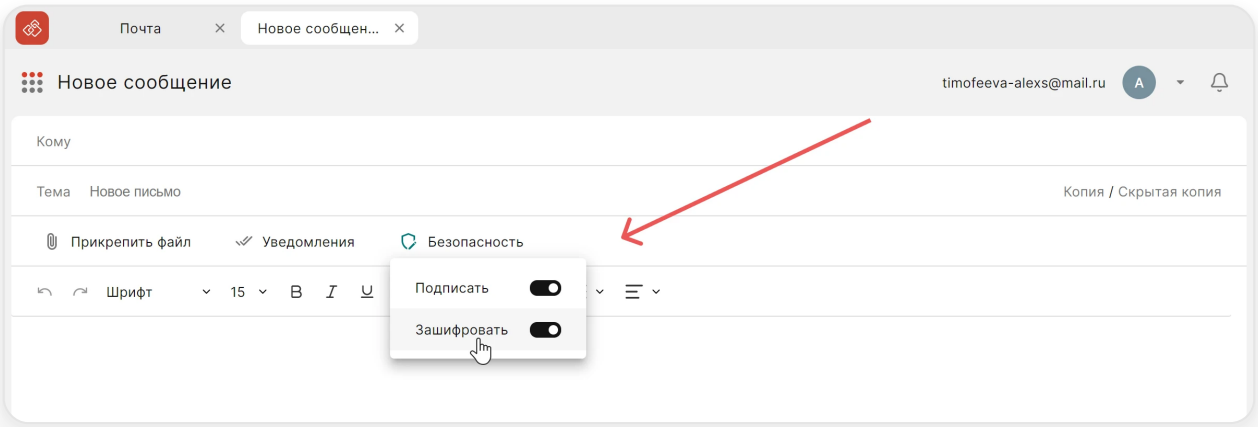
Настройка подписи и шифрования исходящих писем

Чтобы активировать подпись и шифрование для исходящих писем:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Безопасность**.
3. Активируйте переключатели в блоке **Безопасность почты**:
   - **Шифровать содержимое и вложения исходящих сообщений** — автоматическое шифрование писем в адрес получателей, имеющих привязанные сертификаты.
   - **Добавлять электронную подпись к исходящим сообщениям** — автоматическое добавление электронной подписи к исходящим письмам при условии, что к аккаунту привязан сертификат подписи.

Настройки применяются без дополнительного подтверждения.

При открытии вкладки с новым письмом переключатели будут выставлены в соответствии с указанными настройками.

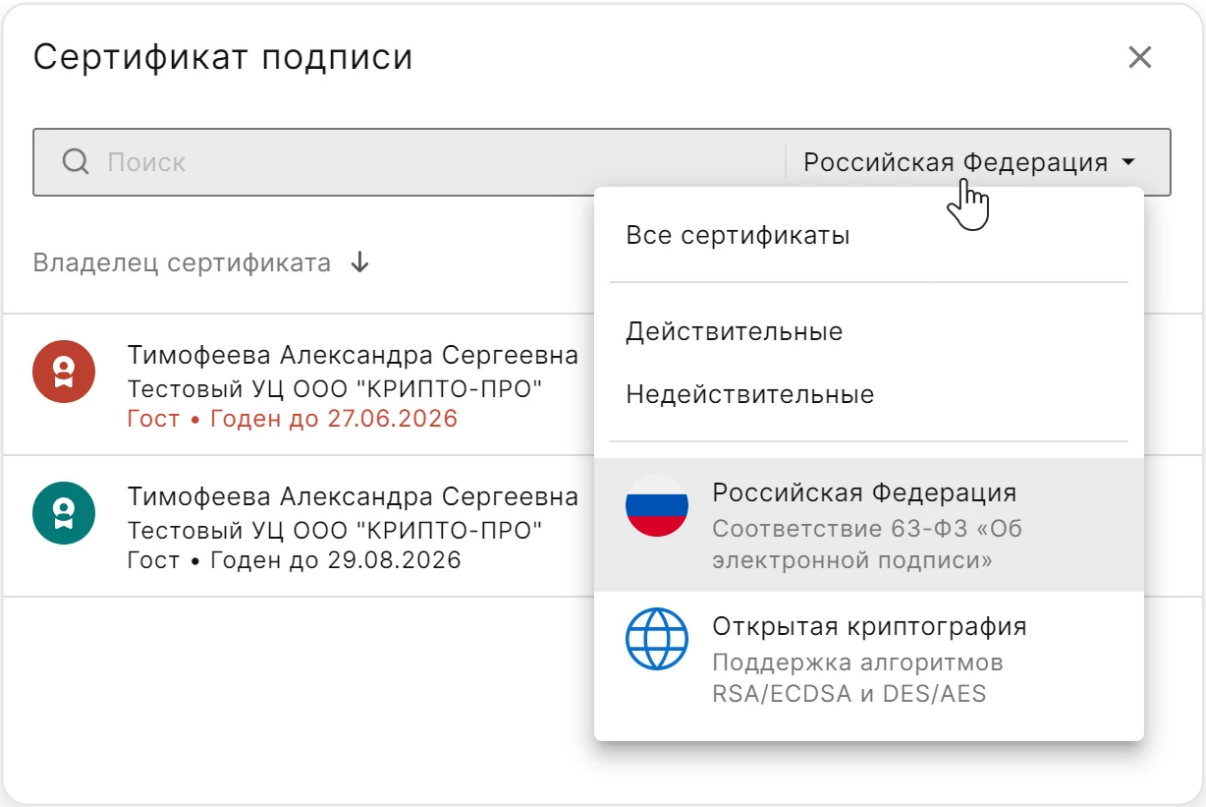


Привязка сертификата подписи

> 💡 В приложении к аккаунту можно привязать только один личный сертификат.

Чтобы привязать сертификат к почтовому аккаунту:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Безопасность**.
3. В блоке **Настройки подписи** нажмите кнопку **Редактировать** .
4. Откроется окно **Сертификат подписи** со списком личных сертификатов.



5. При необходимости воспользуйтесь фильтрацией списка сертификатов:
    - выберите **профиль доверия**:
        - **Российская Федерация** — отображаются сертификаты с алгоритмами ГОСТ;
        - **Открытая криптография** — отображаются сертификаты с алгоритмами RSA;
    - включите отображение только **действительных сертификатов**, если необходимо скрыть недействительные сертификаты;
    - воспользуйтесь **строкой поиска**, чтобы быстро найти сертификат по имени владельца или другим данным.
6. Выберите сертификат.

После выбора сертификат будет автоматически привязан в настройках аккаунта.

При необходимости привязанный сертификат можно заменить или отвязать.

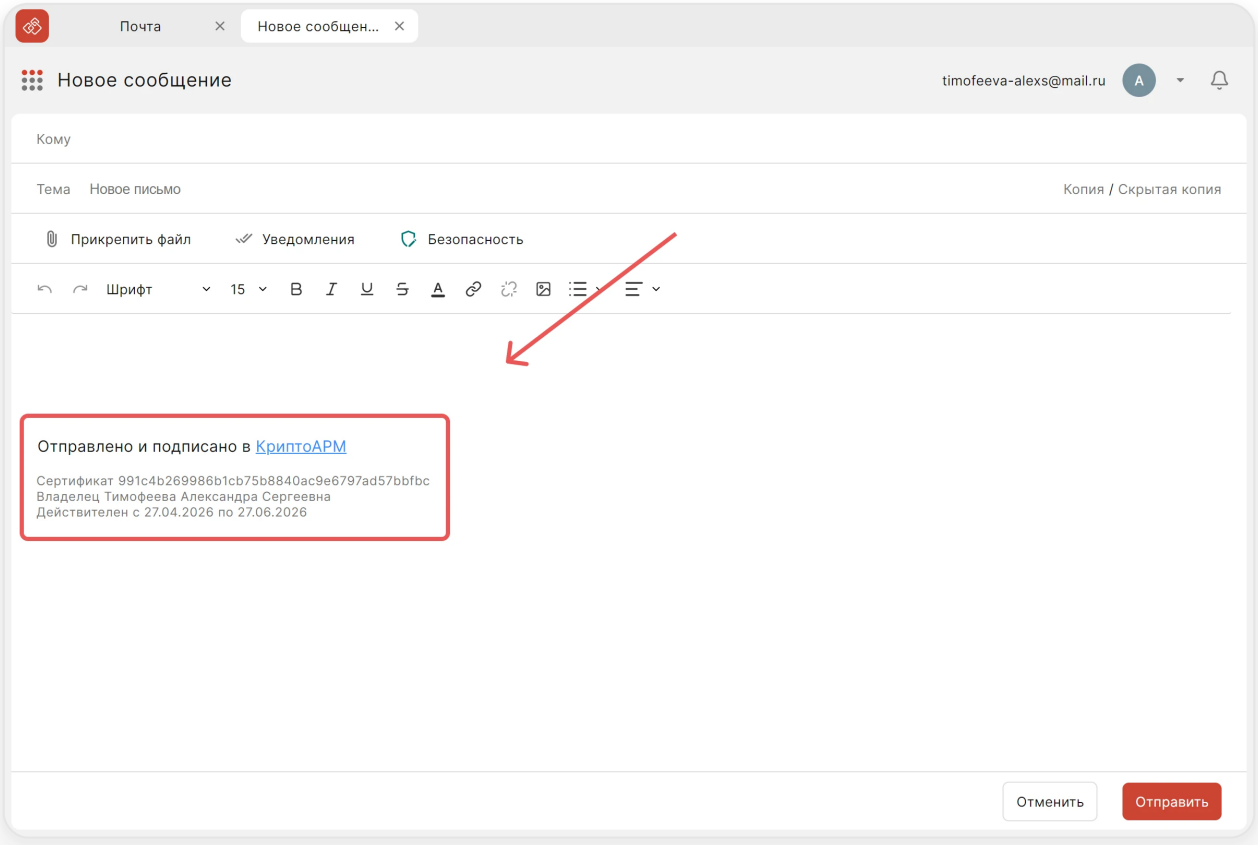
Отображение информации о сертификате

В конце каждого исходящего подписанного письма можно настроить отображение информации о сертификате подписи: отпечаток, имя владельца и срок действия. Это позволит получателям, на устройствах которых не установлено приложение КриптоАРМ, увидеть информацию о сертификате подписи письма.

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Безопасность**.
3. Активируйте переключатель **Отображать информацию об электронной подписи в исходящих письмах**.

Настройки автоматически применяются без дополнительного подтверждения.

Теперь, когда вы отправляете подписанное письмо, данные о сертификате автоматически добавляются в его конец.



Выбор алгоритма шифрования

Чтобы настроить алгоритм шифрования исходящего зашифрованного письма:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Безопасность**.

3. Выберите один из предложенных вариантов: ГОСТ 28147-89, ГОСТ Р 34.12-2015 Магма, ГОСТ Р 34.12-2015 Кузнечик, AES-256-CBC, DES3-CBC.

> 🔐 Алгоритмы ГОСТ доступны при установленном криптопровайдере КриптоПро CSP.

Настройки автоматически применяются без дополнительного подтверждения.

Дополнительные настройки шифрования

Для отправки зашифрованных писем доступны дополнительные настройки:

- **Использовать сертификат получателя и сертификат подписи почтового аккаунта** — исходящие письма будут шифроваться в адрес сертификатов получателей и в адрес сертификата подписи почтового аккаунта. В папке исходящих писем можно ознакомиться с содержимым отправленного зашифрованного письма.
- **Использовать только сертификат получателя** — исходящие письма будут шифроваться **только** в адрес сертификатов получателей. В папке исходящих писем невозможно будет расшифровать такое письмо и узнать его содержание.

Хранение зашифрованных сообщений

- **Хранить входящие сообщения в расшифрованном виде** — все зашифрованные сообщения, которые были хотя бы один раз расшифрованы, будут храниться в расшифрованном виде.
- **Хранить входящие сообщения в зашифрованном виде** — все зашифрованные сообщения (расшифрованные и зашифрованные), будут храниться в зашифрованном виде.

Скачивание писем

- **Получать только текст сообщений** — при получении письма будет загружен только его текст. Загрузка вложений начнется только при открытии письма. Выбор этой настройки позволит ускорить процесс получения писем.
- **Скачивать сообщения полностью** — при получении письмо будет загружено в полном объеме, включая все вложения.

Настройка хранения почты

В приложении доступно два варианта хранения писем:

1. **Локальное хранение на устройстве**
    - Письма удаляются с сервера после загрузки,
    - Письма фильтруются в папку **Сохранённые письма** со всех аккаунтов,
    - Письма отмечаются специальным индикатором ,

2. **Хранение на сервере**
    - Письма остаются в исходной серверной папке
    - Доступны со всех устройств
    - Синхронизируются автоматически

> 💡Чтобы активировать настройку «Хранение почты», необходимо предварительно включить опцию **Скачивать сообщения полностью**.

Варианты настройки:

- **Удалять оригиналы писем с почтового сервера** — оригиналы писем будут удаляться с почтового сервера после синхронизации. Все письма данного почтового аккаунта будут храниться на этом устройстве и видны в папке «Сохранённые письма».
- **Не удалять оригиналы писем с почтового сервера** — данная настройка стоит по умолчанию. Письма не удаляются с почтового сервера автоматически.

Настройки подключения

Изменение адреса электронной почты

Чтобы изменить адрес электронной почты подключенного аккаунта:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта). Нажмите кнопку Редактировать.
2. Перейдите на вкладку **Подключение**.
3. В поле **Электронная почта** укажите новый адрес.
4. Нажмите кнопку **Сохранить** на появившейся панели действий.

Редактирование параметров подключения

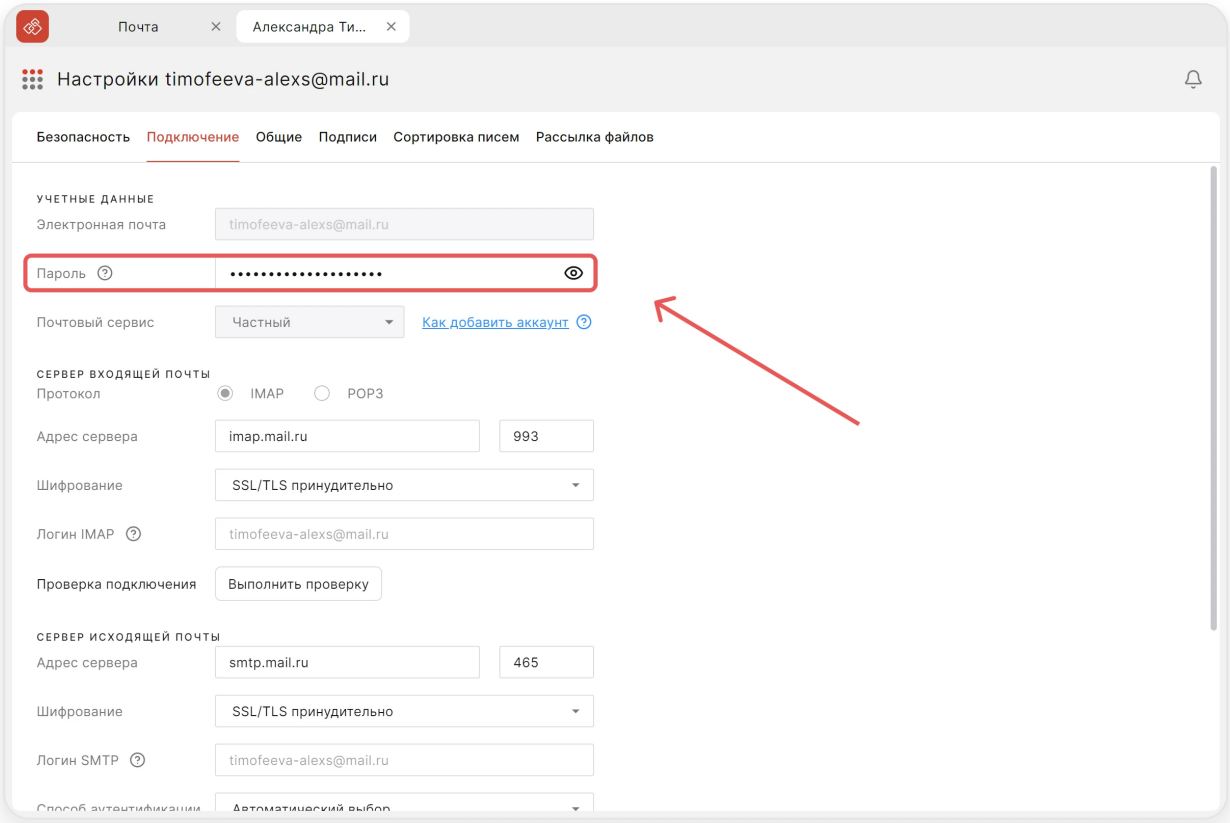
> 💡 При смене настроек подключения убедитесь, что выбран правильный способ аутентификации и указаны актуальные адреса серверов.

Чтобы изменить настройки подключения:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Подключение**.
3. При необходимости измените параметры подключения, включая адреса серверов, протоколы и способ аутентификации.
4. Нажмите кнопку **Сохранить** на появившейся панели действий.

Изменение пароля почтового аккаунта

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Подключение**.
3. Укажите новый пароль в блоке **Учетные данные**.
4. Нажмите кнопку **Сохранить** на появившейся панели действий



Настройка специальных папок

> 📌 **Специальные папки** — это виртуальные папки, предназначенные для удобной организации и просмотра писем по определенным критериям.

Типы специальных папок:

- **Отправленные** — для хранения исходящих писем,
- **Архив** — для долгосрочного хранения важных сообщений,
- **Черновики** — временное хранилище незавершенных писем,
- **Важные** — для приоритетной корреспонденции,
- **Спам** — для удаления нежелательных сообщений,
- **Корзина** — для восстановления удаленных писем,
- **Уведомления** — для отслеживания писем с уведомлениями о доставке и прочтении.

Если в аккаунте отсутствуют перечисленные специальные папки, можно создать их вручную с выбором типа синхронизации:

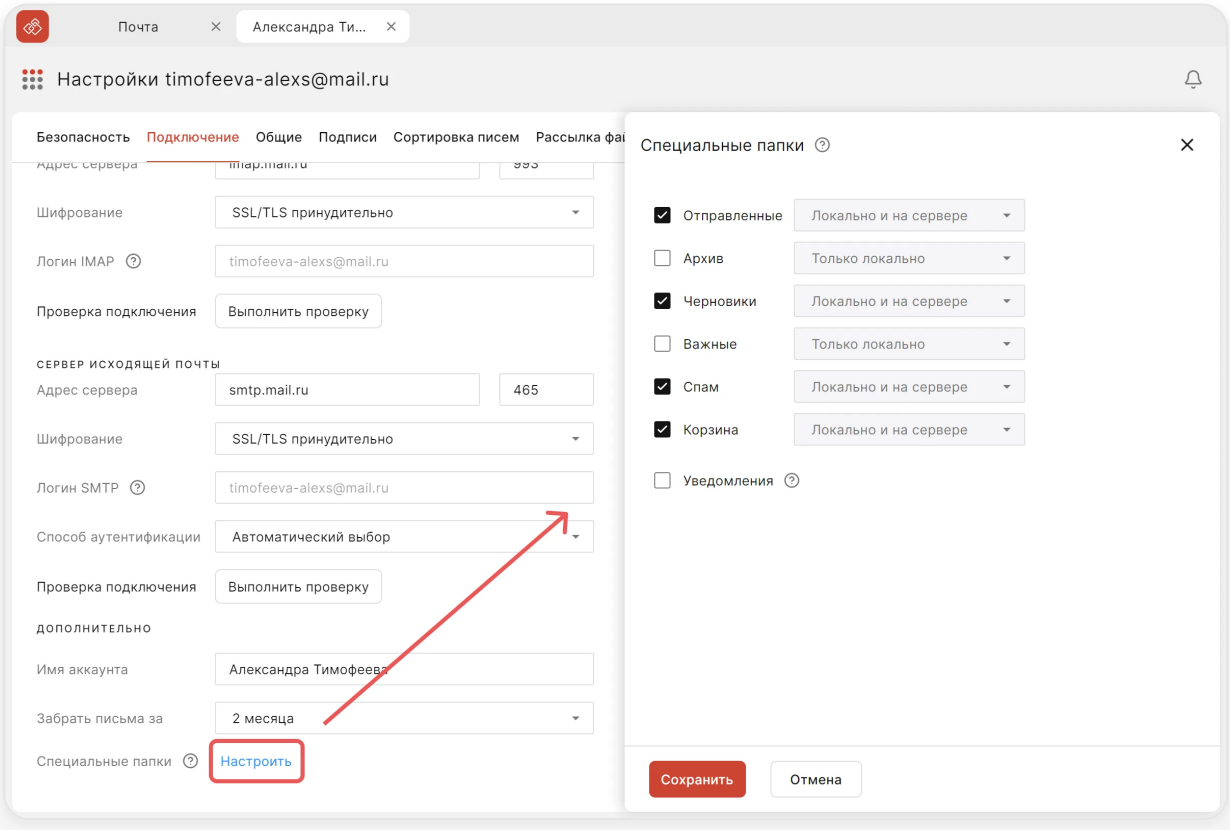
Тип создания	Описание	Протоколы
Локально	Хранится только на устройстве	Доступно для всех протоколов
Локально и на сервере	Синхронизируется с почтовым сервером	Только для IMAP

> 💡 Письма, которые вы поместите в локальную папку, будут удалены с сервера и сохранены на вашем устройстве.

Включение специальной папки

Чтобы включить специальную папку:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Подключение**.
3. В блоке **Специальные папки** нажмите на кнопку **Настроить**.
4. В открывшемся окне отметьте флажками нужные вам специальные папки и выберите тип создания для каждой из них.



5. Нажмите кнопку **Сохранить**.

Указанные папки будут добавлены в почтовом аккаунте.

> 💡 Чтобы отключить специальные папки, снимите их флажки и сохраните изменения.

Общие настройки

Группировка в цепочки

> 📌 **Группировка писем** — это отличный способ сделать переписку более организованной. Все письма, касающиеся одной темы и связанные с одними и теми же участниками, будут собраны на одной странице. В папках эти письма также будут отображаться в виде единой строки. Рядом с темой каждого письма будет указана цифра, которая показывает общее количество писем в данной группе.

Чтобы включить или выключить группировку писем в цепочки:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Общие**.
3. Включите или выключите переключатель **Группировать письма в цепочки**.

Настройки применяются автоматически без дополнительного подтверждения.

Автоматическое прочтение при просмотре

> 📌 По умолчанию при быстром просмотре (в области справа от списка писем) письмо помечается как прочитанное.

Чтобы включить или выключить автоматическое прочтение письма при быстром просмотре:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Общие**.
3. Включите или отключите переключатель **Отмечать как прочитанное при просмотре в области чтения**.

Настройки применяются автоматически без дополнительного подтверждения.

Запрос уведомлений о прочтении и доставке для исходящих писем

Уведомление о доставке подтверждает факт доставки сообщения, но не гарантирует его просмотр или прочтение получателем.

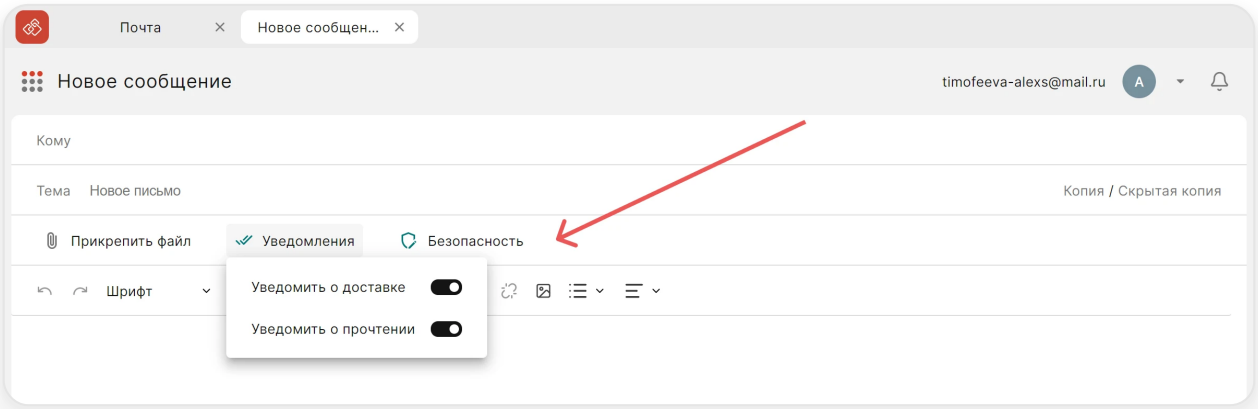
Запрос уведомления о прочтении позволяет узнать, было ли письмо открыто, — подтверждение приходит отдельным сообщением.

Чтобы настроить запрос уведомлений для исходящих писем:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Общие**.
3. Включите или выключите переключатели:
    - **Запрашивать уведомление о доставке для всех исходящих сообщений**.
    - **Запрашивать уведомление о прочтении для всех исходящих сообщений**.

Настройки применяются автоматически без дополнительного подтверждения.

При открытии формы с новым письмом переключатели будут выставлены в соответствии с указанными настройками.



> ⚠️ **Важно понимать**:
>
> - Некоторые почтовые системы отправляют уведомления автоматически.
> - Получатель может отключить подтверждения прочтения.
> - Уведомление может прийти при автоматической пометке письма как прочитанного

Фильтрация уведомлений о доставке и прочтении исходящих писем

Для удобной организации почты вы можете настроить автоматическое перемещение служебных уведомлений в специальную папку **Уведомления**.

Существует два способа настройки фильтрации:

- **Способ 1**: Через настройки подключения.

  Включите специальную папку **Уведомления** в настройках подключения аккаунта.

- **Способ 2**: Через общие настройки:

  1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
  2. Перейдите на вкладку **Общие**.
  3. Включите переключатель **Скрывать уведомления** в блоке **Запрос уведомлений**.

Настройки применяются автоматически без дополнительного подтверждения.

Что происходит после активации:

- В вашем аккаунте автоматически создаётся специальная папка **Уведомления**,
- Все письма, содержащие уведомления о доставке и прочтении писем будут фильтроваться в эту папку.

Чтобы отключить автоматическую фильтрацию, выполните одно из следующих действий:

- Деактивируйте переключатель **Скрывать уведомления** в настройках,
- Отключите специальную папку **Уведомления** в настройках подключения.

После отключения все уведомления будут снова поступать в папку **Входящие**.

Отправка уведомлений о прочтении входящих писем

Чтобы настроить отправку уведомлений о прочтении для входящих писем:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Общие**.
3. Включите или отключите переключатели:
   - ✅ **Всегда отправлять уведомления о прочтении для любого полученного сообщения** — для автоматического подтверждения о прочтении для всех писем с запросом.
   - ❓ **Каждый раз спрашивать, следует ли отправить уведомление о прочтении** — при чтении письма будет предложено отправить подтверждения о прочтении.
   - ❌ **Никогда не отправлять уведомления о прочтении** — функция подтверждения о прочтении будет отключена в приложении.

Настройки применяются автоматически без дополнительного подтверждения.

Подписи (контактная информация)

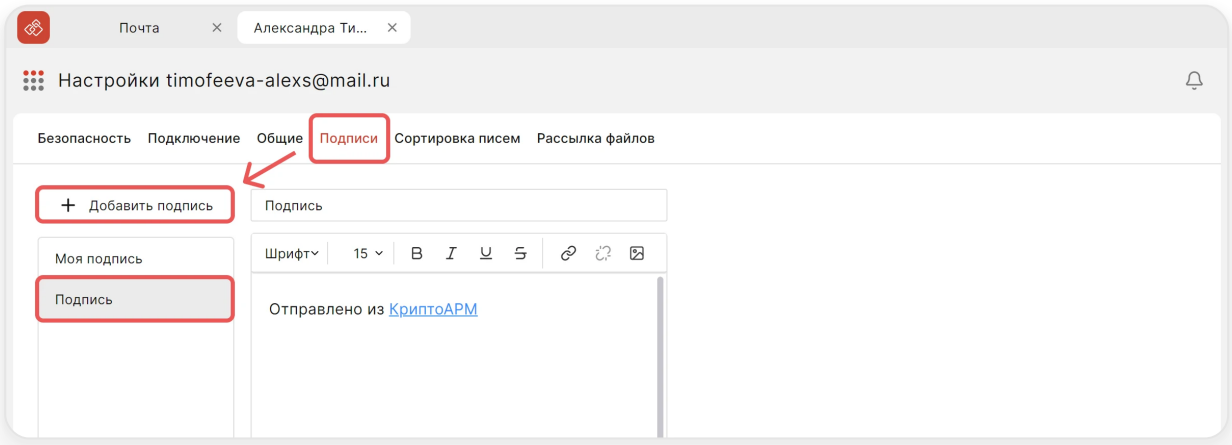
> 📌 **Подпись** - текстовая подпись с контактными данными, которая автоматически добавляться в конец каждого отправляемого письма.

Создание подписи

По умолчанию в приложении задана подпись с текстом **Отправлено из КриптоАРМ** и ссылкой на интернет-магазин cryptoarm.ru.

Чтобы создать новую подпись:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Подписи**.
3. Нажмите **Добавить подпись**.



4. Укажите название подписи.
5. Добавьте содержимое подписи:
   - Настройте стиль и размер шрифта.
   - Добавьте изображение. Формат изображения: `.jpeg`, `.jpg`, `.webp`, `.gif`, максимальный размер — 1024x1024 пикселей, максимальный объем: 2 МБ.
   - Добавьте ссылку. Для добавления ссылки выделите текст, нажмите кнопку **Вставить ссылку**, в появившемся окне укажите адрес ссылки. Вы можете удалить ссылку из подписи, выделив текст и нажав кнопку **Удалить ссылку**.
6. При необходимости установите флаги:
   - **По умолчанию** — подпись будет использоваться по умолчанию во всех исходящих сообщениях.

- **Добавлять перед цитируемым текстом в ответных письмах** — подпись будет добавляться сразу после текста ответа, а не в конце всех писем в цепочке.

Настройки подписи применяются автоматически без дополнительного подтверждения.

Установка подписи по умолчанию

Чтобы установить подпись по умолчанию:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Подписи**.
3. Выберите подпись, которую необходимо установить в качестве подписи по умолчанию.
4. Установите флажок **По умолчанию**.

Теперь выбранная подпись будет использоваться по умолчанию во всех исходящих сообщениях

Удаление подписи

Чтобы удалить подпись из приложения:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Подписи**.
3. Наведите курсор мыши на название подписи и нажмите на всплывающую кнопку **Удалить** .

Подпись будет удалена автоматически без дополнительного подтверждения.

Смотрите также

- Подключение почтового аккаунта — настройка и управление почтовыми аккаунтами в КриптоАРМ.
- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как создать новое письмо в КриптоАРМ

Узнайте, как создавать письма в КриптоАРМ: добавлять получателей, прикреплять файлы, подписывать и шифровать сообщения, а также получать уведомления о доставке и прочтении.

Содержание:

- Открытие формы с сообщением
- Получатели и отправитель
- Оформление сообщения
- Настройка подписи (контактной информации)
- Добавление вложений
- Уведомления о доставке и прочтении
- Подпись и шифрование
- Отправка письма
- Возможные ошибки
- Смотрите также

Открытие формы с сообщением

Чтобы создать новое письмо:

1. Перейдите в раздел **Почта**.
2. Нажмите на кнопку **Новое сообщение** на панели действий.
3. Откроется вкладка с новым письмом.

> 💡 Все неотправленные письма автоматически сохраняются в папке **Черновики**. Чтобы продолжить работу с черновиком, просто откройте его.

Получатели и отправитель

Настройка получателей

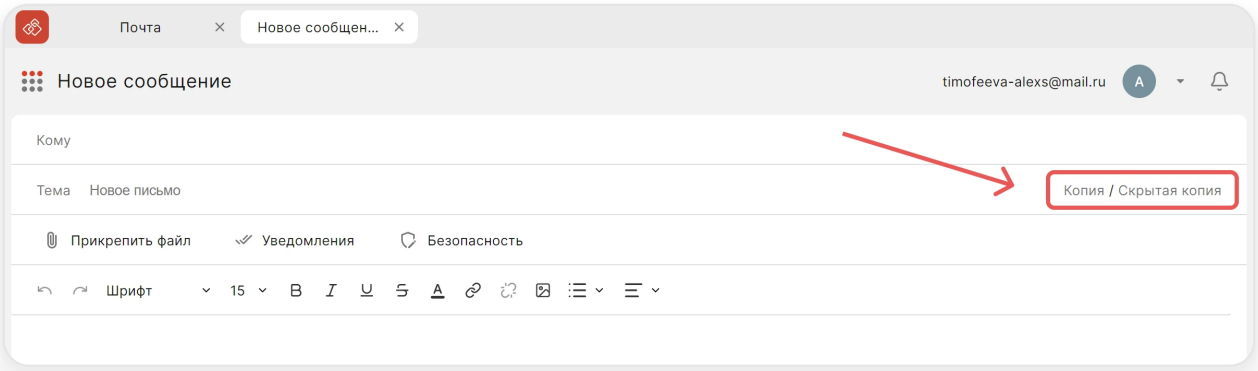
При открытии окна с новым письмом появляется поле **Кому**.

Чтобы активировать поля **Копия** и **Скрытая копия**, просто нажмите на соответствующие кнопки, расположенные на панели **Тема**.

Назначение полей:

- Поле **Кому** — для добавления основных получателей,
- Поле **Копия** — для добавления получателей, которые должны видеть сообщение,
- Поле **Скрытая копия** — для добавления получателей, чьи адреса не будут видны другим получателям.

Вы можете добавить одного или нескольких получателей в каждое поле.



Ввод получателей вручную

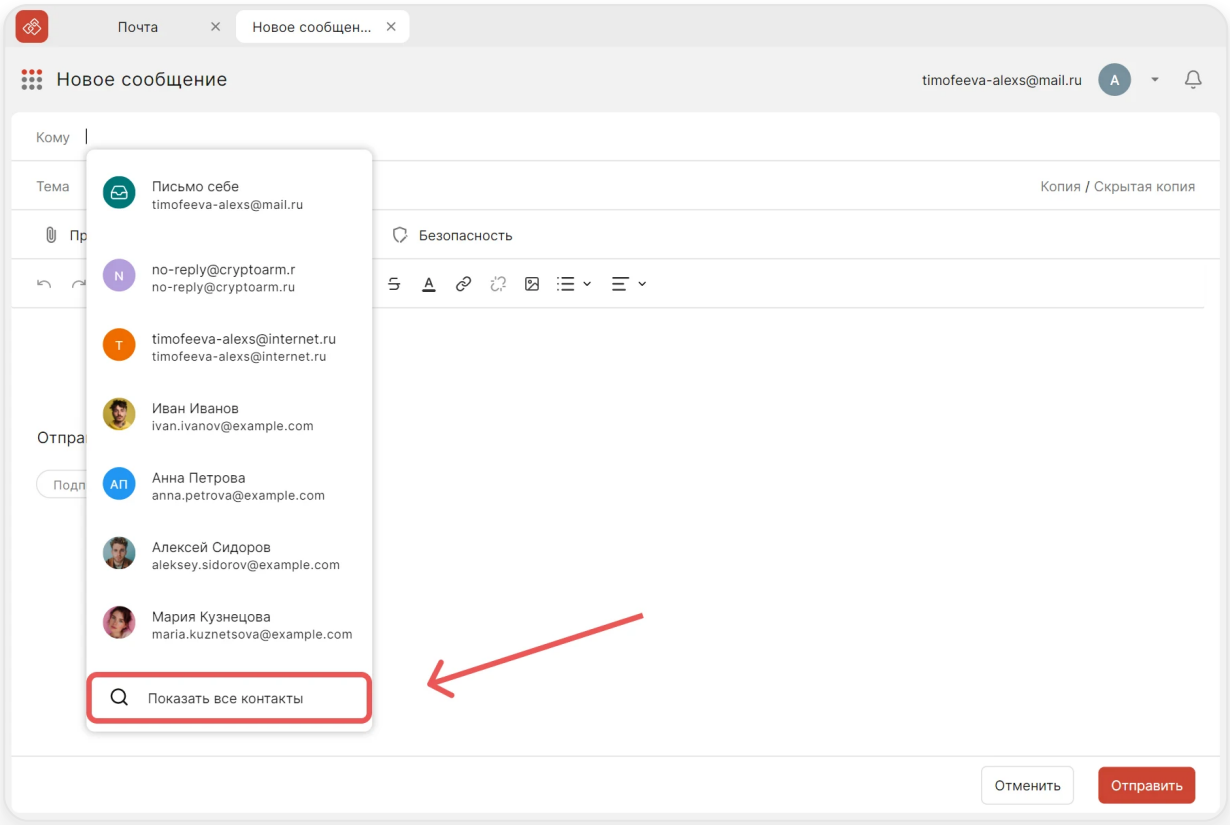
1. Установите курсор в поле **Кому**, **Копия** или **Скрытая копия**.
2. Введите электронные адреса получателей через запятую, точку с запятой или пробел.

> 💡 **Совет**: Некорректные адреса подсвечиваются красным. Для быстрого исправления ошибки в адресе можно дважды кликнуть по нему и отредактировать.

Выбор из адресной книги

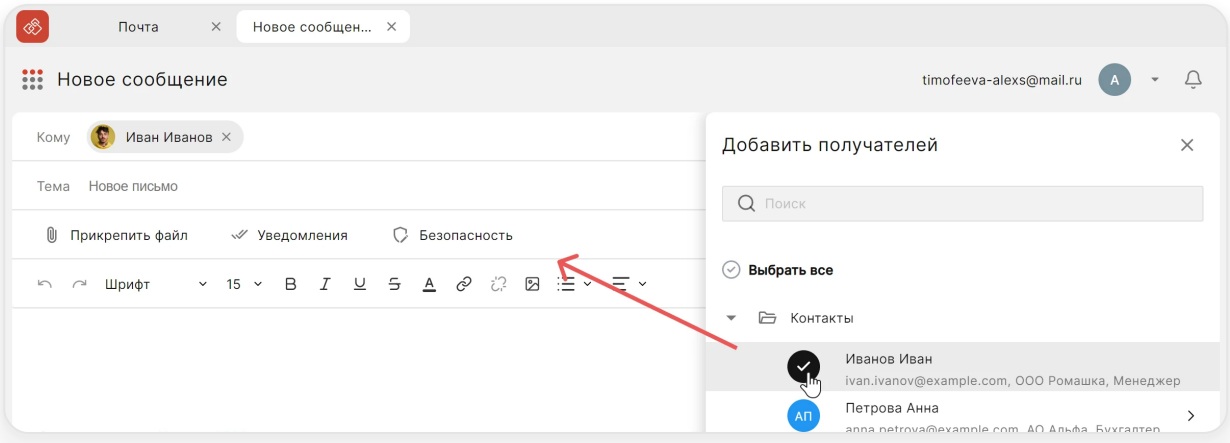
Чтобы выбрать получателей, сохраненных в разделе **Контакты**:

1. Установите курсор в поле **Кому**, **Копия** или **Скрытая копия**.
2. В появившемся меню выберите действие **Показать все контакты**.



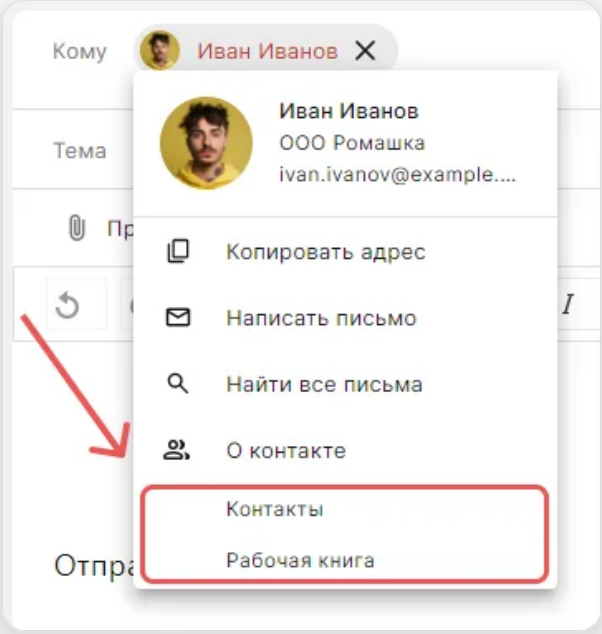
3. Откроется окно со списком адресных книг с контактами. В списке отображаются только контакты с указанными email-адресами. При необходимости можно просмотреть сведения о контакте по кнопке .

4. Выберите один или несколько контактов. Для выбора контакта нажмите на его аватар.



Выбранные контакты автоматически помещаются в соответствующее поле письма.

💡 **Совет**: Если один и тот же контакт присутствует в нескольких адресных книгах, то после выбора получателя отображаются все книги, в которых он найден.



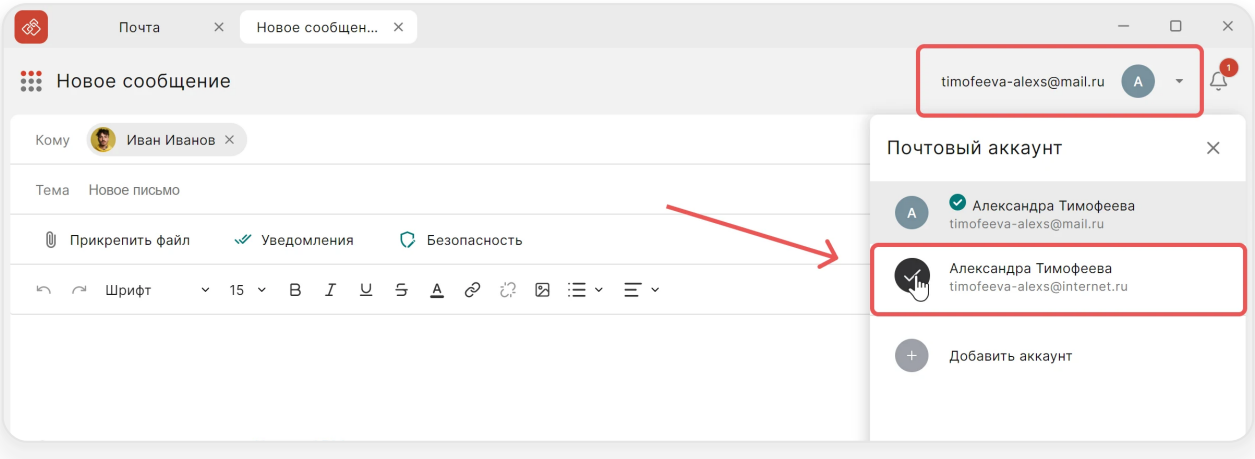
Удаление получателя

Чтобы удалить получателя из поля **Кому**, **Копия** или **Скрытая копия**, нажмите на кнопку **Удалить** ✕, размещенную рядом с адресом.

Настройка отправителя

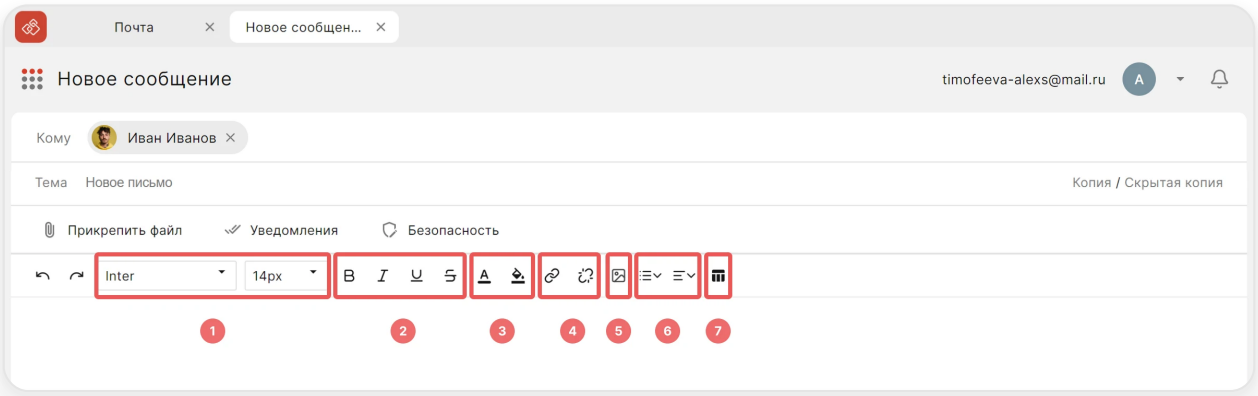
По умолчанию письмо отправляется с активного аккаунта.

Если в приложении добавлено несколько почтовых ящиков, вы можете выбрать тот, который будет использоваться для отправки. Для этого нажмите на имя активного аккаунта в верхнем правом углу и выберите нужный аккаунт в появившемся окне.



Оформление сообщения

Редактор сообщений поддерживает форматирование текста, создание и вставку таблиц, добавление ссылок и изображений, а также работу со списками и выравниванием.



1. Выбор стиля и размера шрифта

Чтобы настроить стиль и размер шрифта:

1. Выделите текст письма.
2. На панели действий нажмите на кнопку **Шрифт** и выберите из выпадающего списка необходимый стиль (Arial, Times New Roman, Verdana и другие).
3. Нажмите на кнопку с размером шрифта и выберите из выпадающего списка необходимый размер (от 8pt до 96pt).

2. Выделение текста

Чтобы настроить выделение текста:

1. Выделите текст письма.
2. Выберите необходимый вариант для настройки выделения на панели действий:
   - **Жирный**
   - Курсив
   - Подчёркнутый
   - ~~Зачёркнутый~~

3. Изменение цвета текста и фона

Чтобы настроить цвета текста и фон:

1. Выделите текст письма.
2. Нажмите на кнопку **Выбор цвета** на панели действий.
3. Выберите нужный цвет текста и фона в появившемся окне.

4. Вставка ссылки

Чтобы добавить гиперссылку:

1. Выделите текст письма.
2. Нажмите кнопку **Вставить ссылку**, в появившемся окне укажите адрес ссылки и нажмите **Добавить**. Вы можете удалить ссылку из подписи, выделив текст и нажав кнопку **Удалить ссылку**.

5. Добавление изображения

Чтобы добавить изображение в тело письмо:

1. Установите курсор в то место в тексте письма, куда хотите вставить изображение.
2. Нажмите на кнопку **Вставить изображение** на панели действий.
3. В появившемся окне выберите файл с компьютера с помощью кнопки **Выбрать путь** или вставьте URL. При необходимости настройте ширину и высоту изображение в пикселях.

> 💡 Некоторые почтовые клиенты блокируют загрузку внешних изображений.

6. Вставка списков и выравнивание

Редактор сообщений позволяет создавать маркированные и нумерованные списки, изменять уровень вложенности, а также выравнивать текст в письме.

Чтобы добавить список или отступ:

1. Выделите текст письма или начните новый абзац.
2. Нажмите на кнопку **Список** или **Выравнивание текста**.
3. Выберите необходимое действие.

7. Вставка таблицы

В редакторе нового письма можно создавать таблицы непосредственно в письме или вставлять готовые таблицы из буфера обмена.

Создание таблицы

Чтобы создать таблицу:

1. Установите курсор в то место письма, куда необходимо добавить таблицу.
2. Нажмите кнопку **Вставить таблицу** на панели действий.
3. Выберите необходимое количество строк и столбцов.
4. После вставки заполните ячейки таблицы.

Вставка таблицы из буфера обмена

Чтобы вставить готовую таблицу:

1. Скопируйте таблицу в поддерживаемом приложении.
2. Установите курсор в то место письма, куда необходимо добавить таблицу.
3. Нажмите **Ctrl+V** или воспользуйтесь командой **Вставить**.

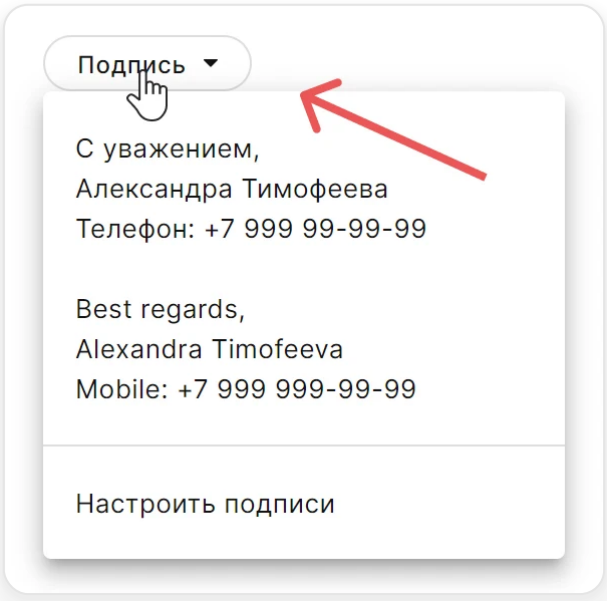
Таблица будет вставлена в письмо с сохранением структуры строк и столбцов. После вставки содержимое таблицы можно редактировать средствами редактора сообщений.

Настройка подписи (контактной информации)

По умолчанию в приложении задана подпись с текстовкой **Отправлено из КриптоАРМ** и ссылкой на магазин cryptoarm.ru. Подробнее про подписи читайте в инструкции Подпись писем.

Если у вас одна подпись, то она автоматически добавляется при создании сообщения.

Если у вас несколько подписей, то вы можете выбрать нужную подпись с помощью кнопки **Подпись**.



При выборе **Настроить подписи** открывается новая вкладка с настройками почты, где вы можете редактировать подписи.

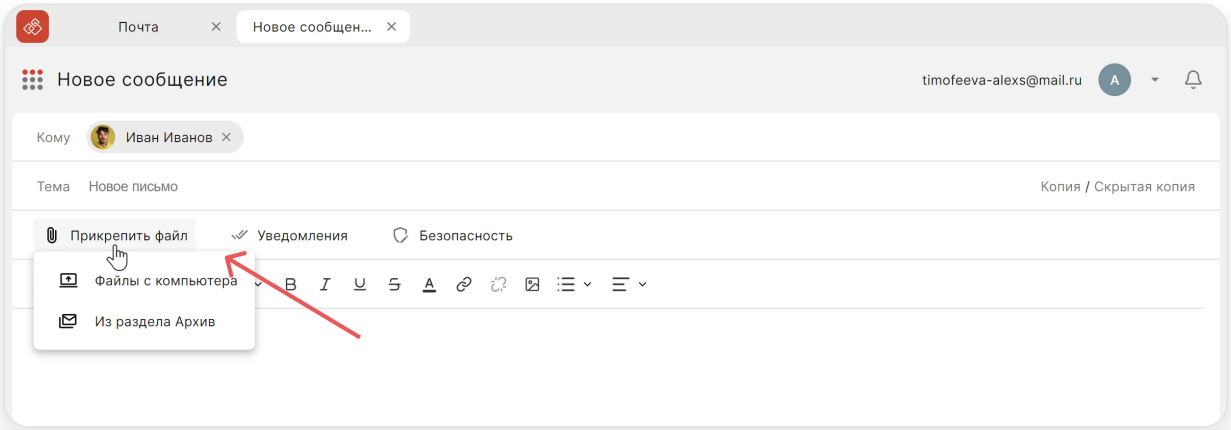
Добавление вложений

> 💡 Максимальный размер вложений зависит от почтовых сервисов отправителя и получателя. Даже если ваш сервер поддерживает большие файлы, они могут быть отклонены сервером получателя.

Добавление вложений с компьютера

Чтобы добавить вложение:

1. Нажмите кнопку **Прикрепить файл**.
2. В появившемся меню выберите **Файлы с компьютера**.



3. Выберите файлы в появившемся окне файлового менеджера.

После выбора файлы отобразятся в письме.

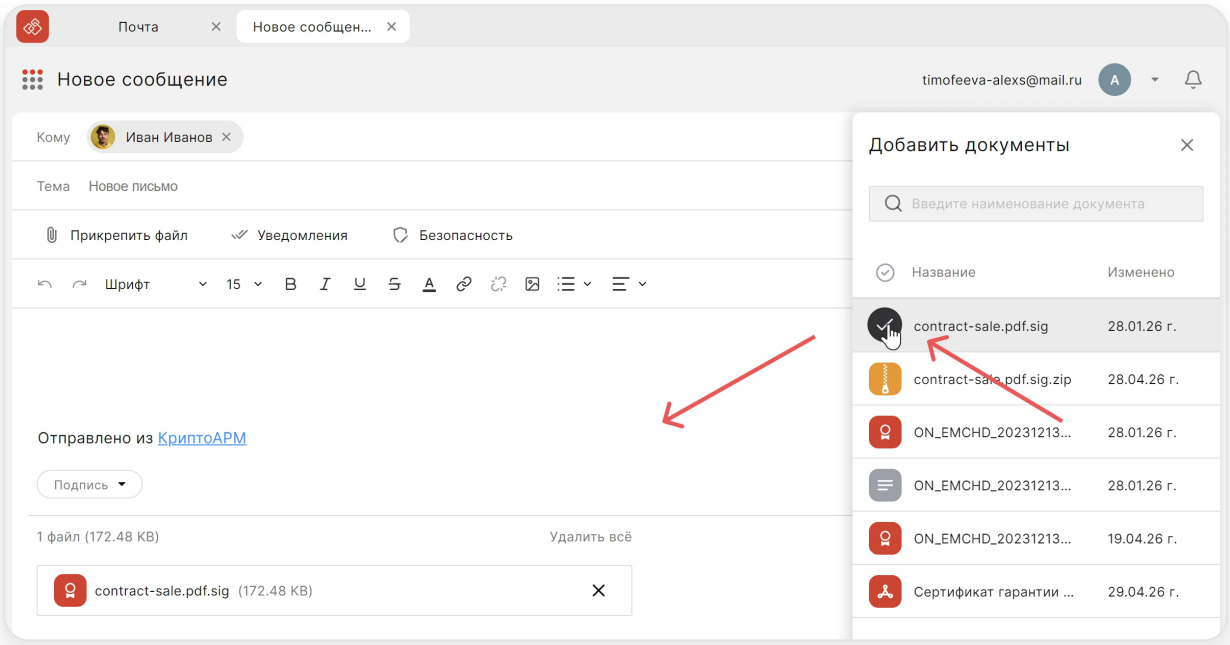
Добавить файлы можно, перетащив их в область создания сообщения. Если перетащить папку с документами, то файлы добавляются списком.

Добавление вложений из «Архива»

> 💡 **Архив** - архивная папка с файлами, созданная в разделе **Документы**.

Чтобы добавить вложение из Архива:

1. Нажмите кнопку **Прикрепить файл**.
2. В появившемся меню выберите действие **Из раздела Архив**.
3. Откроется окно со списком файлов, сохраненных в папке.



4. Отметьте флажком файлы, которые необходимо добавить к письму. При необходимости воспользуйтесь поиском.

После выбора файлы отобразятся в письме.

Удаление вложений

Для удаления ошибочно добавленного вложения нажмите кнопку **Удалить** ✕, размещенную на панели с файлом.

Для удаления всех вложений нажмите **Удалить все**.

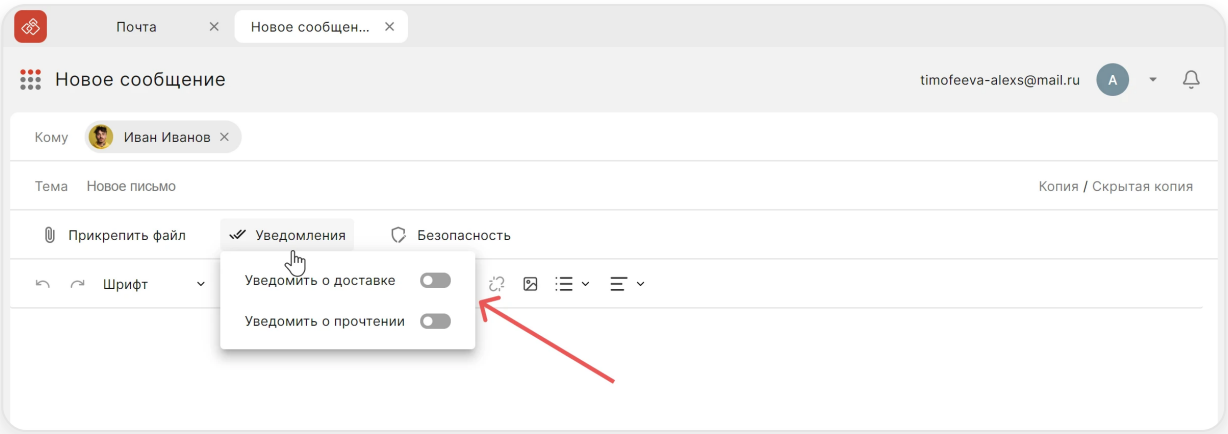
Просмотр вложения

Чтобы просмотреть содержимое добавленного документа, просто нажмите на него. Это действие позволит открыть документ в приложении, которое ассоциируется с его расширением.

Уведомления о доставке и прочтении

Чтобы запросить уведомления для исходящего письма:

1. Нажмите кнопку **Уведомления**.
2. Включите необходимые опции:
   - **Уведомить о доставке** — подтверждает доставку письма в почтовый ящик получателя.
   - **Уведомить о прочтении** — позволяет получить подтверждение о прочтении письма с указанием даты и времени.



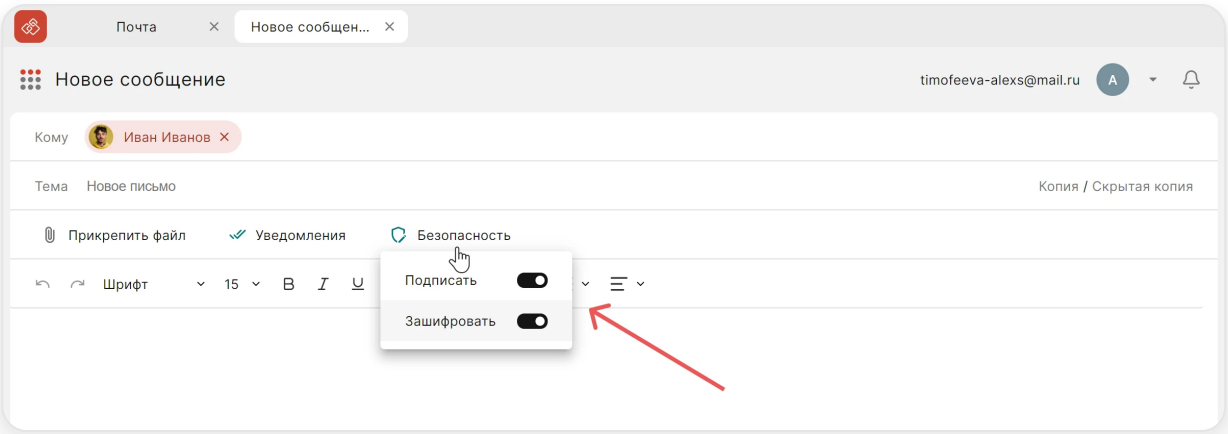
Уведомление о доставке подтверждает факт доставки сообщения, но не гарантирует его просмотр или прочтение получателем.

Запрос уведомления о прочтении позволяет узнать, было ли письмо открыто, — подтверждение приходит отдельным сообщением.

> 💡 **Совет**:
>
> - Настройте автоматическую сортировку писем с уведомлениями в отдельную папку для удобства отслеживания.
> - При необходимости включите отправку уведомлений по умолчанию в настройках почтового аккаунта.

Подпись и шифрование

1. Нажмите кнопку **Безопасность**.
2. Включите необходимые опции:
    - **Подписать** — для отправки подписанного письма,
    - **Зашифровать** — для отправки зашифрованного письма.



> 💡 **Совет**: При необходимости включите отправку подписанных и зашифрованных писем по умолчанию в настройках почтового аккаунта .

Отправка письма

Чтобы отправить готовое письмо:

1. Проверьте содержимое письма и список получателей.
2. Убедитесь в корректности выбранных настроек.
3. Нажмите кнопку **Отправить**.

При отправке подписанных и (или) зашифрованных писем потребуется подтверждение отправки в отдельном окне.

- Нажмите **Продолжить** в окне подтверждения.

  При этом вы подтверждаете, что ознакомились с данными, которые будут подписаны и/или зашифрованы.

- При необходимости введите пароль контейнера или PIN-код закрытого ключа сертификата.

Дождитесь завершения отправки письма.

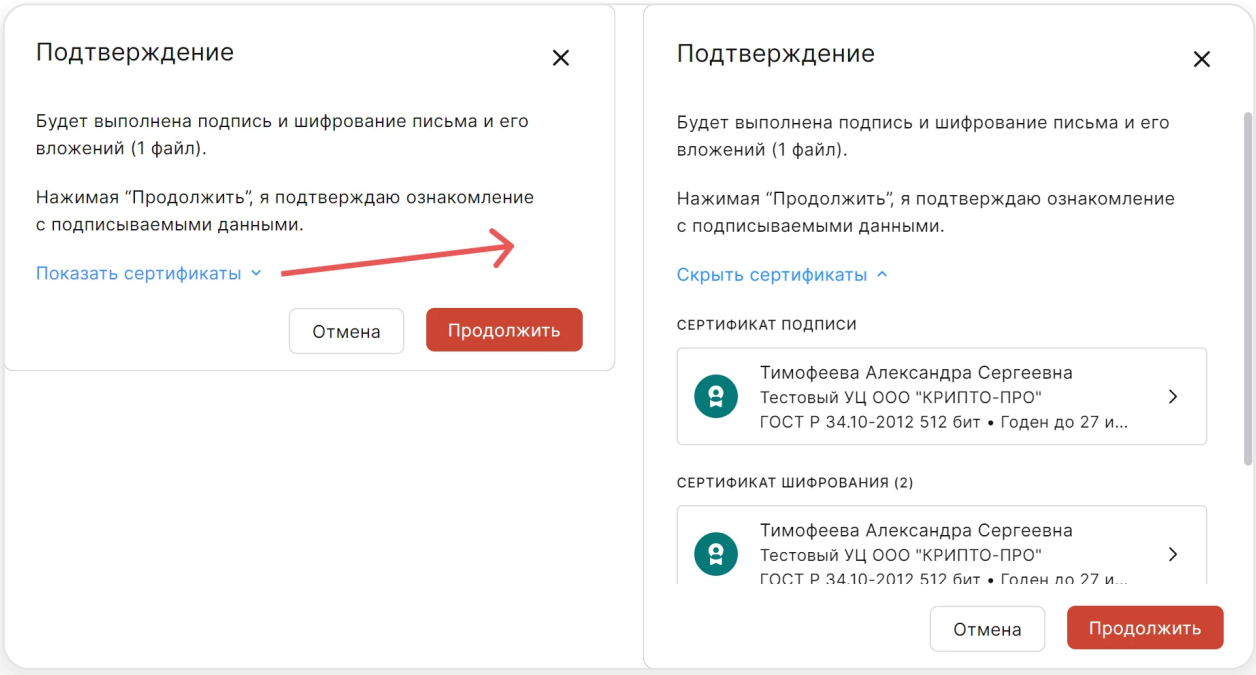
Отправленное письмо автоматически сохраняется в папке **Отправленные**.

Подтверждение отправки писем с подписью и шифрованием

При отправке письма с включённой электронной подписью и (или) шифрованием отображается окно **Подтверждение**.

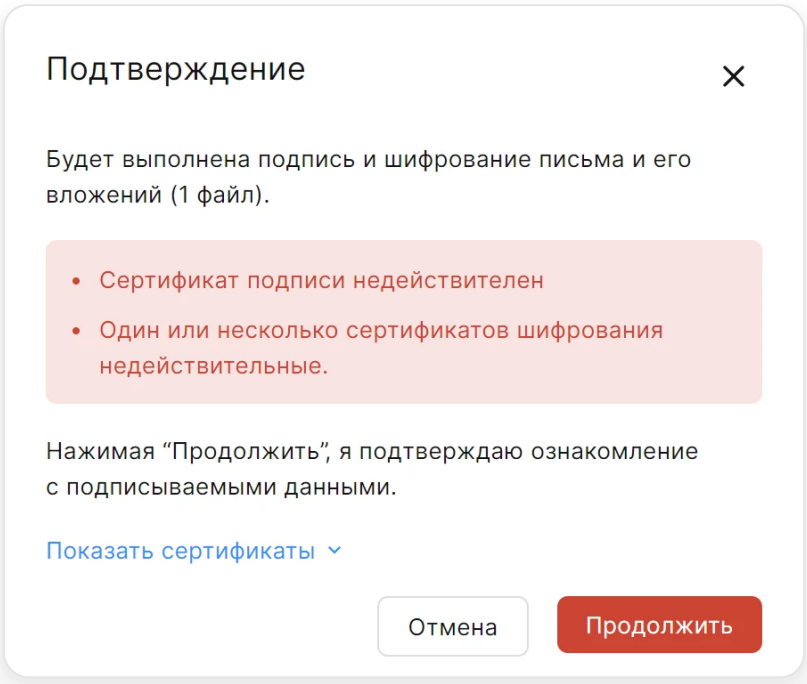
В этом окне отображается информация о выполняемых операциях, а также о сертификатах, используемых для подписи и шифрования.

> 💡 **Совет**: Чтобы просмотреть информацию о сертификате подписи, нажмите на кнопку **Показать сертификат**, затем выберите нужный сертификат в открывшейся панели.



Недействительные сертификаты

Если сертификат подписи или сертификаты шифрования окажутся недействительными, в окне появится соответствующее уведомление:

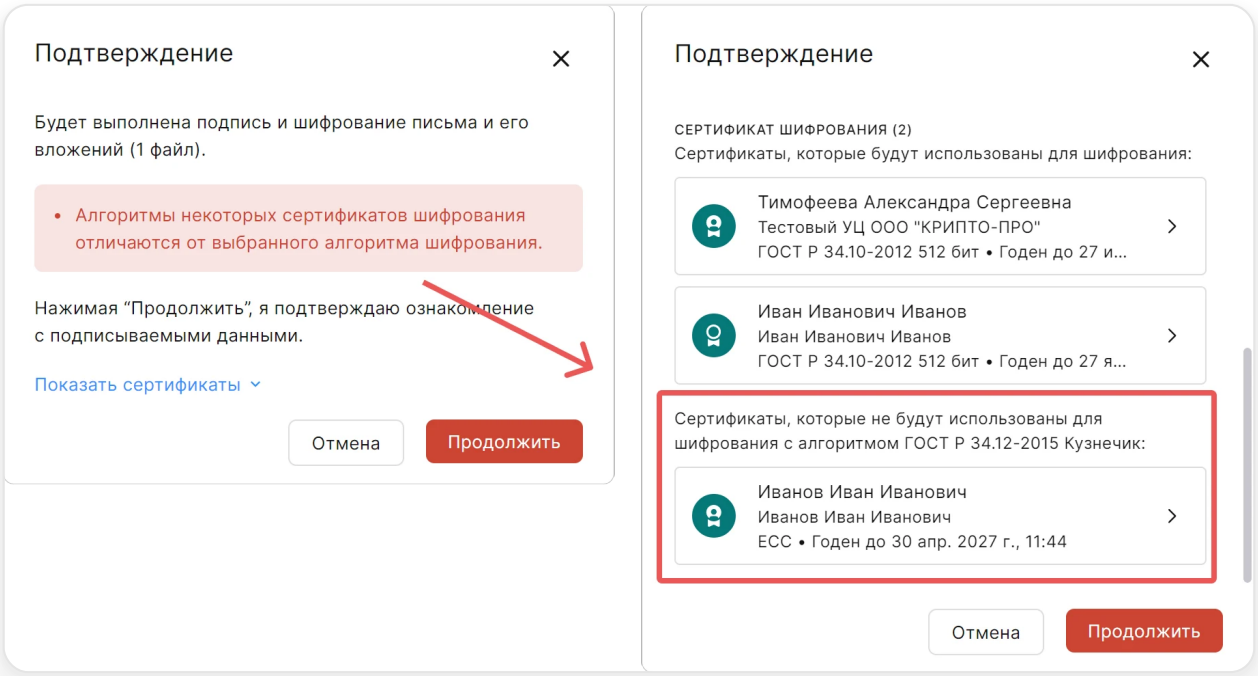


В такой ситуации отправка письма не будет заблокирована, однако следует учесть, что получатель может не принять такое письмо.

Несоответствие алгоритмов шифрования

В случае, если алгоритмы шифрования сертификатов контактов не будут соответствовать настроенному алгоритму шифрования, письмо будет зашифровано в адрес тех сертификатов, которые поддерживают выбранный алгоритм.

В окне подтверждения при этом отобразится уведомление и список используемых сертификатов шифрования:



Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при отправке писем:

Ошибки адресатов

Ошибка	Рекомендуемые действия	Дополнительная информация
Укажите получателей письма в полях Кому, Копия или Скрытая копия	Проверьте заполнение полей	Обязательно должен быть указан хотя бы один получатель в поле "Кому"
	1. Проверьте правильность написания адресов 2. Убедитесь, что адреса	Пример корректного формата: username@domain.ru

Ошибка	Рекомендуемые действия	Дополнительная информация
Адреса user@aa не распознаны. Проверьте правильность ввода адресов	разделены запятыми или точками с запятой 3. Удалите некорректные адреса	

Ошибки подключения

Ошибка	Рекомендуемые действия	Дополнительная информация
Не удалось отправить сообщение	1. Проверьте подключение к Интернету 2. Попробуйте отправить письмо позже 3. Перезагрузите приложение	Может возникать при временных проблемах с соединением
Ошибка соединения	1. Проверьте настройки SMTP-сервера исходящей почты 2. Убедитесь в правильности порта и типа шифрования 3. Проверьте логин и пароль для отправки почты	Настройки можно найти в настройках подключения почтового аккаунта

Ошибки уведомлений

Ошибка	Рекомендуемые действия	Дополнительная информация
Ошибка при отправке (для писем с уведомлениями)	1. Проверьте настройки уведомлений о доставке/прочтении 2. Убедитесь, что почтовые серверы получателей поддерживают уведомления о доставке 3. Попробуйте отключить запрос уведомлений	Некоторые почтовые сервисы не поддерживают стандартные уведомления

Ошибки сертификатов

Ошибка	Рекомендуемые действия	Дополнительная информация
Для подписи письма выберите сертификат в настройках аккаунта и повторите отправку	Сертификат подписи не выбран в настройках аккаунта	1. Выберите сертификат в настройках почтового аккаунта 2. Повторите отправку
Один или несколько сертификатов отсутствуют. Проверьте наличие сертификатов у получателей.	Отсутствуют сертификаты шифрования у одного или нескольких адресатов	1. Проверьте наличие сертификатов у получателей 2. Добавьте сертификаты к контактам 3. Повторите отправку

Лицензии и криптопровайдеры

Ошибка	Рекомендуемые действия	Дополнительная информация
Отсутствует необходимый криптопровайдер. Алгоритм открытого ключа сертификата: ГОСТ Р 34.10-2012 256 бит	Отсутствует криптопровайдер КриптоПро CSP	Установите КриптоПро CSP и перезапустите приложение КриптоАРМ
Отсутствует СКЗИ КриптоПро CSP. Установите дистрибутив с сайта cryptopro.ru и повторите попытку	Отсутствует криптопровайдер КриптоПро CSP	Установите КриптоПро CSP и перезапустите приложение КриптоАРМ
Для операций подписи и расшифрования с использованием ГОСТ алгоритмов требуется лицензия на КриптоАРМ	Отсутствует действующая лицензия КриптоАРМ	Приобретите и активируйте лицензию лицензию
Для операций подписи и расшифрования с использованием ГОСТ алгоритмов требуется лицензия на КриптоПро CSP	Отсутствует действующая лицензия КриптоПро CSP	Приобретите и активируйте лицензию

Смотрите также

- Работа с письмами — управление письмами после их отправки и получения.
- Почтовые настройки — настройка параметров почтового ящика.
- Автоматизация почты — сортировка, фильтры и автоматическая обработка писем.

Открыть статью на сайте

Как работать с письмами в КриптоАРМ

Научитесь быстро и удобно работать с письмами в КриптоАРМ: открывать и организовывать сообщения, отвечать и пересылать письма, управлять вложениями, проверять подписи и расшифровывать письма, а также отслеживать уведомления и работать с черновиками.

Содержание:

- Чтение и управление письмами
- Действия с вложениями
- Проверка подписи письма
- Расшифрование письма
- Отправка и получение уведомлений
- Черновики писем
- Поиск писем
- Смотрите также

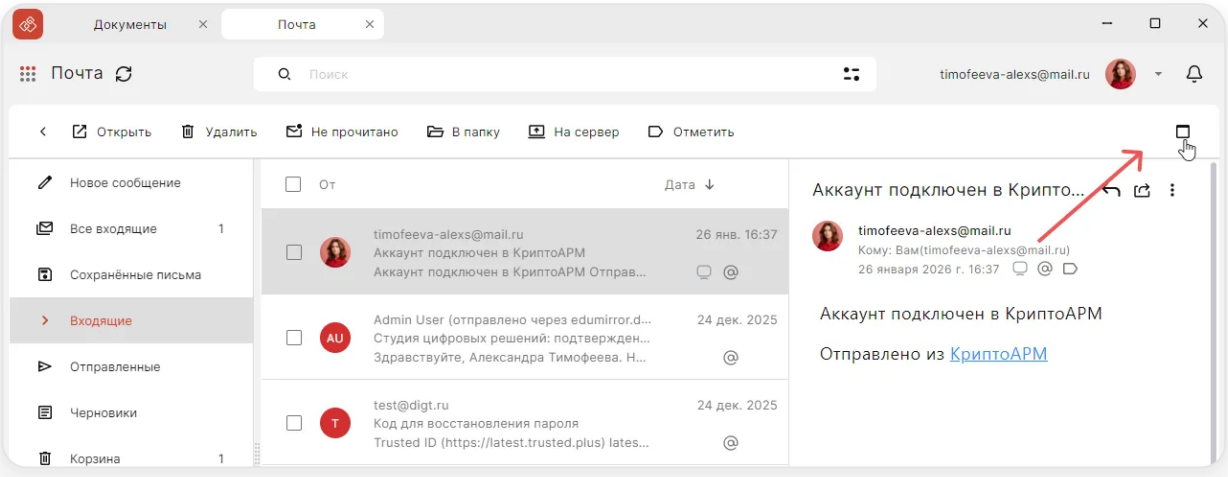
Чтение и управление письмами

Чтение письма

Чтение в области быстрого просмотра

Чтобы открыть письмо в области быстрого просмотра:

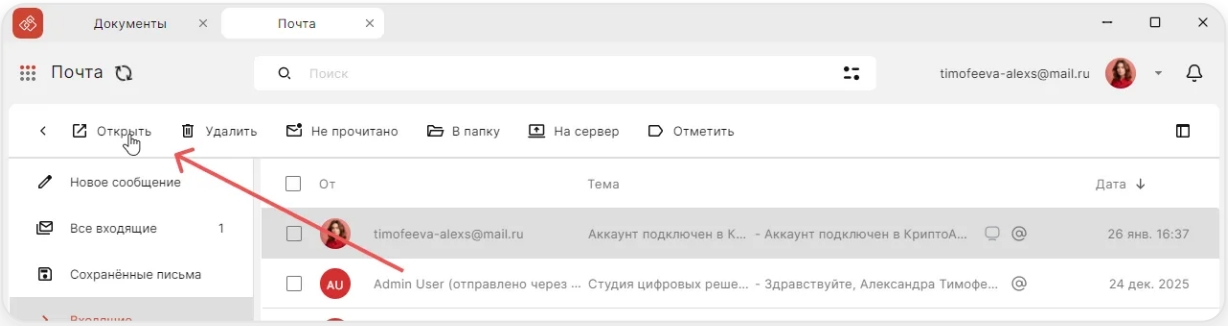
1. Перейдите в раздел **Почта**.
2. Выделите письмо в списке писем.
3. Нажмите иконку **Просмотр** в верхнем правом углу.
4. Справа от списка писем откроется область просмотра письма.



Чтение в новой вкладке

Чтобы открыть письмо в новой вкладке:

1. Перейдите в раздел **Почта**.
2. Выполните действие одним из способов:
   - Выделите письмо в списке писем и нажмите кнопку **Открыть** на панели действий.
   - Дважды кликните по панели с письмом.

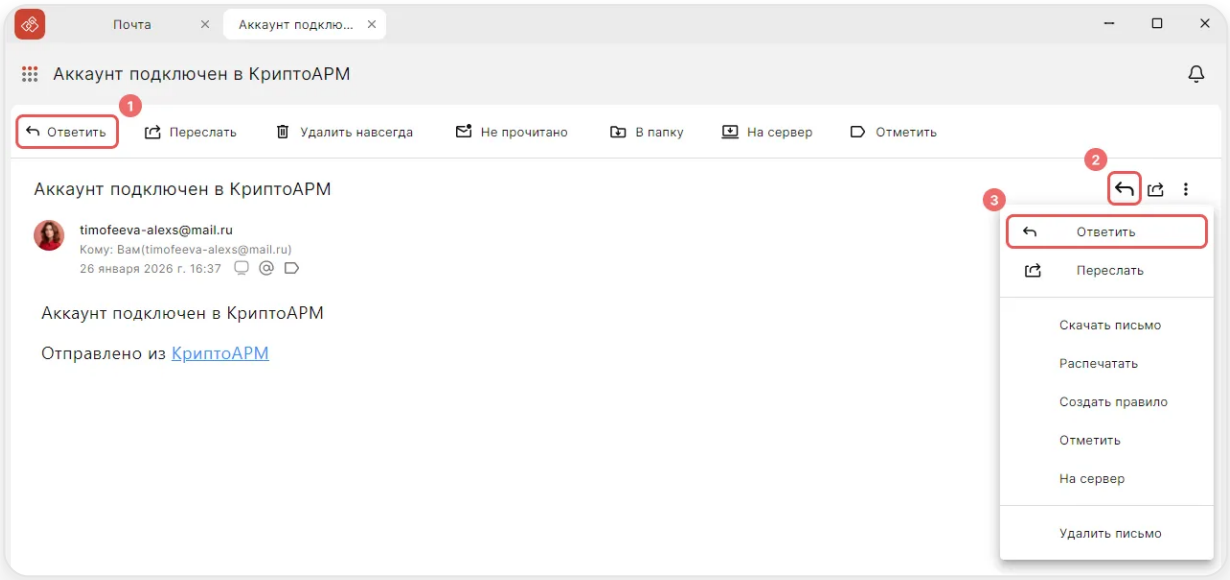


3. Откроется новая вкладка с письмом.

Ответить, Ответить всем, Переслать

Ответить и Ответить всем

1. Перейдите в раздел **Почта**.
2. Откройте письмо, на которое нужно ответить.
3. Нажмите на кнопку **Ответить** или **Ответить всем**:
   - На верхней панели действий,
   - На кнопки ↩ или ↩↩, размещенные справа от темы письма,
   - В меню действий, которое вызывается по кнопке **Еще** ⋮.



4. Откроется окно с новым сообщением.
5. Заполните необходимые поля и отправьте письмо.

Особенности ответа на зашифрованные письма

1. **Автоматическое шифрование ответа**: при ответе на зашифрованное письмо опция **Зашифровать** включается автоматически.
2. **Автоматический поиск нужного сертификата**: для выполнения шифрования письма системе необходим сертификат получателя. Поиск сертификата осуществляется во всех доступных адресных книгах по адресу электронной почты получателя. В результаты поиска включаются все сертификаты, связанные с данным адресом электронной почты.

> ⚠️ **Важно**: Если сертификат не будет найден ни в одном из источников, вы не сможете отправить зашифрованный ответ.

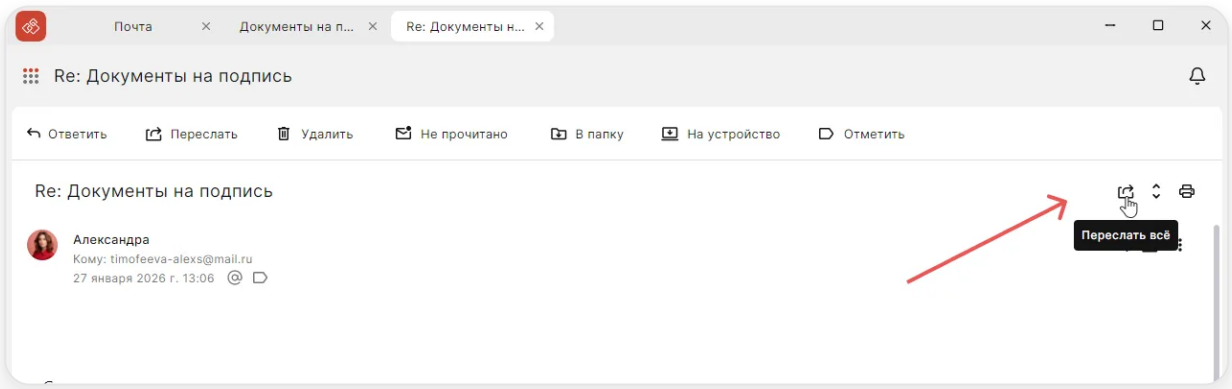
Переслать письмо

1. Перейдите в раздел **Почта**.
2. Откройте письмо, которое нужно переслать.
3. Нажмите на кнопку **Переслать**:
   - На верхней панели действий,
   - На кнопку , размещенную справа от темы письма,
   - В меню действий, которое вызывается по кнопке **Еще** .
4. Откроется окно с новым сообщением.
5. Заполните необходимые поля и отправьте письмо.

Переслать цепочку писем

> 💡 **Совет**: Чтобы письма объединялись в цепочки, активируйте функцию просмотра в виде цепочек.

1. Перейдите в раздел **Почта**.
2. Откройте цепочку, которую нужно переслать.
3. Нажмите на кнопку **Переслать все**, размещенную на панели с темой цепочки.



4. Откроется окно с новым сообщением.
5. Заполните необходимые поля и отправьте письмо.

Отметка «Важно»

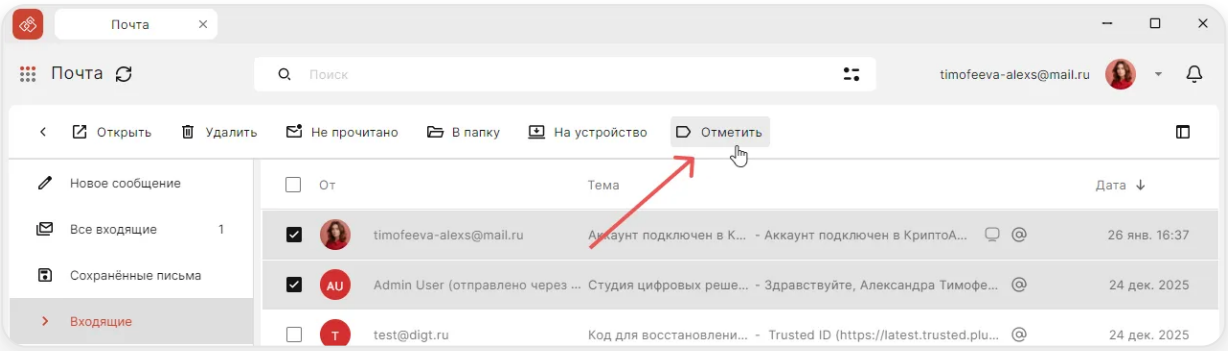
Флаг **Важно** позволяет выделять ключевые сообщения среди общей переписки. Эта функция особенно полезна для отметки срочных писем, выделения важной деловой корреспонденции, организации рабочего процесса с электронной почтой.

> 💡 **Совет**: В расширенном поиске по письмам есть возможность установить фильтр для отметки «Важно».

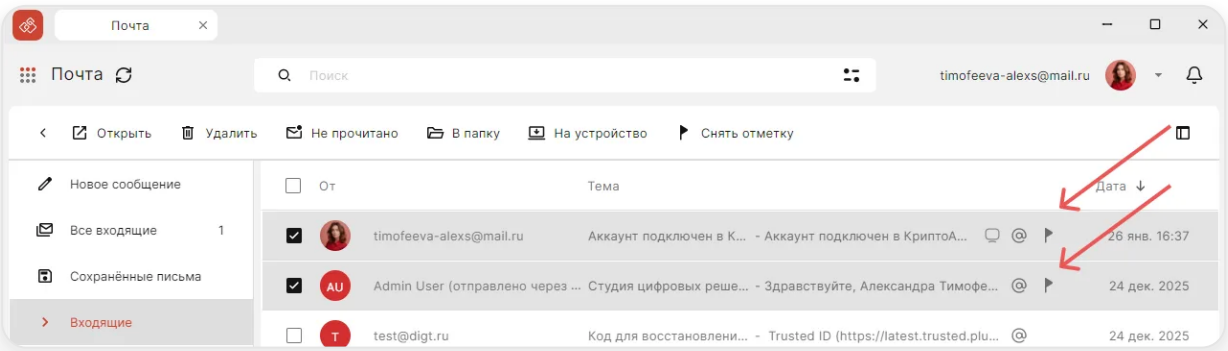
Отметка «Важно» в списке писем

Чтобы отметить письмо флагом «Важно» в списке писем:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **Отметить** на панели действий.



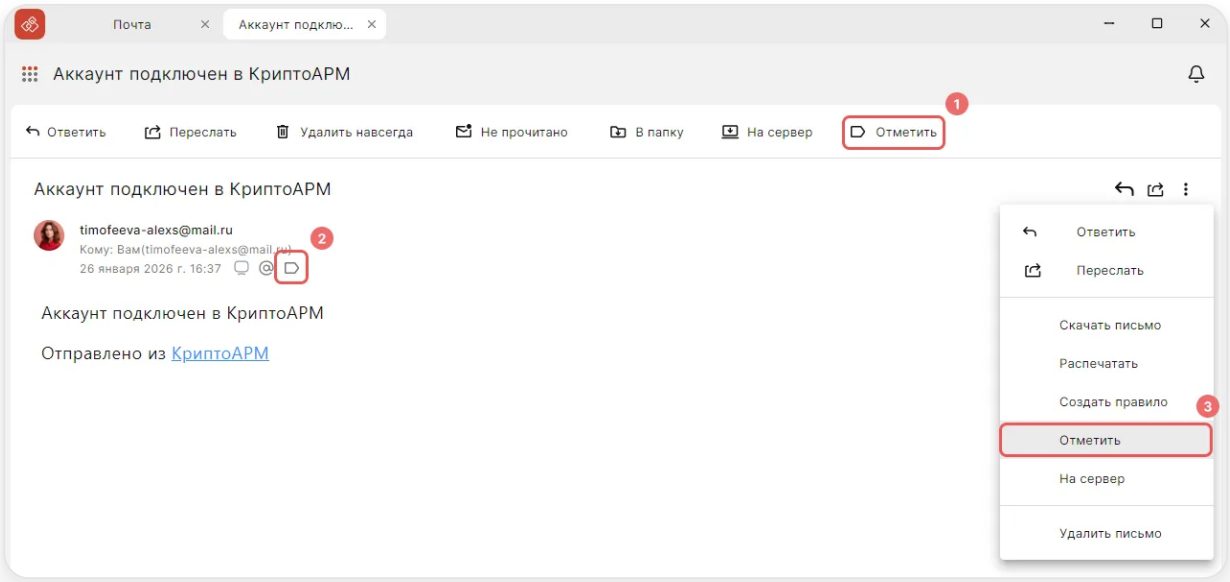
На панели с письмом устанавливается соответствующая отметка. Кнопка **Отметить** меняется на кнопку **Снять отметку**.



Отметка «Важно» при чтении письма

Чтобы отметить письмо флагом «Важно» при чтении письма:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Отметить**:
   - На панели действий,
   - На кнопку , размещенную рядом с темой письма,
   - В меню действий, которое вызывается по кнопке **Еще** .



Удаление отметки «Важно»

Чтобы снять пометку «Важно» с письма в списке, выделите это письмо и нажмите на кнопку **Снять отметку**, расположенную на панели действий.

Чтобы снять отметку «Важно» при чтении письма, нажмите:

- На кнопку **Снять отметку**, расположенную на панели действий,
- На кнопку , размещенную рядом с темой письма,
- На кнопку **Снять отметку**, в меню действий, которое вызывается по кнопке **Еще** .

Отметить письмо как прочитанное или непрочитанное

Отметка в списке писем

Чтобы отметить одно или несколько писем в списке писем:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **Не прочитано** или **Прочитано** на панели действий.

Отметка при чтении письма

Чтобы отметить письмо как прочитанное или непрочитанное при чтении письма:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Не прочитано** или **Прочитано** на панели действий.

Сохранение письма на устройстве

Как работает сохранение писем

В приложении доступно два варианта хранения писем:

1. **Локальное хранение на устройстве**
    - Письма удаляются с сервера после загрузки на устройство,
    - Письма фильтруются в папку **Сохранённые письма** со всех аккаунтов,
    - Письма отмечаются специальным индикатором .
2. **Хранение на сервере**
    - Письма остаются в исходной серверной папке,
    - Доступны со всех устройств,
    - Синхронизируются автоматически.

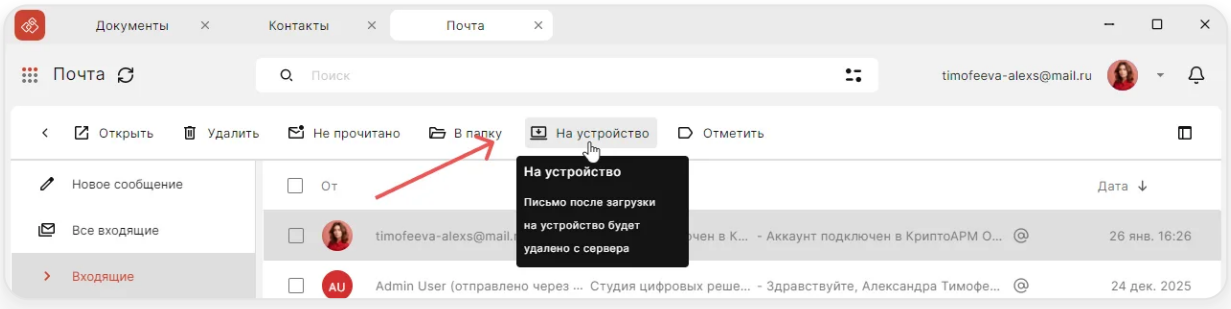
Особенности работы:

- После сохранения письмо доступно в исходной папке и виртуальной папке **Сохранённые письма**,
- Оригинал письма на сервере удаляется,
- Для возврата на сервер требуется активное подключение к почтовому аккаунту,
- Размер локально хранимых писем учитывается в общем объеме данных приложения

Сохранение в списке писем

Чтобы переместить одно или несколько писем с почтового сервера на устройство или наоборот:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку:
    - **На устройство** - для переноса с сервера
    - **На сервер** - для возврата на сервер.



Сохранение при чтении письма

Чтобы переместить письмо с почтового сервера на устройство или наоборот:

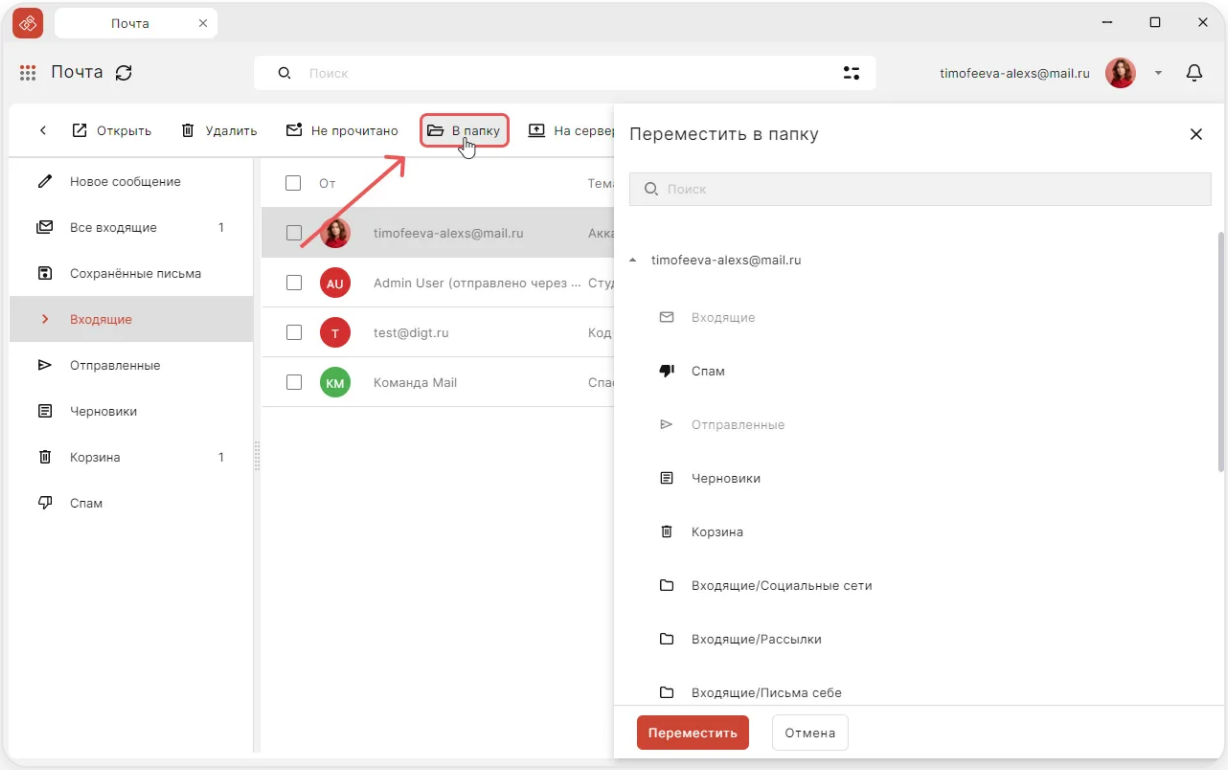
1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Выполните действие одним из способов:
   - Нажмите на кнопку **На устройство**/**На сервер**, размещенную на панели действий,
   - Выберите действие **На устройство**/**На сервер**, в меню действий, которое вызывается по кнопке **Еще** .

Перемещение письма

Перемещение в списке писем

Чтобы переместить одно или несколько писем в списке:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **В папку** на панели действий.
4. Откроется окно **Переместить в папку**.



5. Выберите папку, в которую необходимо переместить письма.
6. Нажмите **Переместить**.

Перемещение при чтении письма

Чтобы переместить письмо на вкладке просмотра:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **В папку**.
4. Откроется окно **Переместить в папку**.
5. Выберите папку, в которую необходимо переместить письмо.
6. Нажмите **Переместить**.

> 💡При перемещении письма в специальную локальную папку:
>
> 1. Письмо удаляется из исходной серверной папки.
> 2. Создаётся локальная копия письма.

Скачивание письма на компьютер

Чтобы скачать письмо на компьютер:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Вызовите меню действий с письмом по кнопке **Еще** ⋮.
4. Выберите действие **Скачать письмо**.
5. Укажите место для сохранения файла с письмом.

Письмо скачивается в формате EML.

Печать писем

Распечатать письмо

Чтобы распечатать письмо:

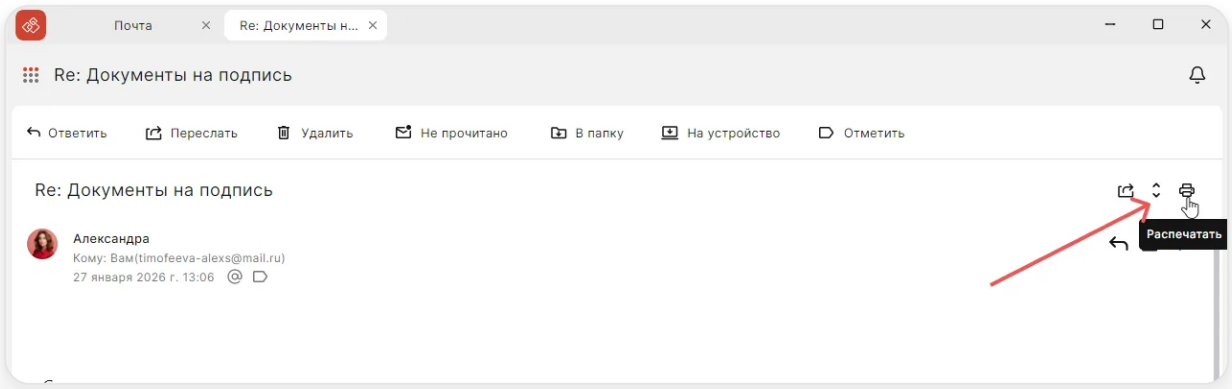
1. Откройте письмо.
2. Вызовите меню действий с письмом по кнопке **Еще** ⋮.
3. Выберите действие **Распечатать**.
4. Откроется окно с печатной формой письма.

Распечатать цепочку писем

> 💡 **Совет**: Чтобы письма объединялись в цепочки, активируйте функцию просмотра в виде цепочек.

Чтобы распечатать цепочку писем:

1. Откройте цепочку писем.
2. Нажмите на кнопку **Распечатать** , размещенную на панели с темой цепочки.



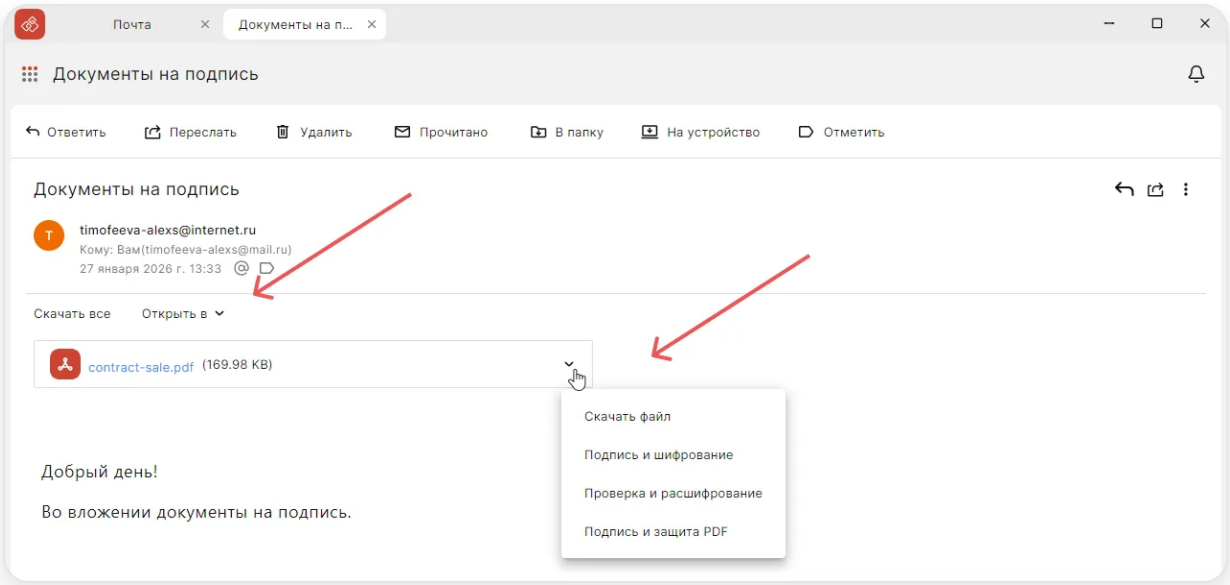
3. Откроется окно с печатной формой цепочки писем.

Действия с вложениями

Открытие вложения в мастере

> 💡 Если в письме есть вложенные файлы, то в списке оно будет отмечено специальным индикатором в виде значка **Скрепка** .

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Дождитесь скачивания вложений, если у вас активна настройка **Получать только текст сообщений**.
4. Выполните действие одним из способов:
   - Вызовите меню действий с вложением по кнопке **Еще** и выберите в меню один мастеров.
   - Вызовите меню действий для всех вложений по кнопке **Открыть в** и выберите в меню один мастеров.



Откроется новая вкладка, на которой вы увидите мастер с уже добавленным в него вложенным файлом из письма.

> 💡 **Совет**: Для проверки отсоединенной подписи добавьте в мастер исходный документ и файл подписи.

Скачивание вложения на компьютер

> 💡 **Совет**: В расширенном поиске есть возможность установить фильтр для писем с вложениями.

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Вызовите меню действий с вложением по кнопке **Еще** .
4. Выберите действие **Скачать файл**.
5. Укажите путь для сохранения файла в окне файлового менеджера.

Скачивание всех вложений в одном архиве

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Скачать все**, размещенную над вложенными файлами.
4. Укажите путь для сохранения архива в окне файлового менеджера.

Открытие вложенного файла

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Дождитесь скачивания вложений, если у вас активна настройка **Получать только текст сообщений**.
4. Нажмите на название вложенного файла.
5. Файл откроется в программе, установленной по умолчанию.

> 💡 Подписанные и зашифрованные документы будут открыты в мастере **Проверка и расшифрование**.

Проверка подписи письма

В списке сообщений подписанные письма отмечаются специальными иконками в виде сертификата  .

При просмотре письма цвет иконок меняется в зависимости от статуса подписи:

Статус	Визуальное обозначение	Описание
Подпись действительная		Подпись прошла все проверки
Подпись недействительная		Обнаружены проблемы с подписью
Статус подписи неизвестен		Обнаружены проблемы с подписью. Возможно, отсутствует поддержка алгоритма сертификата подписи.

Распространенные проблемы

Причины, по которым подпись может быть недействительной:

Причина	Возможность исправления	Рекомендуемые действия
Срок действия сертификата подписи истек, либо сертификат отозван	❌ Невозможно исправить	Запросите новое письмо, подписанное действительным сертификатом
Письмо было изменено после подписания	❌ Невозможно исправить	Запросите новое подписанное письмо

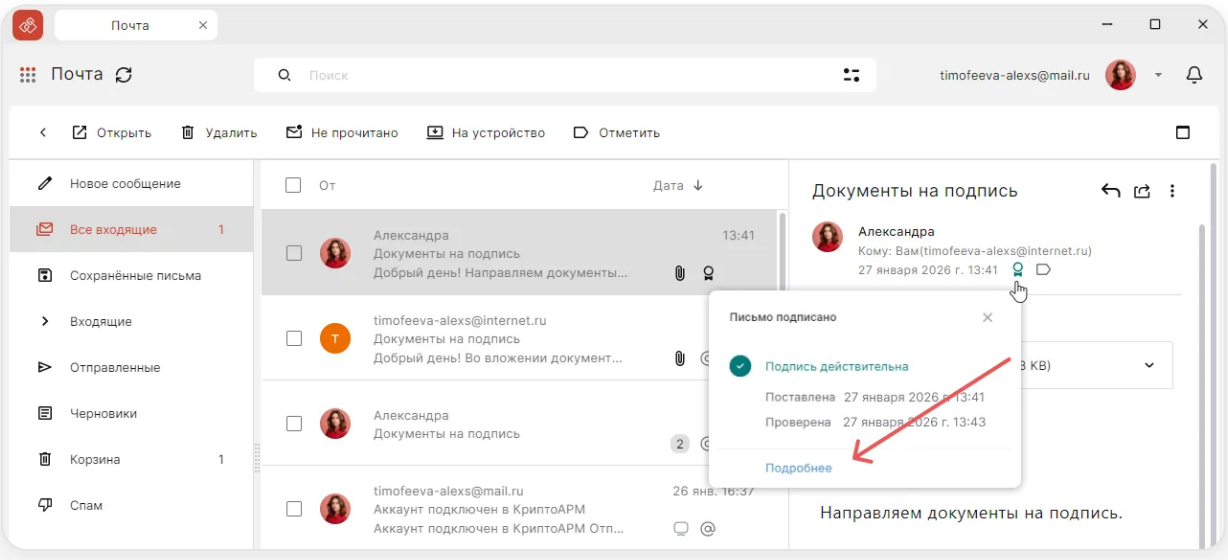
Причина	Возможность исправления	Рекомендуемые действия
Нет доверия к сертификату (отсутствует корневой сертификат)	✅ Можно исправить	Импортируйте корневой сертификат удостоверяющего центра, выпустившего сертификат отправителя
Отсутствует актуальный список отзыва	✅ Можно исправить	Импортируйте актуальный список отзыва сертификатов (CRL)

Как проверить подпись письма

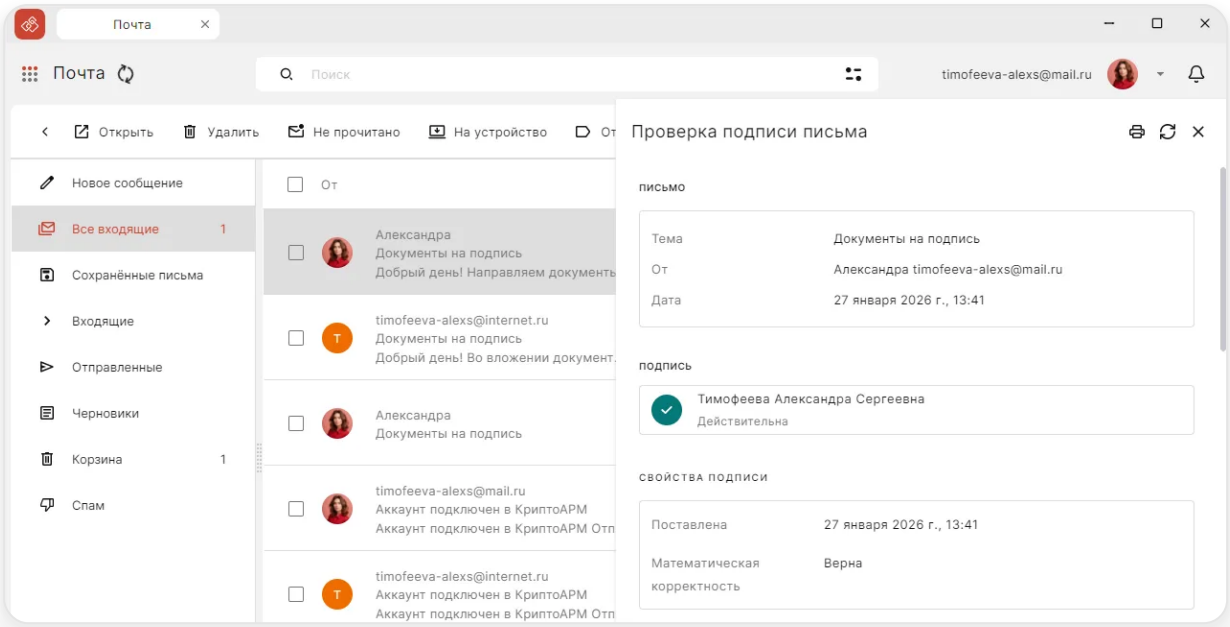
1. Перейдите в раздел **Почта**.
2. Откройте подписанное письмо.
3. В окне просмотра письма будет отображаться иконка .

   В зависимости от статуса подписи письма иконка будет иметь цвет:

   - **зеленый цвет**, если подпись письма **действительная**,
   - **красный цвет**, если подпись **недействительная**,
   - **серый цвет**, если статус подписи **неизвестен**.
4. Нажмите на иконку на панели с подписанным письмом в списке писем или в окне просмотра письма.
5. Откроется окно со статусом подписи, датой подписания и проверки.



Для просмотра детальной информации о подписи нажмите **Подробнее**.



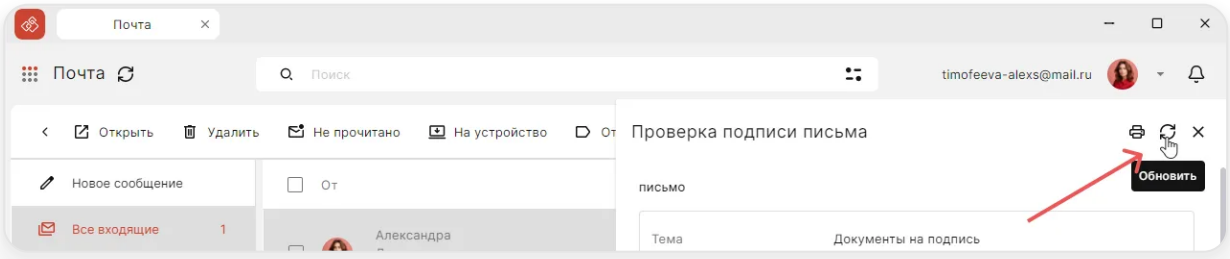
Дополнительные действия

Обновление сведений о подписи письма

В некоторых случаях, например, при установке корневого или промежуточного сертификата, может потребоваться повторная проверка подписи письма.

Чтобы запустить повторную проверку подписи:

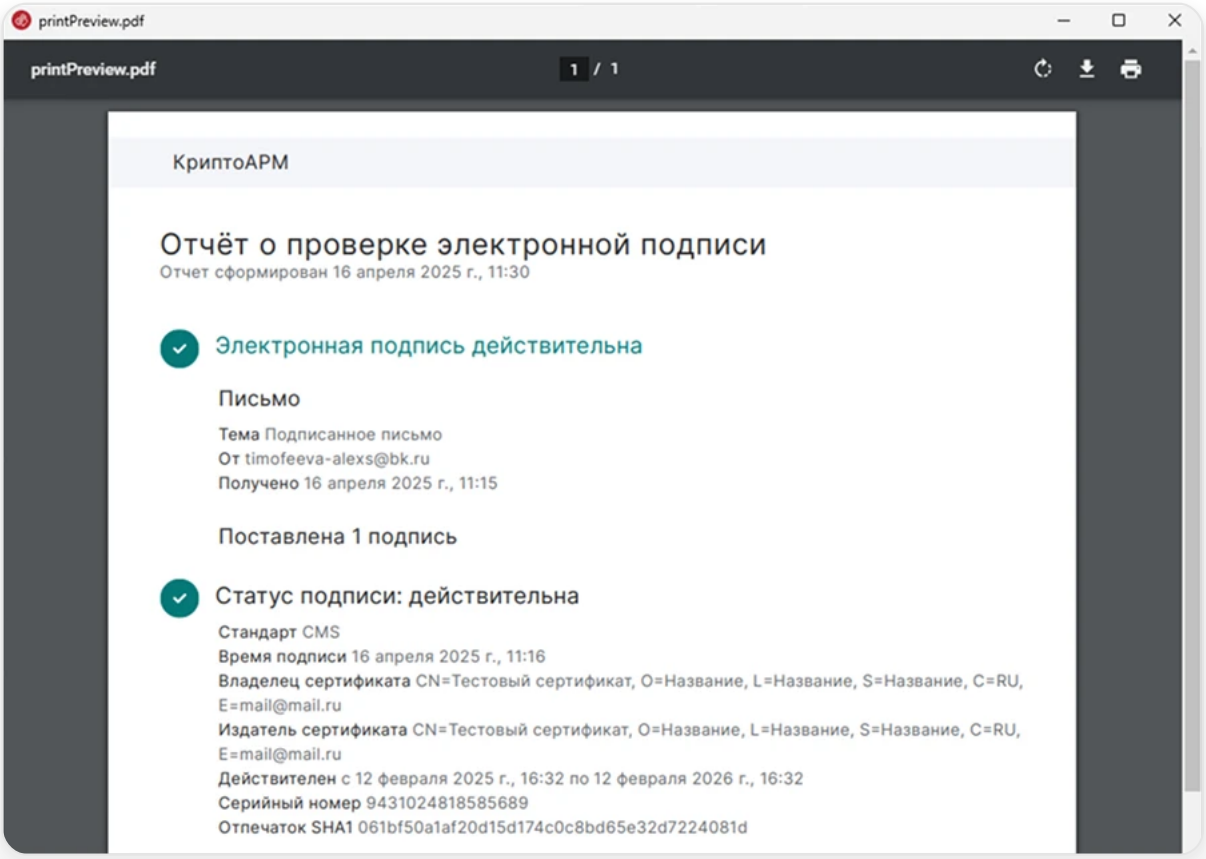
1. Выполните шаги из инструкции Как проверить подпись письма.
2. В окне с детальными сведениями о подписи нажмите на кнопку **Обновить** .



Сведения о подписи будут обновлены.

Печать сведений о подписи письма

1. Выполните шаги из инструкции Как проверить подпись письма.
2. В окне с детальными сведениями о подписи нажмите на кнопку **Печать** .
3. Откроется окно с печатной формой отчета.

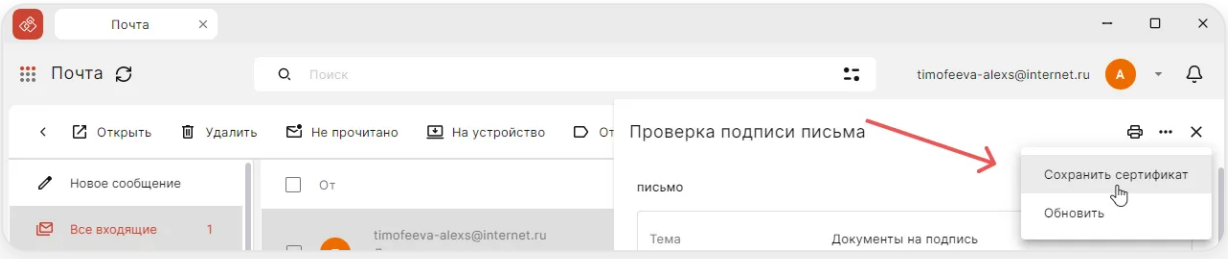


Отчет можно распечатать или скачать на устройство.

Сохранение сертификата подписи

Чтобы сохранить сертификат подписи в разделе **Сертификаты**:

1. Выполните шаги из инструкции Как проверить подпись письма.
2. В окне с детальными сведениями о подписи нажмите на кнопку **Еще**.
3. В появившемся меню с действиями выберите действие **Сохранить сертификат**.



Сертификат подписи письма будет сохранен в хранилище **Сертификаты других пользователей** раздела **Сертификаты**.

Расшифрование письма

Как расшифровать письмо

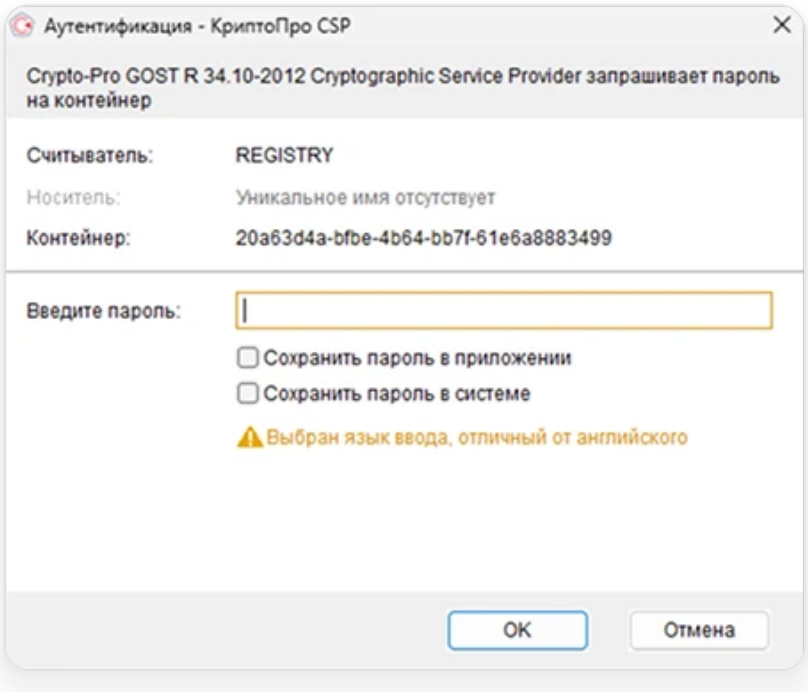
> 💡 В списке сообщений зашифрованные письма обозначаются специальными значками в виде замка 🔒.

1. Перейдите в раздел **Почта**.
2. Откройте письмо, которое необходимо расшифровать.

   > 💡 **Совет**: В расширенном поиске есть возможность установить фильтр для зашифрованных писем.

3. При открытии письмо расшифровывается автоматически, если найден сертификат расшифрования и сохранен пароль к закрытому ключу. Если пароль не был сохранён, вам нужно будет ввести его.

   Пример окна для криптопровайдера КриптоПро CSP:



При необходимости вы можете повторить расшифрование. Для этого на форме просмотра письма вызовите меню действий по кнопке **Еще** ⋮ и выберите действие **Расшифровать**.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены наиболее распространённые ошибки при расшифровании письма:

Ошибка	Рекомендуемые действия
Сообщение не расшифровано	Возможно, в хранилище "Личные" не обнаружен сертификат для расшифрования. Установите сертификат и повторите попытку расшифрования.
Сообщение не расшифровано (Для писем, зашифрованных в адрес сертификата с алгоритмами ГОСТ)	Возможно, отсутствует криптопровайдер, поддерживающий алгоритм шифрования. Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Отсутствует действующая лицензия КриптоАРМ	1. Приобретите или продлите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
Отсутствует действующая лицензия КриптоПро CSP	Установите лицензию КриптоПро CSP

Отправка и получение уведомлений

Исходящие письма с запросом уведомлений

В списке сообщений отправленные письма с уведомлениями отмечаются специальными иконками в виде галочки:

-  для писем с уведомлениями о доставке,
-  для писем с уведомлениями о прочтении.

При получении подтверждения о доставке и прочтении письма цвет значков меняется:

Статус	Визуальное обозначение
Прочитано всеми/Доставлено	
Прочитано не всеми получателям/Не доставлено	
Доставлено всем	
Доставлено не всем получателям	

Как узнать доставлено ли письмо

При получении письма на сервер получателя вам придет автоматическое письмо-уведомление.

Уведомление о доставке подтверждает доставку сообщения, но не гарантирует, что оно было просмотрено или прочитано.

> 💡 **Совет**: Для удобной организации почты вы можете настроить автоматическое перемещение служебных уведомлений в специальную папку **Уведомления**. Подробнее о специальных папках читайте в инструкции Настройки подключения.

Статус доставки можно также просмотреть в папке **Отправленные**:

1. Перейдите в раздел **Почта**.
2. Откройте папку **Отправленные**.
3. Найдите нужное письмо в списке.
4. Нажмите на иконку ✓, размещенную на панели с письмом в списке писем или в окне просмотра письма.
5. Откроется окно со сведениями о доставке.

Как узнать прочитано ли письмо

Чтобы вы могли получить подтверждение прочтения, получатель вашего письма, должен будет сначала его отправить. Подтверждение будет направлено в виде отдельного письма-уведомления, в котором будет указана дата и время, когда ваше сообщение было открыто.

Подтверждение не гарантирует фактическое прочтение письма получателем. Принцип работы с подтверждениями зависит от используемой почтовой системы.

> 💡 **Совет**: Для удобной организации почты вы можете настроить автоматическое перемещение служебных уведомлений в специальную папку **Уведомления**. Подробнее о специальных папках читайте в инструкции Почтовые настройки.

Статус подтверждений можно также просмотреть в папке **Отправленные**:

1. Перейдите в раздел **Почта**.
2. Откройте папку **Отправленные**.
3. Найдите нужное письмо в списке.
4. Нажмите на иконку ✓✓, размещенную на панели с письмом в списке писем или в окне просмотра письма.
5. Откроется окно со сведениями о доставке.

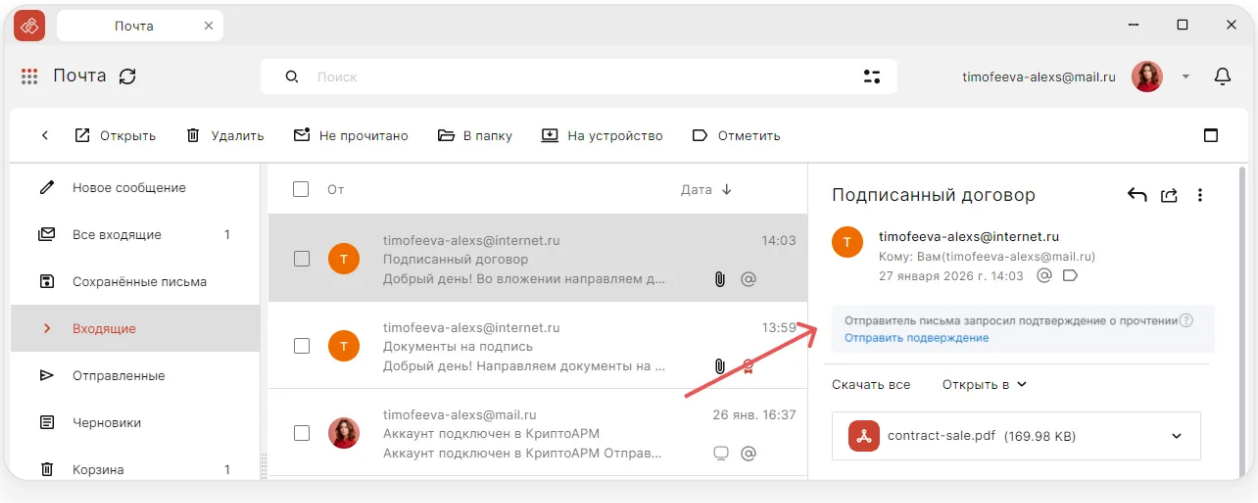
Основные причины отсутствия подтверждений

Функция подтверждений прочтения поддерживается большинством почтовых систем, однако существуют ситуации, когда вы можете их не получить:

- **Групповые рассылки.** При отправке сообщений через списки рассылки или групповые псевдонимы подтверждения могут не приходить.
- **Ограничения администратора.** Ваш системный администратор может ограничить отправку подтверждений только для сотрудников организации или определенных внешних получателей.
- **Тип почтового клиента:**
- Использование программ с протоколом **POP**, которые синхронизируются только по запросу,
- Использование почтовых клиентов **IMAP**, блокирующих подтверждения.

Входящие письма с запросом подтверждения прочтения

Если в настройках вашего почтового аккаунта включена функция "Каждый раз спрашивать, следует ли отправлять уведомление о прочтении", то каждое входящее письмо с запросом на подтверждение получения будет содержать специальный информер.



> 💡 **Совет**: Вы можете скрыть запрос уведомлений о прочтении из интерфейса. Кроме того, можно настроить автоматическую отправку уведомлений о прочтении писем сразу после их получения. Подробнее читайте в инструкции Почтовые настройки.

Отправка подтверждения о прочтении

1. Перейдите в раздел **Почта**.
2. Откройте письмо, прочтение которого необходимо подтвердить.
3. Нажмите **Отправить подтверждение** в информере.

4. Приложение автоматически сформирует и отправит ответ.

После отправки подтверждения информер будет скрыт из письма.

Черновики писем

Создание черновика

Во время написания письма вы можете закрыть черновик и вернуться к нему позже.

Чтобы создать черновик:

1. Перейдите в раздел **Почта**.
2. Нажмите на кнопку **Новое сообщение** в меню слева.
3. Откроется вкладка с новым письмом.
4. Заполните необходимые поля:
    - Укажите получателей (можно оставить пустым),
    - Напишите тему и текст письма,
    - При необходимости добавьте вложения.
5. Закройте вкладку с письмом. Черновик будет сохранен автоматически.

Сохраненный черновик можно найти в папке **Черновики**.

> 💡 Черновик сохраняется до тех пор, пока не будет отправлен или удален.

Продолжение работы с черновиком

Чтобы продолжить работу с черновиком:

1. Перейдите в раздел **Почта**.
2. Откройте папку **Черновики** в меню слева.
3. Откройте черновик одним из способов:
    - Выделите черновик в списке писем и нажмите кнопку **Открыть** на панели действий.
    - Дважды кликните по панели с черновиком.
4. Откроется новая вкладка с черновиком.

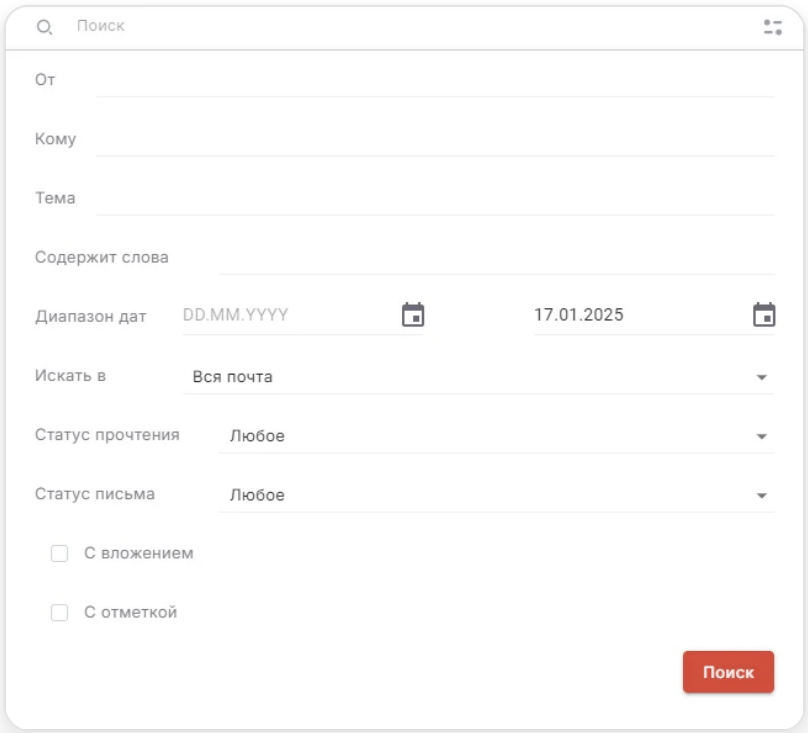
Поиск писем

Базовый поиск

1. Перейдите в раздел **Почта**.
2. Введите в поисковой строке:
    - Имя отправителя;
    - Имя получателя;
    - Тему;
    - Текст содержания.
3. Нажмите **Enter**.

Расширенный поиск

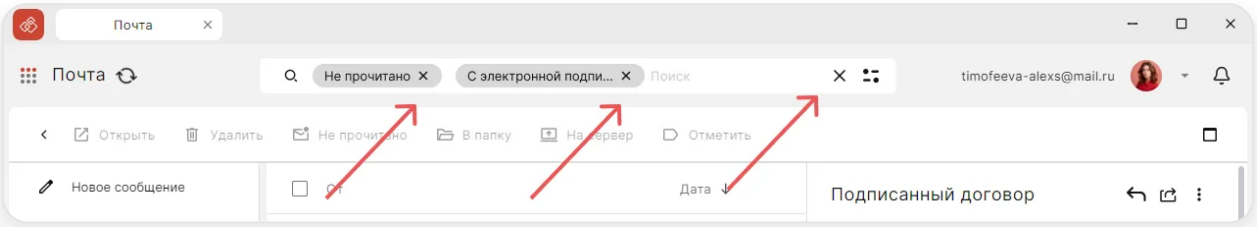
1. Перейдите в раздел **Почта**.
2. В строке поиска нажмите на иконку **Открыть фильтр** .
3. Откроется окно с фильтрами:
    - по имени отправителя;
    - по имени получателя;
    - по теме письма;
    - по содержанию слов в письме;
    - по диапазону дат;
    - относительно папки: **Вся почта**, **Входящие**, **Отправленные**, **Черновики**, **Корзина** и т. д.;
    - по статусу прочтения: **Любое**, **Прочитано**, **Не прочитано**;
    - по статусу письма: **Любое**, **Простое письмо**, **С электронной подписью**, **Зашифрованное**;
    - по параметру **С вложением**;
    - по параметру **С отметкой**.



4. Настройте параметры поиска.
5. Нажмите на кнопку **Поиск**.

Управление результатами поиска

- Для отмены фильтрации необходимо нажать на кнопку **Отмена** ✕ на чипсете с фильтром или в строке поиска.
- Для быстрого доступа к истории поисков используйте выпадающий список в поисковой строке.



Смотрите также

- Создание нового письма — руководство по созданию и отправке писем.
- Почтовые настройки — настройка параметров почтового ящика.
- Работа с письмами — управление письмами после их отправки и получения.

Открыть статью на сайте

Как настроить автоматизацию почты в КриптоАРМ

Автоматизация почты в КриптоАРМ упрощает работу с электронной перепиской: вы сможете создавать правила сортировки, фильтры для писем, автоматически сохранять вложения, пересылать письма и отправлять файлы с уведомлениями. Это позволяет поддерживать порядок в почтовом ящике и ускоряет выполнение рутинных задач.

Содержание:

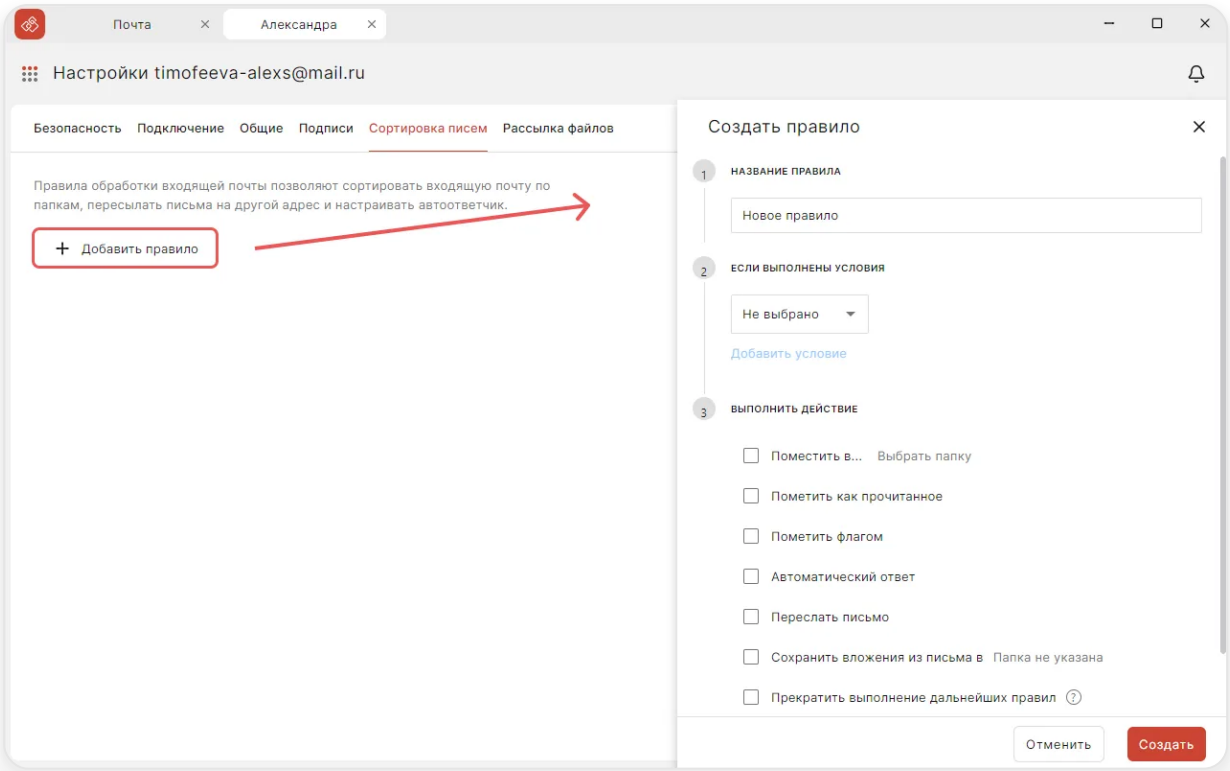
- Сортировка и фильтрация писем
- Автоматическая отправка файлов по почте
- Смотрите также

Сортировка и фильтрация писем

Создание правила сортировки писем

Способ 1: Через настройки почтового аккаунта

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите **Добавить правило**.
4. Откроется окно **Создать правило**.



5. Укажите название правила.

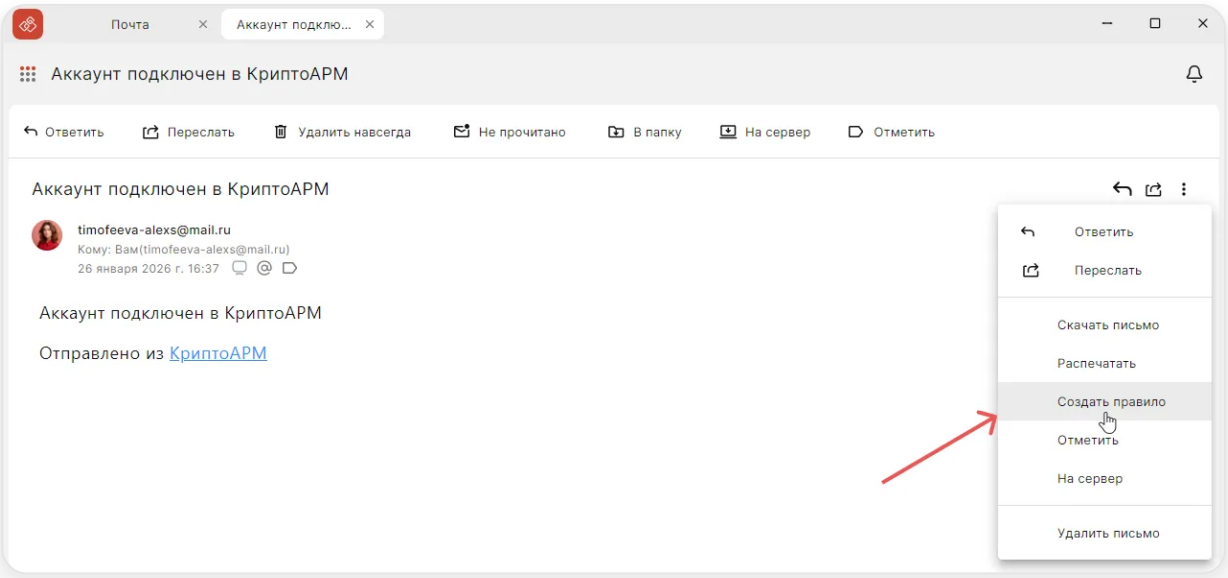
6. Добавьте одно или несколько условий.
7. Укажите действие, которое необходимо выполнить с письмом.
8. Нажмите **Создать**.

> 💡 **Совет:** Используйте понятные названия правил, чтобы быстро ориентироваться в списке.

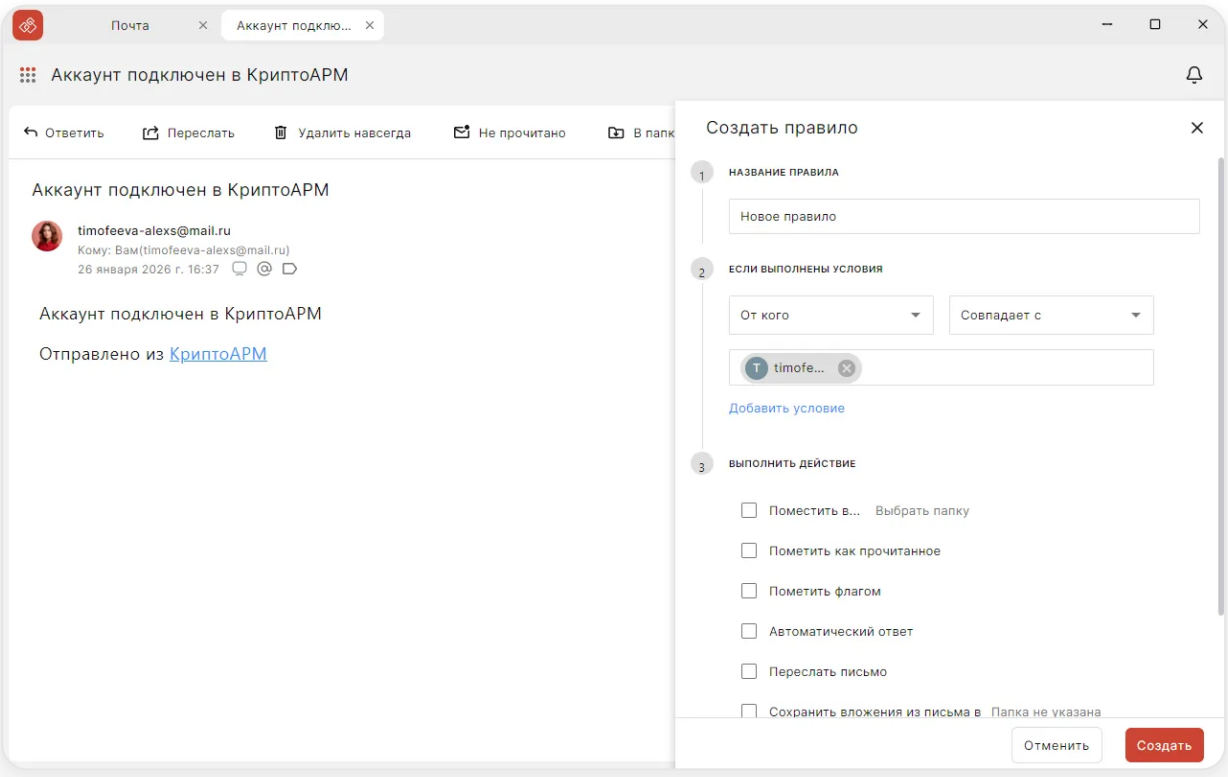
Способ 2: Создание правила на основе письма

1. Перейдите в раздел **Почта**.
2. Откройте письмо, для которого необходимо создать правило.
3. Вызовите меню действий с вложение по кнопке **Еще**.

4. Выберите **Создать правило**.



5. Откроется окно **Создать правило**.



6. Добавьте одно или несколько условий.
7. Укажите действие, которое необходимо выполнить с письмом.
8. Нажмите **Создать**.

Критерии сортировки писем

Вы можете создавать правила на основе следующих параметров:

Критерий	Доступные условия	Описание	Пример использования
Отправитель	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по адресу/имени отправителя	Все письма от *@domain.com
Получатель	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по адресу получателя	Письма для support@company.com
Тема письма	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по словам в теме	Письма с темой "Счёт" или "Invoice"
Содержание письма	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по ключевым словам в теле письма	Письма со словом "договор"
Название вложения	содержит, не содержит, совпадает с, не совпадает с	Фильтрация по имени файлов вложений	Письма с файлом "report.pdf"
Дата получения	До, После	Фильтрация по дате отправки/получения	Письма после 01.01.2023
Статус	Подписанные, Зашифрованные, Содержит вложение	Фильтрация по специальным статусам	Все подписанные письма
Размер	Больше, Меньше	Фильтрация по размеру письма	Письма больше 10 МБ
Все входящие	-	Общее правило для всех писем	Применение действия ко всей входящей почте

> 💡 **Совет:** Используйте несколько условий одновременно для точной фильтрации. Например, письма от определённого отправителя с вложениями определённого типа.

Доступные действия

Для писем, соответствующих заданным условиям, можно настроить:

Действие	Описание
Перемещение в папку	Автоматическое перемещение в указанную папку
Пометка как прочитанного	Изменение статуса письма с непрочитанного на прочитанное
Автоматический ответ	Отправка шаблонного ответа. Настраивается текст и получатели.

Действие	Описание
Пересылка	Перенаправление письма другому адресату. Можно указать несколько получателей.
Сохранение вложений	Автоматическое скачивание файлов. Указывается папка для сохранения.
Прекращение обработки	Остановка выполнения последующих правил. Используется для приоритизации правил.
Применение к существующим	Применение правила к уже полученным письмам в папке «Входящие»

Управление правилами

Редактирование правила сортировки

Чтобы отредактировать правило сортировки:

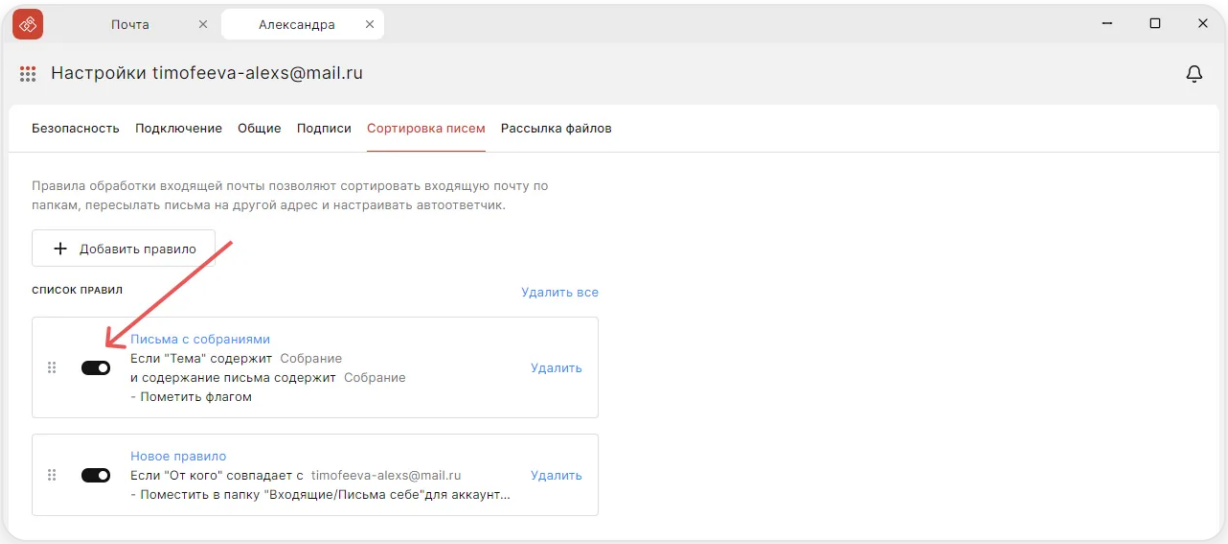
1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите на название правила, настройки которого необходимо отредактировать.
4. В открывшемся окне внесите изменения в настройки и нажмите **Сохранить**.

Изменение активности правила сортировки

Доступна временная активация или деактивация правила без его удаления.

Чтобы включить или отключить правило:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Сортировка писем**.
3. Включите или выключите переключатель на панели с правилом в списке.



Изменения применяются автоматически без дополнительного подтверждения.

Изменение приоритета выполнения правил

Приоритет выполнения правил можно настроить, изменив порядок их отображения.

Чтобы поменять порядок правил:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Сортировка писем**.
3. Наведите курсор мыши на кнопку , размещенную на панели с правилом. Удерживая левую кнопку мыши на кнопке, переместите правило в необходимое место в списке.

Изменения применяются автоматически без дополнительного подтверждения.

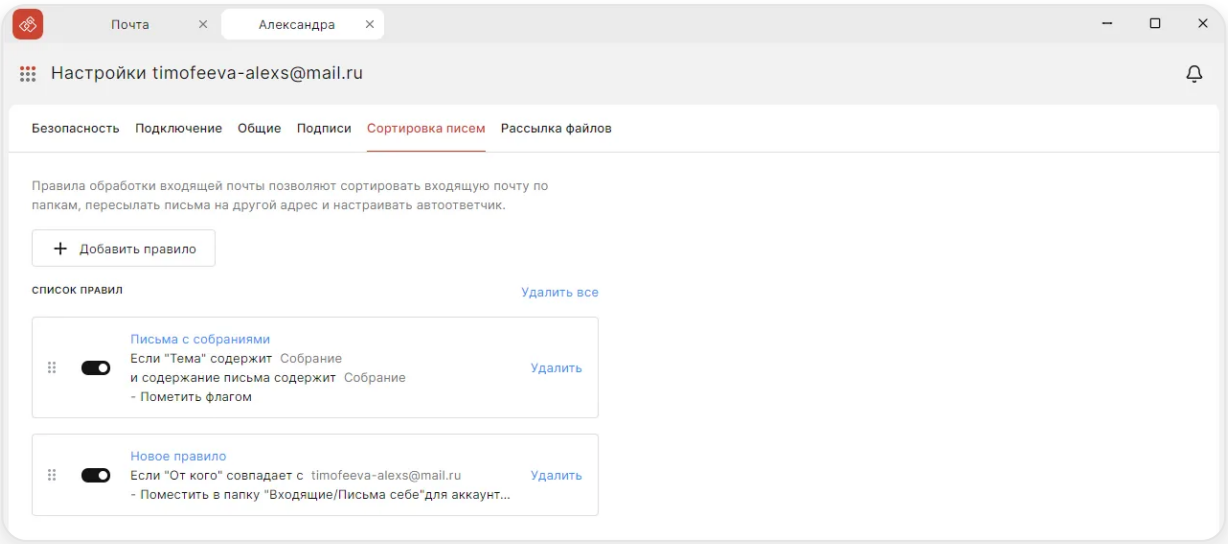
Удаление правил

Чтобы удалить одно правило:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите на кнопку **Удалить**, размещенную на панели с правилом.
4. Подтвердите действие в модальном окне.

Чтобы удалить все правила:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Сортировка писем**.
3. Нажмите на кнопку **Удалить все**, размещенную над списком правил.
4. Подтвердите действие в модальном окне.



Автоматическая отправка файлов по почте

Рассылка файлов — это инструмент, который позволяет настроить автоматическую отправку файлов в виде почтовых сообщений. Укажите папки, из которых будут забраны файлы, задайте параметры, необходимые для формирования письма и запустите рассылку.

Создание рассылки файлов

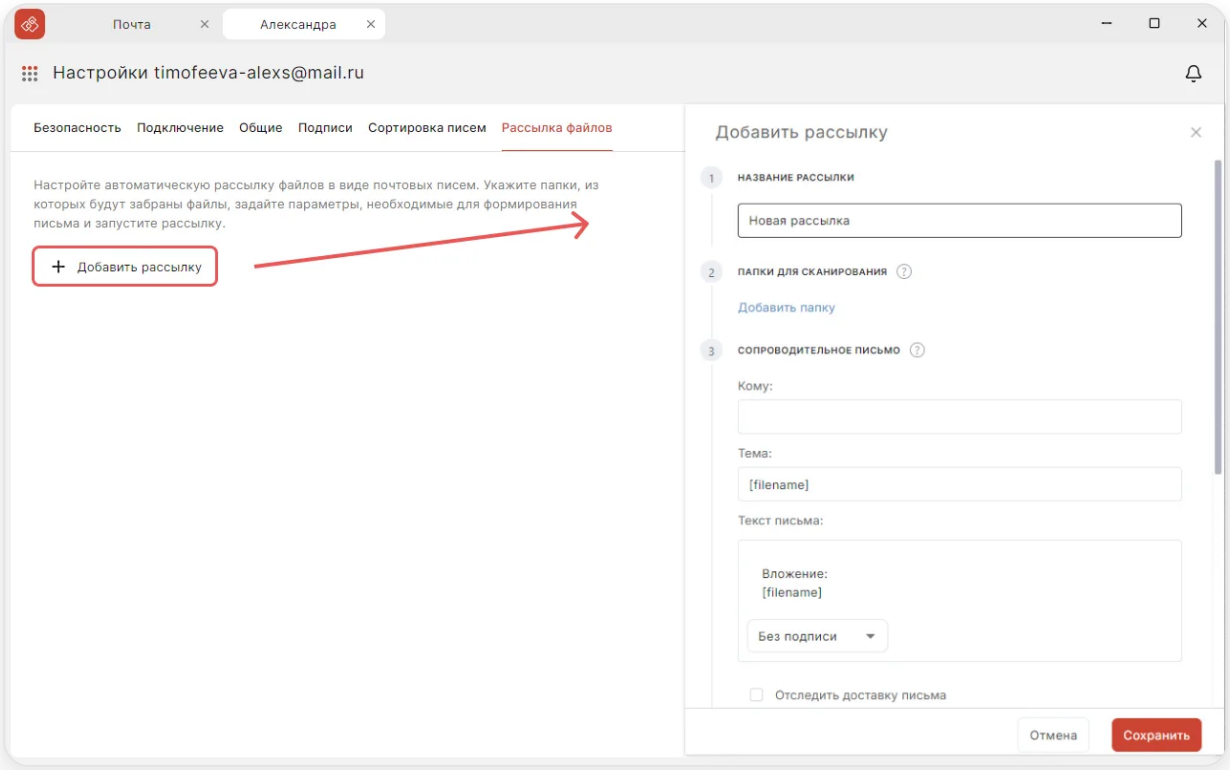
1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Рассылка файлов**.
3. Нажмите **Добавить рассылку**.
4. Откроется окно **Создать рассылку**.
5. Укажите название рассылки.
6. Выберите папки для сканирования с устройства, из которых будут взяты файлы для рассылки.

> ⚠️ **Примечание**: В рассылку попадут файлы только из корневой папки.

7. Добавьте текст сопроводительного письма.

> 💡 **Совет**: В теме и тексте письма можно использовать константы: `[filename]` - имя файла, `[date]` - дата отправки письма, `[datetime]` дата и время отправки письма.

8. Укажите получателей письма:
    - Установите курсор в поле **Кому** и введите электронные адреса получателей,
    - Выберите получателей из адресной книги. Для этого установите курсор в поле **Кому** и в появившемся меню выберите действие **Показать все контакты**. Откроется окно со списком адресных книг с контактами. В списке отображаются только контакты с указанными email-адресами. Выберите один или несколько контактов. Для выбора контакта нажмите на его аватар.

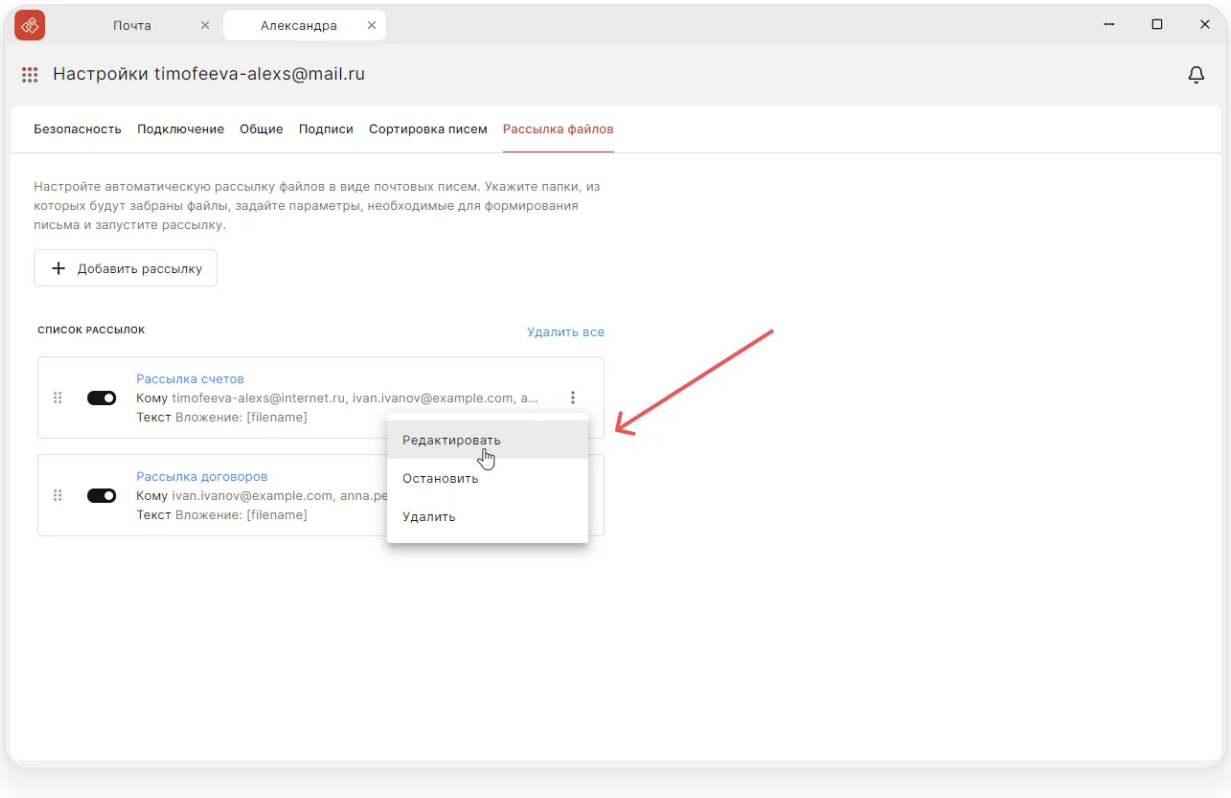


9. При необходимости активируйте запрос уведомлений о доставке и прочтении письма:
    - **Отследить доставку письма** - будет запрошено уведомление о доставке.
    - **Запросить подтверждение о прочтении письма** - будет запрошено уведомление о прочтении.
10. Дополнительно можно указать действия с файлами:
    - Отправленные файлы могут быть удалены с устройства либо перемещены в выбранную папку.
    - Файлы, которые не удалось отправить, можно удалить, оставить в исходной папке, либо переместить в выбранную папку.
11. Укажите настройки активности рассылки. Установите флаг **Запустить рассылку активной**, если нужно запустить рассылку сразу после сохранения;
12. Нажмите **Сохранить**.

Управление рассылками

Редактирование рассылки

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Рассылка файлов**.
3. Вызовите меню действий для рассылки, которую необходимо отредактировать.
4. Выберите **Редактировать**.



5. Откроется форма редактирования рассылки.
6. Внесите изменения.
7. Нажмите **Сохранить**.

Приостановка рассылки

Доступна временная приостановка рассылки без ее удаления.

Чтобы включить или отключить рассылку:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Рассылка файлов**.
3. Деактивируйте переключатель, размещенный на панели с рассылкой, либо нажмите **Остановить** в меню действий с рассылкой.

Изменения применяются автоматически без дополнительного подтверждения.

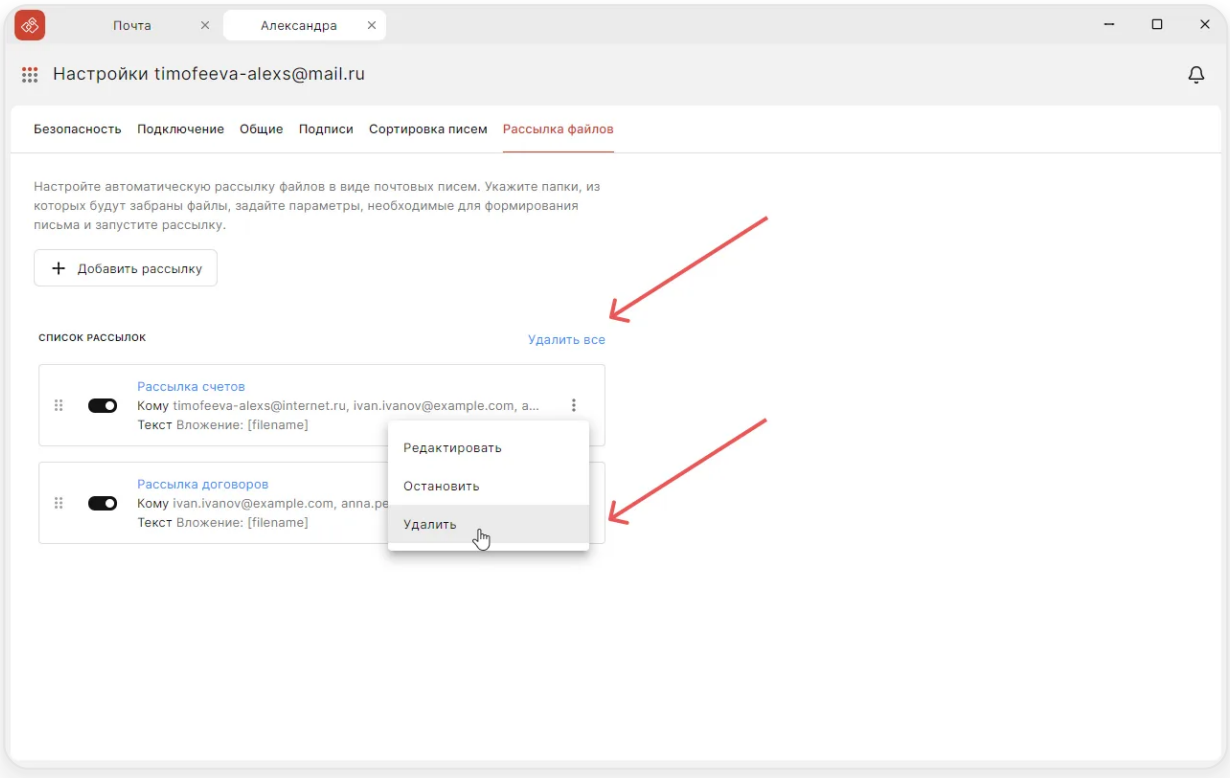
Удаление рассылки

Чтобы удалить одну рассылку файлов:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Рассылка файлов**.
3. Вызовите меню действий для рассылки, которую необходимо удалить.
4. Выберите **Удалить**.
5. Подтвердите действие в модальном окне.

Чтобы удалить все рассылки файлов:

1. Откройте настройки почтового аккаунта (см. раздел Как открыть настройки почтового аккаунта).
2. Перейдите на вкладку **Рассылка файлов**.
3. Нажмите кнопку **Удалить все**, размещенную над списком рассылок.
4. Подтвердите действие в модальном окне.



Смотрите также

- Подключение почтового аккаунта — настройка и управление почтовыми аккаунтами в КриптоАРМ.
- Почтовые настройки — настройка параметров почтового ящика.

- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.

Открыть статью на сайте

Как открыть письмо .eml, .p7s и .p7m в КриптоАРМ

В КриптоАРМ вы можете работать с почтовыми сообщениями, сохранёнными в виде файлов.

В этой инструкции вы узнаете, как работать с почтовыми файлами в КриптоАРМ: открывать `.eml`, проверять подписи `.p7s` и расшифровывать зашифрованные `.p7m` письма.

Содержание:

- Формат .eml — стандартное почтовое сообщение
- Формат .p7m — зашифрованное письмо
- Формат .p7s — подписанное письмо (вложение smime.p7s)
- Смотрите также

Формат .eml — стандартное почтовое сообщение

Файл с расширением `.eml` — это сохранённое электронное письмо со всей исходной структурой: заголовками, текстом, форматированием и вложениями.

Как открыть файл .eml

Если у вас на компьютере сохранен файл с письмом `.eml`, вы можете открыть его в КриптоАРМ одним из способов:

Способ 1: Через контекстное меню файла

1. Найдите файл `.eml` в проводнике.
2. Щёлкните по нему правой кнопкой мыши.
3. В меню выберите **Открыть с помощью** → **КриптоАРМ**.

Способ 2: Двойным щелчком

1. Убедитесь, что EML-файлы ассоциированы с КриптоАРМ.
2. Дважды щелкните по файлу.

После открытия письмо отображается в новой вкладке с сохранением всех оригинальных элементов.

> 💡 **Совет**: Открытое письмо можно импортировать в любой из ваших почтовых аккаунтов, подключенных в КриптоАРМ.

Формат .p7m — зашифрованное письмо

Файл с расширением `.p7m` содержит зашифрованное почтовое сообщение.

Как расшифровать файл .p7m

Если у вас на компьютере сохранен файл с зашифрованным письмом `.p7m`, вы можете расшифровать его в КриптоАРМ одним из способов:

Способ 1: Через мастер в программе

1. В КриптоАРМ откройте раздел **Документы**.
2. Запустите мастер **Проверка и расшифрование**.
3. Добавьте в мастер ваш файл `.p7m` и выполните расшифрование.

Способ 2: Двойным щелчком

1. Убедитесь, что p7m-файлы ассоциированы с КриптоАРМ.
2. Дважды щелкните по файлу.
3. Это автоматически запустит КриптоАРМ с мастером **Проверка и расшифрование**.
4. Выполните расшифрование.

После успешного расшифрования вы получите файл `.eml`, который можно открыть и прочитать как обычное письмо.

Формат .p7s — подписанное письмо (вложение smime.p7s)

Расширение `.p7s` — это файл электронной подписи. Часто такая подпись прикрепляется к письму отдельным файлом с именем `smime.p7s`. Для проверки такой подписи необходимо иметь само исходное письмо, сохранённое в формате `.eml`.

Как проверить подпись smime.p7s

1. Скачайте письмо в формате `.eml` через веб-интерфейс почтового сервиса или через сторонний почтовый клиент.
2. Откройте письмо в формате `.eml` в приложении КриптоАРМ.
3. В окне просмотра письма будет отображаться иконка в виде сертификата .

   В зависимости от статуса подписи письма иконка будет иметь цвет:

   - **зеленый цвет**, если подпись письма **действительная**,
   - **красный цвет**, если подпись **недействительная**,
   - **серый цвет**, если статус подписи **неизвестен**.

4. Нажмите на иконку в виде сертификата.

5. Откроется окно со статусом подписи, датой подписания и проверки.
6. Для просмотра детальной информации о подписи нажмите **Подробнее**.

Смотрите также

- Подключение почтового аккаунта — настройка и управление почтовыми аккаунтами в КриптоАРМ.
- Почтовые настройки — настройка параметров почтового ящика.
- Создание нового письма — руководство по созданию и отправке писем.
- Работа с письмами — управление письмами после их отправки и получения.

Открыть статью на сайте

Обзор операций КриптоАРМ и выбор мастера

В этом разделе мы объясним, как работать с документами в КриптоАРМ: создавать подписи по стандартам CAdES и PAdES, шифровать файлы и выбирать подходящий мастер для конкретной задачи.

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

Содержание:

- Основные операции
- Электронная подпись в КриптоАРМ
- Выбор мастера
- Смотрите также

Основные операции

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

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

- создание электронной подписи,
- архивирование и шифрование документов,
- проверку подписей и расшифрование.

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

Электронная подпись в КриптоАРМ

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

Приложение КриптоАРМ позволяет создавать подписи со стандартами:

- **CAdES** — для любых файлов (DOCX, XLSX, XML и других типов данных)

- **PAdES** — для PDF-документов с возможностью видимого штампа подписи

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

Ниже приведено краткое сравнение стандартов электронной подписи:

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

Подпись со стандартом CAdES

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

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

Подпись CAdES может быть:

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

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

Печатная форма

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

Печатная форма — это копия документа с визуальным отображением штампа подписи. В ней отсутствует электронная подпись и криптографические данные.

> ⚠️ **Примечание**: печатная форма предназначена только для визуального ознакомления и подтверждения факта подписания. Она не обладает юридической силой, так как не содержит электронной подписи.

В текущей версии КриптоАРМ печатные формы можно создавать:

- при выполнении подписи (см. Подпись с созданием печатной формы);
- при просмотре сведений о подписи (см. Создание печатной формы).

Подпись со стандартом PAdES

PAdES — стандарт электронной подписи для PDF-документов. Подпись встраивается непосредственно в PDF-файл без изменения его формата и без создания отдельного файла подписи.

Документ остаётся обычным PDF и может быть открыт в любом просмотрщике.

Подпись PAdES может быть:

- **видимой** — отображается в виде штампа на странице;
- **невидимой** — не отображается визуально, но полностью доступна для проверки.

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

Сертифицирующая подпись PDF

Сертифицирующая подпись — это особый тип электронной подписи, применяемый к PDF-документу до внесения в него других подписей. Она не только подтверждает авторство и целостность документа, но и устанавливает правила его дальнейшего использования.

В отличие от обычной подписи, сертифицирующая подпись позволяет контролировать, какие изменения разрешены после подписания, а любые неразрешённые модификации приводят к утрате валидности подписи.

При сертификации документа определяется перечень допустимых действий, например, установка подписи в заранее размеченные области для подписантов и изменение оформления произвольной области.

Все действия, не включённые в список разрешённых, приведут к тому, что сертифицирующая подпись станет недействительной при проверке.

> ⚠️ **Примечание**: Поставить сертифицирующую подпись может только первый подписант.

Конвертация в формат PDF/A

PDF/A — международный стандарт (ISO 19005) для долгосрочного архивирования PDF-документов и обеспечивает их корректное воспроизведение на любых устройствах в будущем.

КриптоАРМ поддерживает конвертацию в форматы:

- **PDF/A-2b** — обеспечивает базовую стабильность для долгосрочного хранения,

- **PDF/A-3b** — позволяет добавлять структурированные данные и прикрепленные файлы без нарушения стандартов.

При конвертации выполняется удаление или отключение элементов, которые могут нарушить отображение документа или повлиять на его безопасность. К таким элементам относятся скрипты (JavaScript), мультимедиа (аудио, видео), 3D-объекты и интерактивные формы, внешние ссылки на ресурсы, а также шифрование и парольная защита.

> ⚠️ **Примечание**: Конвертация доступна только для неподписанных документов и выполняется совместно с подписью документа.

Выбор мастера

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

- Подпись и шифрование — предназначен для групповой работы с файлами. Позволяет подписывать и шифровать несколько документов одновременно, создавать архивы и использовать стандарты CAdES и PAdES.
- Подпись и защита PDF — оптимален для работы с одним PDF-документом. Предоставляет инструменты просмотра, проверки подписей, разметки областей и добавления новых подписей в одном интерфейсе.
- Проверка и расшифрование — используется для работы с файлами, содержащими электронные подписи и (или) зашифрованные данные. После загрузки файла приложение автоматически определяет его тип и производит доступные действия: проверку электронной подписи, расшифрование данных или выполнение обеих операций одновременно.

Задача / Сценарий	Рекомендуемый мастер	Почему
Подписать / зашифровать **много файлов** сразу	Подпись и шифрование	Групповая обработка, CAdES + PAdES, архивы, шифрование
Работать с **одним PDF**: просмотр, разметка областей, несколько подписантов	Подпись и защита PDF	Встроенный просмотрщик, разметка, сертификация, PDF/A
Проверить подпись / расшифровать документ	Проверка и расшифрование	Автоматически определяет тип файла и предлагает действия
Добавить ещё одну подпись к уже подписанному файлу	Подпись и шифрование или Подпись и защита PDF	Зависит от формата исходного файла

Смотрите также

- Профиль подписи — сохранение параметров операций в профилях для повторного использования.
- Подпись и шифрование — руководство по созданию электронных подписей и шифрованию файлов.
- Проверка и расшифрование — проверка подписей и расшифрование документов.
- Подпись и защита PDF — работа с PDF: просмотр, разметка областей, добавление подписей и сертифицирующая подпись.

Открыть статью на сайте

Создание и управление профилем подписи

Профиль подписи в КриптоАРМ — это готовый шаблон настроек для операций с документами. Используйте профили, чтобы применять нужные параметры в один клик, экономя время на ручной настройке.

В этом руководстве вы узнаете, как создавать и настраивать профили подписи.

Содержание:

- Создание профиля подписи
- Переключение между профилями подписи
- Редактирование настроек профиля подписи
- Сохранение настроек в мастере «Подпись и шифрование»
- Удаление профилей подписи
- Экспорт и импорт профилей подписи
- Смотрите также

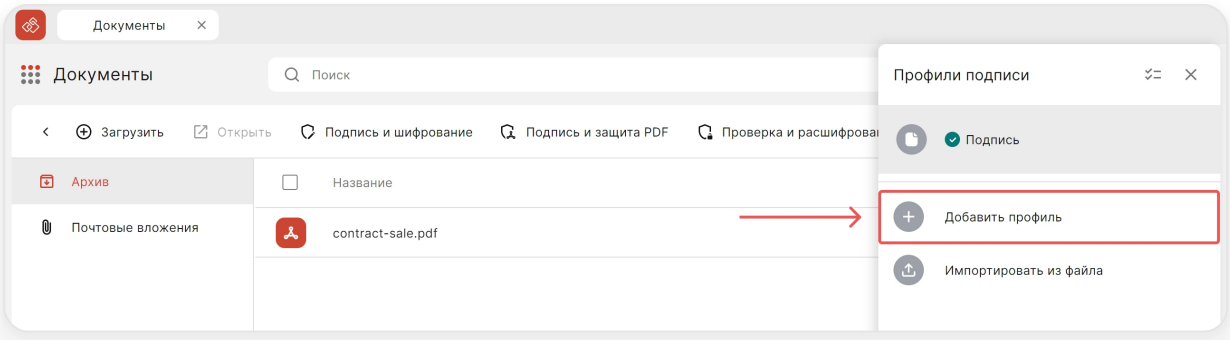
Создание профиля подписи

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

> 💡 **Совет**: Начните с создания базовых профилей для самых частых операций, затем постепенно добавляйте специализированные настройки по мере необходимости.

Способ 1: Создание вручную

1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Выберите **Добавить профиль**.



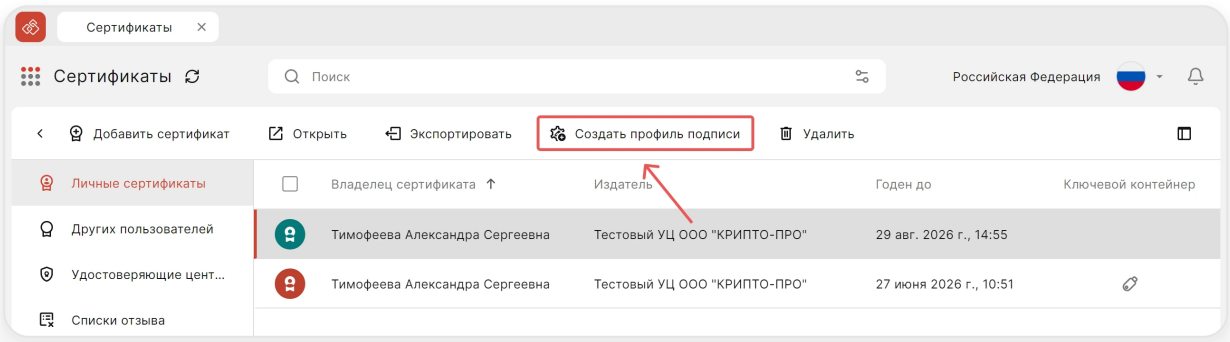
4. Откроется окно **Новый профиль**.
5. В блоке **Операции** укажите какие действия необходимо выполнить с документом.

   Можно выбрать одну операцию или несколько операций одновременно. Например, при выборе комбинации **Подпись + Архивирование + Шифрование** документ сначала будет подписан электронной подписью, затем подписанные файлы упакуются в архив (общий или отдельные, в зависимости от настроек), и после этого архив будет зашифрован для выбранных получателей.
6. Укажите настройки профиля (см. Настройки профиля подписи).
7. Нажмите **Сохранить**.

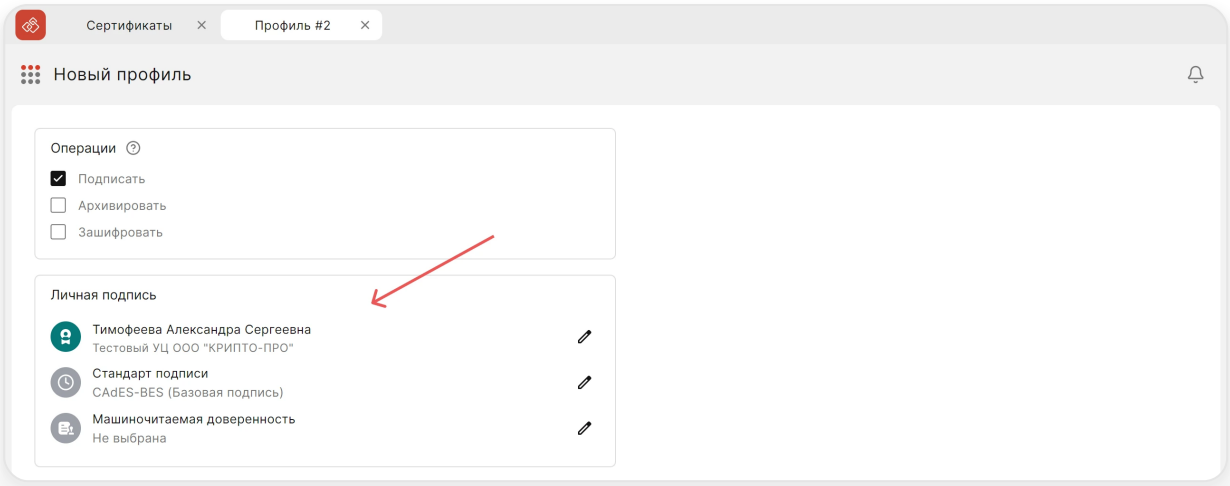
Способ 2: Создание на основе сертификата

> 💡 **Совет**: Этот способ удобен, если профиль создаётся под конкретный сертификат и используется для регулярных операций.

1. Перейдите в раздел **Сертификаты** → хранилище **Личные сертификаты**.
2. Выделите личный сертификат, с помощью которого необходимо создать профиль подписи.
3. На панели действий нажмите на кнопку **Создать профиль подписи**.



4. Откроется окно **Новый профиль**. Личный сертификат будет автоматически привязан в блоке **Личная подпись**.



5. Укажите остальные настройки (см. Настройки профиля подписи).

6. Нажмите **Сохранить**.

Переключение между профилями подписи

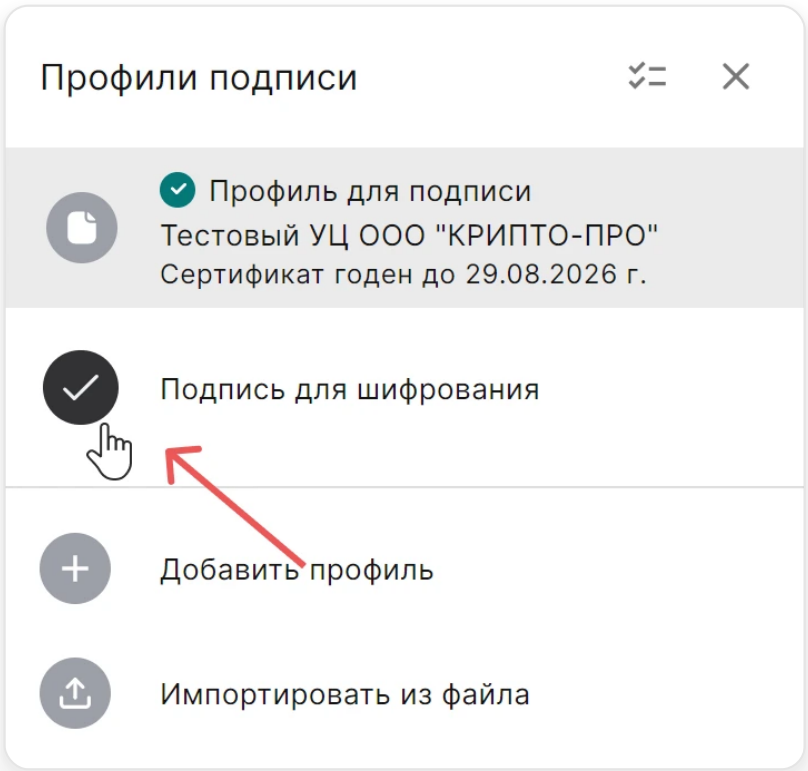
Активный профиль автоматически применяется в мастерах подписи и шифрования.

> 💡 **Совет:** Переключение профиля позволяет быстро применять другой набор настроек без редактирования параметров вручную.

Чтобы переключить профиль:

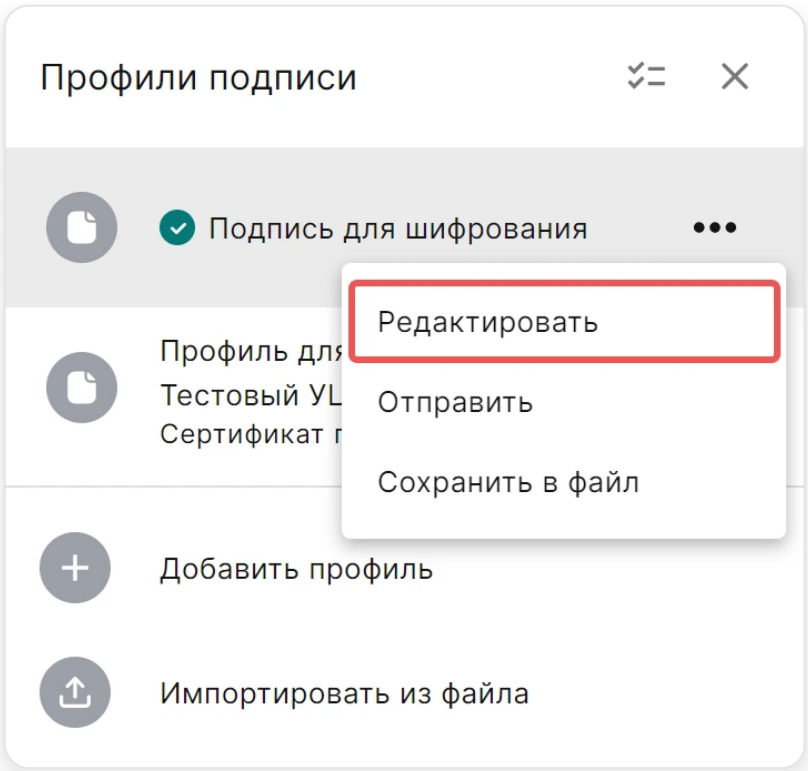
1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подпись и шифрование** или **Подпись и защита PDF**.
3. Нажмите на название активного профиля в верхней части окна.

4. В открывшемся окне нажмите на иконку профиля, который хотите сделать активным.



Редактирование настроек профиля подписи

1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Нажмите на появившуюся кнопку **Еще** ••• .



4. Выберите действие **Редактировать**.

5. Откроется форма редактирования, в которой доступны все параметры профиля.
6. Внесите изменения в настройки (см. Настройки профиля подписи).
7. Нажмите кнопку **Сохранить**.

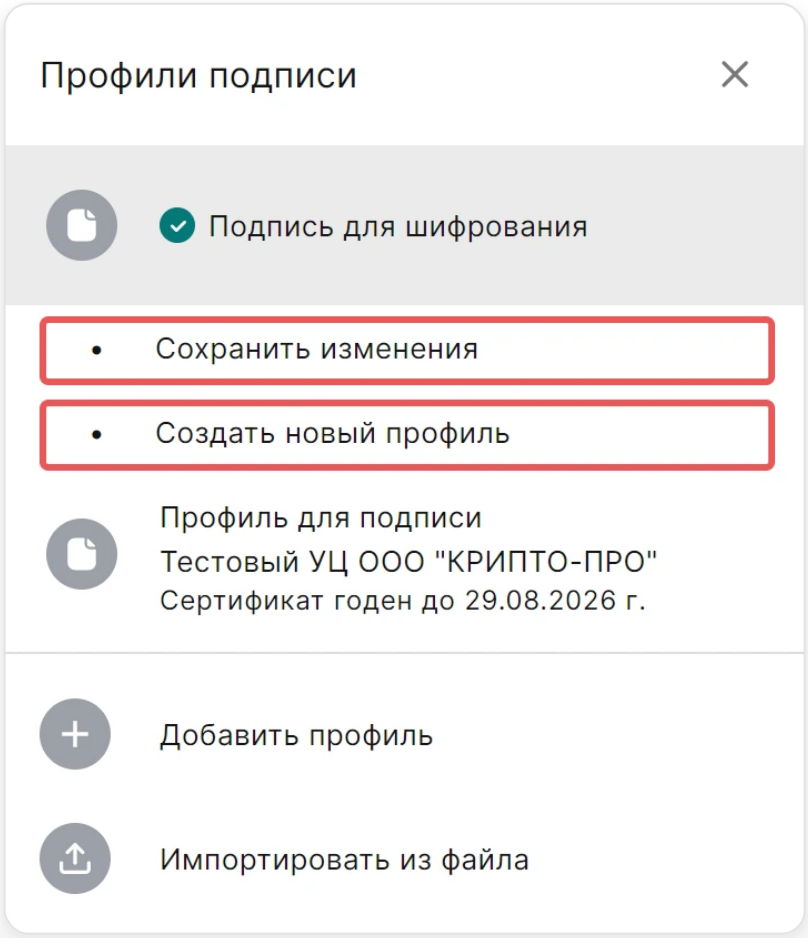
Сохранение настроек в мастере «Подпись и шифрование»

Вы можете изменить параметры операций непосредственно в процессе работы, а затем сохранить эти изменения в текущем профиле или создать на их основе новый профиль.

1. Перейдите в раздел **Документы** → откройте мастер **Подпись и шифрование**.
2. На втором шаге измените любые параметры операции: сертификат подписи, алгоритм, список получателей шифрования, формат выходного файла и т.д.

3. Нажмите на название активного профиля в верхней части окна и выберите одно из действий:

    - **Сохранить изменения** — изменения применятся к текущему профилю. Старые настройки будут заменены новыми.
    - **Создать новый профиль** — откроется окно для ввода названия нового профиля с указанными параметрами.



> 💡 **Важно**: Если вы сохранили изменения в текущем профиле, отменить эту операцию будет нельзя — профиль перезапишется. При необходимости сохраните его копию заранее через экспорт.

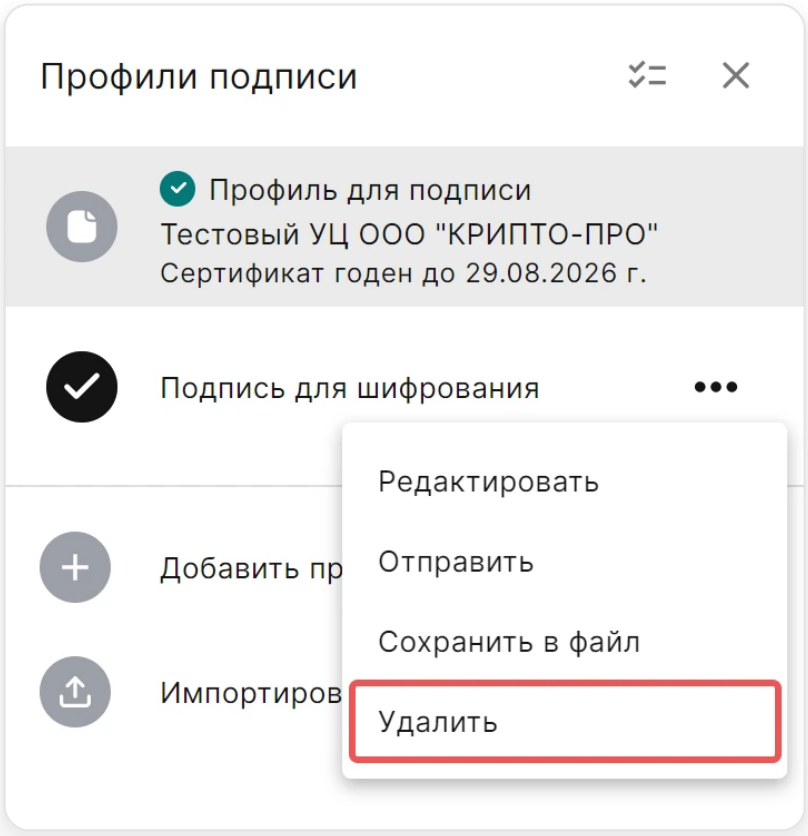
Удаление профилей подписи

> ⚠️ **Примечание**: Активный профиль удалить невозможно. Сначала переключитесь на другой профиль. Это ограничение предотвращает случайное удаление профиля, который используется в данный момент.

Как удалить профиль подписи

1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Наведите курсор на тот профиль, который хотите удалить.

4. Нажмите на кнопку **Еще** ••• и выберите действие **Удалить**.

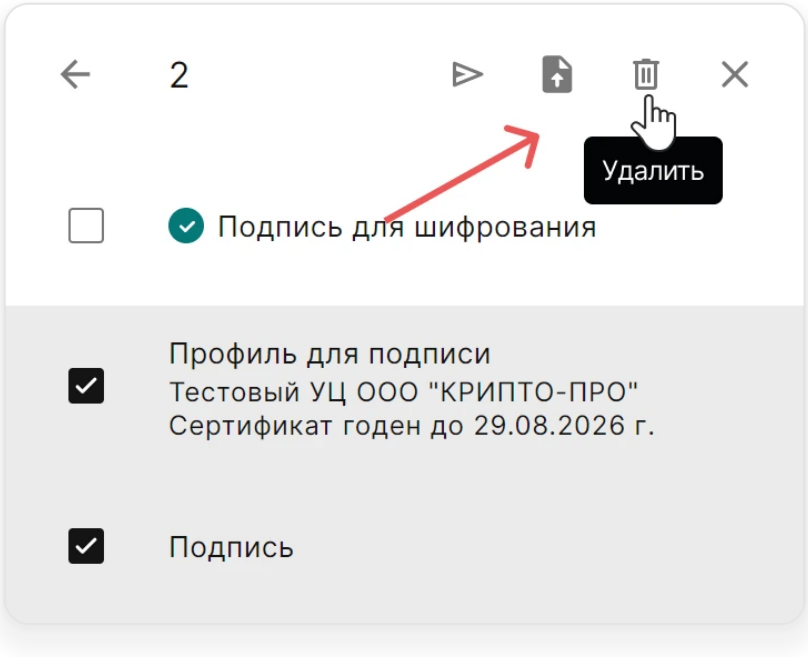


5. Подтвердите действие в модальном окне.

Профиль будет полностью удалён из приложения и больше не будет доступен для использования.

Групповое удаление

1. Перейдите в раздел **Документы** или в мастер **Подпись и шифрование**.
2. Нажмите на название активного профиля в верхней части окна.
3. В окне со списком профилей нажмите на кнопку **Выбрать** .
4. Отметьте флагами профили, которые вы хотите удалить.
5. Нажмите кнопку **Удалить** .



6. Подтвердите действие в модальном окне.

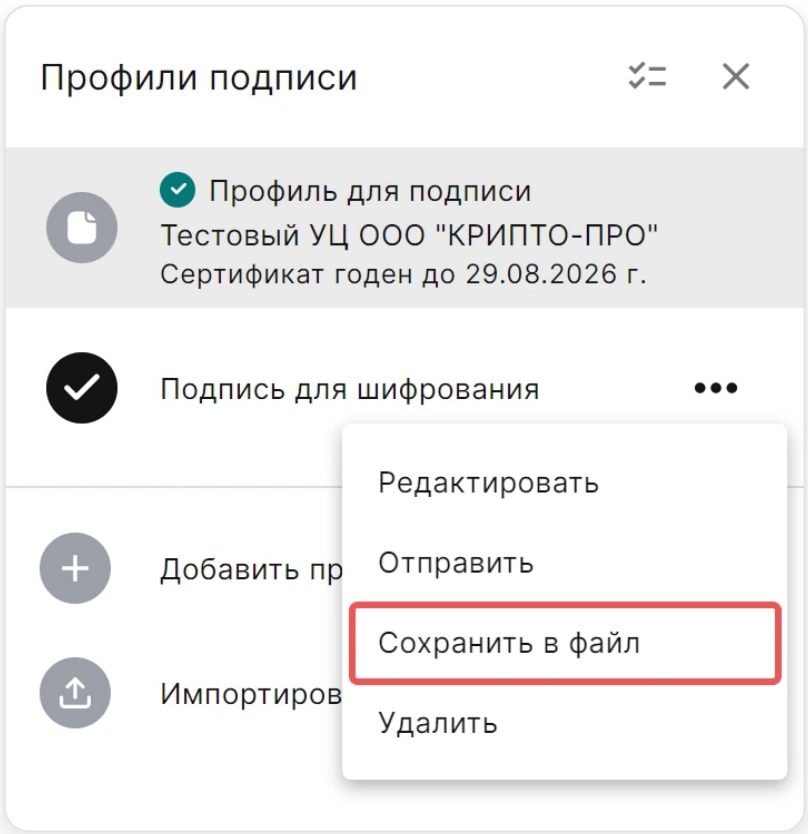
Групповое удаление удобно для очистки списка профилей от неиспользуемых или устаревших настроек.

Экспорт и импорт профилей подписи

Экспорт профиля в файл

Экспорт профиля подписи позволяет сохранить настройки в файл для резервного копирования, переноса на другой компьютер или передачи коллегам.

1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Наведите курсор на профиль, который необходимо экспортировать.
4. Нажмите на появившуюся кнопку **Еще** ••• и выберите действие **Сохранить в файл**.



5. Укажите путь для сохранения файла с профилем.

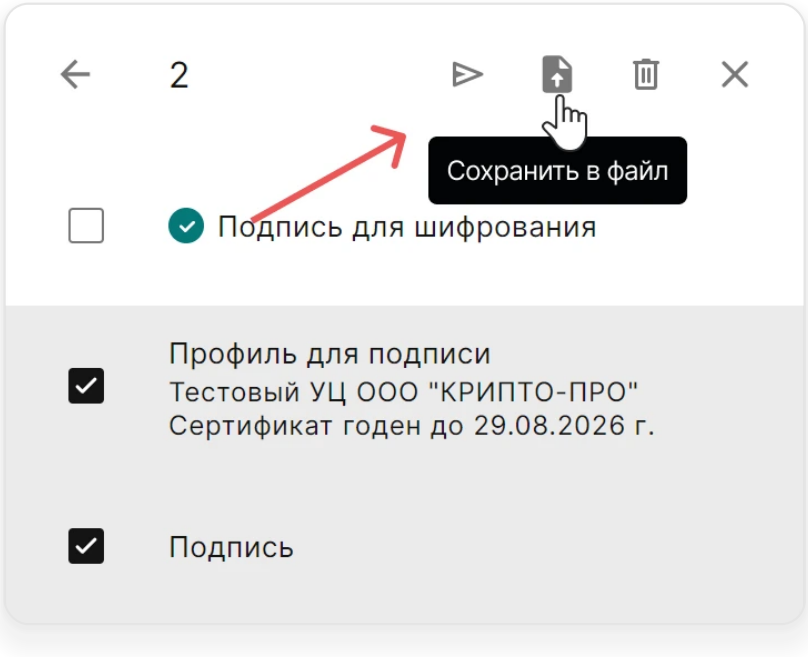
В результате по указанному пути будет сохранен в файл с расширением `.pcarm`.

Файл профиля можно использовать для последующего импорта в КриптоАРМ на этом или другом устройстве.

Групповой экспорт

> 💡 Групповой экспорт позволяет сохранить сразу несколько профилей в один файл.

1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Нажмите кнопку **Выбрать** .
4. Отметьте флагами профили, которые вы хотите экспортировать.
5. Нажмите кнопку **Сохранить в файл**.



6. Укажите путь для сохранения файла профиля.

Профили будут сохранены в файл с расширением `.pcarm`.

Отправка профиля по почте

> ⚠️ **Примечание**: Для отправки профилей подписи по почте в приложении должен быть подключен почтовый аккаунт.

1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Наведите курсор на профиль, который необходимо отправить.
4. Нажмите на появившуюся кнопку **Еще** ••• и выберите действие **Отправить**.
5. Откроется вкладка **Новое письмо**, в котором во вложении будет прикреплен профиль подписи с расширением `.pcarm`.
6. Заполните обязательные поля и отправьте письмо.

Групповая отправка по почте

> 💡 Групповая отправка позволяет отправить сразу несколько профилей в одном письме.

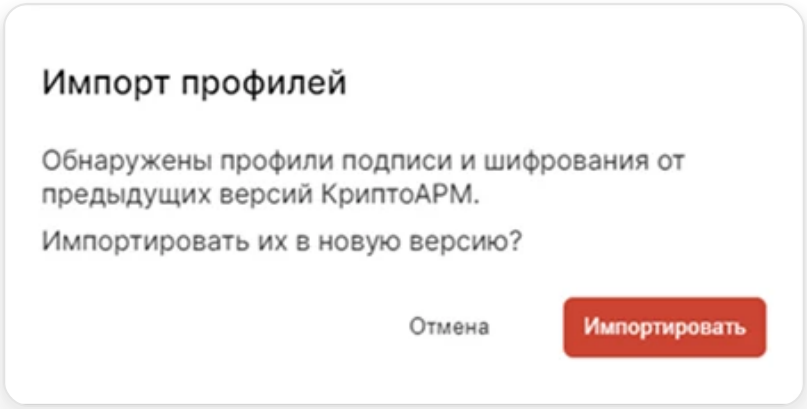
1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Нажмите кнопку **Выбрать** ☑.
4. Отметьте флагами профили, которые вы хотите отправить по почте.

5. Нажмите кнопку **Отправить** .
6. Откроется вкладка **Новое письмо**, в котором во вложении будет прикреплен профиль подписи с расширением `.pcarm`.

Импорт из других версий КриптоАРМ

Автоматический импорт доступен при первом запуске приложения.

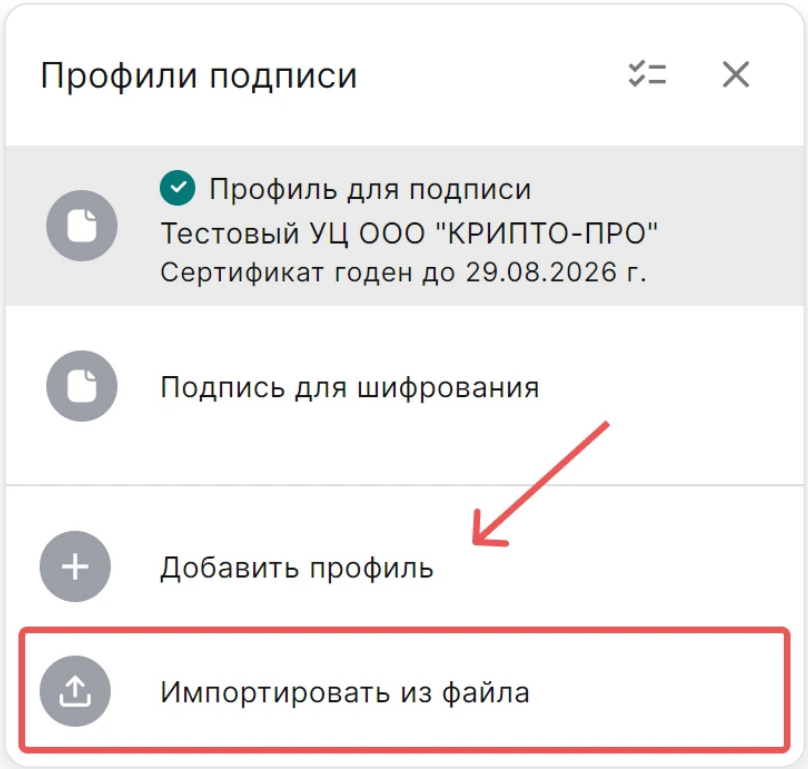
Если в системе будут обнаружены профили подписи из предыдущих версий КриптоАРМ, появится диалоговое окно с предложением импортировать эти профили.



Импорт профиля из файла

Способ 1 (из приложения):

1. Перейдите в раздел **Документы**.
2. Нажмите на название активного профиля в верхней части окна.
3. Нажмите кнопку **Импортировать из файла**.



4. В открывшемся окне файлового менеджера выберите файл профиля подписи в формате `.pcarm`, `.json` или `.xml`.
5. При успешном импорте профиль сохранится в приложении и будет отображаться в списке профилей.

Способ 2 (из файловой системы):

1. Дважды кликните по файлу, либо правой кнопкой мыши вызовите контекстное меню для файла и выберите пункт **Открыть с помощью КриптоАРМ**.
2. После выполнения данных действий запустится приложение КриптоАРМ (если не было запущено) и профиль автоматически импортируется в приложение.

Импорт профиля из письма

1. Перейдите в раздел **Почта**.
2. Откройте письмо, которое содержит во вложении профиль подписи в формате `.pcarm`.
3. Выполните действие одним из способов:
   - Кликните по названию файла в формате `.pcarm`,
   - Вызовите меню действий с вложением по кнопке **Еще** и выберите действие **Импортировать профиль**.

Смотрите также

- Подпись и шифрование — руководство по созданию электронных подписей и шифрованию файлов.
- Проверка и расшифрование — проверка подписей и расшифрование документов.
- Подпись и защита PDF — работа с PDF: просмотр, разметка областей, добавление подписей и сертифицирующая подпись.

Открыть статью на сайте

Подпись и шифрование документов

В этой инструкции вы научитесь подписывать и шифровать документы в КриптоАРМ с помощью мастера **Подпись и шифрование**. С его помощью вы легко подпишете несколько документов одновременно, защитите их шифрованием и выполните смешанные операции — например, сначала подпись, а затем шифрование.

Содержание:

- Работа с пошаговым мастером
- Подпись со стандартом CAdES
- Подпись со стандартом PAdES
- Подпись с созданием печатной формы
- Подпись сертификатом DSS
- Добавление соподписи
- Объединение подписей
- Шифрование
- Действия в мастере
- Возможные ошибки
- Смотрите также

> 💡 **Совет**: Для расширенной работы с одним PDF-документом (разметка области штампа, добавление подписантов и пр.) используйте мастер Подпись и защита PDF.

Работа с пошаговым мастером

Мастер **Подпись и шифрование** состоит из нескольких последовательных шагов:

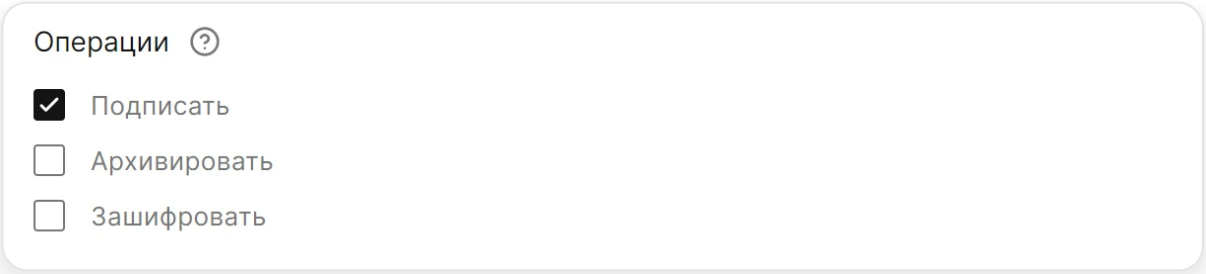
1. **Добавление документов** — выбор файлов для обработки.
2. **Настройка операции** — выбор операции (подпись, шифрование или их комбинация) и основных параметров.
3. **Подтверждение** — проверка выбранных документов и параметров перед выполнением операции.
4. **Выполнение операции** — создание подписи или шифрование документов.

> 💡 **Примечание**: настройки операции могут быть пропущены, если в профиле подписи не установлена настройка **Показывать настройки перед выполнением операции**.

Подпись со стандартом CAdES

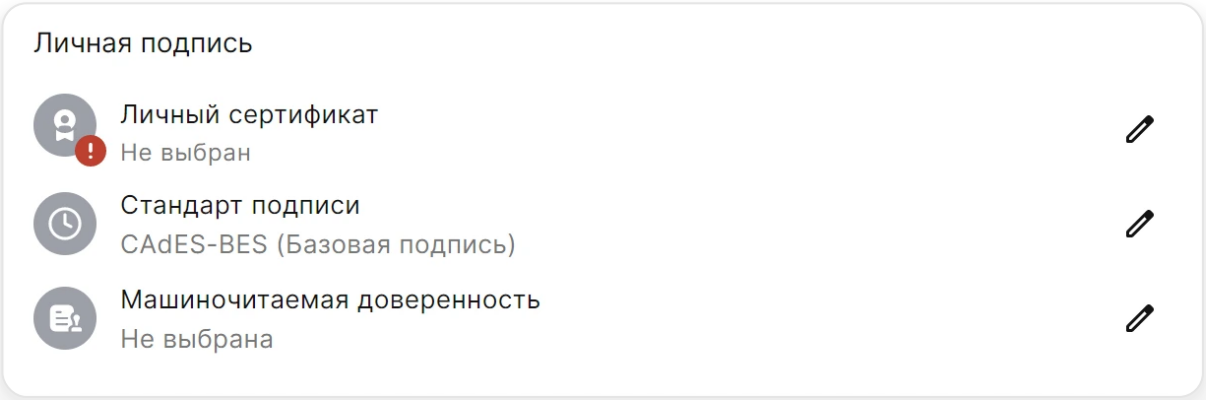
Чтобы подписать файлы со стандартом CAdES:

1. Запустите мастер (см. Запуск мастера).
2. Добавьте файлы в мастер (см. Добавление документов).
3. Нажмите **Далее**.
4. На шаге с настройками установите настройки подписи. По умолчанию используются параметры активного профиля подписи.
5. В блоке **Операции** выберите действие **Подписать**.



6. В блоке **Личная подпись** укажите:
   - **Личный сертификат** (см. Выбор сертификата подписи),
   - **Стандарт подписи** (см. Выбор стандарта подписи),
   - **Машиночитаемую доверенность** (см. Выбор машиночитаемой доверенности).

> 💡 **Примечание**: Если в системе присутствует только один подходящий личный сертификат (с закрытым ключом), он будет автоматически выбран в поле **Личный сертификат**.



7. При необходимости раскройте блок **Настройки подписи** и измените дополнительные параметры:
   - Вид подписи: **Отсоединенная**, **Присоединенная**,
   - Формат файла подписи: **.bin**, **.p7s**, **.sgn**, .**sign**, **.bin**,
   - Данные в подписи: **Сертификат владельца**, **Цепочка без корневого сертификата**, **Все сертификаты цепочки**,
   - Кодировка подписи: **DER**, **BASE-64**,
   - Отключение служебных заголовков.
8. Укажите настройки сохранения результата операции:
   - Сохранить файл в папке с исходным документом или выбрать другую папку,
   - Добавлять пользовательский суффикс,
   - Добавлять ФИО подписанта,
   - Отдельный архив на каждый файл,
   - Создать копию результата в папке **Архив**,

> 💡 **Примечание**: Подробнее про настройки читайте в инструкции Настройки подписи и шифрования.

9. Нажмите кнопку **Далее**.
10. Перед началом подписания появится окно подтверждения (см. Подтверждение операции). Нажмите кнопку **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.
11. Если контейнер закрытого ключа имеет пароль, то необходимо ввести его в окне криптопровайдера.

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

Если операция прошла успешно, подписанные файлы будут сохранены в соответствии с указанными настройками.

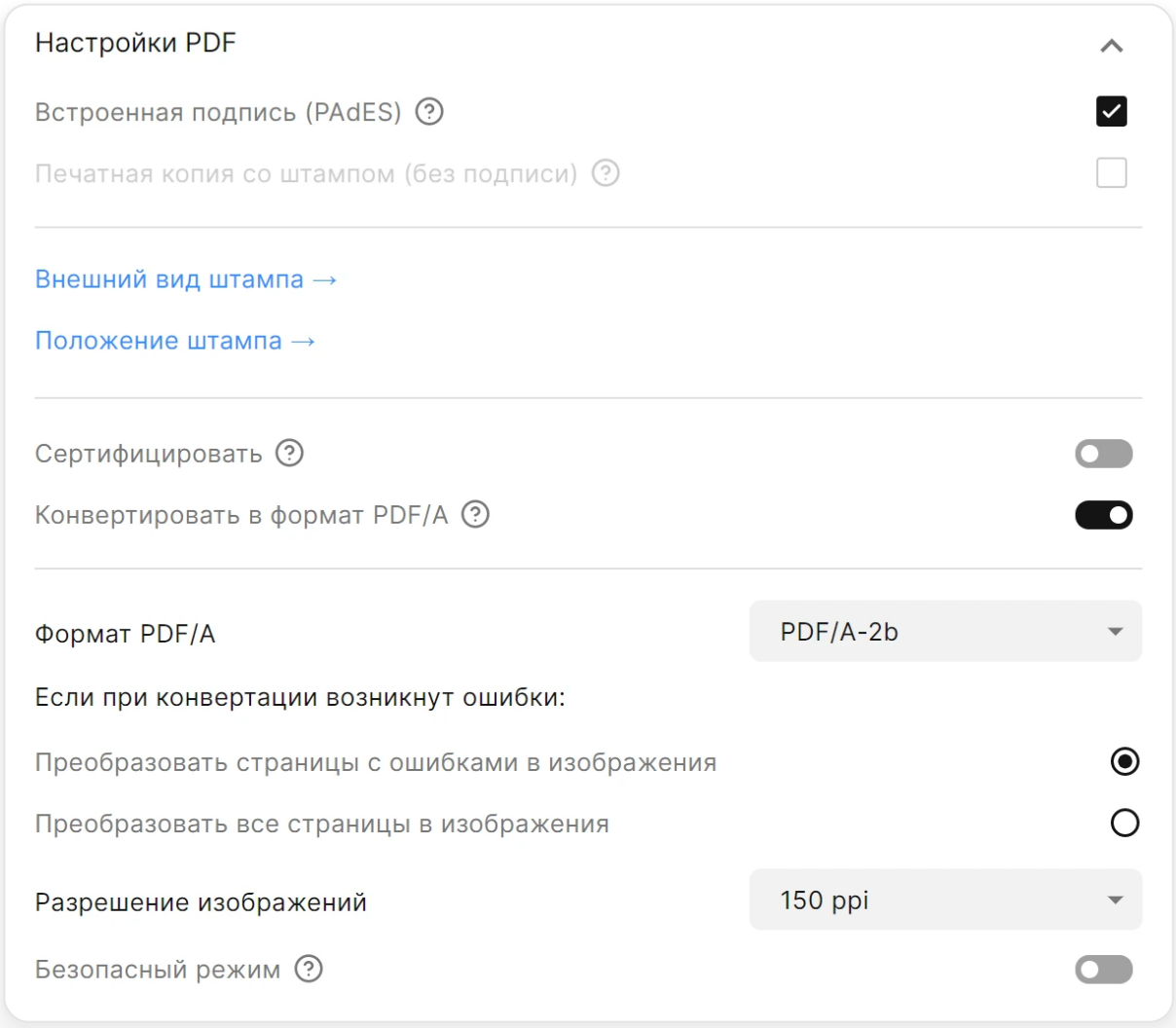
> 💡 В окне с результатами операции вы можете ознакомиться с информацией о подписи, отправить файл по электронной почте, сохранить его в **Архиве** и многое другое. Подробнее читайте в инструкции Управление документами.

Подпись со стандартом PAdES

Чтобы подписать файлы со стандартом PAdES:

1. Откройте мастер, добавьте файлы по аналогии с инструкцией Подпись со стандартом CAdES.

2. На шаге с настройками раскройте блок **Настройки PDF** и установите флажок **Встроенная подпись (PAdES)**.



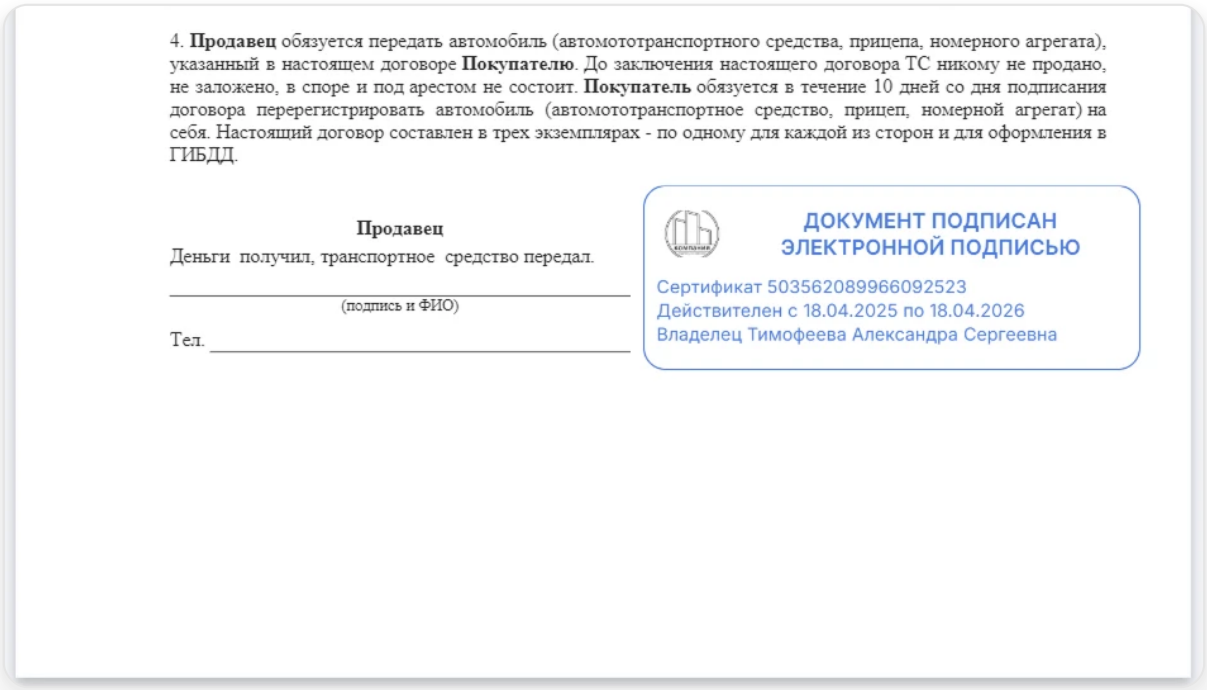
3. Далее настройте:

   - Положение штампа подписи на странице документа (см. Настройка положения штампа),
   - Оформление штампа подписи (см. Настройка внешнего вида штампа),
   - При необходимости включите опцию **Сертифицировать** для создания сертифицирующей подписи,
   - При необходимости включите опцию **Конвертировать в формат PDF/A**, чтобы удалить потенциально опасные элементы.

4. Укажите настройки для сохранения результата операции и нажмите кнопку **Далее**.

Далее выполните стандартные шаги завершения операции подписи: подтверждение операции, ввод пароля контейнера (при необходимости) и ожидание результата (см. инструкцию Подпись со стандартом CAdES).

Пример визуализации штампа подписи:



Подпись с созданием печатной формы

Печатная форма — копия исходного документа с графическим штампом подписи. Подробнее читайте в инструкции Операции в КриптоАРМ.

Чтобы подписать файлы с созданием печатной формы:

1. Откройте мастер, добавьте файлы по аналогии с инструкцией Подпись со стандартом CAdES.

   > ⚠️ **Примечание**: вы можете добавлять документы с любыми расширениями, однако печатная форма будет создана только для PDF-документов.

2. На шаге с настройками подписи раскройте блок **Настройки PDF** и установите флажок **Печатная копия со штампом (без подписи)**.

3. Далее настройте:

   - Положение штампа подписи на странице документа (см. Настройка положения штампа),
   - Оформление штампа подписи (см. Настройка внешнего вида штампа),

4. Укажите настройки для сохранения результата операции и нажмите кнопку **Далее**.

Далее выполните стандартные шаги завершения операции подписи: подтверждение операции, ввод пароля контейнера (при необходимости) и ожидание результата (см. инструкцию Подпись со стандартом CAdES).

Подпись сертификатом DSS

Сертификат DSS — сертификат электронной подписи, ключ от которого генерируется и хранится на сервере Удостоверяющего центра. Благодаря этому владельцу сертификата не требуется записывать и хранить ключ на токене или компьютере. Это позволяет ему подписывать электронные документы с любого устройства и из любого места, где есть доступ в интернет.

Подпись документов с помощью сертификата DSS имеет следующие особенности:

1. **Ограниченные настройки подписи**:
    - Недоступен выбор стандарта подписи PAdES,
    - Отсутствует возможность установки штампов времени.
2. **Процесс аутентификации**:
    - Нужен доступ к интернету,
    - Иногда требуются дополнительные методы подтверждения.

Как подписать сертификатом DSS

> ⚠️ **Примечание**: Для DSS подписи не требуется лицензия на программный продукт КриптоПро CSP.

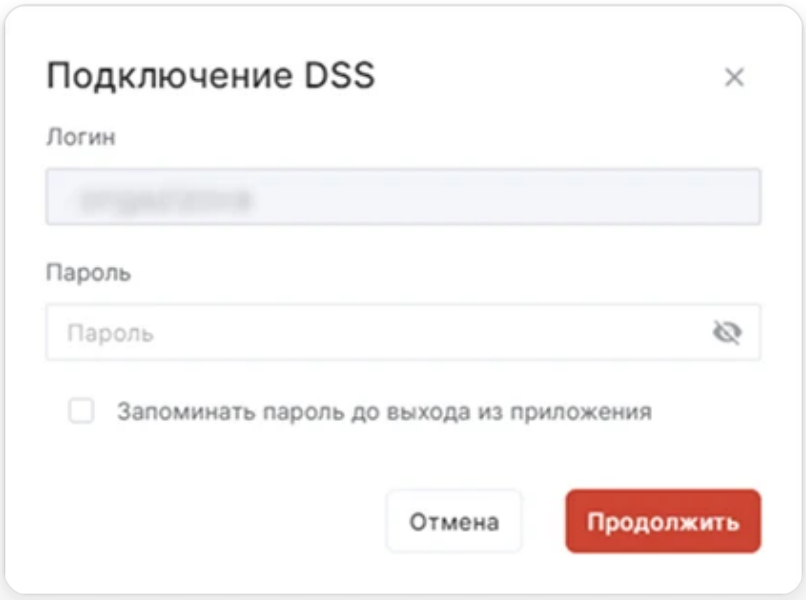
Процесс подписи с использованием сертификата DSS не отличается от подписи с помощью обычного сертификата, за исключением нескольких шагов.

1. Откройте мастер, добавьте файлы по аналогии с инструкцией Подпись со стандартом CAdES.
2. На шаге с настройками подписи выберите DSS-сертификат в блоке **Личная подпись**.
3. Укажите настройки для сохранения результата операции и нажмите кнопку **Далее**.

   Далее выполните стандартные шаги завершения операции подписи: подтверждение операции, ввод пароля контейнера (при необходимости) и ожидание результата (см. инструкцию Подпись со стандартом CAdES).
4. При необходимости пройдите аутентификацию в DSS-сервисе.

В зависимости от настроек вашего DSS-провайдера может быть открыто окно аутентификации:

- **Ввод пароля** — если для аутентификации задан пароль и срок действия токена истёк. Введите пароль и нажмите **Продолжить**.



- **Подтверждение через устройство** — если для аутентификации задан вход по SIM-карте или через мобильное приложение, и срок действия токена истёк. Подтвердите вход на устройстве.

Если токен действителен, шаги аутентификации пропускаются.

5. После аутентификации подтвердите операцию подписи на устройстве. Способ подтверждения зависит от DSS-провайдера: через SIM-карту или мобильное приложение.

Добавление соподписи

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

> ⚠️ **Примечание**: Статус документа с соподписями считается действительным в случае **действительности** всех подписей.

Если исходный документ содержит присоединённую подпись, рекомендуется делать соподпись также присоединённой, чтобы все подписи хранились в одном файле.

Если исходный документ содержит отсоединённую подпись, соподпись лучше делать отсоединённой, чтобы сохранить согласованную схему хранения подписей.

Процесс добавления соподписи идентичен процедуре первичной подписи документа.

Для выполнения соподписи следуйте инструкциям:

- Подпись со стандартом CAdES — для группового подписания любых файлов по стандарту CAdES.
- Подпись со стандартом PAdES — для группового подписания PDF-файлов по стандарту PAdES.
- Подпись PDF-документа — для подписания одного PDF-файла по стандарту PAdES с ручной разметкой области для штампа подписи.
- Подпись PDF-документа в размеченной области — для создания подписи в заранее размеченной области.

> 💡 **Совет**: Перед добавлением подписи убедитесь, что исходный документ не был изменён после предыдущего подписания и все предыдущие подписи действительны.

Объединение подписей

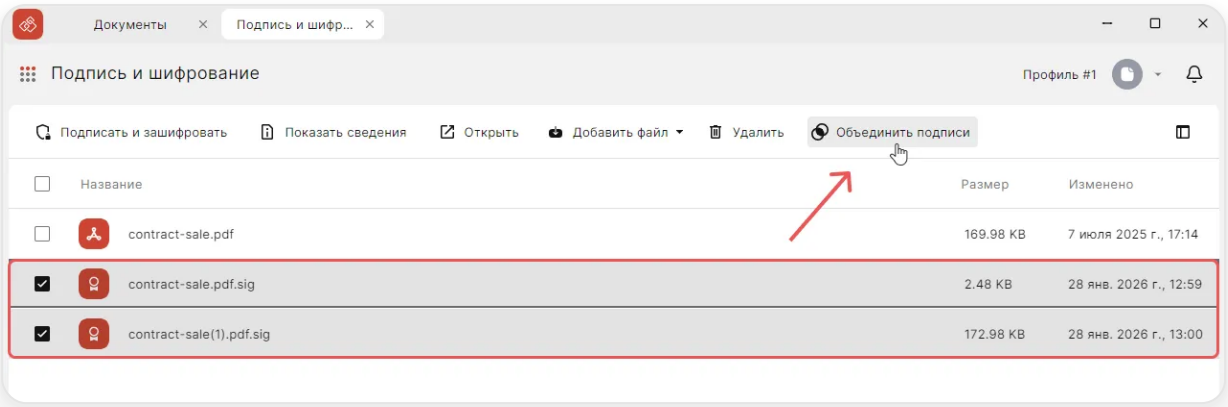
Функция **Объединение подписей** позволяет объединять несколько **отсоединенных подписей** в один файл подписи. Это удобно, когда:

- Необходимо создать **единый файл подписи** для документа, подписанного разными участниками;
- Требуется оптимизировать хранение подписей;
- Нужно подготовить файл для последующей проверки или архивации.

> 💡 **Примечание:** Объединенные подписи сохраняются отдельно и не изменяют исходные файлы.

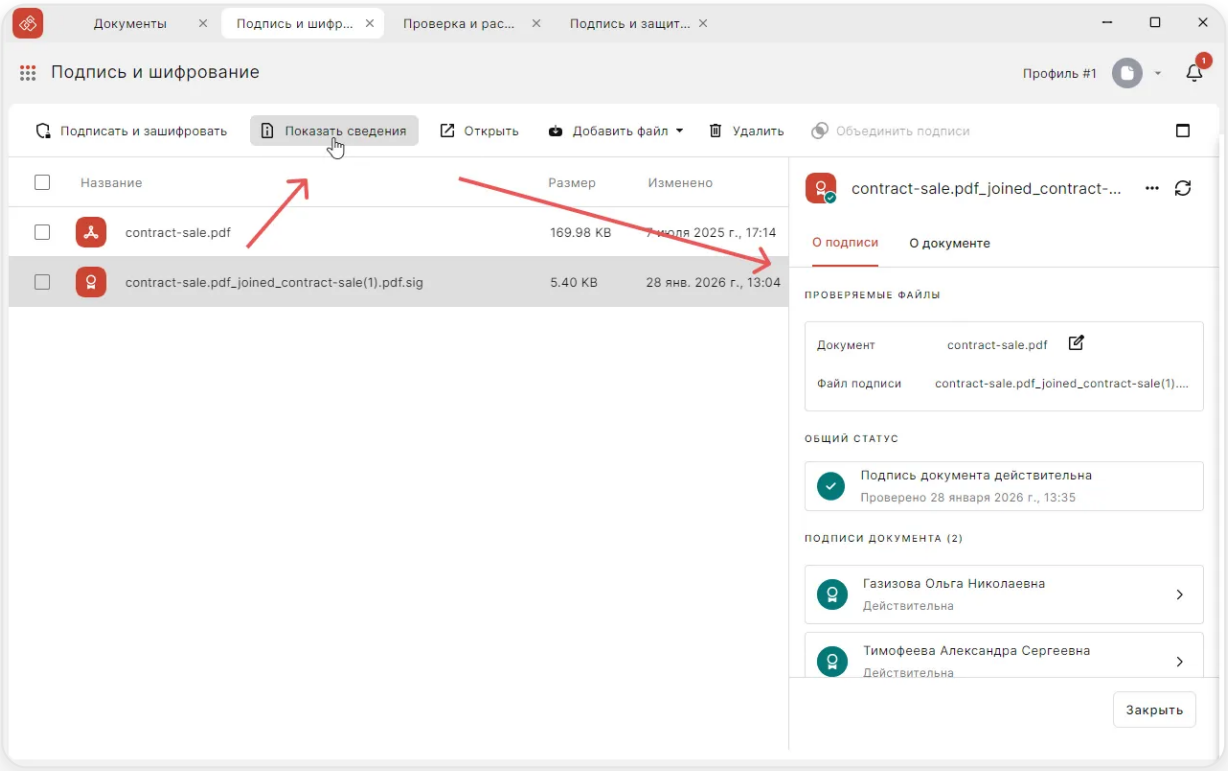
Как объединить подписи

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте файлы с отсоединенными подписями в мастер (см. Добавление документов).
3. Отметьте файлы для объединения с помощью **чекбоксов**.
4. Нажмите кнопку **Объединить подписи**.



- После нажатия выбранные подписи объединяются в **один новый файл**.
- Исходные файлы остаются без изменений, а новый файл получает суффикс `_joined_[количество_подписей]_signs` в названии.

5. Файл сохраняется в папку с исходными подписями.
   - Если исходные подписи находились в разных папках, файл сохраняется в **папке первого файла из списка**.
6. После завершения операции можно сразу проверить результат:
   - В списке файлов **выделите созданный объединённый файл** (с суффиксом `_joined_[количество_подписей]_signs`).
   - Нажмите **Показать сведения** на панели действий.



В открывшемся окне вы сможете увидеть общий статус подписи документа и список всех объединённых подписей.

> 💡 **Совет:** Если при проверке подписи появилось сообщение **Не удалось найти исходный файл для подписи**, укажите путь к исходному файлу документа. Это позволит приложению правильно связать подпись с исходным файлом и корректно отобразить сведения.

Шифрование

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, приложение выполняет шифрование данных в адрес этих сертификатов. Получатели могут расшифровать информацию с помощью своего закрытого ключа.

> 💡 **Совет**: Всегда добавляйте **свой личный сертификат** к списку получателей, если вы планируете в дальнейшем расшифровывать файл.

Как зашифровать файлы

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте файлы в мастер (см. Добавление документов).
3. На шаге с настройками выберите действие **Зашифровать**.
4. Если необходимо создать зашифрованный архив, выберите **Архивировать**. В этом случае все файлы будут помещены в общий архив, который затем будет зашифрован.
5. Добавьте сертификаты получателей в блоке **Сертификаты шифрования** (см. Выбор сертификатов шифрования).

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

6. При необходимости раскройте блок **Настройки шифрования** и измените дополнительные параметры операции.

7. Укажите настройки для сохранения результата операции и нажмите кнопку **Далее**.
8. Перед началом подписания появится окно подтверждения (см. Подтверждение операции). Нажмите кнопку **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.

Если операция прошла успешно, подписанные файлы будут сохранены в соответствии с указанными настройками.

Действия в мастере

Некоторые действия универсальны и необходимы для выполнения любой операции.

Запуск мастера

Мастер **Подпись и шифрование** можно открыть следующими способами:

- Из раздела **Документы**: на панели действий нажмите **Подпись и шифрование**.
- Из папки **Архив**, результатов операции или раздела **Почта**. Выберите файл, затем нажмите **Добавить в** → **Подпись и шифрование**.
- Из глобального меню: нажмите кнопку глобального меню и выберите **Подпись и шифрование**.

После выполнения любого из этих действий мастер откроется в новой вкладке.

Добавление документов

Добавьте документы одним из способов:

1. Перетащите один или несколько файлов в окно приложения.
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

> 💡 **Совет**: Вы можете перетаскивать в мастер не только файлы, но и папки. При этом все файлы из вложенных папок также будут добавлены в мастер.

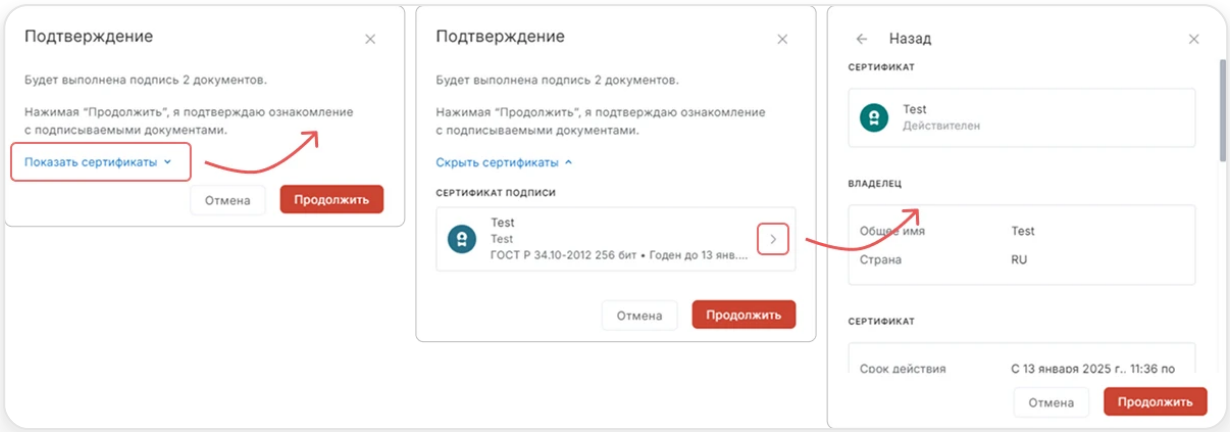
Подтверждение операции

Перед выполнением операции запрашивается ее подтверждение в отдельном окне. Окно содержит сведения о количестве документов, выполняемой операции и сертификатах, которые будут использоваться для подписи или шифрования. При необходимости в этом окне можно удалить лишние сертификаты получателей перед началом операции.

Чтобы подтвердить операцию:

1. Ознакомьтесь со сведениями в окне **Подтверждение**.

Чтобы просмотреть информацию о сертификате, нажмите на кнопку **Показать сертификат**. После этого нажмите на панель с сертификатом.



Перед шифрованием убедитесь, что в списке остались сертификаты получателей, которым необходимо предоставить доступ к зашифрованному документу. Если в списке присутствуют лишние сертификаты, их можно удалить. Для этого наведите курсор на иконку сертификата и нажмите **Удалить**.

2. Нажмите кнопку **Продолжить**, чтобы подтвердить ознакомление с документами.

В окне с подтверждением операции может появиться дополнительное уведомление, если:

- Сертификат подписи или шифрования недействителен,
- Срок действия открытого или закрытого ключа личного сертификата 30 дней и менее,
- Сертификат подписи машиночитаемой доверенности недействительный или сведения о владельце сертификата подписи отличаются от данных в машиночитаемой доверенности.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

> ⚠️ **Примечание**: Коды ошибок (0x...) фиксируются для криптопровайдера КриптоПро CSP.

Общие ошибки

Код ошибки	Ошибка	Рекомендуемые действия
-	**Не удалось открыть файл**	1. Проверьте наличие и доступность файлов 2. Убедитесь, что файлы не

Код ошибки	Ошибка	Рекомендуемые действия
		пустые (имеют ненулевой размер) 3. Повторите добавление файлов в мастер
-	**Не удалось подписать файл**	1. Проверьте права доступа к папке, указанной для сохранения результатов 2. Освободите место на диске
-	**Отсутствует необходимый криптопровайдер. Алгоритм открытого ключа сертификата: ГОСТ Р 34.10-2012 256 бит**	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
-	**Отсутствует действующая лицензия КриптоАРМ**	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
0x8009001d	**Отсутствует действующая лицензия КриптоПро CSP**	Установите лицензию КриптоПро CSP
0xc2100140	**Отсутствует лицензия на модуль КриптоПро TSP Client**	Приобретите и установите лицензию TSP Client
0xc2110140	**Отсутствует лицензия на модуль КриптоПро OCSP Client**	Приобретите и установите OCSP Client
-	**Не установлены модули TSP/ OCSP Client**	Установите недостающие модули
-	**Не выбран сертификат подписи**	Выберите сертификат в настройках подписи
-	**Не указан адрес службы TSP**	Введите корректный адрес TSP-сервера
0x80072ee7	**Некорректный адрес службы TSP**	1. Проверьте правильность введенного адреса 2. Убедитесь в доступности сервера
-	**Сертификат не подходит для усовершенствованной подписи**	Выберите подходящий сертификат или измените настройки стандарта подписи
-	**Не указан адрес прокси-сервера**	1. Введите корректный адрес прокси 2. Проверьте параметры сети
-	**Не указан порт прокси-сервера**	

Код ошибки	Ошибка	Рекомендуемые действия
		1. Укажите правильный порт прокси-сервера 2. Проверьте настройки подключения
0x80072ee6	**Некорректные настройки прокси**	1. Проверьте параметры прокси-сервера 2. Временно отключите прокси для тестирования
-	**Папка для сохранения не найдена**	1. Проверьте существование указанной папки 2. Создайте и укажите новую папку для результатов
-	**Файл МЧД поврежден или не обнаружен**	1. Проверьте целостность файла машиночитаемой доверенности 2. Запросите корректную версию файла
0x80072ee7	**Нет подключения к интернету**	1. Проверьте сетевое подключение 2. Убедитесь, что брандмауэр не блокирует соединение (Для подписей со штампами)

Ошибки при подписании PDF (PAdES и печатная форма)

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

Ошибки при шифровании

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файлов 2. Убедитесь, что файлы не пустые (имеют ненулевой размер) 3. Повторите добавление файлов в мастер
Не удалось зашифровать файл	1. Проверьте права доступа к папке, указанной для сохранения результатов 2. Освободите место на диске
Отсутствует криптопровайдер для выбранного алгоритма шифрования	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ

Смотрите также

- Профиль подписи — сохранение параметров операций в профилях для повторного использования.
- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.

Открыть статью на сайте

Проверка подписи и расшифрование документов

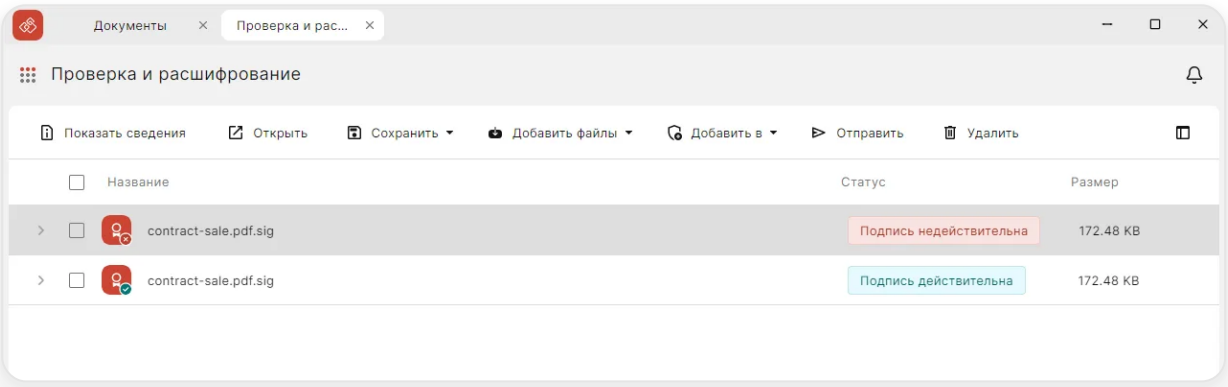
В этой инструкции вы научитесь работать с мастером **Проверка и расшифрование** в КриптоАРМ. Вы сможете проверить электронную подпись и просмотреть её подробные сведения, снять подпись с документа для получения исходного файла, а также расшифровать зашифрованные файлы.

Содержание:

- Проверка подписи
- Снятие подписи с документа
- Расшифрование документа
- Действия в мастере
- Возможные ошибки
- Смотрите также

Проверка подписи

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте файлы в мастер (см. Добавление документов).
3. Проверка запустится автоматически после добавления документов.
4. Статус подписи отобразится на панели с документом.
5. На иконке документа появится индикатор в виде:
   - зеленая галочка , если подпись действительная,
   - красный крестик, если недействительная.



Просмотр сведений о подписи документа

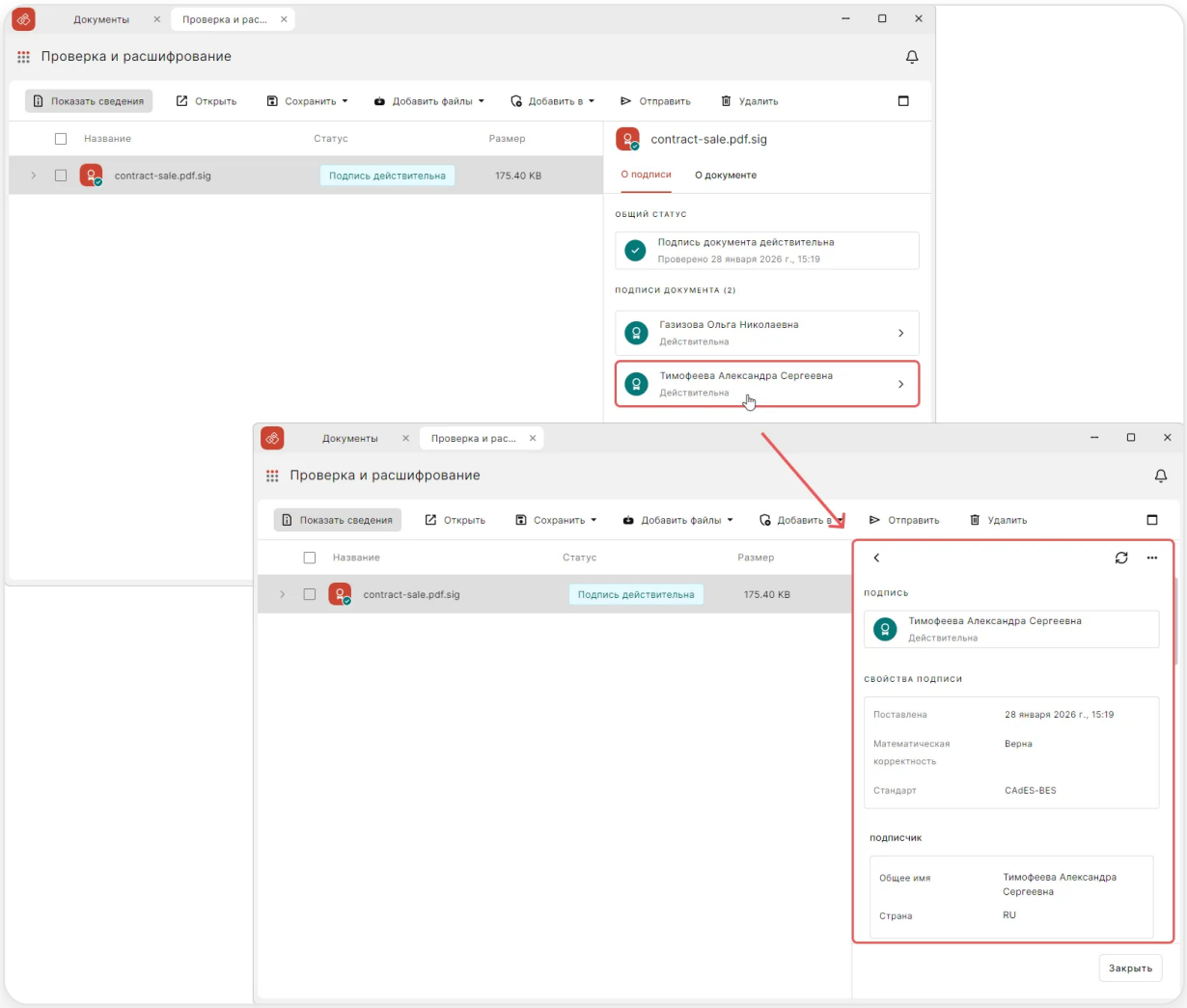
Чтобы просмотреть сведения о подписи документа:

1. Выполните шаги из инструкции Проверка подписи.
2. Нажмите на кнопку **Показать сведения** на панели действий.
3. В правой части окна отобразится область со сведениями о подписи.

> 💡 Просмотреть информацию о подписи и выполнить действия с ней можно не только в мастере **Проверка и расшифрование**, но и в мастере **Подпись и шифрование**, а также прямо в папках **Архив** и **Почтовые вложения**.

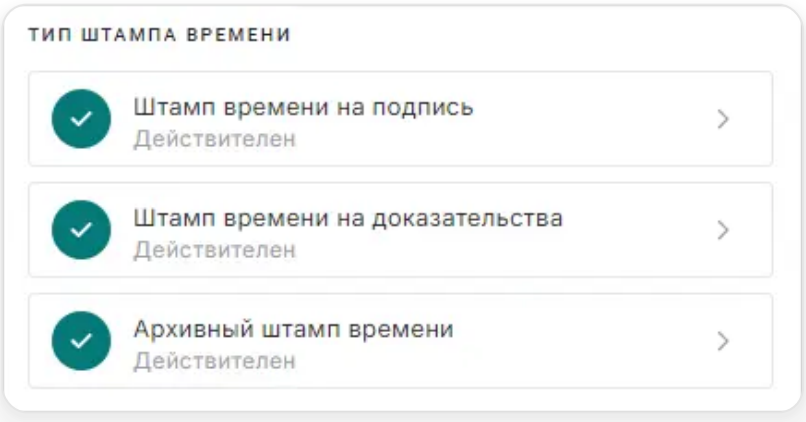
Просмотр сведений о подписи документа с соподписями

1. Выполните шаги из инструкции Проверка подписи для файла, содержащего соподписи.
2. Нажмите на кнопку **Показать сведения** на панели действий.
3. В правой части окна отобразится область со списком подписей.
4. Выберите подпись, сведения о которой необходимо просмотреть.
5. Отобразится подробная информация по выбранной подписи.



Просмотр сведений о штампе подписи

1. Выполните шаги из инструкции Просмотр сведений о подписи документа.
2. Выберите необходимый штамп в блоке **Тип штампа времени**.



3. Отобразится подробная информация по выбранному штампу.

Для усовершенствованных подписей доступны дополнительные блоки с данными проверки статуса:

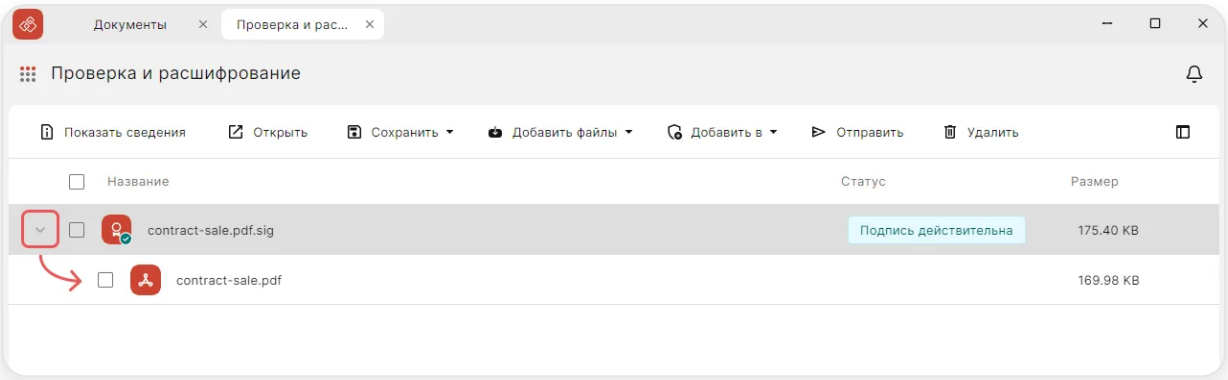
- Блок **Сертификат службы OCSP** содержит сертификат, использованный для подписания ответа OCSP.
- Блок **Ответ службы OCSP** содержит сам ответ с подтверждением статуса сертификата на момент подписания.

Почему подпись не проходит проверку

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
Отсутствует криптопровайдер с поддержкой ГОСТ Р 34.10-2012	✅ Можно исправить	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ. Инструкции по установке: Windows, macOS, Linux.

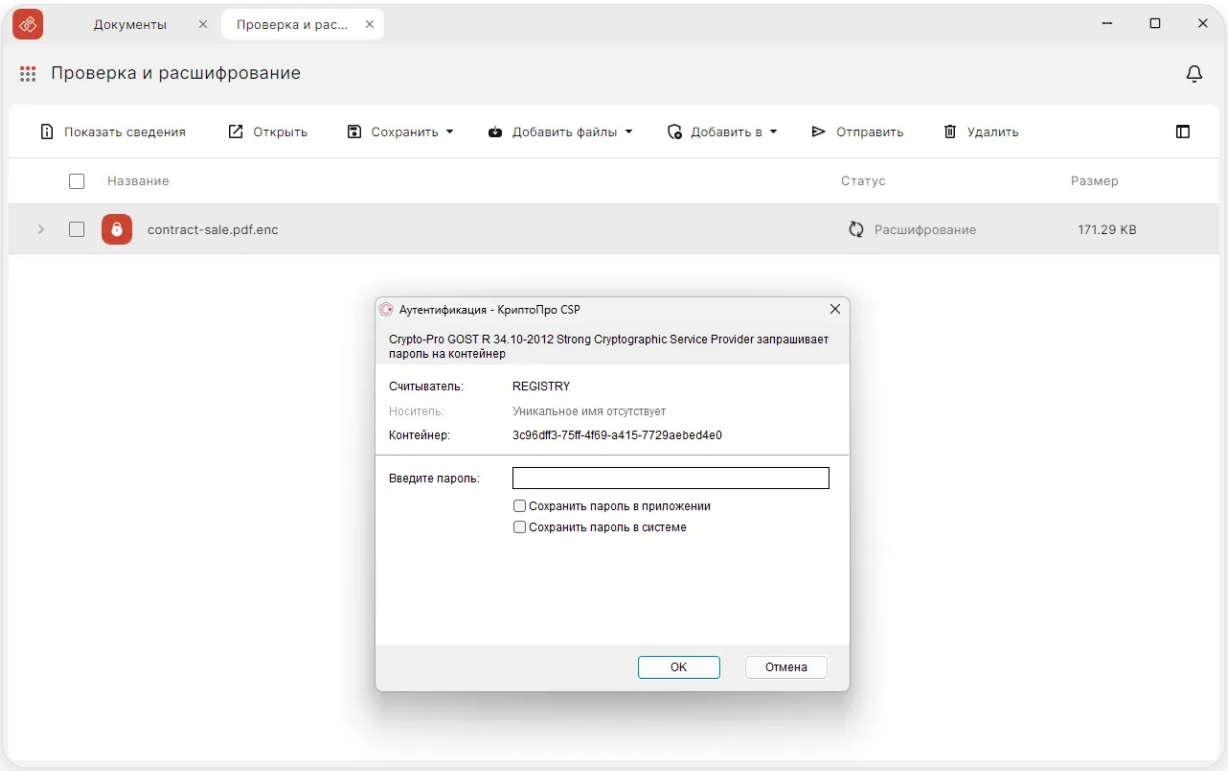
Снятие подписи с документа

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте файлы в мастер (см. Добавление документов).
3. После добавления документов запустится автоматическая проверка подписи.
4. Нажмите кнопку › слева от файла, с которого нужно снять подпись.
5. В списке отобразится исходный документ без подписи.
6. Выполните необходимое действие с документом.

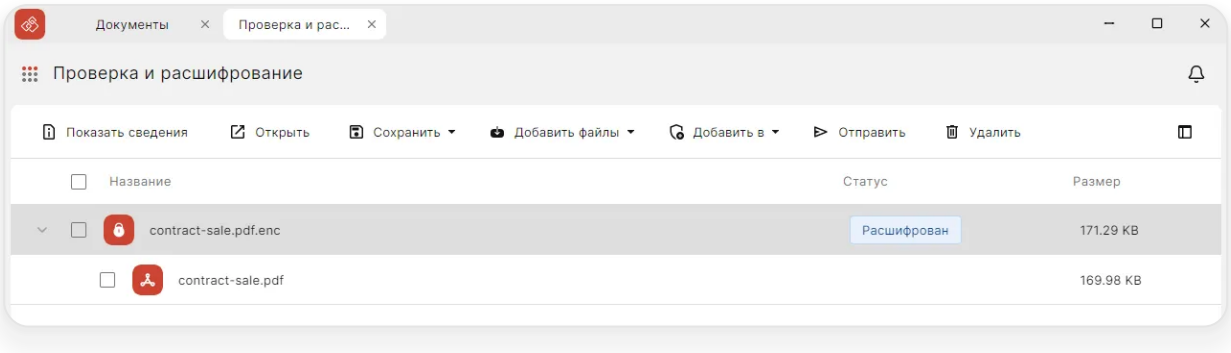


Расшифрование документа

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте файлы в мастер (см. Добавление документов).
3. После добавления документов запустится автоматическое расшифрование и проверка подписи (если есть).
4. Если потребуется, укажите пароль на контейнер с личным сертификатом.



5. Расшифрованный фаил отобразится под зашифрованным. На панели с зашифрованным документом отобразится статус «Расшифрован».



При успешном расшифровании полученные оригиналы документов сохраняются во временной папке и удаляются автоматически после закрытия приложения.

Чтобы сохранить расшифрованные файлы:

1. Выделите в списке файлы, которые нужно сохранить.
2. Выберите одно из действий:
   - **Сохранить** — для сохранения на компьютере или в **Архиве**,
   - **Отправить** — для отправки в качестве вложения в письме.

Действия в мастере

Некоторые действия универсальны и необходимы для выполнения любой операции.

Запуск мастера

Мастер **Проверка и расшифрование** можно открыть следующими способами:

- Из раздела **Документы**: на панели действий нажмите **Проверка и расшифрование**.
- Из папки **Архив**, результатов операции или раздела **Почта**. Выберите файл, затем нажмите **Добавить в** → **Проверка и расшифрование**.
- Из глобального меню: нажмите кнопку глобального меню и выберите **Проверка и расшифрование**.

После выполнения любого из этих действий мастер откроется в новой вкладке.

Добавление документов

Добавьте документы одним из способов:

1. Перетащите один или несколько файлов в окно приложения.
2. Загрузите с помощью кнопки **Загрузить с компьютера** или **Добавить из Архива**.

> 💡 **Совет**: Вы можете перетаскивать в мастер не только файлы, но и папки. При этом все файлы из вложенных папок также будут добавлены в мастер.

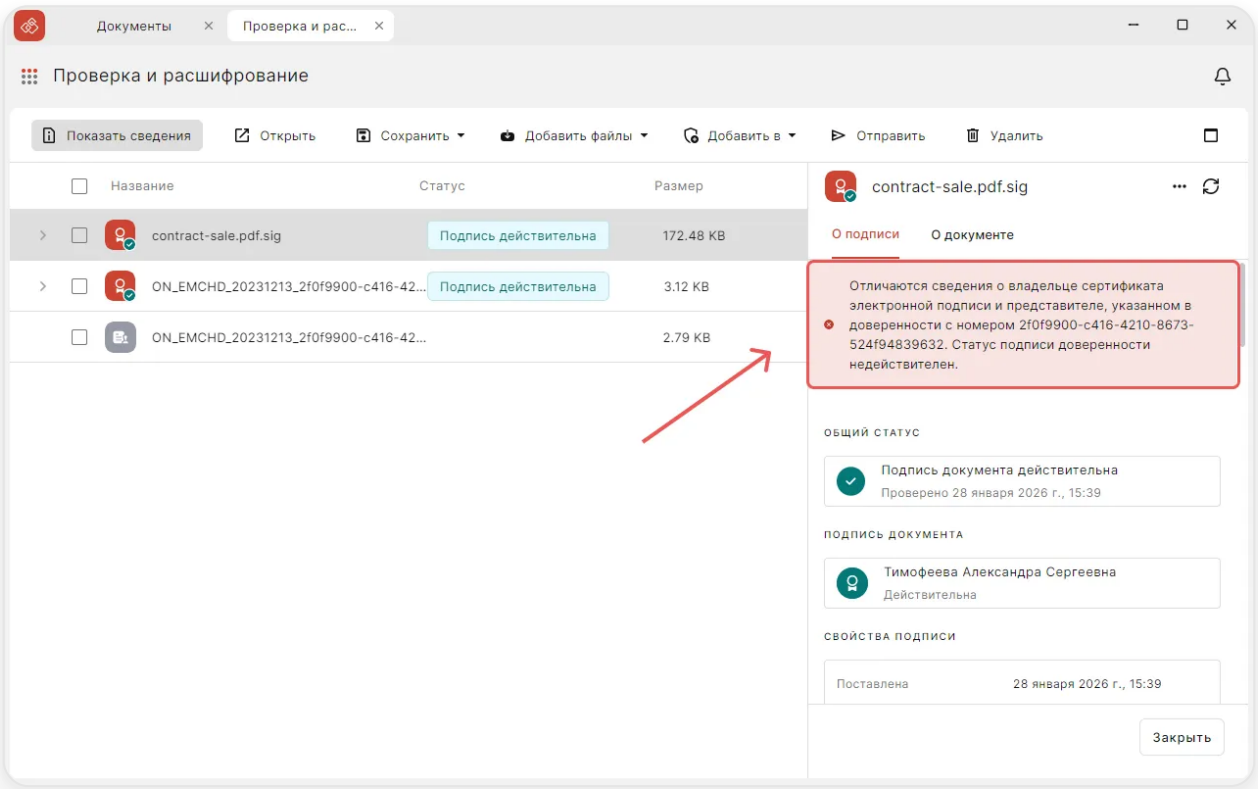
Проверка соответствия МЧД сертификату подписи

При проверке подписи производится дополнительная проверка данных владельца сертификата подписи и владельца машиночитаемой доверенности. Эта проверка осуществляется на основании реквизита ИНН.

> ⚠️ **Примечание**: Проверка доступна для документов, содержащих одну подпись.

Чтобы выполнить проверку:

1. Добавьте в мастер подписанные документы и машиночитаемую доверенность с файлом подписи.
2. Нажмите на кнопку **Показать сведения** .
3. В правой части окна отобразится область со сведениями о подписи. Если проверка не пройдет успешно, отобразится уведомление: «Сведения о владельце сертификата подписи отличаются от данных в машиночитаемой доверенности».



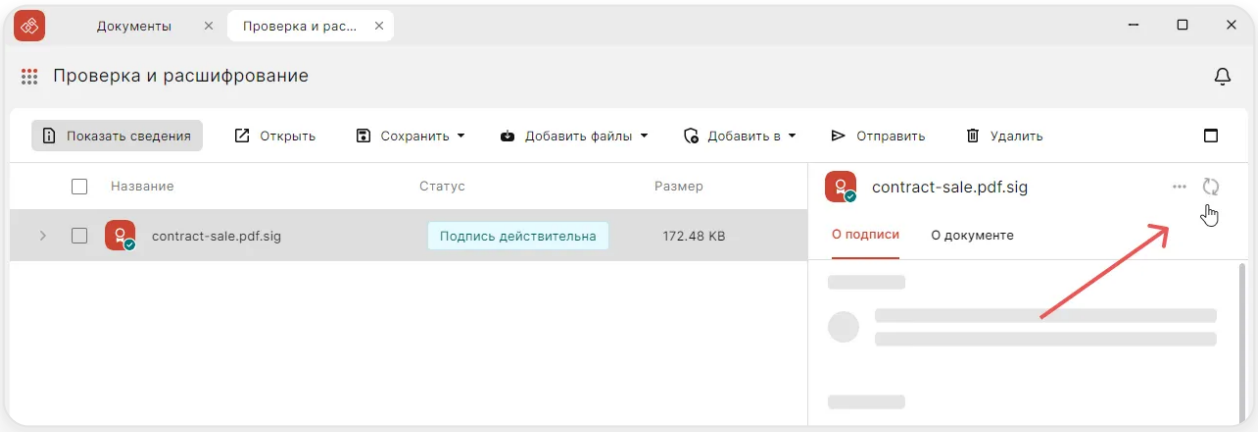
Обновление сведений о подписи

В некоторых случаях, например, при установке корневого или промежуточного сертификата, может потребоваться повторная проверка подписи документа.

Чтобы обновить сведения о подписи документа:

1. Выполните шаги из инструкции Просмотр сведений о подписи документа.
2. В области просмотра со сведениями о подписи нажмите на кнопку **Обновить** .

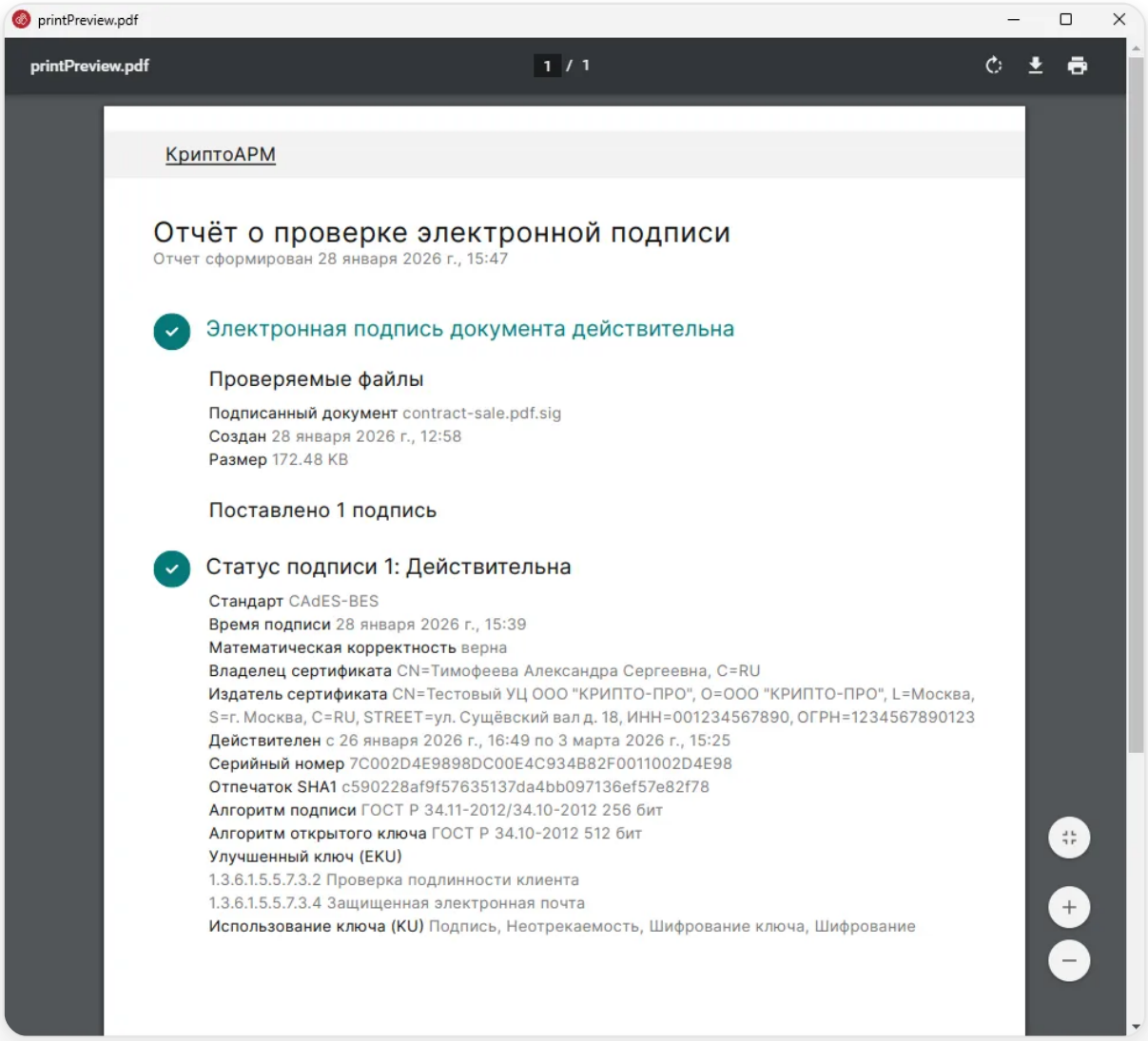
Сведения о подписи будут обновлены.



Отчет о проверке подписи

1. Выполните шаги из инструкции Просмотр сведений о подписи документа.
2. Нажмите на кнопку **Еще** и в появившемся меню выберите действие **Распечатать отчет**.
3. Откроется окно с отчетом о проверке электронной подписи.

Отчет можно распечатать или скачать на устройство.



Создание печатной формы

Для PDF-документов, подписанных подписью CAdES, доступно создание печатной формы с графическим штампом подписи. Подробнее о печатных формах читайте в инструкции Операции в КриптоАРМ.

Если документ содержит **несколько подписей**, в печатной форме будут отображены **все подписи** — для каждой подписи формируется отдельный штамп.

Чтобы создать печатную форму:

1. Выполните шаги из инструкции Просмотр сведений о подписи документа.
2. Нажмите на кнопку **Еще** ••• и в появившемся меню выберите действие **Создать печатную форму со штампом**.

Печатная форма сохранится в папку, в которой находится подписанный документ.

🚨 Вы можете создать печатную форму при подписании PDF-документа. Читайте подробнее в инструкции Подпись с созданием печатной формы.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ошибки при проверке подписи

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер
Не удалось найти исходный файл для подписи	Добавьте в мастер исходный файл, для которого была сделана отсоединенная подпись, либо укажите путь к файлу в области справа.

Ошибки при снятии подписи

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер
Нельзя снять открепённую подпись с файла	При открепленной подписи оригинал документа и так находится в отдельном файле

Ошибки при расшифровании

Ошибка	Рекомендуемые действия
Не удалось открыть файл	1. Проверьте наличие и доступность файла 2. Повторите добавление файла в мастер
Не удалось расшифровать файл	1. Убедитесь, что файл не пустой (имеет ненулевой размер). 2. Убедитесь в наличии сертификата для расшифрования.
Не удалось расшифровать файл	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Отсутствует действующая лицензия КриптоАРМ	1. Приобретите или продлите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы

Ошибка	Рекомендуемые действия
Отсутствует действующая лицензия КриптоПро CSP	Установите лицензию КриптоПро CSP

Смотрите также

- Профиль подписи — сохранение параметров операций в профилях для повторного использования.
- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.

Открыть статью на сайте

Подпись и защита PDF

В этой инструкции вы научитесь работать с мастером **Подпись и защита PDF** в КриптоАРМ. Он позволяет создавать обычные и сертифицирующие подписи с видимым штампом, а также выполнять конвертацию документов в PDF/A.

Содержание:

- Просмотр PDF-документа
- Создание подписи PDF-документа
- Сертифицирующая подпись PDF-документа
- Создание подписи с конвертацией в PDF/A
- Создание подписи в размеченной области
- Проверка подписи PDF-документа
- Действия в мастере
- Возможные ошибки
- Смотрите также

> 💡 **Совет**: Для подписи нескольких PDF-документов одновременно удобнее воспользоваться мастером Подпись и шифрование. Он поддерживает групповые операции создания подписей, архивирования и шифрования, а также работает как со стандартом CAdES, так и PAdES.

Просмотр PDF-документа

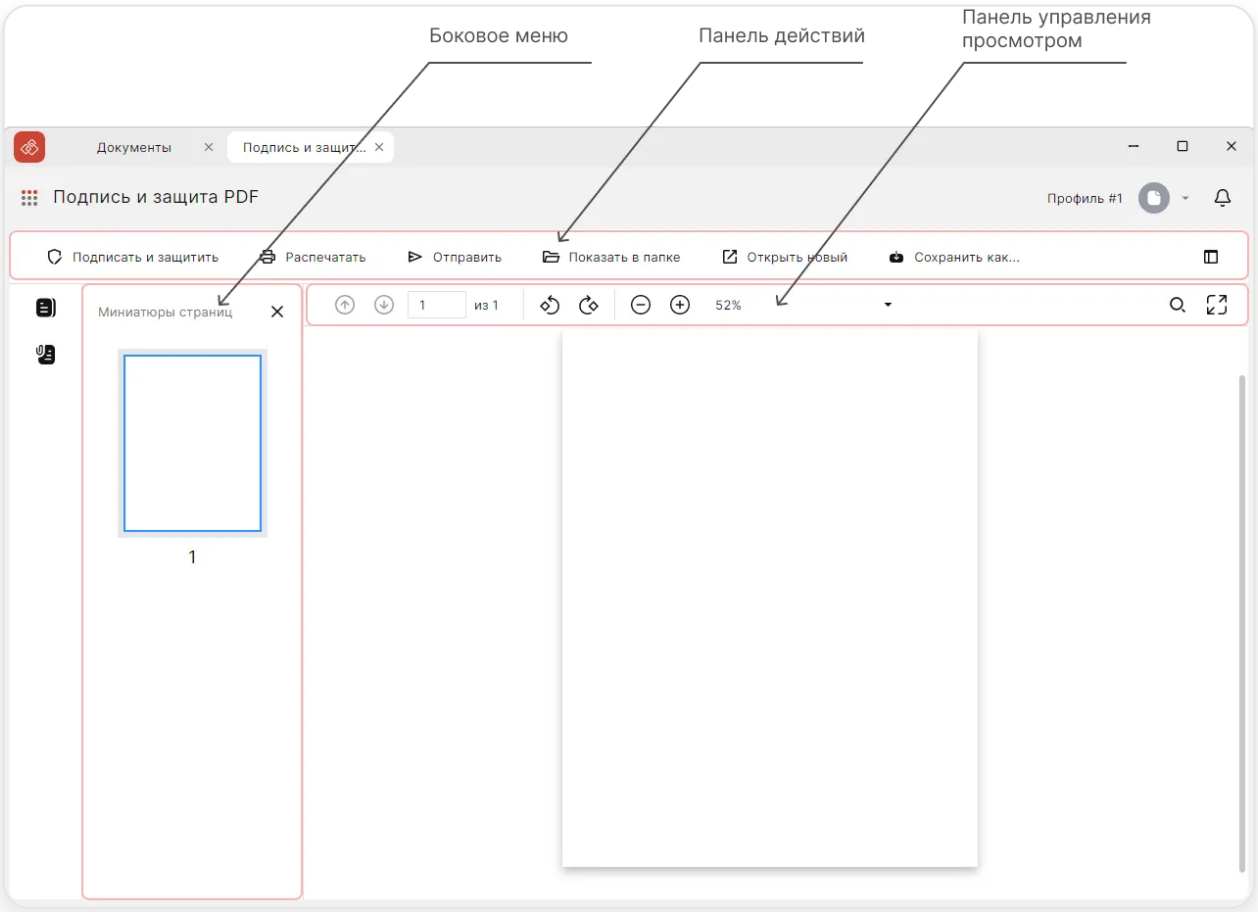
Чтобы открыть PDF-документ для просмотра:

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте в мастер PDF-документ (см. Добавление документа).

После загрузки документ будет открыт для просмотра.

Если в документе есть подписи, то КриптоАРМ автоматически запустит их проверку (см. Проверка подписи PDF-документа).

Инструменты просмотра



Панель действий

Кнопка	Функция	Иконка
Подписать и защитить	Переход к настройкам подписи и разметке областей	-
Распечатать	Печать документа	-
Показать в папке	Открытие расположения файла	-
Открыть новый	Замена текущего документа	-
Сохранить как	Создание копии файла	-
Подробно	Открытие панели сведений	

Панель управления просмотром

Элемент	Функция	Иконка
Навигация по страницам	Листание и переход к конкретной странице	

Элемент	Функция	Иконка
Поворот страниц	Вращение на 90°	
Масштабирование	Увеличение/уменьшение просмотра	
Поиск по тексту	Нахождение слов в документе	-
Режим просмотра	Полноэкранный/обычный режим	

> ⚠️ **Примечание**: Поворот страниц не изменяет исходный файл - только режим просмотра.

Боковое меню навигации

- **Миниатюры страниц** – отображение панели с миниатюрным представлением страниц. При выборе миниатюры страницы происходит переход к нужной странице документа в основной области.
- **Вложения** – открытие панели вложений со списком вложенных файлов. Вложенные файлы могут быть открыты для просмотра средствами ОС.
- **Подписи** – отображение панели с проставленными подписями и свободными областями для подписантов.

Создание подписи PDF-документа

Чтобы подписать PDF-документ:

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте в мастер PDF-документ (см. Добавление документа) и нажмите кнопку **Подписать и защитить** на панели действий.
3. В правой части окна появятся настройки подписи. По умолчанию используются параметры активного профиля подписи.
4. В блоке **Настройте свою подпись** укажите:
    - Личный сертификат (см. Выбор сертификата подписи),
    - Стандарт подписи (см. Настройка стандарта подписи),
    - Разместите штамп для личной подписи (см.Разметка области для штампа подписи),
    - Настройте оформление штампа подписи (см. Настройка оформления штампа подписи), если необходимо поставить «видимую» подпись.
5. При необходимости добавьте и настройте:
    - Подписантов (см. Добавление подписантов),
    - Произвольную область (см. Добавление произвольной области).

6. При необходимости в блоке **Защитите документ** настройте параметры защиты документа:
   - включите опцию **Сертифицировать** для создания сертифицирующей подписи,
   - включите опцию **Конвертировать в формат PDF/A**, чтобы удалить потенциально опасные элементы.

> ⚠️ **Примечание**: поставить сертифицирующую подпись может только первый подписант.

7. Укажите настройки для сохранения результата операции:
   - Сохранить файл в папке с исходным документом или выбрать другую папку;
   - Создать копию результата в папке **Архив**.
8. Нажмите кнопку **Выполнить**.
9. Перед началом подписания появится окно подтверждения (см. Подтверждение операции). Нажмите кнопку **Продолжить**, чтобы подтвердить ознакомление с подписываемыми данными.
10. Если контейнер закрытого ключа имеет пароль, то необходимо ввести его в окне криптопровайдера.

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

Если операция прошла успешно, подписанный файл будет сохранен в соответствии с указанными настройками.

Документ откроется в режиме просмотра и проверки подписи.

Сертифицирующая подпись PDF-документа

Сертифицирующая подпись — это особый тип электронной подписи, который не только подтверждает авторство и целостность документа, но и накладывает ограничения на дальнейшие изменения. Подробнее читайте в инструкции Обзор операций КриптоАРМ и выбор мастера.

Чтобы подписать PDF-документ сертифицирующей подписью:

1. Откройте мастер, добавьте файл и установите настройки подписи по аналогии с инструкцией Создание подписи PDF-документа.
2. В блоке **Защитите документ** включите опцию **Сертифицировать**.
3. При необходимости включите опцию **Конвертировать в формат PDF/A**, чтобы удалить потенциально опасные элементы (см. Создание подписи с конвертацией в PDF/A).
4. Укажите настройки для сохранения результата операции и нажмите кнопку **Выполнить**.

Далее выполните стандартные шаги завершения операции подписи: подтверждение операции, ввод пароля контейнера (при необходимости) и ожидание результата (см. инструкцию Создание подписи PDF-документа).

Создание подписи с конвертацией в PDF/A

При конвертации выполняется удаление или отключение элементов, которые могут нарушить отображение документа или повлиять на его безопасность. К таким элементам относятся скрипты (JavaScript), мультимедиа (аудио, видео), 3D-объекты и интерактивные формы, внешние ссылки на ресурсы, а также шифрование и парольная защита.

> 🔐 **Важно:** если вы конвертируете документ с форматом **PDF/A-3b** в **PDF/A-2b**, все вложенные файлы внутри документа будут удалены, потому что формат **PDF/A-2b** не поддерживает встроенные объекты.

Чтобы подписать PDF-документ с конвертацией в PDF/A:

1. Откройте мастер, добавьте файл и установите настройки подписи по аналогии с инструкцией Создание подписи PDF-документа.
2. В блоке **Защитите документ** включите опцию **Конвертировать в формат PDF/A** и укажите дополнительные настройки:
    - Выберите формат: **PDF/A-2b** или **PDF/A-3b**,
    - Выберите вариант преобразования страниц: **Преобразовать страницы с ошибками в изображения** или **Преобразовать все страницы в изображения**.
    - Укажите разрешение изображений: **70 ppi**, **100 ppi**, **150 ppi**, **200 ppi**, **300 ppi**.
    - При необходимости включите опцию **Безопасный режим** для активации медленного режима работы, при котором страницы будут обрабатываться по очереди друг за другом
3. Укажите настройки для сохранения результата операции и нажмите кнопку **Выполнить**.

Далее выполните стандартные шаги завершения операции подписи: подтверждение операции, ввод пароля контейнера (при необходимости) и ожидание результата (см. инструкцию Создание подписи PDF-документа).

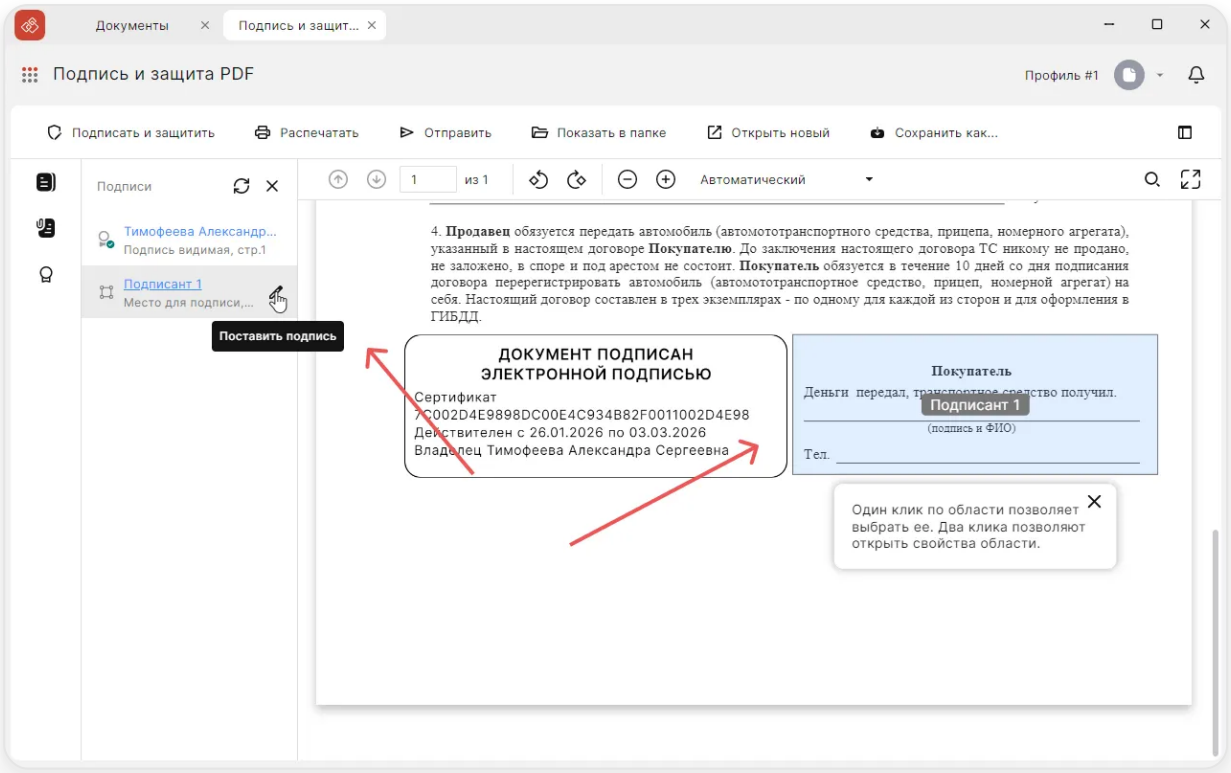
Создание подписи в размеченной области

Если документ содержит размеченные области для подписантов, подпись можно установить в любую из этих областей. Все подготовленные области отображаются на вкладке **Подписи** в боковом меню мастера **Подпись и защита PDF**.

Области могут быть созданы для видимых и невидимых подписей. Подробнее читайте в инструкции Обзор операций КриптоАРМ и выбор мастера.

Чтобы поставить подпись в размеченную область:

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте в мастер PDF-документ (см. Добавление документа).
3. Откройте в боковом меню вкладку **Подписи**.
4. Наведите курсор мыши на свободную область и нажмите на кнопку **Поставить подпись** , либо дважды кликните по области на странице документа (если область для видимой подписи).



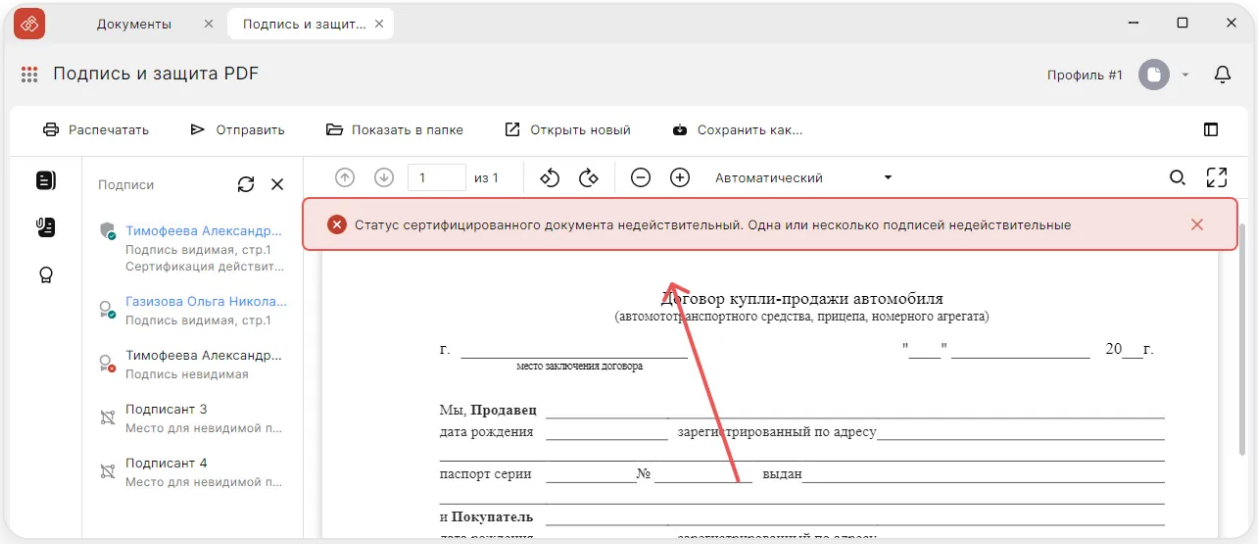
5. В правой части окна появятся настройки подписи. Далее выполните стандартные шаги завершения операции подписи: подтверждение операции, ввод пароля контейнера (при необходимости) и ожидание результата (см. инструкцию Создание подписи PDF-документа).

Проверка подписи PDF-документа

Чтобы проверить подписи PDF-документа:

1. Перейдите в раздел **Документы** и запустите мастер (см. Запуск мастера).
2. Добавьте в мастер PDF-документ (см. Добавление документа).
3. После загрузки документа автоматически запустится проверка подписей.

Общий статус подписи отображается в виде информера в области просмотра документа.



Статус каждой из подписей отображается в виде цветного индикатора в боковом меню:

- зеленая галочка — подпись действительная,
- красный крестик — подпись недействительная.

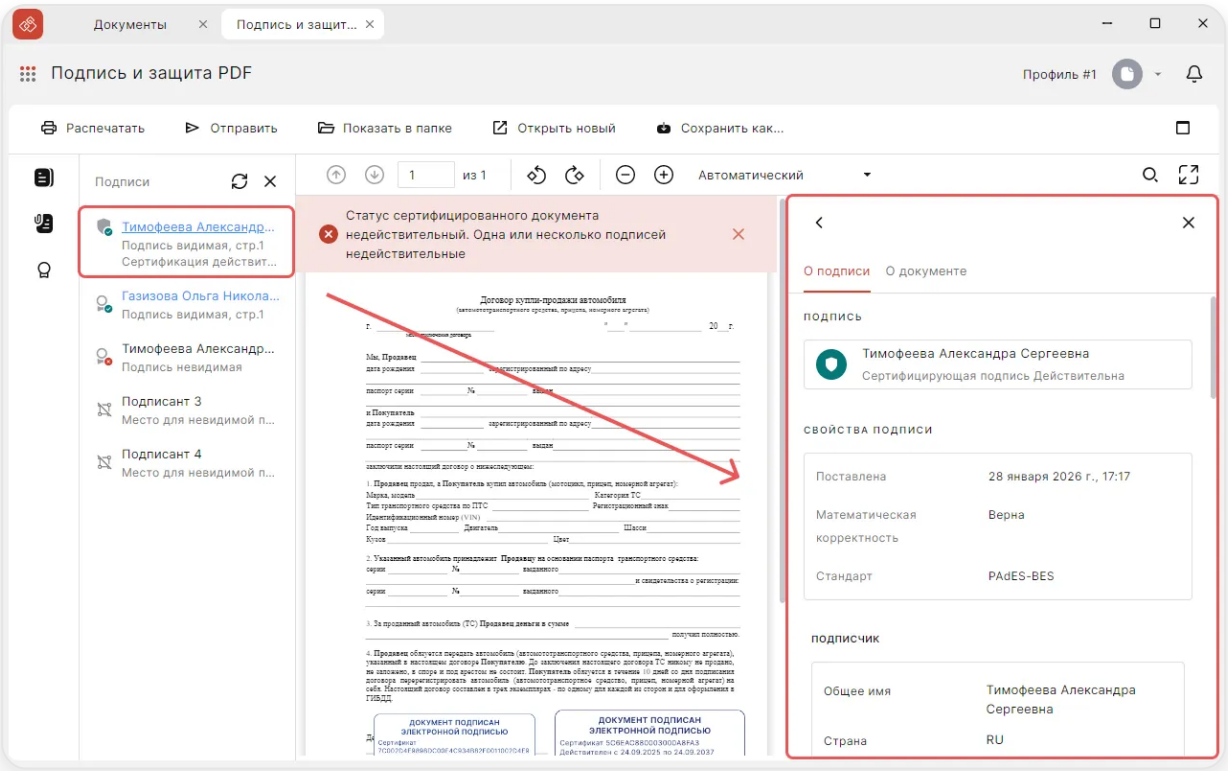
Кроме того, различаются иконки для сертифицирующей и «обычной» подписи:

- «обычная» подпись,
- сертифицирующая подпись.

Просмотр сведений о подписи PDF-документа

Чтобы просмотреть сведения о подписи документа:

1. Выполните шаги из инструкции Проверка подписи PDF-документа.
2. Для просмотра сведений о подписи нажмите на кнопку **Подробно** , размещенную на панели действий.
3. В правой части окна отобразится область со сведениями о подписи.



Действия в мастере

Запуск мастера

Мастер **Подпись и защита PDF** можно открыть следующими способами:

- Из раздела **Документы**: на панели действий нажмите **Подпись и защита PDF**.
- Из папки **Архив**, результатов операции или раздела **Почта**. Выберите файл, затем нажмите **Добавить в** → **Подпись и защита PDF**.
- Из глобального меню: нажмите кнопку глобального меню и выберите **Подпись и защита PDF**.

После выполнения любого из этих действий мастер откроется в новой вкладке.

Добавление документа

Добавьте документ в мастер одним из способов:

1. Перетащите в окно приложения.
2. Загрузите с помощью кнопки **Загрузить с компьютера**.

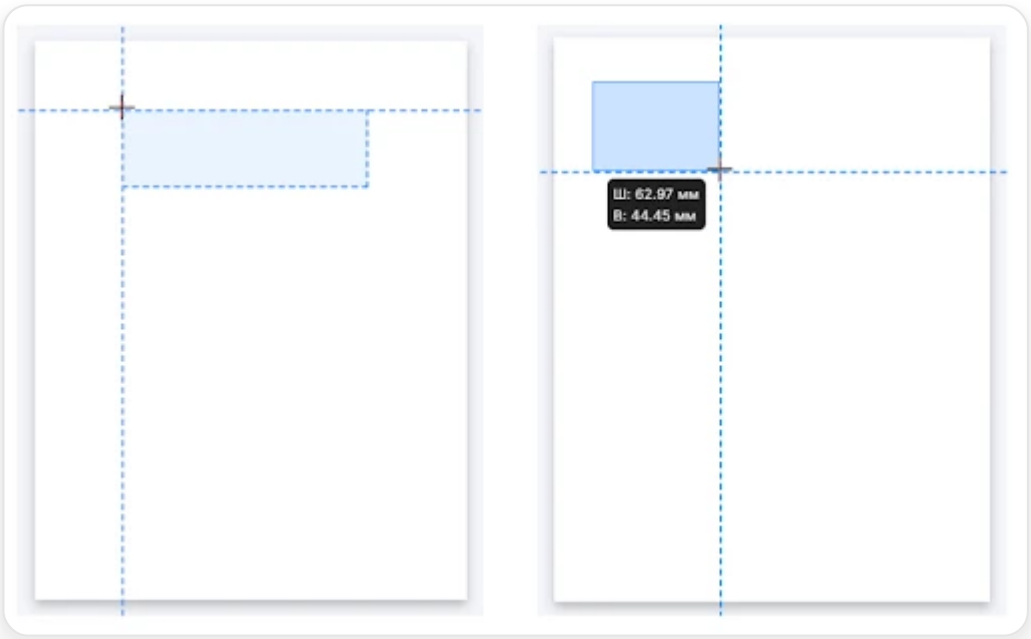
После загрузки документ будет открыт для просмотра.

Разметка области для штампа подписи

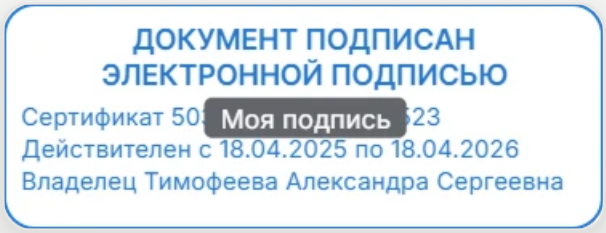
Чтобы разместить штамп для видимой подписи:

1. Нажмите кнопку **Разметить** в блоке **Визуализация**.
2. На странице документа появятся пунктирные линии. При наведении курсора мыши на пересечении линий отобразится схематичный прямоугольник.
3. Наведите курсор мыши на нужное место на странице документа и кликните левой кнопкой мыши. Область автоматически примет размер схематичного прямоугольника. Для того чтобы задать собственный размер области, наведите курсор мыши в нужное место, зажав левую кнопку мыши, разметьте область нужного размера.

> 💡 **Совет**: Чтобы изменить размер или положение штампа, нажмите кнопку **Свойства** на панели **Визуализация** и укажите новые новые параметры.



> ⚠️ **Примечание**: После разметки в области появится метка **Моя подпись**. Данная метка служит исключительно для визуального ориентира и исчезнет после подписи документа.

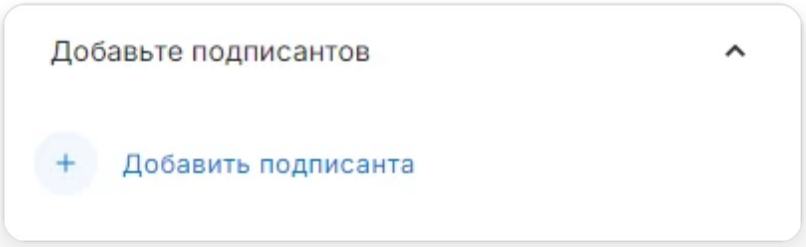


Подписанты

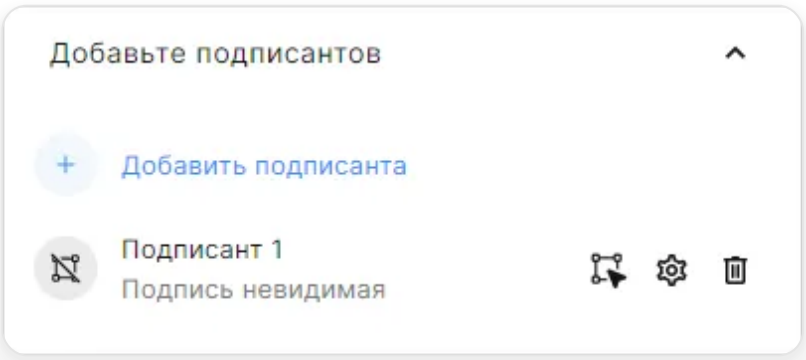
Добавление подписантов

> 💡 В приложении в документ можно добавить до 10 подписантов. По аналогии с личной подписью подпись подписантов может быть видимой и невидимой.

1. Нажмите кнопку **Добавить подписанта**.



2. В блоке **Добавьте подписантов** появится подписант с невидимой подписью.



Разметка области для подписи подписанта

1. Нажмите кнопку **Разметить** на панели с подписантом.
2. На странице документа появятся пунктирные линии. При наведении курсора мыши на пересечении линий отобразится схематичный прямоугольник.

3. Наведите курсор мыши на нужное место на странице документа и кликните левой кнопкой мыши. Область автоматически примет размер схематичного прямоугольника. Для того чтобы задать собственный размер области, наведите курсор мыши в нужное место, зажав левую кнопку мыши, разметьте область нужного размера.

> 💡 **Совет**: Чтобы изменить размер или положение штампа подписанта, нажмите кнопку **Свойства** на панели с подписантом и укажите новые новые параметры.

Удаление подписанта

Чтобы удалить подписанта из документа нажмите на кнопку **Удалить** , расположенную на панели с его именем.

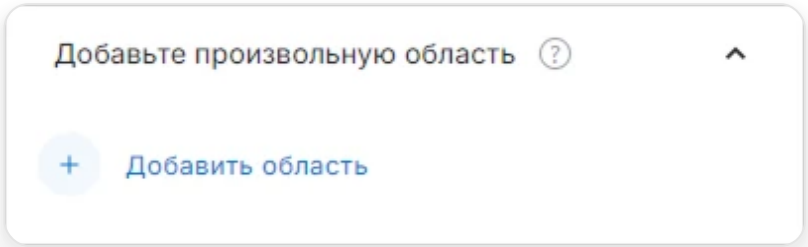
> ⚠️ **Примечание**: Нельзя удалить подписанта в подписанном документе.

Произвольная область

Произвольная область – это область для графического изображения или текста. В области можно разместить свой комментарий, статус или отметку о конфиденциальности документа.

Разметка произвольной области

1. Нажмите кнопку **Добавить область** в блоке **Добавьте произвольную область**.



2. На странице документа появятся пунктирные линии. При наведении курсора мыши на пересечении линий отобразится схематичный прямоугольник.
3. Наведите курсор мыши на нужное место на странице документа и кликните левой кнопкой мыши. Область автоматически примет размер схематичного прямоугольника. Для того чтобы задать собственный размер области, наведите курсор мыши в нужное место, зажав левую кнопку мыши, разметьте область нужного размера.

> 💡 **Совет**: Чтобы изменить размер или положение штампа подписанта, нажмите кнопку **Свойства** на панели с областью и укажите новые новые параметры.

🔍 **Примечание**: Подробная инструкция по настройке произвольной области, включая добавление изображений, текста и управление положением, доступна в статье Настройки подписи и шифрования.

Удаление произвольной области

Чтобы удалить произвольную область из документа нажмите на кнопку **Удалить** в блоке **Добавьте произвольную область**.

💡 **Совет**: Нельзя удалить произвольную область в подписанном документе.

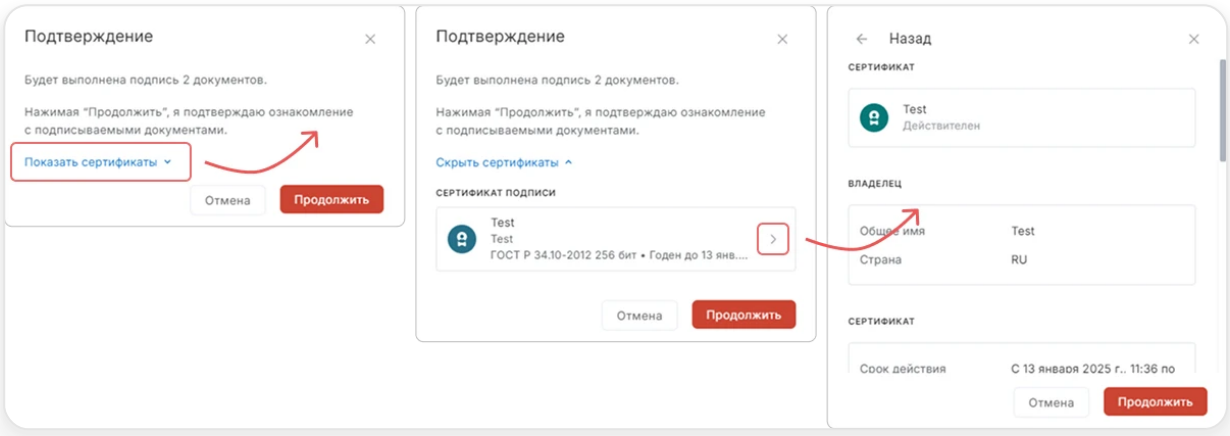
Подтверждение операции

Перед выполнением операции запрашивается ее подтверждение.

Чтобы подтвердить операцию:

1. Ознакомьтесь со сведениями в окне **Подтверждение**. Окно содержит сведения о количестве документов и выполняемой с ними операции, а также сертификатах, которые будут использоваться.

   Чтобы просмотреть информацию о сертификате, нажмите на кнопку **Показать сертификат**. После этого нажмите на панель с сертификатом.



2. В окне с подтверждением операции может появиться дополнительное уведомление, если:
   - Сертификат подписи недействителен,
   - Срок действия открытого или закрытого ключа личного сертификата 30 дней и менее,
3. Нажмите кнопку **Продолжить**, чтобы подтвердить ознакомление с документами.

Возможные ошибки

В процессе работы с PDF-документами могут возникать ошибки, связанные с форматом файла, лицензиями, криптопровайдерами или сетевыми настройками.

Подробности о возникающих ошибках можно найти в Журнале.

Ошибки при открытии файла

Ошибка	Описание	Рекомендуемые действия
Не удалось открыть файл	Файл поврежден или не является PDF	Попробуйте открыть файл в другом приложении или запросите оригинал документа у отправителя
Не удалось открыть файл	Установлены ограничения на просмотр. Возможно, документ защищен паролем.	1. Запросите у отправителя пароль для снятия защиты 2. Попросите предоставить незащищенную версию
Файл не соответствует формату PDF	Выбран файл, несоответствующий формату PDF	Убедитесь, что расширение файла соответствует формату PDF и попробуйте добавить файл еще раз

Ошибки при подписи файла

> ⚠️ **Примечание**: Коды ошибок (0x...) фиксируются для криптопровайдера КриптоПро CSP.

Код ошибки	Ошибка	Рекомендуемые действия
-	**Отсутствует необходимый криптопровайдер. Алгоритм открытого ключа сертификата: ГОСТ Р 34.10-2012 256 бит**	Установите КриптоПро CSP
-	**Отсутствует действующая лицензия КриптоАРМ**	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
0x8009001d	**Отсутствует действующая лицензия КриптоПро CSP**	Установите лицензию КриптоПро CSP
0xc2100140	**Отсутствует лицензия на модуль КриптоПро TSP Client**	Приобретите и установите лицензию TSP Client
0xc2110140		

Код ошибки	Ошибка	Рекомендуемые действия
	Отсутствует лицензия на модуль КриптоПро OCSP Client	Приобретите и установите лицензию OCSP Client
-	**Не установлены модули TSP/ OCSP Client**	Установите недостающие модули
-	**Не выбран сертификат подписи**	Выберите сертификат в настройках подписи
-	**Не указан адрес службы TSP**	Введите корректный адрес TSP-сервера
0x80072ee7	**Некорректный адрес службы TSP**	1. Проверьте правильность введенного адреса 2. Убедитесь в доступности сервера
-	**Сертификат не подходит для усовершенствованной подписи**	Выберите подходящий сертификат или измените настройки стандарта подписи
-	**Не указан адрес прокси-сервера**	1. Введите корректный адрес прокси 2. Проверьте параметры сети
-	**Не указан порт прокси-сервера**	1. Укажите правильный порт прокси-сервера 2. Проверьте настройки подключения
0x80072ee6	**Некорректные настройки прокси**	1. Проверьте параметры прокси-сервера 2. Временно отключите прокси для тестирования
-	**Папка для сохранения не найдена**	1. Проверьте существование указанной папки 2. Создайте и укажите новую папку для результатов
0x80072ee7	**Нет подключения к интернету**	1. Проверьте сетевое подключение 2. Убедитесь, что брандмауэр не блокирует соединение (Для подписей со штампами)

Смотрите также

- Профиль подписи — сохранение параметров операций в профилях для повторного использования.

- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.

Открыть статью на сайте

Настройки подписи и шифрования

В этом разделе описаны настройки электронной подписи и шифрования в мастерах КриптоАРМ, которые можно сохранить в профиле подписи для повторного использования. Вы узнаете, как выбрать личный сертификат, задать параметры для подписи по стандартам CAdES и PAdES и настроить шифрование документов.

Содержание:

- Личная подпись
- Настройки подписи CAdES
- Настройки подписи PAdES
- Настройки защиты PDF-документа
- Печатная форма
- Сертификаты шифрования
- Настройки шифрования
- Сохранение результатов
- Общие настройки
- Смотрите также

Личная подпись

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

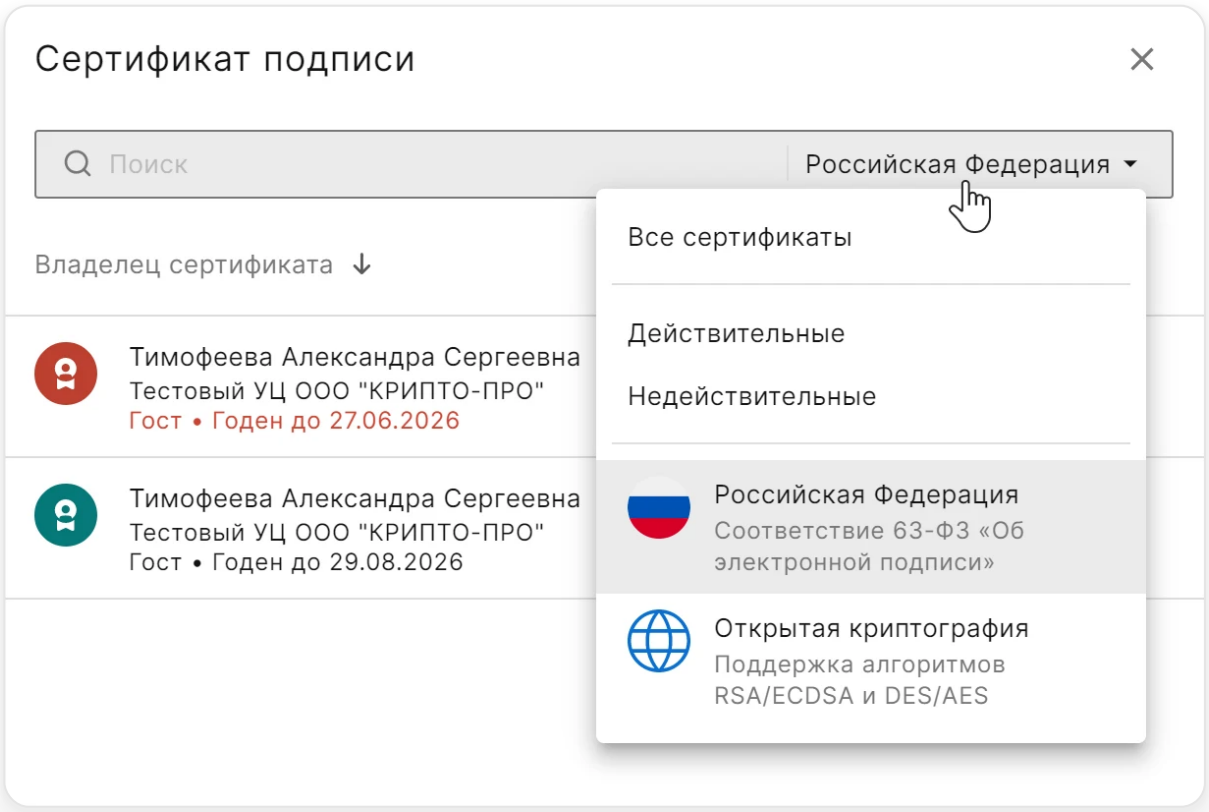
Выбор сертификата подписи

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

Чтобы выбрать сертификат:

1. Нажмите на кнопку **Редактировать** на панели с настройкой сертификата в блоке **Личная подпись**.
2. При необходимости воспользуйтесь фильтрацией списка сертификатов:
    - выберите **профиль доверия**:
        - **Российская Федерация** — отображаются сертификаты с алгоритмами ГОСТ;
        - **Открытая криптография** — отображаются сертификаты с алгоритмами RSA;
    - включите отображение только **действительных сертификатов**, если необходимо скрыть недействительные сертификаты;

- воспользуйтесь **строкой поиска**, чтобы быстро найти сертификат по имени владельца или другим данным.



3. Нажмите на значок нужного сертификата.
4. Закройте окно по кнопке **Закрыть**.

> 💡 **Совет**: При необходимости можно просмотреть сведения о сертификате по кнопке ›.

Выбор стандарта подписи

Если подпись выполняется от имени организации или представителя, можно добавить машиночитаемую доверенность.

1. Нажмите кнопку **Редактировать** на панели с настройкой стандарта в блоке **Личная подпись**..
2. В открывшемся окне выберите необходимый стандарт подписи:
   - **CAdES-BES** — базовая подпись без меток времени.
   - **CAdES-T** — электронная подпись, дополненная штампом времени, который подтверждает время создания подписи.

- **CAdES-X Long Type 1** — усовершенствованная электронная подпись, которая включает все необходимые данные для проверки её действительности: сведения о времени подписания, информацию для подтверждения валидности подписи, а также данные, подтверждающие, что сертификат подписанта был действителен на момент подписания.
- **CAdES-A** — архивная подпись, предназначенная для долгосрочного хранения документов и обеспечивающая возможность проверки подписи спустя длительное время.

3. Для стандартов CAdES-T, CAdES-A и CAdES-X Long Type 1 используется служба штампов времени (TSP). По умолчанию в поле **Служба штампов времени (TSP)** указан адрес сервиса ФНС России **http://pki.tax.gov.ru/tsp/tsp.srf**. При необходимости его можно заменить адресом службы, предоставленной вашим удостоверяющим центром. Формат адреса: `<https>://<сервер>[:порт][/путь]`. Если доступ к службам TSP или OCSP осуществляется через прокси, укажите параметры подключения.

4. Внесите необходимые изменения и закройте окно.

Настройки прокси сервера

Если доступ к службам TSP или OCSP осуществляется через прокси, укажите параметры подключения:

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Адрес прокси сервера	-	IP-адрес или доменное имя прокси-сервера	IPv4/IPv6 адрес или валидное доменное имя
Порт	-	Номер порта для подключения к прокси	Стандартные порты: 80 (HTTP), 3128 (Squid), 8080 (альтернативный HTTP)
Логин	-	Имя пользователя для доступа к прокси	Любая строка до 64 символов
Пароль	-	Пароль для доступа к прокси	Любая строка до 128 символов

Выбор машиночитаемой доверенности

Машиночитаемая доверенность (МЧД) используется при подписании документов представителем организации.

В настройке указывается: файл доверенности `.xml` и файл подписи доверенности `.sig`.

1. Нажмите кнопку **Редактировать** на панели с настройкой доверенности.

2. В открывшемся окне нажмите:

   - На кнопку **Добавить доверенность** для добавления файла доверенности в формате `.xml`.

- На кнопку **Добавить файл** подписи для добавления файла подписи доверенности.

3. Закройте окно по кнопке **Добавить**.

Настройки подписи CAdES

Настройки CAdES определяют способ формирования электронной подписи, формат файла подписи и состав данных, включаемых в подпись.

> ⚠️ **Примечание**: эти параметры доступны только в мастере Подпись и шифрование.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Вид подписи	`Присоединенная`	Выбор формата хранения подписи относительно документа.	`Присоединенная` (подпись и документ в одном файле), `Отсоединенная` (подпись хранится отдельно)
Формат файла подписи	`.sig`	Расширение файла, в который сохраняется подпись.	`.sig`, `.p7s`, `.sgn`, `.sign`, `.bin`
Данные в подписи	`Только сертификат владельца`	Определяет, какие сертификаты добавляются в атрибуты подписи.	`Только сертификат владельца`, `Цепочка без корневого сертификата`, `Все сертификаты цепочки`
Кодировка подписи	`DER`	Определяет способ кодирования данных подписи.	`DER` (стандартная бинарная кодировка), `BASE-64` (текстовая кодировка)
Убрать служебные заголовки	`Выкл`	Доступен для кодировки `BASE-64`. Убирает заголовки `-----BEGIN CERTIFICATE-----` и `-----END CERTIFICATE-----`.	`Вкл` / `Выкл`

Настройки подписи PAdES

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Встроенная подпись (PAdES)	Выкл	Если включено, PDF-документы будут подписаны встроенной подписью по стандарту PAdES вместо CAdES.	Вкл / Выкл

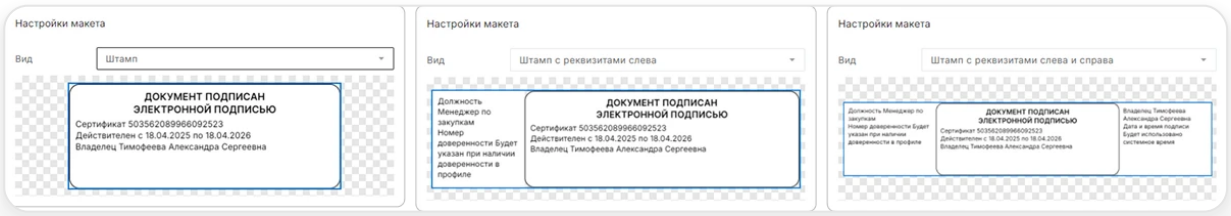
Внешний вид штампа подписи

Настройки внешнего вида определяют, как подпись будет визуально отображаться в PDF-документе. Вы можете настроить макет штампа, реквизиты, фон, границу, цвет текста и границы, а также добавить логотип.

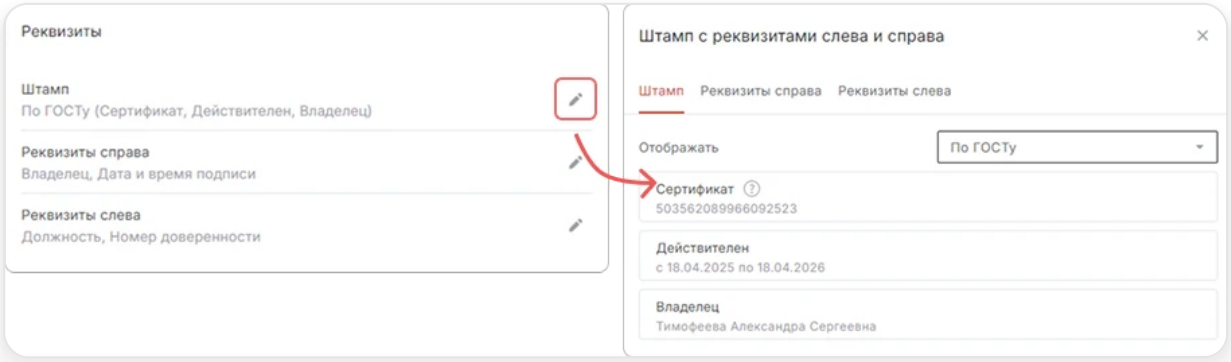
Название настройки	Значение по умолчанию	Описание	Допустимые значения
Вид штампа	Штамп	Определяет внешний вид штампа	Штамп, Штамп с реквизитами слева, Штамп с реквизитами справа, Штамп с реквизитами с обеих сторон
Реквизиты	По ГОСТу	Определяет набор отображаемых реквизитов в штампе	По ГОСТу (стандартный набор в соответствии с ГОСТ Р 7.0.97-2016), Произвольно (ручная настройка реквизитов)
Добавить фон на область	Вкл	Настройка фона штампа. Если включено, в штамп будет добавлен фон #ffffff (hex)	Вкл / Выкл
Добавить границу	Вкл	Настройка границы штампа. Если включено, в штамп будет добавлена граница.	Вкл / Выкл
Настроить цвет границы и текста	#000	Настройка границы и текста в штампе.	Значение в hex-формате
Логотип	-	Позволяет добавить логотип в штамп	Файлы изображений (.webp, .jpg, .svg). Максимальный размер - 10 МБ.

Настройка внешнего вида штампа

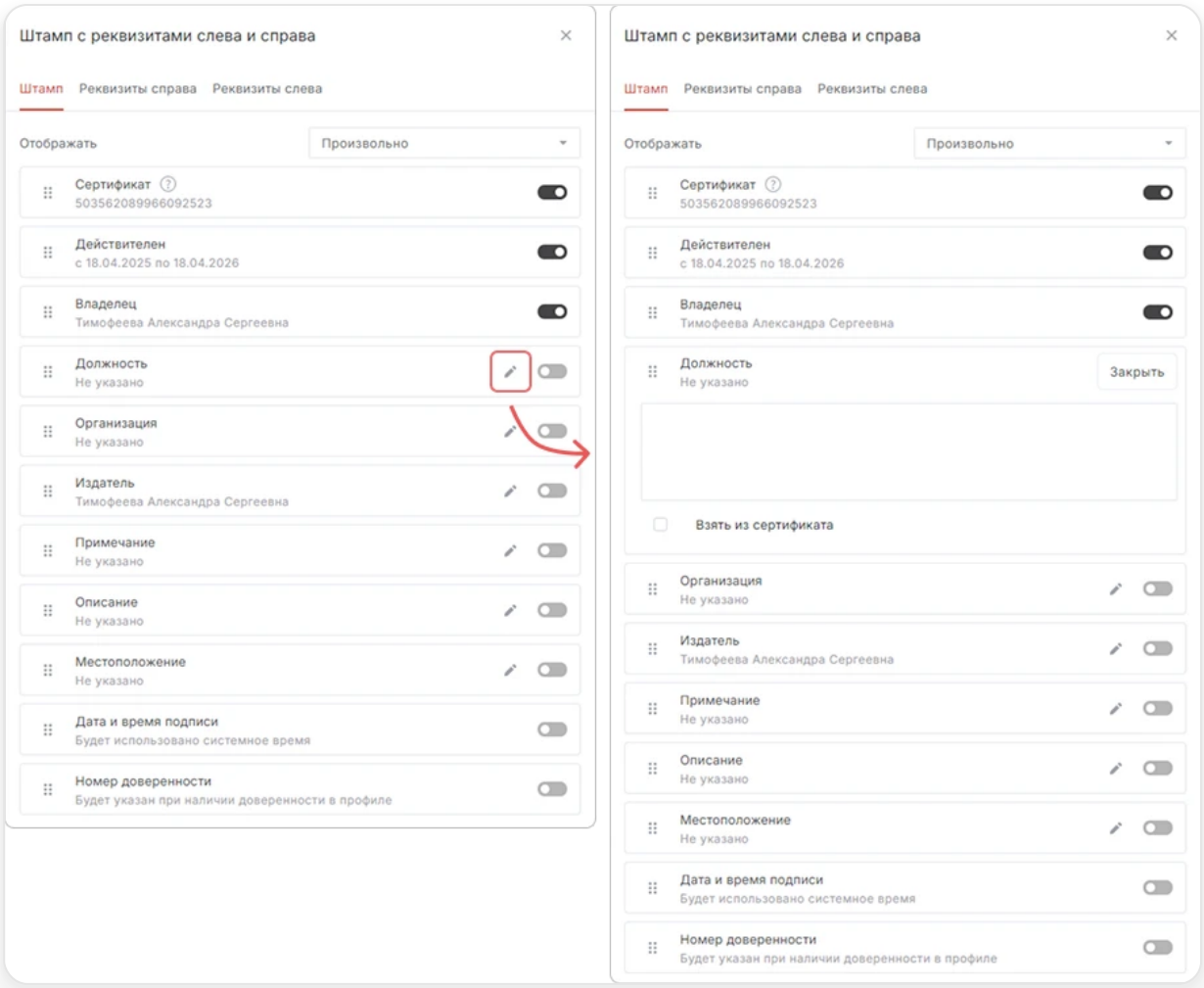
1. Откройте окно настроек:
   - по кнопке **Внешний вид штампа** в мастере **Подпись и шифрование** или **Профиле подписи**,
   - по кнопке **Свойства** на панели **Визуализация** в мастере **Подпись и защита PDF**.
2. В блоке **Настройки макета** выберите макет штампа в настройке **Вид**.



3. В блоке **Реквизиты** нажмите на кнопку **Редактировать** и укажите настройки отображения:
   - **По ГОСТ** — для вывода реквизитов в соответствии с **ГОСТ Р 7.0.97-2016** (Заголовок «Документ подписан электронной подписью», серийный номер сертификата, имя его владельца и срок действия).



   - **Произвольно** — для ручной настройки реквизитов: включение нужных полей, редактирование значений и изменение порядка отображения с помощью кнопки .

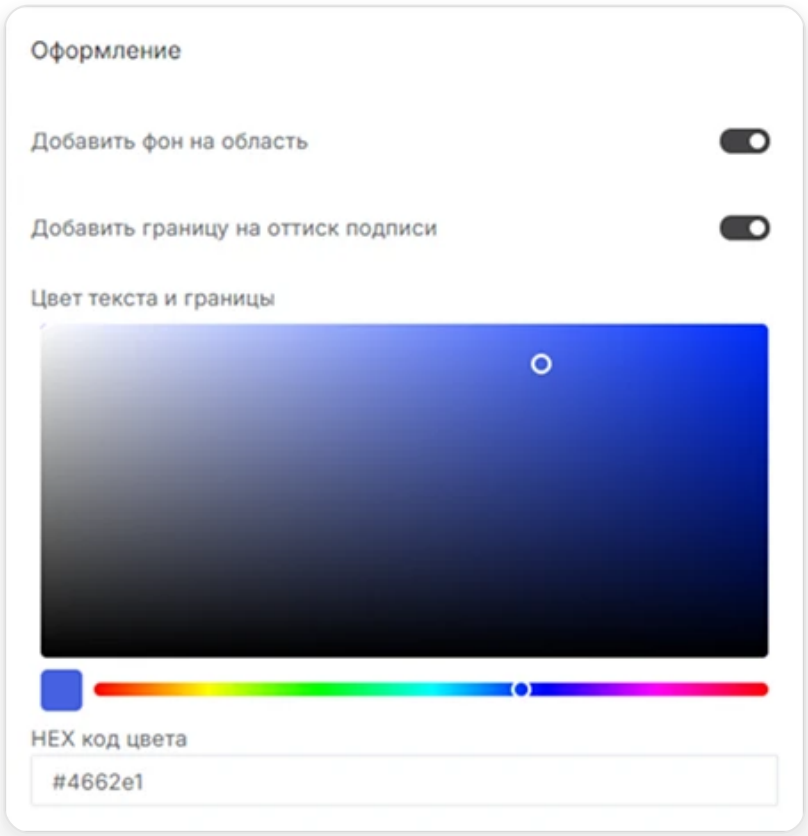


> 💡 **Примечание:** По умолчанию в поле **Владелец** штампа отображается значение **Общее имя (CN)** из сертификата. Если в сертификате указано название организации, а требуется вывести ФИО подписанта, откройте **Настройки визуализации** → **Внешний вид** → **Редактировать** в блоке «Реквизиты», выберите тип штампа «Произвольно» и включите переключатель «ФИО».

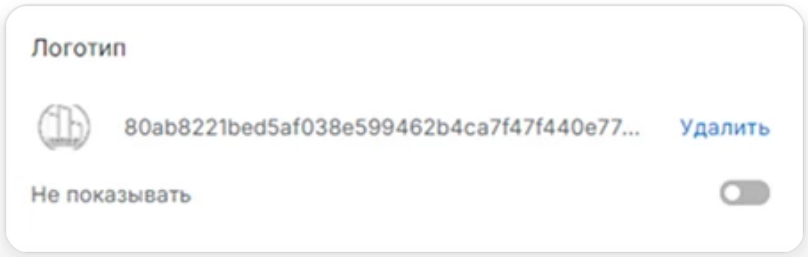
4. Аналогичным образом настройте вывод реквизитов для блоков слева или справа от штампа, если их отображение активировано.

5. В блоке **Оформление** настройте фон и границу:

   - Активируйте переключатель **Добавить фон на область** для добавления фона с цветом: `#ffffff` (hex).
   - Активируйте переключатель **Добавить границу на оттиск подписи** для добавления границы.
   - Настройте цвет границы и текста через палитру или hex-код.



6. В блоке **Логотип** загрузите изображение с гербом или эмблемой по кнопке **Загрузить**.



7. Закройте окно по кнопке **Закрыть**.

Положение штампа подписи

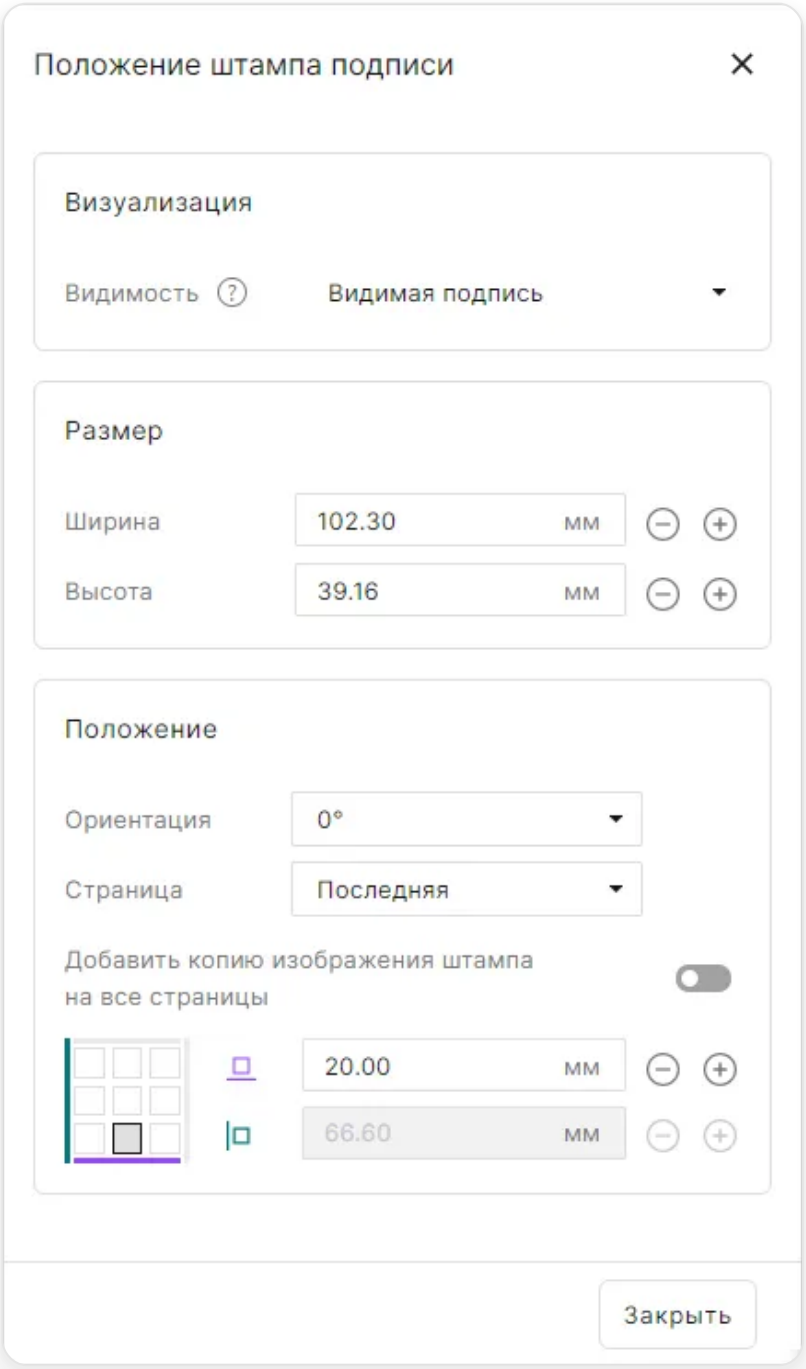
Настройки положения штампа определяют видимость подписи на странице документа, размер, ориентацию и размещение штампа на страницах документа.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Видимость подписи	`Видимая подпись`	Определяет визуальное отображение подписи на документе	`Видимая подпись` (отображается как штамп),

Название настройки	Значение по умолчанию	Описание	Допустимые значения
			Невидимая подпись (подпись существует, но не видна)
Размер штампа	Ширина 102,30 мм, Высота 39,16 мм	Позволяет задать точные размеры штампа подписи	Ширина от 1 до 207.9 мм, Высота от 1 до 294.69 мм (Используется значение для формата A4)
Ориентация	0°	Настройки ориентации штампа	0°, 90°, 180°, 270°
Страница расположения	Последняя	Страница расположения штампа	Последняя, Указать страницу (выбор страницы)
Добавить копию изображения штампа на все страницы	Выкл	Если включено, на все страницы документа добавляется копия изображения штампа	Вкл / Выкл
Координаты расположения штампа	Y 20 мм, X 66,60 мм	Положение штампа на странице	Y от 1 до 256.53 мм, X от 1 до 106.60 мм (Для размера штампа по умолчанию)

Настройка размера и положения штампа подписи

1. Откройте окно настроек:
    - по кнопке **Положение штампа** в мастере **Подпись и шифрование** или **Профиле подписи**,
    - по кнопке **Свойства**  на панели **Визуализация** в мастере **Подпись и защита PDF**.



2. В блоке **Визуализация** настройте визуальное отображение подписи:
   - **Видимая подпись** — подпись отображается в документе в виде штампа,
   - **Невидимая подпись** — подпись существует, но не видна.
3. Укажите ширину и высоту штампа в миллиметрах.

   Задайте параметры штампа в следующих пределах: ширина — от 1 до 207,9 мм, высота — от 1 до 294,69 мм. Эти размеры соответствуют формату страницы A4 и не выходят за его пределы. Важно учесть, что на размер штампа также оказывают влияние значения, указанные в блоке **Положение**.

4. В блоке **Положение** настройте:
   - Значение для ориентации штампа: **0 °**, **90 °**, **180 °**, **270 °**,
   - Страницу расположения штампа,
   - Координаты размещения штампа в миллиметрах,
   - При необходимости активируйте переключатель **Добавить копию изображения** штампа на все страницы.
5. Закройте окно по кнопке **Закрыть**.

Внешний вид произвольной области

Эта настройка позволяет настроить оформление произвольной области при подписи PDF-документа в мастере **Подпись и защита PDF**. Можно выбрать содержимое области (текст, изображение или оставить пустой для следующего подписанта), задать её положение, размер, прозрачность, границу и фон.

> ⚠️ **Примечание**: эти параметры доступны только в мастере Подпись и защита PDF.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Вид	`Оставить пустым`	Определяет внешний вид области, которая будет добавлена в документ	`Оставить пустым` (следующий подписант может добавить комментарий/статус), `Изображение` (загрузка готовой графической отметки), `Текст` (ввод произвольного текста)

Настройка оформления произвольной области

1. Откройте окно настроек по кнопке **Свойства**  в блоке **Добавьте произвольную область**.
2. В появившемся окне перейдите на вкладку **Внешний вид**.
3. Настройте **Вид области** в блоке **Настройки макета**:
   - **Изображение** — в области можно будет загрузить любое изображение размером до 10 МБ.
   - **Текст** — в области можно напечатать любой текст с помощью текстового редактора.
   - **Оставить пустым** — полномочия по оформлению области будут переданы следующему подписанту.
4. Настройте **Положение области** в блоке **Настройки макета**:
   - **Вписать** — штамп будет вписан по ширине и высоте в размеченную область.

- **Подогнать область под макет** — размер размеченной области будет подогнан под размер изображения или текста.

5. Настройте прозрачность контента произвольной области и отображение границы и фона штампа в блоке **Оформление**.

Настройки защиты PDF-документа

Настройки позволяют включить сертификацию документа с ограничением на внесение изменений и преобразовать PDF в формат PDF/A.

Название настройки	Значение по умолчанию	Описание	Дополнительные параметры
Сертифицировать	`Выкл`	Включает режим сертификации PDF с защитой от изменений. Разрешает только: заполнение размеченных областей подписантами и произвольных полей.	`Вкл` / `Выкл`
Конвертировать в PDF/A-2b	`Выкл`	Преобразует документ в архивный формат PDF/A-2b с удалением потенциально опасных элементов: скриптов, динамических форм и нестандартных шрифтов.	`Вкл` / `Выкл`

Настройки конвертации в PDF/A-2b

Название настройки	Значение по умолчанию	Описание	Дополнительные параметры
Если при конвертации возникнут ошибки	`Преобразовать страницы с ошибками в изображения`	Настройка поведения при возникновении ошибок в ходе конвертации	`Преобразовать страницы с ошибками в изображения`, `Преобразовать все страницы в изображения`
Разрешение изображений	`150 ppi`	Настройка разрешения изображений для преобразованных страниц	`70 ppi`, `100 ppi`, `150 ppi`, `200 ppi`, `300 ppi`
Безопасный режим	`Выкл`		`Вкл` / `Выкл`

Название настройки	Значение по умолчанию	Описание	Дополнительные параметры
		При включении активируется медленный режим работы. В этом режиме страницы обрабатываются по очереди друг за другом.	

Печатная форма

В мастере **Подпись и шифрование** при выполнении подписи можно создать отдельную копию PDF-документа с изображением штампа. Такая копия не содержит электронную подпись и предназначена только для визуального представления документа.

> ⚠️ **Примечание**: Печатную форму с отображением штампа подписи можно также создать в мастере **Проверка и расшифрование** (см. Создание печатной формы).

Название настройки	Значение по умолчанию	Описание	Дополнительные параметры
Печатная копия со штампом (без подписи)	Выкл	Создает копию PDF-документа с визуальным штампом подписи. Такая версия не содержит электронной подписи и используется только для просмотра или печати.	Вкл / Выкл

Настройки оформления и расположения штампа выполняются так же, как при создании подписи PAdES:

- Внешний вид штампа подписи,
- Положение штампа подписи.

Сертификаты шифрования

Сертификаты шифрования — сертификаты, используемые при шифровании документа.

> 💡 **Совет**: Всегда добавляйте **свой личный сертификат** к списку получателей, если вы планируете в дальнейшем расшифровывать файл.

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

> ⚠️ **Примечание**: эти параметры доступны только в мастере Подпись и шифрование.

Выбор сертификатов шифрования

Чтобы выбрать сертификаты шифрования:

1. В блоке **Сертификаты шифрования** нажмите на кнопку **Добавить сертификаты**.
2. Откроется окно **Сертификаты** и контакты:
   - на вкладке **Сертификаты** отображаются сертификаты получателей,
   - на вкладке **Контакты** — контакты с привязанными сертификатами, в адрес которых будет зашифрован документ.
3. При необходимости воспользуйтесь фильтрацией списка сертификатов:
   - выберите **профиль доверия**:
     - **Российская Федерация** — отображаются сертификаты с алгоритмами ГОСТ;
     - **Открытая криптография** — отображаются сертификаты с алгоритмами RSA;
   - включите отображение только **действительных сертификатов**, если необходимо скрыть недействительные сертификаты;
   - воспользуйтесь **строкой поиска**, чтобы быстро найти сертификат по имени владельца или другим данным.
4. Нажмите на значок нужного сертификата или контакта.
5. Закройте окно по кнопке **Закрыть**.

Настройки шифрования

Настройки позволяют указать алгоритм и формат зашифрованных файлов, способ их кодирования и возможность удаления оригинальных документов после шифрования.

> 🔐 ГОСТ-алгоритмы шифрования доступны при установленном криптопровайдере КриптоПро CSP.

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Алгоритм шифрования	`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), `AES 256 CBC`, `DES3-CBC`
Формат файла	`.enc`	Определяет расширение для зашифрованных файлов	`.enc` (стандартное), `.p7m`, `.p7e`, `.pem`
Кодировка файлов	`DER`	Задает способ представления зашифрованных данных	`DER`, `BASE-64`
Удалить исходные файлы	`Выкл`	Удаляет оригинальные файлы после успешного шифрования	`Вкл` / `Выкл`

> ⚠️ **Примечание**: эти параметры доступны только в мастере Подпись и шифрование.

Сохранение результатов

Настройки определяют, куда будут помещены файлы после выполнения операций (подпись, шифрование, архивирование) и позволяют при необходимости создать копию в специальной папке приложения.

Название настройки	Значение по умолчанию	Описание	Дополнительные параметры
Сохранение результатов			

Название настройки	Значение по умолчанию	Описание	Дополнительные параметры
	`Папка с исходным документом`	Определяет место сохранения результатов операции	`Папка с исходным документом` (сохраняет рядом с оригиналом), `Сохранить в папку...` (ручной выбор пути)
Добавлять пользовательский суффикс	`Выкл`	Добавляет указанный текст в конец имени файла. Если включено добавление имени подписанта, текст будет добавлен перед именем подписанта.	`Вкл` / `Выкл`
Добавлять ФИО подписанта	`Выкл`	Добавляет имя подписанта из сертификата к имени файла после пользовательского суффикса (если он указан). При необходимости имя можно отредактировать.	`Вкл` / `Выкл`
Отдельный архив на каждый файл	`Выкл`	Каждый файл будет упакован в отдельный архив. Если выключено, все файлы попадут в один общий архив.	`Вкл` / `Выкл`
Создать копию в папке «Архив»	`Выкл`	Дополнительное сохранение результатов в специальную папку приложения	`Вкл` / `Выкл`

Общие настройки

Название настройки	Значение по умолчанию	Описание
Название профиля	-	Название профиля для отображения в интерфейсе
Показывать настройки перед выполнением операции	-	Если включено, в мастере **Подпись и шифрование** отображаются настройки операции.

Смотрите также

- Профиль подписи — сохранение параметров операций в профилях для повторного использования.
- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.

Открыть статью на сайте

Управление документами

В этом разделе вы научитесь управлять документами в приложении **КриптоАРМ**. Вы узнаете, как хранить документы в папке **Архив**, выполнять действия с подписанными и зашифрованными файлами, а также как работать с машиночитаемыми доверенностями (МЧД).

Содержание:

- Папка «Архив»
- Действия с документами
- Действия с МЧД
- Возможные ошибки
- Смотрите также

Папка «Архив»

Папка **Архив** предназначена для безопасного и удобного хранения подписанных, зашифрованных и проверенных документов, обработанных в КриптоАРМ.

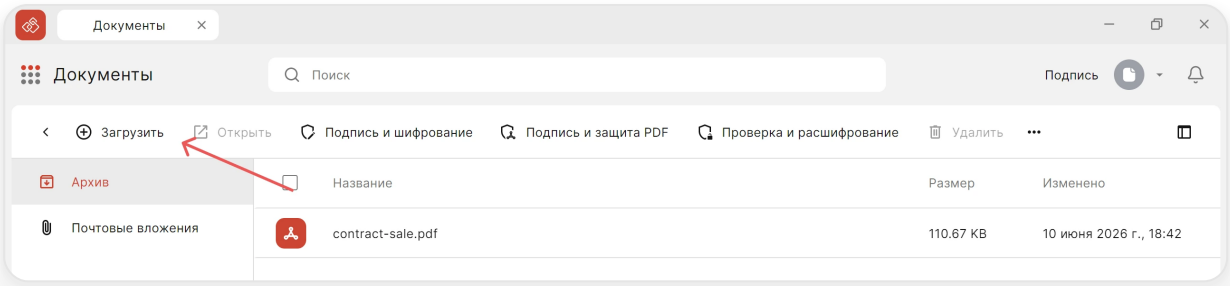
В папке **Архив** можно хранить:

- подписанные документы,
- зашифрованные файлы,
- файлы машиночитаемой доверенности (МЧД),
- резервные копии важных документов.

Загрузка документов в «Архив»

> ⚠️ **Примечание**: Загружаемые файлы учитываются в общем объеме данных приложения.

1. Перейдите в раздел **Документы** → **Архив**.
2. Добавьте файлы одним из способов:
    - Перетащите один или несколько файлов в окно приложения,
    - Нажмите **Загрузить** на панели действий и выберите файлы вручную.



После загрузки документы автоматически появятся в списке.

> 💡 **Совет**: Вы можете перетаскивать как файлы, так и папки. Все содержимое вложенных папок тоже будет добавлено в **Архив**.

Автоматическое сохранение в папку «Архив»

1. Откройте мастер **Подпись и шифрование** или **Подпись и защита PDF** и настройте для выполнения любой операции.
2. В блоке **Сохранение результатов** активируйте опцию **Создать копию в папке «Архив»**.
3. Запустите выполнении операции.

Если операция прошла успешно, подписанные файлы будут автоматически сохранены в указанную папку.

> 💡 **Совет**: Чтобы опция **Создать копию в папке «Архив»** активировалась автоматически, настройте ее в профиле подписи.

Действия с документами

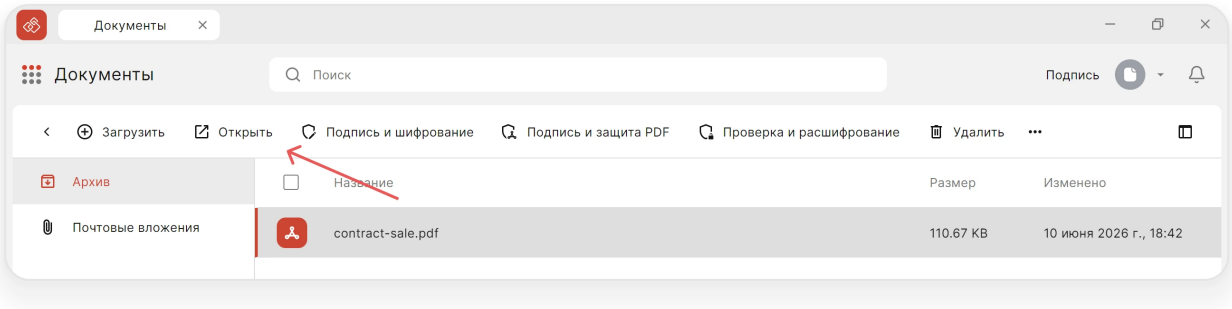
КриптоАРМ предоставляет полный набор инструментов для работы с электронными документами: открытие файлов, просмотр сведений о документе и электронной подписи, отправка документов по электронной почте, поиск расположения файла на компьютере и удаление. Все действия доступны в мастерах **Проверка и расшифрование** и **Подпись и шифрование**, а также в папках **Архив** и **Почтовые вложения**.

Открытие документа

> 🔐 **Важное условие**: Зашифрованные документы требуют предварительного расшифрования. Для открытия зашифрованных документов в хранилище «Личные сертификаты» должен присутствовать сертификат с закрытым ключом, который использовался при шифровании.

Чтобы открыть документ:

1. Выделите документ в одном из разделов:
   - Папка **Архив** или **Почтовые вложения**,
   - Мастер **Подпись и шифрование**,
   - Мастер **Проверка и расшифрование**.
2. Нажмите кнопку **Открыть** на панели инструментов.

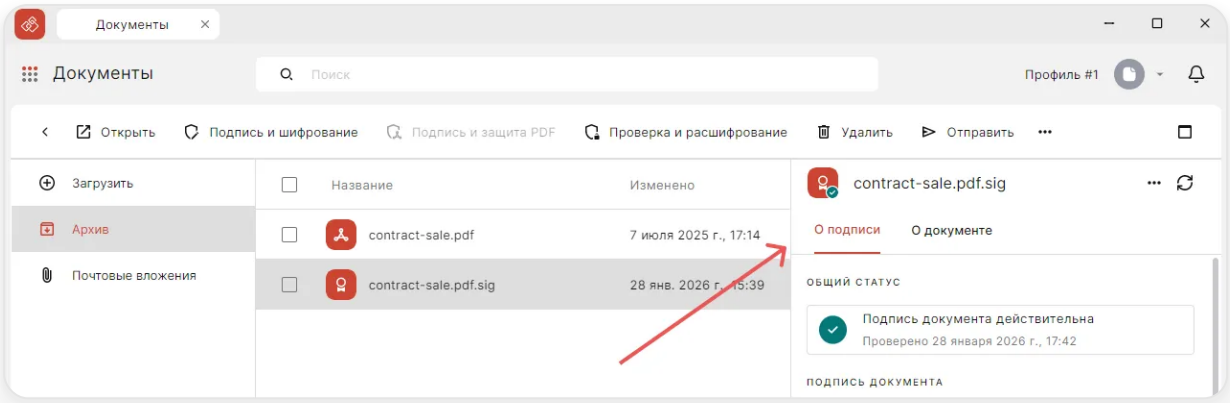


Документ откроется в программе, ассоциированной с его расширением в операционной системе.

> 💡 **Совет**: Для быстрого открытия документа дважды щёлкните по его имени в списке.

Просмотр сведений о документе

1. Выделите документ в одном из разделов:
   - Папка **Архив** или **Почтовые вложения**,
   - Мастер **Подпись и шифрование**,
   - Мастер **Проверка и расшифрование**.
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка писем откроется область со сведениями:
   - Нажмите на вкладку **О подписи** для просмотра сведений о подписи документа,
   - Нажмите на вкладку **О документе** для просмотра сведений о документе.



Отправление по почте

> ⚠️ **Примечание**: Для отправки документов по почте в приложении должен быть подключен почтовый аккаунт.

1. Выделите один или несколько документов в одном из разделов:
    - Папка **Архив**,
    - Мастер **Подпись и шифрование** (в окне с результатами операций),
    - Мастер **Проверка и расшифрование** (в окне с результатами операций).
2. Нажмите на кнопку **Отправить** на панели действий.
3. Откроется вкладка с новым письмом, в которой выбранные файлы будут добавлены во вложения.
4. Заполните обязательные поля и отправьте письмо.

Показать в папке

Функция **Показать в папке** позволяет быстро найти физическое расположение документа в файловой системе компьютера.

> ⚠️ **Примечание**: Функция доступна только для одиночного выбора документов. При множественном выделении кнопка **Показать в папке** неактивна.

1. Выделите документ в одном из разделов:
    - Папка **Архив**,
    - Мастер **Подпись и шифрование**,
    - Мастер **Проверка и расшифрование**.
2. Нажмите кнопку **Показать в папке** на панели действий.

3. Откроется системная папка с файлом.

> 💡 **Совет**: Также перейти в папку с файлом можно при просмотре сведений о документе. Для этого нажмите на ссылку с расположением файла на вкладке **О документе**.

Удаление документа

> ⚠️ **Примечание**: Документы, хранящиеся в папке **Архив**, можно удалить. При этом они будут удалены из файловой системы. Если вы удаляете документы в мастере **Подпись и шифрование** или **Проверка и расшифрование**, список будет очищен, но документы останутся в системе.

Чтобы удалить документ из папки **Архив**:

1. Выделите один или несколько документов в одном из разделов:
   - Папка **Архив**,
   - Мастер **Подпись и шифрование**,
   - Мастер **Проверка и расшифрование**.
2. Нажмите на кнопку **Удалить** на панели действий.

Документ будет удален из списка.

Действия с МЧД

КриптоАРМ позволяет выполнять основные действия с машиночитаемыми доверенностями: просматривать содержимое доверенности, формировать её печатную форму и проверять актуальный статус МЧД на сайте ФНС.

Печать МЧД

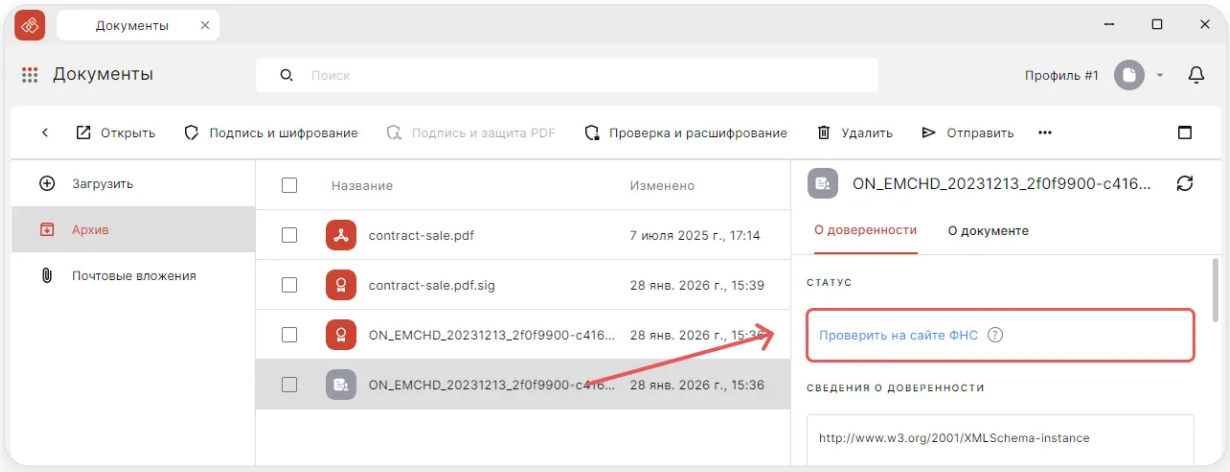
1. Откройте сведения о файле МЧД с расширением `.xml` по инструкции.
2. Перейдите на вкладку **О доверенности**.
3. Нажмите на кнопку **Печать** .
4. Откроется окно с печатной формой МЧД.

МЧД можно распечатать или скачать на устройство.

Проверка статуса МЧД

1. Откройте сведения о файле МЧД с расширением .xml по инструкции.
2. Перейдите на вкладку **О доверенности**.

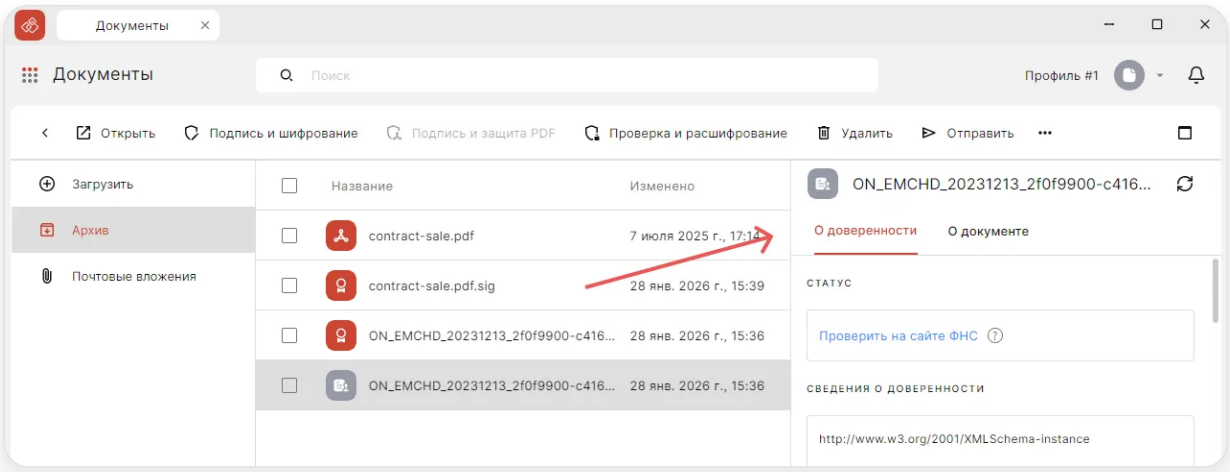
3. В блоке **Статус** нажмите на кнопку **Проверить на сайте ФНС**.



В браузере по умолчанию откроется сайт ФНС со статусом доверенности.

Просмотр печатной формы МЧД

1. Выделите файл МЧД с расширением `.xml` в одном из разделов:
   - Папка **Архив** или **Почтовые вложения**,
   - Мастер **Подпись и шифрование**,
   - Мастер **Проверка и расшифрование**.
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка писем откроется область со сведениями:
   - Нажмите на вкладку **О доверенности** для просмотра печатной формы доверенности,
   - Нажмите на вкладку **О документе** для просмотра сведений о документе.



Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

> ⚠️ **Примечание**: Коды ошибок (0x...) фиксируются для криптопровайдера КриптоПро CSP.

Код ошибки	Ошибка	Описание	Рекомендуемые действия
0x80092004	Не удалось расшифровать файл	Отсутствует сертификат, в адрес которого выполнено шифрование	1. Проверьте наличие в хранилище "Личные сертификаты" нужного сертификата 2. Убедитесь, что сертификат содержит закрытый ключ 3. Проверьте, что это именно тот сертификат, которым производилось шифрование
-	Не удалось расшифровать файл (для файлов, зашифрованных в адрес сертификатов с алгоритмами ГОСТ)	Отсутствует лицензия КриптоАРМ	1. Приобретите лицензию КриптоАРМ 2. Активируйте лицензию в настройках программы
-	Не удалось расшифровать файл	Отсутствует КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
0x8009001d	Не удалось расшифровать файл	Отсутствует действующая лицензия КриптоПро CSP	Установите лицензию КриптоПро CSP
-	Не удалось найти исходный файл для подписи	Исходный документ для файла откреплённой подписи не найден или имеет другое название	1. В боковой панели нажмите **Указать путь к файлу** для выбора исходного документа 2. Укажите путь к исходному документу.

Смотрите также

- Профиль подписи — сохранение параметров операций в профилях для повторного использования.

- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.
- Подключение почтового аккаунта — инструкция по подключению почтовых ящиков в КриптоАРМ.

Открыть статью на сайте

Выполнение операций в командной строке

Научитесь работать с командной строкой (CLI) КриптоАРМ: подписывать, шифровать, расшифровывать и проверять файлы. В этом руководстве собраны команды и практические примеры для Windows, Linux и macOS.

Содержание:

- Общая информация
- Подпись
- Шифрование
- Кодирование и декодирование файлов
- Расшифрование
- Проверка подписи
- Смотрите также

Общая информация

CLI (Command Line Interface, интерфейс командной строки) — это способ управления приложением с помощью текстовых команд, вводимых через терминал или консоль.

Команды определяют, какие операции выполнить, с какими параметрами и над какими файлами.

CLI также подходит для автоматизации — выполнения операций без участия пользователя в составе систем обмена и скриптов `.bat` и `.sh`.

Важные замечания

- Перед использованием CLI убедитесь, что приложение настроено для работы с электронной подписью.

  > 🔍 Подробную информацию о настройке можно найти в инструкции Начало работы.

- Перед вводом команды необходимо указать путь до исполняемого файла. После указания пути до исполняемого файла необходимо поставить пробел, затем вводить команды.
- Все команды и параметры пишутся через пробел.

Синтаксис команд

- `-команда` — команда пишется первой, после пути до исполняемого файла. Далее указываются значения переменных и параметры операции.
- `<текст>` — указываются значения переменной, такие как Серийный номер сертификата, Путь до исходного файла, OID алгоритма шифрования и т.п.
- `[текст]` — необязательные параметры, которые можно как задать, так и не задавать, тогда будут использоваться значения по умолчанию.

Пути к исполняемым файлам

Система	Путь при установке по умочанию
Windows	`%ProgramFiles%\CryptoARM\cryptoarm.exe"`
Linux	`/opt/cryptoarm6/cryptoarm`
macOS	`/Applications/cryptoarm.app/Contents/MacOS/cryptoarm`

Подпись

Команда: `sign` или `sig`

Команда позволяет выполнить операцию подписи одного или нескольких файлов.

Если в качестве исходного файла указать уже подписанный документ, то будет добавлена соподпись.

Синтаксис

```
sign  -cert <serial> [-enc DER|BASE64] [-detached] [-save-copy] [-pin <PIN>] [-ext <sign file extention>] [-sign-type <CadesT|CadesA|CadesXLT1> -tsp <tsp-addr> [-ocsp <ocsp-addr>] [-proxy <proxy-addresss> [-proxy-port <port>] [-proxy-login <login>] [-proxy-password <password>]]] <source-file-name>|<source-folder> <encrypted-file-path>|<folder-to-save-signed>
```

Описание команды

Общие параметры подписи

Параметр	Описание	По умолчанию
`--cert <serial>`	Серийный номер сертификата подписи	—
`--standard <type>`	Стандарт подписи CAdES (`CAdES-BES`, `CAdES-T`, `CAdES-A`, `CAdES-XLT1`)	`"CAdES-BES"`

Параметр	Описание	По умолчанию
`--detached`	Создать отделённую подпись	Отключено
`--save-copy`	Сохранять копию результата в Архиве	Отключено
`--pin <pin-code>`	ПИН-код ключа сертификата	—
`--enc <DER|BASE-64>`	Формат сохранения подписи	`"DER"`
`--ext <sig|p7s|sgn|sign|bin>`	Расширение файла подписи	`"sig"`
`-f, --force`	Использовать недействительный сертификат без подтверждения	Отключено
`--logcrypto`	Включение лога trusted-crypto	Отключено

Объединение подписей

Подробнее про функцию **Объединение подписей** читайте в инструкции Подпись и шифрование.

Параметр	Описание	По умолчанию
`--join-signs <files...>`	Список путей к файлам подписей для объединения (минимум два файла)	—
`--join-signs-folder <folder>`	Путь к папке с файлами подписей для объединения	—

Параметры подписи PDF (PAdES)

Положение и внешний вид штампа подписи:

Параметр	Описание	По умолчанию
`--pades`	Подписать PDF по стандарту PAdES	Отключено
`--overwrite-original-pdf`	Перезаписать исходный файл после подписи	Отключено
`--stamp-width <width>`	Ширина штампа	—
`--stamp-height <height>`	Высота штампа	—
`--stamp-padding-left <padding>`	Отступ слева	—
`--stamp-padding-bottom <padding>`	Отступ снизу	—
`--stamp-color <color>`	Цвет штампа	`#000000`

Параметр	Описание	По умолчанию
`--stamp-no-background`	Прозрачный фон под штамп	Отключено
`--stamp-page <number>`	Страница размещения	Последняя
`--stamp-on-all-pages`	Дублировать штамп на всех страницах	Отключено
`--stamp-pixel-ratio <ratio>`	Pixel Ratio для рендеринга штампа	1

Содержимое штампа подписи:

Параметр	Описание	По умолчанию
`--stamp-mchd <number>`	Добавить номер МЧД в штамп	—
`--stamp-individual`	Добавить ФИО владельца сертификата	—
`--stamp-job-position <value>`	Добавить должность	—
`--stamp-organization-name <value>`	Добавить организацию	—
`--stamp-issuer-friendly-name <value>`	Добавить издателя сертификата	—
`--stamp-mark <value>`	Добавить примечание	—
`--stamp-description <value>`	Добавить описание	—
`--stamp-location <value>`	Добавить местоположение	—
`--stamp-sign-time`	Добавить дату и время подписи (системное время)	—

⚠️ Ключ `--overwrite-original-pdf` необратимо изменяет исходный файл. Используйте его с осторожностью, особенно в скриптах, где путь к файлу контролируется.

Сетевые параметры

Параметр	Описание	По умолчанию
`--tsp <url>`	Адрес службы метки времени TSP	—
`--ocsp <url>`	Адрес службы OCSP	—
`--proxy <address>`	Адрес прокси-сервера	—

Параметр	Описание	По умолчанию
`--proxy-port <port>`	Порт прокси	—
`--proxy-login <login>`	Логин для прокси	—
`--proxy-password <password>`	Пароль для прокси	—

Ввод и вывод

Параметр	Описание	По умолчанию
`--source-file <file>`	Путь к подписываемому файлу	—
`--source-folder <folder>`	Подписать все файлы из папки	—
`--signed-file-path <file>`	Путь для результата подписи	—
`--folder-save-signed <folder>`	Папка для подписанных файлов	—
`-h, --help`	Показать справку	—

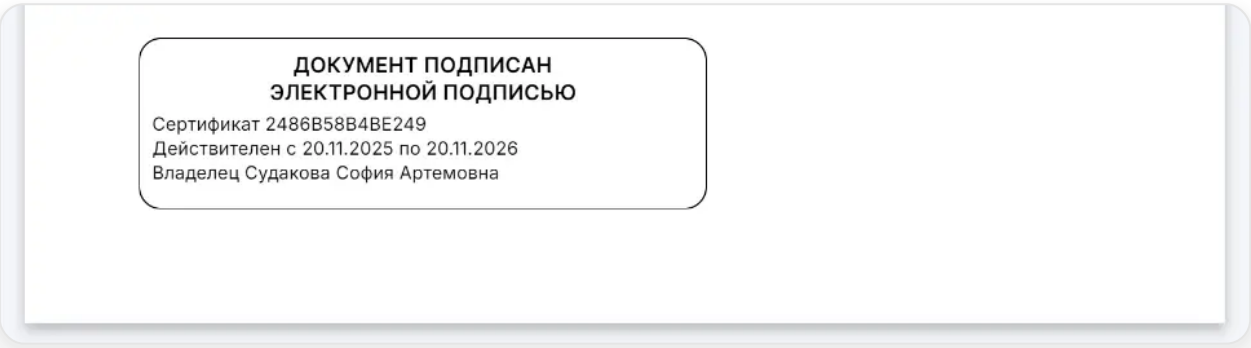
Практические примеры

Пример 1: Подпись со стандартным штампом на последней странице

В этом примере подписывается PDF-файл со штампом размером 100×30 мм, расположенным в 20 мм от левого и нижнего края последней страницы.

```
"C:\Program Files\CryptoARM\cryptoarm.exe" sign \
  --source-file "C:\Doc\Пример.pdf" \
  --cert "5883d78e000300093ab6" \
  --pin "12345678" \
  --pades \
  --stamp-width 100 \
  --stamp-height 30 \
  --stamp-padding-left 20 \
  --stamp-padding-bottom 20
```

Внешний вид штампа:

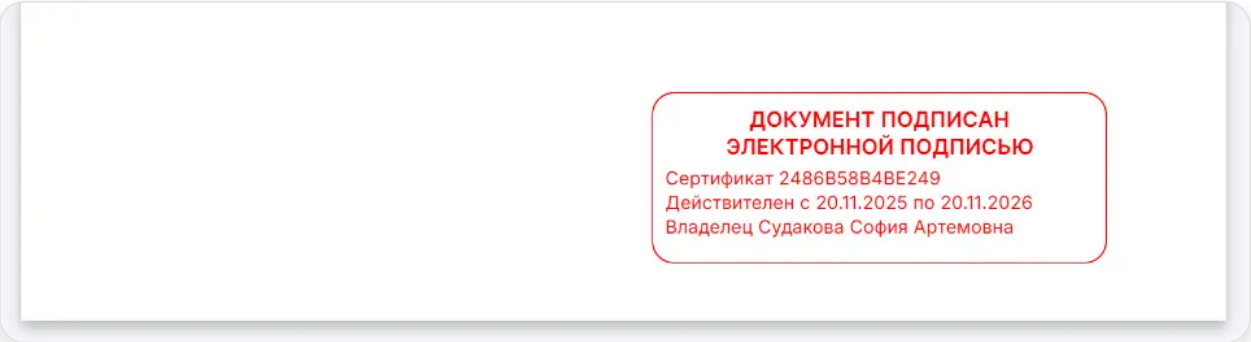


Пример 2: Подпись со штампом красного цвета на всех страницах

В этом примере подписывается PDF-файл со штампом красного цвета. Штамп размещен в правом нижнем углу на каждой странице документа.

```
"C:\Program Files\CryptoARM\cryptoarm.exe" sign \
  --source-file "C:\Doc\Пример.pdf" \
  --cert "5883d78e000300093ab6" \
  --pin "12345678" \
  --pades \
  --stamp-width 80 \
  --stamp-height 30 \
  --stamp-padding-left 110 \
  --stamp-padding-bottom 10 \
  --stamp-color "#FF0000" \
  --stamp-on-all-pages
```

Внешний вид штампа:



Пример 3: Подпись документа с меткой времени

В этом примере подписывается файл со стандартом CAdES-T, который включает метку времени. Файл будет сохранен в формате `.p7s` с кодировкой `BASE-64`. Копия файла будет помещена в папку **Архив** раздела **Документы**.

```
"C:\Program Files\CryptoARM\cryptoarm.exe" sign \
  --source-file "C:\Documents\Example.pdf" \
  --cert "5883d78e000300093ab6" \
  --pin "12345678" \
  --standard "CAdES-T" \
  --tsp "https://example.com/tsp/tsp.srf" \
  --enc "BASE-64" \
  --ext "p7s" \
  --save-copy \
```

Шифрование

Команды: `encrypt` или `enc`

Команда позволяет выполнить шифрование одного или нескольких файлов в адрес одного или нескольких сертификатов.

Синтаксис

```
encrypt --cert <серийный номер сертификата> [--enc DER|BASE64][--alg <alg-oid>] [--delete-source][--save-copy] [--ext <encrypted file extension>] --source-file <путь к файлу>|--source-folder <путь к папке> --encrypted-file-path <путь к файлу с новым именем для сохранения результата>|--folder-save-encrypted <путь к папке для сохранения результата>
```

Описание команды

Параметр	Описание	Значение по умолчанию
`--cert <serial...>`	Серийный номер сертификата подписи (можно указать несколько)	—
`--alg <alg-oid>`	OID алгоритма шифрования	`"1.2.643.2.2.21"`
`--delete-source`	Удаление исходного файла после шифрования	Отключено
`--save-copy`	Сохранение копии результата в Архиве	Отключено
`--ext <enc|p7m|p7e|pem>`	Расширение создаваемого шифрованного файла	`"enc"`
`--enc <DER|BASE-64>`	Кодировка шифруемого файла	`"DER"`
`--logcrypto`	Включает лог trusted-crypto	Отключено
`-f, --force`	Автоматическое согласие на использование недействительных сертификатов	Отключено
`--source-file <path-file>`	Путь к файлу для шифрования	—
`--encrypted-file-path <path-file>`	Путь к файлу для сохранения результата шифрования	—
`--folder-save-encrypted <path-folder>`	Путь к папке для сохранения зашифрованных файлов	—
`--source-folder <path-folder>`	Путь к папке с файлами для шифрования	—

Параметр	Описание	Значение по умолчанию
`-h, --help`	Вывод справки команды	—

Практический пример

В этом примере шифруется файл `Example.txt` с использованием сертификата с серийным номером `5883d78e000300093ab6`. Результат шифрования будет сохранен в файл `Encrypted_Example.enc`. Исходный файл будет удален, а копия зашифрованного файла сохранится в папку **Архив** раздела **Документы**.

```
"C:\Program Files\CryptoARM\cryptoarm.exe" encrypt \
  --cert "5883d78e000300093ab6" \
  --enc "DER" \
  --alg "1.2.643.2.2.21" \
  --delete-source \
  --ext "enc" \
  --save-copy
  --source-file "C:\Documents\Example.txt" \
  --encrypted-file-path "C:\Documents\Encrypted_Example.enc"
```

Кодирование и декодирование файлов

Для команд `sign` (файлы подписи), `certificates` (файлы сертификатов) и `encrypt` (зашифрованные данные) доступны параметры кодирования и декодирования файлов. Параметры позволяют преобразовать бинарные данные в текстовый формат `BASE64` и обратно.

Кодирование удобно использовать, если необходимо передать файл в текстовом виде, например через системы, которые не поддерживают передачу бинарных данных.

Команда	Описание
`--decode <infile>`	Декодирование файла подписи из формата `DER`в `PEM` (`BASE64`).
`encode <infile>`	Кодирование файла подписи из формата `PEM` (`BASE64`) в `DER`.

Параметр `<infile>` – путь к входному файлу.

Расшифрование

Команды: `decrypt` или `dec`

Команда позволяет выполнить расшифрование одного или нескольких зашифрованных файлов.

Синтаксис

```
decrypt [-pin <PIN>] [-save-copy] <source-file-name>|<source-folder> <encrypted-file-path>|
<folder-to-save-decrypted>
```

Описание команды

Параметр	Описание	Значение по умолчанию
`--save-copy`	Сохранение копии результата в Архиве	Отключено
`--logcrypto`	Включает лог trusted-crypto	Отключено
`--pin <pin-code>`	Пин-код ключа расшифрования	-
`--source-file <path-file>`	Путь к файлу для расшифрования	-
`--source-folder <path-folder>`	Путь к папке с файлами для расшифрования	-
`--decrypted-file-path <path-file>`	Путь для сохранения расшифрованного файла	-
`--folder-save-decrypted <path-folder>`	Путь к папке для сохранения результатов расшифрования	-
`-h, --help`	Вывод справки команды	-

Практический пример

В этом примере расшифровывается файл `Encrypted_Example.enc`. Для сертификата шифрования используется ПИН-код `12345678`. Расшифрованный результат сохраняется в `C:\Documents\`.

```
"C:\Program Files\CryptoARM\cryptoarm.exe" decrypt \
  --pin "12345678" \
  --source-file "C:\Documents\Encrypted_Example.enc" \
  --decrypted-file-path "C:\Documents\Decrypted_Example.txt"
```

Проверка подписи

Команды:

- `verify` или `ver`
- `verify_ts` или `vts` - проверка штампов времени из подписи

Команда позволяет выполнить проверку одной или нескольких подписей, либо штампов времени в файле подписи. Есть возможность сохранения отчёт о проверке в отдельный файл в формате `pdf` или `json`.

Синтаксис

```
verify [-save-report|-r [<report-file>]] <source-file-name>|<source-folder>
```

```
verify_ts [-save-report|-r [<report-file>]] <source-file-name>|<source-folder>
```

Описание команды

Параметр	Описание	Значение по умолчанию
`-r-pdf, --save-report-pdf <report-folder>`	Сохранение копии результата в формате PDF	—
`-r-pdf-m, --save-report-pdf-merged <report-folder>`	Сохранение копии результата в формате PDF (объединённый файл)	—
`-r-json, --save-report-json <report-file-path>`	Сохранение копии результата в формате JSON	—
`--document <original-file>`	Указание исходного файла для откреплённой подписи	—
`--logcrypto`	Включение логирование trusted-crypto	Отключено
`--source-file <source-file-path>`	Указание файла подписи для проверки	—
`--source-folder <source-folder-path>`	Указание папки для пакетной проверки подписей	—
`-u, --unsign <output-folder-path>`	Извлечение исходного документа из подписанного файла	—
`-h, --help`	Вывод справки по команде	—

Практический пример

В этом примере выполняется проверка подписи файлов в папке `C:\Foldername` с сохранением отчета о проверке в формате `pdf` в папку с проверяемыми файлами.

```
"C:\Program Files\CryptoARM\cryptoarm.exe" ver --source-folder C:\Foldername -r-pdf
```

Смотрите также

- Активация лицензии — инструкции по активации лицензий КриптоАРМ и КриптоПро CSP.
- Подпись и шифрование — руководство по созданию электронных подписей и шифрованию файлов.
- Проверка и расшифрование — проверка подписей и расшифрование документов.
- Подпись и защита PDF — мастер для работы с PDF: просмотр, разметка областей, добавление подписей и сертифицирующая подпись.

Открыть статью на сайте

Управление сертификатами

В этом разделе вы узнаете о возможностях раздела **Сертификаты**, научитесь находить нужные сертификаты и перейдёте к подробным инструкциям по установке, экспорту и управлению ключевыми контейнерами.

Содержание:

- Обзор раздела «Сертификаты»
- Профили доверия
- Проверка статуса сертификата
- Поиск и фильтрация сертификатов
- Смотрите также

Обзор раздела «Сертификаты»

Раздел **Сертификаты** предназначен для просмотра и управления сертификатами, установленными в хранилищах операционной системы и криптографических провайдеров.

В разделе можно:

- искать и фильтровать сертификаты;
- переключать профили доверия;
- просматривать статус и сведения о сертификатах;
- устанавливать сертификаты;
- экспортировать и удалять сертификаты;
- создавать запросы на сертификаты;
- создавать самоподписанные сертификаты;
- управлять ключевыми контейнерами.

Хранилища сертификатов

Хранилища сгруппированы по назначению и отображаются в левой части окна. Выберите нужное хранилище, чтобы просмотреть содержащиеся в нём сертификаты.

Хранилище	Назначение
Личные	Содержит личные сертификаты пользователя с соответствующими закрытыми ключами. Используются для создания электронной подписи и расшифрования данных.
Другие пользователи	Содержит сертификаты других пользователей и организаций. Используются для проверки подписей и шифрования данных для получателей.

Хранилище	Назначение
Удостоверяющие центры	Содержит сертификаты доверенных корневых и промежуточных удостоверяющих центров, участвующих в построении цепочки доверия.
Списки отзыва	Содержит списки отозванных сертификатов (CRL). Используются для проверки статуса сертификатов и определения, были ли они отозваны удостоверяющим центром.
Запросы	Содержит запросы на получение сертификатов (CSR). Используются для просмотра, экспорта и передачи запросов в удостоверяющий центр для выпуска сертификата.
Ключи	Содержит ключевые контейнеры с закрытыми ключами.

> 💡 **Совет:** Для создания электронной подписи личный сертификат должен находиться в хранилище **Личные** и быть связан с соответствующим закрытым ключом.

Профили доверия

Если в вашей системе смешаны сертификаты разных криптоалгоритмов (ГОСТ и RSA), их легко перепутать. Профили доверия решают эту проблему: они фильтруют сертификаты по типу алгоритма, чтобы вы видели только те, которые нужны для текущей задачи.

В текущей версии доступны два профиля доверия:

Профиль	Отображаемые сертификаты
Российская Федерация	Сертификаты с алгоритмами ГОСТ
Открытая криптография	Сертификаты с алгоритмами RSA

Профили доверия используются:

- в разделе **Сертификаты**;
- в окнах выбора сертификатов.

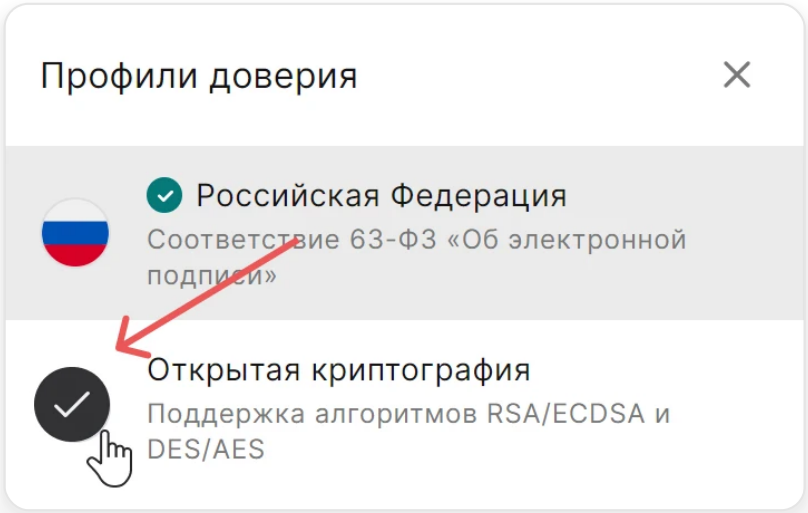
> 💡 Профиль доверия влияет только на отображение сертификатов. Он не изменяет сертификаты и не влияет на выполнение криптографических операций.

Переключение между профилями доверия

Переключение профиля выполняется аналогично выбору профиля подписи в разделе **Документы**.

Чтобы переключить профиль доверия:

1. Перейдите в раздел **Сертификаты**.
2. Нажмите на название активного профиля в верхней части окна.
3. В открывшемся окне нажмите на иконку профиля, который хотите сделать активным.



После переключения профиля список сертификатов обновится автоматически.

Проверка статуса сертификата

В КриптоАРМ можно проверить статус сертификата и просмотреть его подробную информацию.

Проверка позволяет убедиться, что сертификат:

- является действительным;
- не истёк и не отозван;
- имеет корректную цепочку доверия;
- связан с закрытым ключом (для личных).

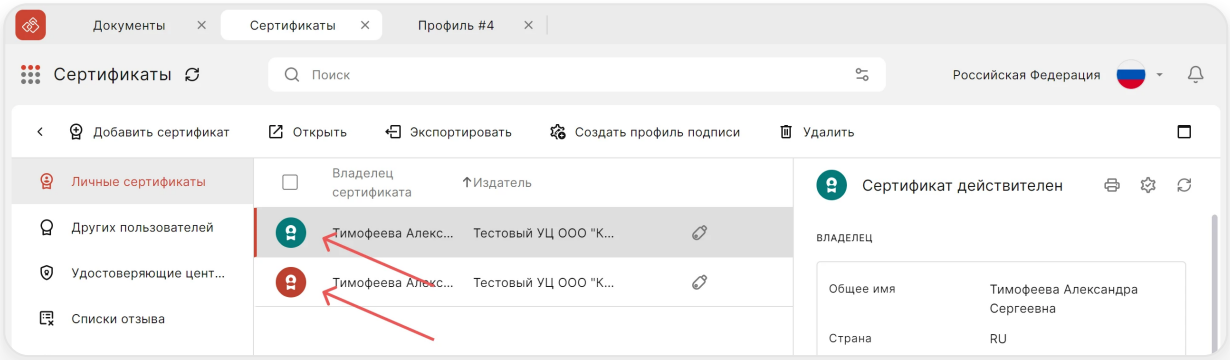
Статус сертификата отображается в списке сертификатов с помощью цветового индикатора на значке сертификата.

Индикатор	Статус	Описание
🟢 Зеленый	Действительный	

Индикатор	Статус	Описание
		Сертификат успешно прошёл проверку и может использоваться
🔴 Красный	Недействительный	Сертификат не может использоваться, например, из-за окончания срока действия

Чтобы получить подробную информацию о сертификате:

1. Перейдите в раздел **Сертификаты**.
2. Выберите нужный сертификат.
3. Нажмите кнопку **Подробнее** .

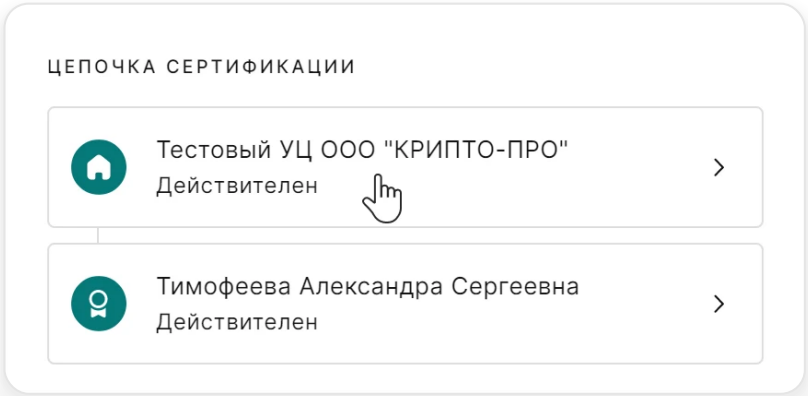


В открывшемся окне можно посмотреть подробные сведения о сертификате, результат проверки и цепочку сертификации.

Цепочка сертификации показывает путь доверия от сертификата пользователя до корневого удостоверяющего центра.

Чтобы просмотреть сведения о сертификате из цепочки:

1. Откройте сведения о сертификате.
2. Найдите блок **Цепочка сертификации**.
3. Нажмите название нужного сертификата.



Поиск и фильтрация сертификатов

Чтобы быстро найти нужный сертификат, используйте строку поиска или расширенную фильтрацию.

Расширенная фильтрация позволяет выполнять поиск одновременно по нескольким критериям.

Доступны следующие параметры фильтрации:

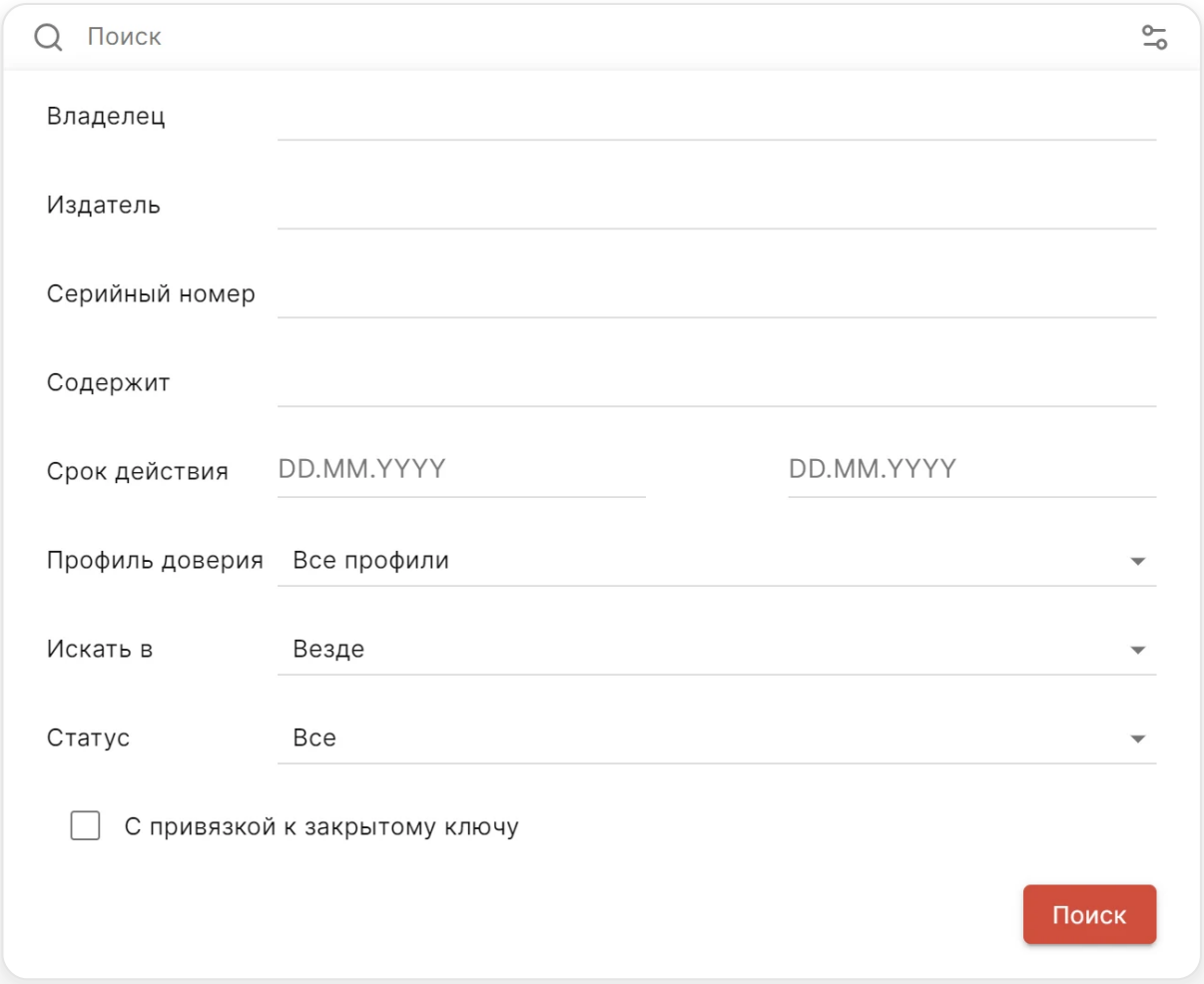
Критерий	Описание
Владелец	Сертификаты конкретного пользователя или организации
Издатель	Сертификаты, выпущенные определённым удостоверяющим центром
Серийный номер	Серийный номер сертификата.
Содержимое	Поиск по информации, содержащейся в сертификате.
Срок действия	Действующие, просроченные или ещё не вступившие в силу сертификаты.
Профиль доверия	Российская Федерация или Открытая криптография.
Хранилище	Хранилище, в котором расположен сертификат.
Статус	Например, действительный или недействительный сертификат.
Привязка к закрытому ключу	Наличие или отсутствие соответствующего закрытого ключа.

Фильтры можно использовать совместно, что позволяет быстро найти нужный сертификат даже при работе с большим количеством сертификатов.

Расширенная фильтрация

Чтобы воспользоваться расширенной фильтрацией:

1. Перейдите в раздел **Сертификаты**.
2. Нажмите на кнопку **Открыть фильтр** .
3. Укажите один или несколько критериев поиска.
4. Нажмите **Поиск**.



Быстрый поиск сертификатов

Если известны основные сведения о сертификате, воспользуйтесь строкой поиска.

Поиск выполняется по основным свойствам сертификата, включая:

- владельца;
- издателя;
- серийный номер;

- содержимое сертификата.

Чтобы быстро найти сертификат:

1. Перейдите в раздел **Сертификаты**.
2. Начните вводить текст в строке поиска.

По мере ввода список сертификатов обновляется автоматически.

Смотрите также

- Установка сертификатов — инструкция по установке личных, корневых и промежуточных сертификатов, сертификатов других пользователей и списков отзыва (CRL).
- Экспорт и удаление сертификатов — инструкция по экспорту и удалению сертификатов в КриптоАРМ.
- Действия с ключевыми контейнерами — работа с ключевыми контейнерами для установки и привязки сертификатов.

Открыть статью на сайте

Как установить сертификаты в КриптоАРМ

В этом руководстве вы узнаете, как установить сертификаты электронной подписи в КриптоАРМ: личные, корневые, промежуточные, сертификаты других пользователей и списки отзыва (CRL).

Руководство подходит для первоначальной настройки КриптоАРМ, устранения ошибок проверки подписи и подготовки среды для подписи и шифрования документов.

Содержание:

- Установка личного сертификата
- Установка сертификата из DSS
- Установка корневого и промежуточного сертификатов
- Установка сертификата другого пользователя
- Установка списка отзыва
- Возможные ошибки
- Смотрите также

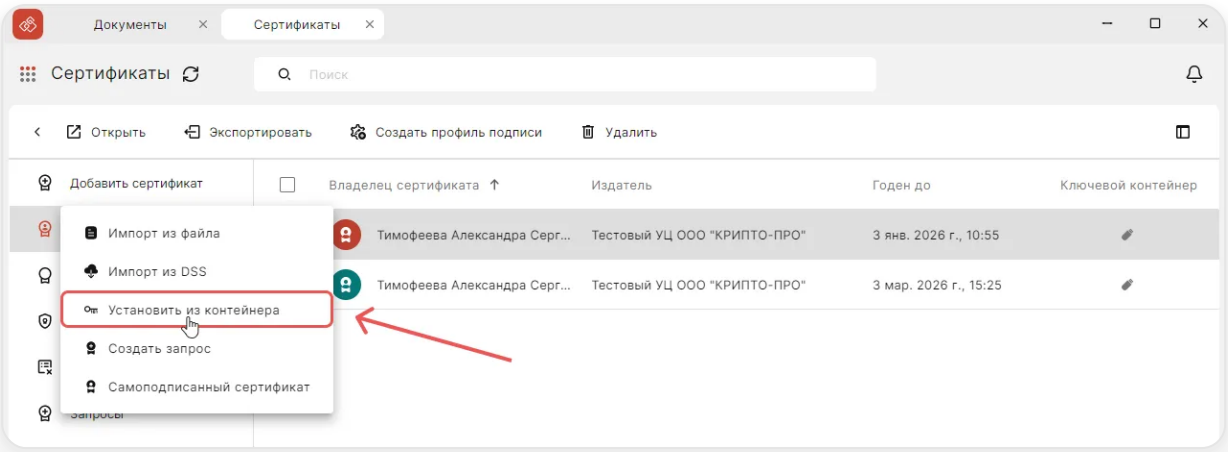
> 🚨 Чтобы сертификаты корректно проверялись, в системе должны быть установлены корневые и промежуточные сертификаты цепочки сертификации, а также загружен актуальный список отозванных сертификатов (CRL).
> Подробнее см. установка корневых и промежуточных сертификатов и установка списка отзыва.

Установка личного сертификата

Установка из ключевого контейнера

Основной способ (через раздел «Сертификаты»)

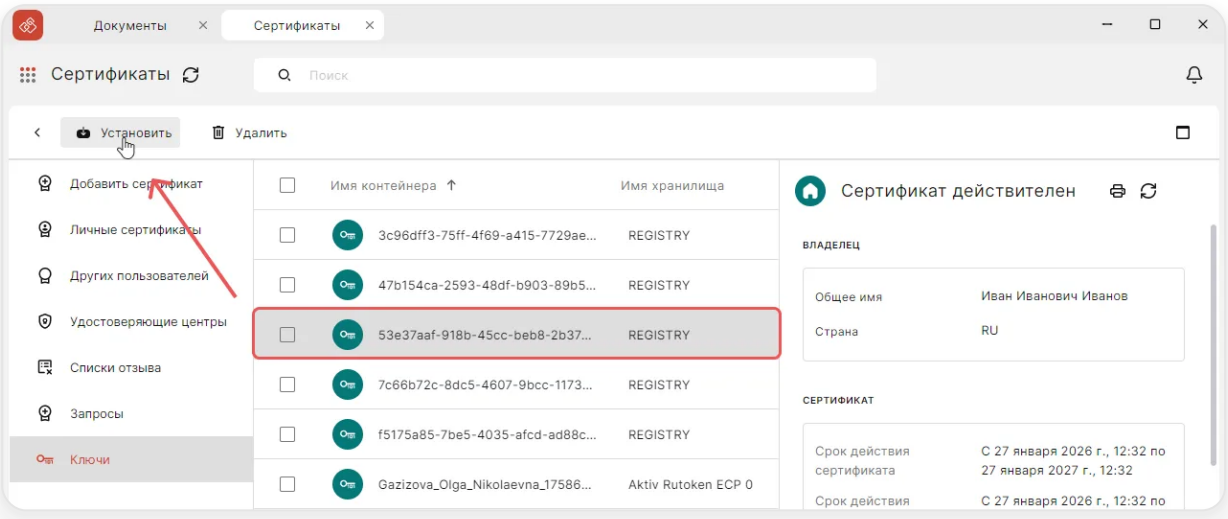
1. Подключите токен к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Нажмите кнопку **Добавить сертификат** в боковом меню.
4. В открывшемся списке действий выберите **Установить из контейнера**.



5. Откроется список контейнеров.
6. Выделите необходимый контейнер в списке.

> 💡 **Совет**: С помощью кнопки **Подробно** можно просмотреть сертификат, находящийся в контейнере.

7. Нажмите кнопку **Установить** на панели действий.



8. При необходимости введите пароль к ключевому контейнеру.

После успешного импорта сертификат появится в разделе **Личные сертификаты**.

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. В открывшемся окне нажмите на кнопку **Добавить** в верхней части окна.
3. Выберите действие **Установить из контейнера**.

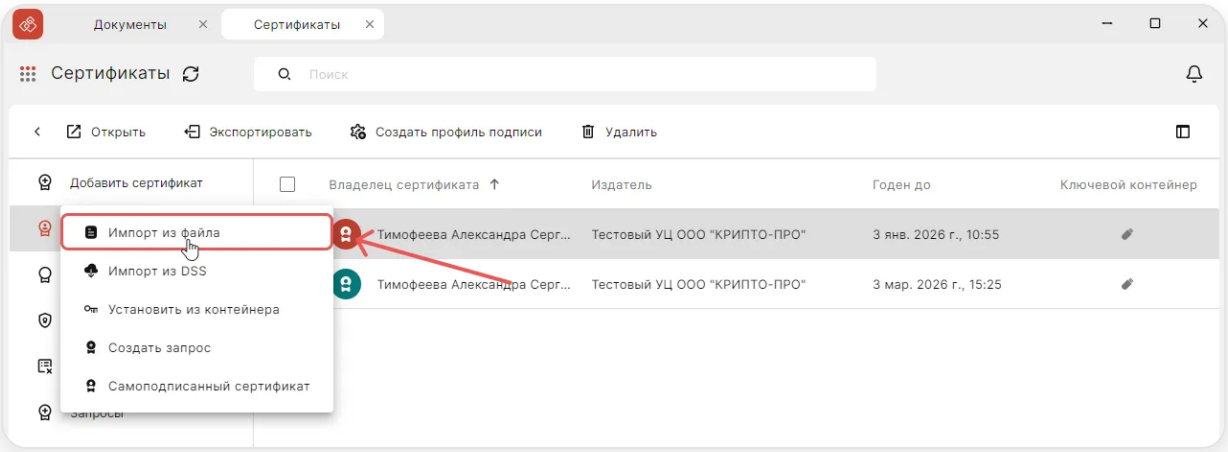
4. В открывшемся окне выберите необходимый контейнер в списке и нажмите кнопку **Установить**.
5. При необходимости введите пароль к ключевому контейнеру.

> 💡 **Совет**: Если после установки сертификат не появляется в разделе **Личные сертификаты**, обновите список сертификатов с помощью соответствующей кнопки .

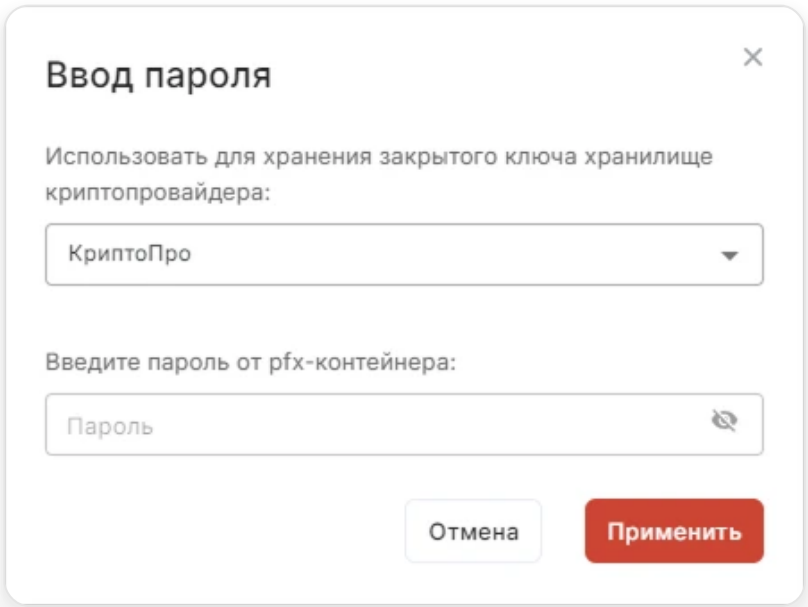
Установка из файла .pfx

Основной способ (через раздел «Сертификаты»)

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Импорт из файла**.



4. В файловом менеджере выберите файл сертификата `.pfx`.
5. В открывшемся окне **Ввод пароля**:
   - Выберите криптопровайдер, в хранилище которого будет установлен сертификат. В текущей версии приложения поддерживаются 2 провайдера: **КриптоПро CSP** и **OpenSSL**.
   - Введите пароль от pfx-контейнера.



6. При необходимости задайте новый пароль к ключевому контейнеру.

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. В открывшемся окне нажмите на кнопку **Добавить** ⊕ в верхней части окна.
3. Выберите действие **Импорт из файла**.
4. В файловом менеджере выберите файл сертификата `.pfx`.
5. В открывшемся окне **Ввод пароля**:
   - Выберите криптопровайдер, в хранилище которого будет установлен сертификат. В текущей версии приложения поддерживаются 2 провайдера: **КриптоПро CSP** и **OpenSSL**.
   - Введите пароль от pfx-контейнера.
6. При необходимости задайте новый пароль к ключевому контейнеру.

Установка с привязкой к ключевому контейнеру

Данный способ установки используется для импорта сертификата открытого ключа и его последующего связывания с существующим ключевым контейнером, содержащим соответствующий закрытый ключ. В результате сертификат становится доступным для использования в криптографических операциях.

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Импорт из файла**.
4. В файловом менеджере выберите файл сертификата `.cer` или `.crt`.
5. При необходимости введите пароль к ключевому контейнеру.

Установка сертификата из DSS

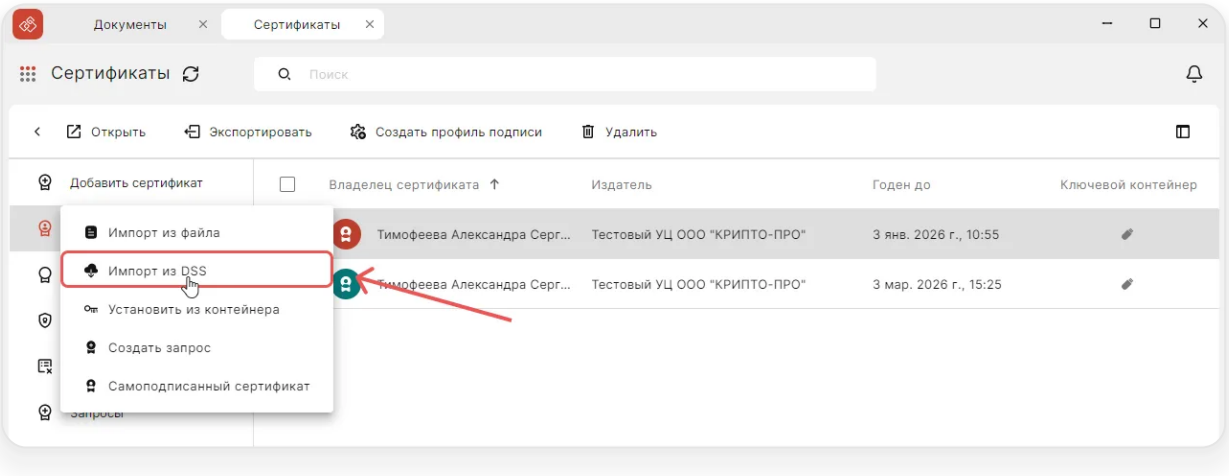
Сертификат DSS — сертификат электронной подписи, ключ от которого генерируется и хранится на сервере Удостоверяющего центра. Благодаря этому владельцу сертификата не требуется записывать и хранить ключ на токене или компьютере. Это позволяет ему подписывать электронные документы с любого устройства и из любого места, где есть доступ в интернет.

Для установки сертификата из DSS необходимо создать подключение к сервису DSS.

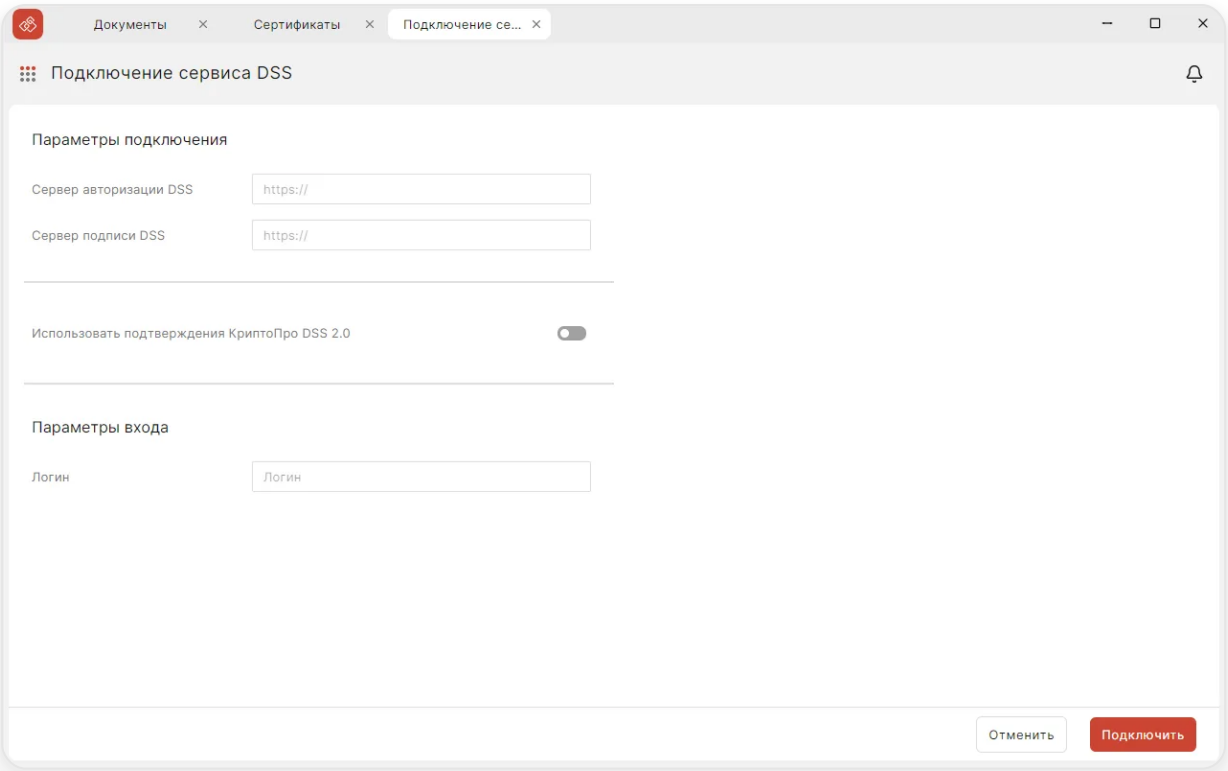
Создание подключения к сервису DSS

Основной способ (через раздел «Сертификаты»)

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В открывшемся списке действий выберите **Импорт из DSS**.



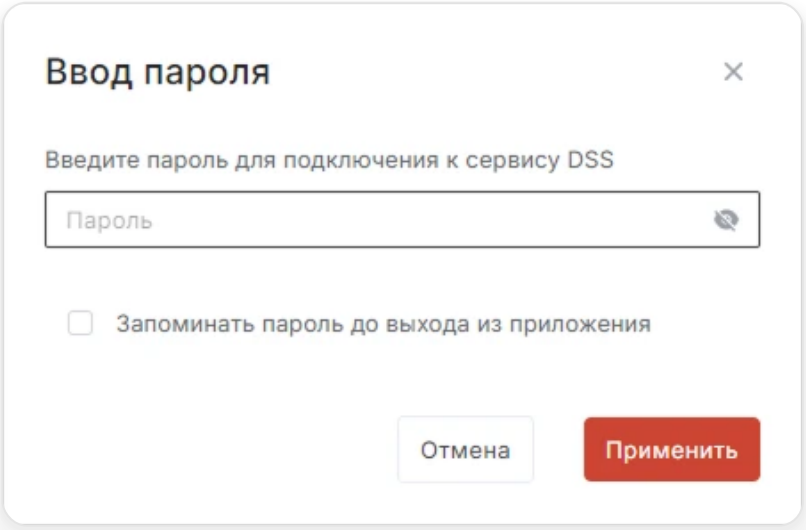
4. Откроется новая вкладка с формой подключения сервиса DSS.
5. Заполните поля:
   - **Сервер авторизации DSS** и **Сервер DSS** — данные адреса необходимо получить в организации, предоставившей вам сертификат электронной подписи;
   - **Использовать подтверждения КриптоПро DSS 2.0** — нужно включить данную опцию, если используется продукт КриптоПро DSS 2.0;
   - **Логин** — ваш логин для доступа к сертификату.



6. Нажмите **Подключить**.

7. Если в личном кабинете DSS в настройках стоит подтверждение по паролю, то на следующем шаге введите пароль для подключения к сервису DSS и нажмите кнопку **Применить**.

   Чтобы каждый раз не вводить пароль для подключения при работе с сертификатом DSS, можно установить флаг **Запоминать пароль до выхода из приложения**.



   Если пароль не задан, то данный шаг пропускается.

8. Если в личном кабинете DSS в настройках стоит подтверждение аутентификации по SIM-карте или с помощью мобильного приложения, то на следующем шаге появляется информационное окно с ожиданием подтверждения операции на телефоне.

   Подтвердите операцию на телефоне.

   Если идентификация настроена не с помощью телефона, то данный шаг пропускается.

При успешной аутентификации сертификат DSS автоматически помещается в хранилище **Личные сертификаты**.

> 💡 Сертификаты DSS в списке отмечаются специальной иконкой ☁.

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. В открывшемся окне нажмите кнопку **Добавить** ⊕ в верхней части окна.
3. Выберите действие **Импортировать из DSS**.
4. Откроется новая вкладка с формой подключения сервиса DSS.
5. Следуйте шагам из инструкции Основной способ (через раздел «Сертификаты»).

Установка корневого и промежуточного сертификатов

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.

Чтобы получить корневой сертификат, посетите официальный сайт удостоверяющего центра. Его обычно можно найти в разделах «Поддержка», «Загрузки» или «Документы».

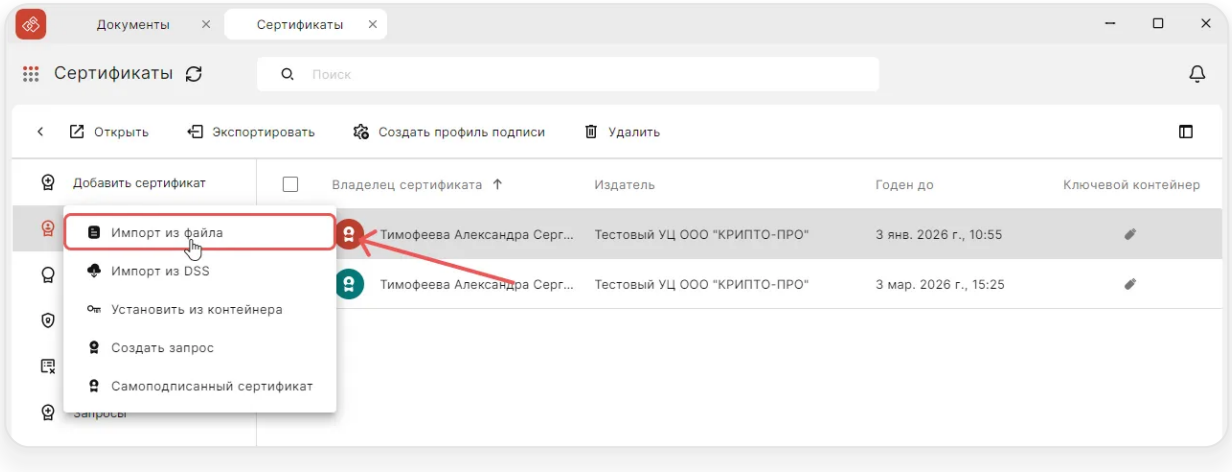
Всегда скачивайте сертификаты только с официальных сайтов УЦ.

Установка из файла

> ⚠️ **Примечание**: Для установки корневого сертификата удостоверяющего центра могут потребоваться права администратора.

Основной способ (через раздел «Сертификаты»)

1. Перейдите в раздел **Сертификаты** → **Удостоверяющие центры**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся меню действий выберите **Импорт из файла**.



4. В окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
5. Подтвердите запрос на установку сертификата.

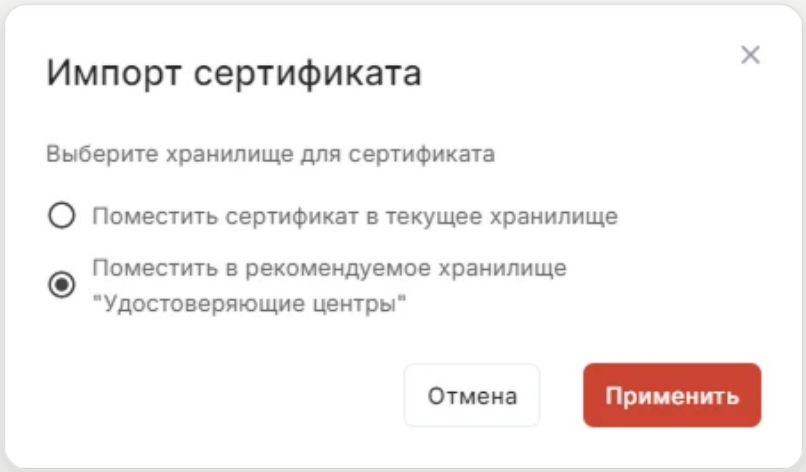
При успешной установке сертификат появится в хранилище сертификатов **Удостоверяющие центры**.

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Сертификаты других пользователей**.
2. В открывшемся окне нажмите кнопку **Добавить** ⊕ в верхней части окна.
3. Выберите действие **Импортировать из файла**.
4. В окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
5. Подтвердите запрос на установку сертификата.

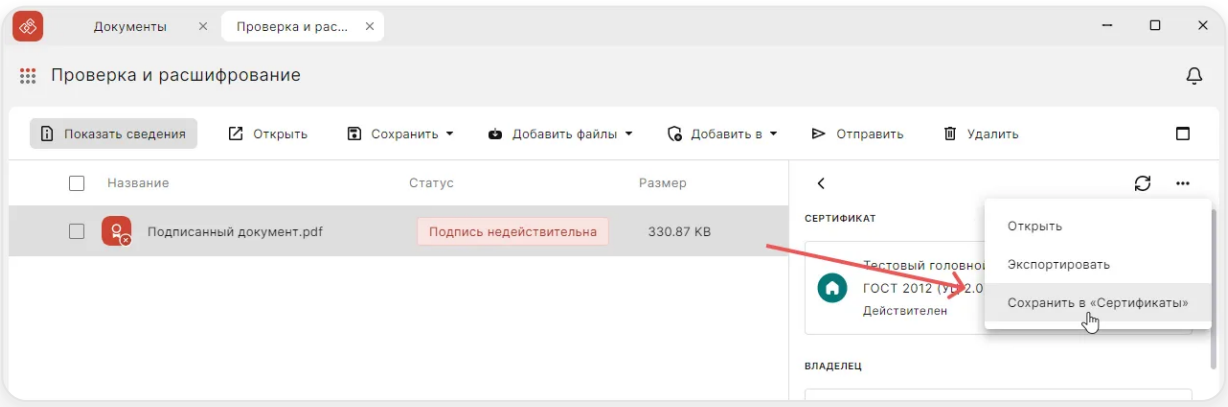
При успешной установке сертификат появится в хранилище сертификатов **Удостоверяющие центры**.

⚠️ **Примечание**: Если выбрано другое хранилище для установки сертификата, КриптоАРМ запросит подтверждение. Для установки сертификата в хранилище «Удостоверяющие центры» выберите опцию «Поместить в рекомендуемое хранилище "Удостоверяющие центры"».



Установка при проверке подписи

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование** (см. Проверка подписи документа).
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка писем откроется область со сведениями.
4. В блоке **Цепочка сертификации** нажмите на сертификат, который необходимо установить.
5. Откроются сведения о сертификате.
6. Вызовите меню действий по кнопке **Еще**.



7. Нажмите на **Сохранить сертификат**.

При успешной установке сертификат появится в хранилище сертификатов **Удостоверяющие центры**.

Установка сертификата другого пользователя

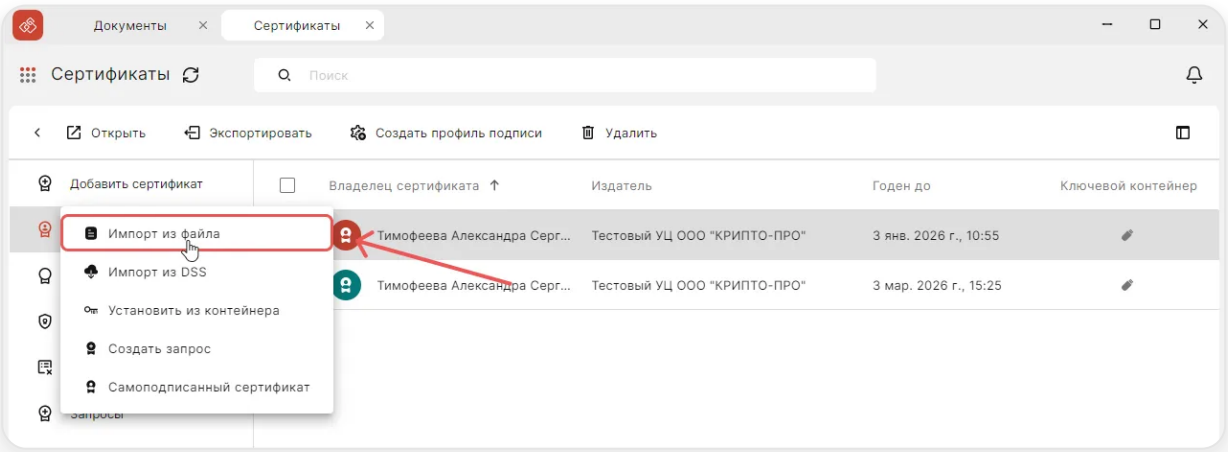
Для шифрования документов, адресованных другому пользователю, вам потребуется его сертификат.

Установка сертификата, который был отправлен вам другим пользователем, происходит в хранилище сертификатов **Других пользователей**. Он нужен для шифрования документов в адрес этого сертификата. Такой сертификат устанавливается без закрытого ключа.

Установка из файла

Основной способ (через раздел «Сертификаты»)

1. Перейдите в раздел **Сертификаты** → **Других пользователей**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В открывшемся меню действий выберите **Импорт из файла**.



4. В окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
5. Подтвердите запрос на установку сертификата.

При успешной установке сертификат появится в списке хранилища сертификатов **Других пользователей**.

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Сертификаты других пользователей**.
2. В открывшемся окне нажмите кнопку **Добавить** ⊕ в верхней части окна.
3. Выберите действие **Импортировать из файла**.

4. В открывшемся окне файлового менеджера выберите файл сертификата (обычно `.cer` или `.crt`).
5. Подтвердите запрос на установку сертификата.

При успешной установке сертификат появится в списке хранилища сертификатов **Других пользователей**.

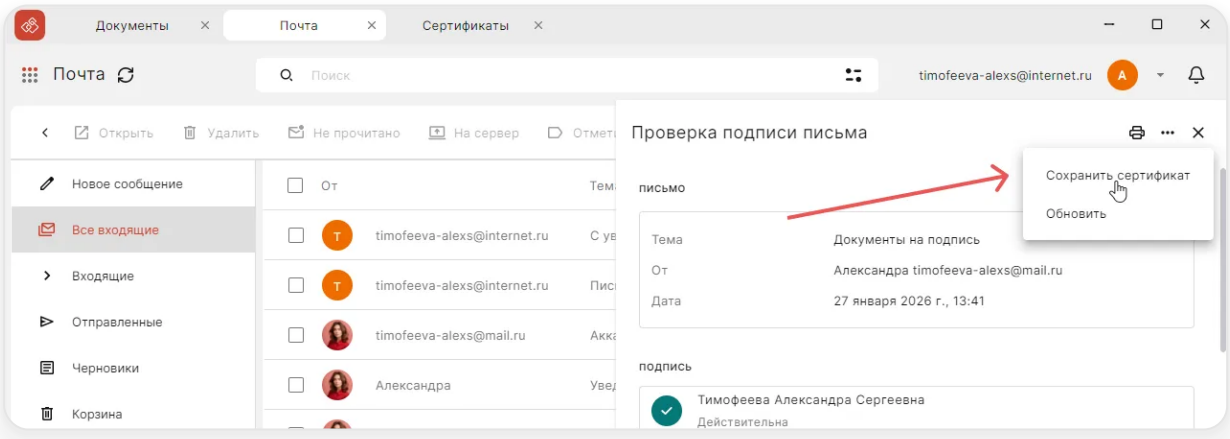
Установка при проверке подписи документа

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование** (см. Проверка подписи документа).
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. Справа от списка откроется область со сведениями.
4. В блоке **Цепочка сертификации** нажмите на сертификат подписанта.
5. Откроются сведения о сертификате.
6. Вызовите меню действий по кнопке **Еще**.
7. Нажмите на **Сохранить сертификат**.

Сертификат будет успешно сохранен в хранилище сертификаты «Других пользователей».

Установка при проверке подписи письма

1. Откройте сведения о подписи письма (см. Как проверить подпись письма).
2. Вызовите меню действий по кнопке **Еще**.



3. Нажмите на **Сохранить сертификат**.

Сертификат будет успешно сохранен в хранилище сертификаты **Других пользователей**.

Установка списка отзыва

Список отзыва сертификатов (COC) 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 COC 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 COC** — 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:

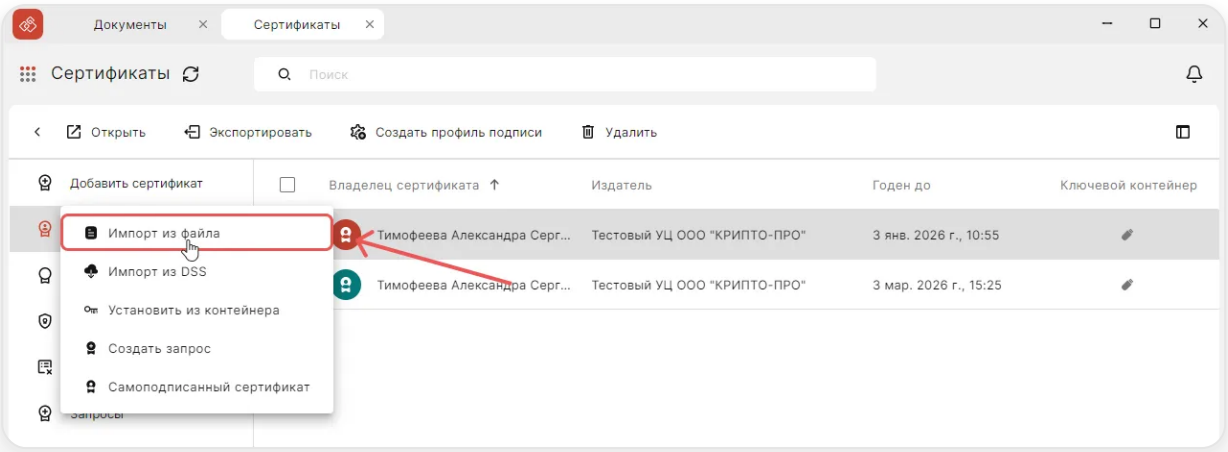
1. **На официальном сайте удостоверяющих центров**: обычно в разделе «Поддержка» или «Загрузки» доступны актуальные версии COC вместе с корневыми и промежуточными сертификатами.
2. **Из личного сертификата**: в свойствах сертификата есть поле **CRL Distribution Point (CDP)**. По указанной там ссылке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

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

Всегда скачивайте списки отзыва только с официальных сайтов УЦ.

Как установить список отзыва

1. Перейдите в раздел **Сертификаты** → **Списки отзыва**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В открывшемся меню действий выберите **Импорт из файла**.



4. В окне файлового менеджера выберите файл списка отзыва (обычно `.crl`).
5. Подтвердите запрос на установку списка.

При успешной установке COC отображается в разделе **Списки отзыва**.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ниже приведены типовые ошибки при установке сертификатов в КриптоАРМ и способы их устранения.

Ошибка	Описание	Рекомендуемые действия
Не удалось импортировать сертификат. Провайдер с поддержкой ГОСТ алгоритмов не найден.	Отсутствует криптопровайдер КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Не удалось импортировать сертификат	При установке сертификата из файла выбран неподходящий криптопровайдер	Попробуйте импортировать сертификат ещё раз. Выберите другой провайдер.
Не удалось импортировать сертификат	Выбранный сертификат не является корневым или промежуточным сертификатом	1. Проверьте расширение файла (`.cer`, `.crt`) 2. Запросите сертификат повторно у УЦ
Не удалось импортировать сертификат	Возможно, выбрано не подходящее хранилище для сертификата	Перейдите в раздел **Сертификаты → Других пользователей** и повторите попытку установки.
Не удалось загрузить контейнеры	Отсутствует криптопровайдер КриптоПро CSP	

Ошибка	Описание	Рекомендуемые действия
		Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ
Не удалось подключиться к серверу DSS (при установке сертификата из DSS)	Возможно, указан неверный логин или пароль	Проверьте правильность заполнения данных
Не удалось подключиться к серверу DSS (при установке сертификата из DSS)	Возможно, указаны некорректные адреса серверов, либо отсутствует подключение к сети Интернет	1. Проверьте правильность заполнения данных, 2. Проверьте подключение к сети Интернет.

Смотрите также

- Создание запроса и самоподписанного сертификата — информация о создании запросов на сертификаты и самоподписанных сертификатов.
- Экспорт и удаление сертификатов — как экспортировать и удалять сертификаты в КриптоАРМ.
- Действия с ключевыми контейнерами — работа с ключевыми контейнерами для установки и привязки сертификатов.

Открыть статью на сайте

Как создать запрос и самоподписанный сертификат в КриптоАРМ

Эта инструкция поможет вам **создать самоподписанный сертификат** и **сформировать запрос на сертификат** электронной подписи в приложении КриптоАРМ.

Вы узнаете, как подготовить запрос на сертификат, создать самоподписанный сертификат для личного или тестового использования, настроить параметры ключей и назначение сертификата, а также сохранить и импортировать готовый сертификат в хранилище.

Содержание:

- Создание запроса
- Самоподписанный сертификат
- Смотрите также

Создание запроса

Что такое запрос на сертификат?

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

Запрос необходим, чтобы УЦ убедился, что создаваемые ключи действительно принадлежат вам, а сведения о владельце верны. Он служит официальным документом для выдачи сертификата.

С помощью запроса можно получить сертификат для:

- Подписи и шифрования документов,
- Обеспечения безопасности электронной почты,
- TLS-сертификатов для сайтов и сервисов.

Шаблоны запросов

В приложении предусмотрены готовые шаблоны запросов, которые помогают быстро и корректно сформировать запрос на сертификат в зависимости от его назначения.

Шаблон	Для кого	Назначение
КЭП ФЛ	Физические лица	Создание запроса на квалифицированный сертификат электронной подписи

Шаблон	Для кого	Назначение
КЭП ИП	Индивидуальные предприниматели	Создание запроса на квалифицированный сертификат электронной подписи для индивидуальных предпринимателей
КЭП ЮЛ	Юридические лица	Создание запроса на квалифицированный сертификат электронной подписи сотрудника организации
Расширенный шаблон	ФЛ / ИП / ЮЛ	Создание запроса с расширенным набором атрибутов, когда требуется гибкая настройка данных владельца или специальных параметров сертификата
УЦ ЦБ. Сертификат для автоматизированной системы	ЮЛ	Создание запроса на сертификат для автоматизированных систем, выполняющих операции без участия пользователя (например, подписание и проверка документов)
УЦ ЦБ. Личный сертификат	ЮЛ	Создание запроса на квалифицированный сертификат в удостоверяющем центре Банка России
DV (Domain Validation) — сертификат от Минцифры	ФЛ, ИП, ЮЛ	Создание запроса на сертификат безопасности (TLS). Сертификат подтверждает, что вы управляете доменом, который указан в сертификате, а передача данных пользователей защищена.
OV (Organization Validation) — сертификат от Минцифры	ФЛ, ИП, ЮЛ	Создание запроса на сертификат безопасности (TLS). Сертификат подтверждает, что вы владеете и управляете доменом, который указан в сертификате, а передача данных пользователей защищена.

> 🔍 Подробнее о DV и OV-сертификатах читайте на портале Госуслуги.

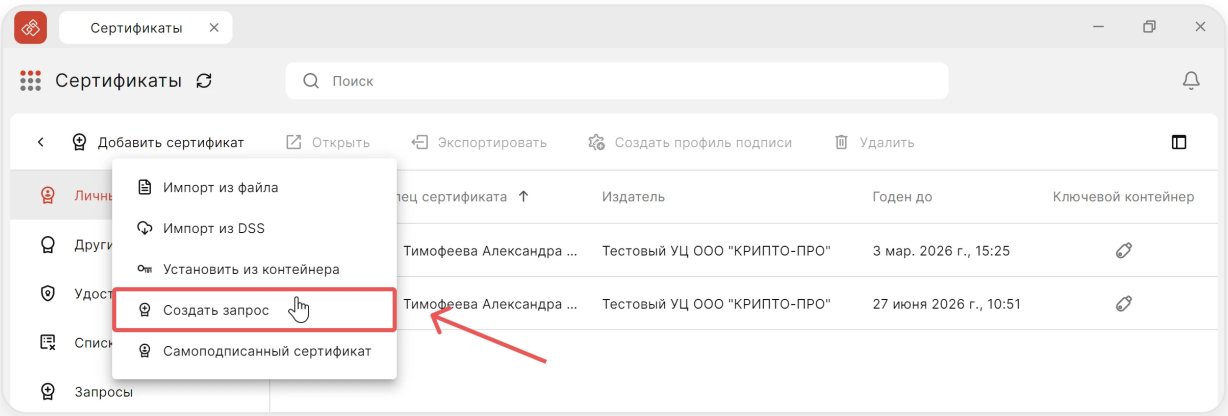
Что включает запрос на сертификат

1. **Сведения о владельце**: ФИО, должность, организация и контактная информация.

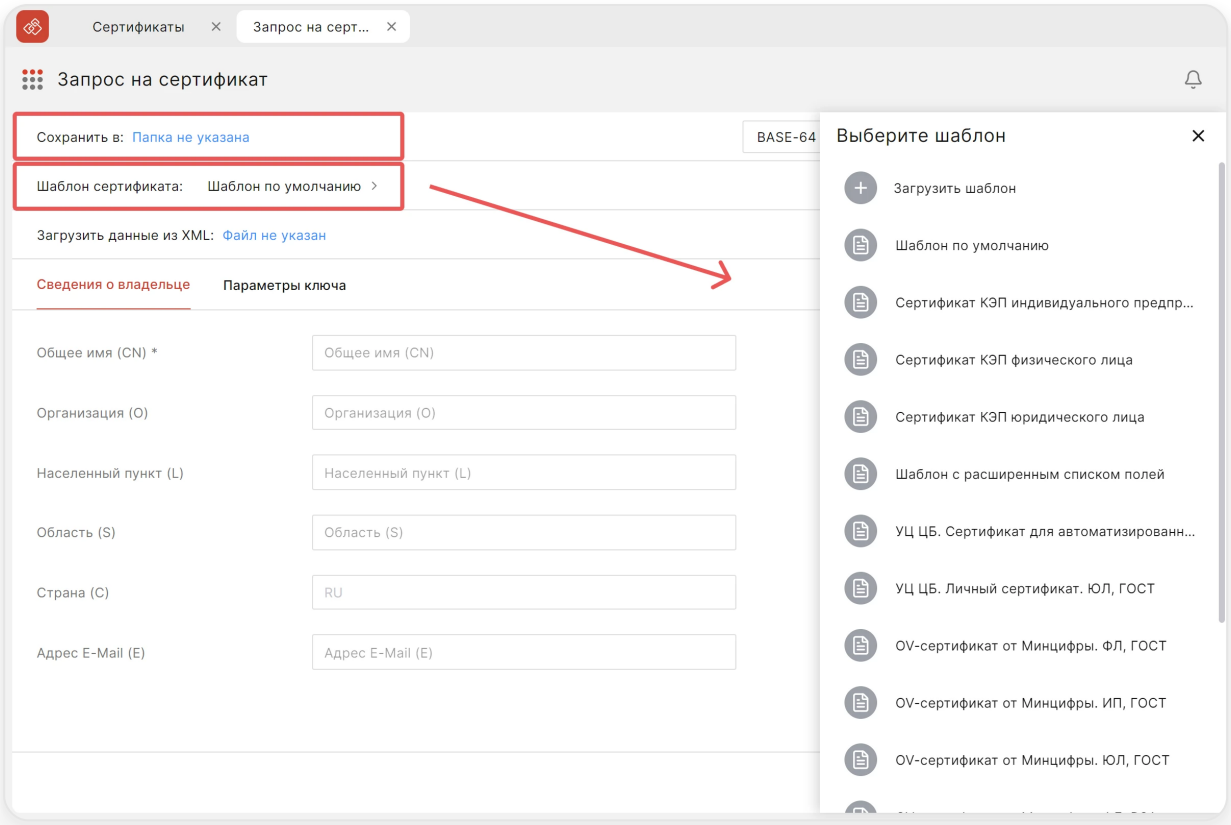
2. **Параметры ключевой пары**: Тип и длина ключа, назначение ключа, возможность экспорта ключа для переноса на другие устройства.
3. **Технические требования к сертификату**: Политики безопасности, срок действия сертификата, настройки использования ключа и прочие.

Создание запроса на сертификат

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Создать запрос**.



4. Откроется форма создания запроса.
5. В поле **Сохранить в** укажите папку для сохранения файла запроса. Если папка не выбрана, файл запроса сохранится в папку: `%USERPROFILE%\.Trusted\CryptoARM <версия>\Requests`.
6. В поле **Шаблон сертификата** выберите шаблон сертификата. Можно выбрать шаблон из списка или загрузить собственный в формате `.json`.



7. При необходимости выберите **кодировку файла запроса** `BASE64` или `DER`.
8. Заполните данные в запросе одним из способов:
    - **Загрузите данные из XML** — позволяет автоматически заполнить поля в запросе с помощью загрузки файлов XML.
    - **Укажите вручную**.
9. Заполните поля вкладки **Сведения о владельце**. Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.
10. Установите настройки на вкладке **Параметры ключа** (см. Параметры ключа).
11. Нажмите **Сохранить**.
12. При необходимости выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
13. При необходимости установите пароль на контейнер.

На основе указанных данных сформируется запрос на сертификат.

Дальнейшие действия

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.

Где хранится созданный запрос

После успешного формирования:

- Файл запроса сохраняется в формате: `<CN сертификата>_<алгоритм >_<дата генерации>`.
- Запрос появляется в папке **Запросы** раздела **Сертификаты**.

Импорт готового сертификата

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

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Импорт из файла**.
4. В файловом менеджере выберите файл сертификата `.cer`.
5. Дождитесь окончания импорта.

После успешного импорта сертификат готов к использованию.

Параметры ключа

Название настройки	Значение по умолчанию	Описание	Допустимые значения
Срок действия сертификата (только для самоподписанного сертификата)	Текущая дата + 1 год	Период, в течение которого сертификат считается действительным	Задается вручную (дата начала и окончания)
Криптопровайдер	КриптоПро CSP (если установлен)	Криптопровайдер, в хранилище которого будет установлен сертификат	- КриптоПро CSP (если установлен), - OpenSSL
Алгоритм	—	Алгоритм подписи	- ГОСТ Р 34.10-2012, - EC, - RSA
Размер ключа	—	Размер ключа	Для ГОСТ Р 34.10-2012: 256 бит и 512 бит, Для EC: 384 бит (P-384), Для RSA: 2048 бит
Идентификация заявителя (только для КриптоПро CSP)	—	Процедура проверки личности	- Личное присутствие, - С использование КЭП, - Электронный документ,

Название настройки	Значение по умолчанию	Описание	Допустимые значения
			`удостоверяющий личность, - С использованием сведений ЕСИА и ЕБС`
Контейнер (только для КриптоПро CSP)	`Автоматически заданное значение`	Название контейнера	—
Пометить ключи как экспортируемые	`Выкл`	Если включено, позволяет экспортировать сертификат вместе с закрытым ключом для переноса на другое устройство	`Вкл` / `Выкл`
OID для массива расширений	—	Базовый объектный идентификатор (OID), используемый при формировании расширений сертификата	Задается вручную
Дополнительное имя субъекта	—	Дополнительные атрибуты субъекта (Subject Alternative Name)	Задается вручную
Дополнительные объектные идентификаторы (OID)	—	Произвольные OID, добавляемые в расширенное назначение ключа (extKeyUsage)	Задается вручную
Средство электронной подписи владельца (только для КриптоПро CSP)	`КриптоПро CSP (версия 5.0.13003)`	Криптографическое средство, которое используется для реализации криптографических функций	—
Политики сертификата (только для КриптоПро CSP)	`Класс средства ЭП КС1`	Класс средства ЭП зависит от используемого средства подписи и указывает на уровень защиты информации	`КС1`, `КС2`, `КС3`, `КВ1`, `КВ2`, `КА`

Использование ключа (keyUsage) и расширенное назначение (extKeyUsage)

Указаны значения, выставленные по умолчанию:

Назначение ключа	Подпись	Шифрование	Подпись и шифрование
Использование ключа (KeyUsage)			
Подпись (digitalSignature)	✅		✅
Шифрование ключей (keyEncipherment)		✅	✅
Неотрекаемость (nonRepudiation)	✅		✅
Шифрование данных (dataEncipherment)		✅	✅
Согласование ключей (keyAgreement)	✅	✅	✅
Подпись сертификатов (keyCertSign)			
Автономное подписание списка отзыва (CRL)			
Только шифрование (encipherOnly)			
Только расшифрование (decipherOnly)			
Расширенное использование ключа (ExtendedKeyUsage)			
Проверка подлинности сервера			
Проверка подлинности клиента	✅	✅	✅
Подпись кода			
Защищенная почта	✅	✅	✅

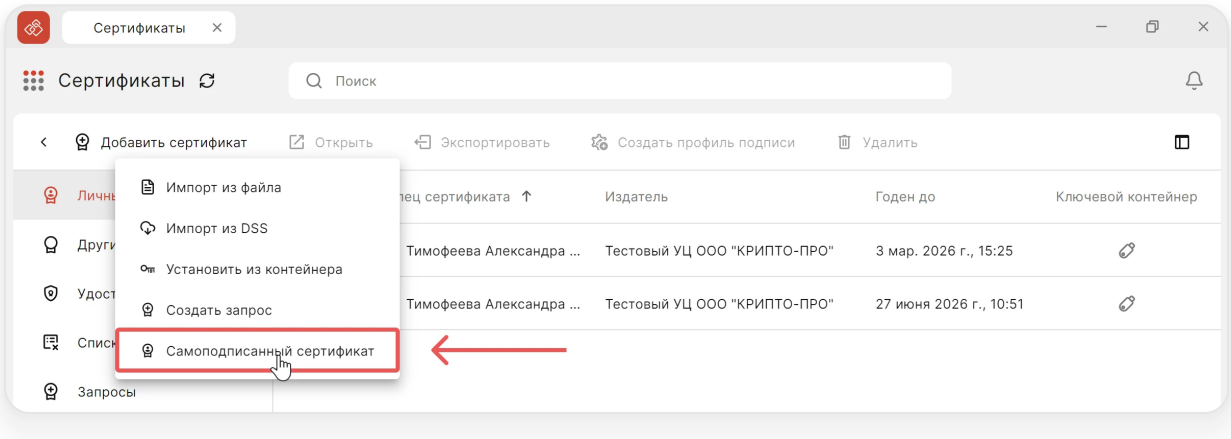
Самоподписанный сертификат

Самоподписанный сертификат — это сертификат электронной подписи, созданный пользователем самостоятельно без обращения в Удостоверяющий центр. Подходит только для личного или внутреннего использования, например, для обмена документами внутри доверенной группы.

Создание самоподписанного сертификата

Основной способ (через раздел «Сертификаты»)

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в боковом меню.
3. В появившемся списке действий выберите **Самоподписанный сертификат**.



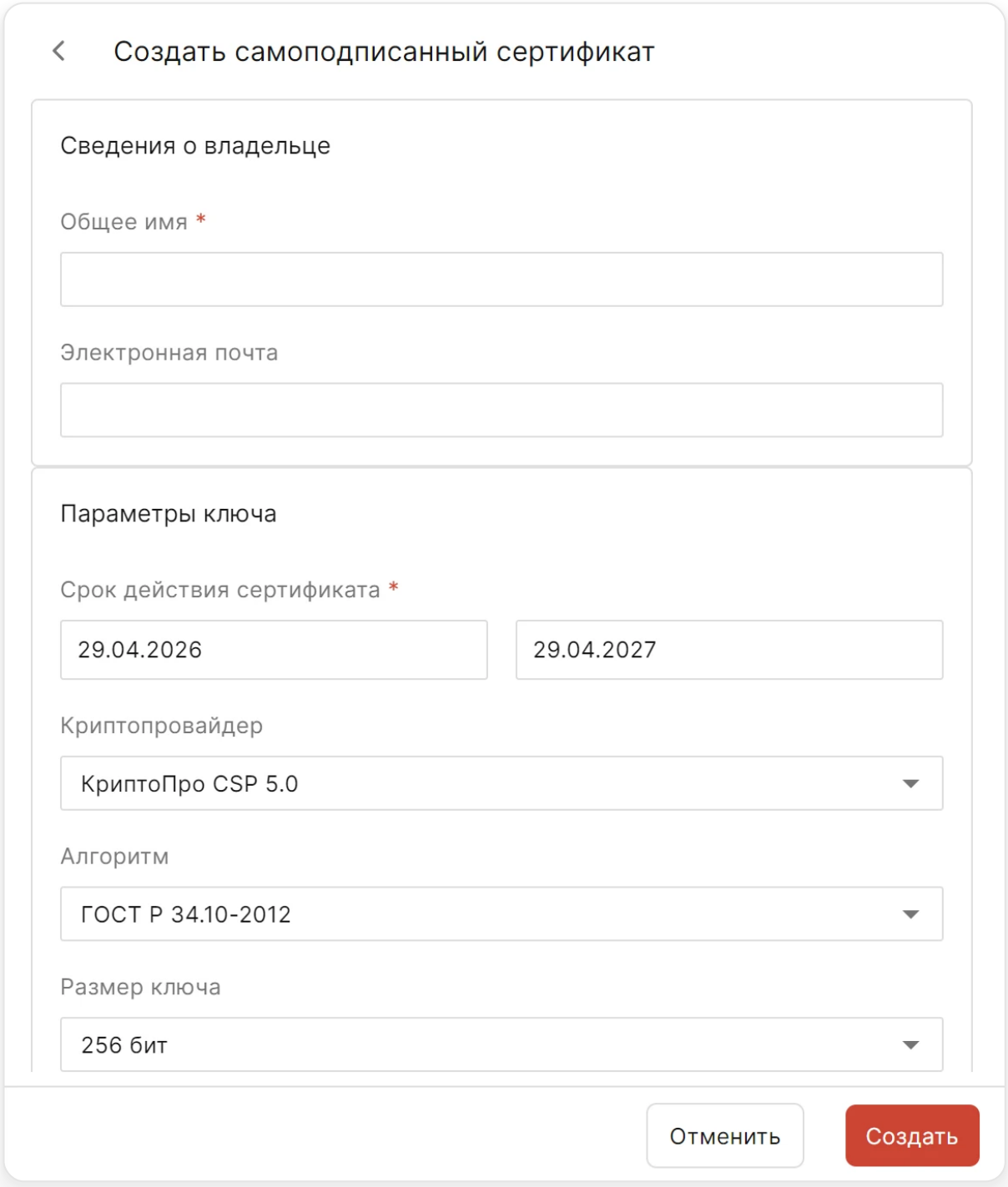
4. Выберите шаблон сертификата.
5. Заполните поля вкладки **Сведения о владельце**. Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.
6. Установите настройки на вкладке **Параметры ключа** (см. Параметры ключа).
7. Нажмите **Сохранить**.
8. Выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
9. При необходимости установите пароль на контейнер.

На основе указанных данных создается самоподписанный сертификат.

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Личные сертификаты**.
2. В открывшемся окне нажмите кнопку **Добавить** .
3. Выберите действие **Создать самоподписанный сертификат**.
4. В открывшемся окне укажите сведения о владельце, параметры ключа, использование ключа.

   Подробнее о настройках читайте в разделе Параметры ключа.



5. Нажмите **Создать**.

6. Выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
7. При необходимости установите пароль на контейнер.

На основе указанных данных создается самоподписанный сертификат.

Результаты создания

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

> 💡 **Совет**: Если после создания сертификат не появляется в разделе **Личные сертификаты**, обновите список сертификатов с помощью соответствующей кнопки .

Дополнительные действия

Чтобы самоподписанный сертификат был действительным:

1. Экспортируйте созданный сертификат без закрытого ключа (см. Экспорт личного сертификата).
2. Установите его в хранилище **Удостоверяющие центры** (см. Установка корневого и промежуточного сертификатов).

Смотрите также

- Установка сертификатов — инструкция по установке личных, корневых и промежуточных сертификатов, сертификатов других пользователей и списков отзыва (CRL).
- Экспорт и удаление сертификатов — инструкция по экспорту и удалению сертификатов в КриптоАРМ.
- Действия с ключевыми контейнерами — работа с ключевыми контейнерами для установки и привязки сертификатов.

Открыть статью на сайте

Как экспортировать и удалять сертификаты в КриптоАРМ

Научитесь экспортировать и удалять личные, промежуточные и сертификаты удостоверяющих центров и других пользователей. Вы узнаете, как сохранить сертификат с открытым или закрытым ключом, создать резервные копии и безопасно перенести сертификаты на новое устройство или передать коллегам.

Содержание:

- Экспорт личного сертификата
- Экспорт сертификата (УЦ, промежуточного или другого пользователя)
- Удаление сертификата
- Смотрите также

Экспорт личного сертификата

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.

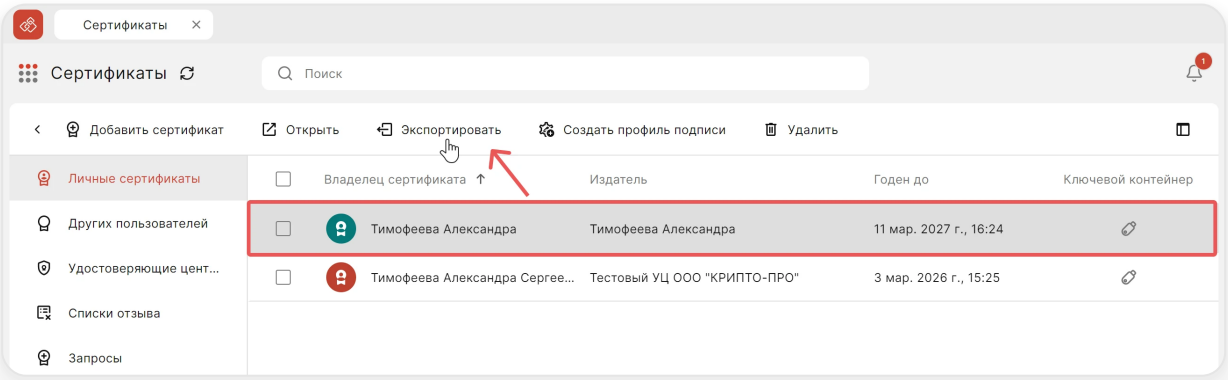
> ⚠️ **Важно**: экспорт с закрытым ключом доступен только если при создании сертификата был установлен флаг «Экспортируемый». Если он не был задан, выполнить экспорт ключа невозможно.

Сравнение способов экспорта

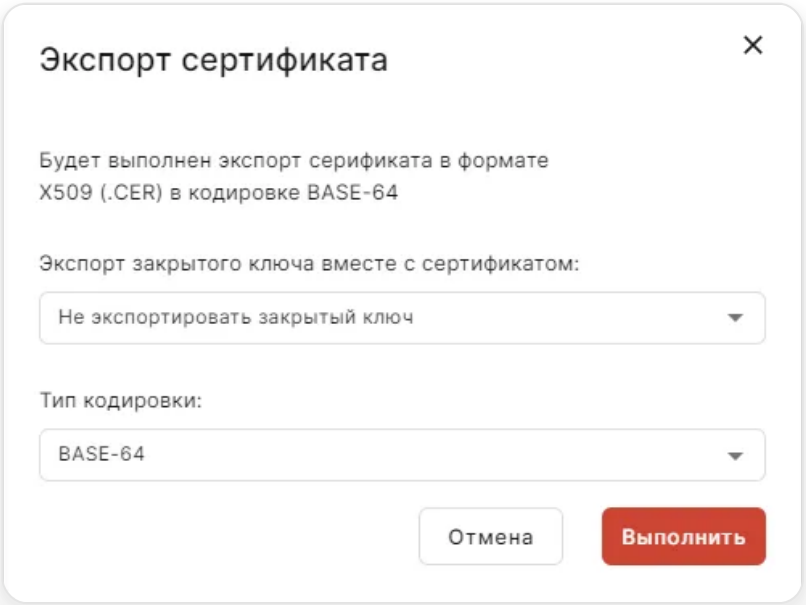
Параметр	Без закрытого ключа	С закрытым ключом
Назначение	Передача сертификата другим людям или системам	Перенос сертификата на другое устройство, резервное копирование
Можно использовать для	Проверки подписи, шифрования данных для вас	Подписи и расшифровки на другом устройстве
Безопасность	Безопасно, 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 раздел **Сертификаты** → **Личные сертификаты**.
2. Выделите личный сертификат в списке.
3. Нажмите кнопку **Экспортировать** на панели действий.



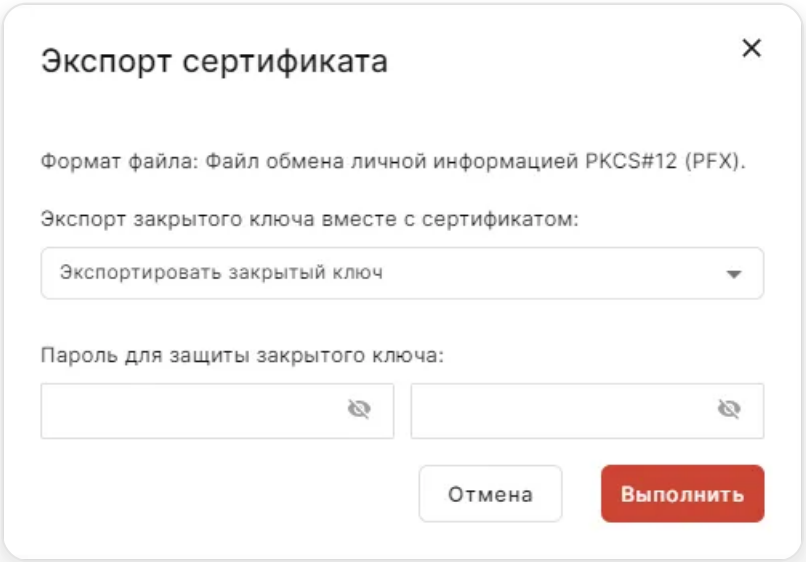
4. При необходимости введите пароль к ключевому контейнеру.
5. Откроется окно **Экспорт сертификата**.
   - Выберите **Не экспортировать закрытый ключ**. Выбор может быть заблокирован, если ключ не экспортируемый.
   - Выберите тип кодировки `BASE64` или `DER`.



6. Нажмите кнопку **Выполнить**.
7. В файловом менеджере задайте путь к файлу сертификата и имя файла.

Экспорт с закрытым ключом

1. Перейдите раздел **Сертификаты** → **Личные сертификаты**.
2. Выделите личный сертификат в списке.
3. Нажмите кнопку **Экспортировать** на панели действий.
4. При необходимости введите пароль к ключевому контейнеру.
5. Откроется окно **Экспорт сертификата**.
    - Выберите **Экспортировать закрытый ключ**. Выбор экспорта закрытого ключа может быть заблокирован, если ключ не экспортируемый.
    - Укажите пароль для PFX-контейнера.



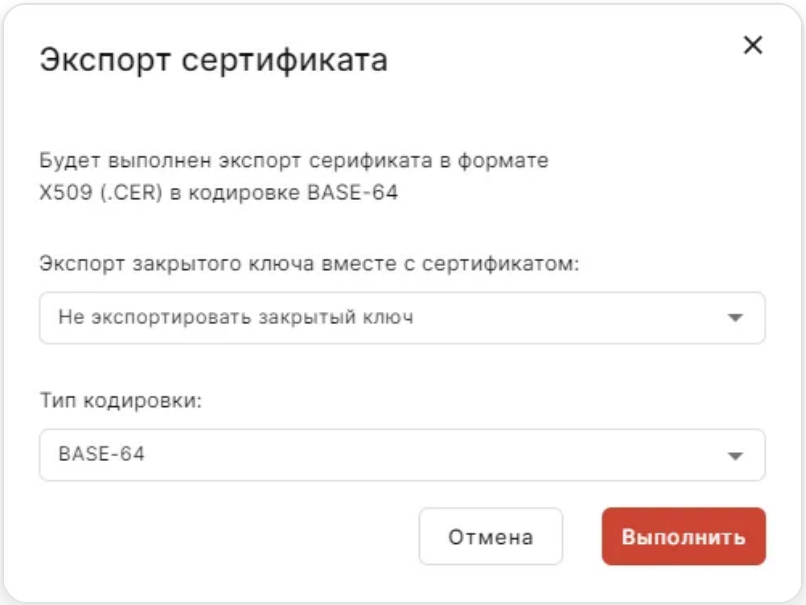
6. Нажмите кнопку **Выполнить**.
7. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Экспорт сертификата (УЦ, промежуточного или другого пользователя)

Основной способ (через раздел «Сертификаты»)

1. Перейдите в раздел **Сертификаты** и выберите хранилище **Удостоверяющие центры** или **Других пользователей**.
2. Выделите сертификат в списке.
3. Нажмите кнопку **Экспортировать** на панели действий.
4. В открывшемся окне **Экспорт сертификата** выберите тип кодировки `BASE64` или `DER` и нажмите кнопку **Выполнить**.

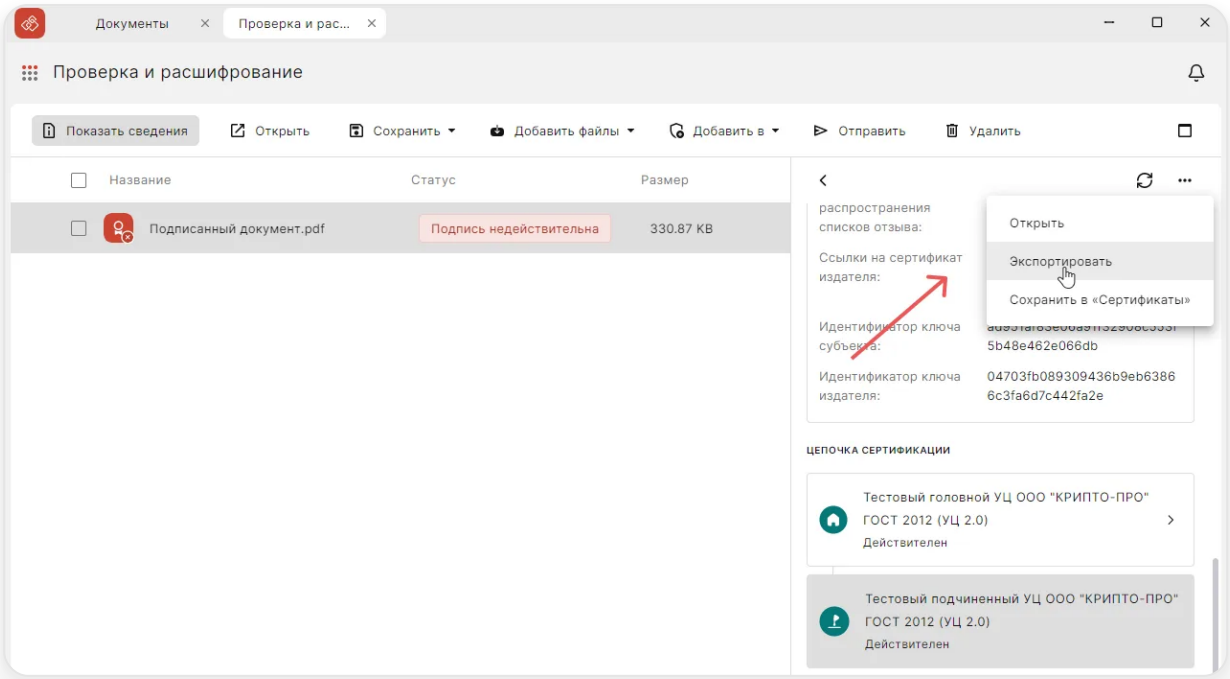


5. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Экспорт при проверке подписи документа

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование** (см. Проверка подписи документа).
2. Нажмите на кнопку **Показать сведения** или кнопку **Подробно** на панели действий.
3. В открывшемся окне со сведениями о подписи найдите блок **Цепочка сертификации** и нажмите на сертификат подписанта.
4. Откроются сведения о сертификате.
5. Вызовите меню действий по кнопке **Еще**.
6. Нажмите на **Экспортировать**.



7. Откроется окно **Экспорт сертификата**.

8. Укажите параметры экспорта и нажмите **Выполнить**.
9. В окне файлового менеджера укажите путь для сохранения файла с сертификатом.

При успешном выполнении операции сертификат экспортируется в файл.

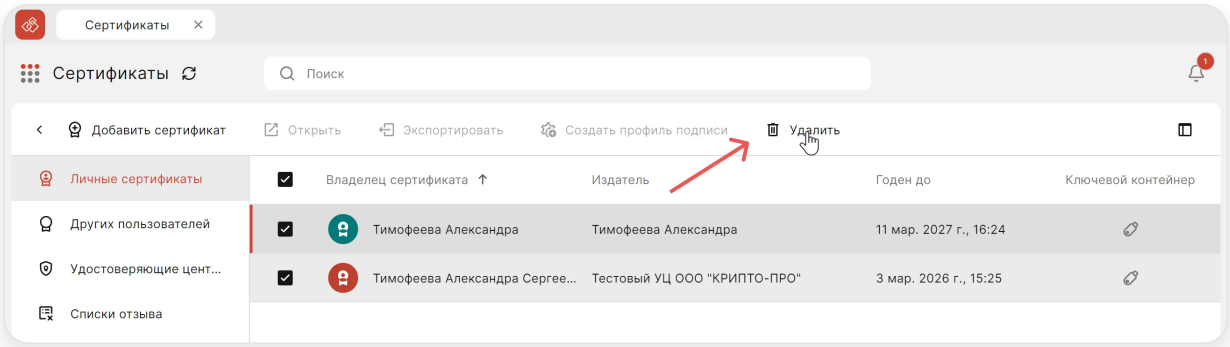
Удаление сертификата

Чтобы удалить сертификат:

1. Перейдите в раздел **Сертификаты**.
2. Выберите хранилище, из которого необходимо удалить сертификат.
3. Выделите один или несколько сертификатов в списке.

4. Нажмите кнопку **Удалить**.

> ⚠️ **Примечание**: если у сертификата есть привязка к закрытому ключу, то при удалении сертификата возможно удаление закрытого ключа. Для этого в окне подтверждения удаления установите флаг **Удалить связанный с сертификатом контейнер**. Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.



5. Подтвердите удаление.

Выбранные сертификаты будут успешно удалены из хранилища.

Смотрите также

- Установка сертификатов — инструкция по установке личных, корневых и промежуточных сертификатов, сертификатов других пользователей и списков отзыва (CRL).
- Создание запроса и самоподписанного сертификата — инструкция по созданию запросов на сертификаты и самоподписанных сертификатов.
- Действия с ключевыми контейнерами — работа с ключевыми контейнерами для установки и привязки сертификатов.

Открыть статью на сайте

Действия с ключевыми контейнерами в КриптоАРМ

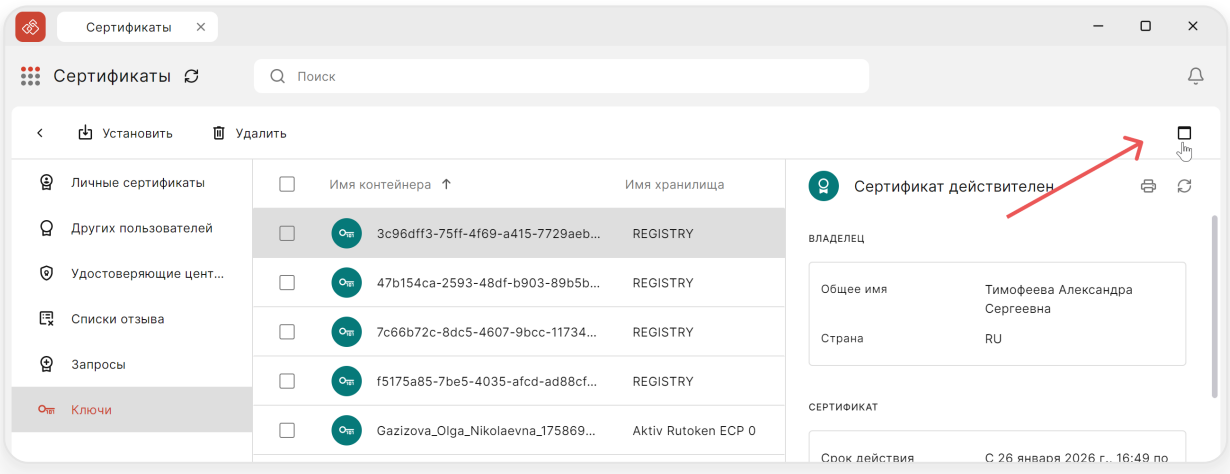
В этой инструкции мы расскажем, как управлять ключевыми контейнерами в КриптоАРМ. Вы узнаете, как просматривать сведения о сертификатах, проверять наличие закрытого ключа, безопасно удалять контейнеры и обновлять список доступных контейнеров.

Содержание:

- Просмотр сведений о сертификате
- Печать сведений о сертификате
- Проверка наличия закрытого ключа
- Удаление контейнера
- Обновление списка контейнеров
- Возможные ошибки
- Смотрите также

Просмотр сведений о сертификате

1. При необходимости подключите ключевой носитель к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Выделите контейнер в списке.
4. Нажмите на кнопку **Подробно** на панели действий.



5. Справа от списка откроется область со сведениями. Если появляется сообщение «В контейнере нет сертификатов», это означает, что контейнер не содержит сертификатов.

Печать сведений о сертификате

> ⚠️ **Примечание**: Данная функция доступна только для контейнеров, в которых есть сертификат.

1. При необходимости подключите ключевой носитель к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Выделите контейнер в списке.
4. Нажмите на кнопку **Подробно** на панели действий.
5. Справа от списка откроется область со сведениями.
6. Нажмите на кнопку **Печать**.

Откроется окно с отчетом о сведениях сертификата.

Отчет можно распечатать или скачать на устройство.

Проверка наличия закрытого ключа

> ⚠️ **Примечание**: Данная функция доступна только для контейнеров, в которых есть сертификат.

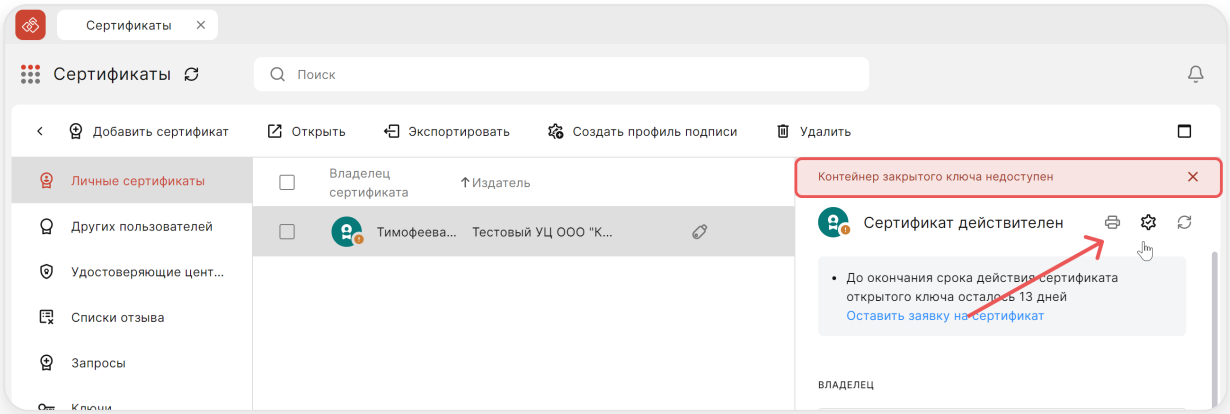
Личный сертификат может использоваться для создания электронной подписи только при наличии соответствующего закрытого ключа.

Чтобы проверить наличие закрытого ключа у личного сертификата:

1. При необходимости подключите ключевой носитель к устройству.
2. Перейдите в раздел **Сертификаты** → **Ключи**.
3. Выделите контейнер в списке.
4. Нажмите на кнопку **Подробно** на панели действий.
5. Справа от списка откроется область со сведениями.
6. Нажмите на кнопку **Протестировать**.
7. При необходимости введите пароль к ключевому контейнеру.

Результаты проверки:

- Контейнер закрытого ключа недоступен.
- Контейнер закрытого ключа доступен.



Удаление контейнера

> ⚠️ **Примечание**: Удаленный контейнер не подлежит восстановлению! Вам придется перевыпускать сертификат.

1. Перейдите в раздел **Сертификаты** → **Ключи**.
2. Выделите контейнер в списке.
3. Нажмите кнопку **Удалить**.
4. Подтвердите удаление.

Если во время удаления был установлен флаг **Удалить связанный с контейнером сертификат**, то сертификат удалится из хранилища **Личные сертификаты**.

Пустые контейнеры, не содержащие ключевой информации, также можно удалить. Процедура удаления выполняется аналогично.

> 💡 Удаление пустых контейнеров позволяет очистить список контейнеров, не затрагивая контейнеры с закрытыми ключами и сертификатами.

Обновление списка контейнеров

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Обновить** , размещенную рядом с заголовком раздела.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ошибка	Описание	Рекомендуемые действия
Не удалось загрузить контейнеры	Отсутствует криптопровайдер КриптоПро CSP	Установите криптопровайдер КриптоПро CSP и перезапустите приложение КриптоАРМ

Смотрите также

- Установка сертификатов — инструкция по установке личных, корневых и промежуточных сертификатов, сертификатов других пользователей и списков отзыва (CRL).
- Создание запроса и самоподписанного сертификата — инструкция по созданию запросов на сертификаты и самоподписанных сертификатов.
- Экспорт и удаление сертификатов — инструкция по экспорту и удалению сертификатов в КриптоАРМ.

Открыть статью на сайте

Как работать с контактами в КриптоАРМ

В этой инструкции вы узнаете, как работать с контактами в КриптоАРМ. Вы научитесь добавлять и редактировать контакты, объединять их в группы, настраивать аватары, привязывать сертификаты, а также экспортировать контакты в формате vCard.

Содержание:

- Добавление контакта в адресную книгу
- Управление контактами
- Аватары контактов
- Сертификаты контактов
- Группы контактов
- Смотрите также

Добавление контакта в адресную книгу

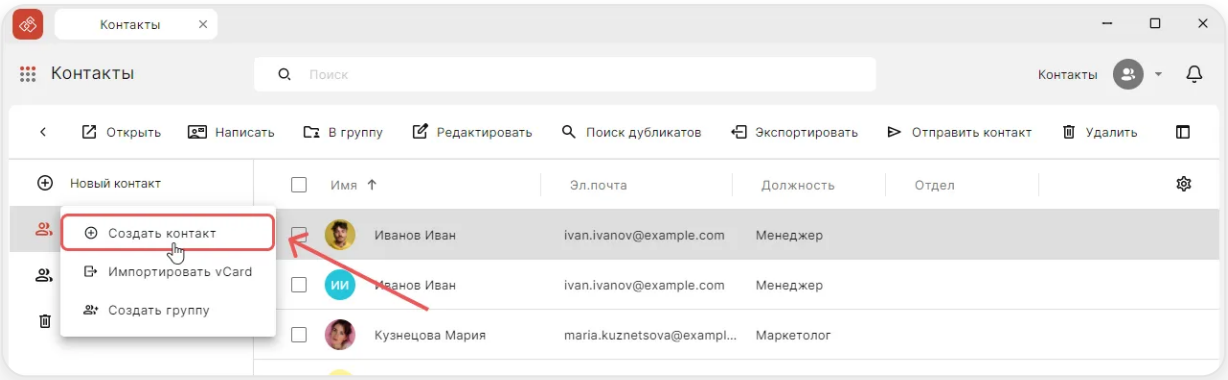
В КриптоАРМ можно создать контакт с расширенным профилем, который будет включать:

- Личные данные (ФИО, должность, компания)
- Различные контактные данные (телефоны, email, адреса)
- Фотографии, загруженные вручную или полученные из сервиса Gravatar
- Сертификаты для безопасной переписки

> 🔍 Gravatar (от англ. globally recognized avatar — глобально распознаваемый аватар) — сервис компании Automattic, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.

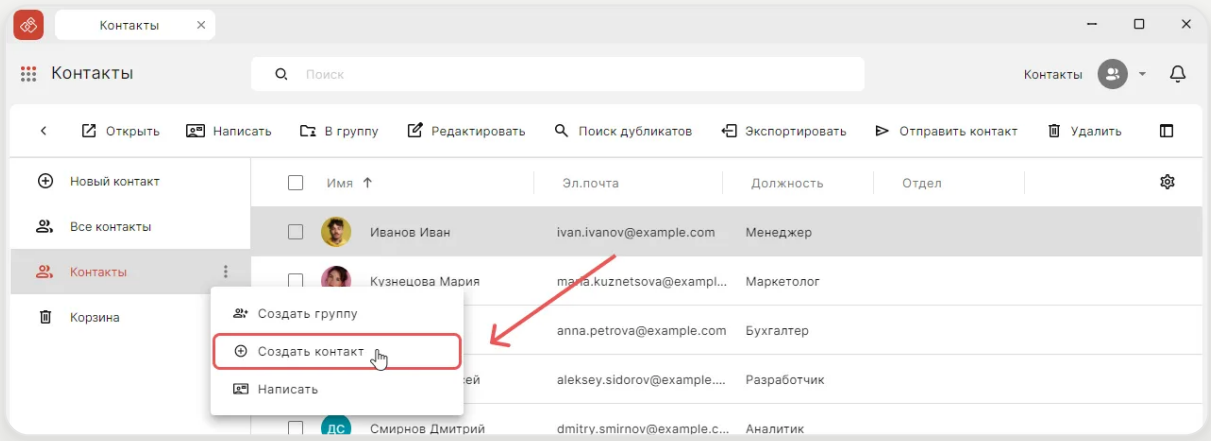
Основной способ (через раздел «Контакты»)

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Нажмите на кнопку **Новый контакт** на панели действий.
3. В появившемся меню выберите **Создать контакт**.



4. В открывшейся форме создания укажите:
   - Данные о контакте,
   - Фото контакта,
   - Электронный сертификат.
5. Нажмите кнопку **Сохранить**.

Контакт будет добавлен в корневую группу адресной книги.

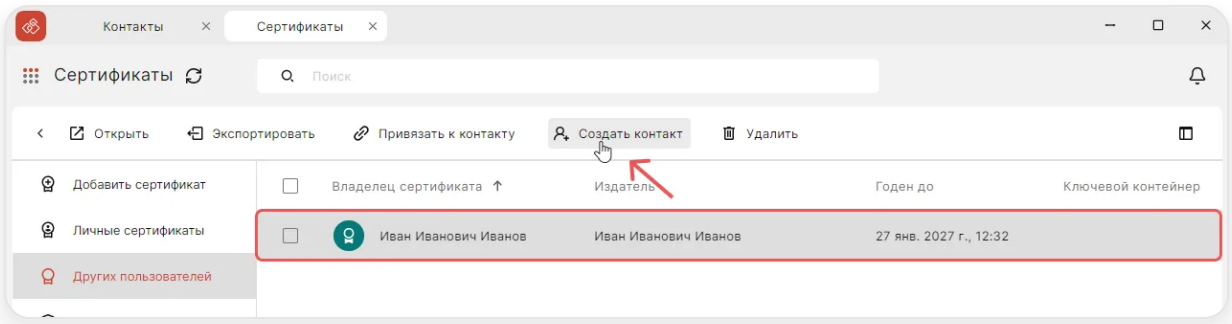
> 💡 **Совет**: Чтобы создать контакт в определенной группе, нажмите на кнопку **Еще** ⋮ на панели с группой в боковом меню. Затем выберите **Создать контакт**.
>
> 
>

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Адресные книги**.
2. В открывшемся окне нажмите на кнопку **Добавить** ⊕ и выберите действие **Создать контакт**.
3. Откроется новая вкладка с формой создания контакта.
4. Следуйте шагам из инструкции Основной способ.

Альтернативный способ (через раздел «Сертификаты»)

1. Перейдите в раздел **Сертификаты** → **Других пользователей**.
2. Выделите сертификат в списке и нажмите **Создать контакт** на панели действий.



3. Откроется форма создания контакта. Данные будут автоматически заполнены на основе сертификата. Сертификат будет привязан к контакту.
4. Следуйте шагам из инструкции Основной способ.

Альтернативный способ (из подписанного письма)

1. Перейдите в раздел **Почта** и откройте письмо, подписанное электронной подписью.
2. Вызовите меню действий по кнопке **Еще** .
3. Выберите действие **Добавить контакт**.
4. Следуйте шагам из инструкции Основной способ.

Описание полей контакта

Раздел	Поле	Тип данных	Обязательное	Описание
Личная информация	Фото	Изображение (JPG/ webp)	Нет	Аватар контакта (макс. 2MB)
	Фамилия	Текст	Нет	
	Имя	Текст	Да	
	Отчество	Текст	Нет	
Рабочие данные	Организация	Текст	Нет	Название компании
	Подразделение	Текст	Нет	Отдел/ Департамент
	Должность	Текст	Нет	
	Номер телефона	Телефон	Нет	

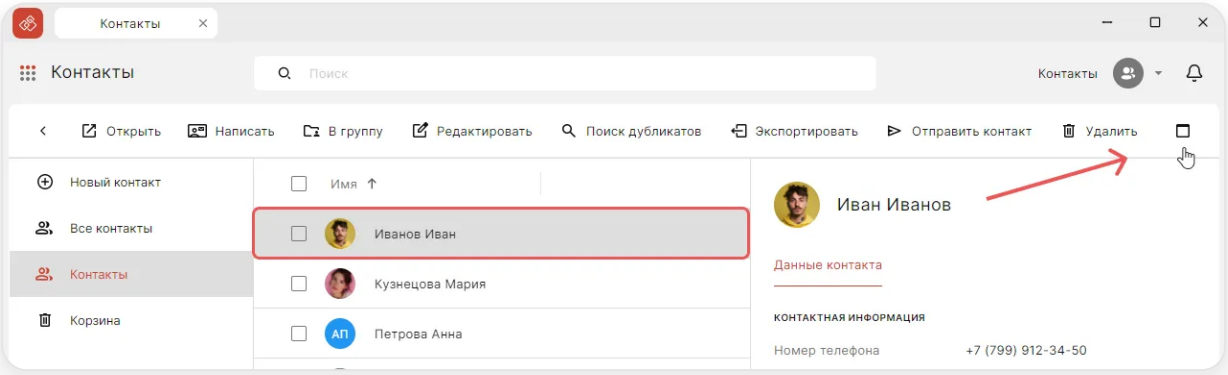
Раздел	Поле	Тип данных	Обязательное	Описание
Контактные данные				Формат: +7 (XXX) XXX-XX-XX
	Адрес электронной почты	Email	Нет	-
Дополнительно	Дата рождения	Дата	Нет	Формат: ДД.ММ.ГГГГ
	Адрес	Текст	Нет	Регион, город, улица, дом, индекс
	Примечание	Текст	Нет	Произвольные заметки
Сертификат	Привязанные сертификаты	Сертификаты	Нет	Сертификат из файла .cer, .crt или из раздела **Сертификаты → Других пользователей**

Управление контактами

Просмотр информации о контакте

Быстрый просмотр

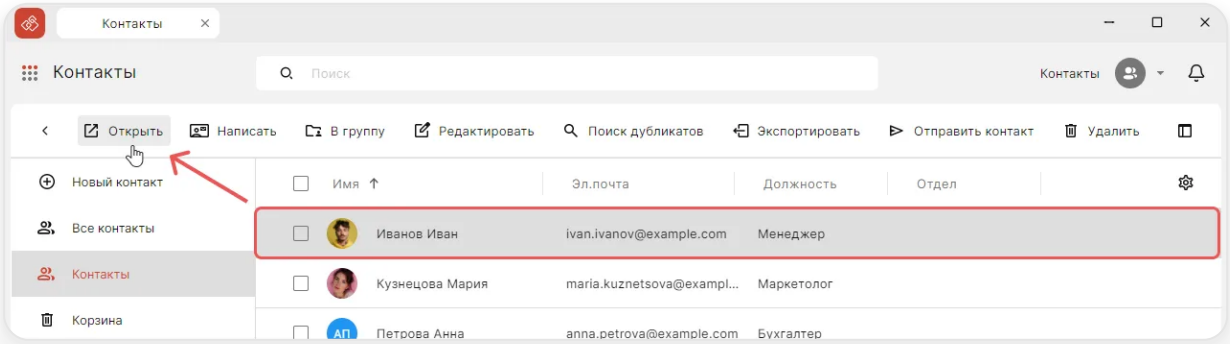
1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Выделите контакт в списке и нажмите кнопку **Просмотр** на панели действий.



3. Справа от списка контактов откроется область со сведениями о контакте.

Просмотр в новой вкладке

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Выделите контакт в списке и нажмите кнопку **Открыть** на панели действий.

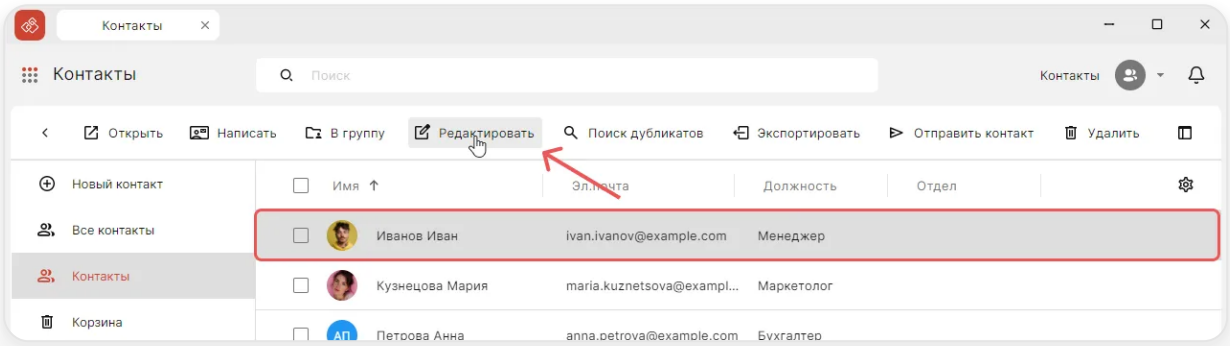


Информация о контакте откроется в новой вкладке.

Редактирование контакта

> ⚠ **Примечание**: Для редактирования доступны только локальные контакты.

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Выделите контакт в списке .
3. Нажмите кнопку **Редактировать** в верхней панели.



4. Внесите изменения в данные контакта.
5. Нажмите **Сохранить**.

Поиск контакта

> ⚠ **Примечание**: Поиск контактов осуществляется в активной адресной книге.

Чтобы найти определенный контакт:

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. В поисковой строке введите параметры поиска: ФИО, e-mail или номер телефона.

Экспорт контакта

> 💡 **Совет**: Можно экспортировать как всю адресную книгу целиком, так и только выбранные контакты — это удобно при передаче данных коллегам или миграции на другую систему.

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Выделите в списке один или несколько контактов.
3. Нажмите кнопку **Экспортировать** на панели действий.
4. В файловом менеджере укажите место сохранения файла.

Контакты сохраняются в формате `.vcf` (vCard).

> 💡 **Совет**: Экспорт контактов доступен также для контактов, получаемых из адресной книги LDAP.

Что сохраняется при экспорте

В экспортируемом файле vCard могут быть записаны:

- ФИО и должность
- номера телефонов и e-mail-адреса
- название организации и подразделения
- почтовые адреса
- день рождения и дополнительные заметки
- фотографии (если добавлены в профиль)
- сертификаты контакта

> 🔐 Если у контакта несколько сертификатов, то сохраняются все.

Отправка по почте

> ⚠️ Примечание: Для отправки профилей подписи по почте в приложении должен быть подключен почтовый аккаунт.

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.

2. Выделите в списке один или несколько контактов.
3. Нажмите кнопку **Отправить контакт** на панели действий.
4. Откроется вкладка с письмом, в которой выбранные контакты будут автоматически добавлены во вложение в формате `.vcf` (vCard).
5. Укажите получателя, добавьте текст письма и нажмите **Отправить**.

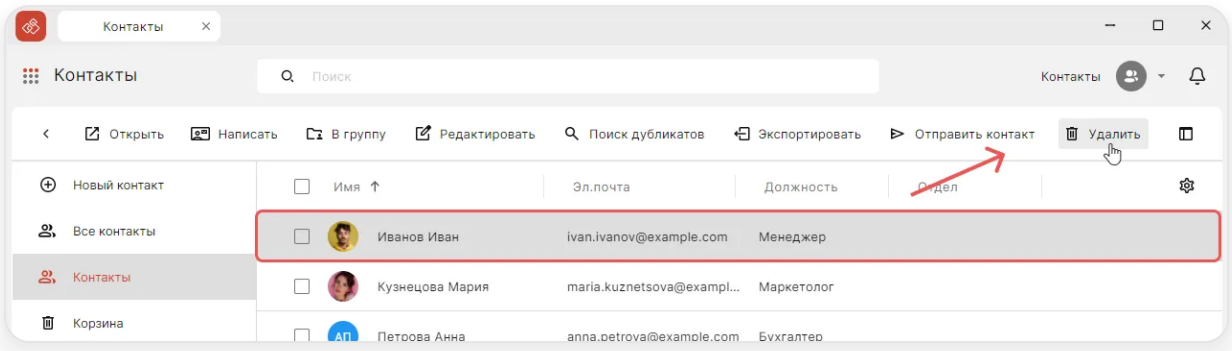
Удаление контакта

Удаленные контакты хранятся в группе «Корзина».

> ⚠️ **Примечание**: Удалить можно только локальные контакты. Контакты из внешних адресных книг будут удалены при удалении самой книги.

Стандартный способ

1. Перейдите в раздел **Контакты**.
2. Выделите контакт в списке.
3. Нажмите кнопку **Удалить** на панели действий.



Выбранный контакт будет перемещен в **Корзину**.

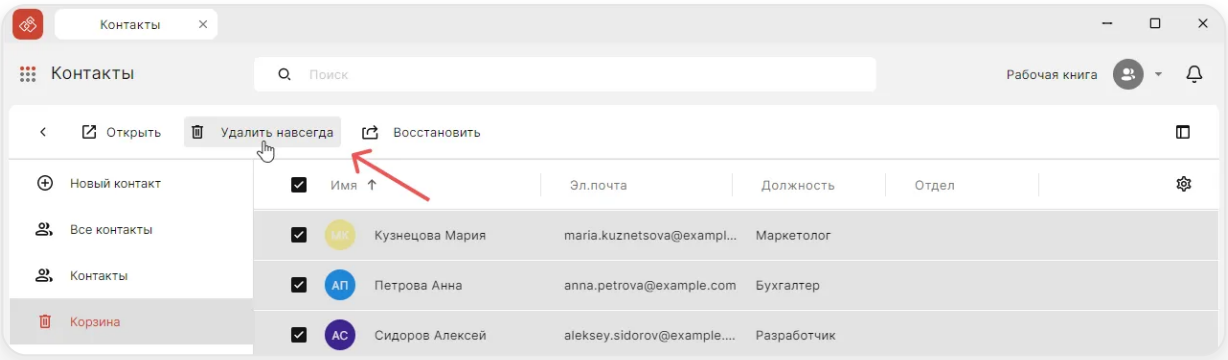
Групповое удаление

1. Перейдите в раздел **Контакты**.
2. Отметьте флажками контакты, которые необходимо удалить.
3. Нажмите кнопку **Удалить** на панели действий.

Выбранные контакты будут перемещены в **Корзину**.

Удаление из «Корзины»

1. Перейдите в раздел **Контакты** → **Корзина**.
2. Отметьте флажками контакты, которые необходимо навсегда удалить.
3. Нажмите **Удалить навсегда** на панели действий.



Выбранные контакты будут удалены из приложения.

> 💡 **Совет**: Чтобы очистить «Корзину», установите флажки для всех контактов в списке и нажмите на кнопку **Удалить навсегда** на панели действий.

Восстановление удаленных контактов

После переноса контакта в «Корзину» его можно восстановить.

1. Перейдите в раздел **Контакты** → **Корзина**.
2. Отметьте флажками контакты, которые необходимо восстановить.
3. Нажмите на кнопку **Восстановить** на панели действий.

Контакт будет восстановлен в группу, из которой был удален.

Аватары контактов

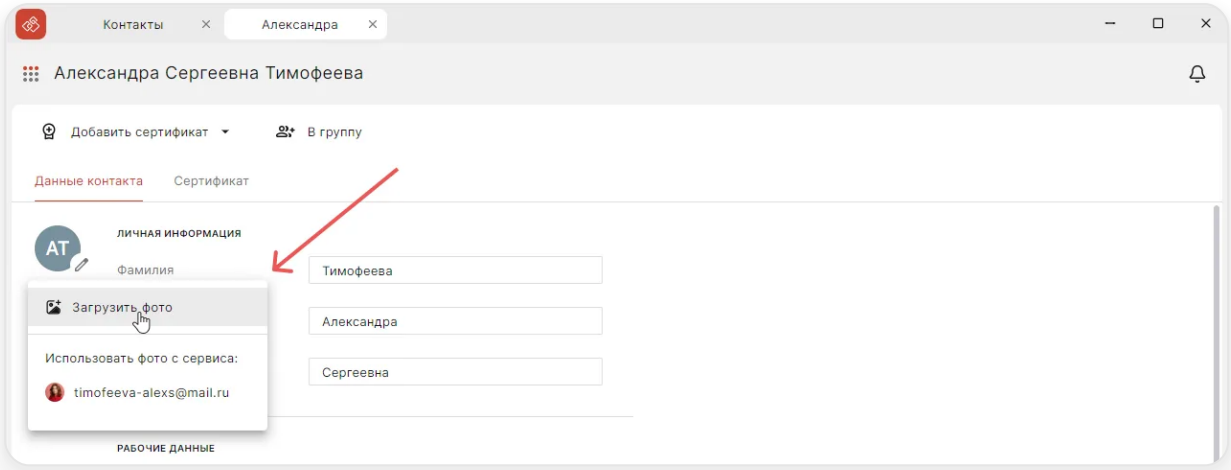
Вы можете персонализировать контакты, добавив к ним изображения одним из способов:

- **Загрузка с компьютера** — используйте собственные фотографии,
- **Сервис Gravatar** — автоматическое получение аватара с сервиса Gravatar.

> 🔍 Gravatar (от англ. globally recognized avatar — глобально распознаваемый аватар) — сервис компании Automattic, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.
>
> 🚨 При экспорте контакта с фотографией в формате `.vcf`, изображение переносится вместе с данными. То же самое происходит и при импорте: если контакт содержит фото в `.vcf`, оно будет загружено вместе с остальными сведениями. Подробнее про поддержку vCard читайте в инструкции.

Загрузка аватара с компьютера

1. Перейдите в раздел **Контакты**.
2. Откройте форму создания или редактирования контакта.
3. Нажмите на аватар контакта.
4. В открывшемся меню выберите действие **Загрузить фото**.



5. Укажите путь к файлу с фото.

> ⚠️ **Примечание**: Для выбора доступны файлы в формате `jpg (jpeg)`, `gif`, `webp`, `bmp` и размером не более 2МБ.

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

Установка аватара из сервиса Gravatar

> ⚠️ **Примечание**: Адрес электронной почты, сохраненный в контакте, должен совпадать с адресом пользователя, зарегистрированным на сервисе Gravatar. Если адреса не совпадают, то аватар отображаться не будет.

1. Перейдите в раздел **Контакты**.
2. Откройте форму создания или редактирования контакта.
3. Нажмите на аватар контакта.
4. Откроется меню действий с аватаром контакта. В меню будут отображены фото, полученные с сервиса Gravatar.
5. Выберите фото.
6. Нажмите **Сохранить** в форме редактирования контакта.

Фотография применится в качестве аватара контакта и будет отображаться во всех разделах приложения.

Удаление аватара

1. Перейдите в раздел **Контакты**.
2. Откройте форму редактирования контакта.
3. Нажмите на аватар контакта.
4. Откроется меню действий с аватаром контакта.
5. Выберите действие **Удалить фото**.

Сертификаты контактов

Для безопасного обмена зашифрованными письмами и документами в приложении необходимо привязать сертификат к контакту.

Общие особенности:

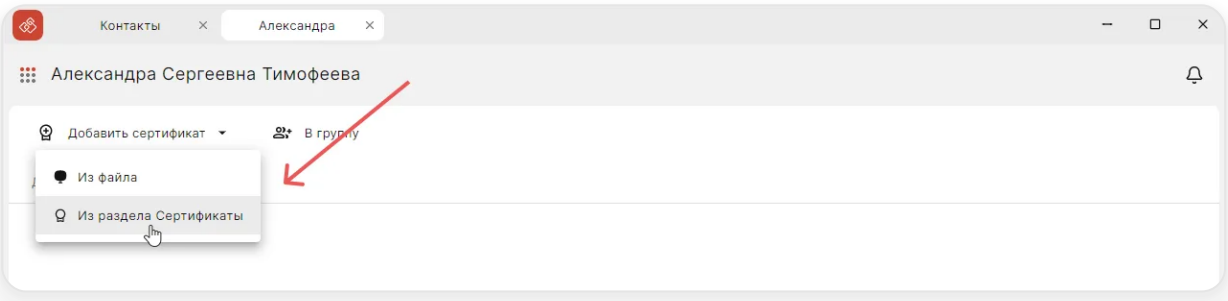
1. Привязка сертификатов доступна только для **локальных** контактов. Контакты из внешних источников редактируются на стороне сервера.
2. Сертификаты имеют срок действия. При перевыпуске обязательно замените их у контактов, чтобы обмен сообщениями продолжался без ошибок.
3. При наличии у контакта нескольких сертификатов приложение автоматически использует тот, который поддерживает выбранный алгоритм шифрования.

> ⚠️ **Примечание**: Удаление сертификатов контакта возможно только при редактировании. Это позволяет избежать случайного удаления важных данных при просмотре информации.

Привязка сертификата из хранилища

К контакту можно привязать сертификаты из хранилищ **Личные сертификаты** и сертификаты **Других пользователей**.

1. Откройте форму создания или редактирования контакта.
2. Нажмите кнопку **Добавить сертификат**.
3. В открывшемся меню выберите действие **Из раздела Сертификаты**.



4. Откроется окно со списком сертификатов из хранилищ **Личные сертификаты** и **Других пользователей**.

5. При необходимости воспользуйтесь фильтрацией списка сертификатов:

    - выберите **профиль доверия**:

        - **Российская Федерация** — отображаются сертификаты с алгоритмами ГОСТ;
        - **Открытая криптография** — отображаются сертификаты с алгоритмами RSA;

    - включите отображение только **действительных сертификатов**, если необходимо скрыть недействительные сертификаты;

    - воспользуйтесь **строкой поиска**, чтобы быстро найти сертификат по имени владельца или другим данным.

6. Выберите сертификат, нажав на иконку сертификата. Возможен множественный выбор. После выбора сертификат автоматически добавится в список сертификатов контакта.

7. После выбора закройте окно со списком сертификатов.
8. Нажмите **Сохранить** в форме редактирования контакта.

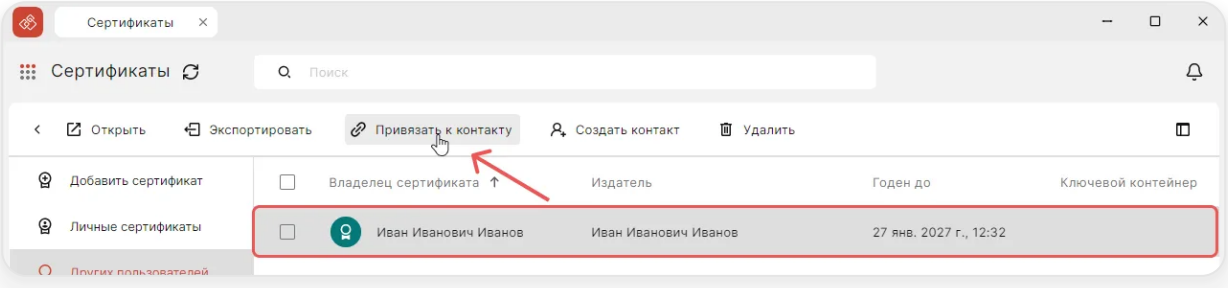
Привязка сертификата из файла

1. Откройте форму создания или редактирования контакта.
2. Нажмите кнопку **Добавить сертификат**.
3. В открывшемся меню выберите действие **Из файла**.
4. Откроется окно файлового менеджера.
5. Выберите файл с сертификатом `.cer` или `.crt`.
6. После выбора сертификат автоматически добавится в список сертификатов контакта.
7. Нажмите **Сохранить** в форме редактирования контакта.

Привязка сертификата из раздела «Сертификаты»

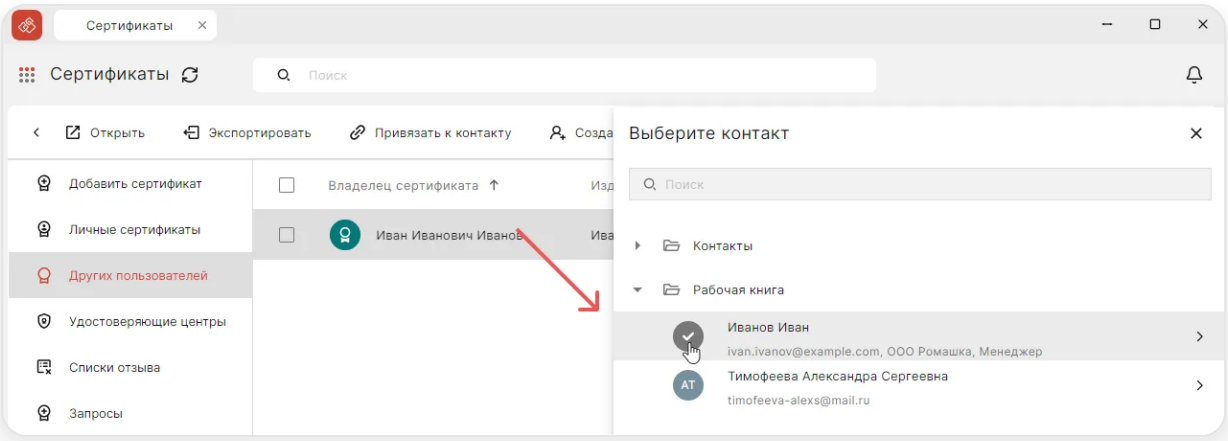
1. Перейдите в раздел **Сертификаты** → **Других пользователей**.
2. Выделите сертификат в списке.

3. Нажмите на кнопку **Привязать к контакту** на панели действий.



4. Откроется окно **Выберите контакт**.

5. Выберите контакт, нажав на его аватар.

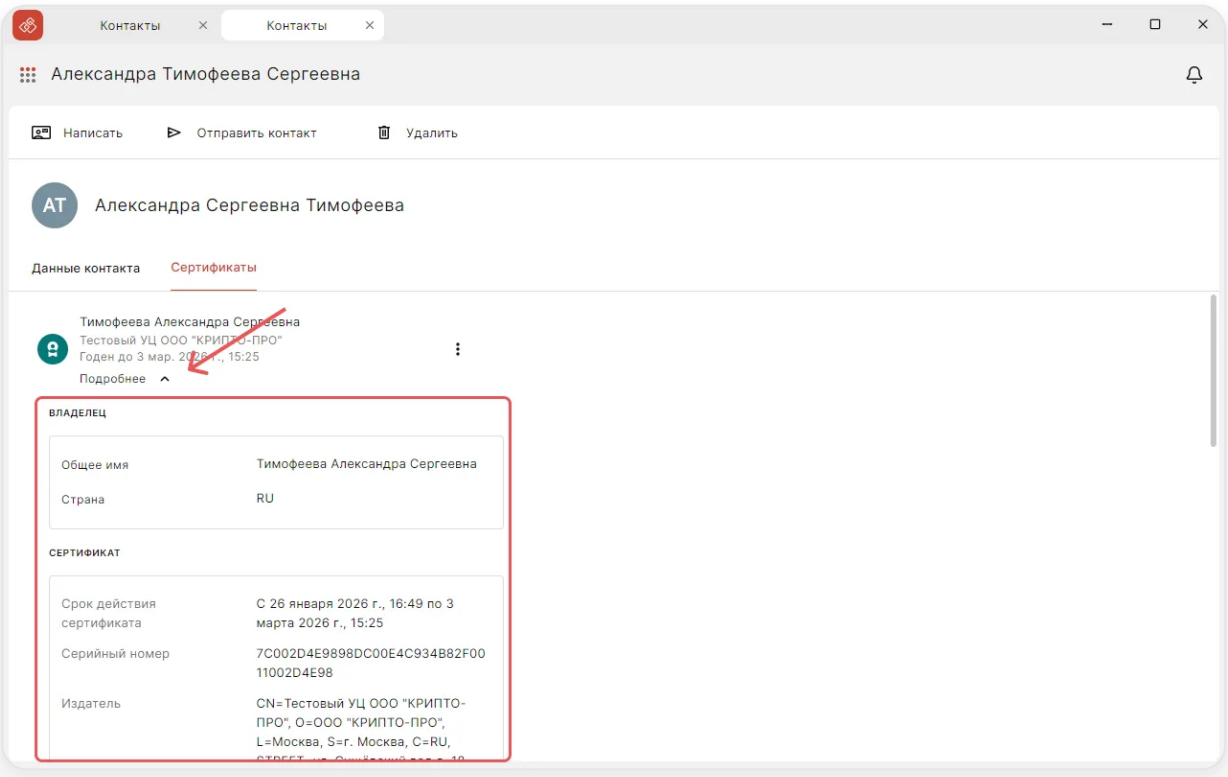


6. Подтвердите действие в модальном окне.

Сертификат успешно привязан к контакту.

Просмотр сведений о сертификате

1. Откройте профиль контакта с привязанным сертификатом любым из способов.
2. Перейдите на вкладку **Сертификаты**.
3. Нажмите на кнопку **Подробнее** на панели с сертификатом.



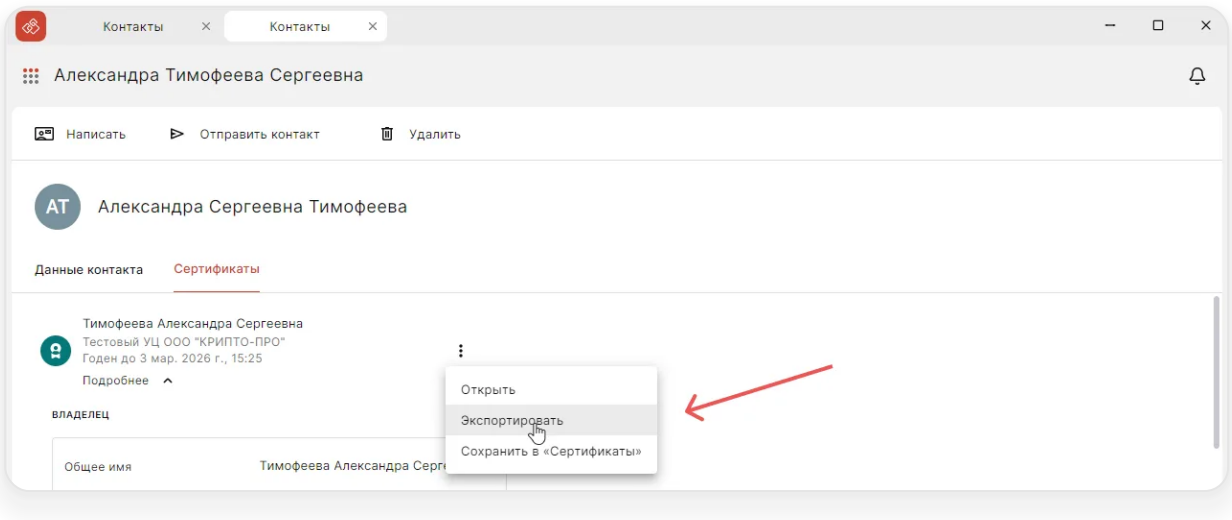
Отобразятся полные технические сведения, включая срок действия и назначение.

> 💡 **Совет**: Для просмотра встроенными средствами ОС Windows нажмите **Еще** → **Открыть**.

Экспорт сертификата контакта

Если вам нужно передать сертификат контакта коллеге или загрузить его в другое приложение, используйте функцию экспорта:

1. Откройте профиль контакта с привязанным сертификатом любым из способов.
2. Перейдите на вкладку **Сертификаты**.
3. Нажмите на кнопку **Еще** на панели с сертификатом.
4. Выберите действие **Экспортировать**.



5. В файловом менеджере укажите место сохранения файла.

Сертификат будет выгружен в формате .cer.

Сохранение сертификата в хранилище

1. Откройте профиль контакта с привязанным сертификатом любым из способов.
2. Перейдите на вкладку **Сертификаты**.
3. Нажмите на кнопку **Еще** на панели с сертификатом.
4. Выберите действие **Сохранить в «Сертификаты»**.

Сертификат контакта будет сохранен в хранилище **Сертификаты других пользователей** раздела **Сертификаты**.

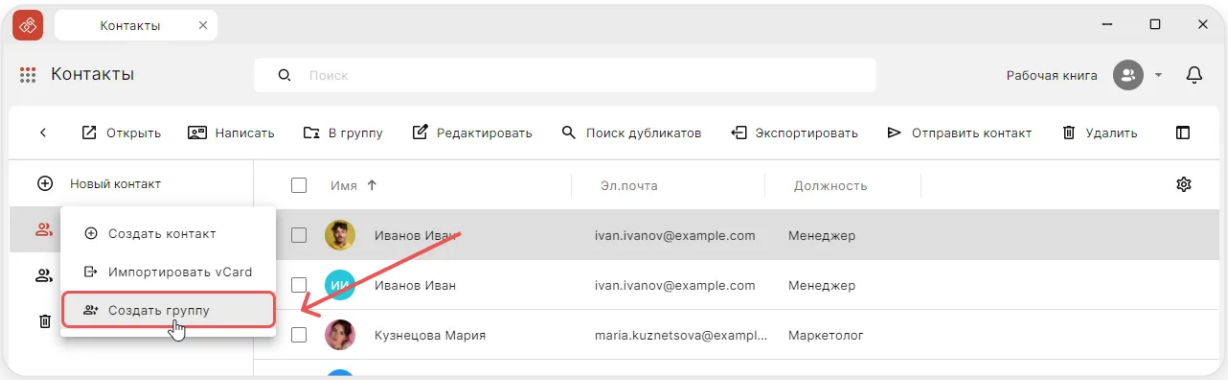
Группы контактов

Группировка контактов помогает удобно организовать вашу адресную книгу. Можно разделить контакты по разным критериям: профессии (коллеги, клиенты, партнёры), проектам или отделам.

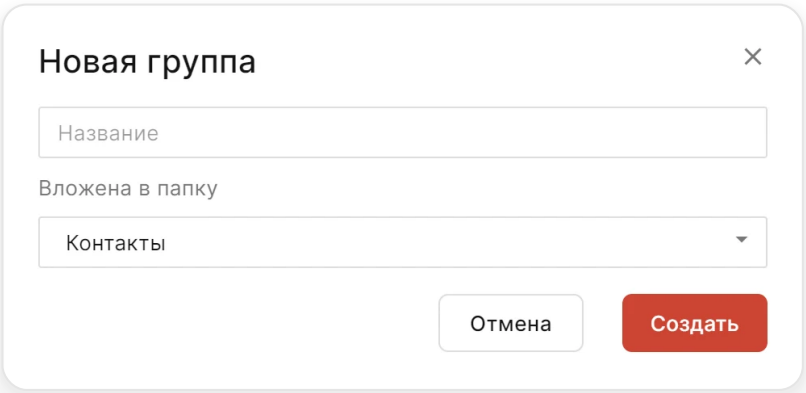
Система поддерживает многоуровневую вложенность групп для детальной классификации.

Создание группы

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Нажмите кнопку **Новый контакт** на панели действий.
3. Выберите **Создать группу**.



4. В открывшемся окне укажите название группы и уровень вложенности (в **Контакты** или в ранее созданную группу).

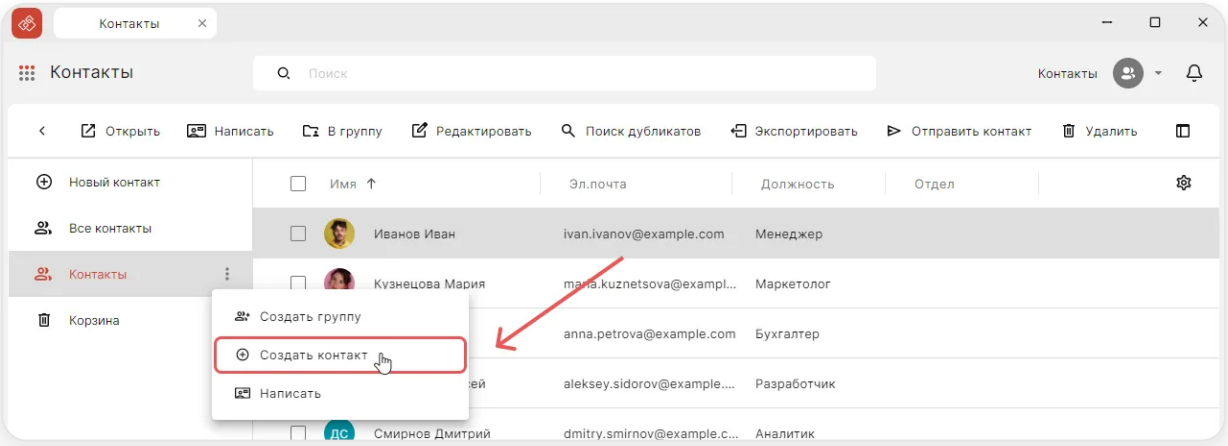


5. Нажмите **Создать**.

Создание вложенной группы

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.

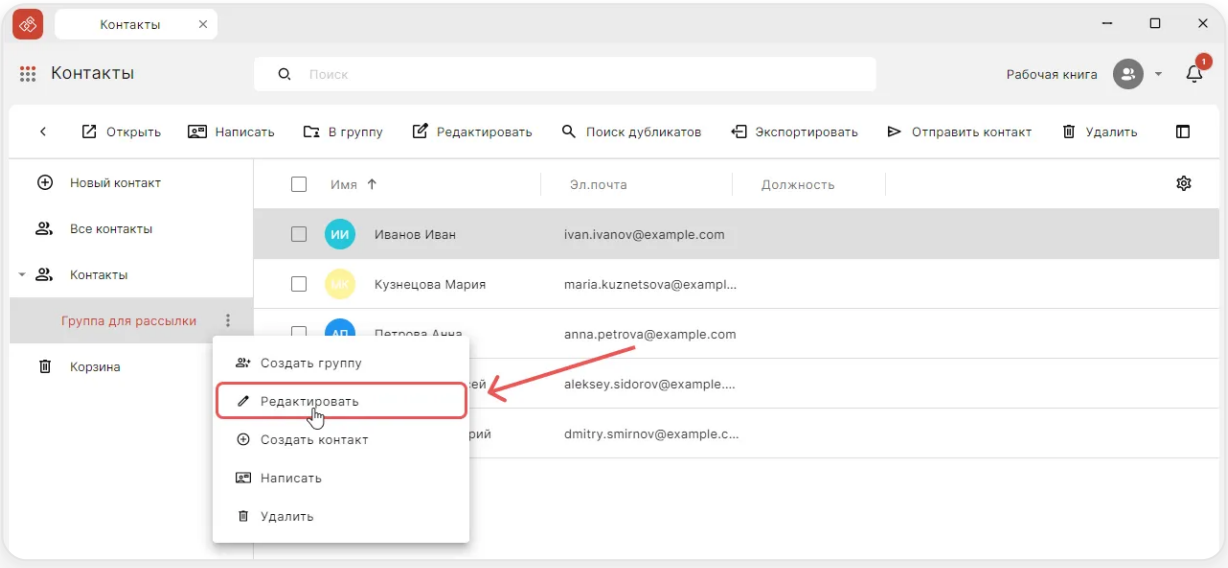
2. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с родительской группой в боковом меню.



3. В открывшемся окне укажите название группы.
4. При необходимости настройте уровень вложенности.
5. Нажмите **Создать**.

Редактирование группы

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с группой в боковом меню.
3. Выберите действие **Редактировать**.
4. Внесите изменения и нажмите **Сохранить**.



Отправка писем всей группе

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с группой в боковом меню.
3. Выберите действие **Написать**.
4. Откроется вкладка с **Новым сообщением**, в котором в поле получатели будут указаны все контакты, состоящие в группе.
5. Укажите содержимое письма и нажмите на **Отправить**.

Удаление группы

> ⚠️ **Примечание**: При удалении группы будут удалены все ее подгруппы и контакты.

1. Перейдите в раздел **Контакты** и переключитесь на необходимую адресную книгу.
2. Вызовите контекстное меню по кнопке **Еще** , размещенной на панели с группой в боковом меню.
3. Выберите действие **Удалить**.
4. Подтвердите удаление группы.

Группа будет удалена, а все ее контакты перемещены в **Корзину**.

Смотрите также

- Адресные книги — организация, группировка и управление адресными книгами.
- Установка сертификатов — инструкция по установке личных, корневых и промежуточных сертификатов, сертификатов других пользователей и списков отзыва (CRL).

Открыть статью на сайте

Как управлять адресными книгами КриптоАРМ

В этой инструкции вы узнаете, как создавать и настраивать адресные книги в КриптоАРМ, подключать внешние источники контактов (LDAP и CardDAV), импортировать контакты в формате vCard, а также управлять адресными книгами и их содержимым.

Содержание:

- Типы адресных книг
- Добавление адресной книги LDAP
- Добавление адресной книги CardDAV
- Импорт контактов vCard
- Управление адресными книгами
- Возможные ошибки
- Смотрите также

Типы адресных книг

Адресные книги в КриптоАРМ предназначены для хранения и управления контактами, которые используются при отправке обычных и зашифрованных писем, а также при шифровании документов.

При установке приложения автоматически создаётся локальная адресная книга «Контакты». Она готова к использованию сразу после запуска — в неё можно добавлять записи вручную или импортировать контакты из файлов.

КриптоАРМ поддерживает несколько типов адресных книг:

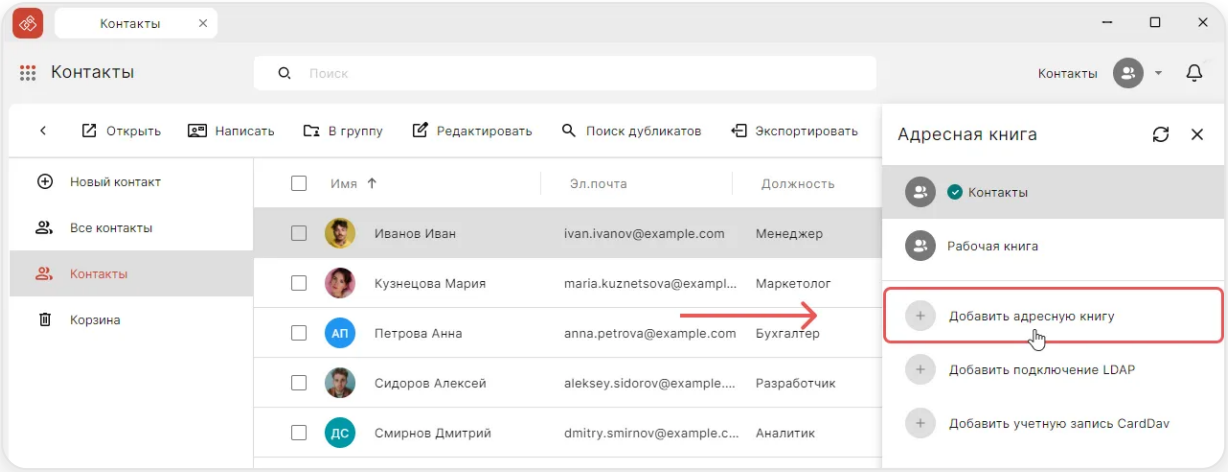
- **Локальная адресная книга** — хранит контакты непосредственно на устройстве пользователя. Поддерживается ручное добавление контактов и импорт из файлов формата vCard.
- **Адресная книга LDAP** — корпоративный каталог, подключаемый по протоколу LDAP.
- **Адресная книга CardDAV** — адресная книга, синхронизируемая с серверами по протоколу CardDAV.

Контакты в адресной книге могут содержать расширенную информацию:

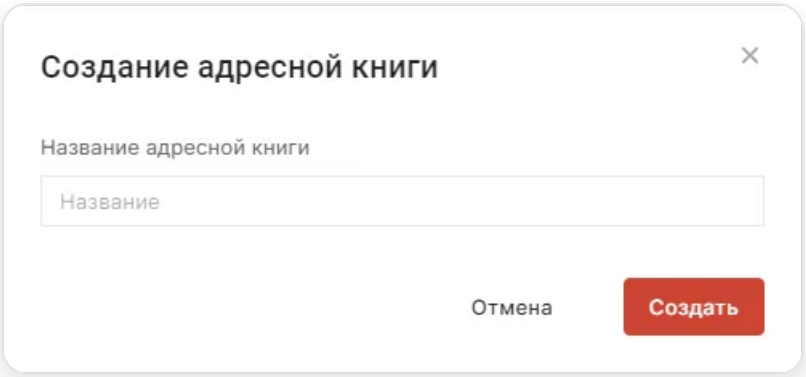
- фамилию, имя, отчество, должность, номера телефонов и e-mail-адреса;
- почтовые адреса и дату рождения;
- фотографии, логотипы и другие мультимедийные элементы;
- электронные сертификаты для защищённой переписки и шифрования данных.

Добавление локальной адресной книги

1. Перейдите в раздел **Контакты** и нажмите на название активной адресной книги.
2. Выберите **Добавить адресную книгу**.



3. В открывшемся окне укажите название адресной книги.
4. Нажмите **Создать**.



> 💡 **Следующий шаг**: переключитесь на новую адресную книгу. Теперь вы можете добавить контакты вручную или импортировать их из файла.

Добавление адресной книги LDAP

Назначение и принцип работы

КриптоАРМ поддерживает интеграцию с корпоративными LDAP-каталогами, что позволяет импортировать контакты из Active Directory и автоматически синхронизировать изменения.

Принцип работы:

1. КриптоАРМ подключается к серверу LDAP с использованием учетной записи пользователя, предназначенной для чтения каталога.
2. По заданной базе поиска и фильтру извлекаются контакты.
3. Полученные записи отображаются в интерфейсе КриптоАРМ как отдельная адресная книга.
4. При включенном автообновлении изменения на сервере автоматически отражаются в КриптоАРМ.

> 💡 **Совет**: Адресная книга LDAP не заменяет локальные контакты, а дополняет их. Можно использовать несколько адресных книг одновременно и комбинировать их с локальными контактами.

Подготовка к подключению

1. Создайте в LDAP учетную запись, с которой будет выполняться подключение к серверу.
2. Настройте фильтры. В зависимости от настроек клиента, могут использоваться фильтры, в которых можно отсечь ненужные записи.
3. Сервер LDAP должен быть доступен по сети с компьютера, на котором работает почтовый клиент.

   Если данный сервер находится за NAT или он закрыт брандмауэром, то необходимо обеспечить доступ по следующим портам:

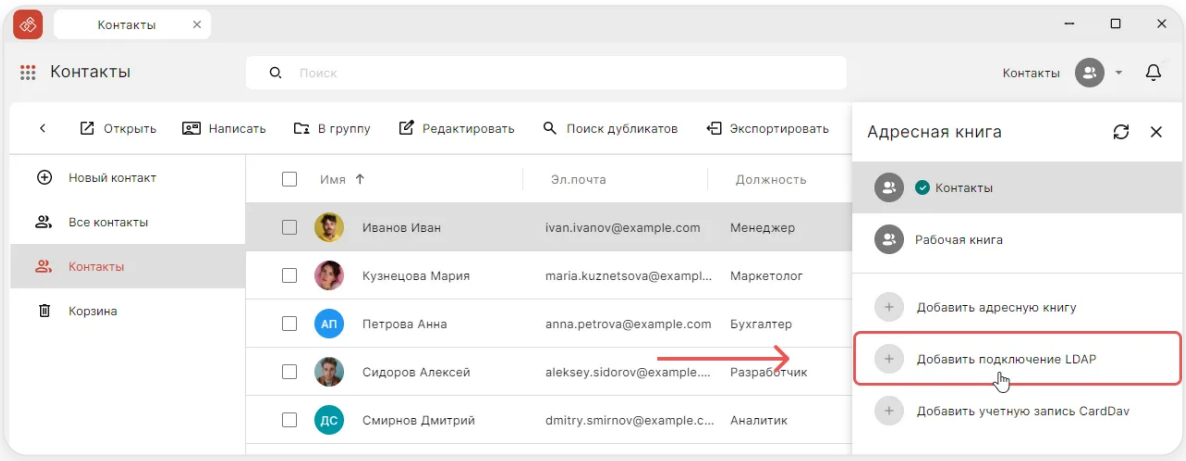
   - 389 tcp или udp. Незащищенный доступ к активному каталогу.
   - 636 tcp или udp. Доступ с защитой SSL.

   Достаточно открыть и использовать один из данных портов, желательно 636.

Создание подключения в КриптоАРМ

1. Откройте форму подключения одним из способов:

   - Перейдите в раздел **Контакты**. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна. Выберите действие **Добавить подключение LDAP**.



- Перейдите в раздел **Настройки** → проверка **Адресные книги**. Нажмите на кнопку **Добавить** ⊕ в верхней части окна и выберите действие **Добавить подключение LDAP**.

2. Откроется форма подключения адресной книги.

3. Укажите параметры подключения:

- **Название адресной книги** — Имя книги, отображаемое в приложении,
- **Имя сервера** — Адрес LDAP-сервера для подключения,
- **Порт** — Порт для подключения к LDAP-серверу,
- **Имя пользователя и пароль** — Учетная запись и пароль для подключения к серверу,

4. Настройте параметры сервера:

- **Время ожидания** — Время ожидания ответа сервера (в секундах),
- **Не возвращать более чем** — Максимальное количество записей за один запрос (0 = без ограничения),
- **Постраничное получение результатов** — При включении позволяет получать результаты частями,
- **Размер страницы** — Количество записей, возвращаемых за одну страницу при постраничном получении,
- **Фильтр поиска** — Фильтр поиска учетных записей в LDAP,
- **База поиска** — DN контейнера, где выполняется поиск,

5. Настройте параметры синхронизации:

- **Получение контактов** — Определяет, какие контакты сохраняются локально,
- **Автообновление каталога** — Настройка синхронизации данных с сервером (Никогда / 1 раз в день / Раз в 60 мин / Раз в 30 мин),
- **Использовать для поиска получателей шифрованных писем** — Если при отправке зашифрованного письма не найден сертификат получателя, система выполнит поиск сертификата во всех доступных книгах. Система выполняет поиск по адресу электронной почты получателя. В результаты поиска включаются все найденные сертификаты, связанные с этим адресом. Данная настройка позволяет исключить адресную книгу из этого автоматического поиска.

6. Нажмите **Сохранить**.

> 💡 **Совет**: После подключения появится новая адресная книга. Чтобы увидеть её контакты, переключитесь на неё (см. Переключение между книгами).

Добавление адресной книги CardDAV

Что такое CardDAV

CardDAV — это открытый интернет-протокол для синхронизации и управления контактами, основанный на стандарте vCard. Протокол обеспечивает централизованное хранение контактной информации на сервере и её доступ с различных устройств и приложений.

Принцип работы:

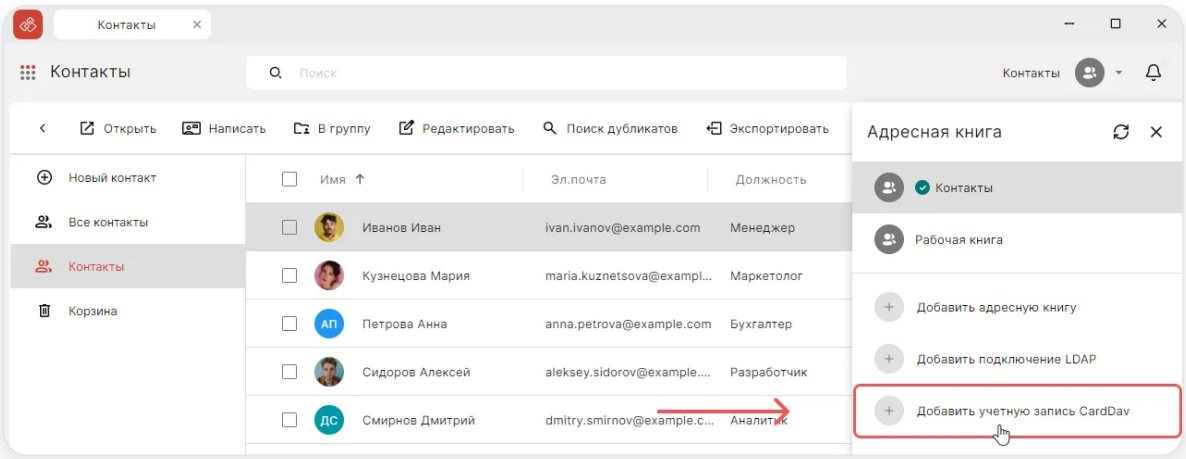
1. **Подключение к серверу**: КриптоАРМ использует учетную запись пользователя для доступа к серверу CardDAV.
2. **Получение контактов**: приложение получает список контактов в формате vCard и отображает их в интерфейсе.
3. **Синхронизация**: изменения, внесённые локально или на сервере, синхронизируются по выбранному интервалу и направлению.
4. **Двусторонняя или односторонняя синхронизация**: данные могут синхронизироваться в обе стороны (локально ↔ сервер) или только с сервера на локальное устройство.

Подготовка учетных данных

В качестве пароля может выступать обычный пароль или специальный пароль приложения, который необходимо создать в настройках сервиса, на котором размещена адресная книга.

Создание подключения в КриптоАРМ

1. Откройте форму подключения:
    - Перейдите в раздел **Контакты** и нажмите на название активной адресной книги. Выберите действие **Добавить учётную запись CardDAV**.



- Перейдите в раздел **Настройки** → проверка **Адресные книги**. Нажмите на кнопку **Добавить** ⊕ в верхней части окна и выберите действие **Добавить учётную запись CardDAV**.

2. Откроется форма добавления адресной книги.

3. Укажите настройки подключения:

   - **Название адресной книги** — Произвольное название, которое будет отображаться в приложении,
   - **Адрес сервера** — Адрес сервера, на котором размещена книга,
   - **Имя пользователя и пароль** — Учетная запись и пароль для подключения к серверу,
   - **Интервал обновления** — Частота синхронизации адресной книги с почтовым сервисом. По умолчанию «Никогда»,
   - **Порядок синхронизации** — По умолчанию выставлено значение «В обе стороны»,
   - **Сохранять новые контакты в учетную запись CardDAV** — По умолчанию настройка неактивна.

4. Нажмите **Сохранить**.

Импорт контактов vCard

vCard (Virtual Contact File) — международный стандарт обмена электронными визитными карточками, предназначенный для хранения и передачи информации о контактах. Формат vCard широко используется в почтовых клиентах, мобильных устройствах, CRM-системах и корпоративных каталогах.

Формат поддерживает хранение различных данных о контакте, включая:

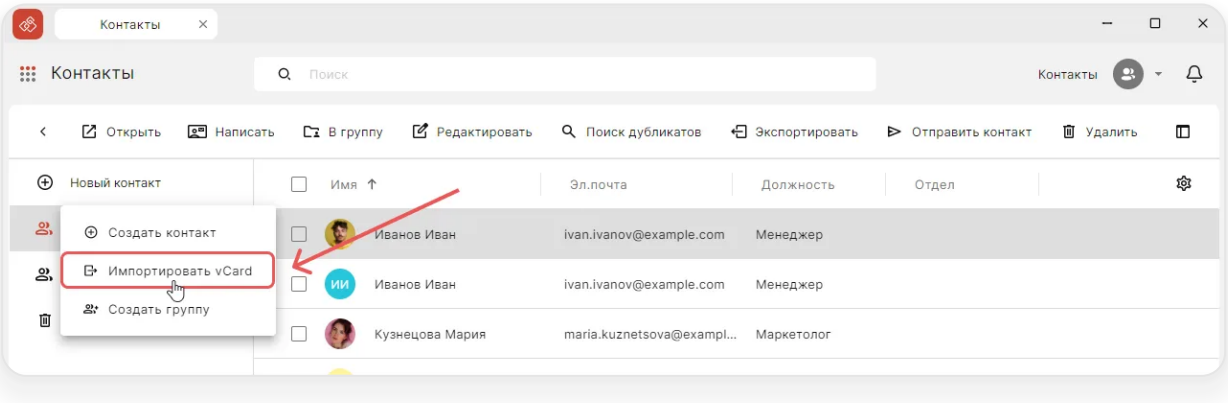
- контактную информацию (ФИО, номера телефонов, e-mail-адреса),
- адресные и демографические данные (место работы, адрес, дата рождения),
- мультимедийные элементы (фотографии, логотипы),
- электронные сертификаты для безопасного обмена документами и письмами.

Принцип работы:

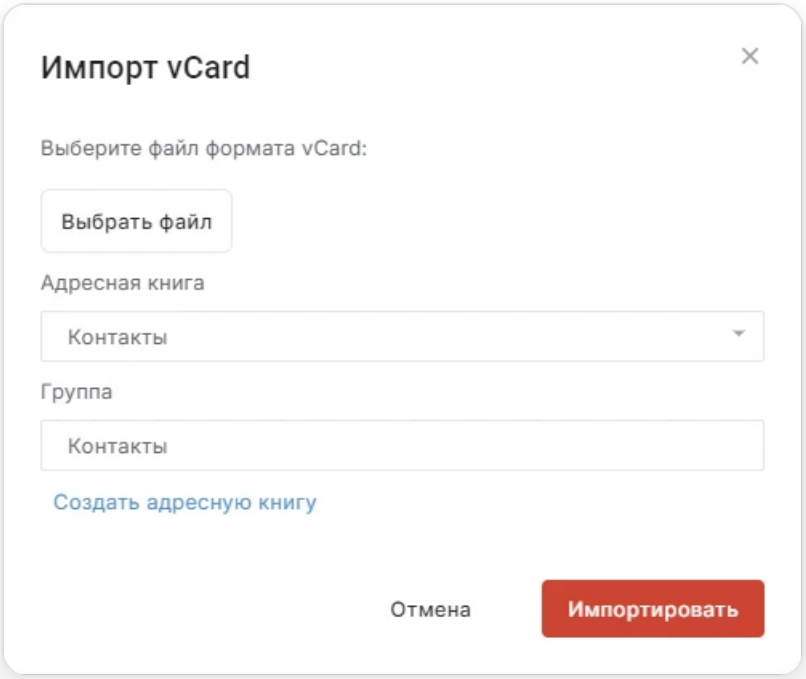
1. Пользователь выбирает файл vCard для импорта.
2. Программа считывает все контакты и извлекает атрибуты (ФИО, телефон, email, и др.).
3. Контакты импортируются в выбранную адресную книгу и при необходимости в заданную группу.
4. При успешном завершении отображается уведомление с количеством импортированных контактов.

Основной способ (через раздел «Контакты»)

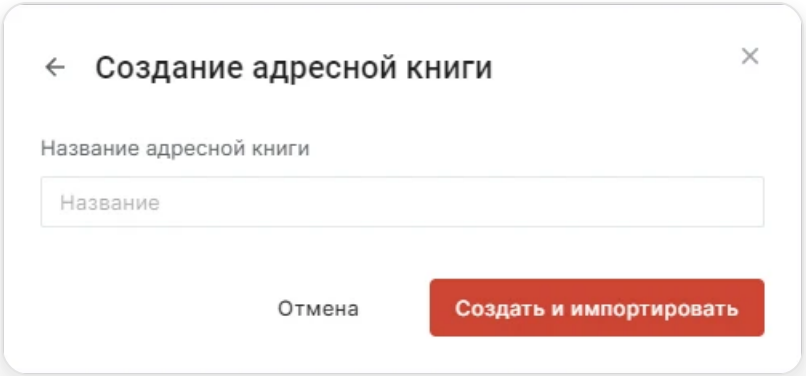
1. Перейдите в раздел **Контакты**.
2. Нажмите на кнопку **Новый контакт** в боковом меню.
3. В появившемся меню выберите **Импорт vCard**.



4. Откроется окно **Импорт vCard**.
    - Нажмите **Выбрать файл** и в появившемся окне файлового менеджера укажите путь к файлу с контактами.
    - Выберите адресную книгу, в которую необходимо импортировать контакты.
    - Укажите группу, в которую будут вложены контакты.



- При необходимости создайте новую группу в указанной адресной книге.



5. Нажмите **Импортировать**.

Будет запущен процесс импорта.

После окончания операции будет выведено уведомление с количеством импортированных контактов.

> 💡 Если экспортируется большой объём контактов, операция может занять некоторое время.

Альтернативный способ (через раздел «Настройки»)

1. Перейдите в раздел **Настройки** → **Адресные книги**.

2. Откроется окно со списком адресных книг (если они обнаружены).
3. Нажмите на кнопку **Добавить** в верхней части окна.
4. Выберите действие **Импортировать из файла vCard**.
5. Откроется окно **Импорт vCard**.
6. Следуйте шагам из инструкции Основной способ.

Управление адресными книгами

Переключение между книгами

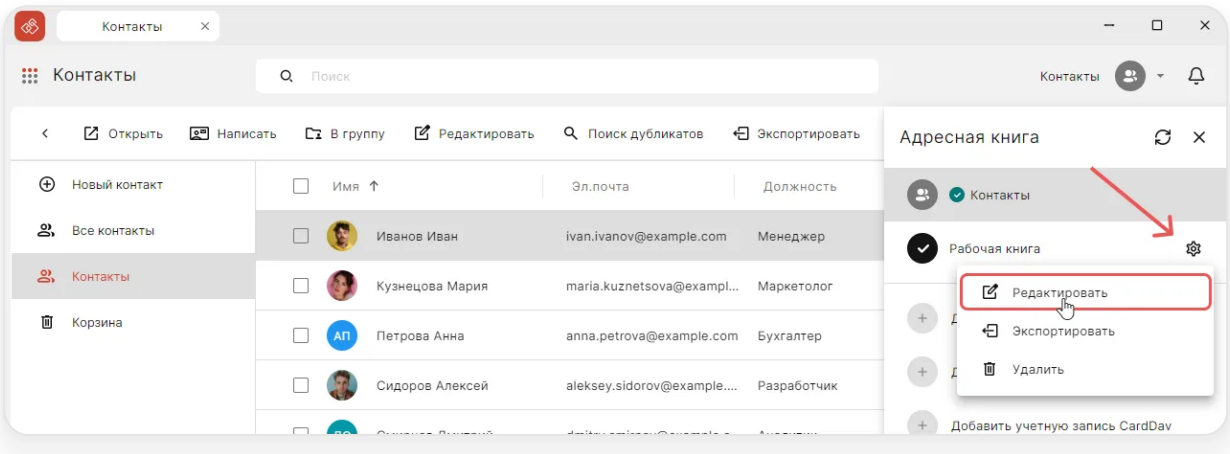
1. Перейдите в раздел **Контакты** и нажмите на название активной адресной книги.
2. В открывшемся окне выберите нужную адресную книгу из списка доступных.

Активная книга отмечается иконкой, список контактов автоматически обновляется в соответствии с выбранной книгой.

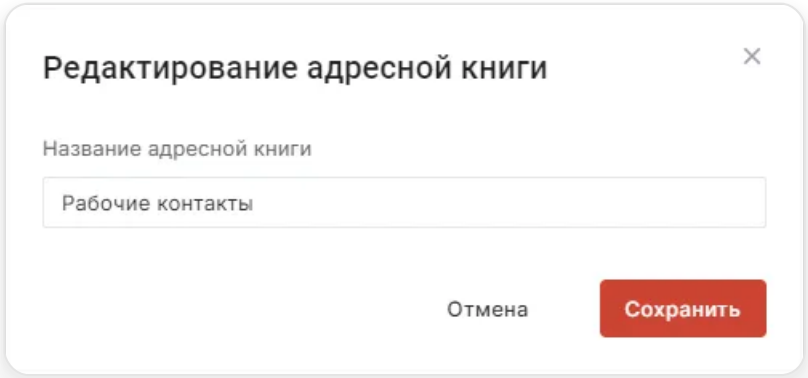
Редактирование адресной книги

> ⚠ **Примечание:** Редактировать можно только название адресной книги. Содержимое контактов редактируется отдельно.

1. Перейдите в раздел **Контакты** и нажмите на название активной адресной книги.
2. В открывшемся окне наведите курсор на панель с адресной книгой.
3. Откройте меню по кнопке **Настройки** и выберите действие **Редактировать**.



4. Укажите новое название адресной книги.



5. Нажмите **Сохранить**.

Экспорт адресной книги

> 💡 **Совет:** Можно экспортировать как всю адресную книгу, так и выбранные контакты (см. Экспорт контакта).

1. Перейдите в раздел **Контакты** и нажмите на название активной адресной книги.
2. В открывшемся окне наведите курсор на панель с адресной книгой.
3. Откройте меню по кнопке **Настройки** и выберите действие **Экспортировать**.
4. Укажите место и имя файла для сохранения.

Экспортируемый файл будет сохранен в формате `.vcf (vCard)`, включая все данные контакта и привязанные сертификаты (если они есть).

Удаление адресной книги

1. Перейдите в раздел **Контакты** и нажмите на название активной адресной книги.
2. В открывшемся окне наведите курсор на панель с адресной книгой.
3. Откройте меню по кнопке **Настройки** и выберите действие **Удалить**.
4. Подтвердите удаление в появившемся окне.

Адресная книга удаляется, а ее контакты помещаются в папку **Корзина**.

Возможные ошибки

Подробности о возникающих ошибках можно найти в Журнале.

Ошибка	Описание	Рекомендуемые действия
Не удалось подключиться к LDAP	Возможно, указаны некорректные параметры подключения	Проверьте параметры подключения адресной книги

Ошибка	Описание	Рекомендуемые действия
Ошибка синхронизации аккаунта CardDAV	Возможно, указаны некорректные параметры подключения	Проверьте параметры подключения адресной книги
Ошибка получения контактов	Возможно, указаны некорректные параметры подключения, либо отсутствует подключение к сети Интернет	1. Проверьте подключение к сети Интернет, 2. Проверьте параметры подключения адресной книги.
Не удалось импортировать контакты (при импорте vCard)	Возможно, файл пустой или поврежден	Проверьте содержимое файла `.vcf` и повторите импорт

Смотрите также

- Работа с контактами — добавление, редактирование и управление контактами в адресной книге.
- Установка сертификатов — инструкция по установке личных, корневых и промежуточных сертификатов, сертификатов других пользователей и списков отзыва (CRL).

Открыть статью на сайте

Описание и возможности API КриптоАРМ

API КриптоАРМ позволяет встроить криптографические операции (подпись, шифрование, работу с сертификатами) прямо в ваше веб- или desktop-приложение. Это руководство подробно объясняет архитектуру протокола `cryptoarm://`, все доступные команды, форматы запросов и пошаговые сценарии интеграции. Вы узнаете, как настроить взаимодействие между вашим порталом и КриптоАРМ для безопасной обработки документов.

Содержание:

- Описание и возможности API КриптоАРМ
- Общая информация
- Доступные команды
- Сценарий выполнения команд для web-приложений
- Сценарий выполнения команд для локальных приложений
- Формат ссылки для web КриптоАРМ API
- Формат ссылки для локального варианта КриптоАРМ API
- Аутентификация
  - mTLS (авторизация по сертификату сервера)
  - OIDC (OpenID Connect)
  - Комбинированная (oidc:mtls)
  - Токен авторизации (customAuth)
- Описание запросов и ответов
  - POST-запрос
  - GET-запрос
  - Ответ
  - Объект Error
  - HTTP-коды

Общая информация

КриптоАРМ поддерживает API с двумя возможными точками вызова:

- Локальное приложение на рабочем месте,
- Web-приложение (сервис).

При вызове операции через API приложение КриптоАРМ будет запущено и отобразит необходимый раздел с переданными параметрами. Команду можно ввести через адресную строку браузера (вы можете размещать их так же, как ссылки на веб-страницы) или в терминале.

Для взаимодействия используется зарегистрированный протокол `cryptoarm://`.

Доступные команды

В таблице ниже перечислены все команды API. Кликните на название команды, чтобы перейти к детальному описанию, синтаксису и примерам JSON.

Команда	Описание
`signAndEncrypt`	выполнение криптографических операций над документами (подпись, шифрование, проверка подписи, расшифрование)
`certificates`	экспорт или импорт сертификатов, просмотр свойств сертификата
`certrequests`	генерация запросов на сертификат
`diagnostics`	диагностика рабочего места
`startView`	открыть окно или вкладку
`sendMail`	создание нового черновика электронного письма с переданными параметрами
`saveDocuments`	импорт документов в хранилище КриптоАРМ
`authorize`	авторизация по протоколу OIDC (OpenID Connect)
`callback`	обратный вызов OIDC-авторизации (используется внутренне, не вызывается напрямую)
`mtlsAuthorization`	авторизация по сертификату (mTLS)

Сценарий выполнения команд для web-приложений

1. **Инициация операции**
   - Пользователь заходит на портал (веб-приложение).
   - Выбирает объекты (например, список документов) и действие (например, подпись).
2. **Генерация ссылки**
   - Портал формирует и отображает (или автоматически перенаправляет) ссылку с протоколом `cryptoarm://`, содержащую идентификатор операции.
   - Опционально может быть передан тип аутентификации (`authType`) как query-параметр.
3. **Запуск и запрос параметров**
   - Если КриптоАРМ не запущен, система автоматически его запускает.

- КриптоАРМ обращается к порталу, запрашивая JSON с параметрами для выполнения операции.
- JSON генерируется на сервере веб-приложения.

4. **Обработка команды**
   - Полученный JSON анализируется.
   - В зависимости от типа операции, КриптоАРМ может выполнить дополнительные запросы к веб-приложению (например, загрузка документов).
5. **Подтверждение пользователем**
   - Пользователь проверяет детали операции и подтверждает её выполнение.
   - На время выполнения функционал приложения блокируется для предотвращения конфликтов.
6. **Отправка результатов**
   - Результаты операции (например, подписанные документы) передаются обратно на сервер веб-приложения.

Сценарий выполнения команд для локальных приложений

1. **Инициация операции**
   - Пользователь открывает стороннее приложение с поддержкой КриптоАРМ API.
   - Выбирает объекты (например, документы) и действие (например, подпись).
2. **Формирование JSON-запроса**
   - Приложение генерирует JSON-объект с параметрами операции и передаёт его в КриптоАРМ (через CLI или API).
3. **Запуск и обработка параметров**
   - Если КриптоАРМ не запущен, он автоматически стартует.
   - Приложение может дополнительно запросить JSON с сервера (если часть параметров хранится удалённо).
4. **Подтверждение пользователем**
   - Пользователь проверяет детали операции и подтверждает её выполнение.
   - Функционал приложения блокируется до завершения операции.
5. **Сохранение результатов**
   - Результаты (например, подписанные файлы) сохраняются в локальную папку, указанную в параметрах операции.

Формат ссылки для web КриптоАРМ API

```
cryptoarm://<command>/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `?id=<id>` - обязательный параметр. Идентификатор транзакции.
- `&authType=<authType>` - необязательный параметр. Тип аутентификации. Возможные значения:
- `oidc` — авторизация через OpenID Connect
- `mtls` — авторизация по сертификату (mTLS)
- `oidc:mtls` — комбинированная авторизация (OIDC + mTLS)

Формат ссылки для локального варианта КриптоАРМ API

Вариант 1 (через файл):

```
cryptoarm://<command>/file:///<путь к JSON-файлу>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URI>` - путь к файлу JSON с параметрами, нужными для выполнения команды

Вариант 2 (JSON встроенный):

```
cryptoarm://<command>/<JSON>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<JSON>` - JSON-RPC объект с параметрами, нужными для выполнения команды

> JSON должен начинаться с `{"jsonrpc":"2.0"...}`.

Дополнительные параметры локального JSON:

Ключ	Тип	Описание
appName	string	

Ключ	Тип	Описание
		Необязательный параметр. Название стороннего приложения, отображаемое в окне подтверждения операции.
`apiKey`	string	Необязательный параметр. Проверочный код, отображаемый в окне подтверждения операции.
`authType`	string	Необязательный параметр. Тип аутентификации (см. выше).

Аутентификация

КриптоАРМ поддерживает несколько механизмов аутентификации, которые могут быть указаны в параметре `authType`.

mTLS (авторизация по сертификату сервера)

При вызове `cryptoarm://<command>/<URL>/?id=<id>&authType=mtls` КриптоАРМ:

1. Запрашивает серверный сертификат с `<URL>`.
2. Сравнивает его с сохранённым сертификатом доверенного сервиса.
3. Если сертификаты совпадают — доступ разрешён автоматически.
4. Если нет — отображает диалог подтверждения для пользователя.

OIDC (OpenID Connect)

При вызове `cryptoarm://<command>/<URL>/?id=<id>&authType=oidc` КриптоАРМ:

1. Запрашивает параметры авторизации с сервера (эндпоинт `authorization.parameters`).
2. Строит URL авторизации и открывает браузер пользователя.
3. После успешной аутентификации получает токен доступа через `callback`.
4. Сохраняет токены в доверенном сервисе и использует их для последующих запросов (передаёт в заголовке `Authorization: Bearer <token>` или в query-параметре, в зависимости от настройки `customAuth`).

Комбинированная (oidc:mtls)

При `authType=oidc:mtls` КриптоАРМ сначала выполняет OIDC-авторизацию, а затем использует клиентский сертификат (mTLS) для защищённых запросов.

Токен авторизации (customAuth)

После успешной авторизации токен доступа автоматически добавляется ко всем последующим запросам к серверу в соответствии с настройками `customAuth`:

- `in: "header"` (по умолчанию) — токен в заголовке `Authorization: Bearer <token>`
- `in: "query"` — токен в query-параметре `?token=<token>`
- `in: "body"` — токен в теле запроса как поле `token`

Название ключа, схема и размещение токена могут быть переопределены через `customAuth.key` и `customAuth.scheme`.

Описание запросов и ответов

Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола **JSON-RPC 2.0**.

В качестве транспорта используется HTTP. Должен использоваться TLS, незащищенные соединения КриптоАРМ отклоняет.

При включенной настройке «Использовать только набор алгоритмов ГОСТ для подключений по API» КриптоАРМ будет принимать только ГОСТ TLS, остальные шифросюиты будут отклоняться.

POST-запрос

КриптоАРМ выполняет HTTP POST-запросы, которые содержат заголовки:

- `Content-Type`: должен быть application/json.
- `Content-Length`: должен содержать правильную длину в соответствии с HTTP-спецификацией.
- `Accept`: должен быть application/json.

GET-запрос

Используются для скачивания файлов с сервера (например, документов для подписи, вложений почты). Заголовки GET-запросов аналогичны POST, но без `Content-Type` и `Content-Length`.

Ответ

HTTP-ответ сервера должен содержать заголовки:

- `Content-Type`: должен быть application/json.
- `Content-Length`: должен содержать правильную длину в соответствии с HTTP-спецификацией.

Объект Error

В случае ошибки сервер должен отправить ответ следующей структуры:

Ключ	Тип	Описание
code	number	Код ошибки
message	string	Короткое описание ошибки
data	string/Object	Необязательное поле. Может содержать дополнительные сведения об ошибке.

HTTP-коды

Код	Ошибка	Описание
200	OK	И для ответов, и для ошибок
204	No Response	Для пустых запросов (нотификация)
405	Method Not Allowed	Метод не доступен
415	Unsupported Media Type	Если `Content-Type` не application/json

Открыть статью на сайте

Команда signAndEncrypt — описание и примеры

Команда `signAndEncrypt` API КриптоАРМ предназначена для подписи, шифрования и проверки документов при интеграции с внешними системами. Она позволяет безопасно обрабатывать одиночные файлы и пакеты документов через JSON-RPC, поддерживает различные режимы операций и может использоваться как механизм аутентификации.

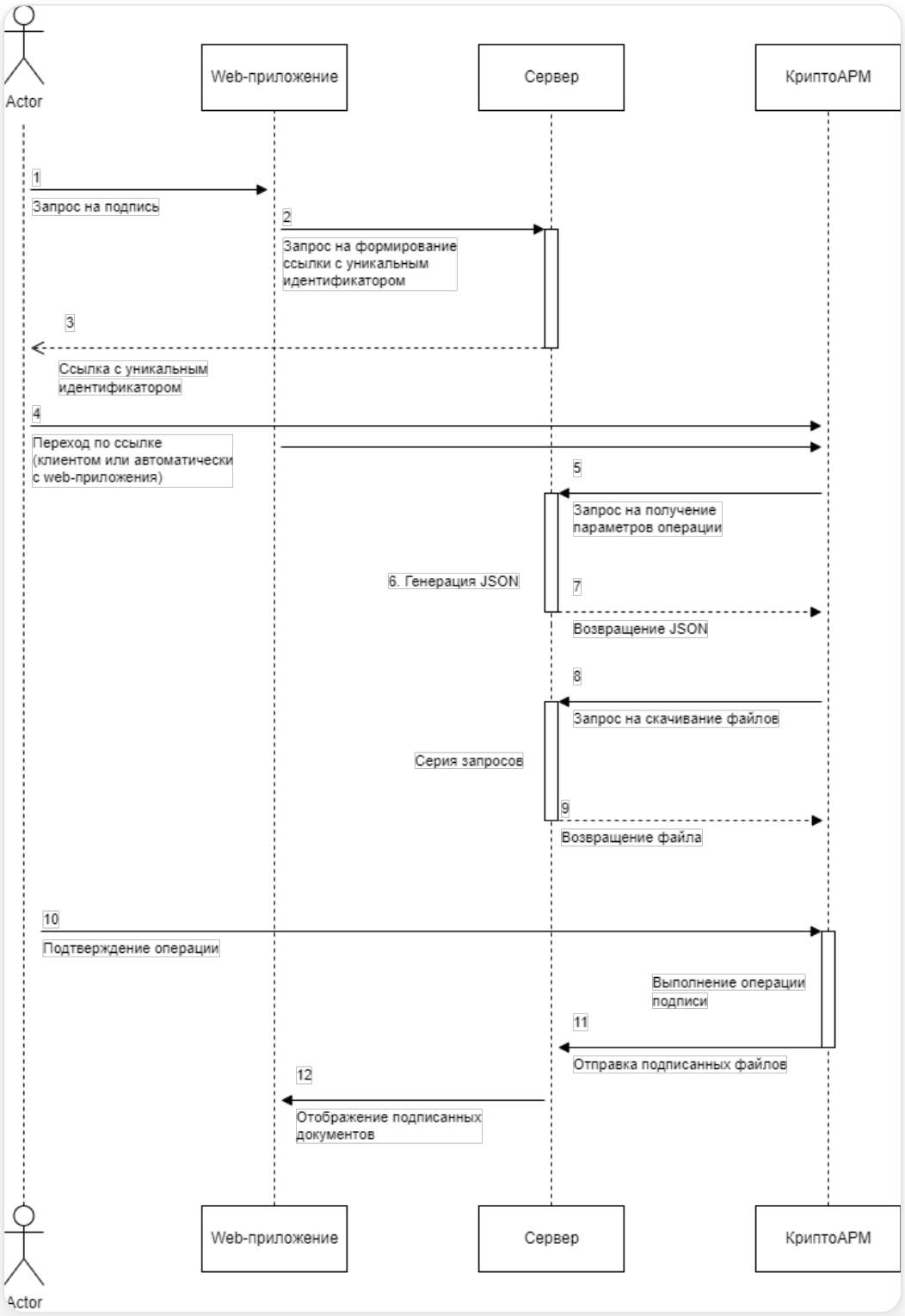
Содержание:

- Общая информация
- Формат ссылки
- Описание запросов и ответов
- Получение параметров операции
- Отправка результатов операций
- Справочник интерфейсов
- Интерфейс приложения

Общая информация

Команда `signAndEncrypt` (подпись и шифрование) используется для запроса на подпись документа или пакета документов. Может использоваться в качестве аутентификатора.

> 📌 Выполнение операции требует действующей лицензии на КриптоАРМ.



Формат ссылки

Для выполнения команды `signAndEncrypt` должна быть сформирована ссылка вида:

```
cryptoarm://signAndEncrypt/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `signAndEncrypt` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `?id=<id>` - обязательный параметр. Идентификатор транзакции.
- `&authType=<authType>` - необязательный параметр. Тип аутентификации.

Пример:

```
cryptoarm://signAndEncrypt/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Описание запросов и ответов

Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0. В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Получение параметров операции

После получения команды `signAndEncrypt` КриптоАРМ отправляет запрос на `<URL>` для получения параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.parameters`	Используемый метод. Всегда `signAndEncrypt.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.
diagnostic	`IDiagnosticsInformation`	Диагностическая информация о рабочем месте. Содержит поля `VERSIONS`, `PROVIDERS`, `LICENSES`.

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
      "VERSIONS": {
        "csp": "5.0.11753",
        "cryptoarm": "2.5.2",
        "openssl": "1.1.1w"
      },
      "PROVIDERS": {
        "GOST2012_256": true,
        "GOST2012_512": true,
        "openssl": true
      },
      "LICENSES": {
        "csp": {
          "status": true,
          "type": "",
          "expiration": ""
        },
        "cryptoarm": {
          "status": true,
          "type": "Permanent",
          "expiration": ""
        }
      }
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ISignAndEncryptParameters`	Объект со сведениями о параметрах операции подписи
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример для прямых операций (SIGN + ARCHIVE + ENCRYPT):

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": [
            "SIGN",
            "ARCHIVE",
            "ENCRYPT"
        ],
        "props": {
            "headerText": "Подпись документов cryptoarm.ru",
            "descriptionText": "Подпись пакета документов",
            "license": "",
            "files": [{
                    "name": "file1.txt",
                    "url": "http://localhost:8080/public/files/file1.txt",
                    "id": "1",
                    "urlDetached": ""
                },
                {
                    "name": "file2.txt",
                    "url": "http://localhost:8080/public/files/file2.txt",
                    "id": "2",
                    "urlDetached": ""
                },
                {
                    "name": "file4.pdf",
                    "url": "http://localhost:8080/public/files/file4.pdf",
                    "id": "4",
                    "urlDetached": ""
                }
            ],
            "uploader": "http://localhost:8080/upload",
            "uploadMethod": "json",
            "extra": {
                "token": "9c7101f7-9c47-4481-b4da-a6a497abde08",
                "signType": 1,
                "signStandard": 1,
                "signEncoding": 1,
                "encryptEncoding": 1,
                "encryptAlgorithm": 2,
                "returnFiles": true,
                "isAddStampToPdf": true
            }
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Пример для проверки подписи (VERIFYSIGN):

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "jsonrpc": "2.0",
    "result": {
        "operation": ["VERIFYSIGN"],
        "props": {
            "files": [{
                "name": "signed_file.txt.sig",
                "url": "http://localhost:8080/public/files/signed_file.txt.sig",
                "id": "8",
                "urlDetached": "http://localhost:8080/public/files/
original_file.txt"
            }],
            "extra": {
                "printReport": true
            }
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка результатов операций

Отправка результата прямых операций

После того, как пользователь выберет нужные сертификаты, КриптоАРМ выполняет операцию. Результаты отправляются POST-запросом в формате JSON или multipart/form-data.

Вариант 1: JSON (по умолчанию, `uploadMethod` = "json")

Файлы результатов кодируются в Base64 и передаются в теле JSON-запроса.

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.outDirectResults`	Используемый метод. Всегда `signAndEncrypt.outDirectResults`.
params	Объект типа `IDirectResults`	Сведения о результатах прямой операции

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
```

```
    "method": "signAndEncrypt.outDirectResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "status": "Completed",
        "directResults": [
          {
            "id": "2",
            "out": "MIIWgQYJKoZIhvcNAQcCoIIWcjCCFm4CA…cN/aHmA=",
            "signValid": true,
            "signers": [
              {
                "isValid": true,
                "signingTime": 1594209848000,
                "isDetached": false,
                "signerCertificate": {
                  "hash": "abc123...",
                  "issuerFriendlyName": "УЦ Тест",
                  "issuerName": "CN=УЦ Тест",
                  "subjectFriendlyName": "Иванов Иван",
                  "subjectName": "CN=Иванов Иван",
                  "status": true,
                  "serial": "1234567890",
                  "notAfter": 1725139200000,
                  "notBefore": 1593603200000
                }
              }
            ]
          }
        ]
    }
}
```


Вариант 2: multipart/form-data (`uploadMethod` = "multipart/form-data")

Файлы результатов передаются как бинарные вложения в multipart-запросе. JSON с метаданными — в поле `operation-response`.

> При использовании multipart/form-data файлы передаются как есть (без Base64-кодирования). Заголовок `Content-Type` устанавливается автоматически (`multipart/form-data`).

Отправка результата проверки подписи

Результаты проверки подписи отправляются POST-запросом.

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.verifySignResults`	Используемый метод.

Ключ	Значение	Описание
params	Объект типа `IVerifySignResults`	Сведения о проверке подписи

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.verifySignResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "status": "Completed",
        "verifySignResults": [
          {
            "id": "2",
            "signValid": false,
            "isSignaturePades": false,
            "signers": [
              {
                "isValid": false,
                "signingTime": 1594209848000,
                "isDetached": true,
                "isCades": true,
                "cadesType": 1,
                "signatureAlgorithm": "1.2.643.7.1.1.3.2",
                "signatureDigestAlgorithm": "1.2.643.7.1.1.2.2",
                "signerCertificate": {
                  "hash": "abc123...",
                  "issuerFriendlyName": "Минкомсвязь России",
                  "issuerName": "Минкомсвязь России",
                  "subjectFriendlyName": "Минкомсвязь России",
                  "subjectName": "Минкомсвязь России",
                  "status": true,
                  "serial": "12345",
                  "provider": "Crypto-Pro GOST R 34.10-2012",
                  "notAfter": 1725139200000,
                  "notBefore": 1593603200000,
                  "rootCAMinComSvyaz": true
                }
              }
            ],
            "outReport": "base64_encoded_pdf_report..."
          }
        ]
    }
}
```

Для операций `VERIFYSIGN` файлы результатов НЕ возвращаются (поле `out` всегда пустое). Вместо них передаются свойства подписи (`signProps`). Если включён `printReport`, в поле `outReport` может быть передан PDF-отчёт в Base64.

Обработка ошибок

При частичном успехе (некоторые файлы обработаны успешно, некоторые — нет) отправляется ответ со `status: "Error"` и `Error: true`, с полем `ErrorDescription`, содержащим описание ошибки, и списком частичных результатов в `directResults`.

Сохранение результатов локально

Если `uploader` содержит путь `file://`, результаты сохраняются локально:

- `file:///path/to/dir` — для каждого файла создаётся JSON-файл с результатами (`direct-result-{id}-{fileId}.json`)
- Через `localResultParams.savePath` — аналогично

Имя файла: `<operation>-result-<id><-fileId>.json` (например, `direct-result-2c48eb32-1.json`).

Справочник интерфейсов

Интерфейс ISignAndEncryptParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string[]	Тип операции. Доступные значения: `SIGN`, `ARCHIVE`, `ENCRYPT`, `VERIFYSIGN`, `UNSIGN`, `UNZIP`, `DECRYPT`. Нельзя смешивать прямые (`SIGN`, `ARCHIVE`, `ENCRYPT`) и обратные (`UNSIGN`, `UNZIP`, `DECRYPT`) операции. `VERIFYSIGN` не комбинируется с другими.
props	`ISignAndEncryptOperationProps`	Параметры операции

Типы операций

Прямые операции (прямые):

Значение	Описание
SIGN	Подпись
ARCHIVE	Архивирование
ENCRYPT	Шифрование

Обратные операции:

Значение	Описание
UNSIGN	Снятие подписи
DECRYPT	Расшифрование
UNZIP	Разархивирование

Проверка подписи:

Значение	Описание
VERIFYSIGN	Проверка подписи

Интерфейс ISignAndEncryptOperationProps

Интерфейс `ISignAndEncryptOperationProps` описывает параметры операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.
license?	string	Необязательное свойство. Содержит временную лицензию, которая будет использоваться для выполнения операции в КриптоАРМ.
uploader	string	Ссылка, на которую будут отправлены или сохранены результаты операции. Поддерживает протоколы `https://` и `file://`. Если указан `file://`, результаты сохраняются локально в указанную директорию.
uploadMethod?	string	Способ отправки результатов. Возможные значения: `"json"` (по умолчанию) — файлы в Base64

Свойство	Тип	Описание
		внутри JSON, `"multipart/form-data"` — файлы как бинарные вложения в multipart-запросе.
files	Массив типа `IFile[]`	Массив файлов на подпись. Если не передан, то должен быть передан параметр `archive`.
archive	`IFile`	Архив файлов на подпись. Распаковываются после получения. Параметр может использоваться вместо `files`.
extra	Объект типа `IExtra`	Настройки операции
localResultParams	Объект типа `ILocalResultParams`	Необязательное свойство. Используется только для локального API. Указывает пути для сохранения результатов.

Интерфейс IFile

Интерфейс `IFile` описывает файлы и ссылки на них.

Свойство	Тип	Описание
name	string	Имя файла (с расширением)
url	string	Ссылка на скачивание файла
id	string	Уникальный идентификатор файла
urlDetached?	string	Необязательный параметр. Используется для откреплённой подписи — ссылка на файл с отделённой подписью.

Интерфейс IExtra

Интерфейс `IExtra` описывает настройки операции.

Если параметр не задан, то пользователю доступен выбор из всех доступных в приложении значений.

Свойство	Тип	Описание
signType?	number/string	Необязательный параметр. Тип подписи. `0` — присоединённая, `1` — отсоединённая.

Свойство	Тип	Описание
signStandard?	number/string	Необязательный параметр. Стандарт подписи. `0` — CAdES-BES (CMS), `1` — CAdES-X Long Type 1, `2` — CAdES-T, `3` — CAdES-A. Также поддерживается псевдоним `signStandart`.
signEncoding?	number/string	Необязательный параметр. Кодировка подписи: `0` — PEM (BASE-64), `1` — DER.
encryptEncoding?	number/string	Необязательный параметр. Кодировка шифрования: `0` — BASE-64, `1` — DER.
encryptAlgorithm?	number	Необязательный параметр. Алгоритм шифрования: `0` — ГОСТ 28147-89, `1` — ГОСТ 34.12-2015 Магма, `2` — ГОСТ 34.12-2015 Кузнечик.
timestampOnSign?	string	Необязательный параметр. Штамп времени на подпись (`"true"`/`"false"`). Если стандарт подписи не CAdES-BES, автоматически включается.
timestampOnData?	string	Необязательный параметр. Штамп времени на данные (`"true"`/`"false"`).
tspURL?	string	Необязательный параметр. Адрес службы штампов времени.
ocspURL?	string	Необязательный параметр. Адрес службы актуальных статусов (OCSP).
token?	string	Необязательный параметр. Токен, который будет использоваться при скачивании файлов с сервиса (добавляется как query-параметр `accessToken`).
encryptCertificates?	string[]	Необязательный параметр. Массив сертификатов шифрования в формате X.509 Base64.
signCertificate?	`{ x509: string }` | `{ issuerName: string, serial: string }` | `{ hash: string }`	

Свойство	Тип	Описание
		Необязательный параметр. Сертификат подписчика: либо X.509 в Base64, либо параметры для поиска в хранилище (по issuerName+serial или по hash).
signatureExtension?	string	Необязательный параметр. Расширение для подписанного файла (например, `"sig"`, `"p7s"`). По умолчанию: `"sig"`.
encryptionExtension?	string	Необязательный параметр. Расширение для зашифрованного файла. По умолчанию: `"enc"`.
isAddStampToPdf?	boolean	Необязательный параметр. Добавить штамп подписи для PDF-файлов.
isSignaturePades?	boolean	Необязательный параметр. Использовать формат подписи PAdES для PDF.
isPdfCertificationSign?	boolean	Необязательный параметр. Сертификационная подпись PDF.
signerChainIncludeKind?	string	Необязательный параметр. Тип включения цепочки сертификатов: `"personal"` (только подписчик) или `"full"` (вся цепочка). По умолчанию: `"personal"`.
isSafeMode?	boolean	Необязательный параметр. Безопасный режим подписи.
printReport?	boolean	Необязательный параметр. Создавать PDF-отчёт о проверке подписи (только для `VERIFYSIGN`).
returnFiles?	boolean	Необязательный параметр. Возвращать ли файлы результатов. По умолчанию: `true`. Если `false`, в ответе передаются только метаданные без содержимого файлов.
showSettingsBeforeOperation?	boolean	Необязательный параметр. Показывать ли окно настроек перед выполнением операции. По умолчанию: `true`.
MCHD?	object	

Свойство	Тип	Описание
		Необязательный параметр. Файл метки доверенного времени (МЧД).
signStampAppearance?	`ISignStampAppearance`	Необязательный параметр. Параметры внешнего вида штампа подписи.
PAdESStampAppearance?	`ISignStampAppearance`	Необязательный параметр. Параметры внешнего вида штампа PAdES.
signStampPAdES?	`{ isDisplayedOnAllPages?: boolean, pageNumbers?: number[], pagesSelection?: PagesSelection, pdfMarkedArea?: IPdfMarkedArea }`	Необязательный параметр. Параметры размещения штампа PAdES.
signStampPosition?	`IPdfAreaDimensions`	Необязательный параметр. Позиция и размеры области штампа подписи.

Интерфейс IDirectResults

Объекты данного типа описывают результаты прямой операции.

Свойство	Тип	Описание
id	string	Идентификатор транзакции.
status	string	Статус выполнения операции: `"Completed"` (успех) или `"Error"` (ошибка).
Error?	boolean	Необязательное поле. Присутствует при ошибке (`true`).
ErrorDescription?	string	Необязательное поле. Описание ошибки.
directResults	`IDirectResultOut[]`	Массив результатов прямых операций

Интерфейс IDirectResultOut

Объекты данного типа содержат результаты прямой операции для файла.

Свойство	Тип	Описание
id	string	Идентификатор исходного файла.

Свойство	Тип	Описание
out	string	Результат операции в BASE-64. Может быть пустой строкой при ошибке конкретного файла.
outReport?	string	Необязательный параметр. PDF-отчёт в Base64.
outSignStamp?	string	Необязательный параметр. PDF со штампом подписи в Base64 (если isAddStampToPdf).
signers?	ISignerStatus[]	Необязательный параметр. Сведения о подписчиках.
signValid?	boolean	Необязательный параметр. Общий статус всех подписей файла.
isSignaturePades?	boolean	Необязательный параметр. Является ли подпись PAdES.

Интерфейс IVerifySignResults

Объекты данного типа описывают результаты проверки подписи.

Свойство	Тип	Описание
id	string	Идентификатор транзакции.
status	string	Статус: "Completed" или "Error".
Error?	boolean	Флаг ошибки.
ErrorDescription?	string	Описание ошибки.
verifySignResults	IVerifySignResult[]	Массив результатов проверки

Интерфейс IVerifySignResult

Объекты данного типа описывают результат проверки подписи для одного файла.

Свойство	Тип	Описание
id	string	Идентификатор исходного файла
signValid	boolean	Общий статус проверки подписи
isSignaturePades	boolean	Является ли подпись формата PAdES

Свойство	Тип	Описание
signers	`ISignerStatus[]`	Информация о подписчиках документа
outReport?	string	Необязательный параметр. PDF-отчёт в Base64 (если `printReport: true`).

Интерфейс ISignerStatus

Объекты данного типа описывают сведения о подписчиках.

Свойство	Тип	Описание
signerCertificate	`ICertificateIdentityInfo`	Сведения о сертификате подписчика. Кроме полей из `ICertificateIdentityInfo` дополнительно содержит поля: `hash`, `issuerFriendlyName`, `issuerName`, `subjectFriendlyName`, `subjectName`, `status`, `serial`, `notAfter` (number), `notBefore` (number), `rootCAMinComSvyaz` (boolean), `provider` (string).
isValid	boolean	Статус подписи
signingTime	number	Время подписи (timestamp в миллисекундах)
isDetached	boolean	Признак отсоединённой подписи
isCades?	boolean	Признак CAdES подписи
cadesType?	number	Тип CAdES подписи
isSignaturePades?	boolean	Признак PAdES подписи
signatureAlgorithm?	string	OID алгоритма подписи
signatureDigestAlgorithm?	string	OID алгоритма хеширования
verifyingTime?	number	Время проверки (timestamp)
extVerifyInfo?	any	Дополнительная информация о проверке

Интерфейс ILocalResultParams

Объекты данного типа используется только в параметрах локального API.

Свойство	Тип	Описание
savePath?	string	Необязательный параметр. Путь для сохранения результатов операции.
saveResultsSeparately?	boolean	Необязательный параметр. Определяет, сохранять ли результаты по каждому файлу в отдельный JSON-файл или в один.

Интерфейс ISignStampAppearance

Интерфейс `ISignStampAppearance` описывает параметры для штампа PDF.

Свойство	Тип	Описание
mockupSettings	`IMockupSettings`	Настройки внешнего вида штампа подписи
requisitesSettings	`IRequisitesSettings`	Настройки содержимого штампа (реквизиты)
pageSelection	string	Определяет, на какой странице или страницах будет отображаться штамп. Значения: `"all"`, `"last"`, `"some"`.
pageNumbers?	string	Необязательный параметр. Страница или диапазон страниц. Пример: `"3"` или `"1-7"`.

Интерфейс IMockupSettings

Интерфейс `IMockupSettings` описывает параметры внешнего вида штампа.

Свойство	Тип	Описание
position	string	Положение штампа внутри области: `"fitArea"`, `"actualSize"`, `"fitMockup"`.
addBackground	boolean	Будет ли добавлен фон на область
addBorders	boolean	Будет ли добавлена граница на область
logotype?	string/boolean	Необязательный параметр. Логотип для штампа: Base64 изображения или boolean.

Интерфейс IRequisitesSettings

Интерфейс `IRequisitesSettings` описывает содержимое (реквизиты) штампа подписи.

Свойство	Тип	Описание
position	string	Расположение реквизитов: `"default"`, `"left"`, `"right"`, `"leftAndRight"`.
centralDisplayType	string	Внешний вид: `"byGost"` (по ГОСТ), `"arbitrary"` (произвольно).
central	`IPdfCertRequisite[]`	Реквизиты центральной части
left	`IPdfCertRequisite[]`	Реквизиты левой части
right	`IPdfCertRequisite[]`	Реквизиты правой части

Интерфейс IPdfCertRequisite

Свойство	Тип	Описание
title	string	Заголовок
dataKey?	string	Необязательный параметр. Название поля сертификата, значение которого будет использовано.
isEditable	boolean	Доступно ли редактирование поля. Если `false`, значение берётся из `editedValue` или из сертификата по `dataKey`.
editedValue?	string	Необязательный параметр. Значение реквизита.
editedValueCharLimit?	number	Необязательный параметр. Максимальная длина строки.

Интерфейс IPdfAreaDimensions

Интерфейс `IPdfAreaDimensions` описывает координаты и размеры области штампа PDF.

Свойство	Тип	Описание
height	number	Высота области под штамп (мм)
width	number	Ширина области под штамп (мм)
horizontalPadding	number	

Свойство	Тип	Описание
		Отступ от левого края документа (мм)
verticalPadding	number	Отступ от нижнего края документа (мм)

Интерфейс приложения

При выполнении операции подписи по ссылке, не относящийся к процедуре интерфейс блокируется.

Пользователю доступны: выбор сертификата, часть настроек подписи (если не заблокированы через `apiLockedFields`). Параметры, переданные в `IExtra`, блокируют соответствующие поля в интерфейсе.

Кнопка «Выполнить» заменяется на «Подпись» и «Отмена». После выполнения команды, приложение будет свернуто в системный трей.

При операциях проверки подписи (`VERIFYSIGN`) окно приложения остаётся видимым после выполнения (не сворачивается в трей).

Открыть статью на сайте

Команда certificates — описание и примеры

Команда `certificates` в **API КриптоАРМ** предназначена для работы с сертификатами в локальных хранилищах.

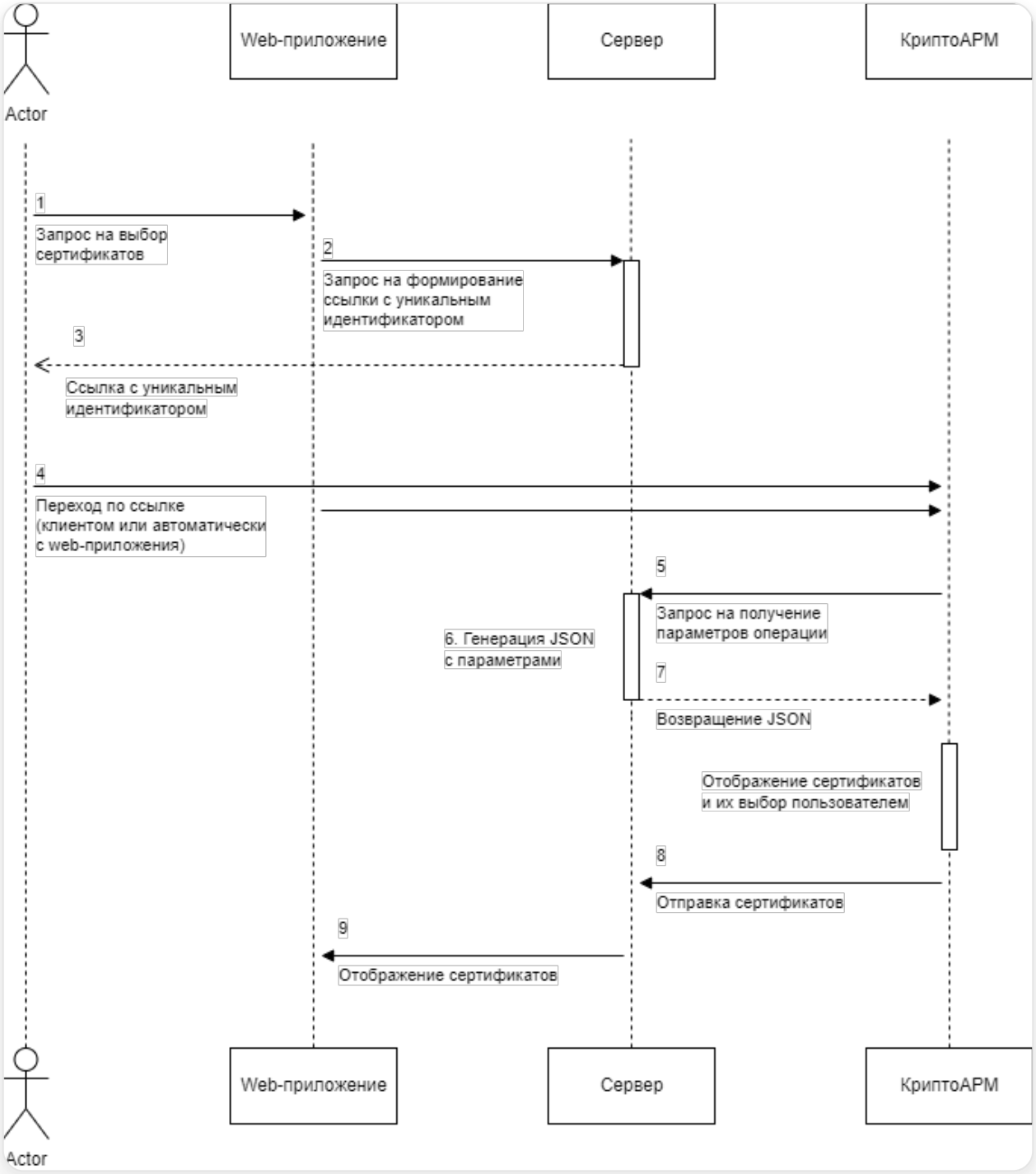
Содержание:

- Команда certificates — описание и примеры
- Общая информация
- Формат ссылки
- Получение параметров операции
  - Формат запроса
  - Формат ответа
- Импорт сертификата
  - Формат запроса результата
- Экспорт сертификатов
  - Формат запроса
- Просмотр информации о сертификате
  - Формат запроса результата
- Справочник интерфейсов
  - Интерфейс ICertificatesParameters
  - Интерфейс ICertificatesOperationProps
  - Интерфейс ICertificateBase64Params
  - Интерфейс ICertificateExportParams
  - Интерфейс ICertificateIdentityInfo
- Интерфейс приложения

Общая информация

Команда `certificates` используется для экспорта сертификата или списка сертификатов, импорта сертификата в локальное хранилище, просмотра информации о сертификате.

Схема взаимодействия (экспорт сертификатов):



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `certificates` должна быть сформирована ссылка вида:

```
cryptoarm://certificates/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `certificates` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции
- `authType` - необязательный параметр. Тип аутентификации.

Пример:

```
cryptoarm://certificates/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `certificates` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.parameters`	Используемый метод. Всегда `certificates.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.
diagnostic	`IDiagnosticsInformation`	Диагностическая информация о рабочем месте. Содержит поля `VERSIONS`, `PROVIDERS`, `LICENSES`.

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
```

```
    "method": "certificates.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
      "VERSIONS": {
        "csp": "5.0.11753",
        "cryptoarm": "2.5.2",
        "openssl": "1.1.1w"
      },
      "PROVIDERS": {
        "GOST2012_256": true,
        "GOST2012_512": true,
        "openssl": true
      },
      "LICENSES": {
        "csp": {
          "status": true,
          "type": "",
          "expiration": ""
        },
        "cryptoarm": {
          "status": true,
          "type": "Permanent",
          "expiration": ""
        }
      }
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ICertificatesParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример ответа для импорта сертификата:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "import",
        "props": {
```

```
            "store": ["MY"],
            "certificateBase64": "MIIFFDCCBMGgAwIBAgIQT...4VVkDWbX/n4="
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Пример ответа для экспорта сертификата:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "export",
        "props": {
            "store": ["MY"],
            "multy": false
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Пример ответа для просмотра информации:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "information",
        "props": {
            "certificateBase64": "MIIFFDCCBMGgAwIBAgIQT...4VVkDWbX/n4="
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Импорт сертификата

При импорте (`operation: "import"`) КриптоАРМ импортирует переданный сертификат в локальное хранилище. Если хранилище не указано, используется `MY`. После успешного импорта при наличии закрытого ключа пользователю может быть предложено выбрать хранилище.

Результат отправляется POST-запросом.

Формат запроса результата

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.import`	Используемый метод.
params	`{ id, status }`	Параметры с результатом импорта

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.import",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "status": "Completed"
    }
}
```

Экспорт сертификатов

При экспорте (`operation: "export"`) КриптоАРМ открывает окно выбора сертификата. Если `multy: true`, пользователю разрешён множественный выбор. Результат всегда передаётся в виде массива `certificates` (даже для одиночного выбора).

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».

Ключ	Значение	Описание
method	`certificates.base64`	Используемый метод.
params	`{ id, certificates: ICertificateExportParams[] }`	Массив сертификатов (один элемент — для одиночного экспорта)

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.base64",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "certificates": [{
                "certificateBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/
n4=",
                "hash": "abc123...",
                "issuerFriendlyName": "Минкомсвязь России",
                "issuerName": "CN=Минкомсвязь России",
                "subjectFriendlyName": "Минкомсвязь России",
                "subjectName": "CN=Минкомсвязь России",
                "status": true,
                "serial": "12345",
                "notAfter": "2025-01-01T00:00:00Z",
                "notBefore": "2020-01-01T00:00:00Z",
                "rootCAMinComSvyaz": true,
                "x509": "MIIFFDCCBMGgAwIBAgIQTm1..."
            },
            {
                "certificateBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/
n4=",
                "hash": "def456...",
                "issuerFriendlyName": "Головной удостоверяющий центр",
                "issuerName": "CN=ГУЦ",
                "subjectFriendlyName": "Головной удостоверяющий центр",
                "subjectName": "CN=ГУЦ",
                "status": true,
                "serial": "67890",
                "notAfter": "2030-01-01T00:00:00Z",
                "notBefore": "2019-01-01T00:00:00Z",
                "rootCAMinComSvyaz": false,
                "x509": "MIIFFDCCBMGgAwIBAgIQTm2..."
            }
        ]
    }
}
```

Просмотр информации о сертификате

При просмотре (`operation: "information"`) КриптоАРМ отображает переданный сертификат в окне информации и оповещает сервер о завершении.

Формат запроса результата

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.information`	Используемый метод.
params	`{ id, status }`	Параметры с результатом

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.information",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "status": "Completed"
    }
}
```

Справочник интерфейсов

Интерфейс ICertificatesParameters

Объекты данного типа описывают параметры команды запроса на сертификат.

Свойство	Тип	Описание
operation	string	Тип операции: `"import"`, `"export"`, `"information"`.
props	`ICertificatesOperationProps`	Параметры операции

Интерфейс ICertificatesOperationProps

Объекты данного типа описывают дополнительные свойства операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.
store?	string[]	Необязательный параметр. Массив имён хранилищ. Если не задан, используется `MY` (личные сертификаты).
multy?	boolean	Необязательный параметр. Разрешён ли множественный выбор. По умолчанию `false`.
certificateBase64?	string	Необязательный параметр. Сертификат в формате X.509, закодированный в Base64. Используется для `import` и `information`.

Интерфейс ICertificateBase64Params

Объекты данного типа описывают параметры запроса для метода `certificates.base64` при одиночном экспорте.

Свойство	Тип	Описание
id	string	Идентификатор транзакции
certificateBase64	string	Сертификат в формате X.509, закодированный в Base64
friendlyName	string	Дружественное имя сертификата

Интерфейс ICertificateExportParams

Объекты данного типа описывают сертификат в составе списка при множественном экспорте. Используется в методе `certificates.base64` с массивом `certificates`.

Свойство	Тип	Описание
certificateBase64	string	Сертификат в формате X.509, закодированный в Base64

Свойство	Тип	Описание
hash	string	SHA1-отпечаток сертификата
issuerFriendlyName	string	Дружественное имя издателя (CN)
issuerName	string	Имя издателя
notAfter	string	Дата окончания действия сертификата
notBefore	string	Дата начала действия сертификата
rootCAMinComSvyaz	boolean	Является ли владельцем корневого сертификата цепочки "Минкомсвязь России"
subjectFriendlyName	string	Дружественное имя субъекта (CN)
subjectName	string	Имя субъекта
status	boolean	Статус сертификата (проверяется вся цепочка)
serial	string	Серийный номер сертификата
x509?	string	Необязательный параметр. Сертификат в формате X.509, закодированный в Base64

Интерфейс ICertificateIdentityInfo

Объекты данного типа описывают объекты, содержащие параметры сертификата, позволяющие идентифицировать его.

Свойство	Тип	Описание
hash	string	SHA1-отпечаток сертификата
notAfter	number	Дата окончания действия сертификата (timestamp)
notBefore	number	Дата начала действия сертификата (timestamp)
isSelfSigned	boolean	Флаг самоподписанного сертификата
key	boolean	Наличие привязки к закрытому ключу

Свойство	Тип	Описание
pubKeyAlg	string	Алгоритм публичного ключа
issuerFriendlyName	string	Дружественное имя издателя (CN)
issuerName	string	Имя издателя
subjectFriendlyName	string	Дружественное имя субъекта (CN)
subjectName	string	Имя субъекта
signatureAlgorithm	string	Алгоритм подписи
signatureDigestAlgorithm	string	Алгоритм хеширования
serial	string	Серийный номер сертификата
organizationName	string	Название организации
provider	string	Тип криптопровайдера
keyUsageString	string	Использование ключа
keyNotAfter	number	Срок действия закрытого ключа (timestamp)

Интерфейс приложения

При выполнении команды запроса на сертификаты, не относящийся к процедуре интерфейс блокируется.

Пользователю доступны:

- Выбор сертификатов,
- Две кнопки: «Готово» и «Отмена».

После выполнения команды, приложение будет свернуто в системный трей.

Открыть статью на сайте

Команда certrequests — описание и примеры

Команда `certrequests` **API КриптоАРМ** предназначена для генерации и экспорта запросов на сертификаты с использованием шаблонов. Она описывает полный цикл взаимодействия приложения с сервером по протоколу JSON-RPC 2.0 — от получения параметров операции до отправки сформированного запроса в формате `Base64`.

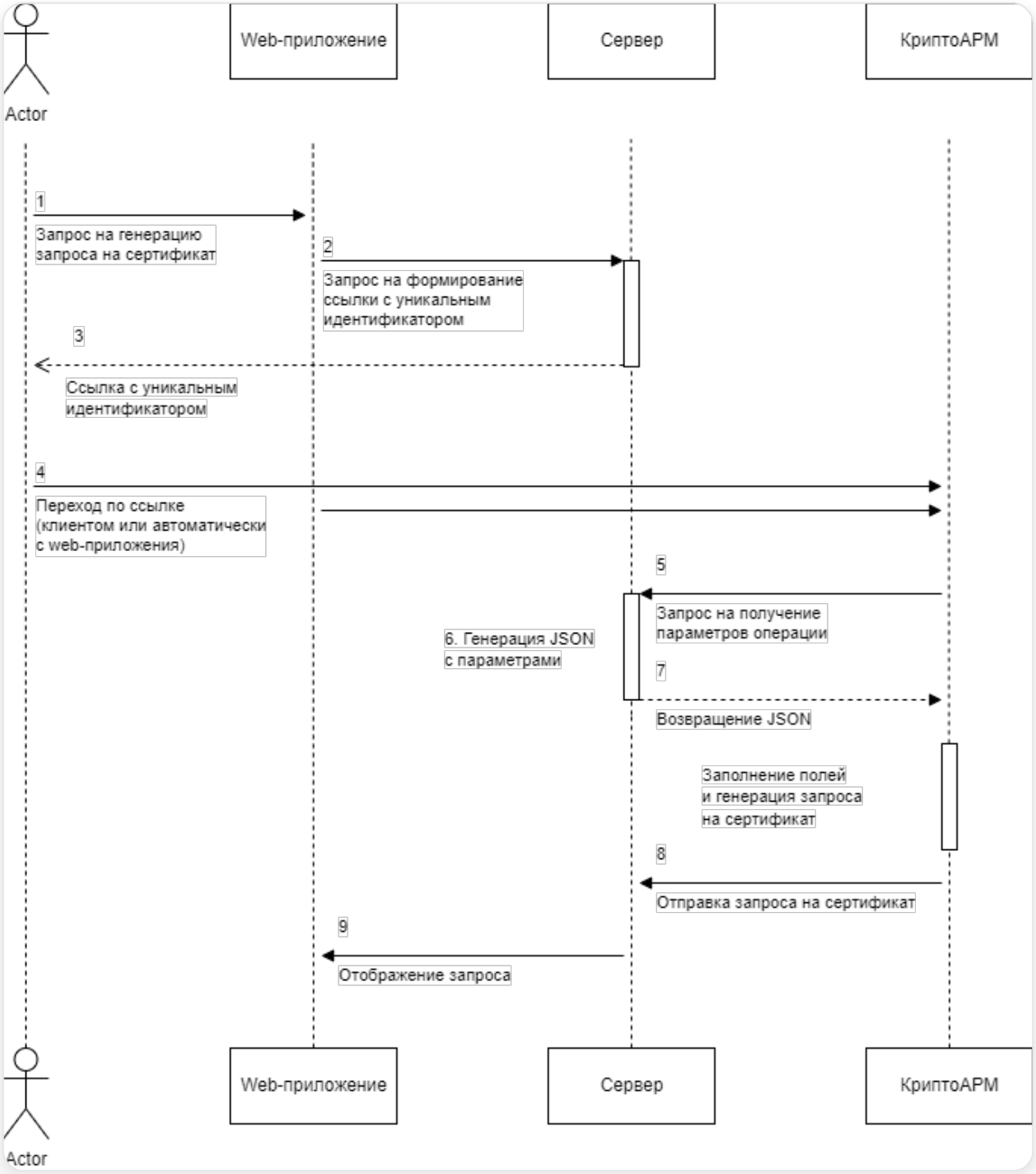
Содержание:

- Общая информация
- Формат ссылки
- Получение параметров операции
- Отправка запроса на сертификат
- Справочник интерфейсов
- Интерфейс приложения

Общая информация

Команда `certrequests` используется для генерации запроса на сертификат по шаблону.

Схема взаимодействия:



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `certrequests` должна быть сформирована ссылка вида:

```
cryptoarm://certrequests/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `certrequests` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции
- `authType` - необязательный параметр. Тип аутентификации.

Пример:

```
cryptoarm://certrequests/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `certrequests` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certrequests.parameters`	Используемый метод. Всегда `certrequests.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.
diagnostic	`IDiagnosticsInformation`	Диагностическая информация о рабочем месте. Содержит поля `VERSIONS`, `PROVIDERS`, `LICENSES`.

Пример:

```
1 Content-Type: application/json
2 Content-Length: ...
3 Accept: application/json
4 {
5     "jsonrpc": "2.0",
```

```
    "method": "certrequests.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ICertrequestsParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример ответа с шаблоном JSONTemplate:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "GENERATE",
        "props": {
            "templateType": "JSONTemplate",
            "template": {
                "Description": "",
                "FriendlyName": "Пользователь",
                "RDN": [{
                    "Oid": "2.5.4.3",
                    "Name": "CN",
                    "Length": 64,
                    "LocalizedName": "Общее имя",
                    "SettingsValues": [],
                    "DefaultValue": null,
                    "ProhibitAnyValue": false,
                    "ProhibitChange": false,
                    "ProhibitEmpty": true
                }],
                "Extensions": {
                    "KeyUsage": [{
                        "Name": "cRLSign",
                        "LocalizedName": "Автономное подписание списка отзыва
(CRL)",
                        "DefaultValue": false,
                        "ProhibitChange": true
```

```
                    }],
                    "ExtendedKeyUsage": [{
                        "Name": "1.3.6.1.5.5.7.3.1",
                        "LocalizedName": "Проверка подлинности сервера",
                        "DefaultValue": false,
                        "ProhibitChange": true
                    }]
                },
                "MarkExportable": false
            }
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Пример ответа с шаблоном CertificateTemplate (на основе сертификата):

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "jsonrpc": "2.0",
    "result": {
        "operation": "GENERATE",
        "props": {
            "templateType": "CertificateTemplate",
            "template": {
                "certificateBase64": "MIIFFDCCBMGgAwIBAgIQT...4VVkDWbX/n4="
            }
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка запроса на сертификат

После генерации запроса, он будет отправлен на сервер.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certrequests.base64`	Используемый метод.
params	`ICertificaterequestBase64Params`	Параметры, содержащие запрос

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certrequests.base64",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "certificaterequestBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/
n4=",
        "friendlyName": "ООО Рога и Копыта"
    }
}
```

Справочник интерфейсов

Интерфейс ICertrequestsParameters

Объекты данного типа описывают параметры команды.

Свойство	Тип	Описание
operation	string	Тип операции. Единственное поддерживаемое значение: `GENERATE`.
props	`ICertrequestsOperationGenerateProps`	Параметры операции

Интерфейс ICertrequestsOperationGenerateProps

Объекты данного типа описывают дополнительные свойства операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина: 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина: 120 символов.
templateType	string	

Свойство	Тип	Описание
		Тип шаблона: `"JSONTemplate"` (JSON-описание) или `"CertificateTemplate"` (на основе существующего сертификата).
template	`IJSONTemplate` или `ICertificateTemplate`	Шаблон для генерации запроса на сертификат.

Интерфейс IJSONTemplate

Объекты данного типа описывают поля для генерации запроса на сертификат.

Свойство	Тип	Описание
Description	string	Описание шаблона
FriendlyName	string	Дружественное имя шаблона
RDN	`IRDN[]`	Набор полей DN (Distinguished Name)
Extensions	`IRequestExtension`	Расширения сертификата
MarkExportable	boolean	Определяет экспортируемость ключей

Интерфейс IRDN

Свойство	Тип	Описание
Oid	string	OID поля
Name	string	Наименование OID
Length	number	Максимальная длина поля
LocalizedName	string	Локализованное наименование OID
SettingsValues	string[]	Список возможных значений
DefaultValue	string	Значение по умолчанию
ProhibitAnyValue	boolean	Флаг, указывающий, что пользователю доступны только значения из `SettingsValues`
ProhibitChange	boolean	Флаг, указывающий, что поле не может быть изменено
ProhibitEmpty	boolean	

Свойство	Тип	Описание
		Флаг, указывающий, что поле должно быть непустым

Интерфейс IRequestExtension

Свойство	Тип	Описание
KeyUsage	`IKeyUsage[]`	Использование ключа
ExtendedKeyUsage	`IExtendedKeyUsage[]`	Расширенное использование ключа

Интерфейс IKeyUsage

Свойство	Тип	Описание
Name	string	Наименование OID (например, `"digitalSignature"`)
LocalizedName	string	Локализованное наименование OID
DefaultValue	boolean	Значение по умолчанию
ProhibitChange	boolean	Флаг, указывающий, что поле не может быть изменено

Интерфейс IExtendedKeyUsage

Свойство	Тип	Описание
Name	string	Наименование OID (например, `"1.3.6.1.5.5.7.3.1"`)
LocalizedName	string	Локализованное наименование OID
DefaultValue	boolean	Значение по умолчанию
ProhibitChange	boolean	Флаг, указывающий, что поле не может быть изменено

Интерфейс ICertificateTemplate

Объекты данного типа используются для генерации запроса на сертификат, где запрос формируется по существующему сертификату.

Свойство	Тип	Описание
certificateBase64	string	Сертификат в формате X.509, закодированный в Base64

Интерфейс ICertificaterequestBase64Params

Свойство	Тип	Описание
id	string	Идентификатор транзакции
certificaterequestBase64	string	Запрос в формате X.509, закодированный в Base64
friendlyName	string	Дружественное имя субъекта

Интерфейс приложения

При выполнении команды запроса на сертификат, не относящийся к процедуре интерфейс блокируется.

Пользователю доступны:

- Заполнение полей запроса,
- Кнопки «Готово» и «Отмена».

После выполнения команды, приложение будет свернуто в системный трей.

Открыть статью на сайте

Команда diagnostics — описание и примеры

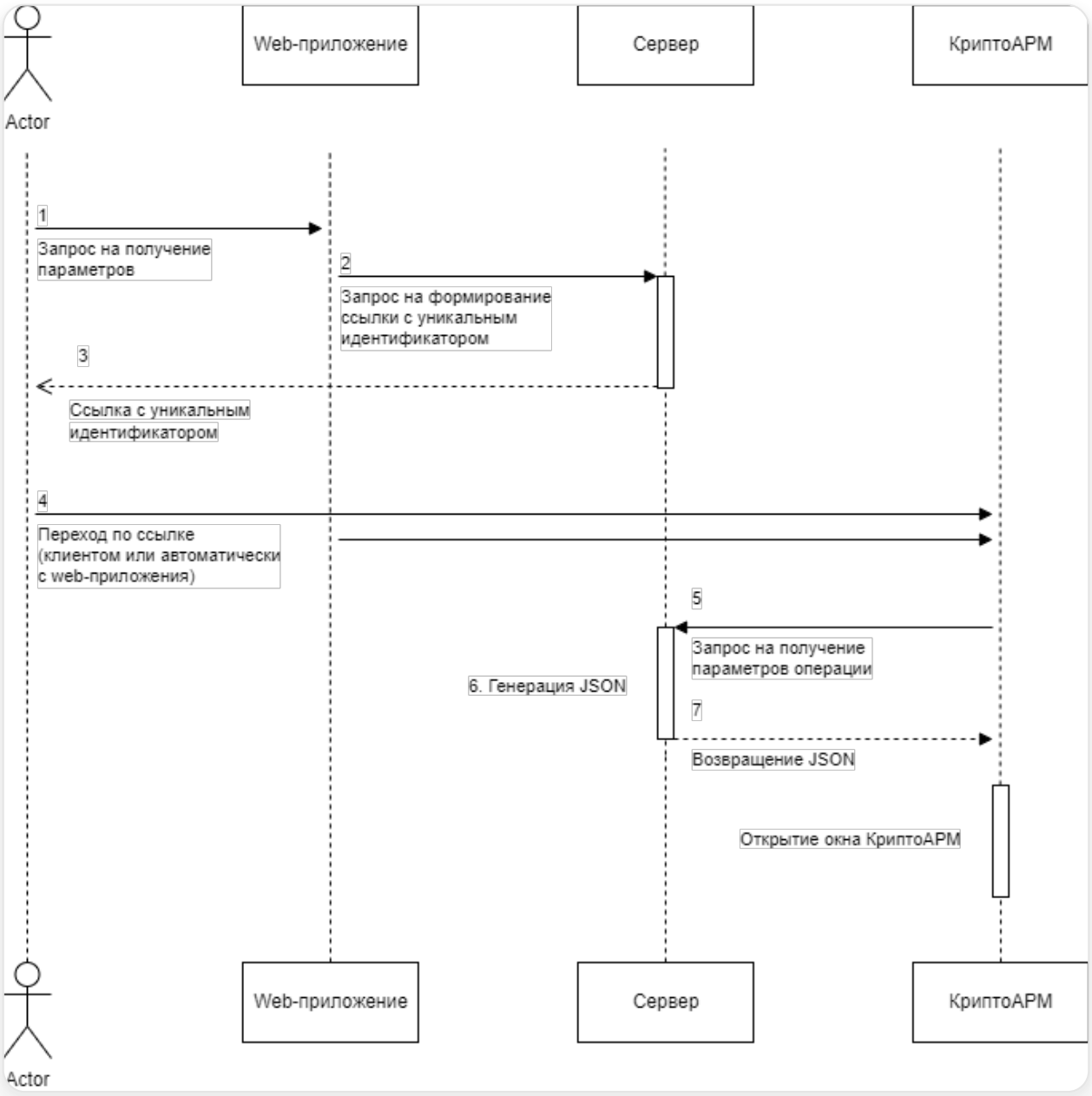
Команда `diagnostics` позволяет выполнять полную диагностику рабочего места пользователя через API КриптоАРМ. С её помощью можно получить сведения о системе, установленных компонентах и лицензиях. Все операции поддерживаются через HTTP и строго соответствуют спецификации JSON-RPC 2.0.

Содержание:

- Общая информация
- Формат ссылки
- Получение параметров операции
- Отправка сведений о рабочем месте
- Справочник интерфейсов

Общая информация

Команда `diagnostics` используется для диагностики рабочего места пользователя.



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.
>
> Для доверенных сервисов с включённым фоновым режимом диагностики (`diagnosticBackgroundMode`) окно подтверждения не отображается; диагностика выполняется автоматически.

Формат ссылки

Для выполнения команды `diagnostics` должна быть сформирована ссылка вида:

```
cryptoarm://diagnostics/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `diagnostics` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции
- `authType` - необязательный параметр. Тип аутентификации.

Пример:

```
cryptoarm://diagnostics/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `diagnostics` КриптоАРМ отправляет запрос на получение параметров операции.

> Удалённый запрос содержит поле `diagnostic` (пустой объект), а не `diagnostics` (как в других командах).

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`diagnostics.parameters`	Используемый метод. Всегда `diagnostics.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.
diagnostic	`{}`	Пустой объект (зарезервировано).

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "diagnostics.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
     }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IDiagnosticsParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример ответа с локальными параметрами:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "operation": ["SYSTEMINFORMATION", "CSP_ENABLED", "LICENSES", "VERSIONS", "P
ROVIDERS"],
        "props": {
            "headerText": "Диагностика cryptoarm.ru",
            "descriptionText":
"Выполняется диагностика рабочего места для работы на портале"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка сведений о рабочем месте

Полученные сведения отправляются POST-запросом.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`diagnostics.information`	Используемый метод.
params	`IDiagnosticsInformation`	Сведения о рабочем месте. `id` — идентификатор транзакции из исходного запроса.

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
  "jsonrpc": "2.0",
  "method": "diagnostics.information",
  "params": {
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "SYSTEMINFORMATION": {
      "type": "Windows_NT",
      "arch": "x64",
      "platform": "win32",
      "packageType": "msi"
    },
    "CSP_ENABLED": true,
    "LICENSES": {
      "csp": {
        "status": true,
        "type": "",
        "expiration": ""
      },
      "cryptoarm": {
        "status": true,
        "type": "Permanent",
        "expiration": ""
      }
    },
    "VERSIONS": {
      "csp": "5.0.11753",
      "cryptoarm": "2.5.2",
      "openssl": "1.1.1w"
    },
    "PROVIDERS": {
      "GOST2012_256": true,
      "GOST2012_512": true,
      "openssl": true
```

```
    }
  }
}
```

Справочник интерфейсов

Интерфейс IDiagnosticsParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string[]	Массив типов диагностических операций. Доступные значения см. Тип IDiagnosticOperation.
props	`IDiagnosticsOperationProps`	Параметры операции

Тип IDiagnosticOperation

Возможные операции диагностики.

Значение	Описание
SYSTEMINFORMATION	Сведения о системе
CSP_ENABLED	Наличие КриптоПро CSP
CADES_ENABLED	Доступность CADES
VERSIONS	Версии используемых компонентов (КриптоАРМ, КриптоПро, OpenSSL)
PROVIDERS	Список криптопровайдеров
LICENSES	Статус лицензий
PERSONALCERTIFICATES	Наличие личных сертификатов

Интерфейс IDiagnosticsOperationProps

Интерфейс `IDiagnosticsOperationProps` описывает параметры операции.

Свойство	Тип	Описание
headerText?	string	

Свойство	Тип	Описание
		Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.
localResultParams?	`{ savePath: string }`	Необязательный параметр. Только для локального API. Путь к файлу для сохранения результатов диагностики.

Интерфейс IDiagnosticsInformation

Объекты данного типа описывают сведения о рабочем месте, отправляемые обратно на сервер.

Свойство	Тип	Описание
id	string	Идентификатор транзакции
SYSTEMINFORMATION	`ISystemInformation`	Сведения о системе
CSP_ENABLED	boolean	Установлен или нет КриптоПро CSP
CADES_ENABLED	boolean	Доступность CADES
VERSIONS	`IVersions`	Версии компонентов
PROVIDERS	`IProviders`	Сведения о провайдерах
LICENSES	`ILicenses`	Сведения о лицензиях
PERSONALCERTIFICATES	`ICertificateIdentityInfo[]`	Список личных сертификатов

Интерфейс ISystemInformation

Объекты данного типа содержат сведения о системе пользователя.

Свойство	Тип	Описание
type	string	Тип системы. Возможные значения: `Linux`, `Darwin`, `Windows_NT`.

Свойство	Тип	Описание
arch	string	Архитектура операционной системы. Возможные значения: `arm`, `arm64`, `ia32`, `mips`, `mipsel`, `ppc`, `ppc64`, `s390`, `s390x`, `x32`, `x64`.
platform	string	Имя платформы. Возможные значения: `aix`, `darwin`, `freebsd`, `linux`, `openbsd`, `sunos`, `win32`.
packageType?	string	Необязательный параметр. Тип поддерживаемого пакета (инсталлятора). Возможные значения: `msi`, `pkg`, `rpm`, `deb`.

Интерфейс IVersions

Объекты данного типа содержат сведения о версиях.

Свойство	Тип	Описание
csp	string	Версия КриптоПро CSP
cryptoarm	string	Версия КриптоАРМ
openssl	string	Версия OpenSSL

Интерфейс IProviders

Объекты данного типа описывают доступность ГОСТ-провайдеров.

Свойство	Тип	Описание
GOST2012_256	boolean	ГОСТ 2012-256
GOST2012_512	boolean	ГОСТ 2012-512
openssl	boolean	Открытая криптография

Интерфейс ILicenses

Объекты данного типа описывают статусы лицензии КриптоАРМ и КриптоПро CSP.

Свойство	Тип	Описание
csp	`ILicenseInfo`	Сведения о лицензии на КриптоПро CSP
cryptoarm	`ILicenseInfo`	Сведения о лицензии на КриптоАРМ

Интерфейс ILicenseInfo

Объекты данного типа описывают сведения о лицензии компонента.

Свойство	Тип	Описание
status	boolean	Действительна или нет лицензия
type	string	Тип лицензии. Возможные значения: `Permanent`, `Subscription`, `Daily`, `Trial`.
expiration?	string	Необязательный параметр. Дата истечения лицензии для триальных лицензий или подписок (UTC).

Открыть статью на сайте

Команда startView — описание и примеры

Команда `startView` открывает выбранное окно приложения КриптоАРМ и передает ему необходимые параметры.

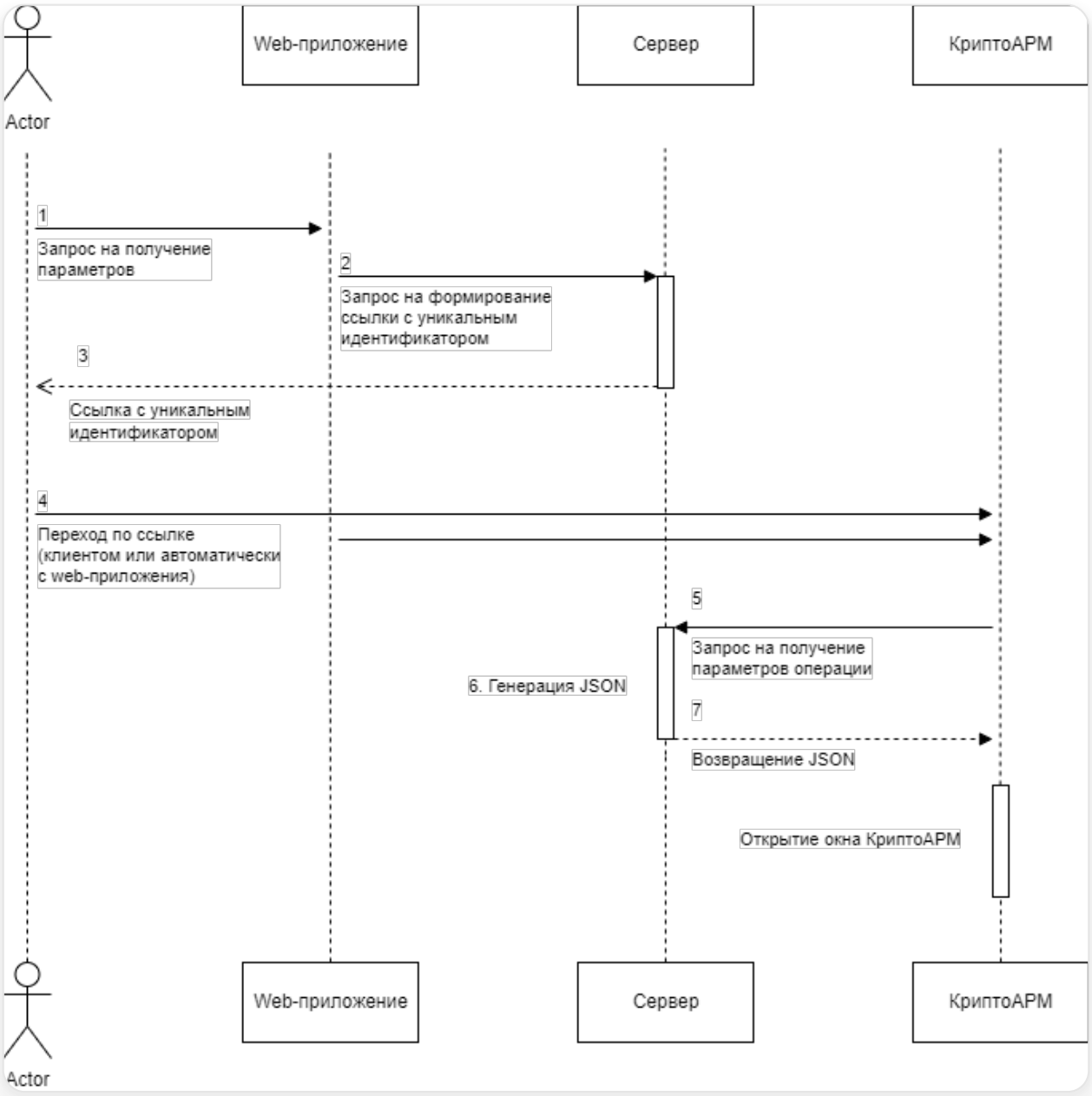
Содержание:

- Команда startView — описание и примеры
- Общая информация
- Формат ссылки
- Получение параметров операции
  - Формат запроса
  - Формат ответа
- Справочник интерфейсов
  - Интерфейс IStartViewParameters
  - Интерфейс IStartViewOperationProps

Общая информация

Команда `startView` используется для открытия конкретного окна приложения КриптоАРМ.

Схема взаимодействия:



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `startView` должна быть сформирована ссылка вида:

```
cryptoarm://startView/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `startView` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `id` - уникальный идентификатор транзакции
- `authType` - необязательный параметр. Тип аутентификации.

Пример:

```
cryptoarm://startView/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `startView` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`startView.parameters`	Используемый метод. Всегда `startView.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.
diagnostic	`IDiagnosticsInformation`	Диагностическая информация о рабочем месте. Содержит поля `VERSIONS`, `PROVIDERS`, `LICENSES`.

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "startView.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
      "VERSIONS": {
        "csp": "5.0.11753",
```

```
        "cryptoarm": "2.5.2",
        "openssl": "1.1.1w"
      },
      "PROVIDERS": {
        "GOST2012_256": true,
        "GOST2012_512": true,
        "openssl": true
      },
      "LICENSES": {
        "csp": { "status": true, "type": "", "expiration": "" },
        "cryptoarm": { "status": true, "type": "Permanent", "expiration": "" }
      }
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IStartViewParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "uiView": "CERTIFICATES_MY",
        "props": {
            "headerText": "ИС cryptoarm.ru",
            "descriptionText": "Запрос на открытие окна"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Справочник интерфейсов

Интерфейс IStartViewParameters

Объекты данного типа описывают вид операции и её параметры.

Ключ	Значение	Описание
uiView	string	Тип окна, которое нужно отобразить пользователю. Доступные значения: `MAIL` — окно почты, `DOCUMENTS` — окно Документы, `SIGN_AND_ENCRYPT` — окно подписи и шифрования, `VERIFY_AND_DECRYPT` — окно проверки и расшифрования, `CERTIFICATES_MY` — Сертификаты / Личные, `CERTIFICATES_ADDRESS_BOOK` — Сертификаты / Другие пользователи, `CERTIFICATES_CA` — Сертификаты / Промежуточные, `CERTIFICATES_ROOT` — Сертификаты / Корневые, `CONTACTS` — окно Контакты, `KEYS` — Сертификаты / Ключевые контейнеры, `ABOUT` и `DIAGNOSTICS` — окно Настройки (О программе), `DIAGNOSTIC_PROBLEM_PERSONAL_CERTIFICATES` — диагностика проблем личных сертификатов (в разработке).
props	`IStartViewOperationProps`	Параметры операции

Интерфейс IStartViewOperationProps

Интерфейс `IStartViewOperationProps` описывает параметры операции.

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.

Открыть статью на сайте

Команда sendMail — описание и примеры

Команда `sendMail` позволяет создать новое электронное письмо (черновик) в КриптоАРМ с переданными параметрами: получатели, тема, содержимое, вложения, флаги подписи и шифрования.

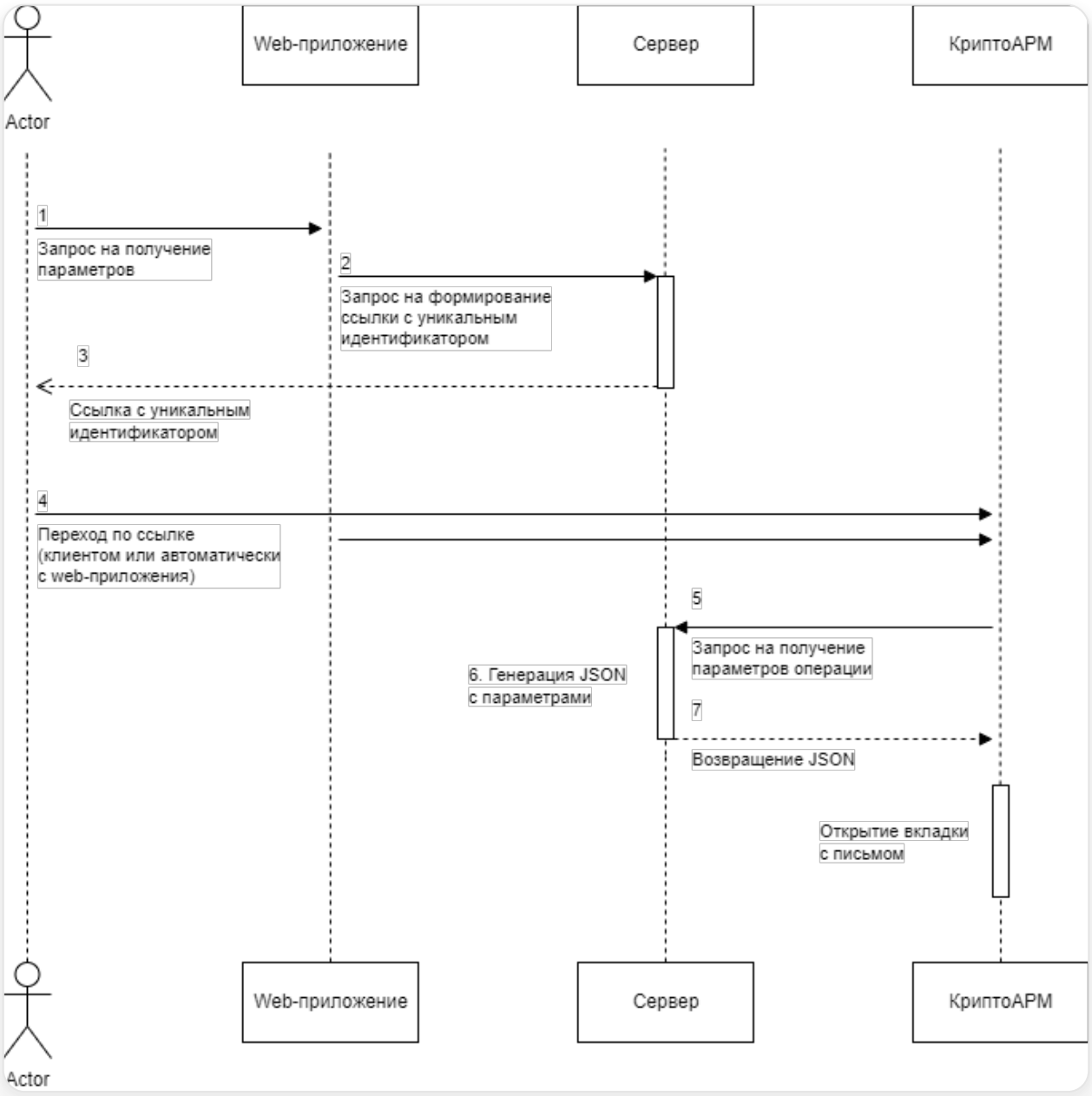
Содержание:

- Команда sendMail — описание и примеры
- Общая информация
- Формат ссылки
- Получение параметров операции
  - Формат запроса (удалённый режим)
  - Формат ответа
- Отправка статуса
  - Формат запроса статуса
- Справочник интерфейсов
  - Интерфейс IMailProps
  - Параметры лицензии и подписи
- Интерфейс приложения

Общая информация

Команда `sendMail` используется для создания нового черновика электронного письма в КриптоАРМ с переданными параметрами. После заполнения и отправки письма пользователем, КриптоАРМ уведомляет сервер о статусе операции.

Схема взаимодействия:



Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `sendMail` должна быть сформирована ссылка вида:

```
cryptoarm://sendMail/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `sendMail` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции
- `authType` - необязательный параметр. Тип аутентификации.

Пример:

```
cryptoarm://sendMail/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

> **Локальный режим**: При использовании через локальное API (`file://` или встроенный JSON), `paramsJson` должен содержать непосредственно объект `IMailOperationProps` (см. ниже).

Получение параметров операции

После получения команды `sendMail` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса (удалённый режим)

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`sendMail.parameters`	Используемый метод. Всегда `sendMail.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.
diagnostic	`IDiagnosticsInformation`	Диагностическая информация о рабочем месте. Содержит поля `VERSIONS`, `PROVIDERS`, `LICENSES`.

Пример:

```
1 Content-Type: application/json
2 Content-Length: ...
3 Accept: application/json
```

```
{
    "jsonrpc": "2.0",
    "method": "sendMail.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
      "VERSIONS": { "csp": "5.0.11753", "cryptoarm": "2.5.2", "openssl": "1.1.1w" },
      "PROVIDERS": { "GOST2012_256": true, "GOST2012_512": true, "openssl": true },
      "LICENSES": {
        "csp": { "status": true, "type": "", "expiration": "" },
        "cryptoarm": { "status": true, "type": "Permanent", "expiration": "" }
      }
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`{ props: { mailProps: IMailProps } }`	Объект со свойствами письма
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример ответа:

```
HTTP/1.1 200 OK
Connection: close
Content-Length: ...
Content-Type: application/json
Date: Sat, 08 Jul 2020 12:04:08 GMT
{
    "jsonrpc": "2.0",
    "result": {
        "props": {
            "mailProps": {
               "to": ["test@example.com"],
               "cc": ["test1@example.com", "test2@example.com"],
               "bcc": ["test3@example.com"],
               "subject": "Message subject",
               "content": "text message content",
               "htmlContent": "<div>HTML message content</div>",
               "attachments": [
                   {
                       "name": "file1.txt",
                       "url": "http://localhost:8080/public/files/file1.txt",
                       "id": "1",
                       "urlDetached": ""
                   },
                   {
```

```
                        "name": "file2.txt",
                        "url": "http://localhost:8080/public/files/file2.txt",
                        "id": "2",
                        "urlDetached": ""
                    }
                ],
                "sign": false,
                "encrypt": false,
                "deliveryReport": false,
                "readReport": false
            }
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка статуса

После того как пользователь отправит письмо или закроет окно, КриптоАРМ отправляет статус операции на сервер.

Формат запроса статуса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`sendMail.status`	Используемый метод.
params	`{ id, status }`	Параметры статуса

Параметр	Тип	Описание
id	string	Идентификатор транзакции
status	string	Статус: `"success"` (письмо отправлено) или `"canceled"` (отменено)

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "sendMail.status",
    "params": {
```

```
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "status": "success"
    }
}
```

Справочник интерфейсов

Интерфейс IMailProps

Объекты данного типа описывают параметры электронного сообщения.

Свойство	Тип	Описание
to	string[]	Массив адресов получателей
cc?	string[]	Массив адресов получателей копии
bcc?	string[]	Массив адресов получателей скрытой копии
subject	string	Тема сообщения
content	string	Текстовое содержимое сообщения
htmlContent?	string	Форматированное содержимое сообщения в формате HTML
attachments?	`IFile[]`	Файлы для прикрепления к сообщению (вложения). Скачиваются КриптоАРМ перед открытием окна письма.
sign	boolean	Флаг, указывающий на необходимость подписать сообщение
encrypt	boolean	Флаг, указывающий на необходимость зашифровать сообщение
deliveryReport	boolean	Флаг, включающий получение отчета о доставке
readReport	boolean	Флаг, включающий получение отчета о прочтении

Параметры лицензии и подписи

Свойство	Тип	Описание
license?	string	Необязательный параметр. Временная лицензия для выполнения операции (добавляется на время сессии).

Интерфейс приложения

При выполнении команды `sendMail` открывается окно создания нового сообщения с предзаполненными полями: получатели, тема, содержимое, вложения. Если передан флаг `sign`, включается подпись сообщения. Если передан флаг `encrypt`, включается шифрование.

Пользователь может отредактировать письмо, выбрать сертификаты для подписи/шифрования и отправить его или отменить операцию. После закрытия окна КриптоАРМ отправляет статус (`success` или `canceled`) на сервер.

Открыть статью на сайте

Команда saveDocuments — описание и примеры

Команда `saveDocuments` предназначена для импорта документов в локальное хранилище КриптоАРМ с внешнего сервера или из локального файла.

Содержание:

- Общая информация
- Формат ссылки
- Получение параметров операции
- Отправка результатов
- Справочник интерфейсов
- Интерфейс приложения

Общая информация

Команда `saveDocuments` используется для скачивания и сохранения файлов в директорию документов КриптоАРМ. Поддерживается только операция `IMPORT`.

Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

В качестве транспорта используется HTTP.

> 🔍 Общее описание указано в разделе Формат ссылки.

Формат ссылки

Для выполнения команды `saveDocuments` должна быть сформирована ссылка вида:

```
cryptoarm://saveDocuments/<URL>/?id=<id>[&authType=<authType>]
```

- `cryptoarm://` - зарегистрированный протокол
- `saveDocuments` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции
- `authType` - необязательный параметр. Тип аутентификации.

Пример:

```
cryptoarm://saveDocuments/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров операции

После получения команды `saveDocuments` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.parameters`	Используемый метод. **Внимание**: в текущей реализации используется `signAndEncrypt.parameters`, а не `saveDocuments.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.
diagnostic	`IDiagnosticsInformation`	Диагностическая информация о рабочем месте. Содержит поля `VERSIONS`, `PROVIDERS`, `LICENSES`.

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
      "VERSIONS": { "csp": "5.0.11753", "cryptoarm": "2.5.2", "openssl": "1.1.1w" },
      "PROVIDERS": { "GOST2012_256": true, "GOST2012_512": true, "openssl": true },
      "LICENSES": {
        "csp": { "status": true, "type": "", "expiration": "" },
        "cryptoarm": { "status": true, "type": "Permanent", "expiration": "" }
      }
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IDocumentsParameters`	Объект со сведениями о параметрах операции
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример ответа:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "jsonrpc": "2.0",
    "result": {
        "operation": ["IMPORT"],
        "props": {
            "headerText": "Импорт документов",
            "files": [
                {
                    "name": "document1.pdf",
                    "url": "https://example.com/files/document1.pdf",
                    "id": "1"
                },
                {
                    "name": "document2.doc",
                    "url": "https://example.com/files/document2.doc",
                    "id": "2"
                }
            ]
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Отправка результатов

После импорта КриптоАРМ отправляет результаты операции на сервер.

Формат запроса результата

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`documents.parameters`	Используемый метод.
params	`{ id, documentsResults }`	Результаты импорта

Поле documentsResults

Массив объектов с результатами импорта по каждому файлу:

Свойство	Тип	Описание
name	string	Имя файла
id	string	Идентификатор файла (из исходного запроса)
result	boolean	Успешность сохранения (`true` — успешно)

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "documents.parameters",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "documentsResults": [
            { "name": "document1.pdf", "id": "1", "result": true },
            { "name": "document2.doc", "id": "2", "result": true }
        ]
    }
}
```

Справочник интерфейсов

Интерфейс IDocumentsParameters

Объекты данного типа описывают параметры команды импорта документов.

Свойство	Тип	Описание
operation	string[]	Массив операций. Единственное поддерживаемое значение: `["IMPORT"]`.
props	`IDocumentsOperationProps`	Параметры операции

Интерфейс IDocumentsOperationProps

Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
files	`IFile[]`	Массив файлов для импорта. Каждый файл скачивается по URL и сохраняется в директорию документов КриптоАРМ.
license?	string	Необязательная временная лицензия на время операции.

Интерфейс приложения

При выполнении команды `saveDocuments` КриптоАРМ скачивает указанные файлы и сохраняет их в хранилище документов. После завершения окно приложения не сворачивается в трей — обновляется список документов.

Открыть статью на сайте

Команда authorize — описание и примеры

Команда `authorize` реализует авторизацию пользователя через протокол OpenID Connect (OIDC) с поддержкой PKCE. Может вызываться как самостоятельная команда или автоматически при наличии `authType=oidc` в других командах.

Содержание:

- Общая информация
- Формат ссылки
- Получение параметров авторизации
- Процесс авторизации
- Callback (обратный вызов)
- Справочник интерфейсов
- Интерфейс приложения

Общая информация

Команда `authorize` выполняет аутентификацию пользователя через OIDC-провайдер:

1. Запрашивает параметры авторизации с сервера (или получает их из локального JSON).
2. Строит URL авторизации с PKCE (Proof Key for Code Exchange).
3. Открывает браузер пользователя для входа на стороне провайдера.
4. Получает код авторизации через `callback` и обменивает его на токены доступа.
5. Сохраняет токены в доверенном сервисе и использует для последующих запросов.

Поддерживается также безвзаимодейственная (silent) авторизация с использованием клиентского сертификата (mTLS), если `prompt=none`.

Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

Формат ссылки

```
cryptoarm://authorize/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `authorize` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами авторизации

- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://authorize/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров авторизации

После получения команды `authorize` КриптоАРМ запрашивает параметры авторизации с сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`authorization.parameters`	Используемый метод. Всегда `authorization.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "authorization.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
params	`{ authorizationParams: IAuthorizationParams }`	Параметры авторизации

Ключ	Значение	Описание
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "jsonrpc": "2.0",
    "params": {
        "authorizationParams": {
            "clientId": "my-client-id",
            "issuer": "https://auth.example.com",
            "redirectUri": "http://localhost:3000/callback",
            "scope": "openid profile",
            "wellKnownUrl": "https://auth.example.com/.well-known/openid-
configuration",
            "resource": "https://api.example.com",
            "responseTypes": "code",
            "prompt": "login"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Процесс авторизации

После получения параметров авторизации:

1. КриптоАРМ отображает диалог авторизации с информацией о сервисе.
2. Если пользователь подтверждает (`prompt != "none"`):
    - Генерируется code_verifier и code_challenge (PKCE).
    - Строится URL авторизации провайдера.
    - Открывается браузер пользователя.
    - Пользователь проходит аутентификацию на стороне провайдера.
    - После успешного входа провайдер перенаправляет на `redirectUri` с параметрами `code` и `state`.
    - Этот редирект должен быть перехвачен и передан КриптоАРМ через команду `callback`.
3. Если `prompt="none"` (безвзаимодейственная авторизация):
    - Используется клиентский сертификат (mTLS) для получения кода авторизации напрямую.

- Код обменивается на токены через token endpoint.

После успешной авторизации:

- Токены (`access_token`, `id_token`, `refresh_token`) сохраняются в доверенном сервисе.
- Профиль пользователя извлекается из `id_token` или через `userinfo endpoint`.
- Отображается диалог успешной авторизации с именем пользователя.

Callback (обратный вызов)

Команда `callback` используется для обработки редиректа от OIDC-провайдера после успешной аутентификации. Обычно вызывается автоматически операционной системой при переходе по зарегистрированному протоколу `cryptoarm://`.

Формат ссылки

```
cryptoarm://callback/<redirected_url>?id=<id>&authType=<authType>
```

Параметры `state`, `code`, `session_state` и другие передаются в query-строке редиректа от провайдера и извлекаются КриптоАРМ автоматически.

КриптоАРМ обменивает полученный код авторизации на токены, извлекает профиль пользователя и сохраняет всё в доверенном сервисе.

> **Важно**: Команда `callback` является внутренней и не предназначена для прямого вызова. Она автоматически обрабатывается КриптоАРМ при получении редиректа от OIDC-провайдера.

Справочник интерфейсов

Интерфейс IAuthorizationParams

Параметры, необходимые для OIDC-авторизации.

Свойство	Тип	Описание
clientId	string	Идентификатор клиента, зарегистрированный у OIDC-провайдера
issuer	string	URL издателя токенов (Issuer)
redirectUri	string	

Свойство	Тип	Описание
		URI для редиректа после авторизации
scope	string	Запрашиваемые области (scopes), например `"openid profile"`
wellKnownUrl?	string	URL well-known конфигурации OIDC (если отличается от стандартного `.well-known/openid-configuration`)
resource?	string/string[]	Идентификатор ресурса, к которому запрашивается доступ
responseTypes?	string/string[]	Типы ответа (response_type). По умолчанию `"code"`.
prompt?	string	Параметр prompt. `"login"` — интерактивная авторизация, `"none"` — безвзаимодейственная (silent).
override?	`{ issuer: { authorization_endpoint, token_endpoint, ... } }`	Переопределение метаданных издателя (если well-known недоступен).

Интерфейс ICustomAuth (настройки передачи токена)

После успешной OIDC-авторизации токен доступа может передаваться в последующих запросах. Настройки `customAuth` определяют способ передачи:

Свойство	Тип	Описание
token?	string	Токен доступа (заполняется автоматически)
in?	string	Способ передачи: `"header"` (заголовок), `"query"` (параметр), `"body"` (тело). По умолчанию: `"header"`.
key?	string	Имя ключа/заголовка. По умолчанию: `"Authorization"` для header, `"token"` для query/body.
scheme?	string	Схема авторизации. По умолчанию: `"Bearer"`.
thumbprint?	string	Отпечаток клиентского сертификата для mTLS.

Интерфейс приложения

Процесс авторизации состоит из нескольких этапов:

1. **Диалог подтверждения** — отображается информация о запрашиваемом сервисе. Кнопки: «Продолжить» и «Отмена».
2. **Авторизация в браузере** — открывается системный браузер со страницей входа провайдера.
3. **Ожидание редиректа** — КриптоАРМ ожидает `callback` с кодом авторизации.
4. **Успешная авторизация** — отображается имя авторизованного пользователя. Кнопка «Готово».

При отмене на любом этапе процесс прерывается.

Открыть статью на сайте

Команда mtlsAuthorization — описание и примеры

Команда `mtlsAuthorization` реализует авторизацию пользователя через взаимный TLS (mTLS) с использованием клиентского сертификата. Может вызываться как самостоятельная команда или автоматически при наличии `authType=mtls` в других командах.

Содержание:

- Общая информация
- Формат ссылки
- Получение параметров авторизации
- Процесс авторизации
- Справочник интерфейсов
- Интерфейс приложения

Общая информация

Команда `mtlsAuthorization` выполняет запрос к указанному URL с использованием клиентского сертификата (взаимный TLS). Это позволяет серверу аутентифицировать пользователя КриптоАРМ по его личному сертификату.

Основные этапы:

1. Запрашивает параметры с сервера (URL, HTTP-метод, описание, тело запроса).
2. Отображает диалог выбора сертификата пользователем.
3. Выполняет GET или POST запрос к указанному URL с клиентским сертификатом.
4. Отображает результат (успех/неудача).

Все запросы между КриптоАРМ и сервером ДОЛЖНЫ соответствовать спецификации протокола JSON-RPC 2.0.

Формат ссылки

```
cryptoarm://mtlsAuthorization/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `mtlsAuthorization` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами авторизации
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://mtlsAuthorization/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Получение параметров авторизации

После получения команды `mtlsAuthorization` КриптоАРМ запрашивает параметры авторизации с сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`authorization.parameters`	Используемый метод. Всегда `authorization.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "authorization.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
params	`IMTLSAuthorizationParams`	Параметры mTLS-авторизации
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию.

Пример:

```
HTTP/1.1 200 OK
Content-Type: application/json
{
    "jsonrpc": "2.0",
    "params": {
        "url": "https://api.example.com/auth/mtls",
        "method": "POST",
        "description": "Авторизация на портале Example",
        "body": {
            "clientId": "my-client",
            "timestamp": "2026-01-01T00:00:00Z"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Процесс авторизации

После получения параметров:

1. КриптоАРМ проверяет, что указан валидный `url` и HTTP-метод (`GET` или `POST`).
2. Отображается диалог с информацией о сервисе и выбором сертификата.
3. Пользователь выбирает личный сертификат (из хранилища `MY`) и подтверждает операцию.
4. КриптоАРМ выполняет HTTP-запрос к указанному URL:
    - **GET**: без тела, с клиентским сертификатом в TLS handshake.
    - **POST**: с телом `body` (сериализуется в JSON), с клиентским сертификатом.
5. Результат отображается пользователю: «Успешно» или «Ошибка».

Пользователь может отменить операцию на любом этапе.

Справочник интерфейсов

Интерфейс IMTLSAuthorizationParams

Параметры, необходимые для mTLS-авторизации.

Свойство	Тип	Описание
url	string	

Свойство	Тип	Описание
		URL, на который будет выполнен запрос с клиентским сертификатом. **Обязательный параметр.**
method	string	HTTP-метод: `"GET"` или `"POST"`. По умолчанию `"GET"`.
description	string	Описание операции, отображаемое в диалоге выбора сертификата.
body	object	Тело запроса (для `POST`). Сериализуется в JSON.

Интерфейс приложения

Процесс mTLS-авторизации состоит из трёх этапов:

1. **Выбор сертификата** — отображается диалог с описанием операции. Пользователь выбирает личный сертификат (из хранилища `MY`). Кнопки: «Продолжить» и «Отмена». Также может быть отображён рекомендуемый сертификат, сохранённый в доверенном сервисе.
2. **Выполнение запроса** — отображается индикатор загрузки. КриптоАРМ выполняет HTTP-запрос к серверу с использованием выбранного клиентского сертификата. Пользователь может отменить операцию.
3. **Результат** — отображается результат операции: «Успешно» или «Ошибка» (с описанием). Кнопка «Готово».

При отмене на любом этапе процесс прерывается, окно закрывается.