Цифровые технологии

КриптоАРМ Защищенная почта

Документация продукта

Релиз v6.0

Архивная документация. Актуальный релиз: v7.3

Исходная документация на CryptoARM.ru

Редакция от 26.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

КриптоАРМ 10

Общие сведения

- О продукте 11
- Функциональность 13
- Лицензирование 17
- Общие вопросы 20
- Криптопровайдеры 24

Начало работы

- Установка КриптоАРМ
  - Установка КриптоАРМ на ОС Windows 26
  - Установка КриптоАРМ на Linux 30
  - Установка КриптоАРМ на macOS 40
- Установка КриптоПро CSP
  - Установка КриптоПро CSP на ОС Windows 44
  - Установка КриптоПро CSP на Linux 45
  - Установка КриптоПро CSP на macOS 48
- Установка лицензионного ключа
  - Как ввести лицензионный ключ КриптоАРМ 50
  - Как ввести лицензионный ключ КриптоПро CSP 52
  - Как ввести лицензионный ключ на модули TSP и OCSP 54
  - Проверка рабочего места 55

Почта

- Начало работы с почтой 58
- Добавление аккаунта
  - Добавление аккаунта 60
  - Добавление аккаунта mail.ru 62
  - Добавление аккаунта yandex.ru 64
  - Добавление аккаунта gmail.com 66
  - Добавление аккаунта outlook.com 68
  - Добавление аккаунта icloud.com 70

Добавление аккаунта rambler.ru ... 72

Почтовые настройки

Редактирование настроек почты ... 74

Настройки подписи и шифрования писем ... 79

Удаление почтового аккаунта ... 82

Изменение активного аккаунта ... 83

Работа с письмами

Просмотр писем ... 84

Действия с письмами ... 89

Отправка письма ... 93

Отправка подписанного и зашифрованного письма ... 97

Отправка письма с уведомлениями ... 100

Сортировка писем ... 102

Группировка писем в цепочки ... 104

Удаление и восстановление писем ... 105

Отметить письмо как прочитанное или непрочитанное ... 109

Поиск писем ... 110

Рассылка файлов ... 112

Работа с расширениями .eml, .p7s, .p7m ... 115

Документы

Описание раздела ... 117

Профили подписи

Профили подписи ... 118

Описание настроек профиля подписи ... 129

Подпись и шифрование

Подпись документа ... 134

Шифрование документа ... 143

Соподпись ... 147

Проверка и расшифрование

Проверка подписи документа ... 148

Снятие подписи с документа ... 154

Расшифрование документа ... 156

Групповые операции
Прямые групповые операции ... 159
Обратные групповые операции ... 160
Результаты операций ... 161
Подпись и защита PDF-документов
Загрузка PDF-документа ... 163
Просмотр PDF-документа ... 164
Подпись PDF-документа ... 166
Сертификация PDF-документа ... 181
Конвертация PDF-документа ... 182
Подпись PDF-документа в существующую разметку ... 184
Проверка подписи PDF-документа ... 185
Выполнение операций в командной строке или терминале ... 186
Действия с документами
Просмотр информации о документе ... 191
Просмотр документа ... 196
Удаление документа ... 198
Добавление в мастер ... 199
Как открыть папку с файлом на компьютере ... 201
Архивирование документов ... 203
Сертификаты
Описание раздела ... 205
Установка личного сертификата ... 208
Установка сертификата из DSS ... 211
Создание запроса ... 214
Создание самоподписанного сертификата ... 217
Установка корневого и промежуточного сертификатов ... 220
Установка сертификатов других пользователей ... 222
Установка списка отзыва ... 225
Экспорт личного сертификата ... 226
Экспорт сертификата ... 229
Удаление сертификата ... 231
Действия с ключевыми контейнерами ... 232

Контакты
Описание раздела ... 236
Локальные контакты
Добавление контакта ... 238
Просмотр информации о контакте ... 241
Привязка сертификата к контакту ... 242
Редактирование контакта ... 244
Удаление локальных контакта ... 245
Восстановление удаленных контактов ... 247
Поиск контакта ... 248
Группа контактов ... 249
Добавление фото к контакту ... 254
Адресная книга LDAP
Добавление адресной книги LDAP ... 256
Редактирование настроек адресной книги LDAP ... 260
Удаление адресной книги LDAP ... 262
Адресная книга ALD Pro ... 263
Адресная книга CardDAV ... 268
Импорт контактов vCard ... 271
Переключение между адресными книгами ... 273
Уведомления
Работа с уведомлениями ... 274
Работа с журналом событий ... 275
API КриптоАРМ
Общее описание ... 278
Описание запросов и ответов ... 281
Команда signAndEncrypt
Описание ... 283
Формат ссылки ... 285
Описание запросов и ответов
Общее ... 286
Получение параметров операции ... 287

Отправка результата прямых операций ... 290
Отправка результата обратных операций ... 291
Отправка результата проверки подписи ... 292

Типы данных

Интерфейс ISignAndEncryptParameters ... 293
Тип ISignAndEncryptOperationDirect ... 294
Тип ISignAndEncryptOperationReverse ... 295
Тип ISignAndEncryptOperationVerify ... 296
Интерфейс ISignAndEncryptOperationProps ... 297
Интерфейс IFile ... 298
Интерфейс IExtra ... 299
Интерфейс IDirectResults ... 301
Интерфейс IDirectResultOut ... 302
Интерфейс IReverseResults ... 303
Интерфейс IReverseResultOut ... 304
Интерфейс IVerifySignResults ... 305
Интерфейс IVerifySignResult ... 306
Интерфейс ISignerStatus ... 307
Интерфейс ILocalResultParams ... 308
Интерфейс ISignStampAppearance ... 309
Интерфейс IMockupSettings ... 310
Интерфейс IRequisitesSettings ... 311
Интерфейс IPdfCertRequisite ... 312
Интерфейс IPdfMarkedArea ... 313

Команда certificates

Описание ... 314
Формат ссылки ... 315

Описание запросов и ответов

Общее ... 316
Получение параметров операции ... 317
Отправка сертификата ... 319
Отправка списка сертификатов ... 320
Отправка сведений о сертификате ... 321

Типы данных
Интерфейс ICertificatesParameters ... 322
Интерфейс ICertificatesOperationProps ... 323
Интерфейс ICertificateBase64Params ... 324
Интерфейс ICertificateInfo ... 325
Интерфейс ICertificateIdentityInfos ... 326
Интерфейс КриптоАРМ при выборе и отправке сертификатов ... 327
Команда certrequests
Описание ... 328
Формат ссылки ... 329
Описание запросов и ответов
Общее ... 330
Получение параметров операции ... 331
Отправка запроса на сертификат ... 333
Типы данных
Интерфейс ICertrequestsParameters ... 334
Тип CertrequestsOperation ... 335
Интерфейс ICertrequestsOperationGenerateProps ... 336
Интерфейс ICertificatesParameters ... 337
Интерфейс IRDN ... 338
Интерфейс IRequestExtension ... 339
Интерфейс IKeyUsage ... 340
Интерфейс IExtendedKeyUsage ... 341
Интерфейс ICertificatesParameters ... 342
Интерфейс ICertificaterequestBase64Params ... 343
Команда diagnostics
Описание ... 344
Формат ссылки ... 345
Описание запросов и ответов
Общее ... 346
Получение параметров операции ... 347
Отправка сведений о рабочем месте ... 349

Типы данных
Интерфейс IDiagnosticsParameters ... 350
Тип IDiagnosticOperation ... 351
Интерфейс IDiagnosticsOperationProps ... 352
Интерфейс IDiagnosticsInformation ... 353
Интерфейс ISystemInformation ... 354
Интерфейс IVersions ... 355
Интерфейс IProviders ... 356
Интерфейс ILicenses ... 357
Интерфейс ILicenseInfo ... 358
LicenseType Enum ... 359
Команда startView
Описание ... 360
Формат ссылки ... 361
Описание запросов и ответов
Общее ... 362
Получение параметров операции ... 363
Типы данных
Интерфейс IStartViewParameters ... 365
Интерфейс IStartViewOperationProps ... 366
Команда mail
Описание ... 367
Формат ссылки ... 368
Описание запросов и ответов
Общее ... 369
Получение параметров операции ... 370
Типы данных
Интерфейс IMailParameters ... 372
Интерфейс IMailOperationProps ... 373
Интерфейс IMailProps ... 374
FAQ
Часто задаваемые вопросы ... 375

Глоссарий 378

Дополнительные статьи

API КриптоАРМ 384

Открыть статью на сайте

КриптоАРМ

КриптоАРМ 6

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 6 — 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 6 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 6.

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

О продукте

КриптоАРМ — приложение для электронной подписи и шифрования файлов со встроенным почтовым клиентом. Приложение предназначено для обеспечения безопасного и юридически значимого обмена электронными документами с государственными, коммерческими организациями и физическими лицами.

Приложение предназначено для обмена конфиденциальной почтовой корреспонденцией по протоколам SMTP, SMTPS, IMAP, IMAPS, POP3 между пользователями почтовых систем.

Приложение обеспечивает подготовку, хранение и просмотр писем на локальном рабочем месте, выполняя шифрование и подпись писем по алгоритмам ГОСТ 28147-89, ГОСТ Р 34.10-2012, ГОСТ Р 34.11-2012, ГОСТ Р 34.12-2015, ГОСТ Р 34.13-2015, ГОСТ 34.12-2018.

Поддерживаемые криптопровайдеры

Поддерживается криптопровайдер КриптоПро CSP версии 5.0 и выше.

Подробнее о том, что такое криптопровайдеры в инструкции Криптопровайдеры.

Поддерживаемые ключевые носители

Поддерживается работа с ключевыми носителями Рутокен, JaCarta, Esmart через криптопровайдер КриптоПро CSP.

Полный список поддерживаемых ключевых носителей, в зависимости от используемой программно-аппаратной платформы, можно найти в формуляре криптопровайдера КриптоПро CSP.

Кроме того, ознакомиться со списком поддерживаемых носителей можно на сайте компании КриптоПро.

Системные требования

Минимальные системные требования

- Процессор с архитектурой x86-64 с тактовой частотой 1,0 ГГц;
- Оперативная память 2 Гбайт;
- Пространство для установки на жестком диске 500 МБ;
- Монитор с разрешением 1024x768.

Рекомендуемые системные требования

- Процессор с архитектурой x86-64 с тактовой частотой 2,0 ГГц и выше;
- Оперативная память 4 Гбайт и выше;

- Пространство для установки на жестком диске 5 Гбайт и выше;
- Монитор с разрешением 1920x1080 и выше.

Поддерживаемые операционные системы

Клиентские:

- Microsoft Windows 8.1, 10 32bit, 10 64bit, 11
- Ubuntu 20.04, 22.04
- macOS 11 Big Sur, 12 Monterey, 13 Ventura
- Astra Linux Special Edition 1.7 Смоленск
- Альт Рабочая станция 10, 10К
- Альт 10 Образование
- РЕД ОС 7.3
- РОСА ХРОМ 12 Рабочая станция

Серверные:

- Windows Server 2016
- Windows Server 2019
- Ubuntu Server 20.04, 22.04
- CentOS 8
- Альт Сервер 10
- РЕД ОС Сервер 7.3
- РОСА ХРОМ 12 Сервер

Открыть статью на сайте

Функциональность

Возможности	
Работа с документами	работа с результатами выполнения операций с документами
	хранение копии документов, полученных в результате выполнения операций
	переход в мастер прямых (подпись и шифрование) и обратных (проверка подписи и расшифрование) операций
	работа с почтовыми вложениями: открыть, добавить в мастер прямых или обратных операций, отправить, показать в папке
Мастер Подпись и защита PDF	подпись и сертификация файлов в формате PDF
	хранение копии документов, полученных в результате операций
	разметка областей под подписи
	добавление произвольной области под изображение или текст
	конвертация PDF - документов в формат PDF/A - 2b
Электронная подпись	электронная подпись и проверка подписи произвольных файлов на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	добавление электронной подписи (функция создания соподписи) на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	создание присоединенной и отсоединенной электронной подписи
	создание подписи стандарта CAdES-BES, CAdES-T, CAdES-X Long Type 1, CAdES-A
	подпись сертификатом DSS
	формирование отчёта о проверке электронной подписи документа в формате .pdf

Возможности	
	снятие электронной подписи с документа
Шифрование/расшифрование	шифрование и расшифрование файлов на поддерживаемых платформах; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	удаление исходных файлов после шифрования
	шифрование по стандарту PKCS#7
	шифрование в адрес нескольких получателей
	шифрование в адрес контактов
	расшифрование сертификатом DSS
Архивирование	архивирование файлов перед шифрованием; размер файла не может быть больше, чем свободная оперативная память, гарантированный размер файла — 2 Гб
	разархивирование из формата .zip
Управление контактами	создание, редактирование, удаление и восстановление локальных контактов
	поиск, группировка, сортировка контактов
	управление колонками в списке контактов
	добавление сертификата к контакту
	импорт контактов из каталога LDAP
	поддержка адресной книги ALD Pro
	поддержка vCard
	поддержка протокола CardDAV
	уровни вложенности групп контактов в виде древа
	поиск дубликатов и объединение контактов в одну запись
	шифрование документов в адрес контактов
	отправка писем в адрес группы
Управление сертификатами и ключами	отображение сертификатов и привязанных к ним закрытых ключей относительно хранилищ для поддерживаемых криптопровайдеров

Возможности	
	проверка корректности выбранного сертификата с построением цепочки доверия и скачиванием актуального списка отзыва
	просмотр свойств сертификата электронной подписи
	хранение закрытых ключей на носителях Рутокен (Актив), JaCarta (Аладдин Р.Д.), ESMART (ISBC) при условии использования криптопровайдера КриптоПро CSP
	создание запросов на сертификат
	импорт сертификатов с привязкой к закрытому ключу
	экспорт сертификатов
	удаление сертификатов
	импорт сертификатов из DSS
	формирование отчёта действительности сертификата электронной подписи
Почта	добавление почтового аккаунта для подключения к почтовому серверу по протоколам SMTP, SMTPS, IMAP, IMAPS, POP3
	добавление почтового аккаунта Microsoft Exchange, Communigate
	редактирование настроек почтового аккаунта
	удаление подключённого аккаунта
	добавление нескольких почтовых аккаунтов
	работа с письмами — получение, просмотр, отправка, хранение, удаление (в том числе с почтового сервера), добавление вложений, отправка файлов с устройства в виде рассылки; синхронизация писем с почтовым сервером
	уведомления о получении/прочтении писем
	поиск и фильтрация писем
	сортировка списка писем
	группировка и отображение писем в цепочки

Возможности	
	перенос писем между папками активного аккаунта
	подпись и шифрование электронных писем с поддержкой российских криптоалгоритмов; автоматическая расшифровка и проверка подписи для полученных писем
	просмотр свойств электронной подписи письма
	формирование отчёта о проверке электронной подписи письма в формате .pdf
	хранение писем в зашифрованном виде
	хранение писем локально на устройстве
Работа с журналом событий и уведомлениями	отображение списка событий по уровням детализации
	просмотр уведомлений о событиях
	сохранение в формате .log
	отправка в формате .log
	распечатка информации о событиях
	загрузка архива
	показ в папке

Открыть статью на сайте

Лицензирование

Для работы с криптографическими операциями необходима лицензия.

В интернет-магазине cryptoarm.ru можно приобрести годовую или бессрочную версию лицензии КриптоАРМ.

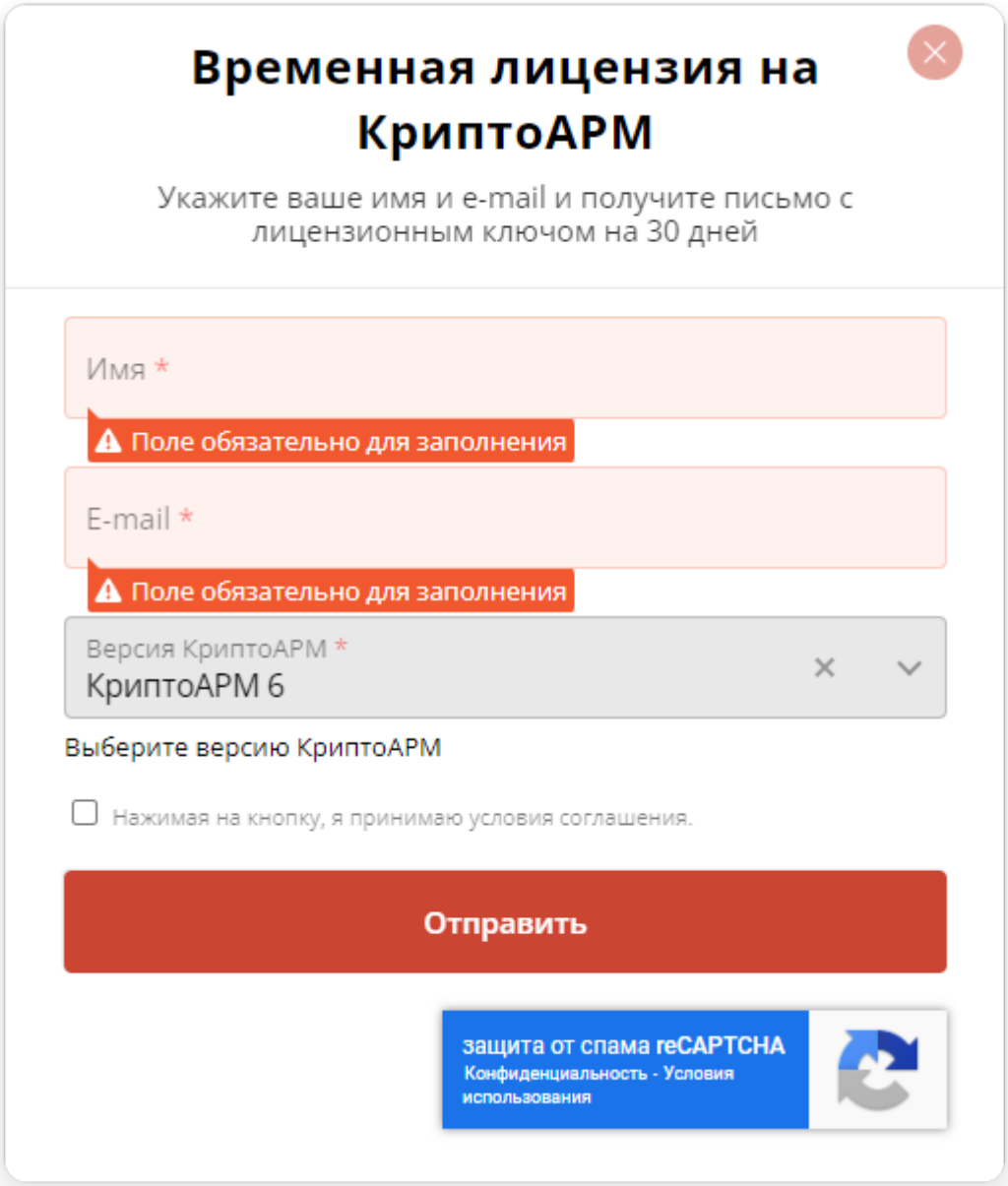
Как получить пробную лицензию КриптоАРМ

При первом запуске приложения активируется ознакомительная лицензия сроком на 30 дней.

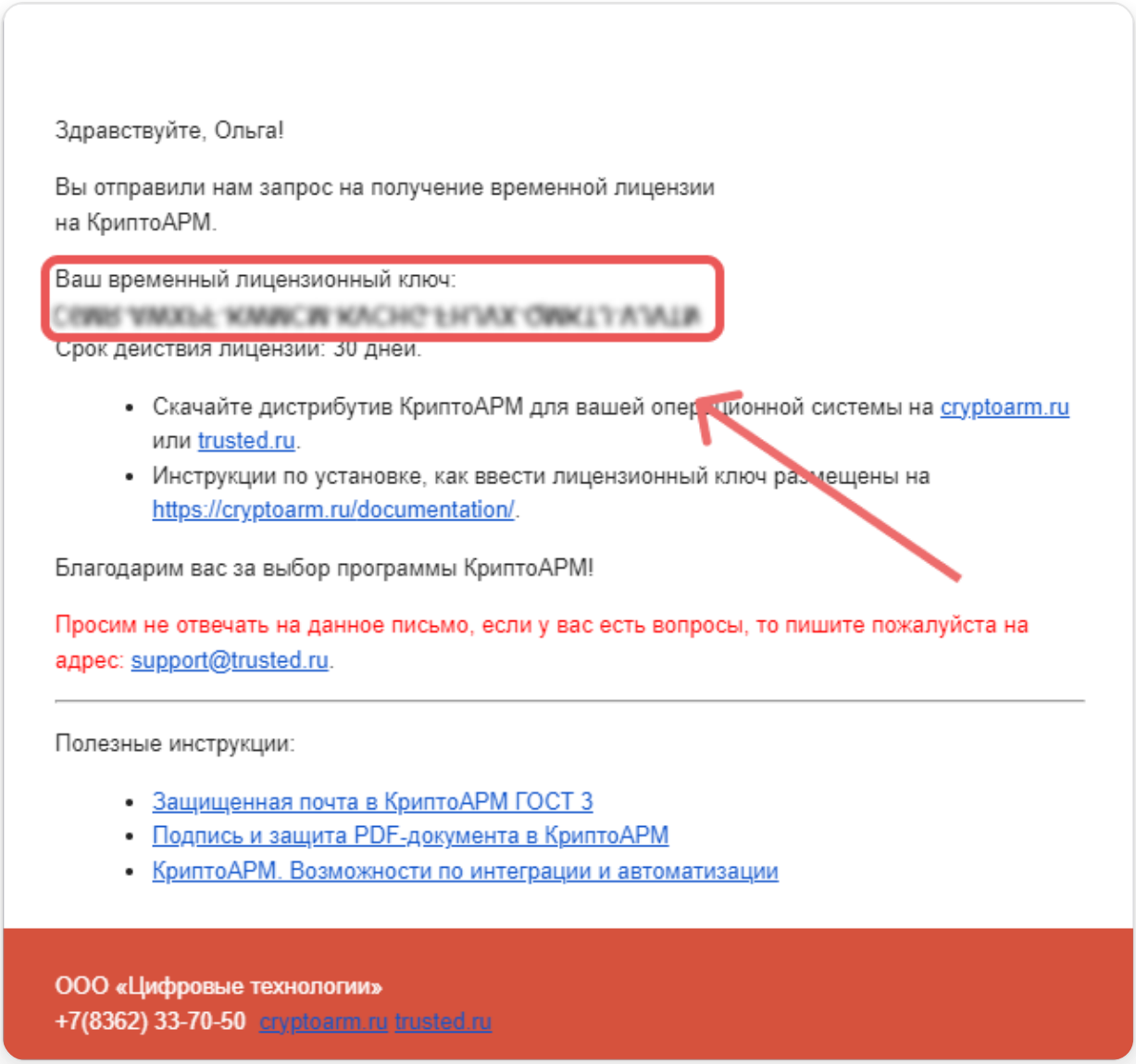
По окончании ознакомительного периода для полнофункциональной работы приложения требуется приобретение лицензии КриптоАРМ.

Если для знакомства со всеми возможностями КриптоАРМ недостаточно ознакомительного периода, вы можете получить дополнительную лицензию, заполнив форму заявки на сайте cryptoarm.ru.

1. Откройте форму заявки.
2. Укажите имя, адрес электронной почты, выберите версию КриптоАРМ 6.
3. Ознакомьтесь и примите условия лицензионного соглашения.
4. Нажмите кнопку **Отправить.**



5. На указанный адрес электронной почты будет направлено письмо с ключом временной лицензии.



Здравствуйте, Ольга!

Вы отправили нам запрос на получение временной лицензии на КриптоАРМ.

Ваш временный лицензионный ключ:
[redacted]
Срок действия лицензии: 30 дней.

- Скачайте дистрибутив КриптоАРМ для вашей операционной системы на cryptoarm.ru или trusted.ru.
- Инструкции по установке, как ввести лицензионный ключ размещены на https://cryptoarm.ru/documentation/.

Благодарим вас за выбор программы КриптоАРМ!

Просим не отвечать на данное письмо, если у вас есть вопросы, то пишите пожалуйста на адрес: support@trusted.ru.

Полезные инструкции:

- Защищенная почта в КриптоАРМ ГОСТ 3
- Подпись и защита PDF-документа в КриптоАРМ
- КриптоАРМ. Возможности по интеграции и автоматизации

ООО «Цифровые технологии»
+7(8362) 33-70-50 cryptoarm.ru trusted.ru

Как ввести лицензионный ключ в КриптоАРМ описано в инструкции.

Открыть статью на сайте

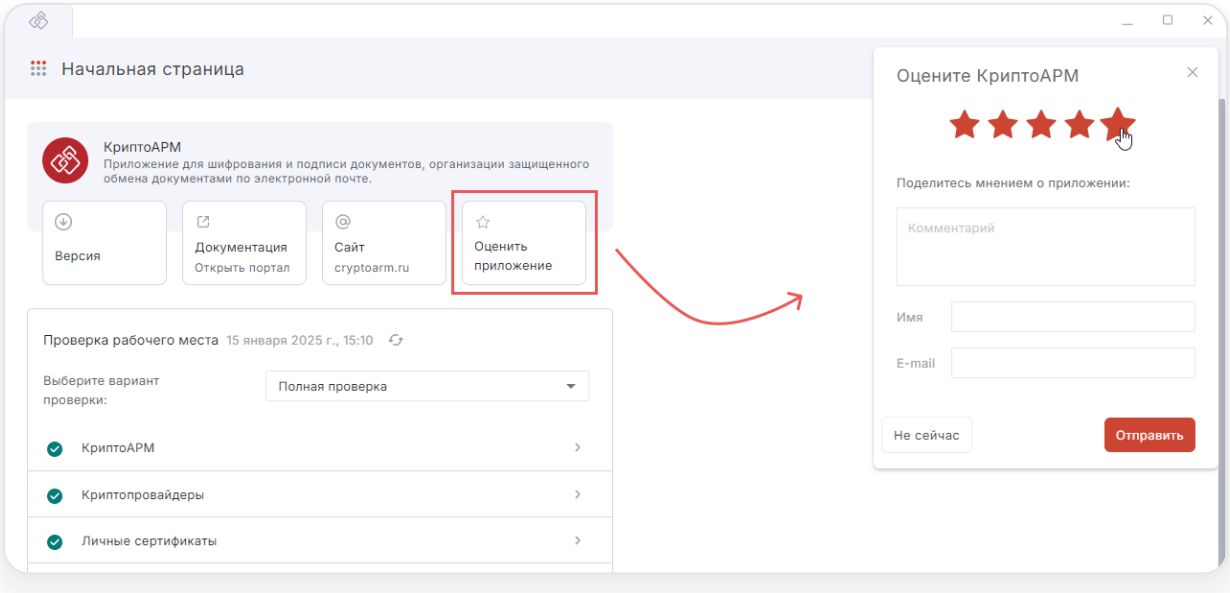
Общие вопросы

Как поставить оценку

Вы можете оценить приложение и поделиться мнением.

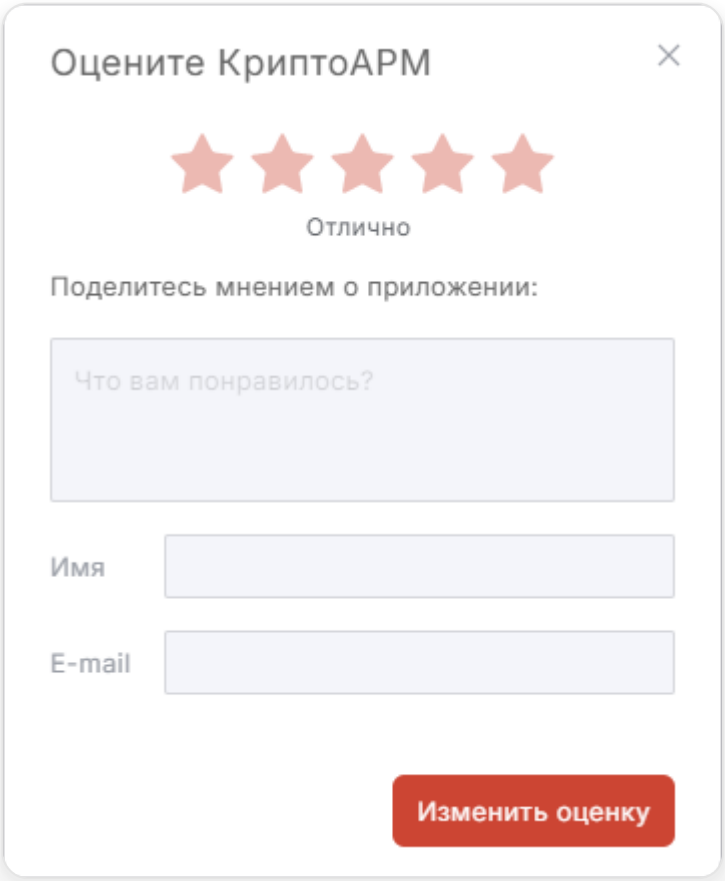
1. Откройте раздел **Начальная страница**.
2. Нажмите на **Оценить приложение** в блоке со сведениями о продукте.
3. Откроется окно **Оцените КриптоАРМ**:
    - Поставьте оценку,
    - Оставьте свой отзыв.
    - Укажите имя и адрес электронной почты.

    Поля с отзывом, именем и адресом почты можно оставить пустыми.
4. Нажмите **Отправить** для отправки отзыва.



Как изменить оценку

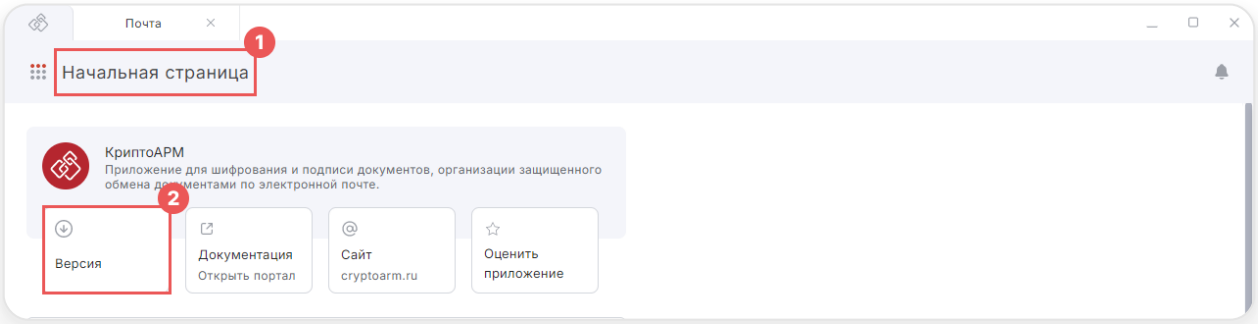
1. Откройте раздел **Начальная страница**.
2. Нажмите на **Оценить приложение** в блоке со сведениями о продукте..
3. Откроется окно **Оцените КриптоАРМ**.
4. Нажмите **Изменить оценку**.



5. Внесите изменения.
6. Нажмите **Отправить** для отправки отзыва.

Как узнать, какая версия КриптоАРМ установлена

Чтобы узнать, какая версия КриптоАРМ установлена на вашем компьютере, перейдите в раздел **Начальная страница**. Номер версии будет указан в первом блоке со сведениями о продукте.



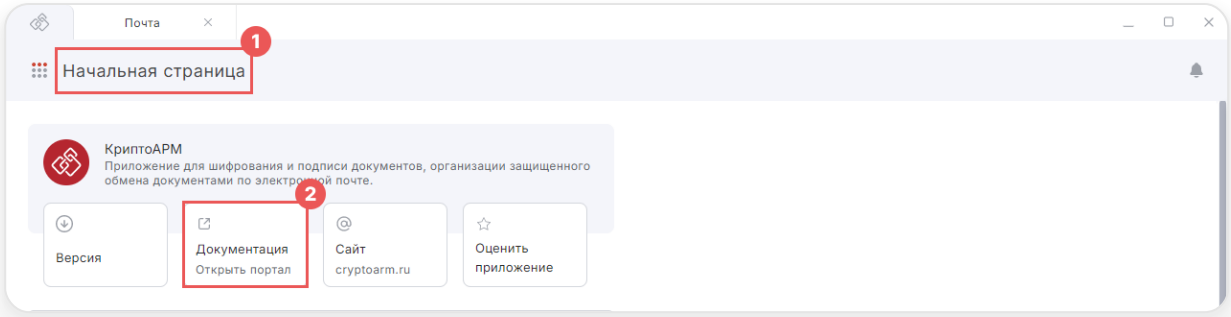
Как найти документацию

Руководство пользователя, ответы на часто задаваемые вопросы и описание API КриптоАРМ размещены на портале документации на сайте cryptoarm.ru.

Перейти на портал документации можно из приложения.

Чтобы открыть портал документации:

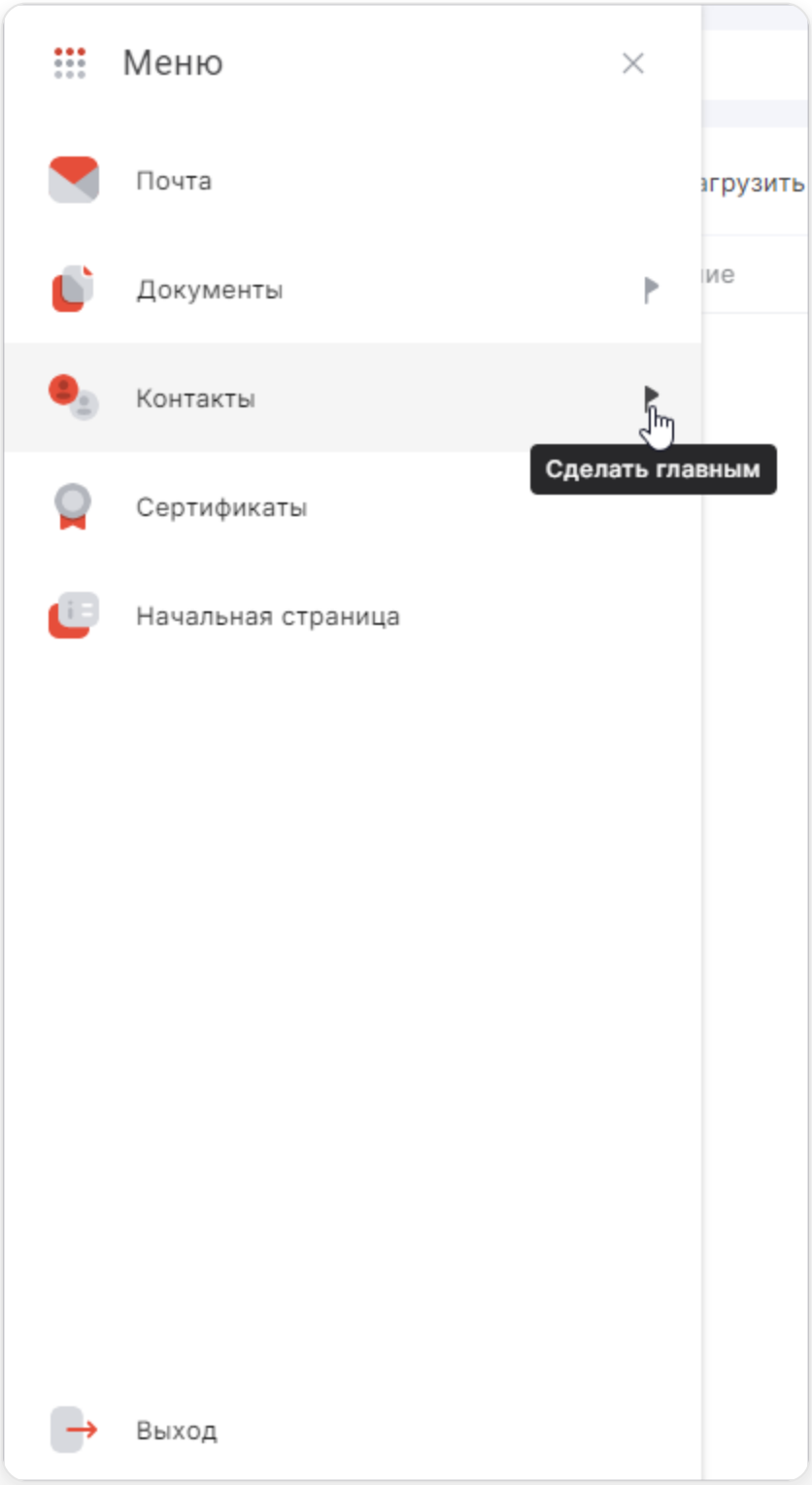
1. Откройте раздел **Начальная страница**.
2. Нажмите на виджет **Документация** в блоке со сведениями о продукте.
3. Ссылка на портал будет открыта в браузере по умолчанию.



Как изменить раздел при запуске

1. Откройте меню с разделами приложения по кнопке **Меню**, которая расположена в верхнем левом углу окна.
2. Наведите курсор мыши на раздел, который должен открываться при запуске приложения.
3. Нажмите на кнопку **Сделать главным**.

Выбранный раздел откроется автоматически при следующем запуске приложения.


Меню
Почта
Документы
Контакты
Сделать главным
Сертификаты
Начальная страница
Выход

Открыть статью на сайте

Криптопровайдеры

Что такое криптопровайдер

Криптопровайдер (или CSP, от английского Cryptography Service Provider) — это специализированный модуль для операционной системы.

Криптопровайдер — это неотъемлемая часть программы для создания и проверки цифровых подписей и шифрования данных. Он предоставляет доступ к криптографическим алгоритмам и функциям, которые обеспечивают безопасное шифрование информации и создание цифровых подписей.

Криптопровайдер управляет ключами, генерирует и проверяет цифровые подписи, а также осуществляет шифрование и дешифрование данных, используя защищенные алгоритмы. Без этого компонента программа не сможет выполнять свои важнейшие функции, что делает его критически важным для обеспечения безопасности и целостности данных в процессе их передачи и хранения.

В частности, криптопровайдер нужен для выполнения следующих криптографических функций:

- создание и проверка электронной подписи;
- шифрование данных;
- хранение ключей всех типов.

Система Windows управляет криптопровайдерами через специальный интерфейс CryptoAPI.

Для авторизации, контроля целостности данных и других задач операционная система взаимодействует с криптопровайдером. Это позволяет обеспечить конфиденциальность и юридическую значимость электронных документов, которыми обмениваются контрагенты.

Другими словами, криптопровайдер — это программа, которая выступает посредником между операционной системой и программой, с которой работает пользователь, когда подписывает документ электронной подписью.

На некоторых сайтах не требуется наличие криптопровайдера, так как его функции выполняет программное обеспечение на сервере ресурса. В таком случае для простой электронной подписи криптопровайдер не нужен, но возможности такой электронной подписи будут ограничены.

В России невозможно использовать стандартные средства Windows CSP, так как продукты Microsoft не имеют российской сертификации. Это означает, что их нельзя применять в документообороте с государственными органами. В связи с этим в России используются программные продукты сторонних криптосервисов.

КриптоПро CSP

Для работы с программой КриптоАРМ необходимо установить криптопровайдер КриптоПро CSP от компании «КриптоПро».

Криптопровайдер СКЗИ КриптоПро CSP — специальная программа, осуществляющая криптографические операции подписи и шифрования на устройстве. Без лицензии на данный криптопровайдер нельзя подписывать и шифровать электронные письма и документы в программе КриптоАРМ.

- Как установить КриптоПро CSP на ОС Windows
- Как установить КриптоПро CSP на Linux
- Как установить КриптоПро CSP на macOS

Открыть статью на сайте

Установка КриптоАРМ на ОС Windows

Вы можете скачать установочный файл на сайте интернет-магазина cryptoarm.ru или на сайте компании-разработчика trusted.ru.

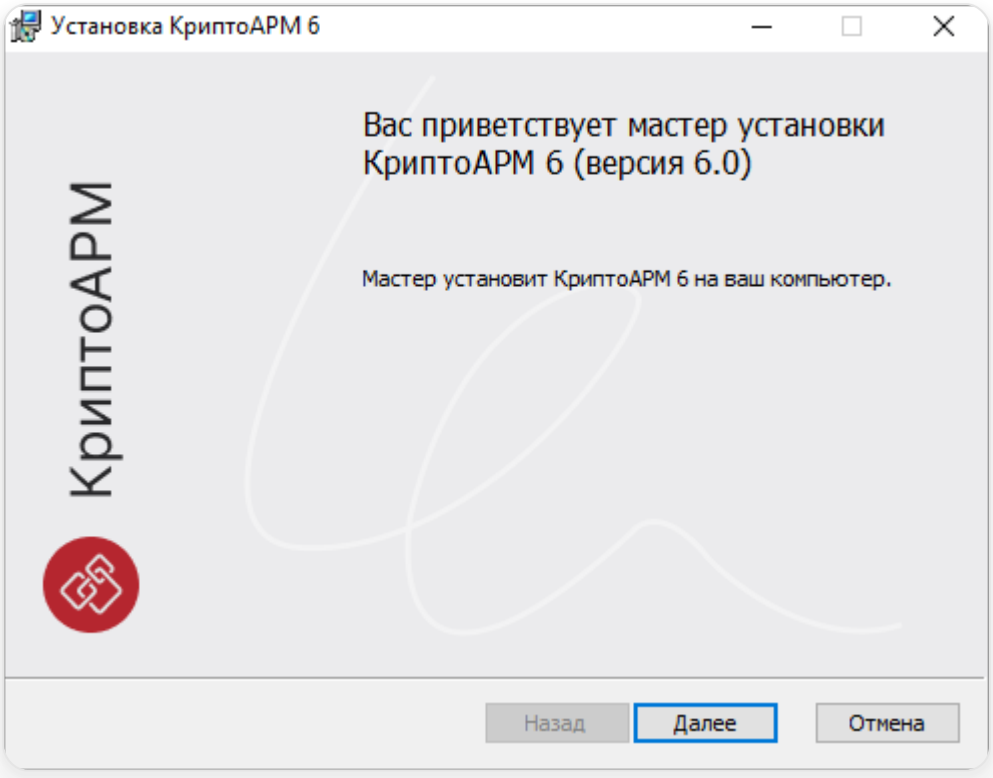
Примечание. Для установки приложения требуются права администратора.

Для корректной работы приложения необходимо дополнительно установить пакеты Visual Studio C++:

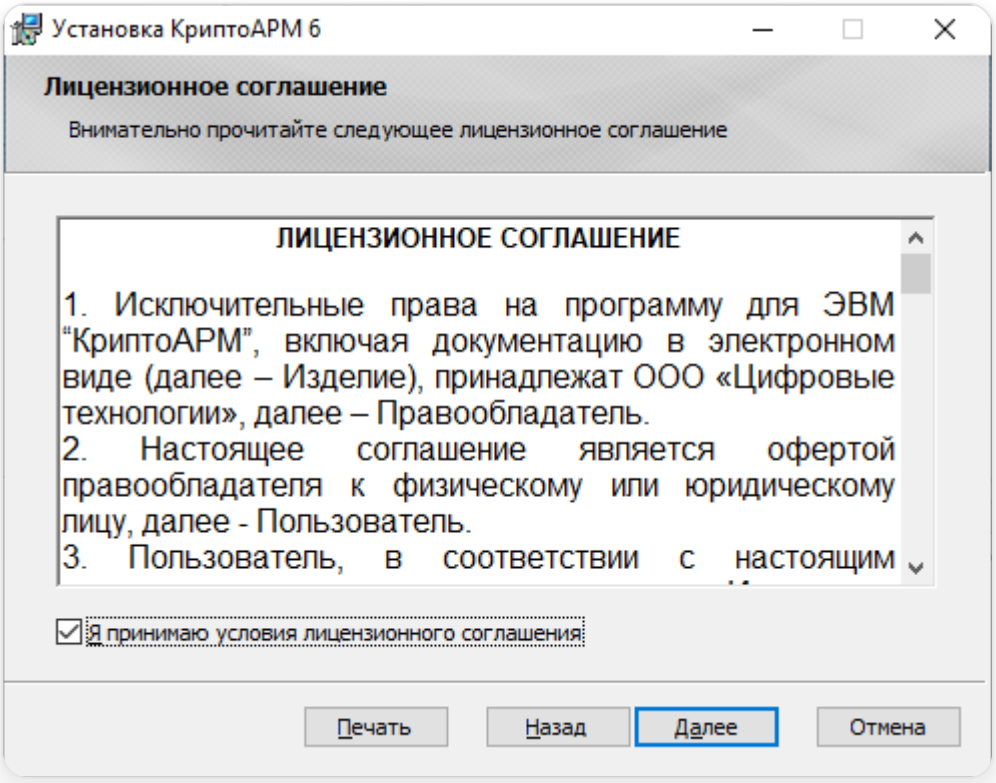
- Распространяемые пакеты VS C++ 2013 (x64),
- Распространяемые пакеты VS C++ 2019 (x64).

Как установить КриптоАРМ на ОС Windows

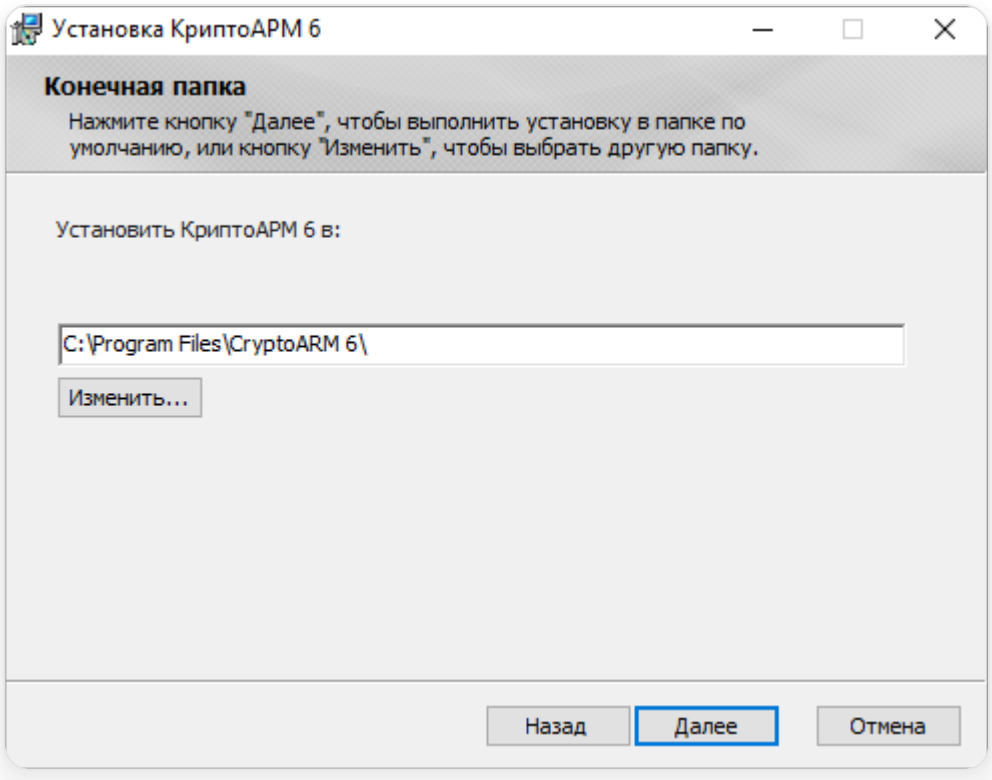
1. Скачайте и запустите установочный файл. Дистрибутив приложения можно скачать с сайта cryptoarm.ru.
2. Откроется мастер установки. Нажмите **Далее**.



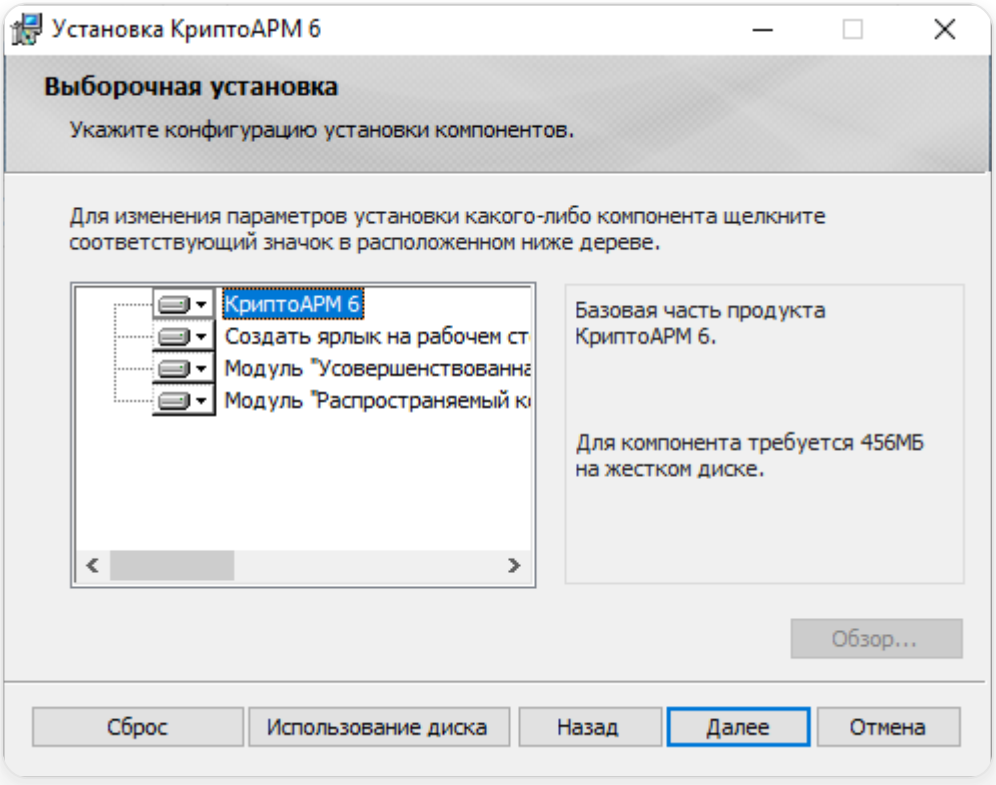
3. Ознакомьтесь с условиями лицензионного соглашения. Если вы согласны со всеми пунктами, нажмите **Принять**. Затем нажмите **Далее**.



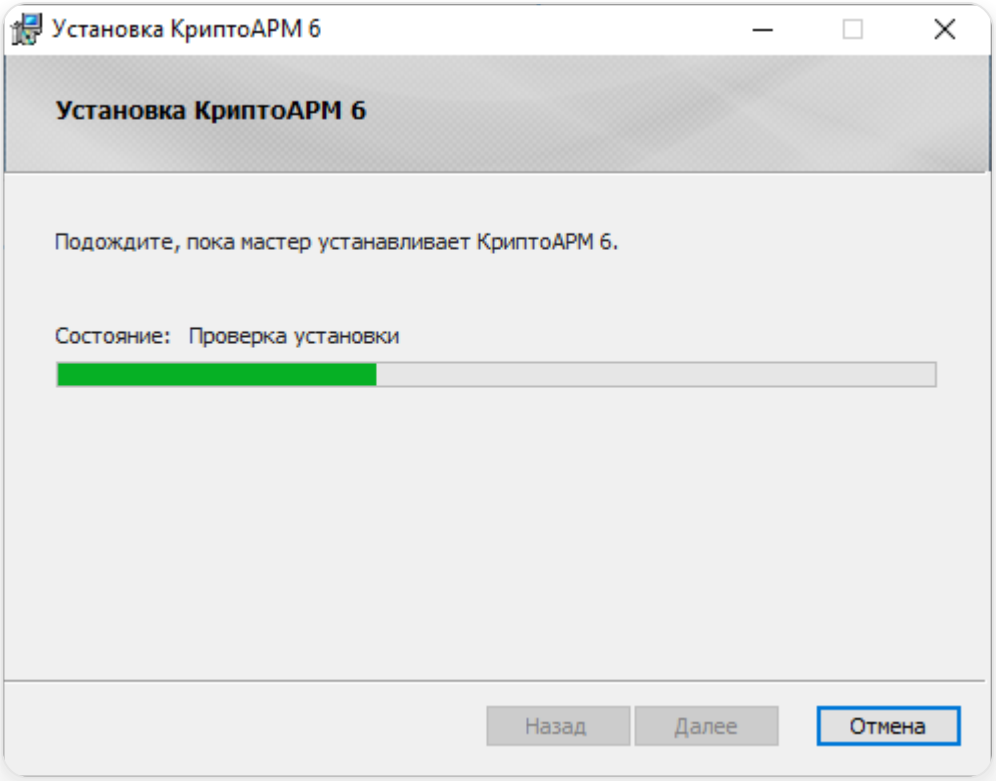
4. Выберите каталог для установки приложения. По умолчанию приложение устанавливается в каталог C:\Program Files\CryptoARM 6.



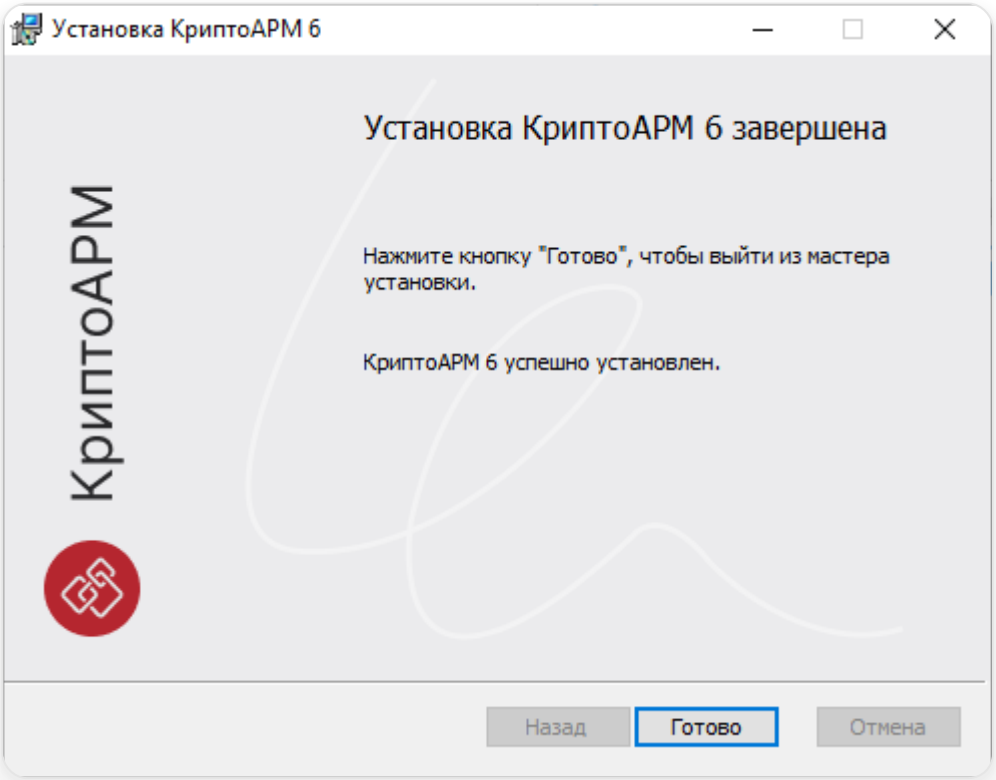
5. При необходимости отключите создание ярлыка на рабочем столе и установку модулей для создания усовершенствованной подписи.



6. Нажмите **Установить**.



Для закрытия мастера нажмите кнопки **Готово**.



Программа успешно установлена.

Открыть статью на сайте

Установка КриптоАРМ на Linux

Вы можете скачать установочный файл на сайте интернет-магазина cryptoarm.ru или на сайте компании-разработчика trusted.ru.

Установить приложение на операционную систему Linux можно несколькими способами:

- В графическом режиме с помощью мастера установки пакетов.
- В режиме командной строки через терминал.
- Путем обычной распаковки из архива.

По умолчанию приложение устанавливается в каталог /opt/cryptoarm_6/.

Графическая установка

1. Запустите на исполнение файл:
    - **cryptoarm-x.x.x-linux-x64.rpm** (где x.x.x – номер версии) для 64-разрядных ОС, основанных на RPM;
    - **cryptoarm-x.x.x-linux64-x86.deb** (где x.x.x – номер версии) для 86-разрядных ОС, основанных на DEB.
2. Откроется пакетный менеджер. Нажмите **Установить**.
3. Введите пароль администратора системы (Root).
4. Дождитесь окончания установки.

Установка через терминал

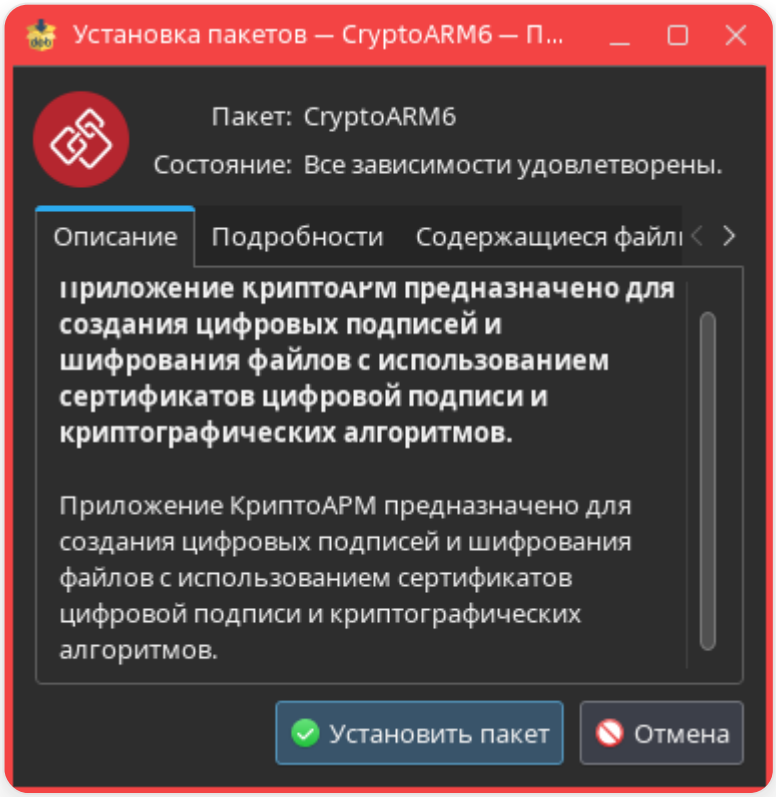
1. Запустите терминал и введите команду:
    - **sudo dpkg -i cryptoarm-x.x.x-x64.deb** — для ОС, основанных на DEB;
    - **sudo rpm -i cryptoarm-x.x.x-x64.rpm** — для ОС, основанных на RPM.
2. Укажите путь к установочному файлу и его название вручную или перетащите его в поле терминала.
3. Нажмите Enter.
4. Дождитесь окончания установки.

Установка КриптоАРМ на ОС Astra Linux

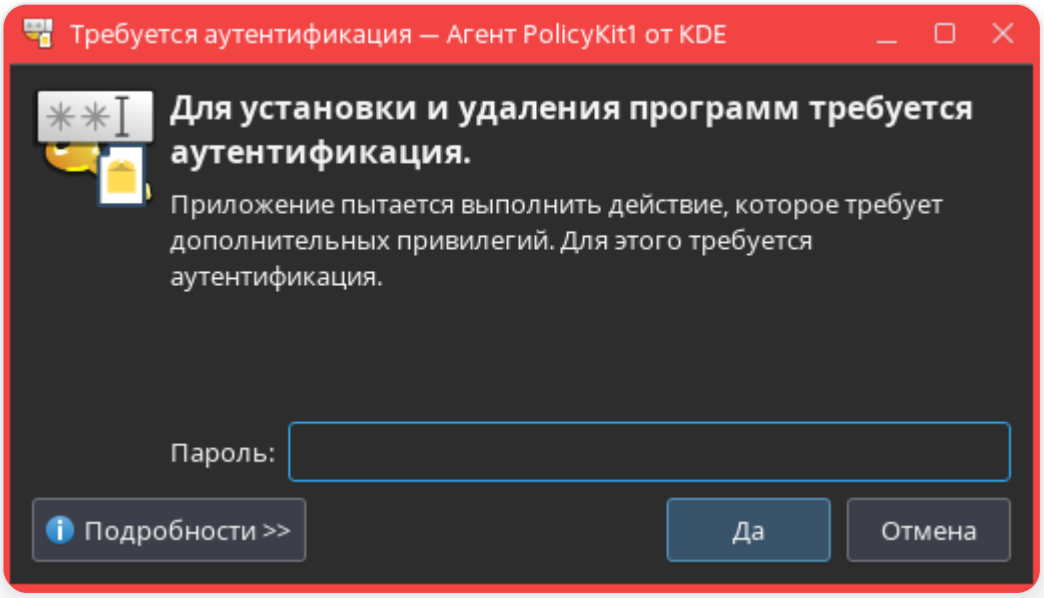
Графическая установка

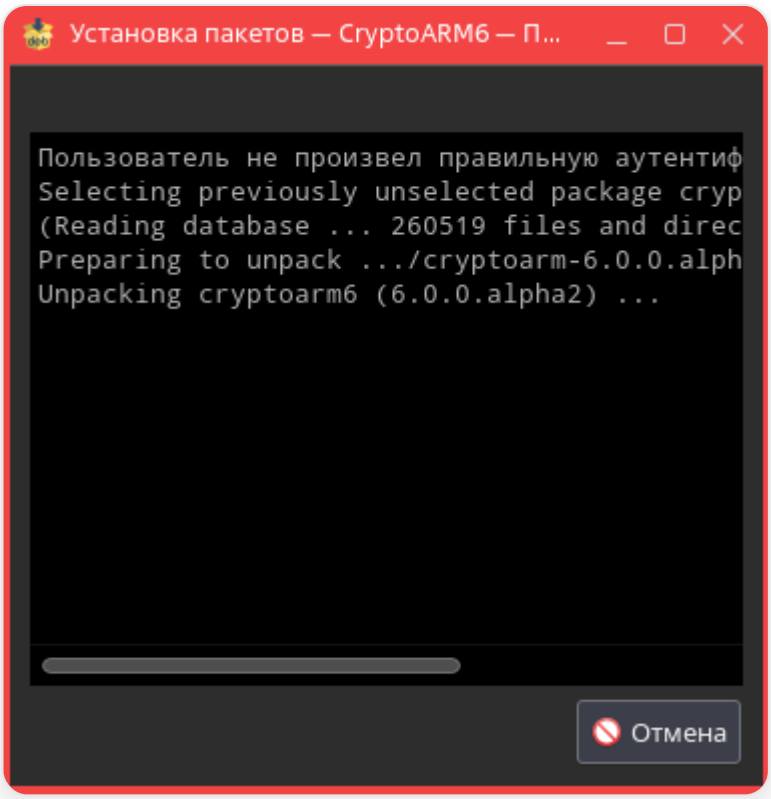
1. Запустите установочный файл. Дистрибутив приложения можно скачать с сайта cryptoarm.ru

2. Откроется окно **Установка пакетов**. Нажмите **Установить пакет**.

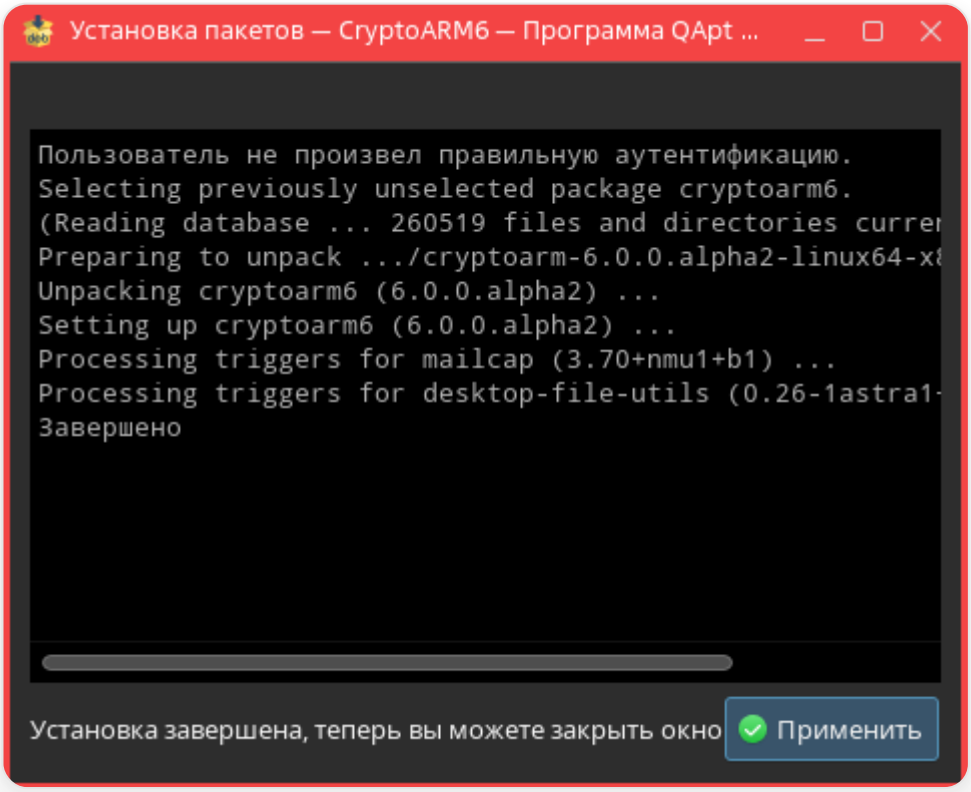


3. Введите пароль системного администратора root. Начнётся установка пакетов.



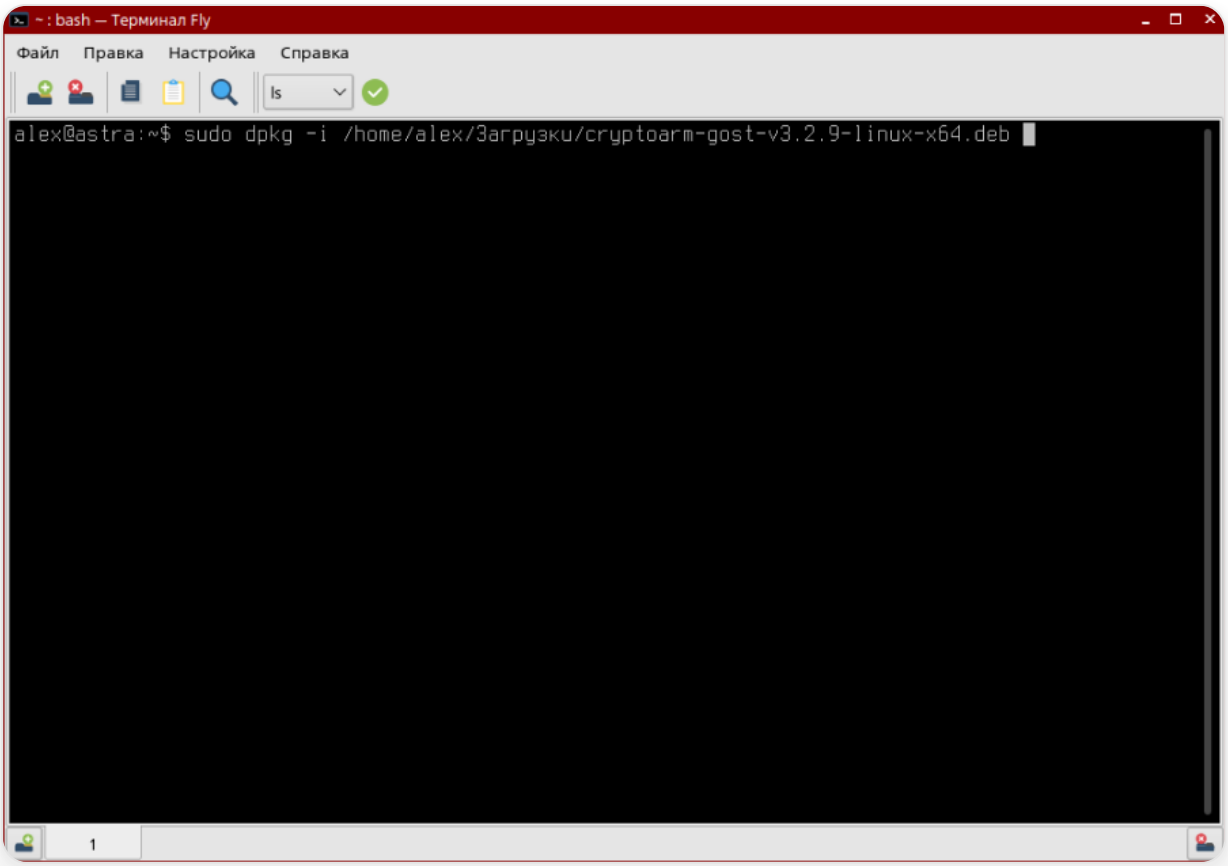


4. После успешной установки программы закройте окно установки.

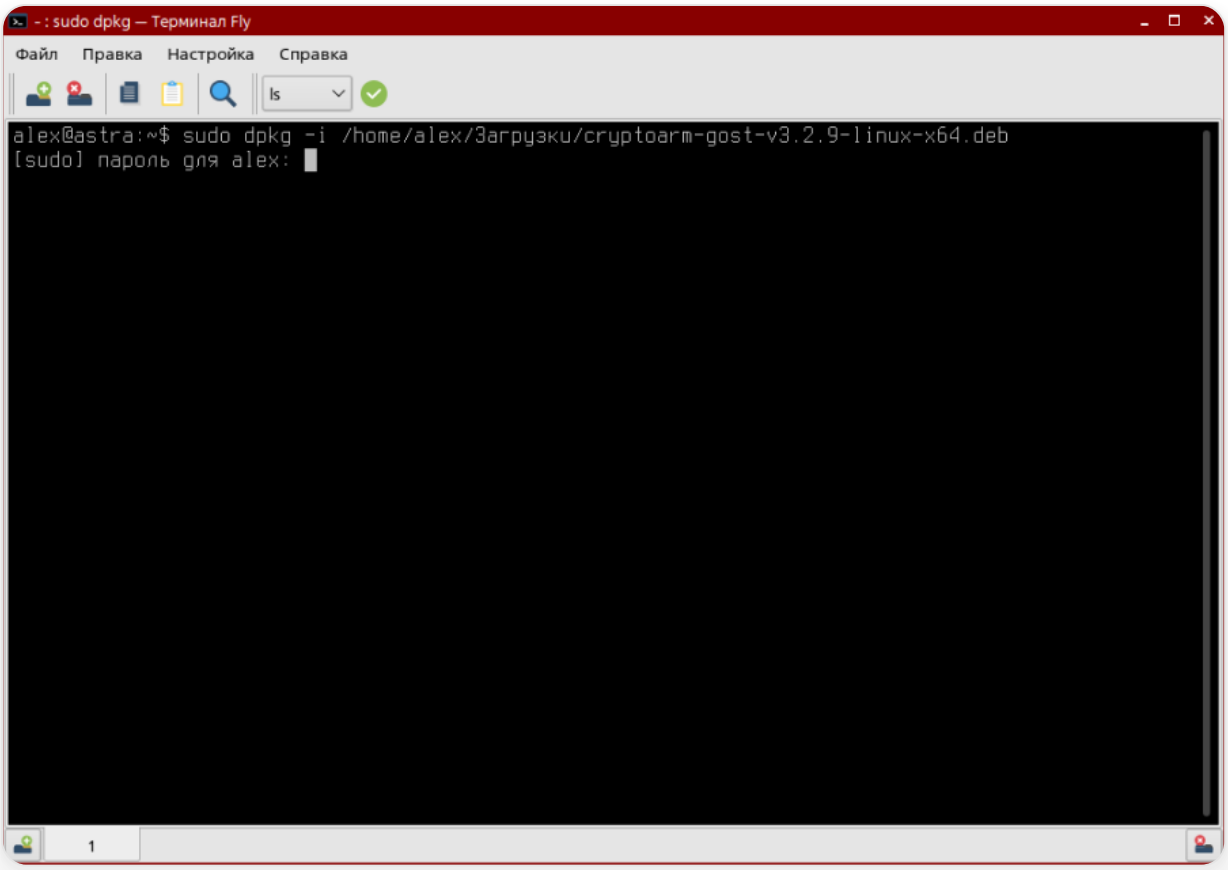


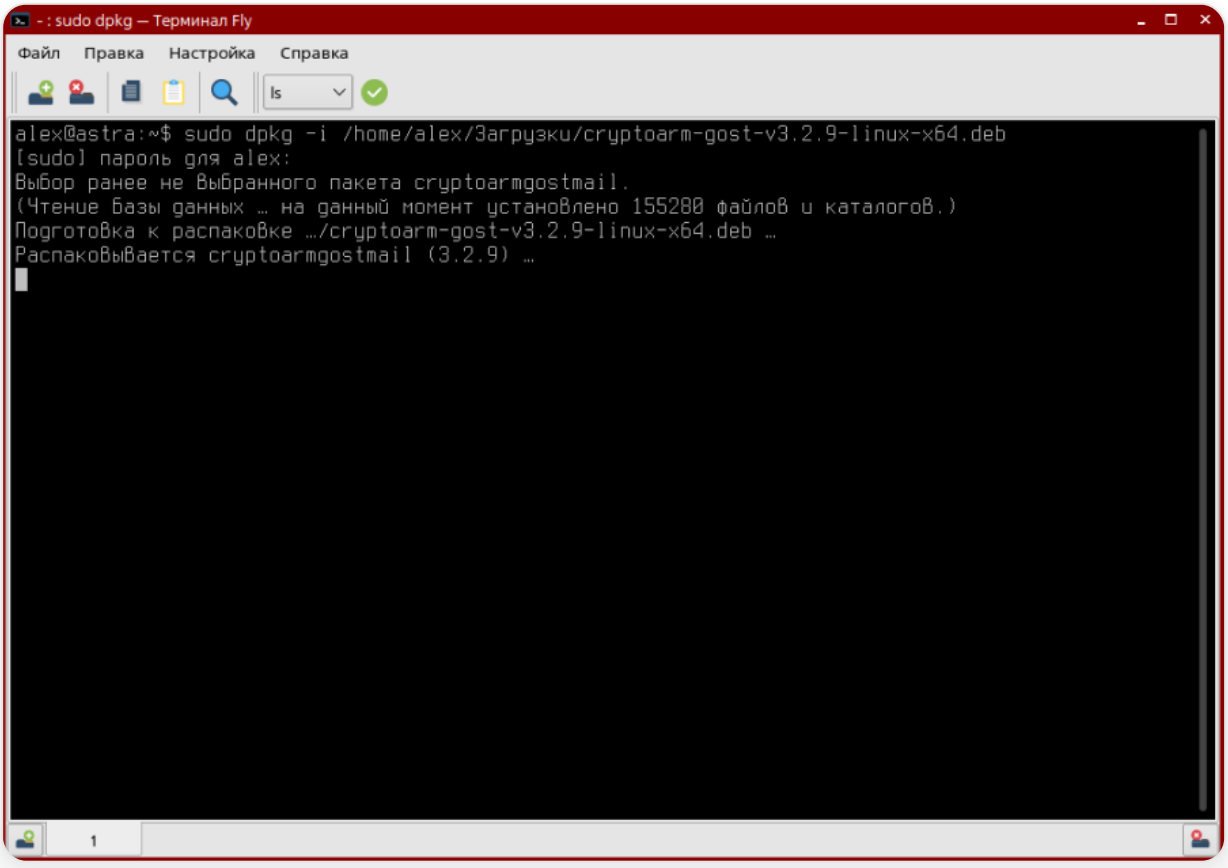
Установка через терминал

1. Запустите терминал и введите команду: **sudo dpkb -i <путь_к_файлу/название_файла.deb>**
2. Укажите путь к установочному файлу и его название вручную или перетащите его в поле терминала.



3. Нажмите Enter. Запустится распаковка и установка.


- : sudo dpkg — Терминал Fly
Файл Правка Настройка Справка
ls
alex@astra:~$ sudo dpkg -i /home/alex/Загрузки/cryptoarm-gost-v3.2.9-linux-x64.deb
[sudo] пароль для alex:
1


- : sudo dpkg — Терминал Fly
Файл Правка Настройка Справка
ls
alex@astra:~$ sudo dpkg -i /home/alex/Загрузки/cryptoarm-gost-v3.2.9-linux-x64.deb
[sudo] пароль для alex:
Выбор ранее не выбранного пакета cryptoarmgostmail.
(Чтение базы данных … на данный момент установлено 155280 файлов и каталогов.)
Подготовка к распаковке …/cryptoarm-gost-v3.2.9-linux-x64.deb …
Распаковывается cryptoarmgostmail (3.2.9) …
1

4. Дождитесь окончания установки.

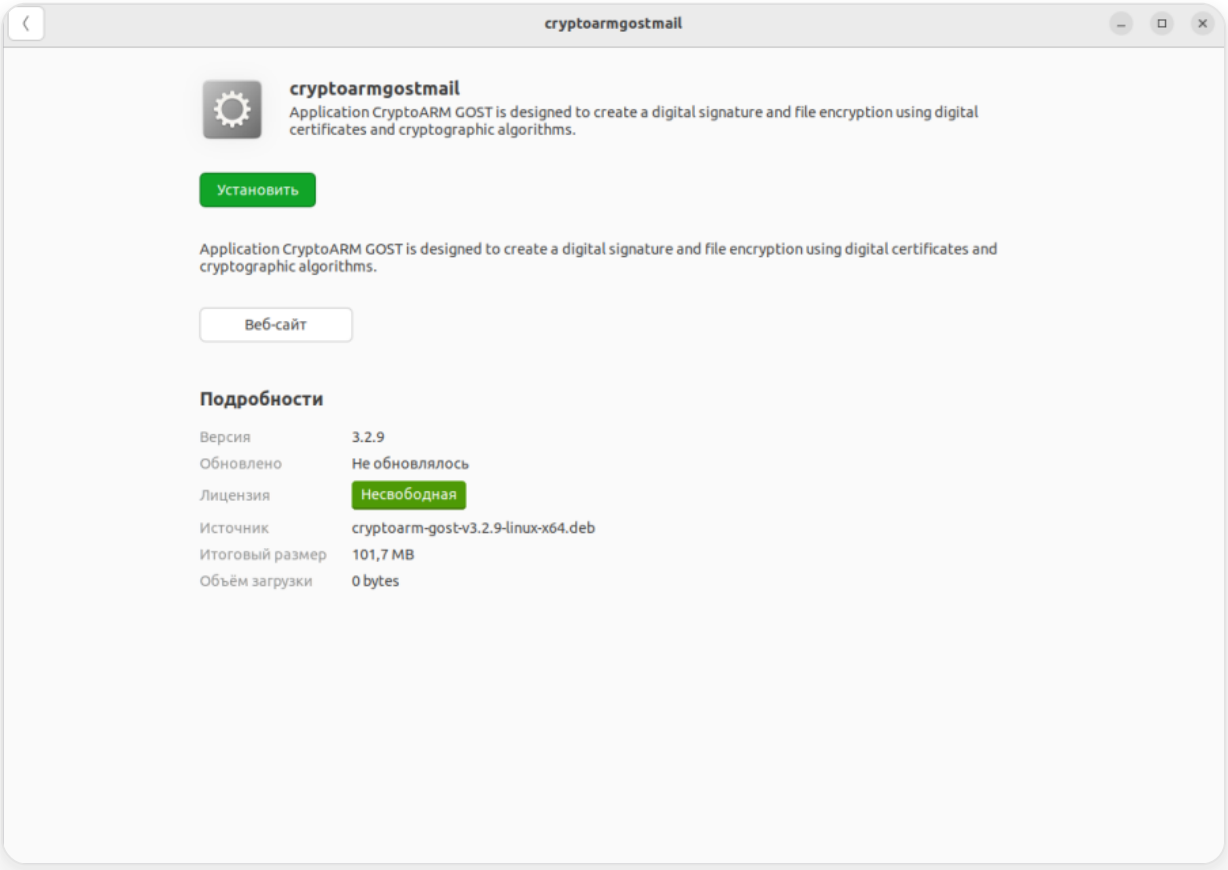
Установка КриптоАРМ на ОС Ubuntu

Важно. Для Ubuntu версии 20.04 требуется дополнительная установка:

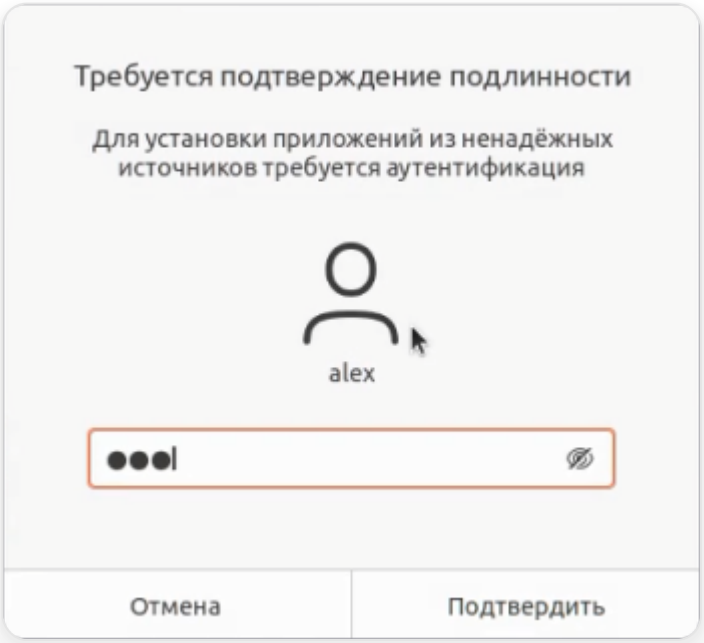
- sudo apt install libtidy-dev
- sudo apt install libctemplate-dev

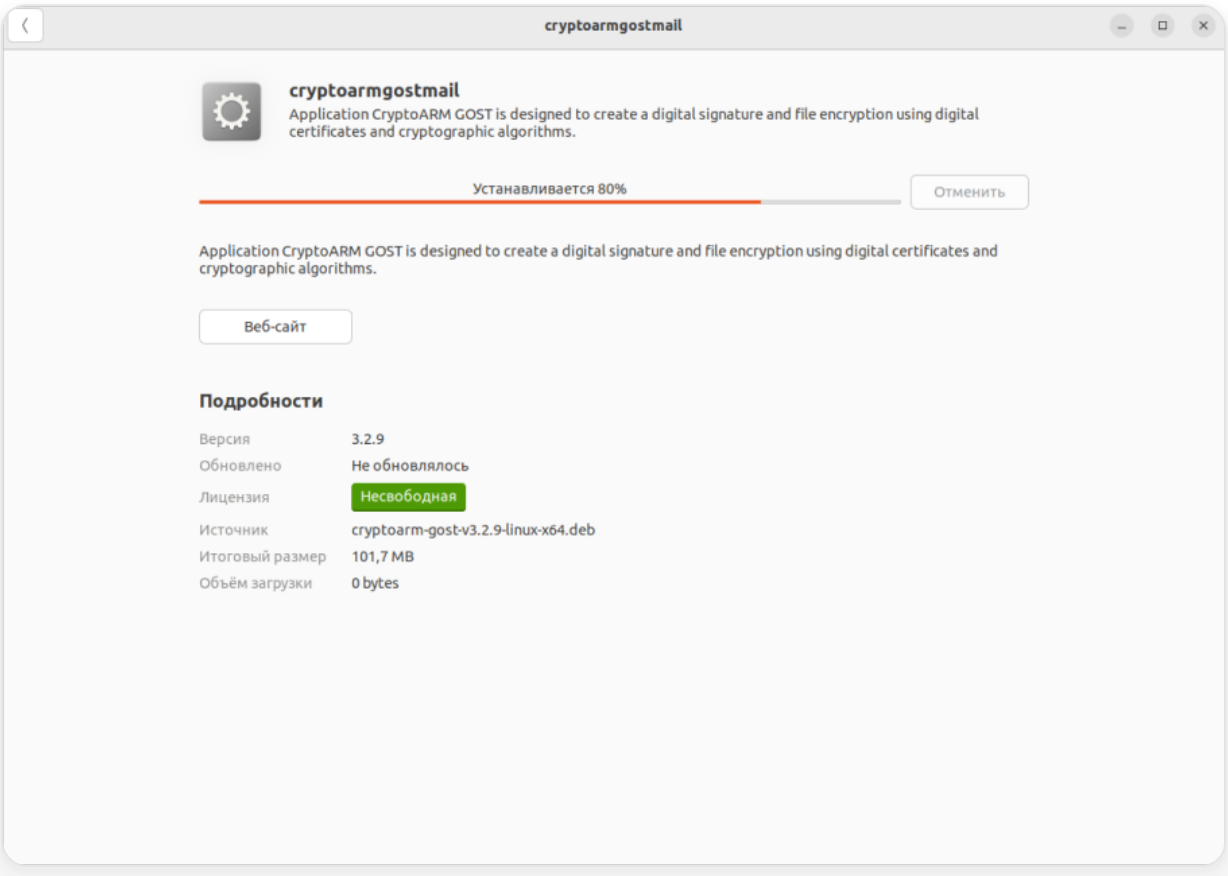
Графическая установка

1. Запустите установочный файл.
2. В открывшемся окне нажмите на **Установить**.

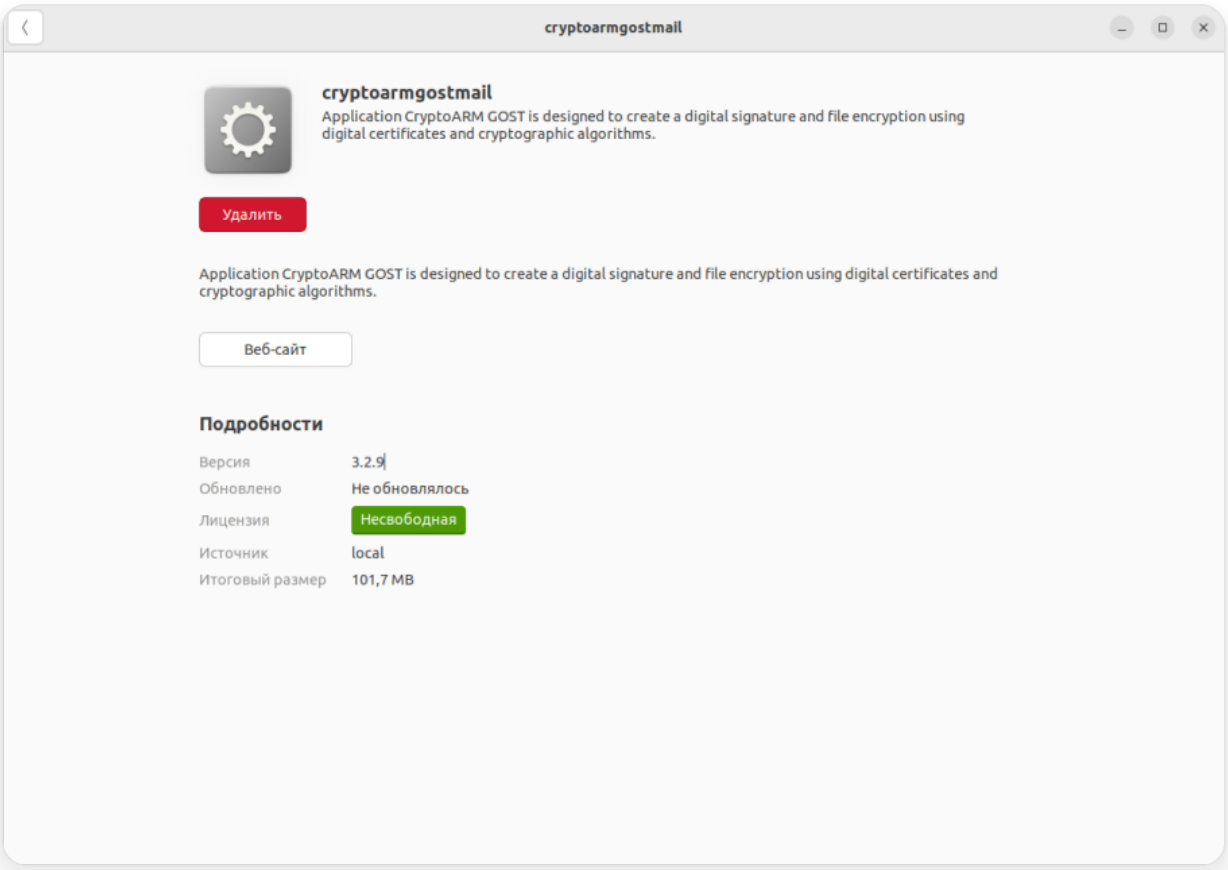


3. Введите пароль системного администратора root и нажмите **Подтвердить**. Запустится установка.





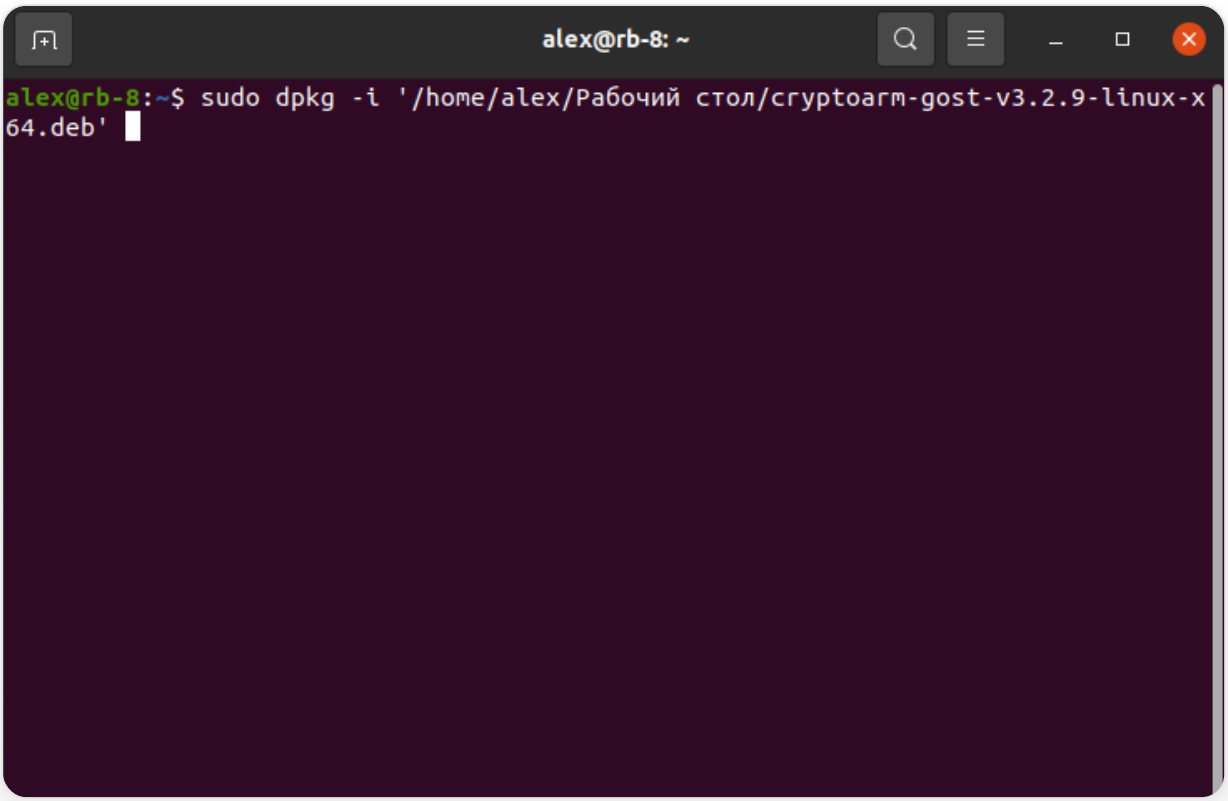
4. После успешной установки программы закройте окно установки.



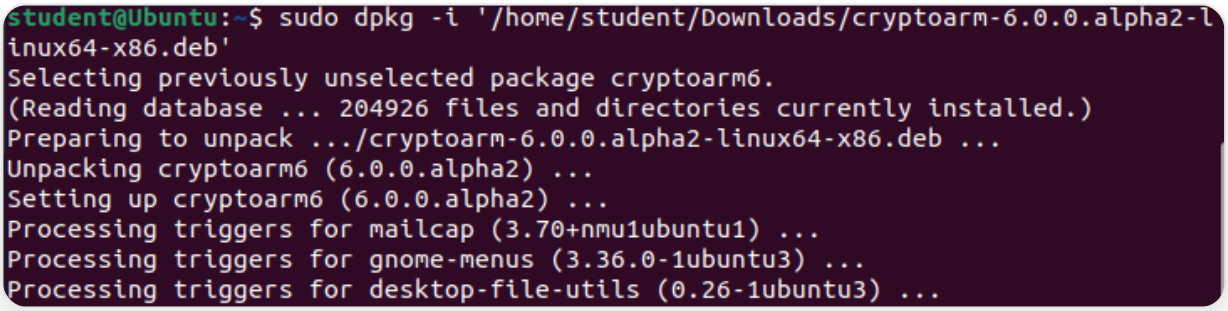
5. После установки приложения в меню появится ярлык приложения.

Установка через терминал

1. Запустите терминал и введите команду: **sudo dpkg -i <путь_к_файлу/название_файла.deb>**
2. Укажите путь к установочному файлу и его название вручную или перетащите его в поле терминала.



3. Введите пароль системного администратора root и нажмите **Enter**. Запустится установка.



4. Дождитесь окончания установки.

Открыть статью на сайте

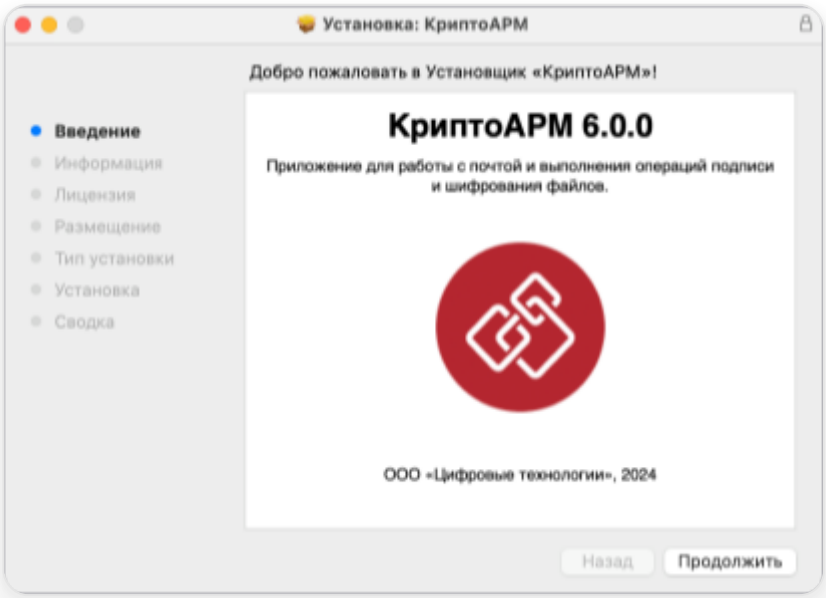
Установка КриптоАРМ на macOS

Вы можете скачать установочный файл на сайте интернет-магазина cryptoarm.ru или на сайте компании-разработчика trusted.ru.

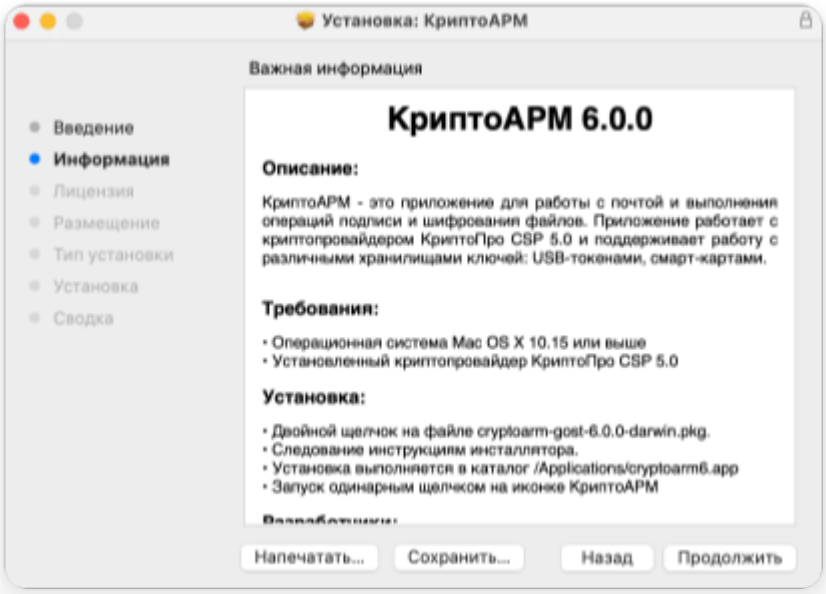
Дистрибутив приложения поставляется в упакованном виде в формате .dmg и представляет собой образ диска, содержащий пакет установки **cryptoarm-x.x.x-x64.pkg,** описание приложения, каталог со скриптами удаления приложения.

1. Для установки пакета через графический интерфейс откройте образ диска с дистрибутивом **cryptoarm-x.x.x-x64.dmg**.
2. Для установки пприложения запустите на исполнение файл **cryptoarm-x.x.x-64.pkg**.

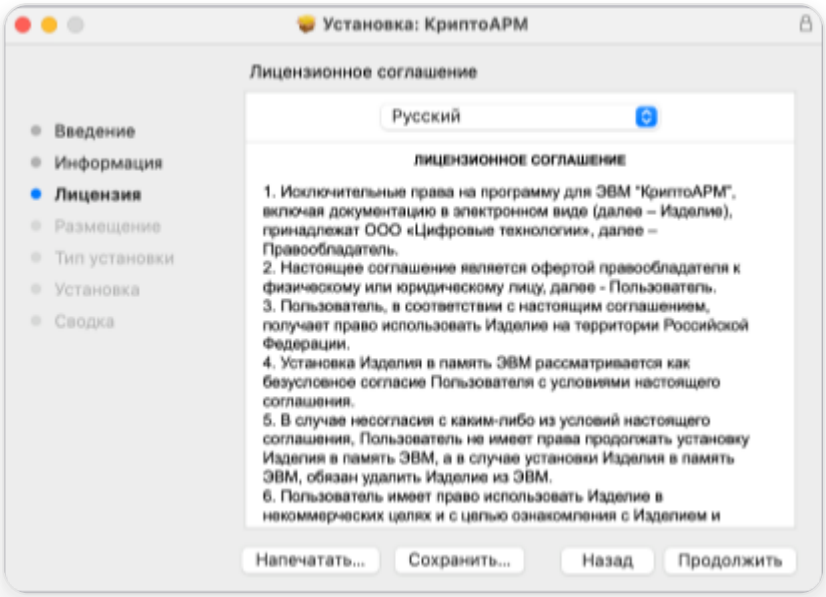
   Установочный пакет для приложения может поставляться вне образа диска. В таком случае нужно сразу запустить файл **cryptoarm-x.x.x-64.pkg** (где x.x.x – номер версии).
3. Откроется мастер установки. Нажмите **Продолжить**.



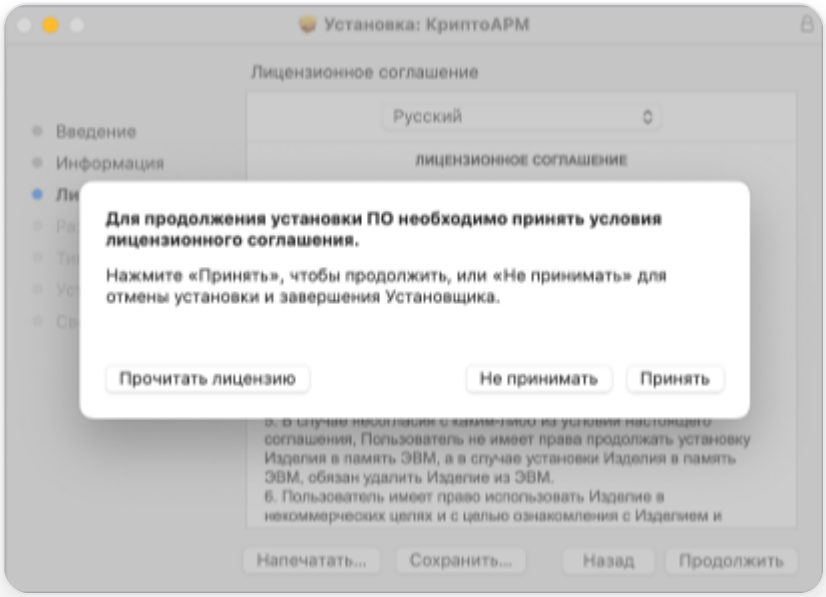
4. Откроется окно с описанием программы. Нажмите **Продолжить**.



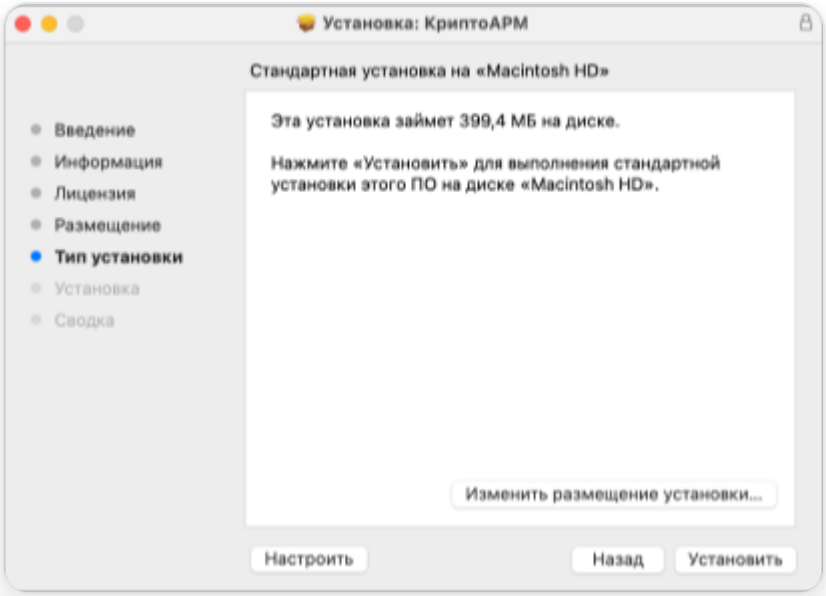
5. Ознакомьтесь с условиями лицензионного соглашения. Нажмите **Продолжить**.



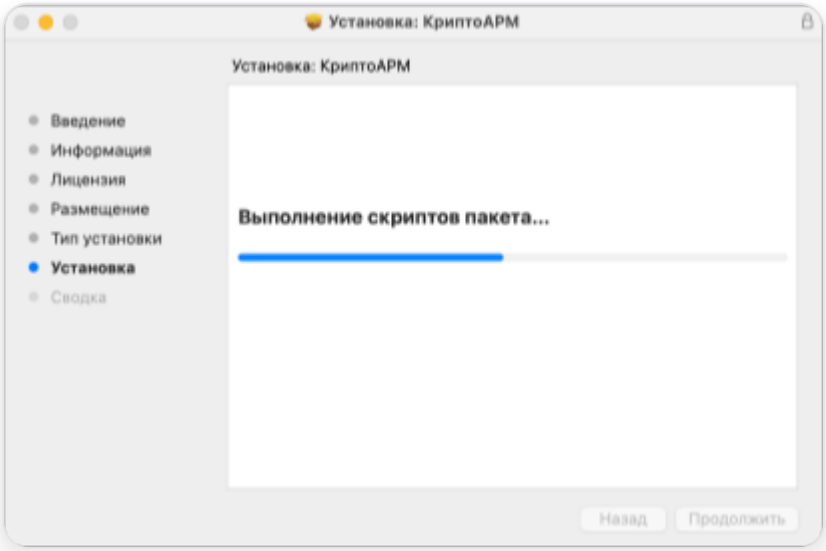
Примите условия лицензионного соглашения по кнопке **Принять**. По кнопке **Не принимать** произойдет отмена установки.



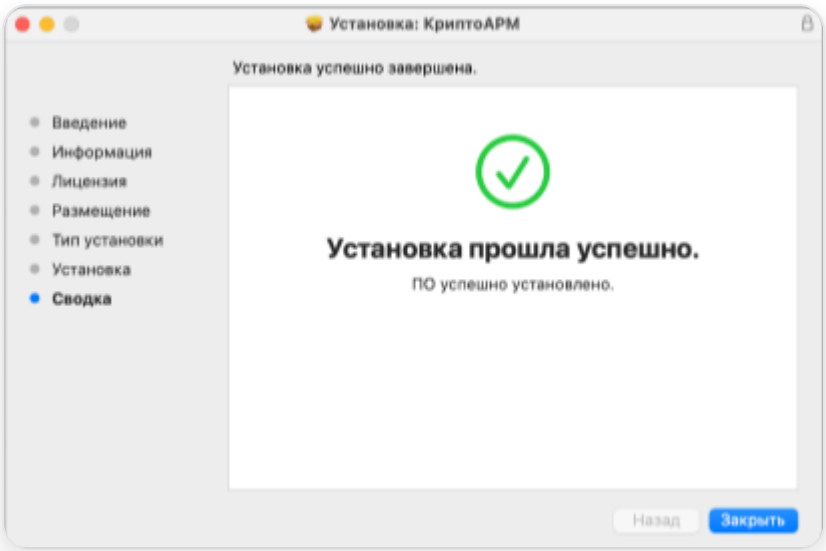
6. На последнем шаге мастера нажмите **Установить** для завершения установки.



Запустится установка программы на компьютер.



7. Закройте окно установки.



После установки программы в Launchpad появится ярлык приложения. В каталоге **Applications** (Программы) будут созданы подкаталоги приложения.

Открыть статью на сайте

Установка КриптоПро CSP на ОС Windows

Как скачать КриптоПро CSP

Скачать установочный файл КриптоПро CSP можно с сайта разработчика — компании «КриптоПро» по ссылке.

Скачивание дистрибутива доступно только после регистрации. Это связано с тем, что криптопровайдер представляет собой средство криптографической защиты информации, а это значит, что его распространение подлежит учету в соответствующих государственных органах.

1. После регистрации или авторизации выберите КриптоПро CSP в Центре загрузки.
2. Откроется страница продукта КриптоПро CSP.
3. Нажмите **Скачать**.
4. Ознакомьтесь и согласитесь с лицензионным соглашением.
5. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

Важно. КриптоАРМ работает с КриптоПро CSP версии 5.0 и выше.

Как установить КриптоПро CSP

1. Запустите установочный файл. При необходимости разрешите программе внести изменения на вашем компьютере.

2. Откроется мастер установки. Нажмите **Установить**.

   В процессе установки может быть выведено окно с условиями лицензионного соглашения и окно по установке лицензионного ключа КриптоПро CSP.

3. После завершения установки закройте мастер и перезагрузите компьютер.

Открыть статью на сайте

Установка КриптоПро CSP на Linux

Как скачать КриптоПро CSP

Скачать установочный файл КриптоПро CSP можно с сайта разработчика — компании «КриптоПро» по ссылке.

Скачивание дистрибутива доступно только после регистрации. Это связано с тем, что криптопровайдер представляет собой средство криптографической защиты информации, а это значит, что его распространение подлежит учету в соответствующих государственных органах.

1. После регистрации или авторизации выберите КриптоПро CSP в Центре загрузки.
2. Откроется страница продукта КриптоПро CSP.
3. Нажмите **Скачать**.
4. Ознакомьтесь и согласитесь с лицензионным соглашением.
5. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

Важно. КриптоАРМ работает с КриптоПро CSP версии 5.0 и выше.

Как установить КриптоПро CSP

Установка, удаление и обновление ПО осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo.

Примечание. Директория расположения утилит КриптоПро CSP /opt/cprocsp/bin/amd64/

Установка базовых пакетов скриптом

В терминале запустите файл **install.sh** или **install_gui.sh** из архива.

Далее описана установка пакетов на примере DEB системы.

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 к файлу>/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 к файлу>/cprocsp-rdr-pcsc-<...>.deb

2. Для ключевого носителя **Рутокен**:

   sudo dpkg -i <путь к файлу>/cprocsp-rdr-rutoken-<...>.deb

   sudo dpkg -i <путь к файлу>/ifd-rutokens_<...>.deb

3. Для ключевого носителя **JaCarta**:

   sudo dpkg -i <путь к файлу>/cprocsp-rdr-jacarta -<...>.deb

4. Для ключевого носителя **ESMART**:

   sudo dpkg -i <путь к файлу>/cprocsp-rdr-esmart -<...>.deb

Установка лицензии на КриптоПро CSP

Установить лицензию можно в разделе Начальная страница приложения КриптоАРМ или в терминале системы.

1. Откройте терминал.

2. Введите лицензию командой:

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

Примечание. Серийный номер следует вводить с соблюдением регистра символов.

Установка пакета для модулей TSP и OCSP

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

1. Скачайте архив **КриптоПро ЭЦП SDK 2.0** по ссылке. Как и в случае с дистрибутивом КриптоПро CSP, для скачивания может потребовать регистрация.
2. Распакуйте архив.

3. Установите пакет:

   sudo dpkg –i <путь к файлу>/cprocsp-pki-x.x.x-amd64-cades.deb

Для создания подписи со штампом времени или усовершенствованной подписи необходима установка лицензии на модули TSP и/или OCSP.

Для проверки подписи лицензии на данные модули устанавливать не нужно.

Установка лицензии на модулей TSP и OCSP

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 к файлу>/cprocsp-rsa-<...>.deb

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

   chmod u+x <путь к скрипту>/script.sh

4. Далее введите команду:

   sudo bash <путь к скрипту>/script.sh

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

Открыть статью на сайте

Установка КриптоПро CSP на macOS

Как скачать КриптоПро CSP

Скачать установочный файл КриптоПро CSP можно с сайта разработчика — компании «КриптоПро» по ссылке.

Скачивание дистрибутива доступно только после регистрации. Это связано с тем, что криптопровайдер представляет собой средство криптографической защиты информации, а это значит, что его распространение подлежит учету в соответствующих государственных органах.

1. После регистрации или авторизации выберите КриптоПро CSP в Центре загрузки.
2. Откроется страница продукта КриптоПро CSP.
3. Нажмите **Скачать**.
4. Ознакомьтесь и согласитесь с лицензионным соглашением.
5. Скачайте дистрибутив в соответствии с установленной операционной системой и её разрядностью.

Важно. КриптоАРМ работает с КриптоПро CSP версии 5.0 и выше.

Как установить КриптоПро CSP

1. Распакуйте загруженный файл macos-uni.tgz.

2. Перейдите в распакованную папку.

   Примечание. Установка осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды 'sudo'.

   При установке КриптоПро CSP сначала устанавливается провайдер, затем устанавливаются остальные модули, входящие в состав комплектации.

   В ОС Mac OS X для установки ПО применяются пакеты (packages). Пакет – архив дистрибутива, содержащий файлы устанавливаемого приложения и файлы, использующиеся инсталлятором для конфигурирования среды.

   Дистрибутив поставляется в упакованном виде, имеет формат .dmg и представляет собой образ диска, содержащий пакет. Для установки пакета откройте двойным щелчком образ диска с дистрибутивом (dmg).

3. Вызовите контекстное меню для файла .dmg и выберите в меню **Открыть**.

4. В открывшемся окне вызовите контекстное меню для файла .pkg и выберите в меню **Открыть**.
5. Появится окно с предупреждением. Нажмите **Продолжить**.

6. В следующем окне нажмите «Разрешить».
7. Ознакомьтесь и примите лицензионное соглашение и продолжите установку.
8. Выберете все установочные пакеты и нажмите **Продолжить — Установить**.
9. После завершения установки закройте мастер установки.

Как установить пакет для модулей TSP и OCSP

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

Скачать архив для **MacOS** можно по ссылке КриптоПро ЭЦП SDK 2.0. Как и в случае с дистрибутивом КриптоПро CSP, для скачивания может потребовать регистрация.

Установите пакет **cprocsp-pki-x.x.x.pkg**, следуя инструкциям на каждом шагу установщика.

Для создания подписи со штампом времени или усовершенствованной подписи необходима установка лицензии на модули TSP и/или OCSP. Установить лицензии можно в разделе Начальная страница приложения КриптоАРМ или в терминале системы.

Для создания классической подписи без штампа времени лицензии на данные модули устанавливать не нужно.

Как активировать лицензии на модули TSP и OCSP в терминале

Для активации лицензий КриптоПро TSP Client и КриптоПро OCSP Client необходимо использовать в Терминале команды вида:

- **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**

где вместо **XXXXX-XXXXX-XXXXX-XXXXX-XXXXX** необходимо указать серийный номер приобретенной лицензии КриптоПро TSP Client и КриптоПро OCSP Client.

При появлении строки **Password** необходимо ввести пароль пользователя macOS (символы вводимого пароля не отображаются) и нажать **Enter**.

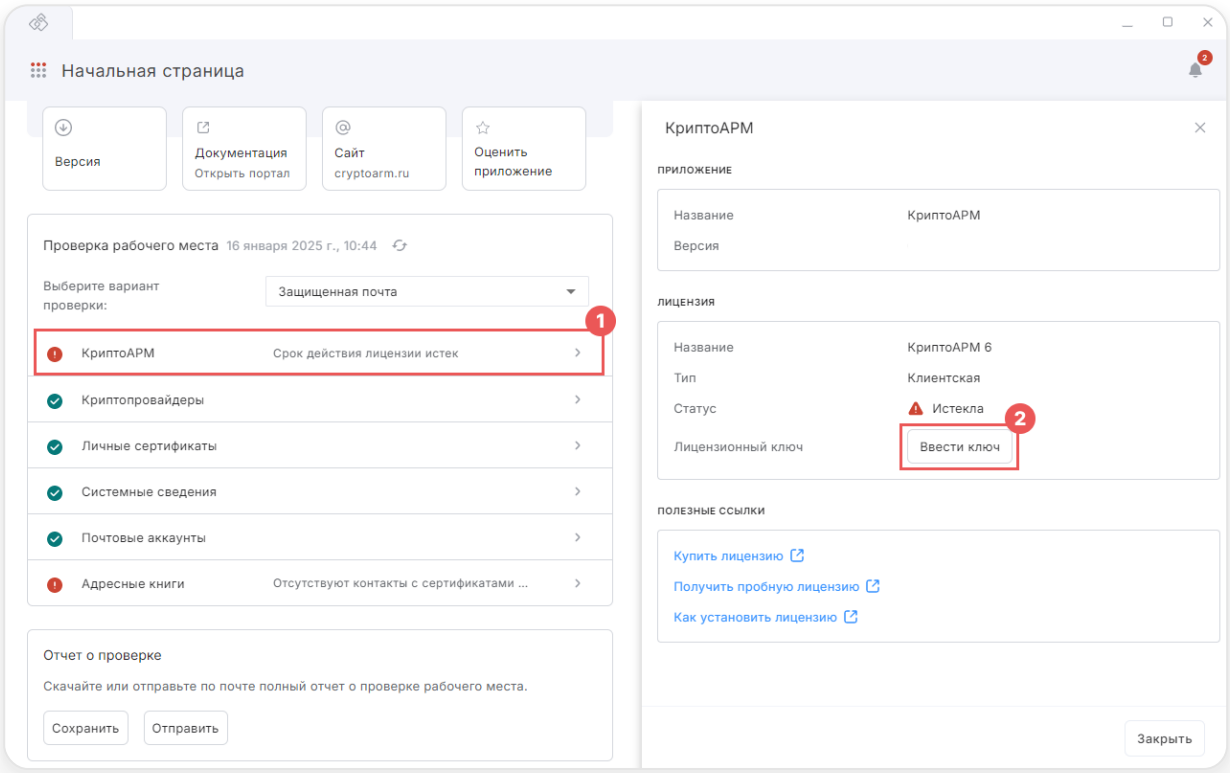
Проверить статус лицензий можно командами:

- **/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/tsputil license**
- **/Applications/CryptoPro_ECP.app/Contents/MacOS/bin/ocsputil license**

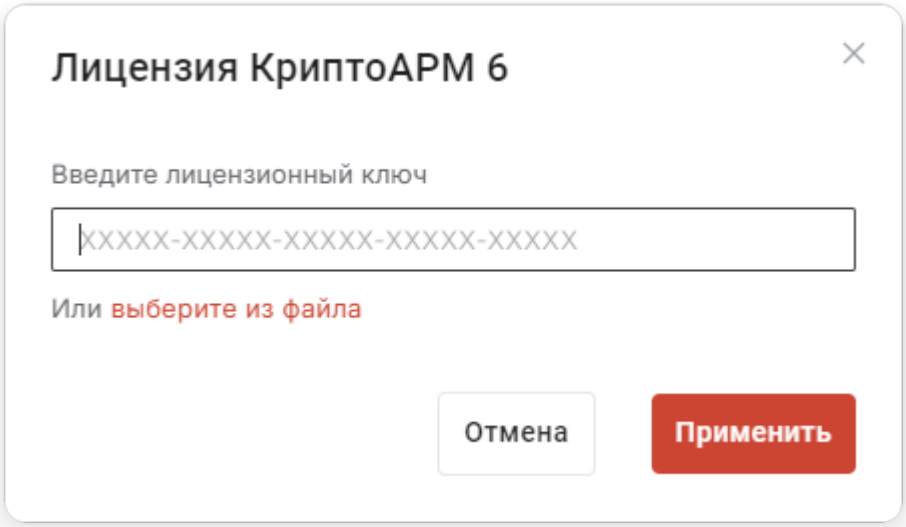
Открыть статью на сайте

Как ввести лицензионный ключ КриптоАРМ

1. Перейдите в раздел **Начальная страница**.
2. Нажмите на панель **КриптоАРМ** в блоке **Проверка рабочего места**.
3. Откроется окно **КриптоАРМ** со сведениями о лицензии.



4. Нажмите на кнопку **Ввести ключ**.
5. В открывшемся окне введите лицензионный ключ или укажите путь к файлу с ним.



6. Нажмите **Применить**.

Дождитесь окончания активации лицензии.

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

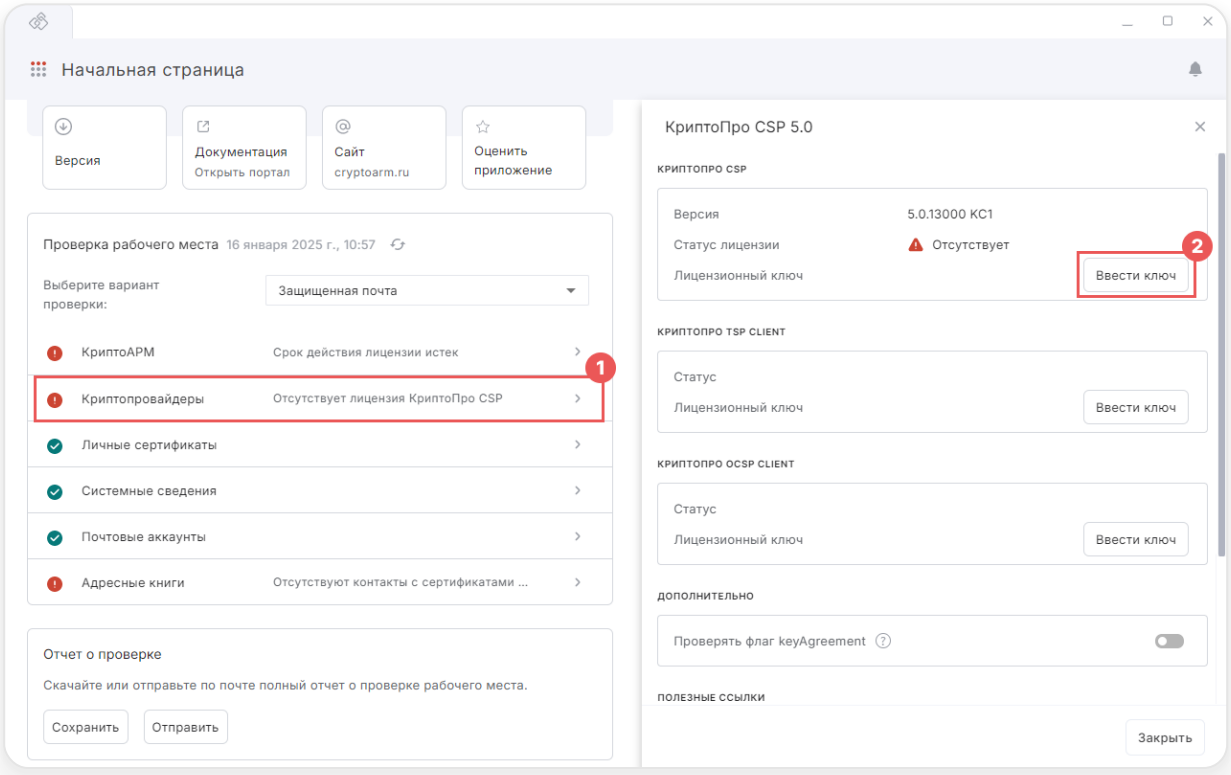
Как узнать статус лицензии КриптоАРМ

1. Перейдите на вкладку **Начальная страница**.
2. Выберите вариант проверки **Полная проверка**, если он не был выбран, и при необходимости запустите повторную проверку.
3. Нажмите на панель **КриптоАРМ**.
4. Откроется окно **КриптоАРМ** со сведениями о лицензии.

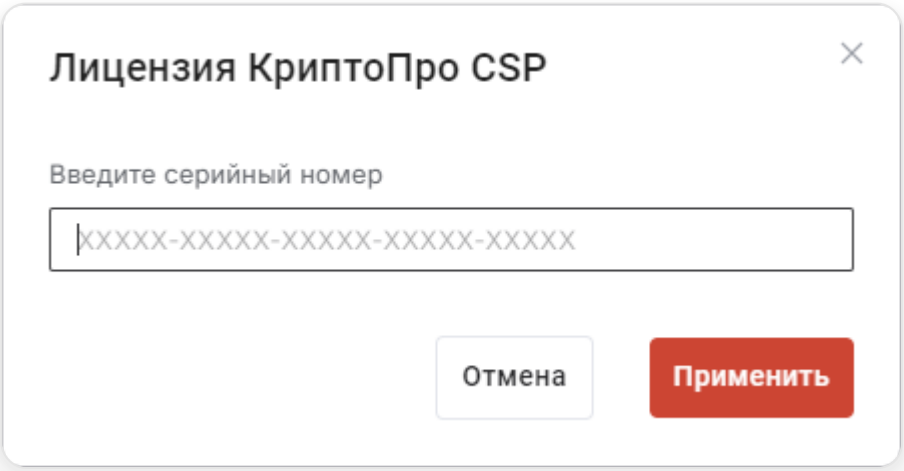
Открыть статью на сайте

Как ввести лицензионный ключ КриптоПро CSP

1. Перейдите в раздел **Начальная страница**.
2. Нажмите на панель **Криптопровайдеры** в блоке **Проверка рабочего места**.
3. Откроется окно со сведениями о лицензиях криптопровайдера КриптоПро CSP, модулей КриптоПро TSP Client и КриптоПро OCSP Client.



4. Нажмите на кнопку **Ввести ключ** в блоке **КриптоПро CSP**.
5. В открывшемся окне введите лицензионный ключ.



6. Нажмите **Применить**.

Дождитесь окончания активации лицензии.

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

Как узнать статус лицензии КриптоПро CSP

1. Перейдите на вкладку **Начальная страница**.
2. Выберите вариант проверки **Полная проверка**, если он не был выбран, и при необходимости запустите повторную проверку.
3. Нажмите на панель **Криптопровайдеры**.
4. Откроется окно **КриптоПро CSP** со сведениями о лицензии.

Открыть статью на сайте

Как ввести лицензионный ключ на модули TSP и OCSP

Ввод лицензии на модули TSP Client и OCSP Client выполняется аналогично установке лицензии на КриптоПро CSP.

Чтобы ввести лицензионный ключ на модули TSP Client и OCSP Client:

1. Перейдите в раздел **Начальная страница**.
2. Нажмите на панель **Криптопровайдеры** в блоке **Проверка рабочего места**.
3. Откроется окно со сведениями о лицензиях криптопровайдера КриптоПро CSP, модулей КриптоПро TSP Client и КриптоПро OCSP Client.
4. Нажмите на кнопку **Ввести ключ** в блоке **КриптоПро TSP Client** или **КриптоПро OCSP Client**.
5. В открывшемся окне введите лицензионный ключ.
6. Нажмите **Применить**.

Дождитесь окончания активации лицензии.

Открыть статью на сайте

Проверка рабочего места

Проверка рабочего места — это удобный инструмент, который позволяет оценить готовность рабочего места для работы с электронной подписью.

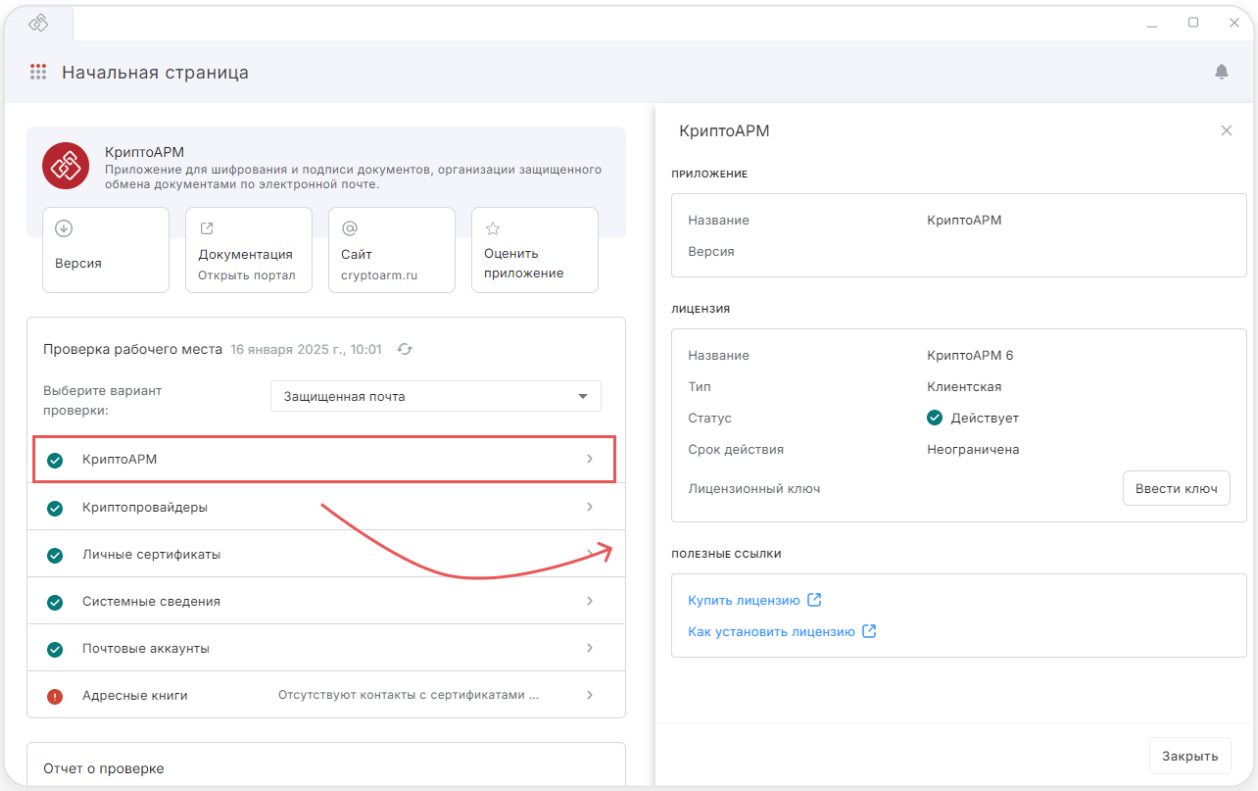
Проверка рабочего места размещена на первой вкладке **Начальная страница**.

В зависимости от цели использования приложения, вы можете выбрать различные варианты проверки:

- **Полная проверка** - проверяются все компоненты приложения на наличие ошибки.
- **Защищенная почта** - проверяются компоненты, отвечающие за обмен подписанными и зашифрованными письмами.
- **Электронная почта** - проверяются компоненты, которые необходимы для отправки писем.
- **Подпись документов со штампами времени** - проверяются компоненты, необходимые для создания подписи со штампом времени.
- **Подпись документов без штампов времени** - проверяются компоненты, необходимые для создания классической подписи.
- **Шифрование документов** - проверяются компоненты, необходимые для шифрования файлов в адрес контактов или сертификатов других пользователей.
- **Расшифрование документов** - проверяются компоненты, задействованные в расшифровании файлов.

Каждый пункт проверки имеет свой статус, который отображается в виде значка.

Чтобы увидеть результаты проверки, необходимо нажать на панель, соответствующую проверке. При просмотре результатов у вас будет возможность исправить выявленные ошибки.



Как запустить проверку

Проверка запускается автоматически при открытии приложения. В любой момент доступен ручной запуск проверки.

Чтобы запустить проверку:

1. Перейдите на вкладку **Начальная страница**.
2. Выберите подходящий вариант проверки в блоке **Проверка рабочего места**.
3. Нажмите на кнопку **Обновить**.
4. Дождитесь завершения проверки.

Отчет о системе

Результаты проверки рабочего места можно сохранить в виде отчёта о системе. Этот отчёт может оказаться полезным, если возникнет необходимость обратиться в техническую поддержку.

Отчёт можно сохранить в виде файла .txt или отправить по электронной почте прямо из приложения.

В файл будет записана следующая информация:

- сведения об операционной системе, процессоре и оперативной памяти;
- сведения о лицензии и версии приложения КриптоАРМ;

- сведения о криптопровайдере КриптоПро CSP и его лицензии;
- общее количество личных действительных сертификатов;
- общее количество контактов;
- сведения о почтовых аккаунтах (количество и протоколы).

Как выгрузить отчет о системе

1. Перейдите на вкладку **Начальная страница**.
2. При необходимости запустите повторную проверку в блоке **Проверка рабочего места**.
3. Выберите одно из действий в блоке **Отчет о проверке**:
    - **Сохранить** - сохранение файла с отчетом на устройстве,
    - **Отправить** - отправка файла с отчетом из приложения.

Открыть статью на сайте

Начало работы с почтой

Раздел **Почта** предназначен для получения, чтения и отправки электронных писем.

Одной из ключевых особенностей почтового клиента в КриптоАРМ является поддержка стандарта S/MIME с использованием ГОСТ-алгоритмов. Это позволяет пользователям подписывать письма вместе с вложениями электронной подписью и шифровать их перед отправкой получателю.

Приложение работает с почтой разных сторонних служб: Mail, Yandex, Gmail, Tegu, iCloud, Communigate Pro, Exchange.

С чего начать

1. Добавьте почтовый аккаунт.
    - Как добавить аккаунт
2. Установите личный сертификат.
    - Как установить сертификат из ключевого контейнера
    - Как установить сертификат из файла .pfx
    - Как установить сертификат из DSS
    - Как создать самоподписанный сертификат
3. Привяжите личный сертификат в почтовому аккаунту.
    - Как привязать сертификат подписи к аккаунту
4. Настройте подпись, которая будет автоматически добавляться в конец каждого отправляемого письма.
    - Как создать подпись
5. Настройте правила обработки входящей почты.
    - Как создать правила сортировки писем
6. Создайте контакты.
    - Как создать контакт
    - Как импортировать контакт из файла vCard
    - Как подключить адресную книгу LDAP
    - Как подключить адресную книгу ALD Pro
    - Как подключить адресную книгу по протоколу CardDAV
    - Как привязать к контакту сертификат

Чтобы оценить, готово ли ваше рабочее место для работы с почтой, воспользуйтесь Проверкой рабочего места.

Важно. Для подписи, шифрования и расшифрования почтовых сообщений необходима лицензия на КриптоАРМ и КриптоПро CSP.

Открыть статью на сайте

Добавление аккаунта

Приложение поддерживает работу с почтой разных сторонних служб: Mail, Yandex, Gmail, Tegu, iCloud, Communigate Pro, Exchange.

Как подключить почтовый аккаунт

Шаг 1. Настройки подключения

1. Перейдите в раздел **Почта**.
2. Нажмите **Добавить аккаунт**:
   - В центре окна, если в приложении не подключены аккаунты.
   - В окне со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Откроется окно **Добавить аккаунт**.
4. Укажите адрес электронной почты и пароль.

   Важно. В качестве пароля от почтового ящика может выступать обычный пароль или специальный пароль приложения, который необходимо создать в настройках почтового сервиса.
5. Укажите протокол, настройки сервера входящей и исходящей почты.

   Примечание. В приложении сохранены шаблоны настроек для популярных почтовых сервисов. При обнаружении шаблона данные для серверов входящей и исходящей почты подставятся автоматически.
6. Нажмите на кнопку **Далее**.

Шаг 2. Настройки почтового ящика

1. Укажите имя аккаунта, которое будет отображаться в приложении.
2. Укажите период, за который необходимо загрузить письма с сервера.
3. Укажите настройки загрузки 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.

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** — на устройство загрузятся дубликаты писем. Письма сохранятся на сервере.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить**.

При успешном подключении аккаунт добавится в приложение и будет запущено получение писем и папок. Данная операция может занять некоторое время.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным. Подробнее в инструкции Изменение активного аккаунта.

Возможные ошибки

Ошибки, которые могут возникнуть при подключении аккаунта, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Ошибка соединения** — проверьте ресурс, к которому настроено подключение. Убедитесь в наличии подключения к Интернету.
2. **Ошибка подключения** — проверьте корректность адреса электронной почты, пароля, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Добавление аккаунта mail.ru

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса. Как создать пароль приложения Mail.ru.

Шаг 2. Настройки подключения

1. Перейдите в раздел **Почта**.
2. Нажмите **Добавить аккаунт**:
    - В центре окна, если в приложении не подключены аккаунты.
    - В окне со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Откроется окно **Добавить аккаунт**.
4. Укажите адрес электронной почты и пароль.
5. Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Mail.ru.
6. Нажмите на кнопку **Далее**.

Шаг 3. Настройки почтового ящика

1. Укажите имя аккаунта, которое будет отображаться в приложении.
2. Укажите период, за который необходимо загрузить письма с сервера.
3. Укажите настройки загрузки 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.
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** — на устройство загрузятся дубликаты писем. Письма сохранятся на сервере.
5. При необходимости настройте специальные папки.

6. Нажмите **Добавить**.

При успешном подключении аккаунт добавится в приложение и будет запущено получение писем и папок. Данная операция может занять некоторое время.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным. Подробнее в инструкции Изменение активного аккаунта.

Возможные ошибки

Ошибки, которые могут возникнуть при подключении аккаунта, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Ошибка соединения** — проверьте ресурс, к которому настроено подключение. Убедитесь в наличии подключения к Интернету.
2. **Ошибка подключения** — проверьте корректность адреса электронной почты, пароля, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Добавление аккаунта yandex.ru

Как подключить почтовый аккаунт

Шаг 1. Настройки в Яндекс Почте

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.

Шаг 2. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса. Как создать пароль приложения Яндекс.

Шаг 3. Настройки подключения

1. Перейдите в раздел **Почта**.
2. Нажмите **Добавить аккаунт**:
    - В центре окна, если в приложении не подключены аккаунты.
    - В окне со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Откроется окно **Добавить аккаунт**.
4. Укажите адрес электронной почты и пароль.
5. Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Яндекс.
6. Нажмите на кнопку **Далее**.

Шаг 4. Настройки почтового ящика

1. Укажите имя аккаунта, которое будет отображаться в приложении.
2. Укажите период, за который необходимо загрузить письма с сервера.
3. Укажите настройки загрузки 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.

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** — на устройство загрузятся дубликаты писем. Письма сохранятся на сервере.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить**.

При успешном подключении аккаунт добавится в приложение и будет запущено получение писем и папок. Данная операция может занять некоторое время.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным. Подробнее в инструкции Изменение активного аккаунта.

Возможные ошибки

Ошибки, которые могут возникнуть при подключении аккаунта, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Ошибка соединения** — проверьте ресурс, к которому настроено подключение. Убедитесь в наличии подключения к Интернету.
2. **Ошибка подключения** — проверьте корректность адреса электронной почты, пароля, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Добавление аккаунта gmail.com

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса. Как создать пароль приложения Gmail.

Шаг 2. Настройки подключения

1. Перейдите в раздел **Почта**.
2. Нажмите **Добавить аккаунт**:
    - В центре окна, если в приложении не подключены аккаунты.
    - В окне со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Откроется окно **Добавить аккаунт**.
4. Укажите адрес электронной почты и пароль.
5. Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Gmail.
6. Нажмите на кнопку **Далее**.

Шаг 3. Настройки почтового ящика

1. Укажите имя аккаунта, которое будет отображаться в приложении.
2. Укажите период, за который необходимо загрузить письма с сервера.
3. Укажите настройки загрузки 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.
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** — на устройство загрузятся дубликаты писем. Письма сохранятся на сервере.
5. При необходимости настройте специальные папки.

6. Нажмите **Добавить**.

При успешном подключении аккаунт добавится в приложение и будет запущено получение писем и папок. Данная операция может занять некоторое время.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным. Подробнее в инструкции Изменение активного аккаунта.

Возможные ошибки

Ошибки, которые могут возникнуть при подключении аккаунта, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Ошибка соединения** — проверьте ресурс, к которому настроено подключение. Убедитесь в наличии подключения к Интернету.
2. **Ошибка подключения** — проверьте корректность адреса электронной почты, пароля, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Добавление аккаунта outlook.com

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса. Как создать пароль приложения Outlook.

Шаг 2. Настройки подключения

1. Перейдите в раздел **Почта**.
2. Нажмите **Добавить аккаунт**:
    - В центре окна, если в приложении не подключены аккаунты.
    - В окне со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Откроется окно **Добавить аккаунт**.
4. Укажите адрес электронной почты и пароль.
5. Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Outlook.
6. Нажмите на кнопку **Далее**.

Шаг 3. Настройки почтового ящика

1. Укажите имя аккаунта, которое будет отображаться в приложении.
2. Укажите период, за который необходимо загрузить письма с сервера.
3. Укажите настройки загрузки 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.
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** — на устройство загрузятся дубликаты писем. Письма сохранятся на сервере.
5. При необходимости настройте специальные папки.

6. Нажмите **Добавить**.

При успешном подключении аккаунт добавится в приложение и будет запущено получение писем и папок. Данная операция может занять некоторое время.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным. Подробнее в инструкции Изменение активного аккаунта.

Возможные ошибки

Ошибки, которые могут возникнуть при подключении аккаунта, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Ошибка соединения** — проверьте ресурс, к которому настроено подключение. Убедитесь в наличии подключения к Интернету.
2. **Ошибка подключения** — проверьте корректность адреса электронной почты, пароля, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Добавление аккаунта icloud.com

Как подключить почтовый аккаунт

Шаг 1. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса. Как создать пароль приложения ICloud.

Шаг 2. Настройки подключения

1. Перейдите в раздел **Почта**.
2. Нажмите **Добавить аккаунт**:
    - В центре окна, если в приложении не подключены аккаунты.
    - В окне со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Откроется окно **Добавить аккаунт**.
4. Укажите адрес электронной почты и пароль.
5. Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки ICloud.
6. Нажмите на кнопку **Далее**.

Шаг 3. Настройки почтового ящика

1. Укажите имя аккаунта, которое будет отображаться в приложении.
2. Укажите период, за который необходимо загрузить письма с сервера.
3. Укажите настройки загрузки 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.
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** — на устройство загрузятся дубликаты писем. Письма сохранятся на сервере.
5. При необходимости настройте специальные папки.

6. Нажмите **Добавить**.

При успешном подключении аккаунт добавится в приложение и будет запущено получение писем и папок. Данная операция может занять некоторое время.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным. Подробнее в инструкции Изменение активного аккаунта.

Возможные ошибки

Ошибки, которые могут возникнуть при подключении аккаунта, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Ошибка соединения** — проверьте ресурс, к которому настроено подключение. Убедитесь в наличии подключения к Интернету.
2. **Ошибка подключения** — проверьте корректность адреса электронной почты, пароля, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Добавление аккаунта rambler.ru

Как подключить почтовый аккаунт

Шаг 1. Настройки в сервисе Rambler

Для работы с письмами через почтовый клиент включите **Доступ к почтовому ящику с помощью почтовых клиентов**. Как включить настройку на сервисе Rambler.

Шаг 2. Создание пароля приложения

В качестве пароля от почтового ящика выступает специальный пароль приложения, который необходимо создать в настройках почтового сервиса. Как создать пароль приложения Rambler.

Шаг 3. Настройки подключения

1. Перейдите в раздел **Почта**.
2. Нажмите **Добавить аккаунт**:
    - В центре окна, если в приложении не подключены аккаунты.
    - В окне со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Откроется окно **Добавить аккаунт**.
4. Укажите адрес электронной почты и пароль.
5. Настройки сервера входящей и исходящей почты будут поставлены автоматически. Если этого не произойдет, заполните их самостоятельно. Ссылка на настройки Rambler.
6. Нажмите на кнопку **Далее**.

Шаг 4. Настройки почтового ящика

1. Укажите имя аккаунта, которое будет отображаться в приложении.
2. Укажите период, за который необходимо загрузить письма с сервера.
3. Укажите настройки загрузки 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.

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** — на устройство загрузятся дубликаты писем. Письма сохранятся на сервере.
5. При необходимости настройте специальные папки.
6. Нажмите **Добавить**.

При успешном подключении аккаунт добавится в приложение и будет запущено получение писем и папок. Данная операция может занять некоторое время.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным. Подробнее в инструкции Изменение активного аккаунта.

Возможные ошибки

Ошибки, которые могут возникнуть при подключении аккаунта, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Ошибка соединения** — проверьте ресурс, к которому настроено подключение. Убедитесь в наличии подключения к Интернету.
2. **Ошибка подключения** — проверьте корректность адреса электронной почты, пароля, настройки сервера входящей и исходящей почты.

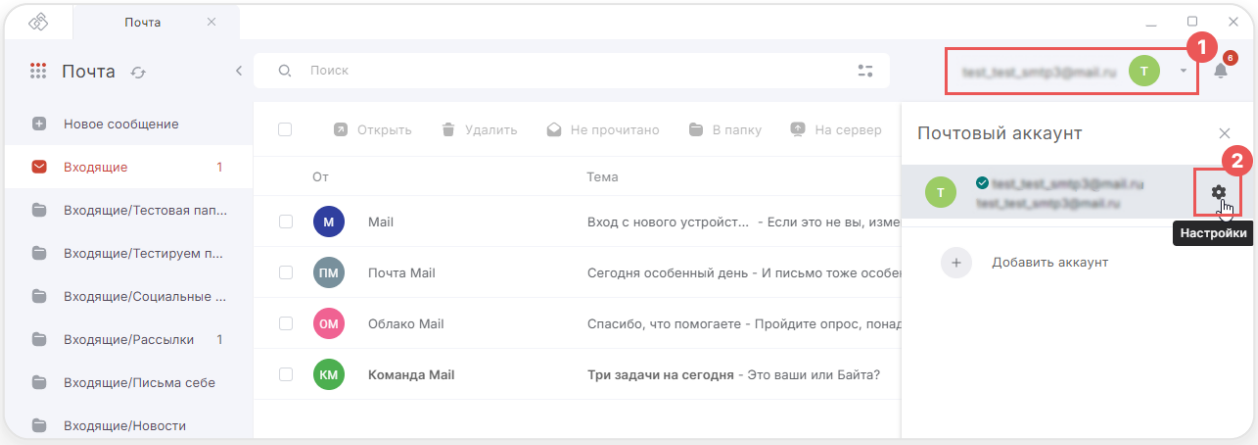
Открыть статью на сайте

Редактирование настроек почты

Вы можете настроить шифрование и электронную подпись сообщений, системные уведомления и изменить другие параметры почты.

Как открыть почтовые настройки

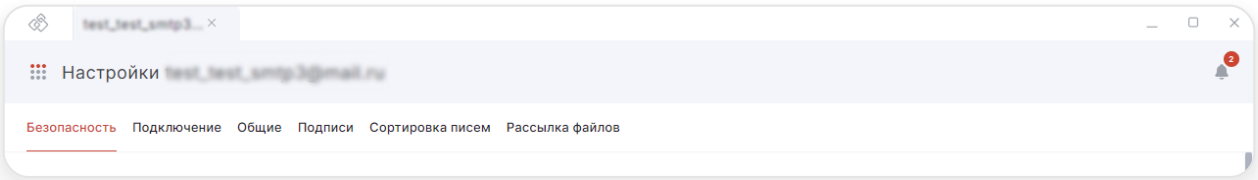
1. Перейдите в раздел **Почта**.
2. Нажмите на имя активного аккаунта в верхнем правом углу окна.
3. Откроется окно со списком аккаунтов.
4. Наведите курсор на аккаунт, настройки которого надо изменить.
5. Нажмите кнопку **Настройки**.
6. Откроется новая вкладка с настройками почтового аккаунта.



О разделе

Настройки состоят из вкладок:

- **Безопасность** — настройки для подписи и шифрования писем.
- **Подключение** — содержит настройки подключения почтового аккаунта.
- **Общие** — показывает настройки действий с входящими сообщениями и уведомлениями о доставке и прочтении.
- **Подписи** — отображает подписи для исходящих писем.
- **Сортировка писем** — содержит настройки для обработки входящей корреспонденции: сортировка по папкам, пересылка писем и автоответчик.
- **Рассылка файлов** — позволяет настроить автоматическую рассылку файлов в виде почтовых писем.



Настройки для подписи и шифрования писем

На вкладке **Безопасность** можно установить настройки для отправки и получения подписанных и зашифрованных писем.

- Как настроить подпись и шифрование исходящих писем
- Как привязать сертификат подписи к аккаунту
- Как настроить отображение информации о сертификате в подписи письма

Также на вкладке доступны дополнительные настройки для скачивания и хранения писем. Подробнее в инструкции Настройки подписи и шифрования писем.

Настройки подключения почтового аккаунта

На вкладке **Подключение** можно отредактировать настройки подключения почтового аккаунта и специальные папки.

Для редактировать доступны поля: **Электронная почта**, **Пароль**, **Сервер входящей почты**, **Сервер исходящей почты**, **Имя аккаунта**, **Забрать письма за**, **Специальные папки**.

Как изменить пароль в почтовом аккаунте

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Подключение**.
3. Укажите новый пароль в блоке **Учетные данные**.
4. Нажмите **Сохранить**.

Если подключение с новым паролем пройдёт успешно, начнётся обмен письмами с почтовым сервером. Это может занять некоторое время.

Общие настройки

На вкладке **Общие** отображаются настройки действий с входящими сообщениями и уведомлениями о доставке и прочтении.

Группировка писем в цепочки

В приложении можно настроить объединение сообщений в цепочки.

Письма объединяются в цепочку, если у них есть общие адресаты, отправители или тема, а также если они содержат заголовок с тем же идентификатором.

В папках цепочки будут отображаться в виде единой строки. Рядом с темой письма будет указываться общее количество сообщений в цепочке.

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Общие**.
3. Включите или отключите переключатель **Группировать письма в цепочки**.

Автоматическое прочтение при просмотре

По умолчанию при быстром просмотре письмо помечается как прочитанное.

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

Запрос уведомлений о прочтении и доставке письма

Уведомление о доставке подтверждает доставку сообщения электронной почты в почтовый ящик получателя, но не гарантирует, что оно было просмотрено или прочитано.

Чтобы узнать, прочитано ли получателем отправленное письмо, можно запросить подтверждение прочтения. Подтверждение будет направлено в виде отдельного письма, в котором будет указана дата и время, когда ваше сообщение было открыто.

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Общие**.
3. Включите или отключите переключатели:
    - Запрашивать уведомление о доставке для всех исходящих сообщений.
    - Запрашивать уведомление о прочтении для всех исходящих сообщений. При выборе данных опций кнопки с запросом уведомлений при написании нового сообщения будут всегда активны.
    - Скрывать уведомления.

Отправка уведомлений о прочтении письма

Чтобы уведомить отправителя о том, что вы прочитали его письмо с уведомлением о прочтении, активируйте функцию отправки таких уведомлений.

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Общие**.
3. Включите или отключите переключатели:
    - Всегда отправлять уведомления о прочтении для любого полученного сообщения.

- Никогда не отправлять уведомления о прочтении.
- Каждый раз спрашивать, следует ли отправить уведомление о прочтении.

Подпись писем

На вкладке **Подписи** можно создать подпись, которая будет автоматически добавляться в конец каждого отправляемого письма.

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

В приложении можно создать несколько подписей для своих писем. При создании нового письма вы можете выбрать нужную подпись или настроить подпись по умолчанию.

Как создать подпись

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Подписи**.
3. Нажмите **Добавить подпись**.
4. Укажите название подписи.
5. Добавьте содержимое подписи:
   - Настройте стиль и размер шрифта, выделить текст курсивом, жирным, подчеркнутым, зачеркнутым.
   - Добавьте изображение. Формат изображения может быть .jpeg, .jpg, .png, .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.

Для удаления подписи наведите курсор мыши на название подписи и нажмите на всплывающую иконку **Удалить подпись**.

Инструкции по теме

1. Как добавить почтовый аккаунт.
2. Как отправить подписанное и зашифрованное сообщение.

3. Как привязать сертификат к контакту.
4. Как установить личный сертификат.
5. Как отправлять электронные письма.
6. Группировка сообщений в цепочки.
7. Как просматривать письма.
8. Как посмотреть уведомления.

Открыть статью на сайте

Настройки подписи и шифрования писем

Настройки для отправки и получения подписанных и зашифрованных писем доступны в настройках почтового аккаунта на вкладке **Безопасность**.

Как настроить подпись и шифрование исходящих писем

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. Активируйте переключатели в блоке **Безопасность почты**:
    - **Шифровать содержимое и вложения исходящих сообщений** - при включенной настройке исходящие письма будут шифроваться в адрес получателей при условии, что к контакту получателя привязан сертификат,
    - **Добавлять электронную подпись к исходящим сообщениям** - при включенной настройке исходящие письма будут подписываться электронной подписью при условии, что в настройках аккаунта выбран сертификат подписи.

Настройки автоматически применяются без дополнительного подтверждения.

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

Как привязать сертификат подписи к аккаунту

При подписи писем используется сертификат, сохраненный в аккаунте.

Примечание. В приложении к аккаунту можно привязать только один сертификат из хранилища «Личные сертификаты».

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. Нажмите **Выбрать сертификат** в блоке **Сертификат подписи**.
4. Откроется окно **Сертификат подписи** со списком личных сертификатов, установленных в приложении.
5. Выберите сертификат.

После выбора сертификат будет автоматически привязан в настройках приложения.

При необходимости привязанный сертификат можно заменить или отвязать.

Как настроить отображение информации о сертификате в подписи письма

В конце каждого исходящего письма можно настроить отображение информации о сертификате подписи: отпечаток, имя владельца и срок действия. Когда вы отправляете подписанное письмо, эти данные автоматически добавляются в конец сообщения. Это позволяет получателям, на устройствах которых не установлено приложение КриптоАРМ, увидеть информацию о сертификате подписи письма.

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Безопасность**.
3. Активируйте переключатель **Отображать информацию об электронной подписи в исходящих письмах** в блоке **Сертификат подписи**.

Настройки автоматически применяются без дополнительного подтверждения.

Шифрование исходящих писем

Для отправки зашифрованных писем доступны дополнительные настройки:

- **Использовать сертификат получателя и сертификат подписи почтового аккаунта** — при включённой настройке исходящие письма будут шифроваться в адрес сертификатов получателей и в адрес сертификата, привязанного к почтовому аккаунту. В папке исходящих писем можно ознакомиться с содержимым зашифрованного отправленного письма.
- **Использовать только сертификат получателя** — при включённой настройке исходящие письма будут шифроваться **только** в адрес сертификатов получателей. В папке исходящих писем расшифровать такое письмо и ознакомиться с его содержанием нельзя.

Хранение входящих зашифрованных сообщений

- **Хранить входящие сообщения в расшифрованном виде** — выбор параметра означает, что все полученные зашифрованные сообщения, которые были хотя бы один раз прочитаны, будут храниться в расшифрованном виде.
- **Хранить входящие сообщения в зашифрованном виде** — выбор параметра означает, что все полученные зашифрованные сообщения, даже прочитанные, 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** (вместе с вложениями) — при получении письмо будет загружено в полном объеме, включая все вложения.

Хранение почты

- **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.

Открыть статью на сайте

Удаление почтового аккаунта

Чтобы удалить почтовый аккаунт в приложении:

1. Перейдите в раздел **Почта**.
2. Откройте окно со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. В списке наведите курсор на почтовый аккаунт, который хотите удалить.
4. Нажмите всплывающую кнопку **Настройки**.
5. Откроется форме просмотра настроек аккаунта.
6. Нажмите кнопку **Удалить**  .
7. Подтвердите удаление.

Если в вашем аккаунте имеются письма в папке «Сохраненные письма», вам необходимо выбрать, как с ними поступить:

- Нет, удалить — все письма будут безвозвратно удалены.
- Да, сохранить — все письма из этого аккаунта сохранятся в папке «Сохраненные письма», а сам аккаунт будет удален из списка подключенных.

Если удалённый аккаунт был выбран активным, то активным становится первый в списке аккаунт.

Инструкции по теме

1. Как сделать почтовый аккаунт активным.
2. Как добавить почтовый аккаунт.

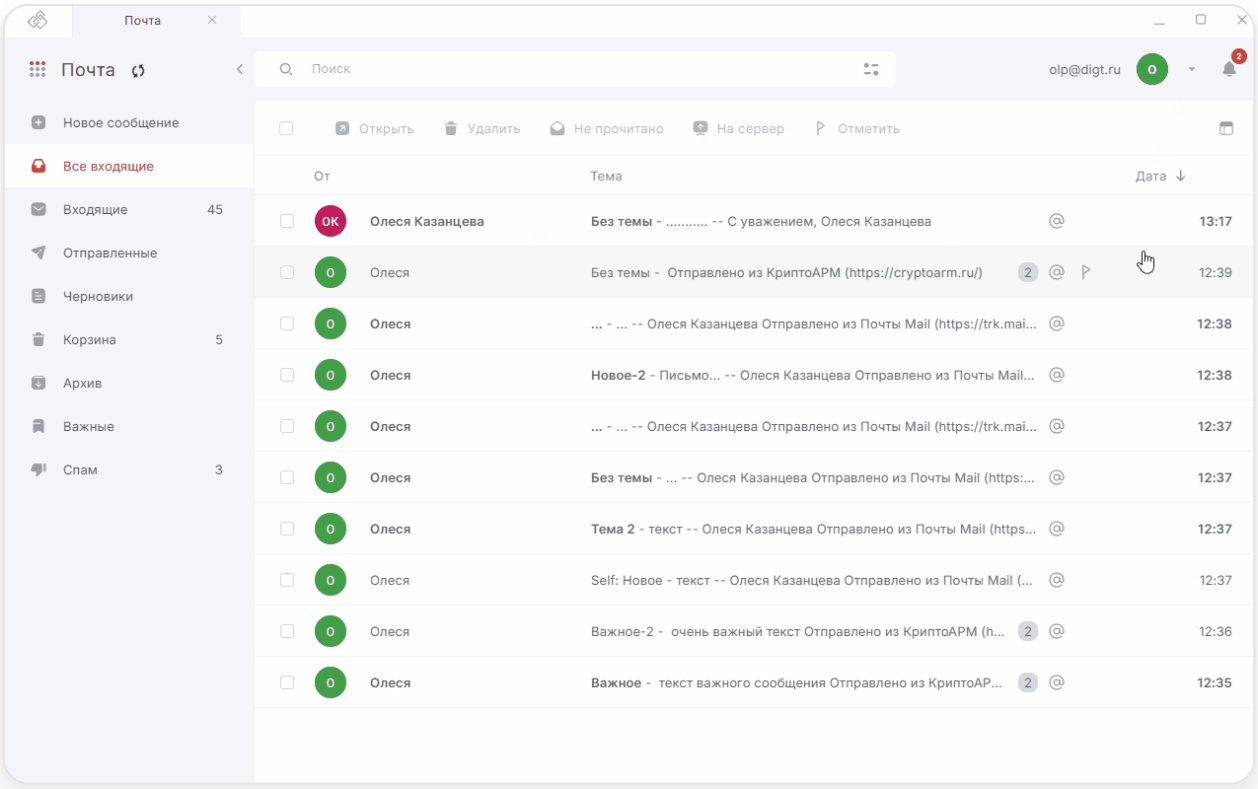
Открыть статью на сайте

Изменение активного аккаунта

Вы можете добавлять несколько почтовых аккаунтов. В таком случае в папке **Все входящие** отображаются входящие письма из всех аккаунтов, а в остальных — письма активного аккаунта.

Как изменить активный аккаунт

1. Перейдите в раздел **Почта**.
2. Откройте окно со списком почтовых аккаунтов, которое вызывается по клику на имя активного аккаунта.
3. Наведите курсор на аккаунт, который хотите сделать активным, и нажмите на его аватар.



Статичный кадр демонстрации. Открыть анимацию

Аккаунт становится активным. В списке писем **Входящие** и вложенных папках отображаются все письма добавленного аккаунта.

Инструкции по теме

1. Как добавить почтовый аккаунт.
2. Как редактировать настройки почты.

Открыть статью на сайте

Просмотр писем

Как открыть письмо

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.

Чтобы открыть письмо в новой вкладке:

1. Перейдите в раздел **Почта**.
2. Выделите письмо в списке писем.
3. Нажмите кнопку **Открыть** на панели действий.
4. Откроется новая вкладка с письмом.

Вложения в письмо

Если в письме есть вложение, то в списке писем оно отображается в виде значка **Скрепка** .

Как скачать вложенный файл на компьютер

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Вызовите меню действий с вложение по кнопке **Еще** .
4. Выберите действие **Скачать файл**.

Как скачать все вложения одним архивом

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Скачать все**, размещенную над вложенными файлами.

Как открыть вложенный файл в мастере

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Вызовите меню действий с вложение по кнопке **Еще** .

4. Выберите мастер из списка.
    - Подпись и шифрование,
    - Проверка и расшифрование,
    - Подпись и защита PDF - мастер доступен для файлов с расширением PDF.

Как просмотреть вложенный файл

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на название вложенного файла.
4. Файл откроется в программе по умолчанию. Если документ подписан электронной подписью и/или зашифрован, то открывается мастер обратных операций.

Просмотр подписанных писем

Важно. Для проверки подписи писем должен быть установлен криптопровайдер КриптоПро CSP.

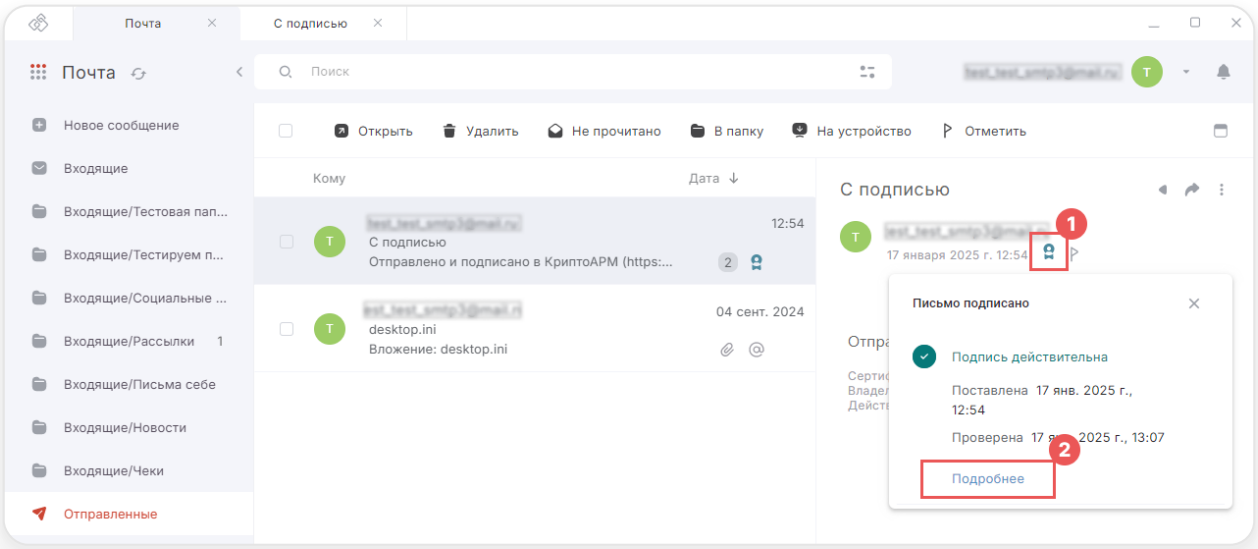
Если письмо содержит подпись, то в списке писем такое письмо помечается иконкой в виде сертификата .

- Для действительной подписи письма иконка отображается с зеленой заливкой ;
- Для недействительной подписи письма иконка отображается с красной заливкой .

Как проверить подпись письма

1. Перейдите в раздел **Почта**.
2. Нажмите на иконку в виде сертификата  на панели с подписанным письмом в списке писем или в окне просмотра письма.
3. Откроется окно со статусом подписи, датой ее постановки и проверки.
4. Нажмите **Подробнее**.

Откроется окно со сведениями о подписи письма.



Причины по которым подпись может быть недействительной:

- Срок действия сертификата истек — в таком случае подпись будет недействительной, такую ситуацию невозможно исправить, только попросить отправителя подписать письмо действительным сертификатом и отправить снова.
- Письмо было изменено с момента подписи — такую ситуацию невозможно исправить, только попросить отправителя подписать письмо снова и отправить.
- Нет доверия к сертификату подписи. Не установлен корневой сертификат — вы можете импортировать корневой сертификат для сертификата отправителя.
- Нет полного доверия к сертификату. Не удалось найти актуальный список отзыва — вы можете импортировать список отзыва сертификатов для сертификата отправителя.

Как обновить сведения о подписи письма

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

1. Выполните шаги из инструкции Как проверить подпись письма.
2. В области просмотра со сведениями о подписи нажмите на кнопку **Обновить**.

Сведения о подписи будут обновлены.

Как распечатать сведения о подписи письма

1. Выполните шаги из инструкции Как проверить подпись письма.
2. В области просмотра со сведениями о подписи нажмите на кнопку **Печать**.
3. Откроется окно с отчетом о проверке подписи письма.

Отчет можно распечатать или скачать на устройство.

Просмотр зашифрованных писем

Важно. Для расшифрования писем требуется действующая лицензия на криптопровайдер КриптоПро CSP и КриптоАРМ.

Для расшифрования письма требуется личный сертификат, в адрес которого письмо зашифровано. Личный сертификат должен быть установлен в «Личном хранилище».

Если письмо зашифровано, то в списке писем такое письмо помечается иконкой в виде замка .

Как расшифровать письмо

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

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

Просмотр отправленных писем с уведомлениями о доставке и прочтении

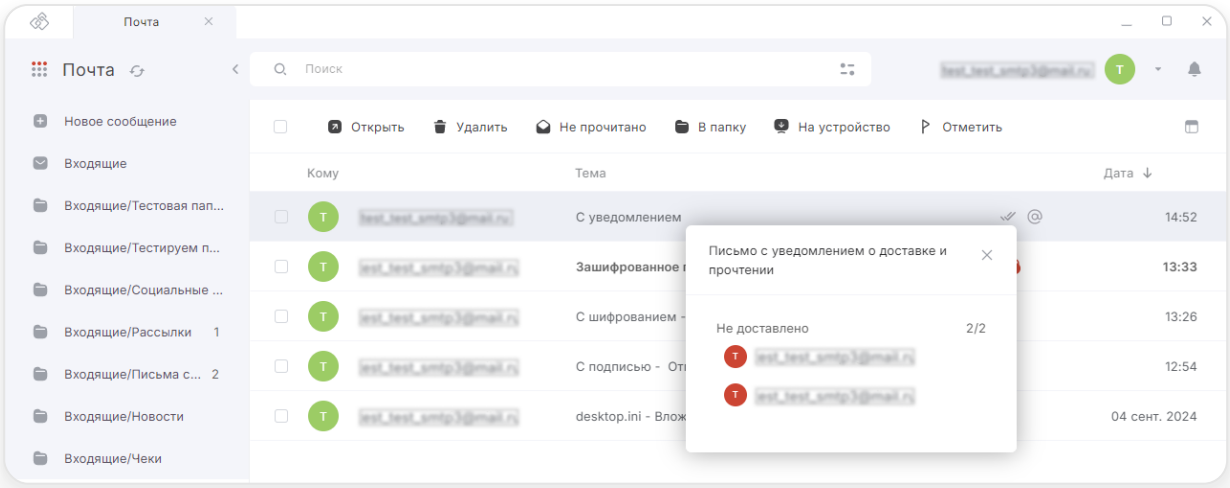
Письмо, отправленное с уведомлением, помечается иконкой в виде галочки .

Для письма с уведомлением возможны несколько статусов:

-  Прочитано всеми/Доставлено
-  Прочитано не всем получателям/Не доставлено
-  Доставлено всем
-  Доставлено не всем получателям.

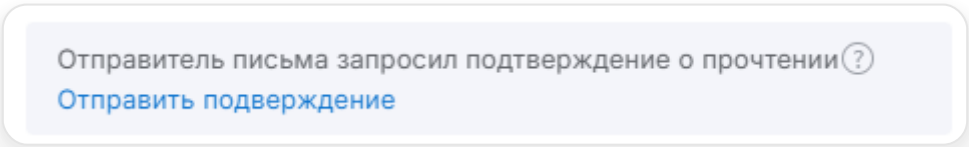
Как узнать доставлено ли письмо

1. Перейдите в раздел **Почта**.
2. Нажмите на иконку в виде галочки  в списке писем или в окне просмотра письма.
3. Откроется окно со сведениями о доставке.



Просмотр входящих писем с уведомлениями о прочтении

Письмо, отправленное вам с уведомлением о прочтении, будет содержать информер с запросом подтверждения о прочтении.



Как отправить подтверждение о прочтении

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

После отправки подтверждения информер будет скрыт из письма.

Инструкции по теме

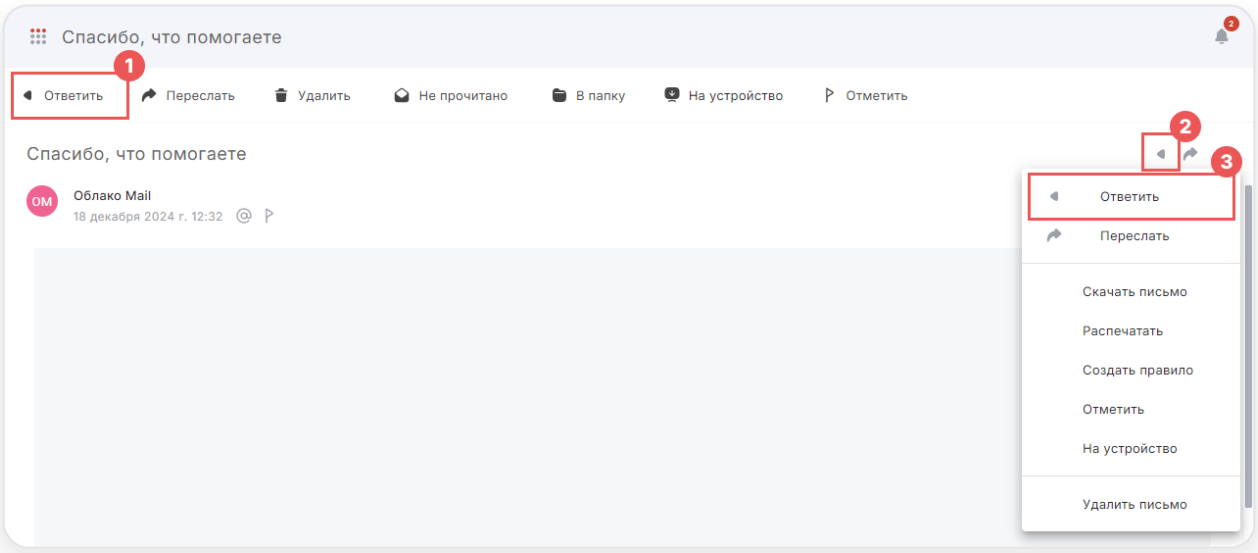
1. Как отправлять электронные письма.
2. Действия с электронными письмами.
3. Как удалять и восстанавливать удаленные письма.

Открыть статью на сайте

Действия с письмами

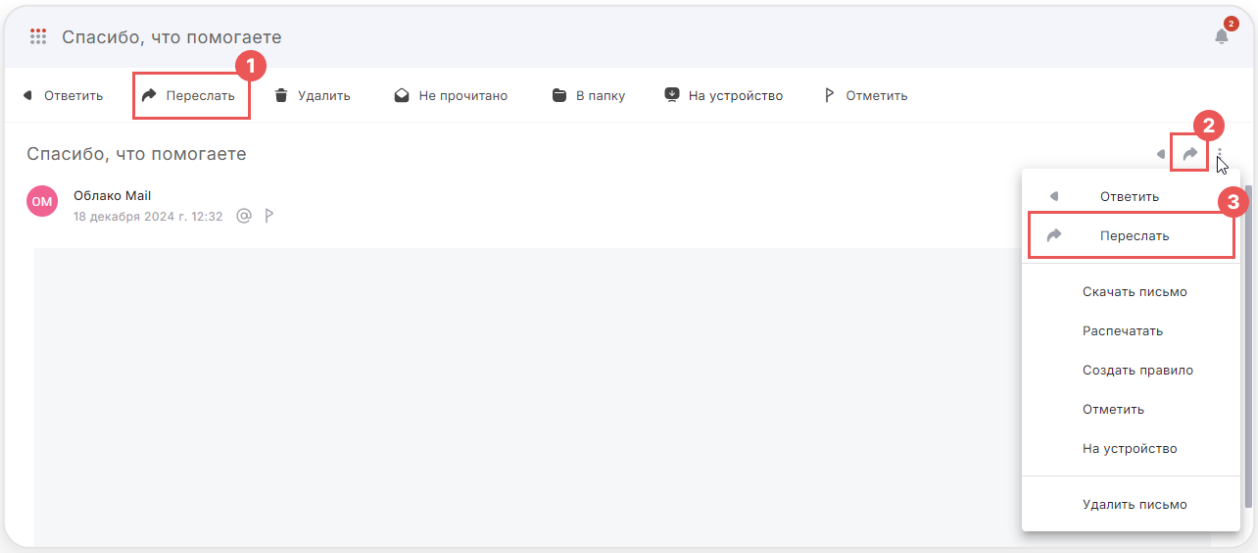
Как ответить на письмо

1. Перейдите в раздел **Почта**.
2. Откройте письмо, на которое нужно ответить.
3. Нажмите на кнопку **Ответить** или **Ответить всем**.
4. Откроется окно **Новое сообщение**.
5. Введите свой ответ.
6. Нажмите **Отправить**.



Как переслать письмо

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Переслать**.
4. Откроется окно **Новое сообщение**.
5. Укажите получателей.
6. Нажмите **Отправить**.



Как поставить отметку Важно

В приложении КриптоАРМ пользователь может отметить одно или несколько писем флагом «Важно». К письму будет присвоена соответствующая метка, которая будет отображаться при просмотре писем в списке, области быстрого просмотра, либо на отдельной вкладке.

При установке отметки «Важно» в программе КриптоАРМ, данная отметка будет отображаться у получателя письма, если получатель тоже использует приложение КриптоАРМ.

Чтобы отметить письмо флагом «Важно» в списке писем:

1. Перейдите в раздел **Почта**.
2. Выделите письмо в списке.
3. Нажмите на кнопку **Отметить**.

Чтобы отметить письмо флагом «Важно» на вкладке просмотра:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Отметить**.

Кнопка **Отметить** меняется на кнопку **Снять отметку**, для писем, отмеченных флагом «Важно». При нажатии на кнопку **Снять отметку**, флаг Важно снимается с письма.

В расширенном поиске по письмам, есть возможность отфильтровать поиск по отметке «Важно».

Как переместить письмо в другую папку

Чтобы переместить одно или несколько писем в списке писем:

1. Перейдите в раздел **Почта**.

2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **В папку**.
4. Откроется окно **Переместить в папку**.
5. Выберите папку, в которую необходимо переместить письма.
6. Нажмите **Переместить**.

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**.

Примечание. Письмо может быть перемещено не только между папками, но и между подключёнными аккаунтами.

Как скачать письмо

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.

Как распечатать письмо.

1. Откройте письмо.
2. Вызовите меню действий с письмом по кнопке **Еще**.
3. Выберите действие **Распечатать**.
4. Укажите место для сохранения файла с письмом.

Инструкции по теме

1. Как открыть письмо.
2. Как отправлять электронные письма.
3. Как расшифровать документ.
4. Как снять подпись с документа.
5. Как проверить подпись документа.
6. Как установить корневой и промежуточный сертификаты.
7. Как импортировать список отзыва сертификатов (COC).
8. Как установить личный сертификат.
9. Как удалять и восстанавливать удаленные письма.

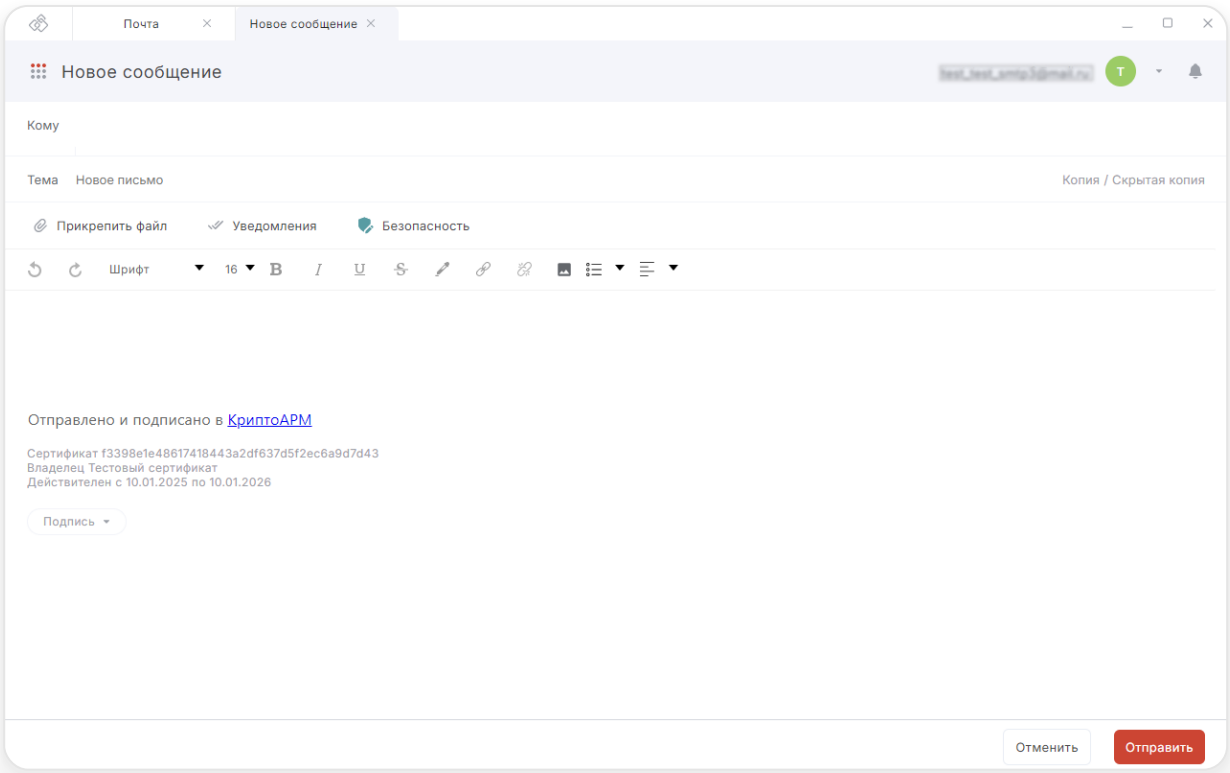
10. Группировка сообщений в цепочки.

Открыть статью на сайте

Отправка письма

Как отправить письмо

1. Перейдите в раздел **Почта**.
2. В боковом меню нажмите на кнопку **Новое сообщение**.
3. Откроется вкладка **Новое сообщение**.
4. Добавьте получателей в поле «Кому», также получателей можно добавить в поле «Копия» или «Скрытая копия». Адреса получателей можно ввести вручную через запятую, точку с запятой, пробел или выбрать из адресной книги раздела **Контакты**.
5. Укажите тему, содержимое и настройте подпись письма.
6. Добавьте вложения (при необходимости). Инструкция Как добавить вложение.
7. Выставите настройки для отправки письма с уведомлениями. Инструкция Как отправить письмо с уведомлениями.
8. Выставите настройки для отправки письма с подписью и шифрованием. Инструкция Как отправить подписанное и зашифрованное письмо.
9. Нажмите **Отправить**.



Оформление сообщения

Для оформления сообщения доступны инструменты:

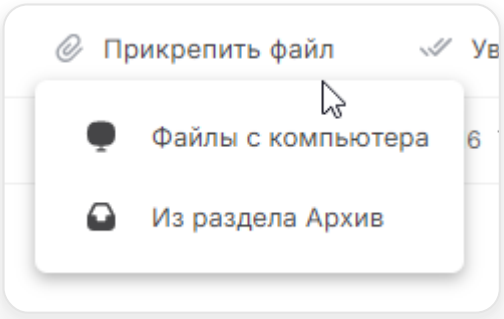
- выбор стиля шрифта;
- размер шрифта;
- выделение текста курсивом, жирным, подчеркнутым, зачеркнутым;
- изменение цвета шрифта текста, фона;
- формирование ссылки в тексте;
- добавление изображения в тело письма;
- маркированный список, нумерованный список и отступы;
- выравнивание шрифта (слева, справа, по центру, выровнять).

Инструменты для оформления текста письма расположены выше области для содержимого.



Как добавить вложение в письмо

1. Перейдите в раздел **Почта**.
2. В боковом меню нажмите на кнопку **Новое сообщение**.
3. Откроется вкладка **Новое сообщение**.
4. Нажмите на **Прикрепить файл**.
5. Выберите одно из действий в выпадающем меню:
   - Файлы с компьютера - для выбора файлов с локального диска.
   - Из раздела Архив - для выбора файлов, сохраненных в папке «Архив» раздела **Документы**.



6. После выбора файлы отобразятся в теле письма.

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

Для удаления ошибочно добавленного вложения нажмите кнопку **Удалить**. Для удаления всех вложений нажмите **Удалить все**.

Для просмотра содержимого добавленного документа нажмите на него, он открывается в приложении, ассоциируемом с расширением документа.

Как сохранить черновик

Черновики писем автоматически сохраняются в папке «Черновики» каждые 10 секунд.

Чтобы продолжить работу с черновиком, просто откройте его.

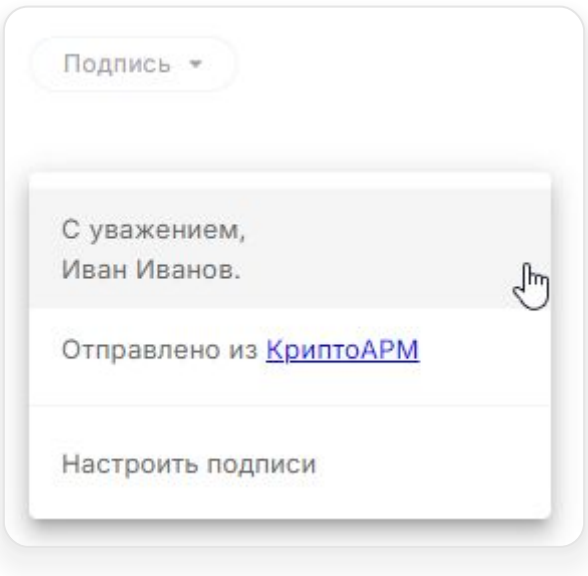
Как выбрать другую подпись письма

Подписи создаются в настройках почты. Подробнее в инструкции Как создать подпись.

По умолчанию в приложении задана дефолтная подпись с текстовкой **Отправлено из КриптоАРМ** и ссылкой на магазин cryptoarm.ru.

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

Если у вас несколько подписей, то на форме нового письма вам доступна возможность выбора подписи с помощью кнопки:



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

Возможные уведомления

Ошибки, которые могут возникнуть при отправке письма, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Укажите получателей письма в полях Кому, Копия или Скрытая копия** — проверьте заполнение указанных полей.
2. **Адреса user@aa не распознаны. Проверьте правильность ввода адресов** — проверьте электронные адреса получателей на корректность.
3. **Не удалось отправить сообщение** — проверьте подключение к Интернету.
4. **Ошибка при отправке** — проверьте, включены ли уведомления о доставке/прочтении письма и все ли почтовые сервера получателей поддерживают автоматические уведомления о доставке.
5. **Ошибка соединения** — проверьте настройки сервера исходящей почты.

Инструкции по теме

1. Как добавить почтовый аккаунт.
2. Как отправить подписанное и зашифрованное сообщение.
3. Как настроить отправку писем с уведомлениями о доставке и прочтении.
4. Как редактировать настройки почты.
5. Группировка сообщений в цепочки.
6. Как создать контакт.
7. Как посмотреть уведомления.

Открыть статью на сайте

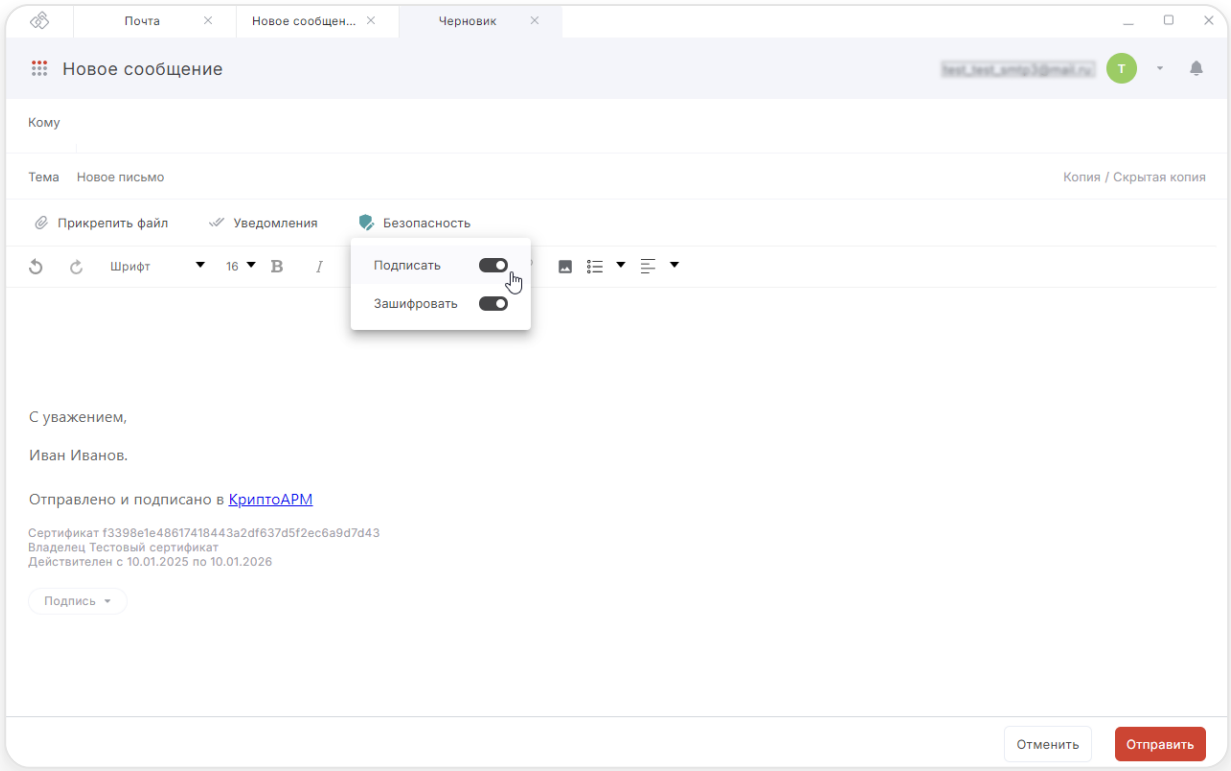
Отправка подписанного и зашифрованного письма

Чтобы отправлять подписанные и/или зашифрованные письма, убедитесь в том, что приложение настроено для работы с защищенной почтой. Подробнее в инструкции Начало работы с почтой.

Важно. Для подписи, шифрования и расшифрования почтовых сообщений необходима лицензия на КриптоАРМ и КриптоПро CSP.

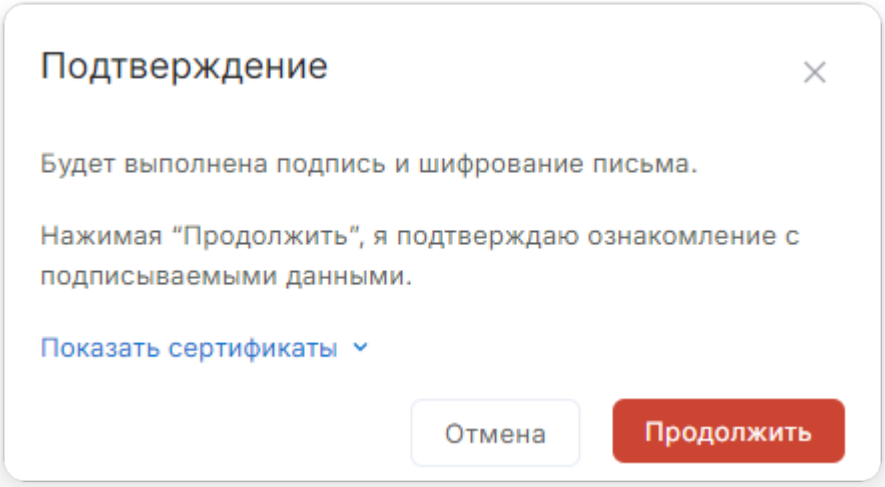
Как отправить подписанное и зашифрованное сообщение

1. Перейдите в раздел **Почта**.
2. В боковом меню нажмите на кнопку **Новое сообщение**.
3. Откроется вкладка **Новое сообщение**.
4. Добавьте получателей в поле «Кому», также получателей можно добавить в поле «Копия» или «Скрытая копия». Адреса получателей можно ввести вручную через запятую, точку с запятой, пробел или выбрать из адресной книги раздела **Контакты**.
5. Укажите тему, содержимое и настройте подпись письма.
6. Добавьте вложения (при необходимости). Инструкция Как добавить вложение.
7. Выставите настройки для отправки письма с уведомлениями. Инструкция Как отправить письмо с уведомлениями.
8. Выставите настройки для отправки письма с подписью и шифрованием.
    - Подписать - для отправки подписанного письма,
    - Зашифровать - для отправки зашифрованного письма.



9. Нажмите **Отправить**.

10. Подтвердите действие в модальном окне. При необходимости в этом окне можно просмотреть сертификаты, которые будут использоваться для подписи и шифрования.



Примечание. Настройки **Подписать** и **Зашифровать** можно заранее установить в настройках почтового аккаунта. Подробнее в инструкции Настройки подписи и шифрования писем.

Возможные уведомления

Ошибки, которые могут возникнуть при отправке письма, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. Укажите получателей письма в полях Кому, Копия или Скрытая копия — проверьте заполнение указанных полей.
2. Адреса user@aa не распознаны. Проверьте правильность ввода адресов - проверьте электронные адреса получателей на корректность.
3. Не найден личный сертификат электронной подписи — вы можете отправить неподписанное письмо или вернуться к письму и выбрать сертификат подписи в настройках почты, а затем отправить письмо снова.
4. Личный сертификат недействителен — вы можете подписать письмо недействительным сертификатом или вернуться к письму и заменить сертификат подписи в настройках почты, а затем отправить письмо снова.
5. Один или несколько сертификатов отсутствуют — проверьте наличие сертификатов у получателей, добавьте сертификаты к контактам и повторите отправку письма.
6. Не удалось отправить сообщение — проверьте подключение к Интернету.

Инструкции по теме

1. Установка КриптоПро CSP на платформу Windows.
2. Установка КриптоПро CSP на платформу Linux.
3. Как установить личный сертификат.
4. Как привязать сертификат к контакту.
5. Как отправлять электронные письма.
6. Как редактировать настройки почты.
7. Как настроить отправку писем с уведомлениями о доставке и прочтении.
8. Как посмотреть уведомления.

Открыть статью на сайте

Отправка письма с уведомлениями

В приложении доступна отправка письма со следующими уведомлениями:

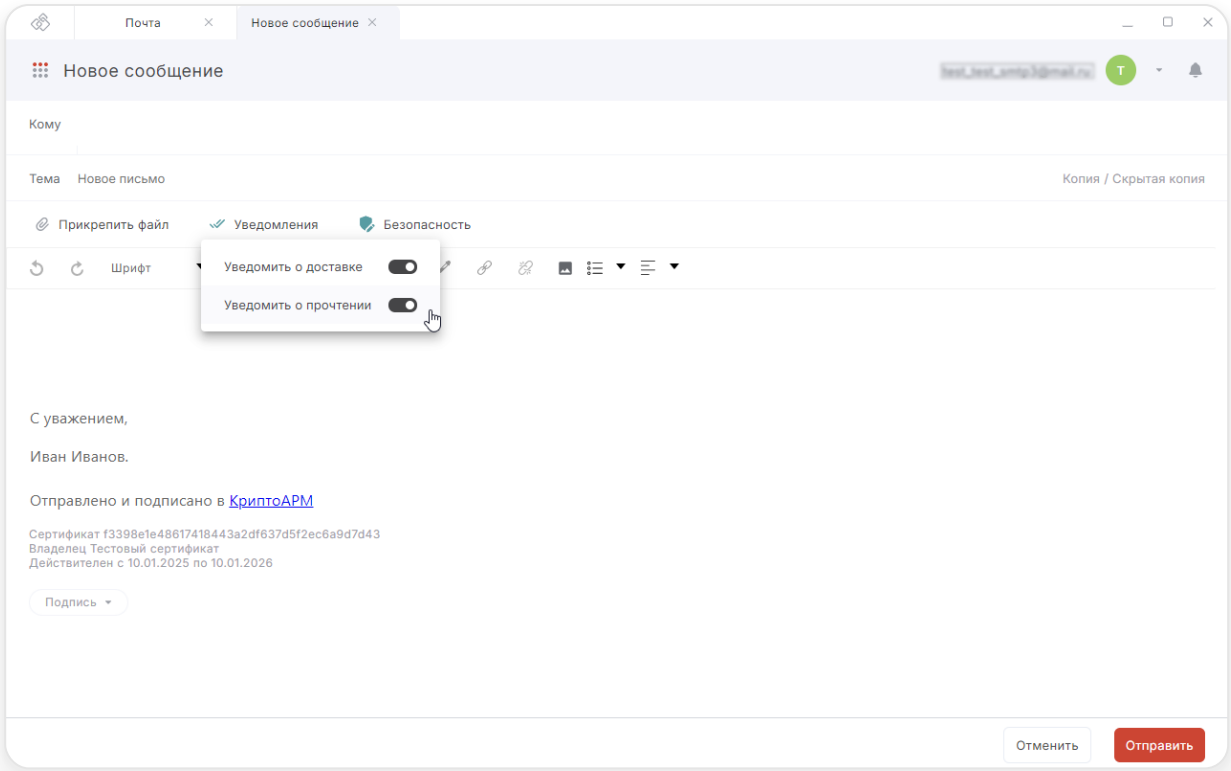
- **Уведомление о доставке** - уведомление подтверждает доставку сообщения в почтовый ящик получателя, но не гарантирует, что оно было просмотрено или прочитано.
- **Уведомление о прочтении** - уведомление подтверждает прочтение письма получателем. Подтверждение будет направлено в виде отдельного письма, в котором будет указана дата и время, когда ваше сообщение было открыто.

Важно. Подтверждение о доставке или прочтении не всегда означает, что письмо доставлено и прочитано.

Даже если вы получили уведомление о прочтении вашего письма, это не всегда означает, что адресат действительно ознакомился с ним. Способ работы с подтверждениями может отличаться в зависимости от почтовой системы, которую использует получатель. Например, вам может прийти уведомление о прочтении, если пользователь почтового клиента IMAP пометил ваше сообщение как прочитанное, не открывая его. Некоторые почтовые системы для мобильных устройств, которые не используют протокол IMAP, могут не отправлять такие подтверждения.

Как отправить письмо с уведомлениями

1. Перейдите в раздел **Почта**.
2. В боковом меню нажмите на кнопку **Новое сообщение**.
3. Откроется вкладка **Новое сообщение**.
4. Добавьте получателей в поле «Кому», также получателей можно добавить в поле «Копия» или «Скрытая копия». Адреса получателей можно ввести вручную через запятую, точку с запятой, пробел или выбрать из адресной книги раздела **Контакты**.
5. Укажите тему, содержимое и настройте подпись письма.
6. Добавьте вложения (при необходимости). Инструкция Как добавить вложение.
7. Выставите настройки для отправки письма с уведомлениями:
    - Уведомить о доставке,
    - Уведомить о прочтении.
8. Выставите настройки для отправки письма с подписью и шифрованием. Инструкция Как отправить подписанное и зашифрованное письмо.



9. Нажмите **Отправить**.

Примечание. Настройки **Уведомить о доставке** и **Уведомить о прочтении** можно заранее установить в настройках почтового аккаунта. Подробнее в инструкции Редактирование настроек почты.

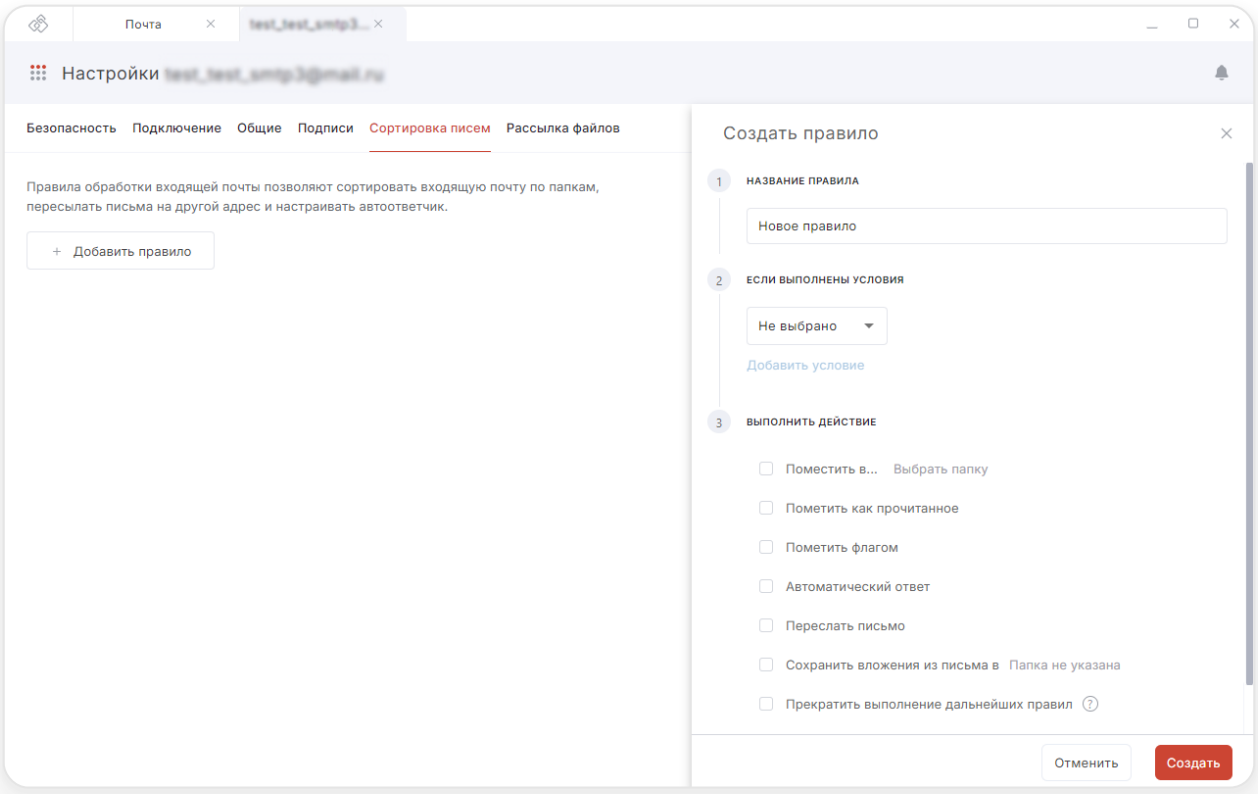
Открыть статью на сайте

Сортировка писем

В приложении можно настроить правила обработки входящих писем для автоматической сортировки электронных сообщений.

Как создать правило сортировки

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
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:
   - от кого;
   - кому;
   - тема письма;
   - содержание письма;
   - дата получения;
   - название вложения;
   - статус;
   - размер;
   - ко всем входящим письмам.
7. Укажите действие, которое необходимо выполнить с письмом:
   - поместить в выбранную папку;
   - пометить как прочитанное;
   - направить автоматический ответ с набранным текстом;
   - переслать письмо, указав получателя;
   - сохранить вложения из письма в выбранную папку;
   - прекратить выполнение дальнейших правил — все правила, которые находятся ниже, будут игнорироваться. Правила, расположенные выше, выполняются по умолчанию;
   - применить к существующим письмам.
8. Нажмите **Создать**.



Как создать правило сортировки из 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**.

Открыть статью на сайте

Группировка писем в цепочки

В приложении можно настроить объединение сообщений в цепочки.

Письма объединяются в цепочку, если у них есть общие адресаты, отправители или тема, а также если они содержат заголовок с тем же идентификатором.

В папках цепочки будут отображаться в виде единой строки. Рядом с темой письма будет указываться общее количество сообщений в цепочке.

Если в цепочке более четырех писем, в интерфейсе отображается первое и два последних письма, промежуточные скрываются.

Как включить группировку писем

Чтобы настроить группировку писем в цепочки, перейдите в настройки почтового аккаунта. Подробнее в инструкции Редактирование почтового аккаунта.

Инструкции по теме

1. Как редактировать настройки почты.
2. Как просматривать письма.

Открыть статью на сайте

Удаление и восстановление писем

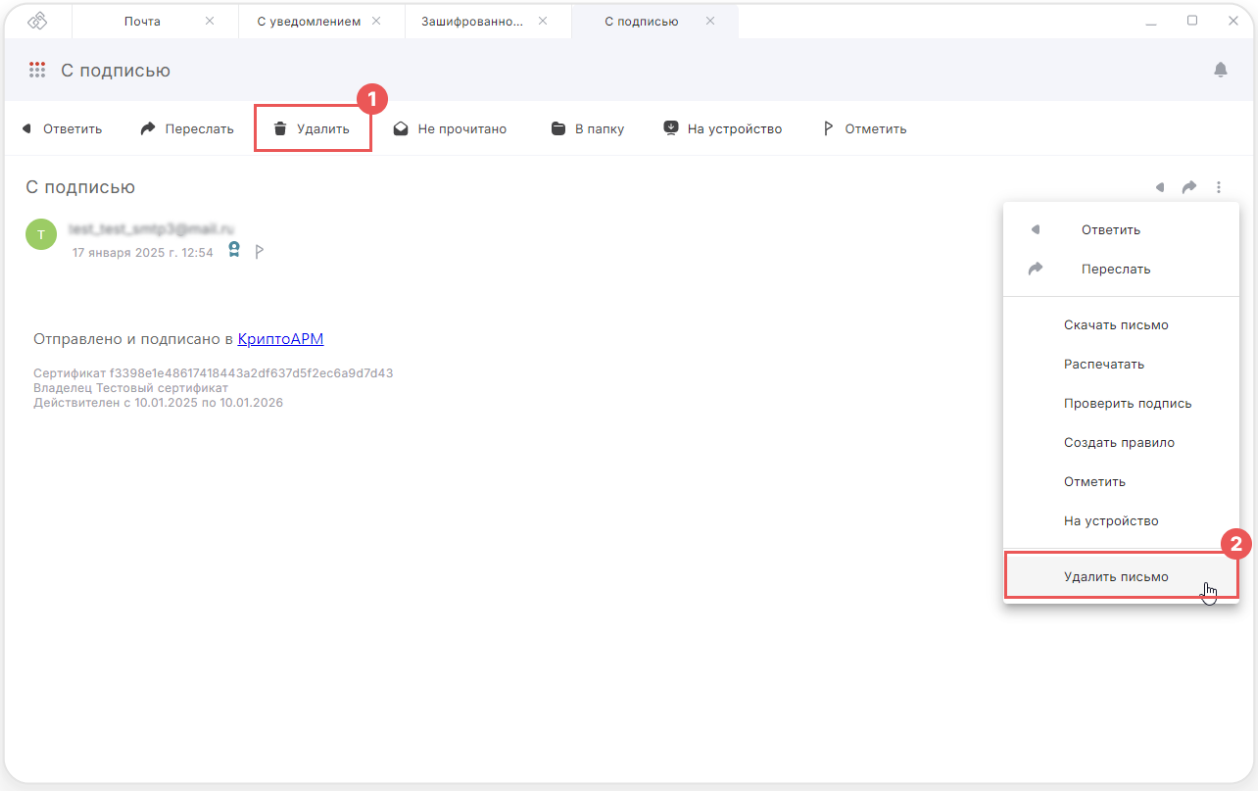
Как удалить письмо

Чтобы удалить одно или несколько писем в списке писем:

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **Удалить** на панели действий.
4. Письма будут перемещены в «Корзину».

Чтобы удалить письмо на вкладке просмотра:

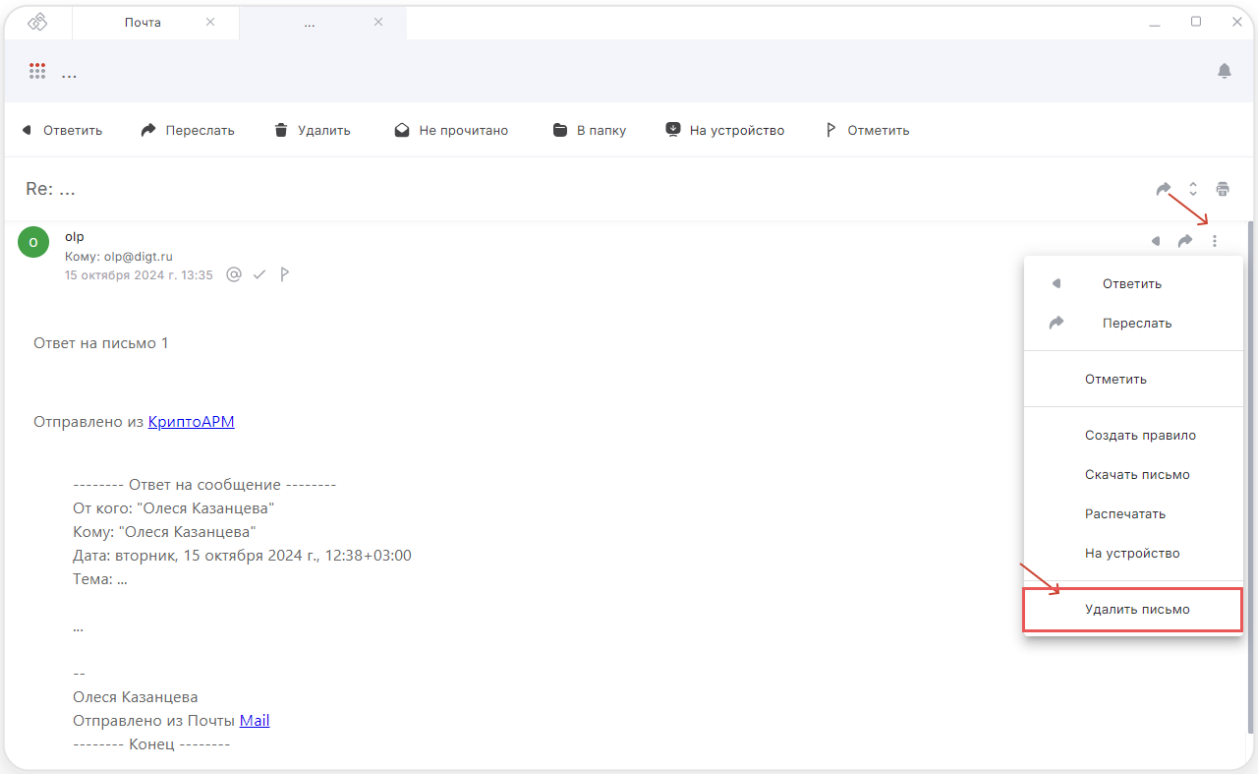
1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **Удалить**.
4. Письмо будет перемещены в «Корзину».



Как удалить письмо из цепочки

1. Перейдите в раздел **Почта**.
2. Откройте цепочку писем.
3. Вызовите меню действий для письма. которое необходио удалить по кнопке **Еще**.

4. Нажмите на кнопку **Удалить**.
5. Письмо будет перемещены в «Корзину».



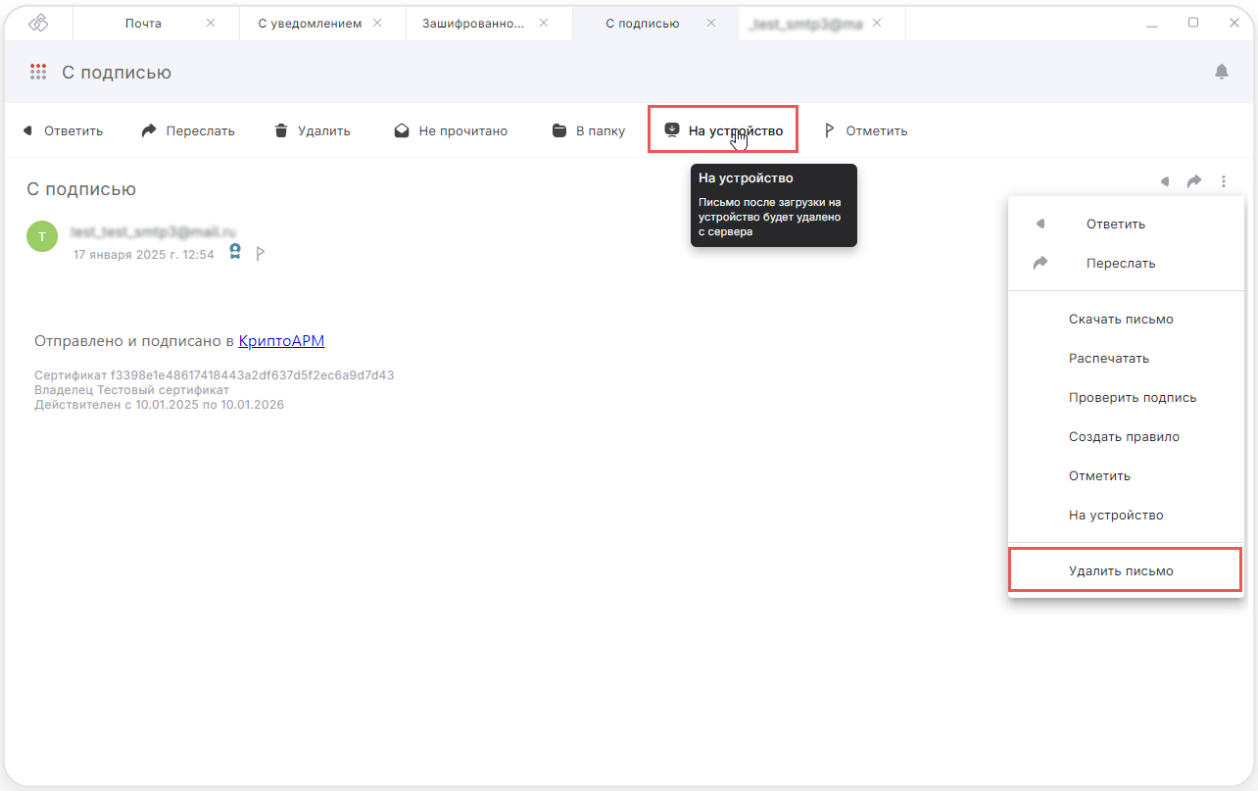
Как удалить письма с почтового сервера

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

1. Перейдите в раздел **Почта**.
2. Выделите одно или несколько писем в списке.
3. Нажмите на кнопку **На устройство** на панели действий.
4. Письма будут перемещены с сервера на устройство.

Чтобы переместить письмо с почтового сервера на устройство на вкладке просмотра:

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на кнопку **На устройство**.
4. Письмо будет перемещено с сервера на устройство.



Письмо, перемещенное с сервера на устройство, хранится локально в папке **Сохранённые письма**.

При необходимости письмо можно вернуть обратно на сервер.

Как очистить корзину

1. Перейдите в раздел **Почта**.
2. Откройте папку **Корзина**.
3. Установите флажки напротив писем, которые хотите навсегда удалить.
4. Нажмите **Удалить навсегда**.
5. Подтведите действие в модальном окне.

Как восстановить письма

Если вы переместили письмо в «Корзину», его можно восстановить.

1. Перейдите в раздел **Почта**.
2. Откройте папку **Корзина**.
3. Установите флажки напротив писем, которые хотите восстановить.
4. Нажмите на кнопку **В папку** на панели действий.
5. Откроется окно со списком папок.
6. Выберите нужную папку.
7. Нажмите **Переместить**.

Инструкции по теме

1. Как открыть письмо.

Открыть статью на сайте

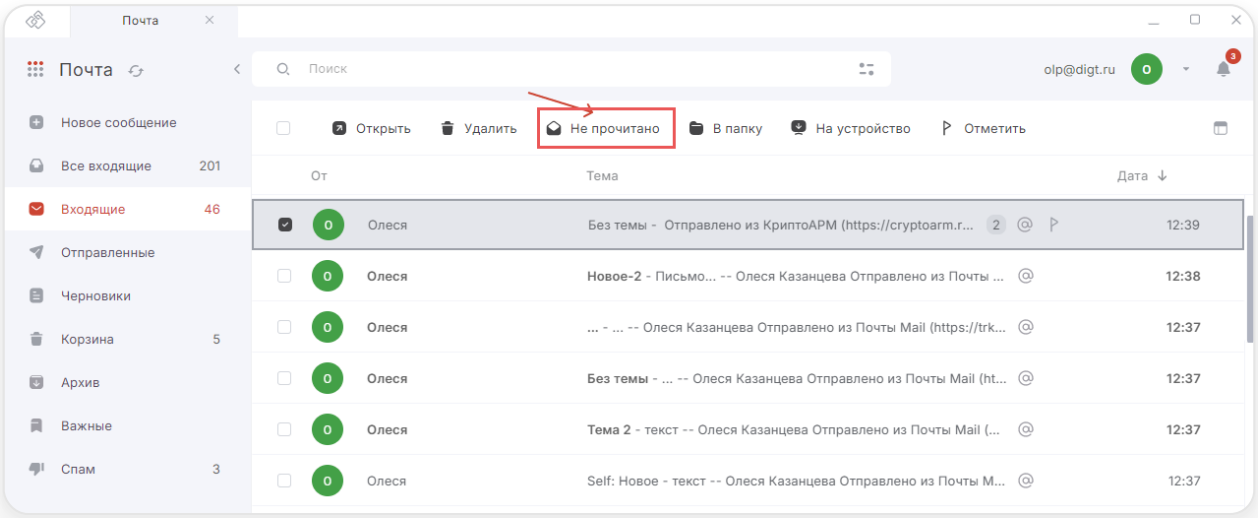
Отметить письмо как прочитанное или непрочитанное

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**/**Прочитано**.

Чтобы отметить письмо как прочитанное или непрочитанное на вкладке просмотра:

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



Открыть статью на сайте

Поиск писем

Как найти письмо

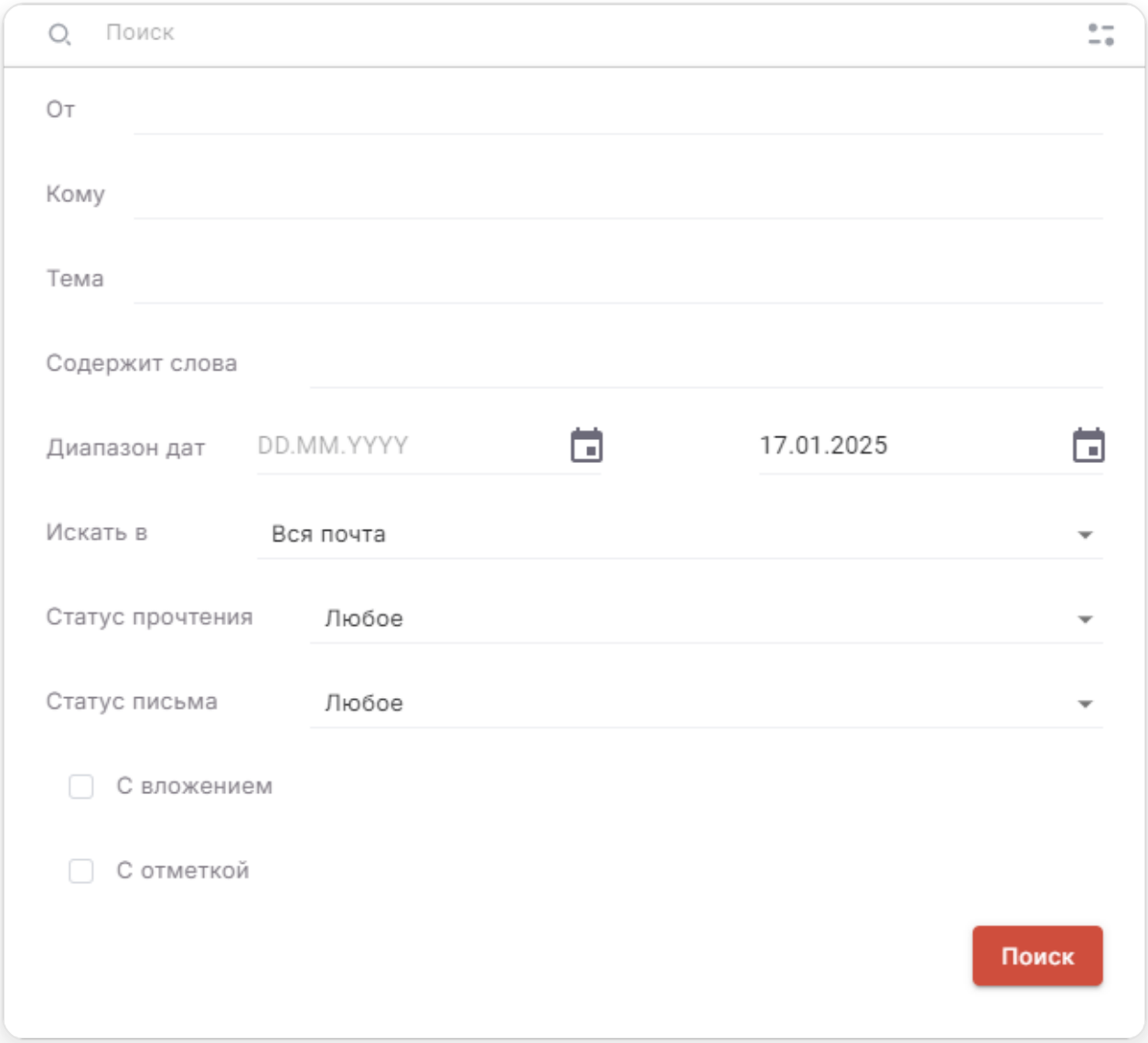
1. Перейдите в раздел **Почта**.
2. Введите в поисковой строке:
    - Имя отправителя;
    - Имя получателя;
    - Тему;
    - Содержание письма.
3. Нажмите Enter.

Если поиск происходит в папке **Входящие**, то поиск осуществляется по всем папкам в рамках выбранного почтового аккаунта.

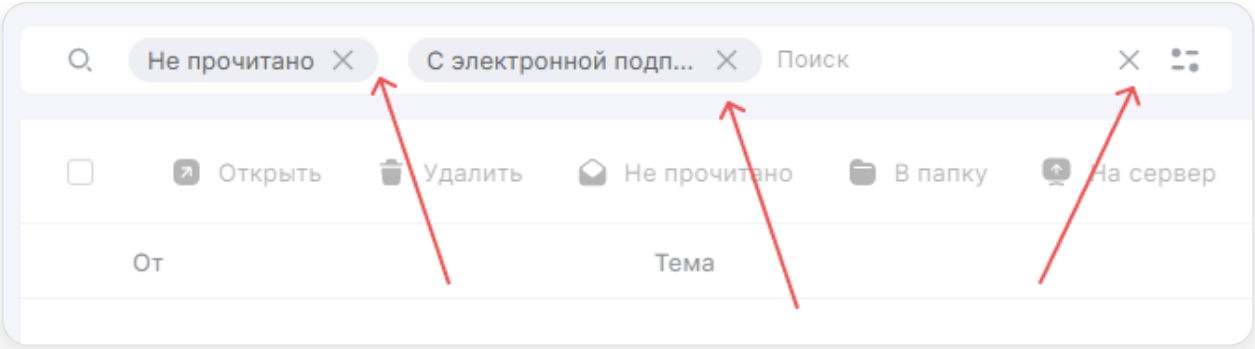
Если поиск происходит в папке **Отправленные, Корзина, Черновики**, то поиск запускается по данной папке.

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 **Поиск**.



Для отмены фильтрации необходимо нажать на кнопку **Отмена** на чипсете с фильтром.



Открыть статью на сайте

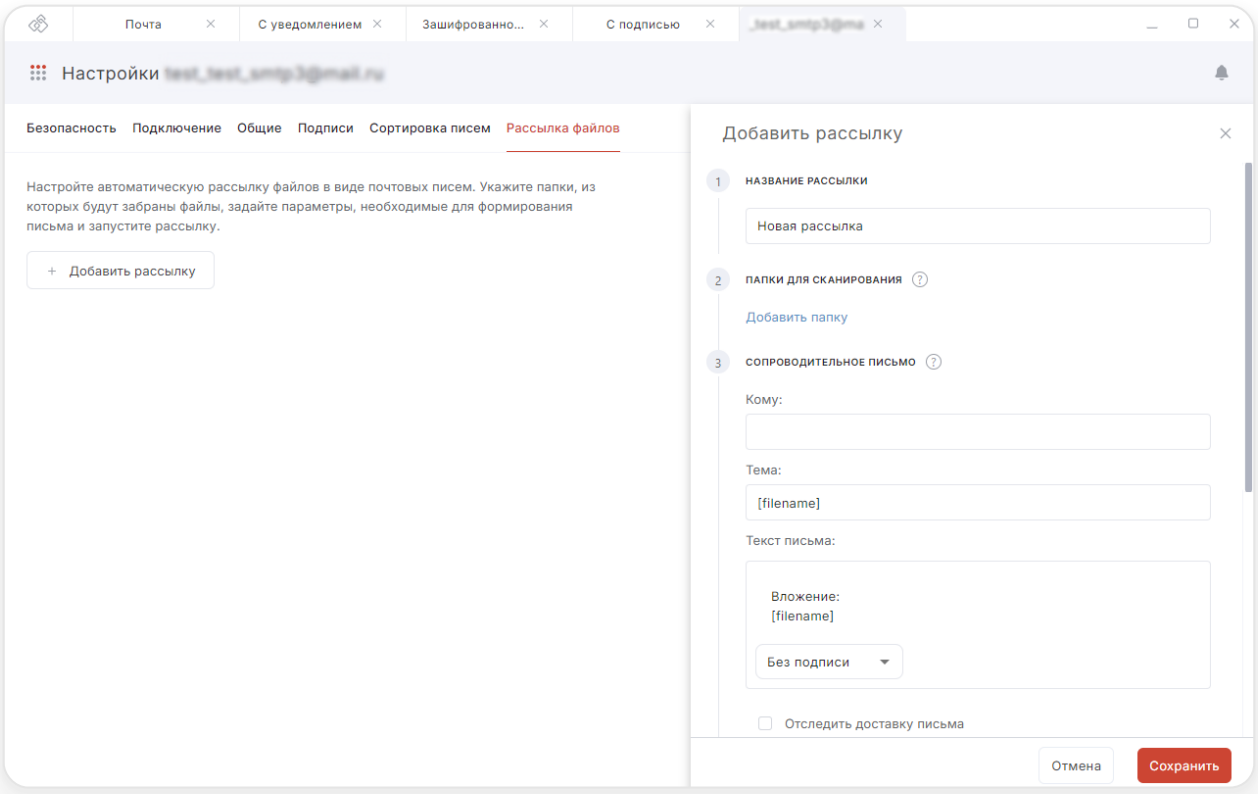
Рассылка файлов

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.

Как настроить рассылку файлов

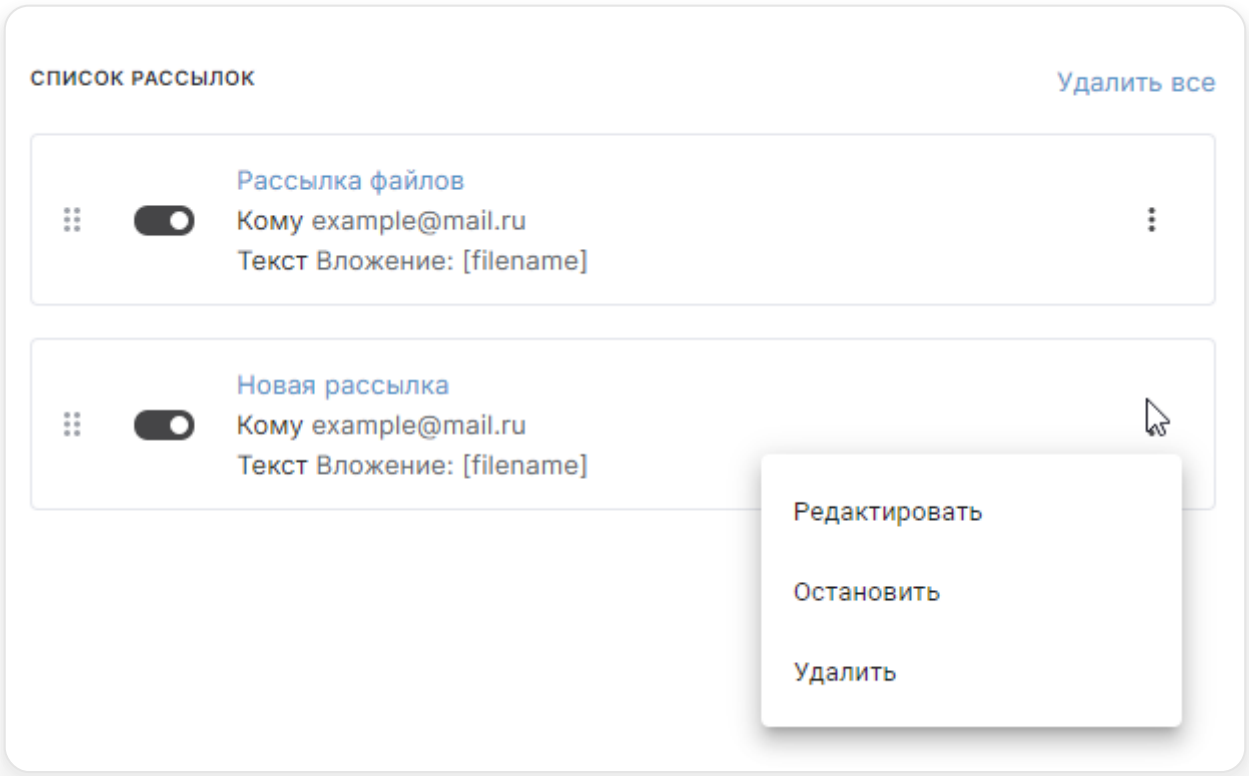
1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Рассылка файлов**.
3. Нажмите **Добавить рассылку**.
4. Откроется окно **Создать рассылку**.
5. Укажите название рассылки.
6. Выберите папки для сканирования с устройства, из которых будут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

   Важно. В рассылку попадут файлы только из корневой папки.
7. Добавьте текст сопроводительного письма.
8. Укажите получателей.
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, которые были отправлены. 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**.



Как изменить рассылку файлов

1. Откройте настройки почтового аккаунта. Как открыть настройки описано в инструкции.
2. Перейдите на вкладку **Рассылка файлов**.
3. Вызовите меню действий для рассылки, которую необходио отредактировать.
4. Выберите **Редактировать**.
5. Откроется форма редактирования рассылки.
6. Внесите изменения.
7. Нажмите **Сохранить**.



Как удалить рассылку файлов

Чтобы удалить одну рассылку файлов:

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

Чтобы удалить все рассылки файлов:

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

Как приостановить рассылку файлов

Чтобы остановить рассылку файлов, деактивируйте переключатель, размещенный на панели с рассылкой, либо нажмите **Остановить** в меню действий с рассылкой.

Открыть статью на сайте

Работа с расширениями .eml, .p7s, .p7m

Файлы с расширением .eml

EML — это файловый формат, разработанный компанией Microsoft для Outlook и Outlook Express.

EML-файлы — это заархивированные электронные письма, в которых сохраняются оригинальный формат и заголовки HTML.

В КриптоАРМ реализована поддержка формата EML. В разделе «Почта» вы можете открывать письма в формате.eml для чтения или импорта в любой из подключенных аккаунтов.

Как открыть письмо в формате .eml

1. Вызовите контекстное меню для письма в формате .eml в файловом менеджере или на рабочем столе.
2. Выберите пункт **Открыть с помощью** и далее выберите программу КриптоАРМ.
3. Приложение КриптоАРМ запустится (если не было запущено), а письмо откроется на новой вкладке для просмотра.

Также можно открыть письмо для просмотра в КриптоАРМ, дважды щелкнув по файлу с расширением.eml (если приложение уже ассоциировано с этим расширением в системе).

Файлы с расширением .p7m

Во входящих письмах могут отображаться файлы с расширением .p7m, это говорит о том, что данное письмо зашифровано и не удалось расшифровать контент письма. Весь контент письма находится в зашифрованном виде в формате .p7m. В КриптоАРМ есть возможность расшифровать файлы такого типа и отобразить зашифрованную часть в виде письма.

Как расшировать письмо в формате.p7m:

1. Запустите приложение КриптоАРМ.
2. Перейдите в раздел **Документы**.
3. Откройте мастер проверки и расшифрования.
4. Добавьте в мастер файл с расширением .p7m.
5. Выполните расшифрование.

В результате данных действий зашифрованная часть письма будет расшифрована и получен файл с расширением .eml, который можно просмотреть как письмо на отдельной вкладке.

Добавить файл в мастер проверки и расшифрования можно также с помощью двойного клика по файлу с расширением .p7m.

Файлы с расширением .p7s

Расширение файла .p7s означает, что данный файл содержит электронную подпись. В случае с письмами, внутри подписанного письма могут находиться файлы в виде smime.p7s. В приложении КриптоАРМ такие письма определяются как подписанные и отображается соответствующая иконка на письмах. В сторонних приложениях проверить подпись таких писем не всегда возможно.

Как проверить подпись письма с вложением smime.p7s

1. Скачайте письмо в формате .eml через web - интерфейс почтового сервиса или через сторонний почтовый клиент.
2. Откройте письмо в формате .eml в приложении КриптоАРМ. Как открыть письмо в формате .eml
3. Письмо откроется на отдельной вкладке.
4. Нажмите на иконку в виде сертификата  в шапке письма.
5. Откроется окно со статусом подписи, датой ее постановки и проверки.
6. Нажмите **Подробнее**.

Откроется окно со сведениями о подписи письма.

Открыть статью на сайте

Описание раздела

В разделе **Документы** представлен список документов специального каталога «Архив», который предназначен для сохранения архивной копии результатов выполнения операций.

В разделе «Документы», помимо каталога «Архив», также доступен каталог «Почтовые вложения». В этом каталоге отображаются файлы, которые были вложены в письма подключенных почтовых аккаунтов.

Документы каталога «Архив» расположены в папке пользователя в каталоге **\.Trusted\CryptoARM 6\Documents**.

В боковой панели можно перейти в разделы с мастерами:

- **Подпись и шифрование**.
- **Проверка и расшифрование**.
- **Подпись и защита PDF**.

В верхнем правом углу раздела доступен выбор профиля подписи, который предназначен для сохранения настроек параметров операций.

Инструкции по теме

1. Как посмотреть информацию о документе.
2. Как открыть документ на просмотр.
3. Как удалить документы.
4. Как создать профиль подписи.
5. Как подписать документ.
6. Как зашифровать документ.
7. Как проверить подпись.
8. Как расшифровать документ.
9. Как архивировать документ.

Открыть статью на сайте

Профили подписи

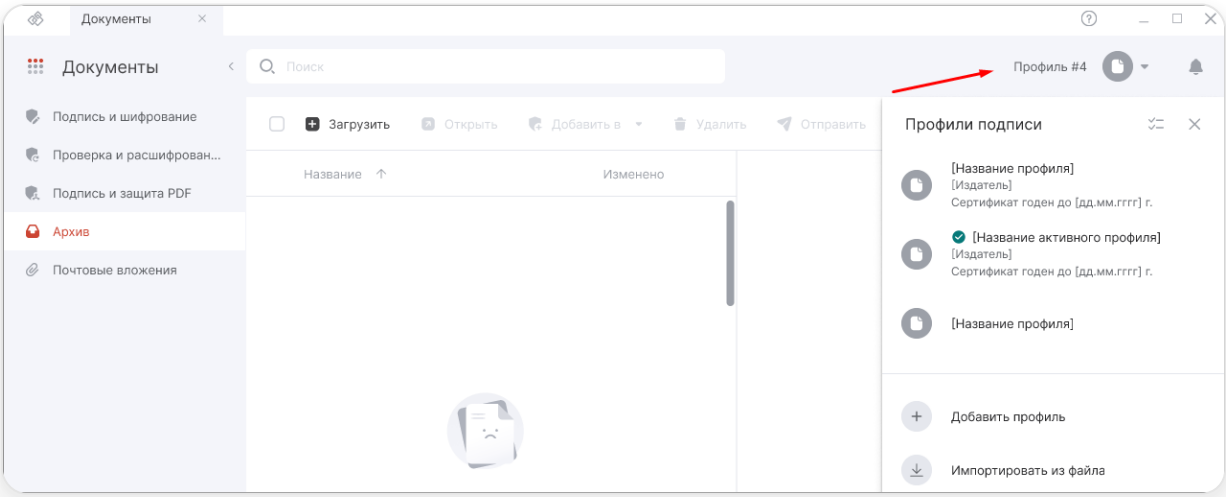
Профили подписи — это заранее подготовленные наборы настроек, которые можно применять для выполнения подписи, архивирования и шифрования. Подробнее про настройки профиля в инструкции Описание настроек профиля подписи.

Доступные действия с профилями подписи:

- Создание профиля подписи,
- Создание профиля подписи из сертификата,
- Редактирование настроек профиля подписи,
- Переключение между профилями,
- Экспорт профиля подписи,
- Импорт профиля подписи,
- Удаление профиля подписи.

Как создать профиль

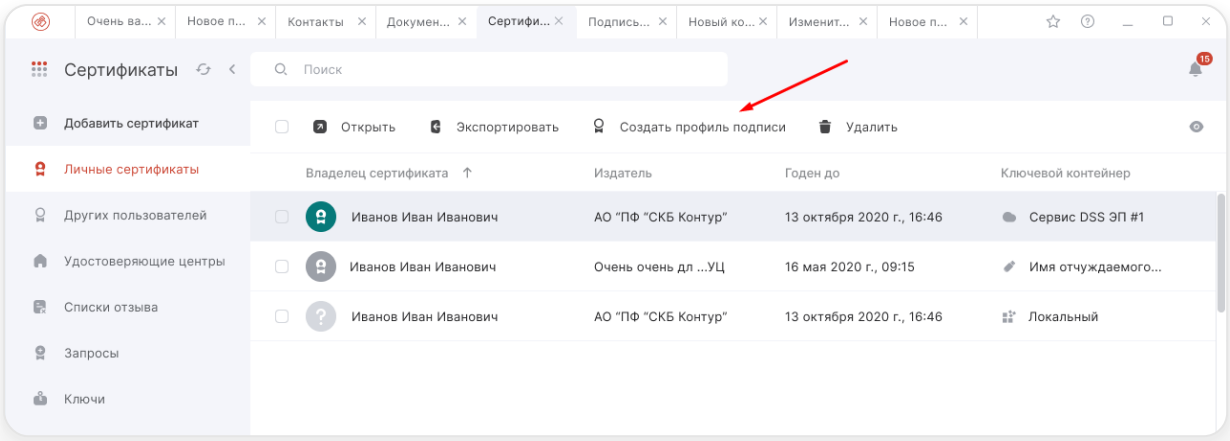
1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Выберите **Добавить профиль**.
4. Откроется окно **Новый профиль**.
5. Укажите настройки. Подробнее про настройки в инструкции Описание настроек профиля подписи.
6. Нажмите **Сохранить**.



После сохранения в списке профилей появится новый профиль.

Как создать профиль из Сертификата

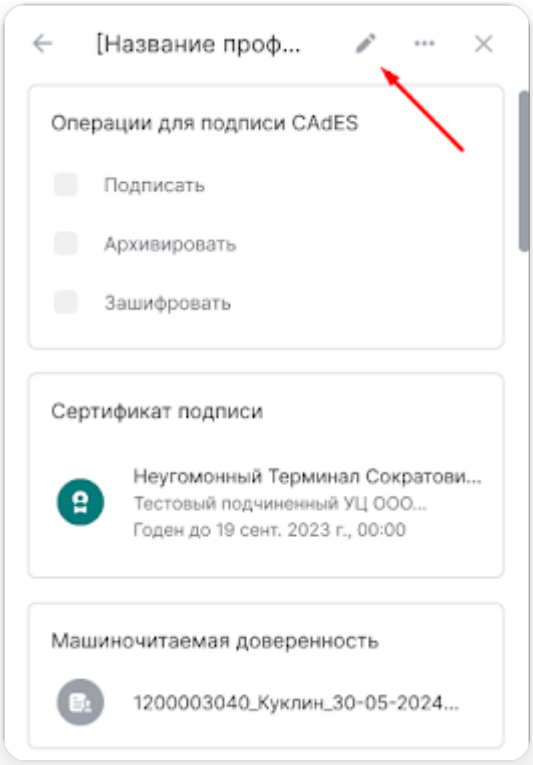
1. Перейдите в раздел **Сертификаты** → хранилище **Личные сертификаты**.
2. Выделите сертификат.
3. На панели действий нажмите на кнопку **Создать профиль подписи**.
4. Откроется окно **Новый профиль**. Личный сертификат будет автоматически привязан в блоке **Сертификат подписи**.
5. Укажите остальные настройки. Подробнее про настройки в инструкции Описание настроек профиля подписи.
6. Нажмите **Сохранить**.



Как изменить настройки профиля

Для редактирования профиля подписи, необходимо выполнить следующие действия:

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Наведите на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки**.
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Редактировать**.
7. Откроется форма для редактирования настроек профиля.
8. Внесите изменения в настройки. Подробнее про настройки в инструкции Описание настроек профиля подписи.
9. Нажмите кнопку **Сохранить**.



Переключение между профилями подписи

Вы можете переключаться между профилями подписи для выполнения операций с заранее настроенными параметрами в профилях.

Чтобы переключить профиль:

1. Перейдите в раздел **Документы**, в мастер **Подпись и шифрование** или **Подпись и защита PDF**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Нажмите на иконку профиля, который хотите сделать активным.

Примечание. Параметры, заданные в выбранном профиле, автоматически применяются в настройках мастеров **Подпись и шифрование** и **Подпись и защита PDF**.

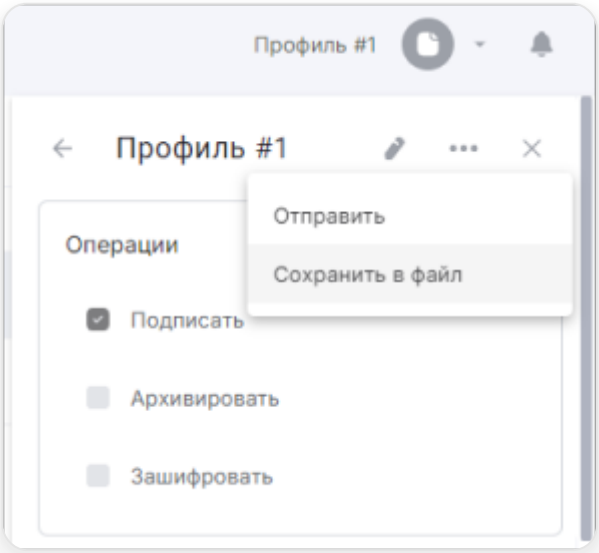
Экспорт профиля

Профили подписи можно экспортировать в файл .pcarm. или отправлять по почте.

Как экспортировать профиль

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.

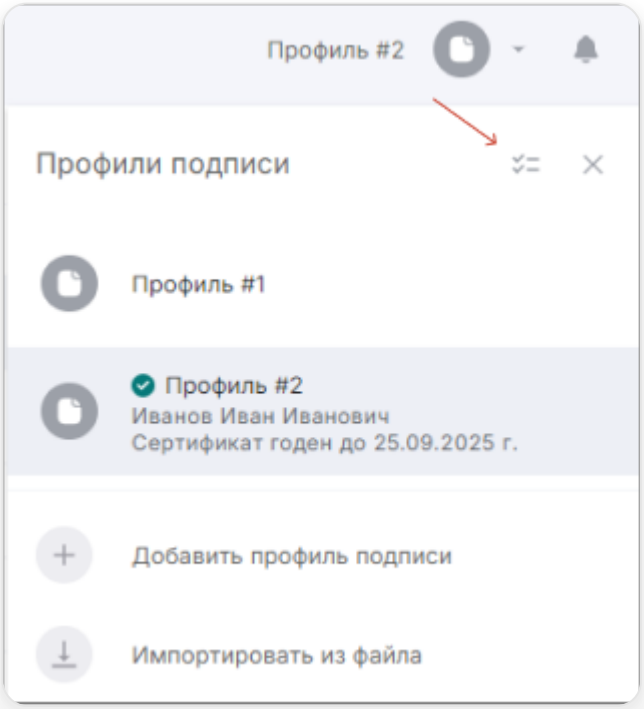
3. Наведите на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки**.
5. Откроется окно с предпросмотром настроек.
6. Вызовите меню действий с профилем по кнопке **Еще**.
7. Выберите **Сохранить в файл**.
8. Укажите путь для сохранения файла с профилем.



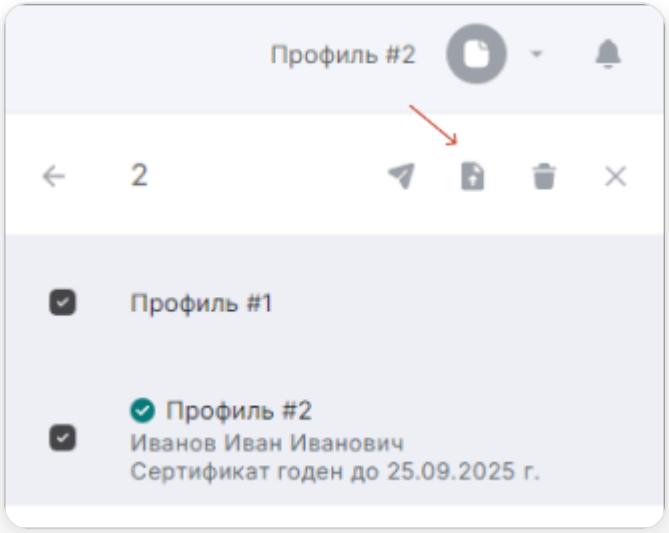
В результате по указанному пути будет сохранен в файл с расширением .pcarm.

Как экспортировать несколько профилей в файл

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Нажмите кнопку **Выбрать**.



4. Отметьте флагами профили, которые вы хотите экспортировать.



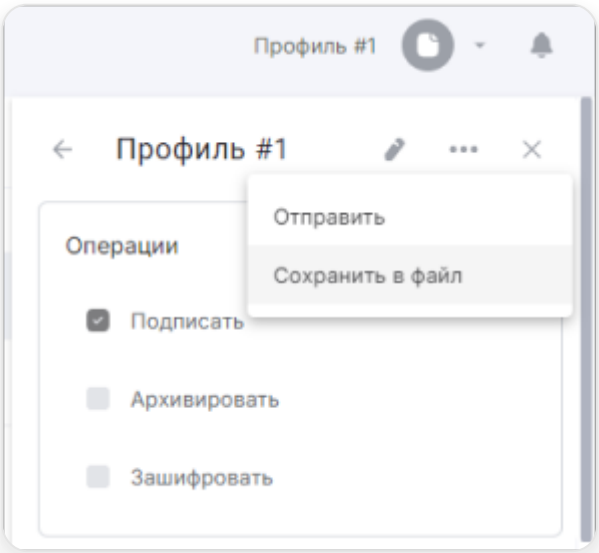
5. Нажмите кнопку **Сохранить в файл**.
6. Укажите путь для сохранения файла профиля.

После выполнения данных действий, профили будут сохранены в файл с расширением .pcarm

Как отправить профиль по почте

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.

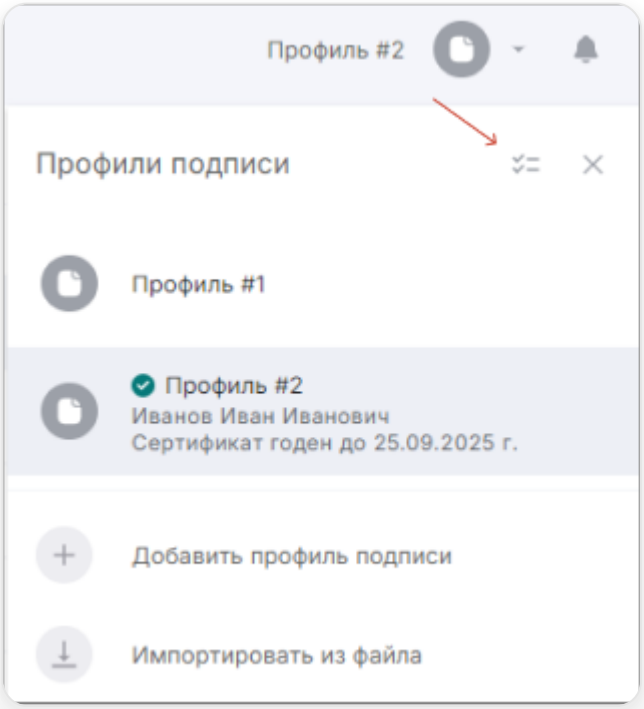
3. Наведите на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки**.
5. Откроется окно с предпросмотром настроек.
6. Вызовите меню действий с профилем по кнопке **Еще**.
7. Выберите **Отправить**.



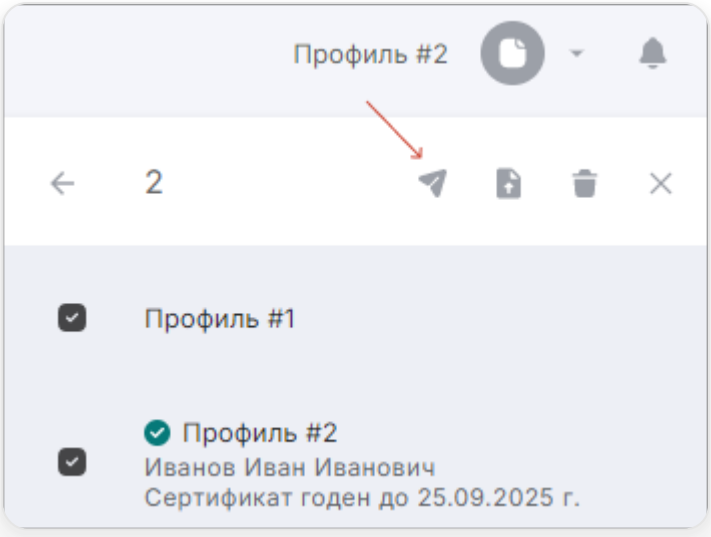
8. Откроется вкладка **Новое письмо**, в котором во вложении будет прикреплен профиль подписи с расширением .pcarm.

Как отправить несколько профилей по почте

1. Перейдите в раздел **Документы**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Нажмите кнопку **Выбрать**.



4. Отметьте флагами профили, которые вы хотите отправить по почте.
5. Нажмите кнопку **Отправить**.



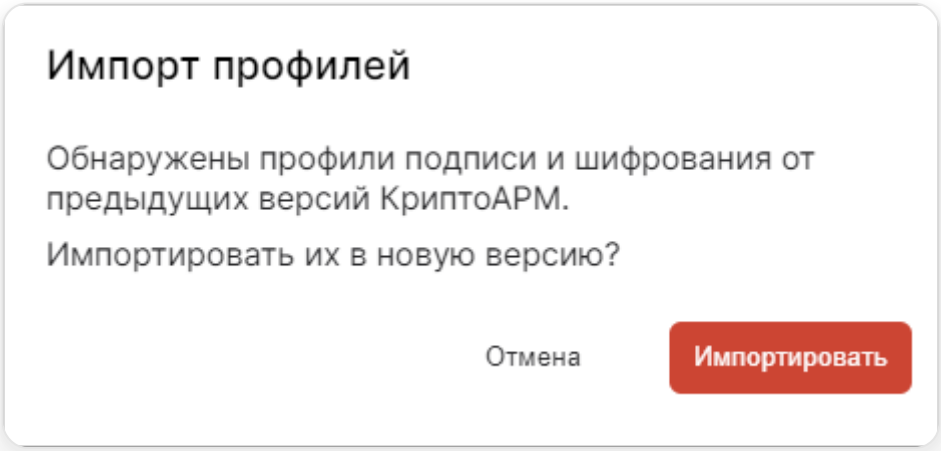
6. Откроется вкладка **Новое письмо**, в котором во вложении будет прикреплен профиль подписи с расширением .pcarm.

Важно. Для отправки профилей подписи по почте в приложении должен быть подключен почтовый аккаунт.

Импорт профиля подписи

Профили подписи можно импортировать в приложение из файлов или вложений письма в формате .pcarm, .json или .xml, либо при первом запуске приложения.

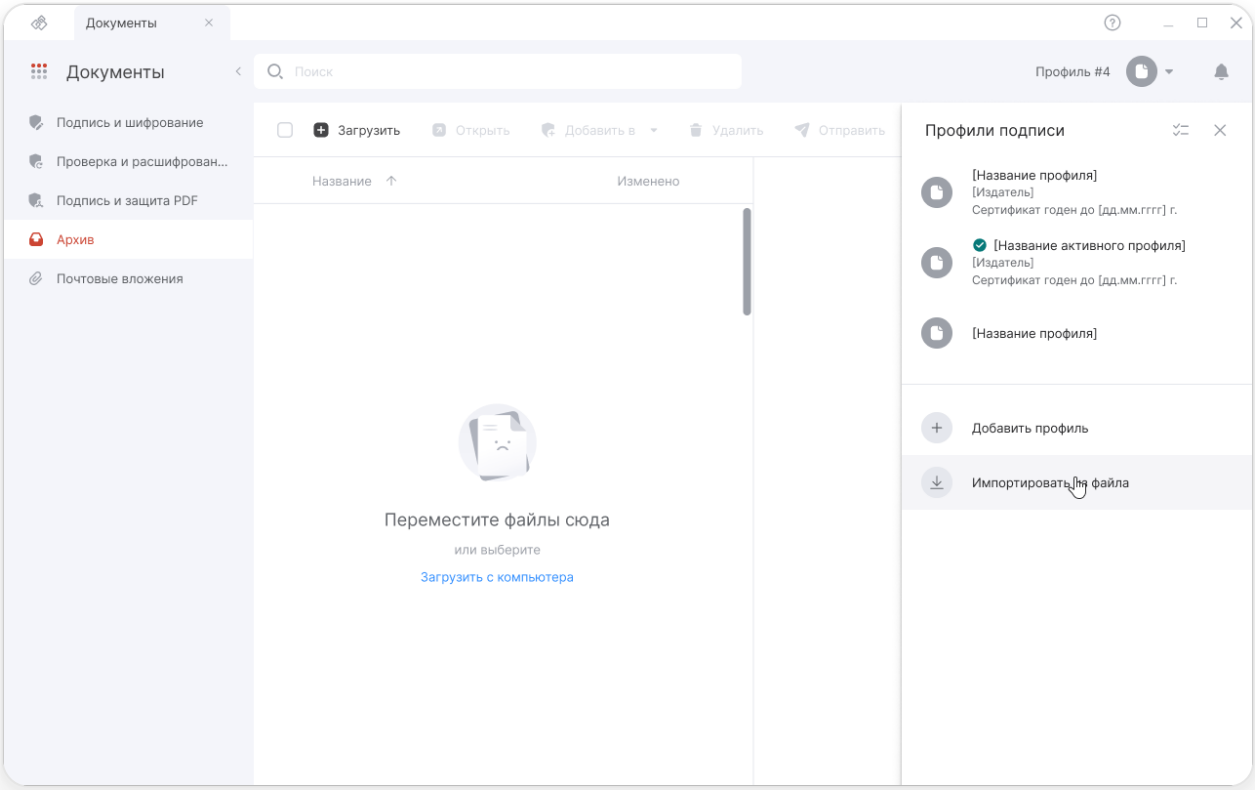
При первом запуске приложения, если в системе обнаружены профили подписи из других версий КриптоАРМ, откроется диалоговое окно, с предложением импортировать профили из других версий или нет.



Как импортировать профиль из файла

1. Перейдите в раздел **Документы** или в мастер **Подпись и шифрование**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Нажмите кнопку **Импортировать из файла**.
4. В открывшемся окне проводника выберите файл профиля подписи в формате .pcarm, .json или .xml.

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



Для импорта профиля подписи из файловой системы, необходимо выполнить следующие действия:

1. Через проводник, перейдите в папку, где хранится файл с расширением .pcarm.
2. Дважды кликните по файлу, либо правой кнопкой мыши вызовите контекстное меню для файла и выберите пункт **Открыть с помощью КриптоАРМ**.

После выполнения данных действий запустится приложение КриптоАРМ (если не было запущено) и профиль будет импортирован в приложение будет отображаться в списке профилей.

Как импортировать профиль из письма

1. Перейдите в раздел **Почта**.
2. Откройте письмо, которое содержит во вложении профиль подписи в формате .pcarm.
3. Кликните по названию файла в формате .pcarm, либо вызовите меню действий для вложения и нажмите на кнопку **Импортировать профиль подписи**.

Импорт профиля из папки Архив или Почтовые вложения

1. Перейдите в раздел **Документы** → **Архив** или **Почтовые вложения**.
2. Дважды кликните по файлу профиля подписи с расширением .pcarm.

Важно. Для импорта профилей из папки **Архив**, предварительно необходимо поместить в нее файл с расширением .pcarm. Для импорта профилей из папки Почтовые вложения, необходимо, чтобы в приложении был подключен почтовый аккаунт, в письмах которого, в виде вложений, содержатся файлы профилей с расширением .pcarm.

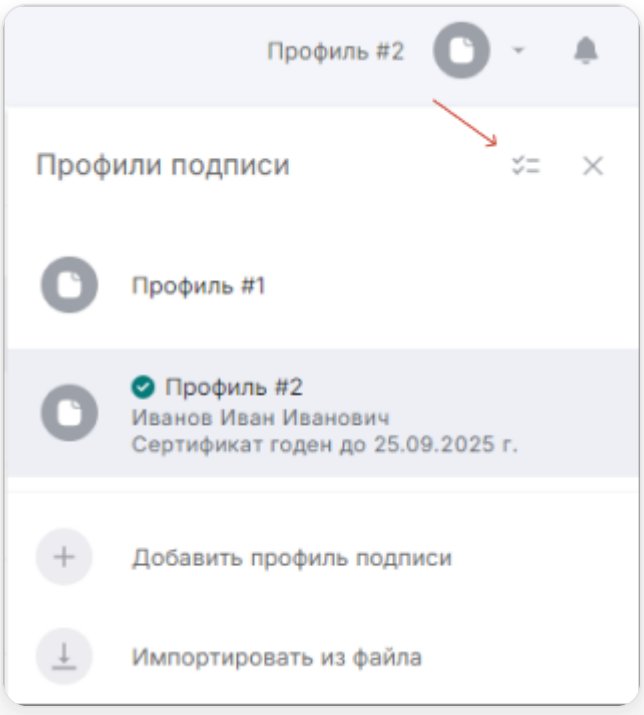
Удаление профилей

Как удалить один профиль подписи

1. Перейдите в раздел **Документы** или в мастер **Подпись и шифрование**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. Наведите курсор на тот профиль, который хотите удалить.
4. Нажмите на кнопку **Настройки**.
5. Откроется окно с предпросмотром настроек.
6. Вызовите меню действий с профилем по кнопке **Еще**.
7. Нажмите **Удалить**.
8. Подтвердите действие в модальном окне.

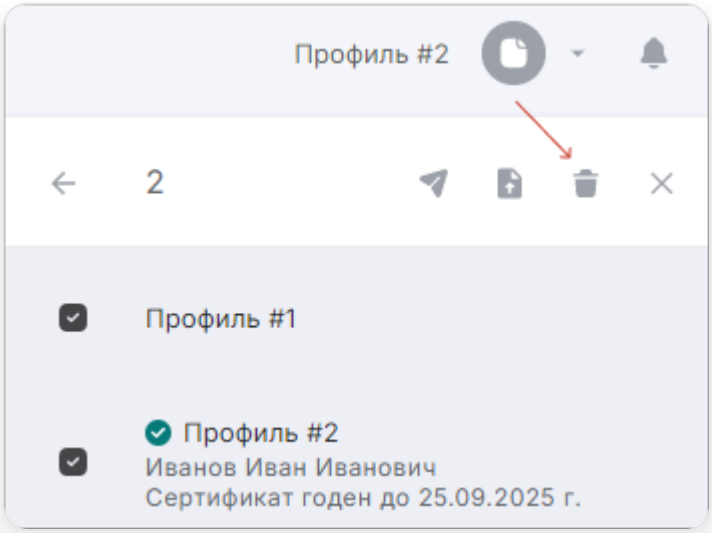
Как удалить несколько профилей подписи

1. Перейдите в раздел **Документы** или в мастер **Подпись и шифрование**.
2. Откройте окно со списком профилей. Для этого нажмите на название активного профиля в верхнем правом углу окна.
3. В окне со списком профилей нажмите на кнопку **Выбрать**.

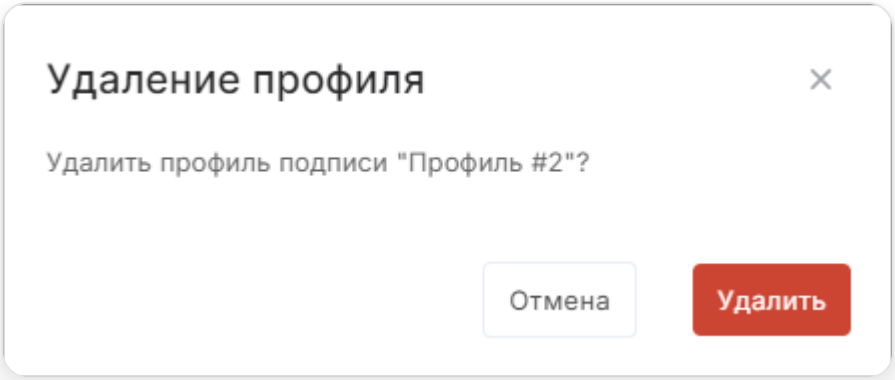


4. Отметьте флагами профили, которые вы хотите удалить.

5. Нажмите кнопку **Удалить**.



6. Подтвердите действие в модальном окне.



Открыть статью на сайте

Описание настроек профиля подписи

Операции

Название поля	Описание
Операции	- Подпись, - Архивирование, - Шифрование.

Личная подпись

Название поля	Описание
Личный сертификат	Личный сертификат, который будет использоваться для подписи документов
Стандарт подписи	- CAdES-BES - вариант по умолчанию. Классическая подпись. - CAdES-T - подпись со штампом времени, - CAdES-A - подпись с архивным штампом времени, - CAdES-X Long Type 1 - усовершенствованная подпись.
Машиночитаемая доверенность	Укажите путь к файлу доверенности и файлу подписи доверенности. Доверенность будет автоматически добавлена к пакету подписанных документов.
Включить в подпись	- Только сертификат владельца - вариант, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат; - Цепочка сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата; - Все сертификаты цепочки сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат.

Настройки групповой подписи

Название поля	Описание
Создать отдельный пакет (архив) для каждого подписываемого документа	Для каждого документа в списке будет создан отдельный архив с пакетом документов

Название поля	Описание
Использовать для PDF-документов встроенную подпись со стандартом PAdES	Если в списке будут обнаружены PDF-документы, они будут подписаны встроенный подписью с использованием стандарта PAdES.

Настройки подписи CAdES

Название поля	Описание
Кодировка подписи	- DER - вариант по умолчанию. - BASE-64 - для этого варианта кодирования вы можете указать флаг «Отключить служебные заголовки».
Вид подписи	- Присоединенная - вариант по умолчанию. Подпись, в процессе создания которой формируется специальный контейнер, в котором находятся как подписываемый документ, так и файл подписи. - Отсоединенная - файл подписи формируется и хранится отдельно от подписываемого документа.
Формат файла подписи	- .sig - вариант по умолчанию. - .p7s - .sgn - .sign - .bin

Настройки подписи PAdES

Настройка внешнего вида штампа подписи

Название поля	Описание
Вид	- Штамп - вариант по умолчанию. В области будет размещен только штамп. - Штамп с реквизитами слева - в области будет размещен штамп, а также блок с реквизитами слева от штампа. - Штамп с реквизитами справа - в области будет размещен штамп, а также блок с реквизитами справа от штампа. - Штамп с реквизитами слева и справа - в области будет размещен штамп, а также блок с реквизитами
Реквизиты	- По ГОСТу - вариант по умолчанию. В штамп будут выведены обязательные реквизиты, перечисленные в ГОСТ. - Произвольно - доступна самостоятельная настройка выводимых реквизитов.

Название поля	Описание
Оформление	- Добавить фон на область штампа, - Добавить границу на штамп, - Настройка цвета границы и текста в штампа.
Логотип	Настройте логотип, который будет отображаться в штампе

Настройка положения штампа подписи

Название поля	Описание
Видимость	- Видимая подпись - вариант по умолчанию. Подпись отображается на странице документа в виде штампа. - Невидимая подпись - подпись, которая визуально на странице документа не видна.
Размер	Ширина и высота штампа подписи
Положение	- Ориентация - угол отображение штампа внутри размеченной области. - Страницы - страница размещения штампа. - Настройка положения штампа на странице.

Настройка внешнего вида произвольной области

Название поля	Описание
Вид	- Оставить пустым - вариант по умолчанию. Следующий подписант документа сможет разместить свой комментарий, статус или отметку о конфиденциальности документа. - Изображение - загрузите изображение, которое будет отображаться в области. Например, отметку «Утверждено», «В работу». - Текст - введите текст, который будет отображаться в области.

Настройки зашиты PDF-документа

Название поля	Описание
Сертифировать	Сертификация позволяет защитить PDF-документ от изменений путем его подписания электронной подписью, с указанием типа изменений, разрешенных для документа. В приложении при сертификации разрешается заполнение размеченных областей для подписантов и для

Название поля	Описание
	произвольной области. При сертификации выполняется обязательная конвертация документа в формат PDF/A-2b.
Конвертировать в формат PDF/A-2b	При конвертации документа в формат PDF/A-2b происходит удаление скриптов, форм и прочие элементов, влияющие на безопасность и целостность документа.

Настройки печатной формы для PDF-документов

Название поля	Описание
Создать печатную форму для PDF-документов со штампом подписи	В печатной форме отображается штамп подписи, с информацией о сертификате, владельце сертификата и сроке действия сертификата. Печатная форма не содержит подпись.
Настройки внешнего вида штампа подписи	Настройки аналогичны Настройкам подписи PAdES
Настройки положения штампа подписи	Настройки аналогичны Настройкам подписи PAdES

Сертификаты шифрования

Название поля	Описание
Сертификаты шифрования	Сертификаты, которые будут использоваться при шифровании

Настройки шифрования

Название поля	Описание
Алгоритм шифрования	- ГОСТ28147-89, - ГОСТ Р 34.12-2015 Магма (ГОСТ Р 34.12-2018 Магма) - вариант по умолчанию, - ГОСТ Р 34.12-2015 Кузнечик (ГОСТ Р 34.12-2018 Кузнечик)
Кодировка файлов	- DER - вариант по умолчанию. - BASE-64.
Формат файла	- .enc - вариант по умолчанию. - .p7m - .p7e - .pem

Название поля	Описание
Удалить исходные файлы после шифрования	Исходные файлы, подлежащие шифрованию, удаляются из файловой системы после завершения процесса.

Сохранение результатов

Название поля	Описание
Сохранение результатов	- Папка с исходным документов - вариант по умолчанию, - Сохранить в папку... - выбор папки для сохранения результатов, - Создать копию в папке «Архив» - в папку «Архив» раздела «Документы» будет сохранена копия результатов операции.

Открыть статью на сайте

Подпись документа

С чего начать

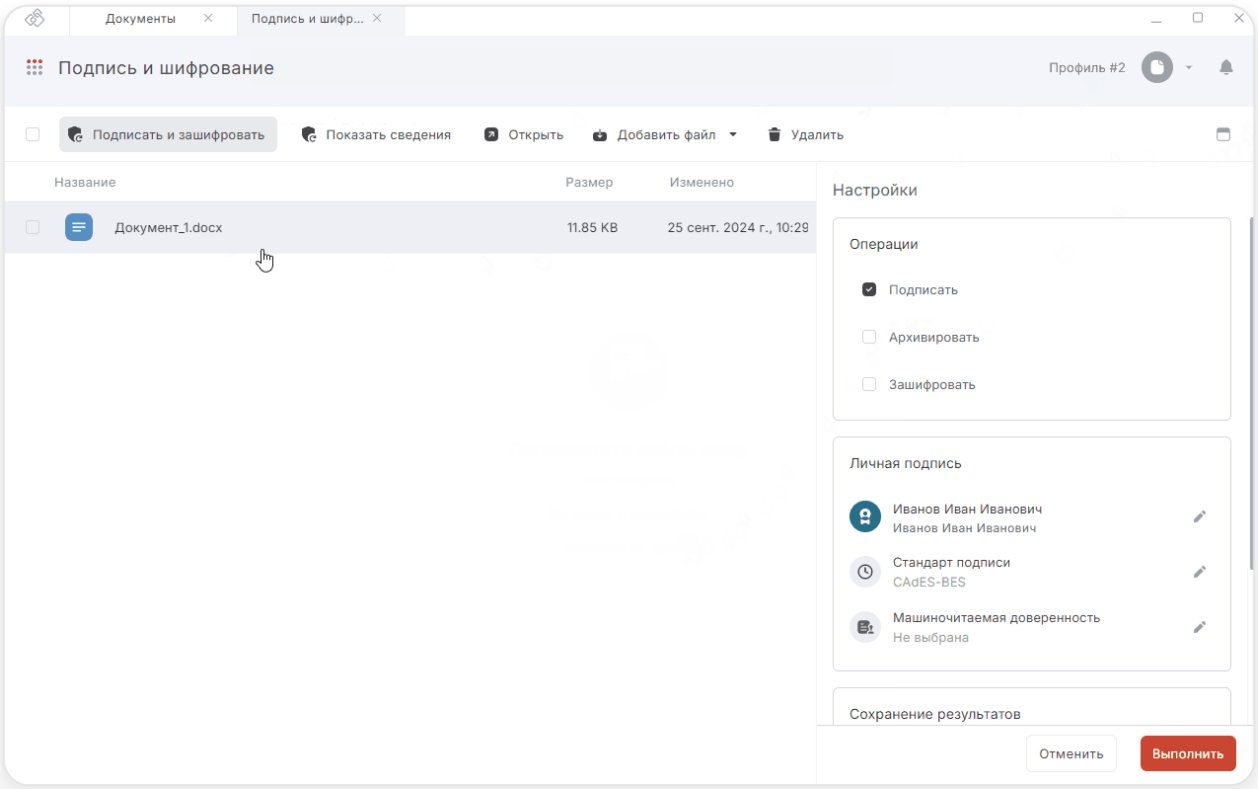
1. Убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP и имеется действующая лицензия на КриптоАРМ и КриптоПро CSP.
2. Установите личный сертификат.
   - Как установить сертификат из ключевого контейнера
   - Как установить сертификат из файла .pfx
   - Как установить сертификат из DSS
   - Как создать самоподписанный сертификат
3. Настройте профиль подписи
   - Как создать профиль подписи

Чтобы оценить, готово ли ваше рабочее место для подписи документов, воспользуйтесь Проверкой рабочего места.

Как подписать документ

1. Откройте мастер **Подписи и шифрования** одним из способов:
   - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
   - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Укажите настройки подписи, либо выберите профиль подписи с сохраненными настройками. Настройки мастера автоматически перезаполняются при выборе профиля. Подробнее про настройки в инструкции Описание настроек профиля подписи.
4. Нажмите кнопку **Выполнить**.
5. Подтвердите действие в модальном окне.

Результат будет выведен в окне Результаты операции.



Статичный кадр демонстрации. Открыть анимацию

Как подписать документ сертификатом DSS

Подпись сертификатом DSS ничем не отличается от подписи обычным сертификатом, за исключением некоторых шагов.

1. При выборе сертификата подписи DSS некоторые настройки операции подписи, такие как выбор стандарта подписи и установка штампов времени, недоступны.
2. При нажатии на кнопку **Выполнить** открывается:
   - Окно для ввода пароля к ключевому контейнеру. Введите пароль.

     Если пароль не задан, то данный шаг пропускается.
   - Окно для ввода пароля для аутентификации на сервисе DSS, если для аутентификации задан пароль и время действия токена аутентификации истекло. Введите пароль.

     Если токен аутентификации не истек, то данный шаг пропускается.
   - Окно для подтверждения аутентификации на сервисе DSS, если для аутентификации задан вход по SIM-карте или по мобильному приложению и время действия токена аутентификации истекло. Подтвердите операцию входа на сервис на устройстве.

     Если токен аутентификации не истек, то данный шаг пропускается.

- Окно ожидания подтверждения операции подписи, если в настройках аутентификации стоит подтверждение операции подписи по SIM-карте или с помощью мобильного приложения.

  Подтвердите операцию на устройстве.

Примечание. Для DSS подписи наличие лицензии на программный продукт КриптоПро CSP необязательно.

Как выполнить подпись со стандартом CAdES-T

Стандарт подписи CAdES-T (Timestamp) — это формат электронной подписи, в которую автоматически добавляется штамп времени на подпись.

Примечание. Создать подпись со штампом времени вы можете только при установленном модуле КриптоПро TSP Client и лицензии на него.

1. Откройте мастер **Подписи и шифрования** одним из способов:

   - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
   - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».

2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.

3. Укажите настройки, либо выберите профиль подписи с заранее сохраненным шаблоном настроек. Подробнее про настройки в инструкции Описание настроек профиля подписи.

4. В блоке **Личная подпись** → **Стандарт подписи**:

   - Выберите стандарт **CAdES-T**,
   - Укажите адрес **Служба штампов времени (TSP)**. Адрес службы можно узнать у поставщика услуги. Услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: \<протокол>://\<сервер>[:порт][/путь]. В качестве протокола может быть указан "http" и "https".
   - Если при подключении к службе TSP используется прокси-сервер, активируйте переключатель **Использовать прокси-сервер**. Заполните поля **Адрес прокси-сервера, Логин, Пароль,** которые можно узнать у системного администратора.

5. Нажмите кнопку **Выполнить**.

6. Подтвердите действие в модальном окне.

Результат будет выведен в окне Результаты операции.

Как выполнить подпись со стандартом Cades-X Long Type 1

Усовершенствованная квалифицированная электронная подпись поможет доказать юридическую значимость документа в спорных ситуациях. Например, когда помимо авторства и целостности документа (которые дает обычная КЭП) необходимо подтвердить, что сертификат был действителен в момент подписания документа.

Формат усовершенствованной подписи предусматривает включение в электронную подпись информации о времени создания подписи (TSP) и о статусе сертификата электронной подписи (OCSP) в момент подписания.

Примечание. Создание усовершенствованной подписи доступно только при наличии установленных модулей TSP Client и OCSP Client и лицензий на них.

1. Откройте мастер **Подписи и шифрования** одним из способов:
    - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
    - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Укажите настройки, либо выберите профиль подписи с заранее сохраненным шаблоном настроек. Подробнее про настройки в инструкции Описание настроек профиля подписи.
4. В блоке **Личная подпись** → **Стандарт подписи**:
    - Выберите стандарт **CAdES-X Long Type 1**,
    - Укажите адрес **Служба штампов времени (TSP)**. Адрес службы можно узнать у поставщика услуги. Услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: \<протокол>://\<сервер>[:порт][/путь]. В качестве протокола может быть указан "http" и "https".
    - При необходимости укажите адрес **Служба онлайн статусов (OCSP)**. Данное поле не обязательно для заполнения, чаще всего адрес прописан в сертификате подписи.
    - Если при подключении к службе TSP используется прокси-сервер, активируйте переключатель **Использовать прокси-сервер**. Заполните поля **Адрес прокси-сервера, Логин, Пароль,** которые можно узнать у системного администратора.
5. Нажмите кнопку **Выполнить**.
6. Подтвердите действие в модальном окне.

Результат будет выведен в окне Результаты операции.

Как выполнить подпись со стандартом CAdES-A

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. Данный формат используется для архивации долгосрочных подписей.

Вы можете создать подпись стандартом CadesA, только при наличии установленных модулей TSP Client и OCSP Client и лицензий на них.

Примечание. Создание подписи со стандартом CAdES-A доступно только при наличии установленных модулей TSP Client и OCSP Client и лицензий на них.

1. Откройте мастер **Подписи и шифрования** одним из способов:
    - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
    - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Укажите настройки, либо выберите профиль подписи с заранее сохраненным шаблоном настроек. Подробнее про настройки в инструкции Описание настроек профиля подписи.
4. В блоке **Личная подпись** → **Стандарт подписи**:
    - Выберите стандарт **CAdES-A**,
    - Укажите адрес **Служба штампов времени (TSP)**. Адрес службы можно узнать у поставщика услуги. Услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: \<протокол>://\<сервер>[:порт][/путь]. В качестве протокола может быть указан "http" и "https".
    - При необходимости укажите адрес **Служба онлайн статусов (OCSP)**. Данное поле не обязательно для заполнения, чаще всего адрес прописан в сертификате подписи.
    - Если при подключении к службе TSP используется прокси-сервер, активируйте переключатель **Использовать прокси-сервер**. Заполните поля **Адрес прокси-сервера, Логин, Пароль,** которые можно узнать у системного администратора.
5. Нажмите кнопку **Выполнить**.
6. Подтвердите действие в модальном окне.

Результат будет выведен в окне Результаты операции.

Как выполнить подпись со стандартом PAdES

В мастере **Подпись и шифрование** можно выполнить групповую подпись PDF-файлов со стандартом PAdES. Для подписи одного файла лучше использовать мастер **Подпись и защита PDF**.

Важно. Сертификат DSS не подходит для встроенной подписи PDF-файлов стандартом Pades.

Важно. Если в списке файлов на подпись будут документы, не относящиеся к формату PDF, то вложенная подпись будет выполнена только для PDF-файлов, а для остальных — классическая подпись.

1. Откройте мастер **Подписи и шифрования** одним из способов:
   - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
   - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте PDF-документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Укажите настройки для подписи со стандатом PAdES, либо выберите профиль подписи с заранее сохраненным шаблоном настроек. Подробнее про настройки в инструкции Описание настроек профиля подписи.
   - В блоке **Настройки групповой подписи** активируйте флаг **Использовать для PDF-документов встроенную подпись со стандартом PAdES**.
   - В блоке **Настройки подписи PAdES** укажите внешний вид и положение штампа подписи.
4. Нажмите кнопку **Выполнить**.
5. Подтвердите действие в модальном окне.

Результат будет выведен в окне Результаты операции.

Подпись PDF-файлов с созданием печатной формы

В мастере **Подпись и шифрование** вы можете создать печатную форму для PDF-файлов, в которой будет отображаться штамп подписи, с информацией о сертификате, владельце сертификата и сроке действия сертификата. Поля штампа можно изменить в профиле подписи, либо в мастере **Подпись и шифрование** в **Настройках операции**.

1. Откройте мастер **Подписи и шифрования** одним из способов:
   - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
   - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте PDF-документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Укажите настройки, либо выберите профиль подписи с заранее сохраненным шаблоном настроек. Подробнее про настройки в инструкции Описание настроек профиля подписи.
   - В блоке **Печатная форма** активируйте флаг **Создать печатную форму для PDF-документов со штампом подписи**.

- Укажите внешний вид и положение штампа подписи.

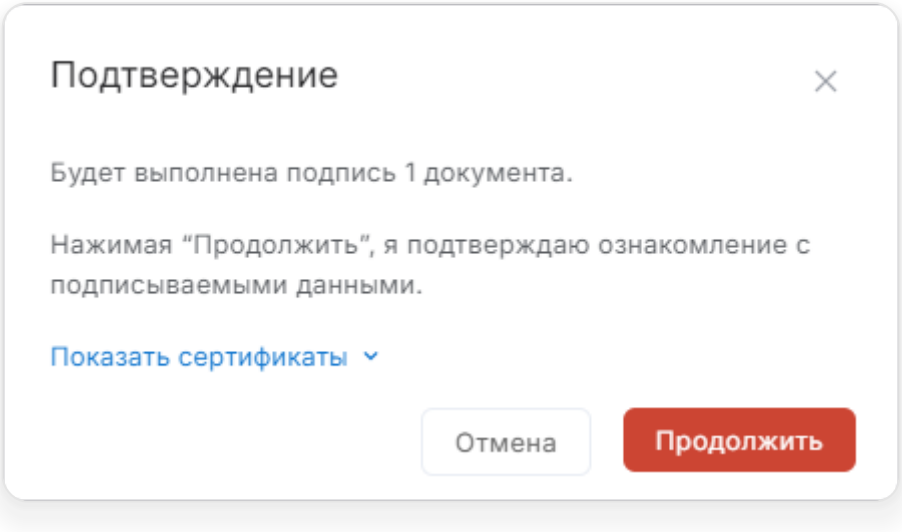
4. Нажмите кнопку **Выполнить**.
5. Подтвердите действие в модальном окне.

После выполнения, в результатах операции сформируются подписанные PDF-файлы в формате .sig (sgn, sign, p7s, bin) и копия оригинала PDF-файла со штампом подписи.

Подтверждение операции

Перед выполнением подписи в приложении запрашивается подтверждение.

После нажатия на кнопку «Выполнить» появляется модальное окно с запросом подтверждения. В этом окне отображается информация о количестве документов, которые будут подписаны, а также сертификат подписи.

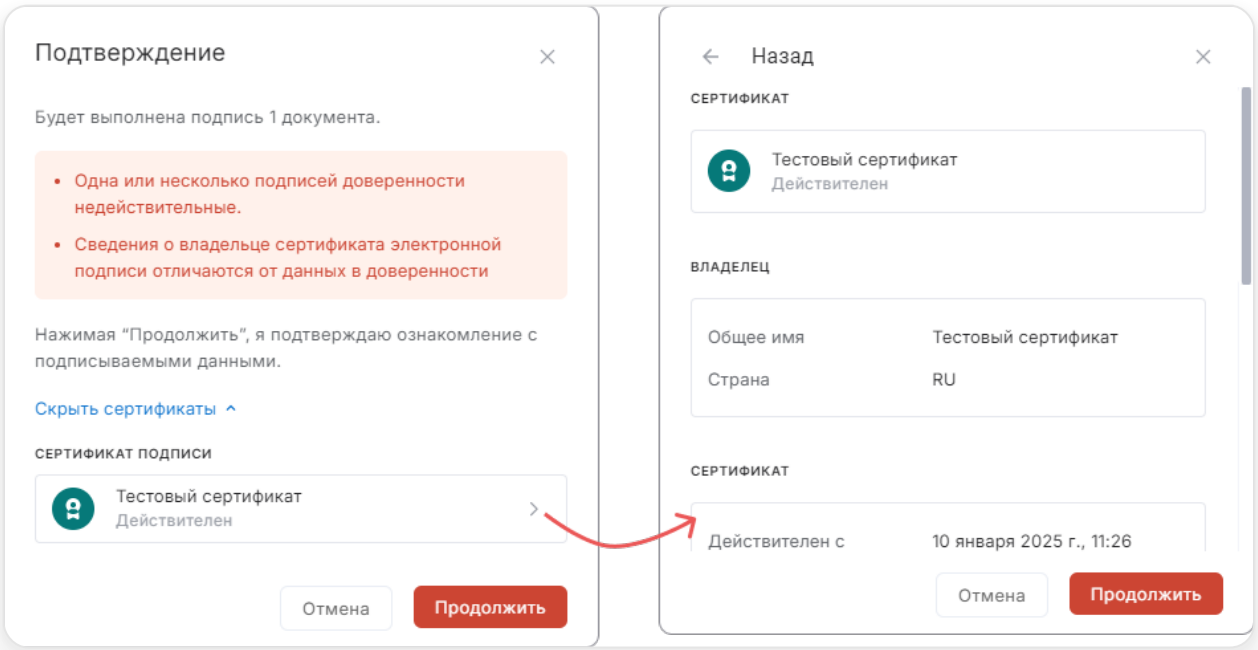


Также в окне могут появиться дополнительные уведомления, если:

- Сертификат подписи недействителен,
- Срок действия открытого или закрытого ключа 30 дней и менее,
- Сертификат подписи машиночитаемой доверенности недействительный,
- Сведения о владельце сертификата подписи отличаются от данных в машиночитаемой доверенности.

Чтобы просмотреть информацию о сертификате подписи, нажмите на кнопку «Показать сертификат». После этого нажмите на панель с сертификатом.

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



Результат выполнения операции

Во время выполнения операции в нижней части окна появляется панель с индикатором выполнения и кнопкой «Отмена». Операции происходят с документами последовательно. Если вы нажмёте на кнопку «Отмена», операция будет приостановлена на том документе, с которым производилась операция на момент отмены.

Если операция прошла успешно, подписанные файлы будут сохранены в каталоге, который был указан в настройках мастера. Если каталог не указывался, то результаты будут размещены рядом с исходным файлом.

Если установлен флаг **Создать копию в Архиве**, то копия подписанных документов сохраняется в специальную папку, документы которой доступны в разделе **Документы → папка Архив**.

Примечание. Если в настройках подписи выбрана отсоединённая подпись, то в заданный каталог и в **Архив** кроме файла подписи создается копия исходного файла.

После выполения операции происходит автоматическая проверка подписи. На иконке документа с действительной подписью отображается зеленая галочка. На иконке документа с недействительнйо подписью - красный крестик.



В результатах операции можно посмотреть информацию о подписи. Подробнее в инструкции Действия с документами.

Возможные уведомления

Ошибки, которые могут возникнуть при выполнении операции, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Не удалось открыть файл** — добавленные в мастер документы были удалены или по какой-то причине доступны, добавлен пустой файл (с нулевым размером).
2. **Не удалось подписать файл** — ошибка в адресе службы штампов времени, если подпись со штампом или усовершенствованная. Ошибка подключения к прокси-серверу.
3. **Не удалось подписать файл** — ошибки, связанные с истекшими лицензиями КриптоПро TSP Client, OCSP Client, КриптоПро CSP.

Инструкции по теме

1. Как установить личный сертификат.
2. Как создать профиль подписи.
3. Как переключаться между профилями подписи.
4. Как добавить документы в мастер.
5. Как посмотреть уведомления.
6. Действия с результатами операций.
7. Как проверить подпись документа.

Открыть статью на сайте

Шифрование документа

С чего начать

1. Убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP.
2. Установите в хранилище «Других пользователей» сертификат или привяжите сертификат к контакту, в адрес которого будет проводиться шифрование.
   - Как привязать к контакту сертификат
   - Как установить сертификат другого пользователя
3. Установите личный сертификат, если потребуется шифрование в адрес личного сертификата.
   - Как установить сертификат из ключевого контейнера
   - Как установить сертификат из файла .pfx
   - Как установить сертификат из DSS
   - Как создать самоподписанный сертификат
4. Настройте профиль подписи.
   - Как создать профиль подписи

Чтобы оценить, готово ли ваше рабочее место для подписи документов, воспользуйтесь Проверкой рабочего места.

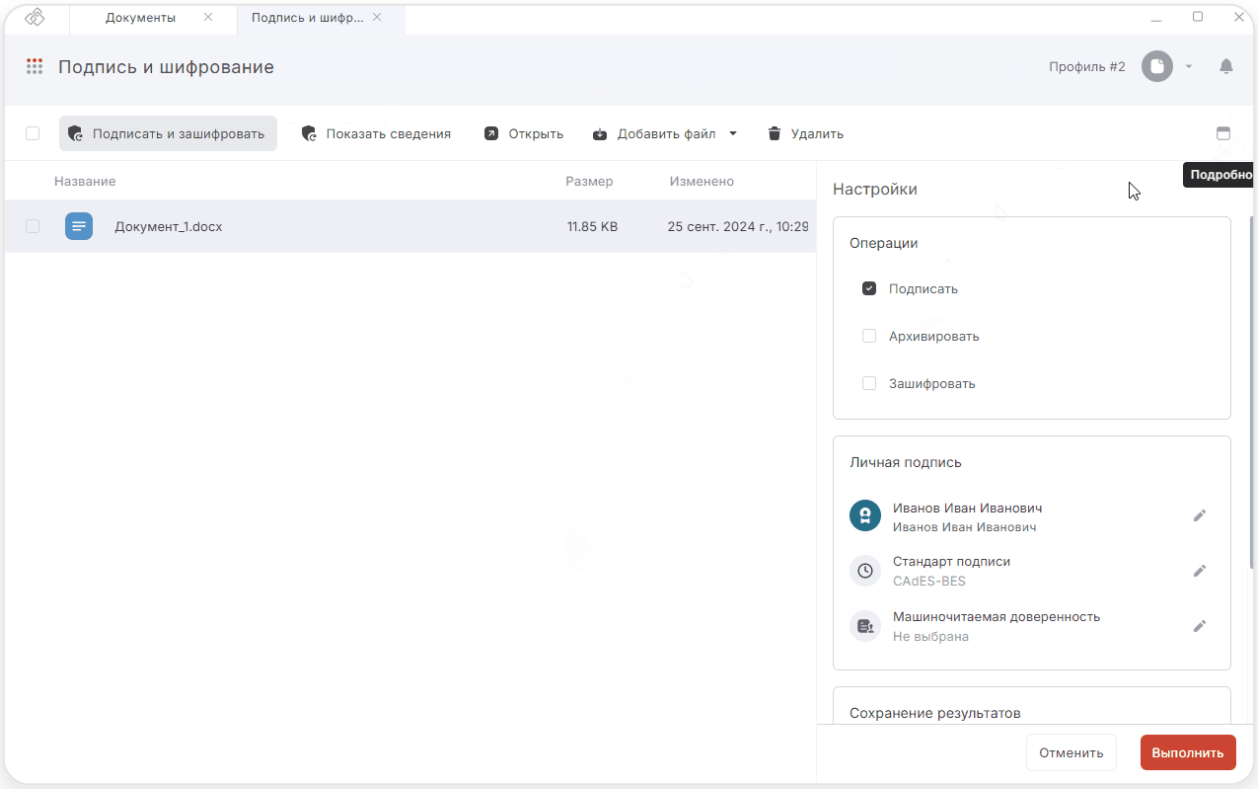
Как зашифровать документ

1. Откройте мастер **Подписи и шифрования** одним из способов:
   - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
   - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Укажите настройки подписи, либо выберите профиль подписи с сохраненными настройками. Настройки мастера автоматически перезаполняются при выборе профиля. Подробнее про настройки в инструкции Описание настроек профиля подписи.
   - В блоке **Операции** выберите **Зашифровать**,
   - В блоке **Сертификаты шифрования** укажите сертификаты получателей, в адрес которых необходимо выполнить шифрование.
   - В блоке **Настройки шифрования** настройте алгоритм, кодировку и формат файла.
   - В блоке **Сохранение результатов** укажите настройки сохранения результатов операции.

4. Нажмите кнопку **Выполнить**.

5. Подтвердите действие в модальном окне.

Результат будет выведен в окне Результаты операции.

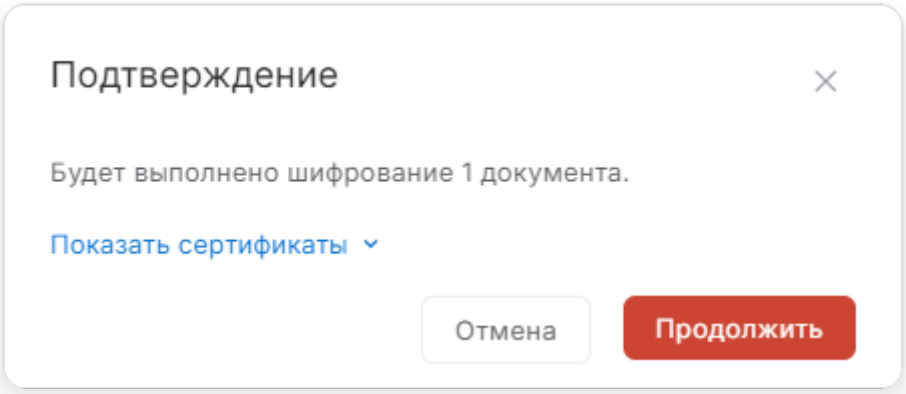


Статичный кадр демонстрации. Открыть анимацию

Подтверждение операции

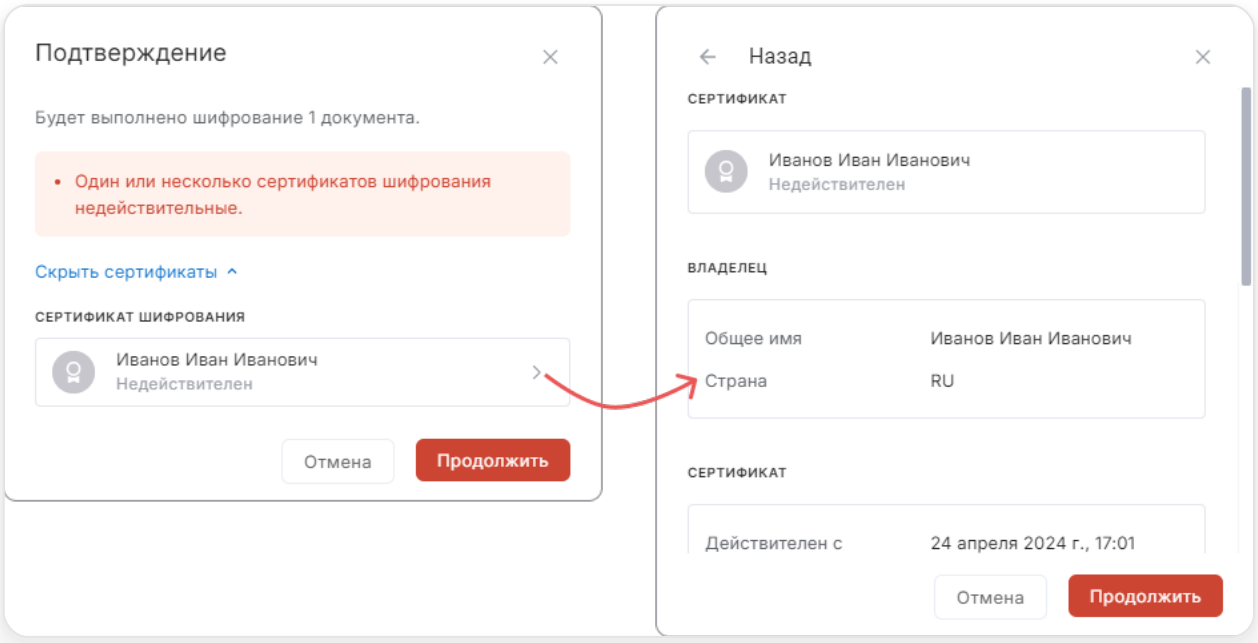
Перед выполнением шифрования в приложении запрашивается подтверждение.

После нажатия на кнопку «Выполнить» появляется модальное окно с запросом подтверждения. В этом окне отображается информация о количестве документов, которые будут зашифрованы, а также сертификаты шифрования.



Также в окне может появиться дополнительное уведомление, если один или несколько сертификатов шифрования недействительны.

Чтобы просмотреть информацию о сертификате шифрования, нажмите на кнопку «Показать сертификат». После этого нажмите на панель с сертификатом.



Результат выполнения операции

Во время выполнения операции в нижней части окна появляется панель с индикатором выполнения и кнопкой «Отмена». Операции происходят с документами последовательно. Если вы нажмёте на кнопку «Отмена», операция будет приостановлена на том документе, с которым производилась операция на момент отмены.

Если операция прошла успешно, зашифрованные файлы будут сохранены в каталоге, который был указан в настройках мастера. Если каталог не указывался, то результаты будут размещены рядом с исходным файлом.

Если установлен флаг **Создать копию в Архиве**, то копия зашифрованных документов сохраняется в специальную папку, документы которой доступны в разделе **Документы → вкладка Архив**.

Если в параметрах шифрования была выбрана опция **Удалить файлы после шифрования**, то промежуточные файлы и оригиналы документов будут удалены после шифрования.

Возможные уведомления

Ошибки, которые могут возникнуть при выполнении операции, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Не удалось зашифровать файл — добавленные в мастер документы были удалены или по какой-то причине не доступны; добавлен пустой файл (с нулевым размером).

Инструкции по теме

1. Как создать профиль подписи.
2. Как переключаться между профилями подписи.
3. Как добавить документы в мастер.
4. Как посмотреть уведомления.
5. Действия с результатами операций.
6. Как импортировать сертификаты других пользователей.
7. Как привязать сертификат к контакту.

Открыть статью на сайте

Соподпись

Приложение КриптоАРМ позволяет добавлять электронные подписи к уже подписанному файлу. Такой вариант подписи используется, когда необходимо подписать файл нескольким пользователям (например, при согласовании документа сотрудниками одного отдела). При этом соподпись и первичная подпись будут иметь равный статус (равнозначны).

Выполнение соподписи аналогично проставлению первой подписи. Подробнее в инструкции Подпись документа.

Инструкции по теме

1. Как установить личный сертификат.
2. Как создать профиль подписи.
3. Как переключаться между профилями подписи.
4. Как добавить документы в мастер.
5. Как посмотреть уведомления.
6. Действия с результатами операций.

Открыть статью на сайте

Проверка подписи документа

Для проверки подписи предназначен мастер «Подпись и шифрование». В мастере можно проверить не только статус подписи, но и посмотреть сведения о подписи.

Информация о подписи документа также доступна в мастере «Подпись и шифрование», в папках «Архив» и «Почтовые вложения». Подробнее в инструкции Просмотр информации о документе.

Примечание. В приложении доступна проверка подписи для файлов расширением .sig, .p7s, .sgn, .sign, .bin.

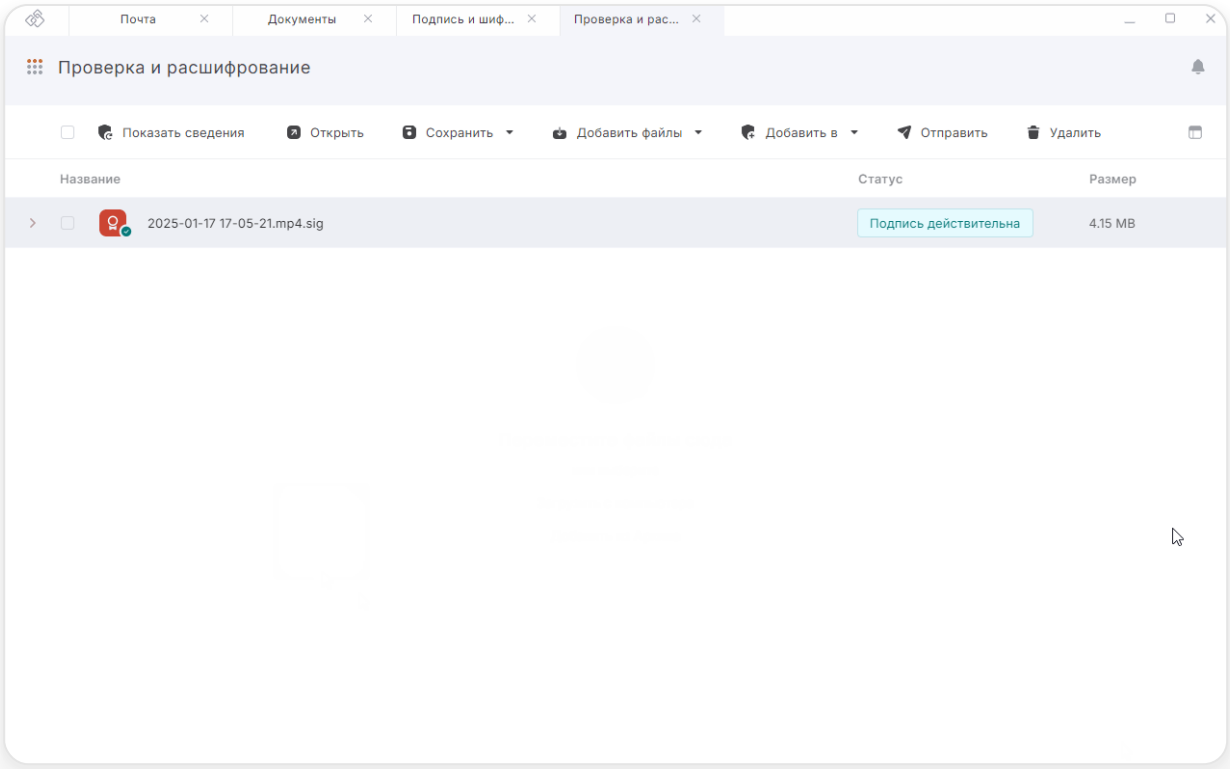
С чего начать

1. Убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP.
2. Установите корневой и промежуточные сертификаты для сертификата подписанта. Подробнее об установке сертификатов в инструкции Установка корневого и промежуточного сертификатов.

Чтобы оценить, готово ли ваше рабочее место для проверки подписи документов, воспользуйтесь Проверкой рабочего места.

Как проверить подпись документа

1. Откройте мастер **Проверка и расшифрование** одним из способов:
    - Нажмите **Проверка и расшифрование** в левом боковом меню раздела **Документы**,
    - Вызовите действие **Добавить в** → **Проверка и расшифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте документы с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. После добавления документов будет запущен процесс проверки.
4. Статус подписи будет выведен на панели с документом.
5. На иконке документа отобразится зеленая галочка, если подпись действительная, и красный крестик, если недействительная.
6. Нажмите на кнопку **Показать сведения**.
7. Справа от списка документов появится область просмотра со сведениями о подписи.

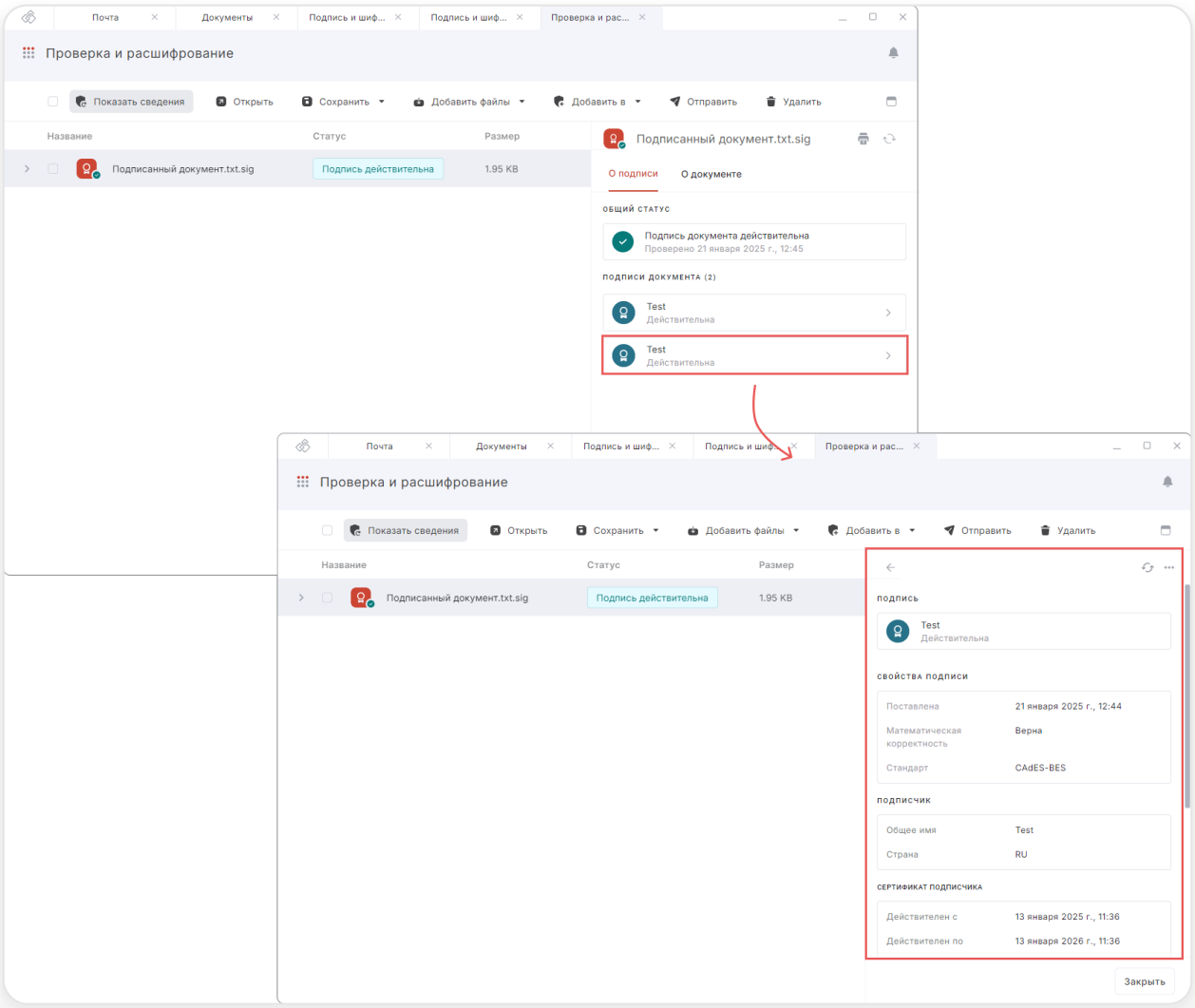


Статичный кадр демонстрации. Открыть анимацию

Как просмотреть сведения о подписи документа с соподписями

1. Выполните шаги из инструкции Как проверить подпись документа.
2. В блоке **Подписи документа** выберите подпись, сведения о которой необходимо просмотреть.

В области просмотра отобразятся сведения о подписи.

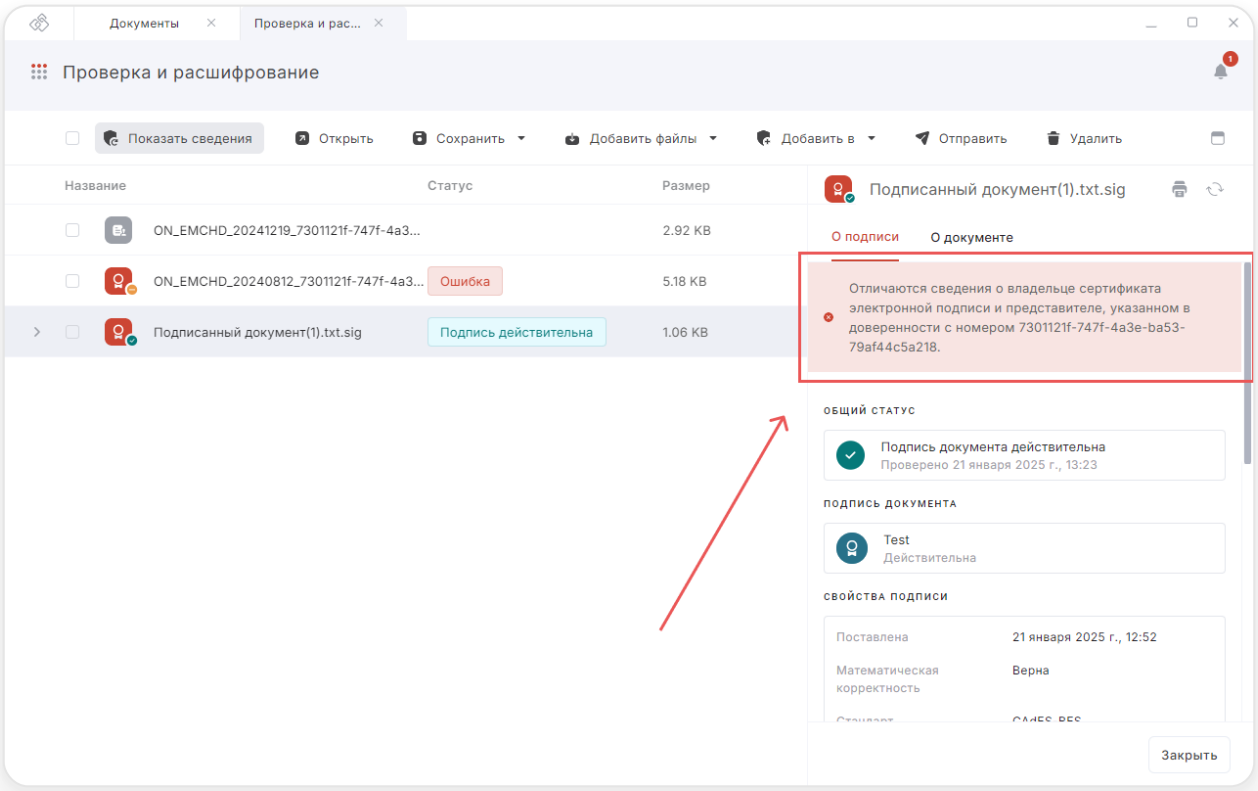


Проверка соответствия МЧД сертификату подписи

В мастере **Подпись и шифрование** выполняется дополнительная проверка сведений владельца сертификата подписи и владельца машиночитаемой доверенности. Проверка выполняется по реквизиту ИНН.

Проверка доступна для документов, содержащих одну подпись.

1. Добавьте подписанные документы и машиночитаемую доверенность с файлом подписи.
2. После добавления документов будет запущен процесс проверки.
3. Статус подписи будет выведен на панели с документом.
4. Нажмите на кнопку **Показать сведения**.
5. Справа от списка документов появится область просмотра со сведениями о подписи. Если проверка не будет пройдена, отобразится уведомление: «Сведения о владельце сертификата подписи отличаются от данных в машиночитаемой доверенности».



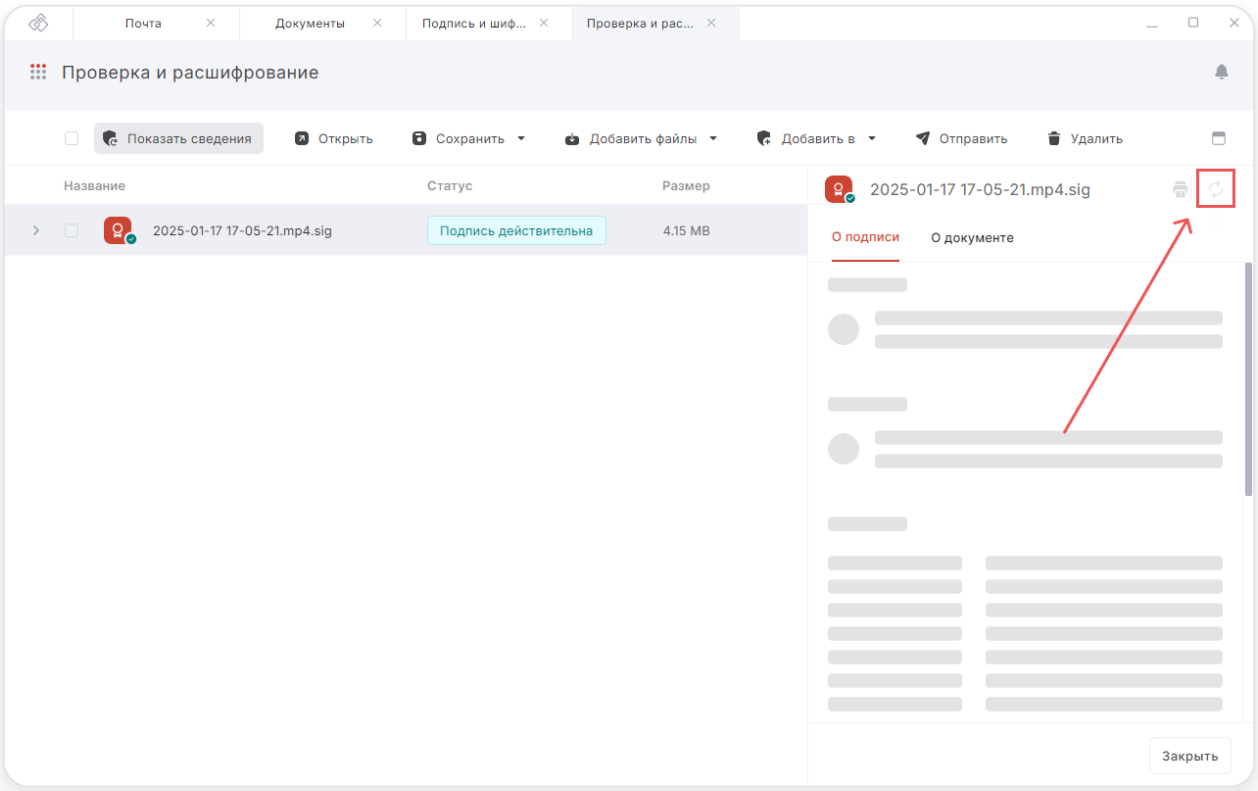
Как обновить сведения о подписи документа

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 Как проверить подпись документа.
2. В области просмотра со сведениями о подписи нажмите на кнопку **Обновить**.

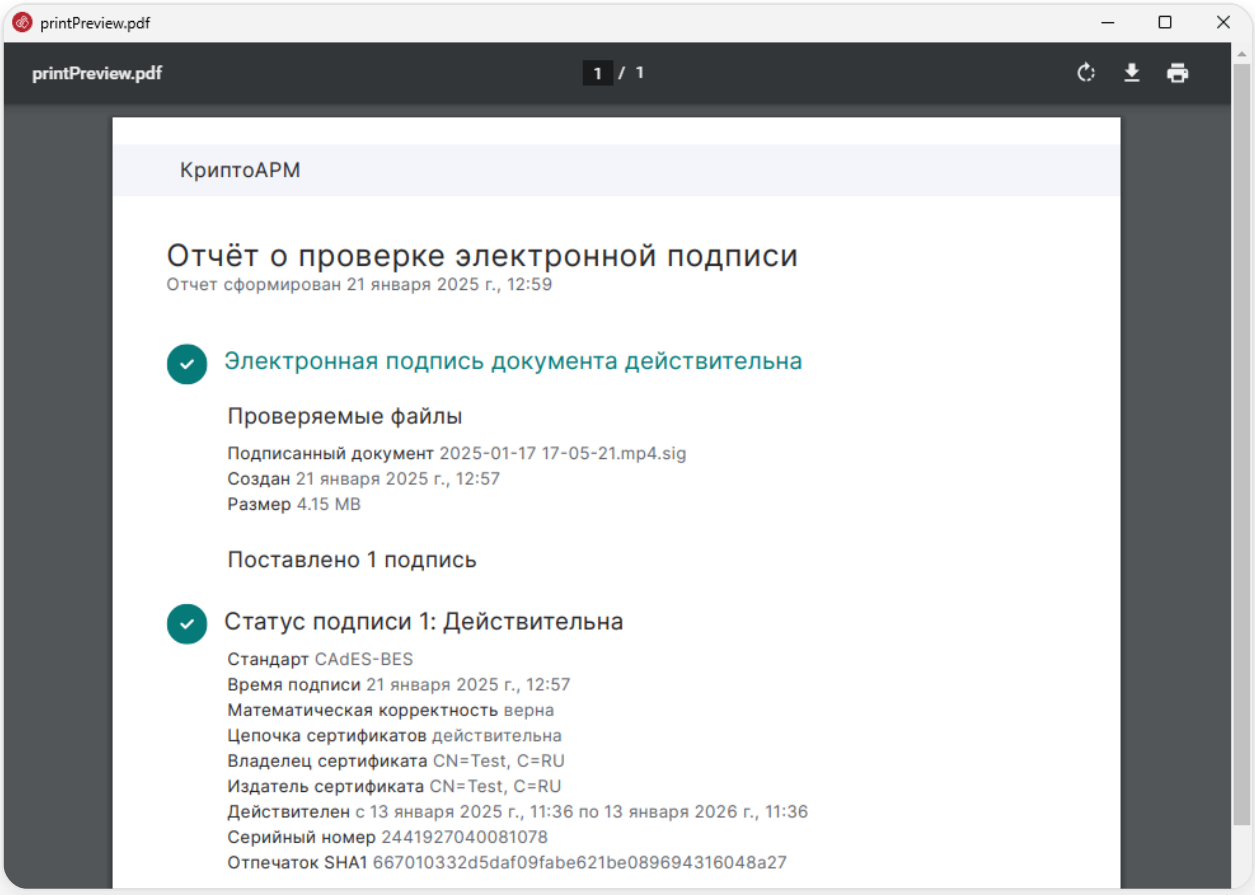
Сведения о подписи будут обновлены.



Как распечатать сведения о подписи документа

1. Выполните шаги из инструкции Как проверить подпись документа.
2. Нажмите на кнопку **Печать**.
3. Откроется окно с отчетом о проверке электронной подписи.

Отчет можно распечатать или скачать на устройство.



Возможные уведомления

Ошибки, которые могут возникнуть при выполнении операции, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Не удалось открыть файл** — добавленные в мастер документы были удалены или по какой-то причине доступны.
2. **Не удалось найти исходный файл для подписи** — в мастер добавлен файл с отсоединённой подписью без исходного документа.

Инструкции по теме

1. Как добавить документы в мастер.
2. Как посмотреть уведомления.
3. Как установить корневой и промежуточный сертификаты.
4. Действия с результатами операций.

Открыть статью на сайте

Снятие подписи с документа

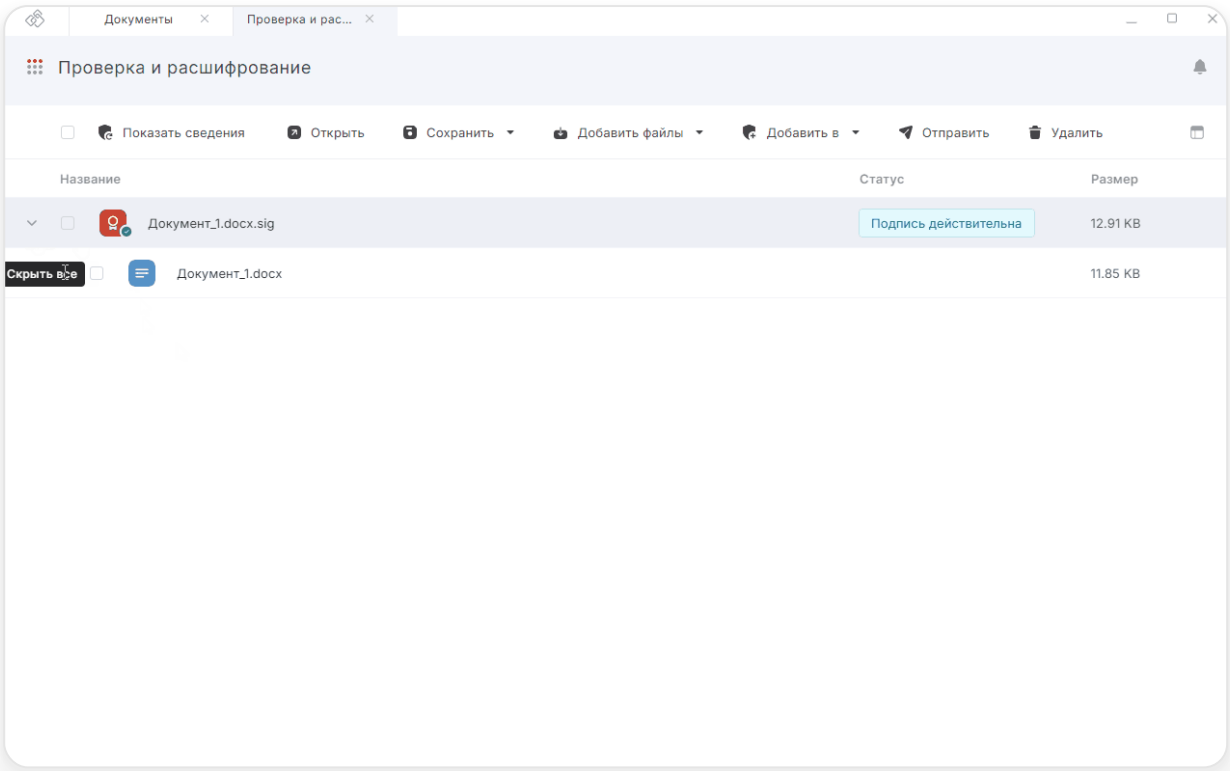
Важно. Прежде чем приступить к выполнению операции, убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP.

Чтобы оценить, готово ли ваше рабочее место для работы с электронной подписью, воспользуйтесь Проверкой рабочего места.

В приложении доступна снятие подписи для файлов расширением .sig/.p7s/.sgn/.sign/.bin.

Как снять подпись с документов

1. Откройте мастер **Проверка и расшифрование** одним из способов:
    - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
    - Вызовите действие **Добавить в** → **Проверка и расшифрование** для файла в папке «Архив», результатах операции или в разделе «Почта». 3. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**. 4. После добавления документов будет запущен процесс расшифрования. Если в хранилище **Личные** будет обнаружен сертификат для расшифрования, то файл автоматически расшифруется. При необходимости укажите пароль на контейнер с сертификатом. 5. Нажмите кнопку слева от файла, с которого надо снять подпись.



Статичный кадр демонстрации. Открыть анимацию

Возможные уведомления

Ошибки, которые могут возникнуть при выполнении операции, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Нельзя снять открепленную подпись с файла** — при откреплённой подписи оригинал документа и так находится в отдельном файле.
2. **Не удалось открыть файл** — добавленные в мастер документы были удалены или по какой-то причине не доступны.

Инструкции по теме

1. Как добавить документы в мастер.
2. Как посмотреть уведомления.
3. Действия с результатами операций.

Открыть статью на сайте

Расшифрование документа

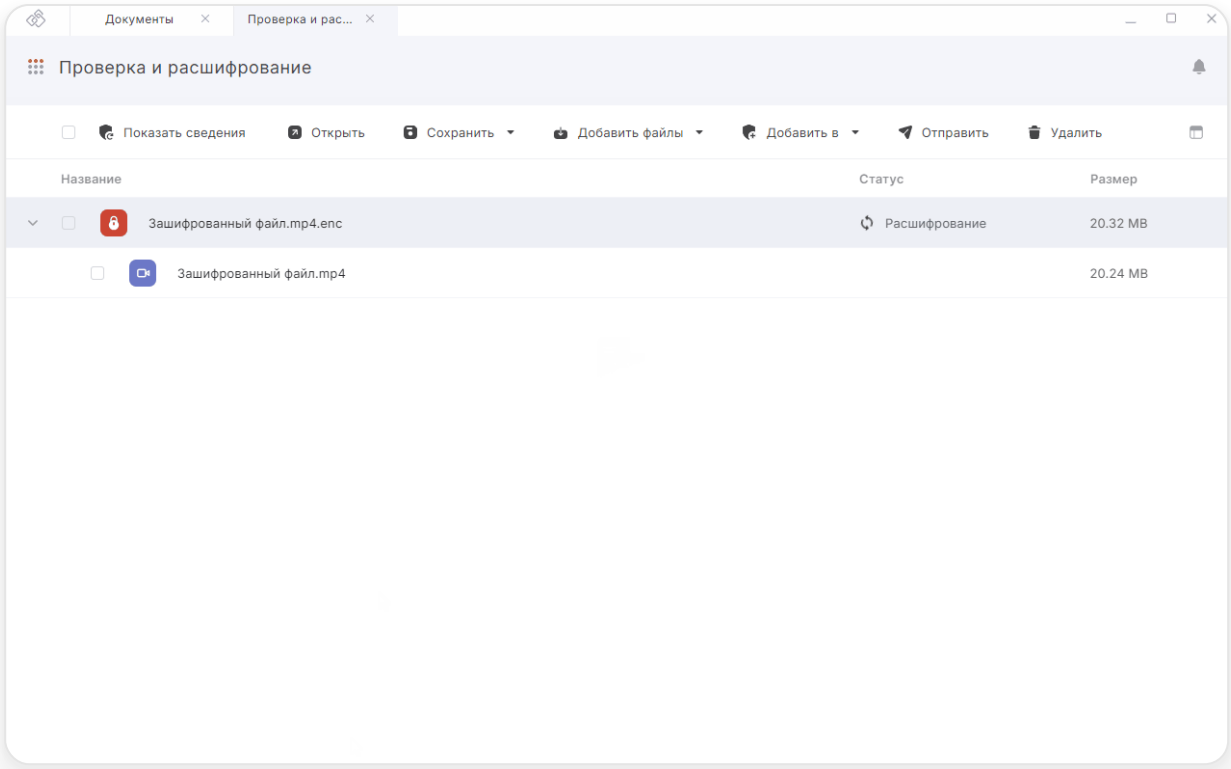
Важно. Прежде чем расшифровывать документы, убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP. Также для подписи и расшифрования документов необходима лицензия на КриптоАРМ и КриптоПро CSP.

Для расшифрования документов нужно установить в хранилище «Личные сертификаты» сертификат, в адрес которого было выполнено шифрование.

Чтобы оценить, готово ли ваше рабочее место для подписи, шифрования и расшифрования документов, воспользуйтесь Проверкой рабочего места.

Как расшифровать документ

1. Откройте мастер **Проверка и расшифрование** одним из способов:
    - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
    - Вызовите действие **Добавить в** → **Проверка и расшифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. После добавления документов будет запущен процесс расшифрования. На панели с зашифрованным документом отобразится статус «Расшифрование».
4. При необходимости укажите пароль на контейнер с сертификатом.
5. Расшифрованный фаил будет отображен под зашифрованным. На панели с зашифрованным документом отобразится статус «Расшифрован».



Статичный кадр демонстрации. Открыть анимацию

Результат выполнения операции

При успешном расшифровании полученные оригиналы документов сохраняются во временной папке и удаляются после выполнения другой операции.

Вы можете сохранить полученные после расшифрования документы на компьютере или в папку «Архив», нажав **Сохранить** и выбрав действие в меню **На компьютере** или **В Архив**.

Возможные уведомления

Ошибки, которые могут возникнуть при выполнении операции, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Не удалось открыть файл** — добавленные в мастер документы были удалены или по какой-то причине не доступны.
2. **Не удалось расшифровать файл** — добавлен пустой файл (с нулевым размером). Не найден сертификат для расшифрования.
3. **Не удалось расшифровать файл** — ошибки, связанные с истекшей лицензией КриптоПро CSP.

Инструкции по теме

1. Как установить личный сертификат.
2. Как добавить документы в мастер.
3. Как посмотреть уведомления.
4. Действия с результатами операций.

Открыть статью на сайте

Прямые групповые операции

В мастере **Подпись и шифрование** можно объединить подпись, архивирование и шифрование файлов в одну операцию.

Выполнение комбинации перечисленных операций принято называть «прямыми групповыми операциями».

Доступен выбор из следующих комбинаций:

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

Важно. Прежде чем подписывать документы, убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP. Также для подписи и расшифрования документов необходима лицензия на КриптоАРМ и КриптоПро CSP.

Чтобы подписывать документы электронной подписью, нужно установить в «Личное» хранилище сертификат с закрытым ключом.

Для шифрования документов нужно установить в хранилище «Других пользователей» сертификат или привязать сертификат к контакту, в адрес которого будет проводиться шифрование.

Выполнение прямых групповых операций осуществляется по аналогии с одиночными операциями:

- Как подписать документ
- Как зашифровать документ
- Как заархивировать документ

Инструкции по теме

1. Как установить личный сертификат.
2. Как импортировать сертификаты других пользователей.
3. Как привязать сертификат к контакту.
4. Как создать профиль подписи.
5. Как переключаться между профилями подписи.
6. Как добавить документы в мастер.
7. Как посмотреть уведомления.
8. Действия с результатами операций.

Открыть статью на сайте

Обратные групповые операции

Операции по расшифрованию, разархивированию, проверке и снятию подписи принято называть «обратными групповыми операциями».

Для выполнения перечисленных операций предназначен мастер **Проверка и расшифрование**.

Важно. Прежде чем приступить к расшифрованию, проверке и снятию подписи, убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP. Также для расшифрования документов необходима лицензия на КриптоАРМ и КриптоПро CSP.

Для расшифрования документов нужно установить в хранилище «Личные сертификаты» сертификат, в адрес которого было выполнено шифрование.

Для корректной проверки подписи у вас должны быть установлены корневой и промежуточные сертификаты подписанта документа.

Чтобы оценить, готово ли ваше рабочее место для выполнения обратных операций, воспользуйтесь Проверкой рабочего места.

Выполнение обратных групповых операций осуществляется по аналогии с одиночными операциями:

- Как расшифровать документ
- Как проверить подпись документа
- Как снять подпись с документа

Инструкции по теме

1. Как добавить документы в мастер.
2. Как посмотреть уведомления.
3. Как проверить подпись.
4. Действия с результатами операций.
5. Как установить личный сертификат.

Открыть статью на сайте

Результаты операций

Результаты прямых операций

В мастере **Подпись и шифрование** во время выполнения прямых операции появляется панель с индикатором выполнения и кнопкой «Отмена». Операции происходят с документами последовательно. Если вы нажмёте на кнопку «Отмена», операция будет приостановлена на том документе, с которым производилась операция на момент отмены.

Если операция прошла успешно, файлы будут сохранены в каталоге, который был указан в настройках мастера. Если каталог не указывался, то результаты будут размещены рядом с исходным файлом.

Если установлен флаг **Создать копию в Архиве**, то копия с результатами операции сохранится в специальную папку **Архив**.

После выполнения операции происходит автоматическая проверка подписи. На иконке документа с действительной подписью отображается зеленая галочка. На иконке документа с недействительной подписью - красный крестик.



В результатах операции можно посмотреть информацию о подписи. Подробнее в инструкции Как открыть сведения о подписи документа.

Результаты обратных операций

В мастере **Проверка и расшифрование** во время выполнения обратных операции на панели с документом отображается статус: «Расшифрование», «Разархивирование», «Проверка подписи» или «Снятие подписи». После завершения операции статусы меняются на: «Расшифрован», «Разахивирован», «Подпись действительна» или «Подпись недействительна». Файл, полученный в результате обратной операции, отображается под исходным.

Действия с документами в результатах операции

- **Показать сведения** — в правой боковой панели показывается информация о файле. Подробнее в инструкции Просмотр информации о документе.
- **Открыть** — файл открывается с помощью программы по умолчанию. Подробнее в инструкции Просмотр документа.

- **Сохранить в Архив** — позволяет вам сохранить документ в специальную папку. Файлы данной папки доступны в **Архиве**. Если в данной папке файл с таким именем уже существует, то он не заменяется на новый.
- **Добавить в** — вы можете выбрать мастер, в который будут добавлены выделенные в списке документы для выполнения дополнительных операций.
- **Промежуточные файлы** — по кнопке отображаются промежуточные файлы, которые были созданы во время операции. Данные файлы располагаются во временной папке. При отображении промежуточных файлов название кнопки меняется на **Скрыть промежуточные**, при нажатии на которую файлы скрываются, в списке остаются только полученные после операций документы.

Инструкции по теме

1. Как посмотреть уведомления.
2. Как проверить подпись.
3. Как открыть документ для просмотра.

Открыть статью на сайте

Загрузка PDF-документа

Для начала работы необходимо загрузить документ.

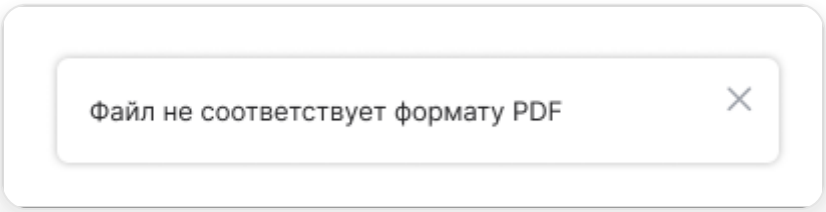
Допускается загрузка одного документа в формате PDF.

Загрузить документ можно несколькими способами:

- Перетащить файл с помощью мыши в область приложения.
- Нажать кнопку **Загрузить с компьютера** и выбрать файл в файловом менеджере.

При загрузке документа происходит проверка документа на формат PDF и на содержание в документе подписи и размеченных областей.

Если документ соответствует формату PDF, то он загружается в мастер. Для загруженного файла становятся доступны функции просмотра документа. Если документ не соответствует формату PDF, появляется уведомление об ошибке. Следует выбрать другой документ.

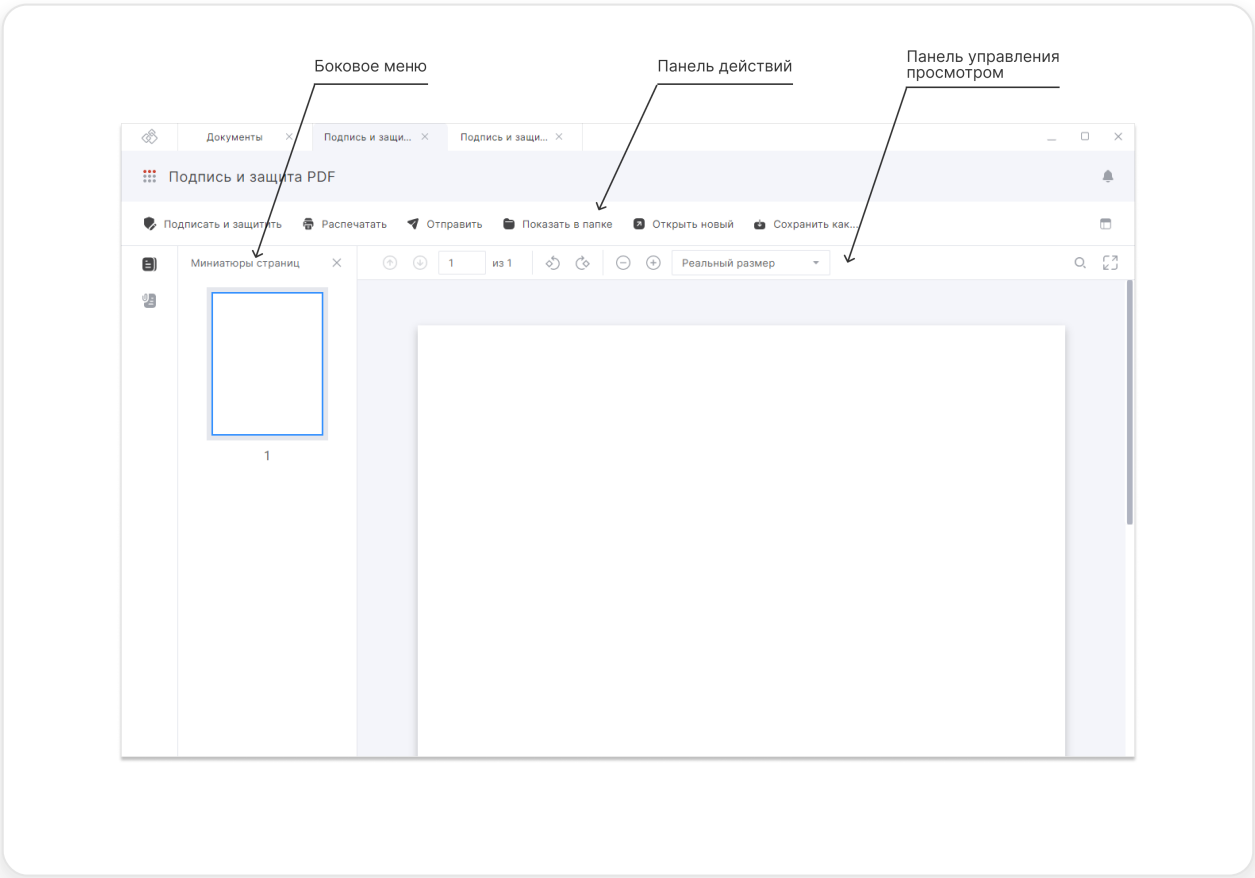


Если документ содержит одну или несколько подписей, то запускается проверка валидности подписей. Подробнее в Проверка подписи PDF-документа.

Открыть статью на сайте

Просмотр PDF-документа

Для загруженного документа становятся доступны панель действий, панель управления просмотром и боковое меню.

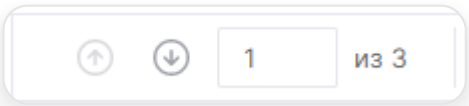


Панель действий содержит кнопки вызова функций для работы с PDF-документом:

- **Подписать и защитить** – переход к настройкам подписи и разметке областей.
- **Распечатать** – отправка документа на печать.
- **Показать в папке** – открытие каталога, в котором располагается файл.
- **Открыть новый** – замена загруженного документа.
- **Сохранить как** – создание копии документа.
- **Подробно** – открытие правой боковой панели, содержащей подробные сведения о файле или подписи документа.

Панель управления просмотром позволяет настраивать режимы просмотра PDF-документа:

- **Следующая и предыдущая страницы** - переход между страницами по стрелкам вверх и вниз. Также можно ввести номер страницы в текстовом поле, чтобы перейти к нужной странице.



- **Повернуть против и по часовой стрелке** – поворот страниц документа с шагом 90 градусов. Это действие не является изменением ориентации страницы.



- **Уменьшить и увеличить** – уменьшение или увеличение масштаба отображения страниц документа. При изменении масштаба автоматически меняется значение в поле выбора масштаба. Возможно изменение масштаба страниц документа с помощью меню.

- **Найти в документе** – поиск слов внутри документа.
- **На весь экран и свернуть** – скрыть или развернуть панель действий и панель с кнопкой основного меню и заголовком раздела.

В **боковом меню** доступна навигация по содержимому документа:

- **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.

Открыть статью на сайте

Подпись PDF-документа

Для обеспечения юридической значимости, гарантии авторства и неизменности содержания файла PDF-документы могут быть подписаны «встроенной» электронной подписью.

«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.

Важно. Если подписанный документ содержит свободные размеченные области для подписантов, то можно поставить подпись в любую из этих свободных областей.

С чего начать

1. Убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP и имеется действующая лицензия на КриптоАРМ и КриптоПро CSP.
2. Установите личный сертификат.
    - Как установить сертификат из ключевого контейнера
    - Как установить сертификат из файла .pfx
    - Как установить сертификат из DSS
    - Как создать самоподписанный сертификат
3. Настройте профиль подписи
    - Как создать профиль подписи

Чтобы оценить, готово ли ваше рабочее место для подписи документов, воспользуйтесь Проверкой рабочего места.

Как подписать документ PDF

Важно! Чтобы подписать несколько PDF-документов, воспользуйтесь мастером **Подпись и шифрование**.

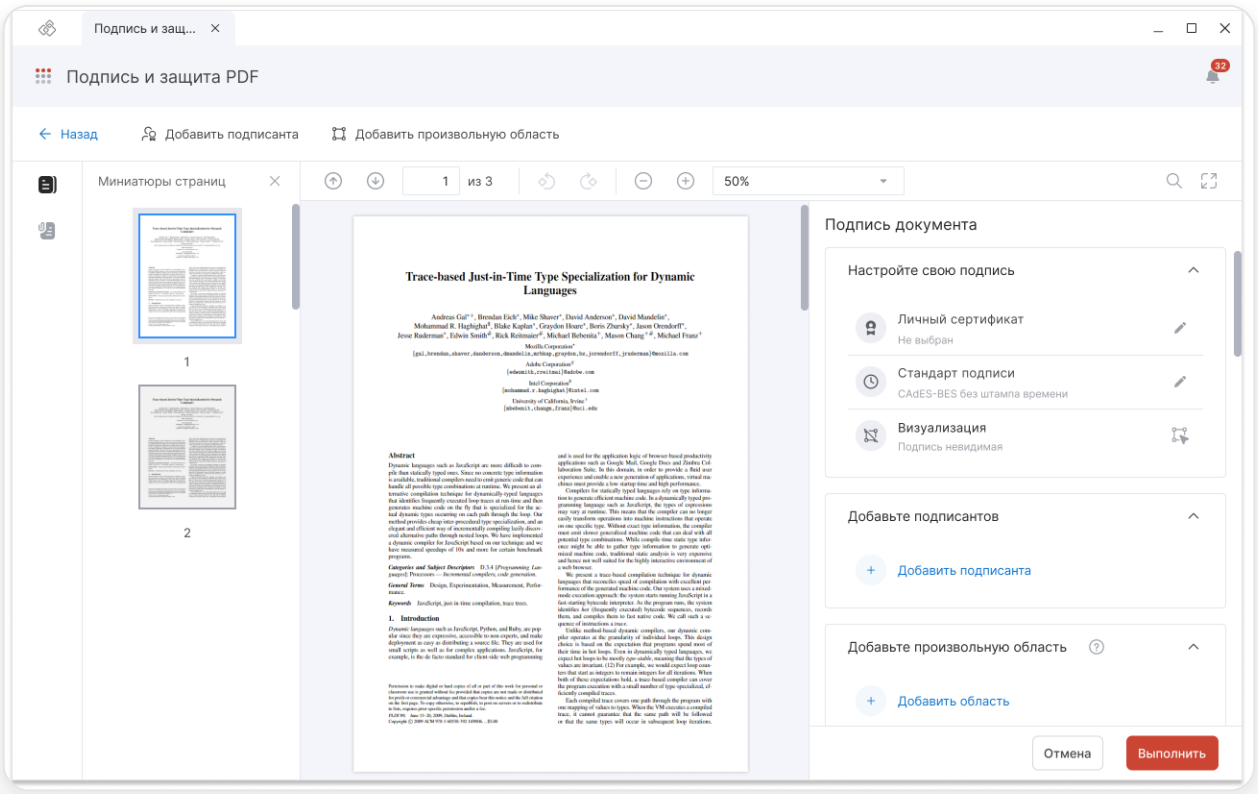
1. Загрузите PDF-документ. Подробнее в инструкции Загрузка PDF-документа.
2. Нажмите на кнопку **Подписать и защитить** на панели действий.
3. В открывшейся правой боковой панели укажите настройки, либо выберите профиль подписи с заранее сохраненным шаблоном настроек.:
    - Выберите сертификат подписи.
    - Настройте стандарт подписи.

- При необходимости разместите штамп для личной подписи и настройте его оформление.
- При необходимости добавьте подписантов.
- При необходимости добавьте произвольную область и настройте ее оформление.
- Настройте параметры защиты PDF-документа.

4. Укажите каталог для сохранения результата операции.

5. Нажмите кнопку **Выполнить**.

При успешном выполнении операции новый файл сохраняется в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан. Документ открывается в режиме просмотра и проверки подписи.

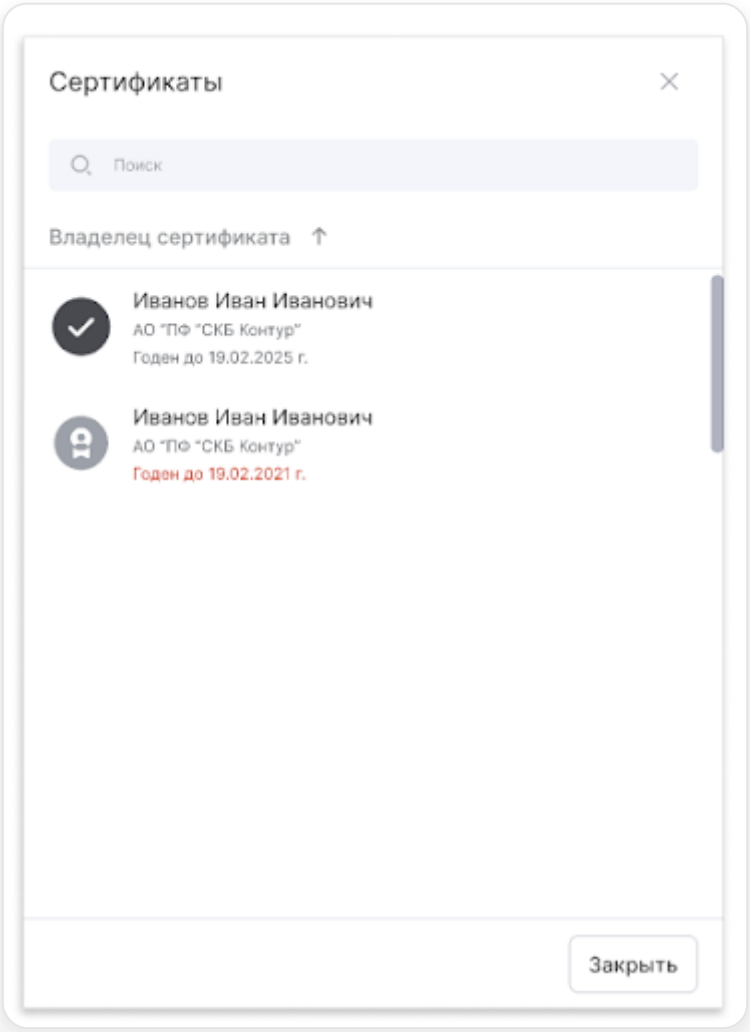


Как выбрать сертификат в мастере

1. Нажмите на кнопку **Выбрать** в блоке **Личный сертификат**.
2. В открывшейся правой боковой панели отметьте чекбоксом нужный сертификат.
3. Закройте панель с помощью кнопки **Закрыть**.

Выбранный сертификат можно изменить с помощью кнопки **Заменить** в блоке **Личный сертификат**.

Важно. Для подписи необходимо указать сертификат с привязкой к закрытому ключу. Если в приложении такой сертификат отсутствует, то можно установить его в разделе **Сертификаты**.



Как настроить стандарт подписи в мастере

В приложении доступна подпись PDF-документа со стандартами:

- **CAdES-BES** - «классическая» подпись;
- **CAdES-T** - подпись, которая содержит информацию о времени создания подписи (TSP);
- **CAdES-X Long Type 1** - подпись, которая содержит информацию о времени создания подписи (TSP) и о статусе сертификата электронной подписи (OCSP) в момент подписания;
- **CAdES-A** - подпись с архивными штампами времени.

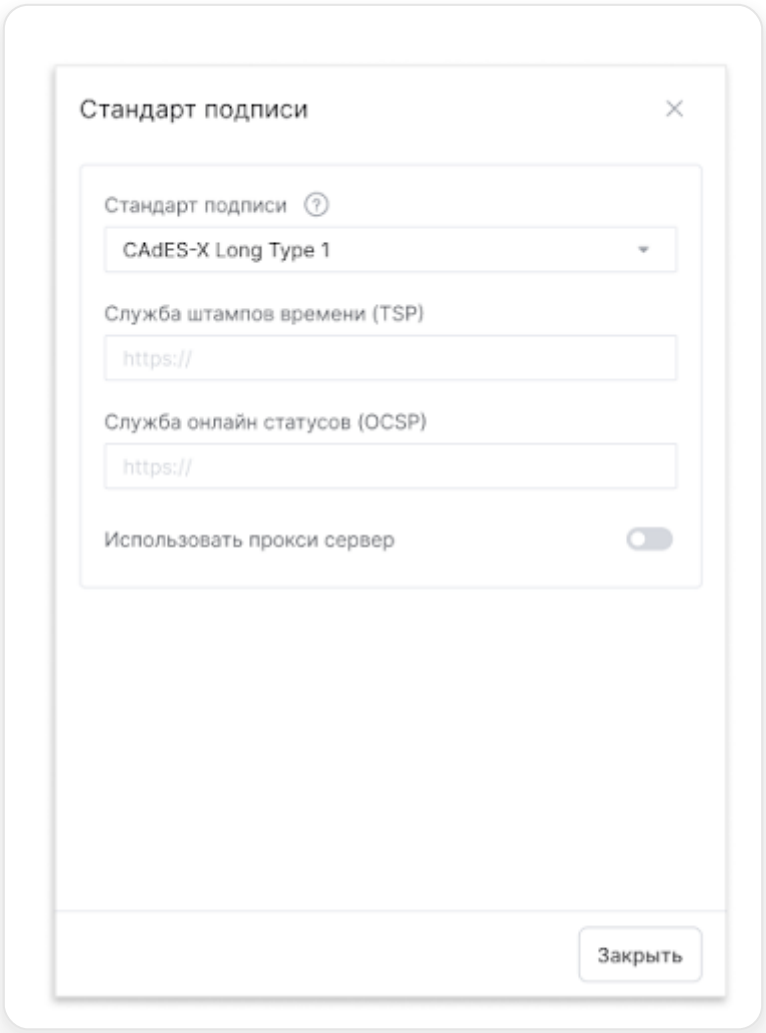
По умолчанию будет произведена «классическая» подпись со стандартом CAdES-BES.

Важно. Создание подписи со штампами возможно только при установленных модулях КриптоПро TSP Client и КриптоПро OCSP Client и лицензий на них.

Чтобы выбрать стандарт подписи:

1. Нажмите кнопку **Редактировать** в блоке **Стандарт подписи**.
2. В появившейся правой боковой панели выставите необходимый стандарт подписи.

3. Для стандартов CAdES-T, CAdES-X Long Type 1 и CAdES-A заполните обязательное поле **Служба штампов времени** (TSP). Адрес службы штампов времени можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры.
4. Поле **Служба онлайн статусов** (OCSP) заполняется в случае, если адрес отсутствует в сертификате.
5. Если при подключении к службам TSP и OCSP используется прокси сервер, активируйте настройку **Использовать прокси сервер** и укажите настройки подключения.
6. Закройте панель с настройкой стандарта подписи по кнопке **Закрыть**.



Изменить настройки стандарта можно нажатием кнопки **Редактировать** в блоке **Стандарт подписи**.

Как разметить область для штампа подписи

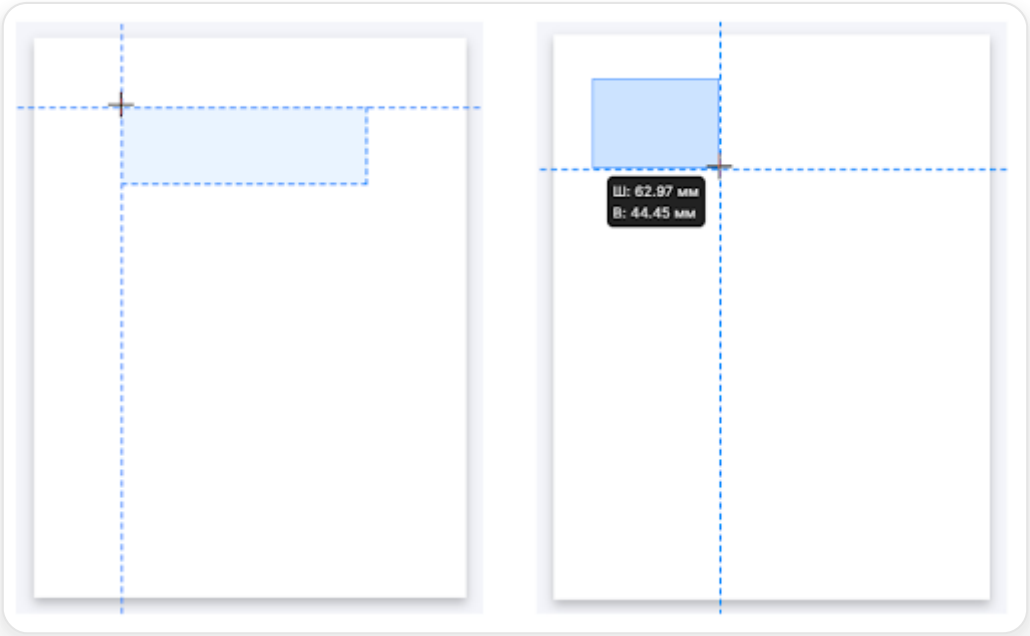
Личная подпись может быть добавлена в документ как видимая или невидимая.

Видимая подпись отображается на странице документа в виде штампа. Невидимая подпись визуально на странице документа не видна. При проверке как видимой, так и невидимой подписи можно получить сведения о статусе подписи и сертификате подписанта.

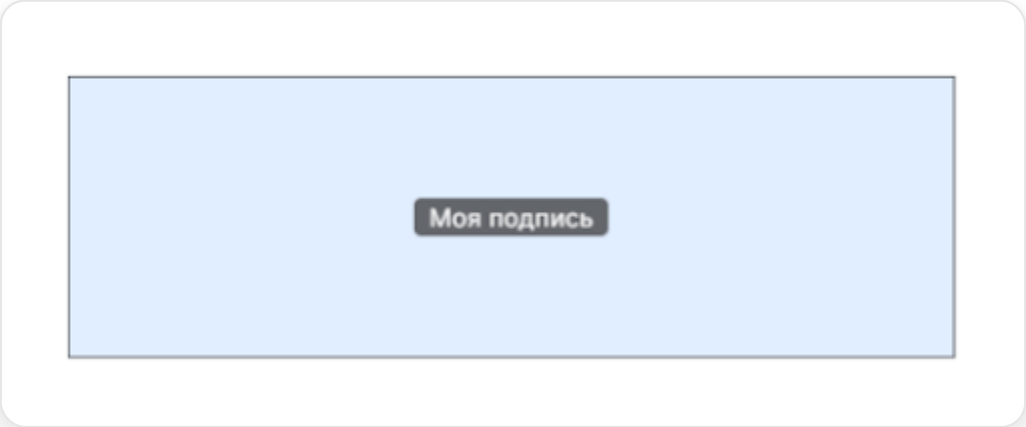
По умолчанию будет проставлена видимая подпись.

Чтобы разместить штамп для видимой подписи:

1. Нажмите кнопку **Разметить** в блоке **Визуализация**.
2. На странице документа появятся пунктирные направляющие. При наведении курсора мыши на пересечении направляющих отобразится схематичный прямоугольник.
3. Наведите курсор мыши в место размещения штампа на странице документа и кликните левой кнопкой мыши. В этом случае размер области будет соответствовать размеру схематичного прямоугольника. Для того чтобы задать собственный размер области, наведите курсор мыши в место размещения штампа и, зажав левую кнопку мыши, разметьте область нужного размера.

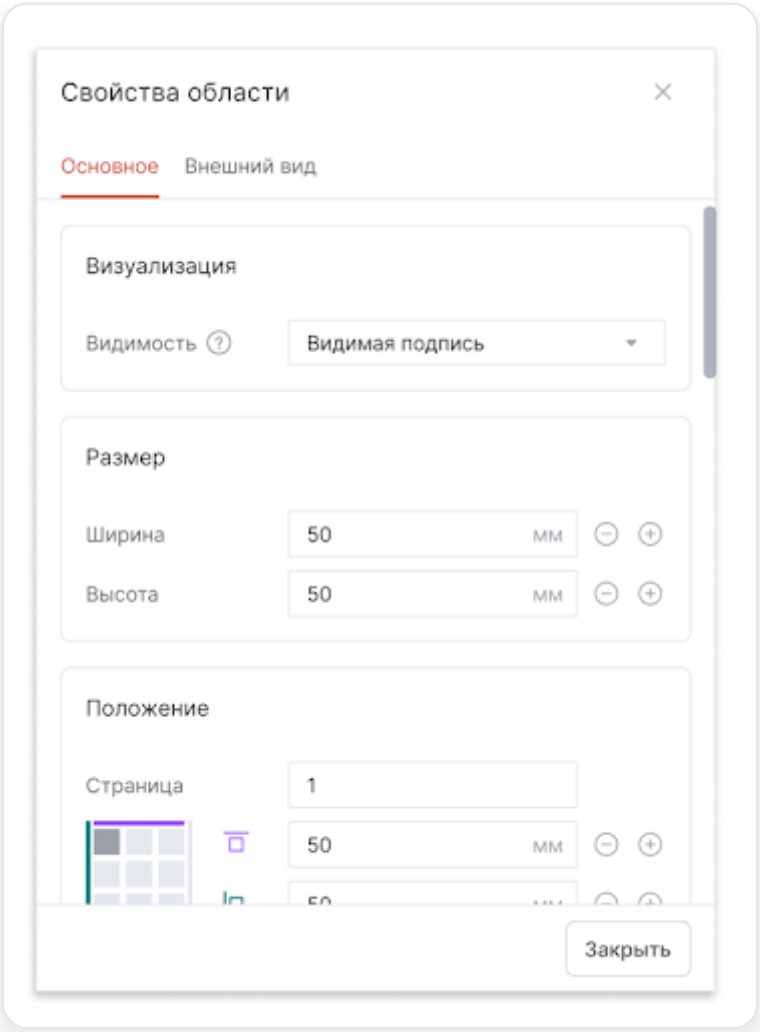


Важно. После разметки в области для подписи будет отображен лейбл **Моя подпись**. Лейбл носит информационный характер и не будет отображаться после подписи документа.



Как изменить размер и положение области для штампа подписи

1. Нажмите на кнопку **Свойства** в блоке **Визуализация**. Откроется правая боковая панель **Свойства области**.
2. В блоке **Размер** укажите новые значения ширины и высоты области в миллиметрах.
3. В блоке **Положение** измените страницу расположения области, способ выравнивания области на странице и укажите новые значения для отступов от края страницы.
4. Закройте панель с настройкой положения области по кнопке **Закрыть**.



Как изменить вид подписи с видимой на невидимую

1. Нажмите на кнопку **Свойства** в блоке **Визуализация**. Откроется правая боковая панель **Свойства области**.
2. В блоке **Визуализация** выставите настройку **Видимость** на **Невидимая подпись**.
3. Закройте панель с настройкой положения области по кнопке **Закрыть**.

Как настроить оформление штампа подписи

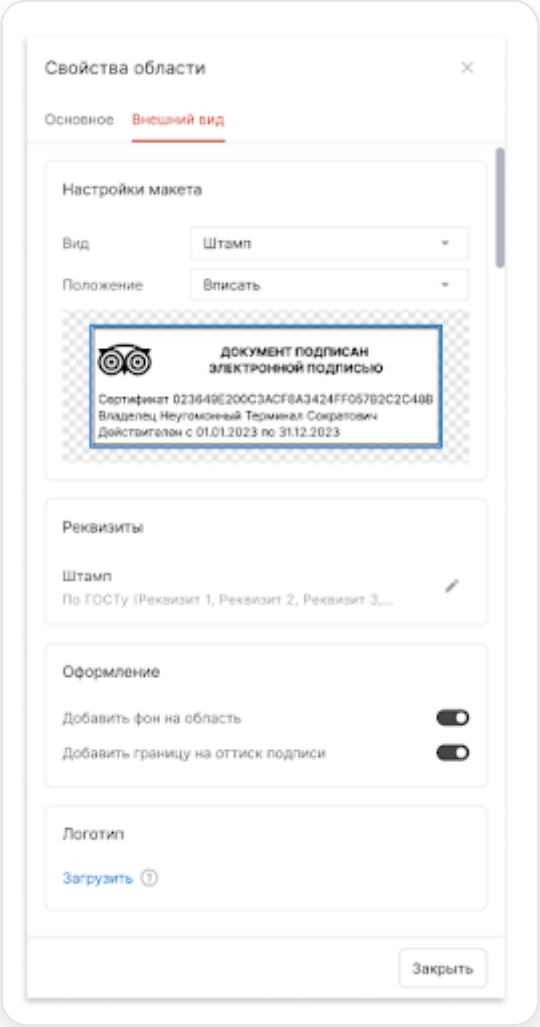
По умолчанию визуализация информации об электронной подписи задается в соответствии с требованиями ГОСТ Р 7.0.97-2016. В штамп подписи выводятся заголовок «Документ подписан электронной подписью», серийный номер сертификата, имя владельца сертификата и срок действия сертификата.

1. Разместите штамп подписи на странице документа.
2. Нажмите на кнопку **Свойства** в блоке **Визуализация**.
3. В появившейся правой боковой панели перейдите на вкладку **Внешний вид**.

4. Настройте **Вид штампа** в блоке **Настройки макета**:
    - Штамп - в области будет размещен только штамп.
    - Штамп с реквизитами слева - в области будет размещен штамп, а также блок с реквизитами слева от штампа.
    - Штамп с реквизитами справа - в области будет размещен штамп, а также блок с реквизитами справа от штампа.
    - Штамп с реквизитами слева и справа - в области будет размещен штамп, а также блок с реквизитами слева и справа от штампа.



5. Настройте вывод информации в штампе. Для этого нажмите на кнопку **Редактировать** в блоке **Реквизиты** и укажите вывод информации **По ГОСТу** или **Произвольно**:
    - По ГОСТу - в штамп будут выведены обязательные реквизиты, перечисленные в ГОСТ.
    - Произвольно - самостоятельная настройка выводимых реквизитов.
6. Аналогичным образом настройте вывод информации для блоков слева или справа от штампа, если их отображение активировано.
7. Настройте отображение границы и фона штампа в блоке Оформление.
8. Загрузите изображение с гербом или эмблемой в блоке Логотип. Изображение будет размещено в верхнем левом углу штампа подписи.



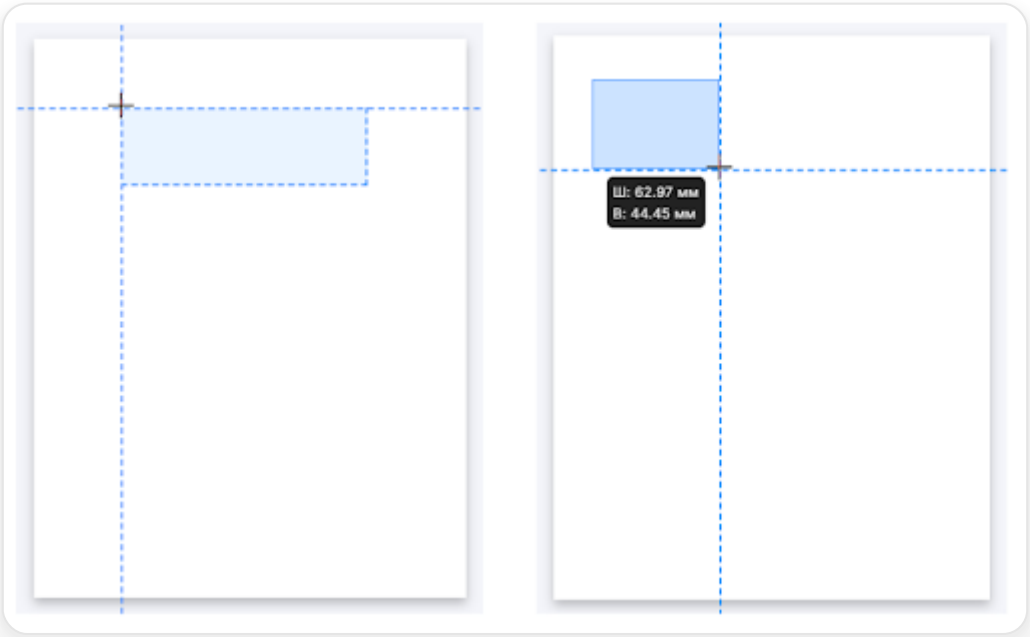
Как добавить подписантов

В приложении в документ можно добавить до 10 подписантов. По аналогии с личной подписью подпись подписантов может быть видимой и невидимой.

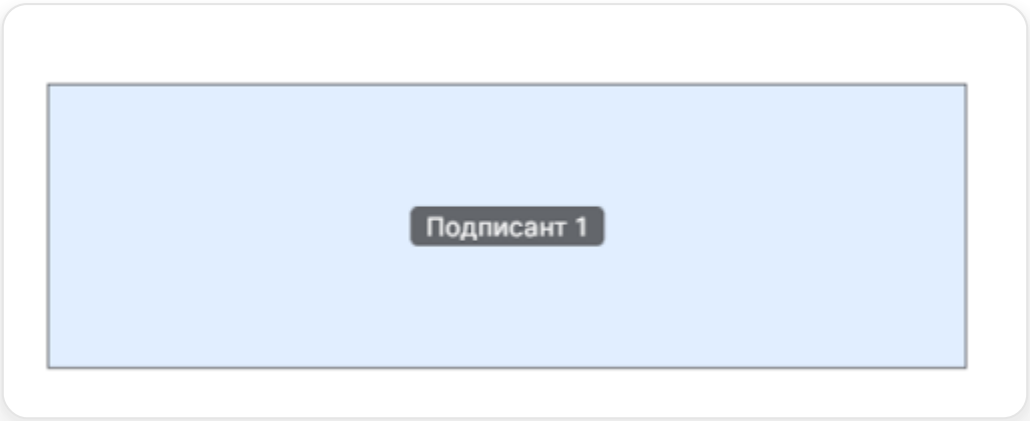
1. Нажмите кнопку **Добавить подписанта**.
2. В блоке **Добавьте подписантов** появится подписант с невидимой подписью.

Как разметить область для подписи подписанта

1. Нажмите кнопку **Разметить** на панели с подписантом.
2. На странице документа появятся пунктирные направляющие. При наведении курсора мыши на пересечении направляющих отобразится схематичный прямоугольник.
3. Наведите курсор мыши в место размещения штампа на странице документа и кликните левой кнопкой мыши. В этом случае размер области будет соответствовать размеру схематичного прямоугольника. Для того, чтобы задать собственный размер области, наведите курсор мыши в место размещения штампа и, зажав левую кнопку мыши, разметьте область нужного размера.

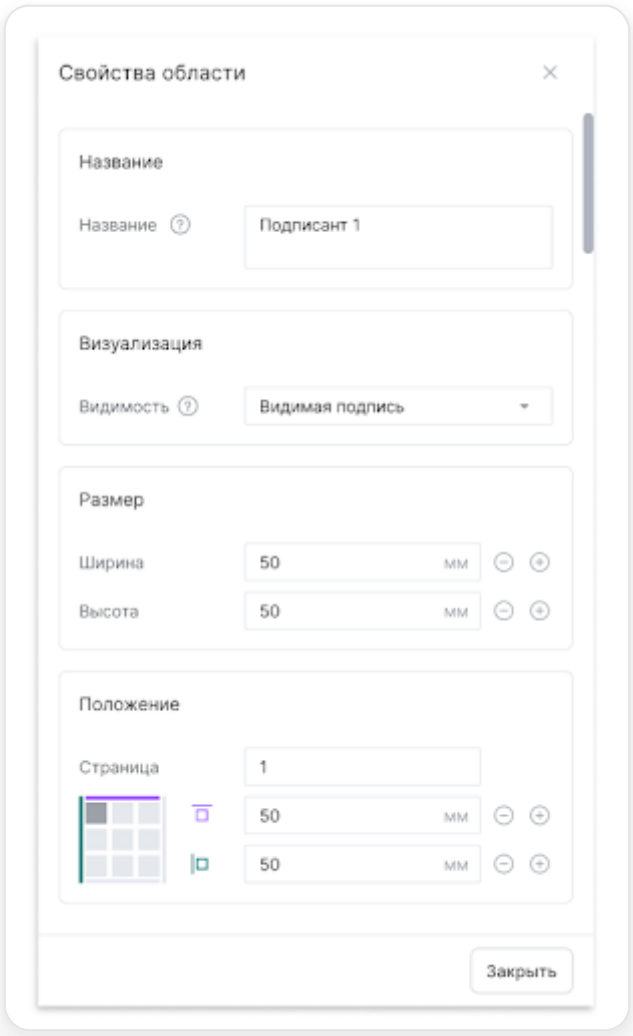


Важно. После разметки в области для подписанта будет отображен лейбл с названием подписанта. Лейбл носит информационный характер и не будет отображаться после простановки подписи в область.



Как изменить размер и положение области для подписанта

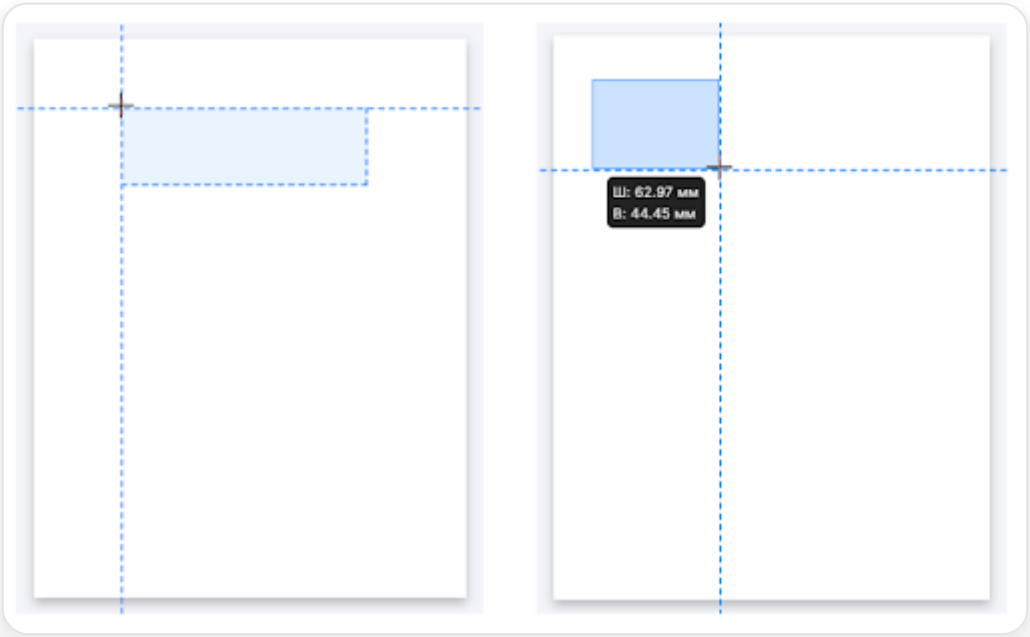
1. Нажмите на кнопку **Свойства** в блоке **Визуализация**. Откроется правая боковая панель **Свойства области**.
2. В блоке **Размер** укажите новые значения ширины и высоты области в миллиметрах.
3. В блоке **Положение** измените страницу расположения области, способ выравнивания области на странице и укажите новые значения для отступов от края страницы.
4. Закройте панель с настройкой положения области по кнопке **Закрыть**.



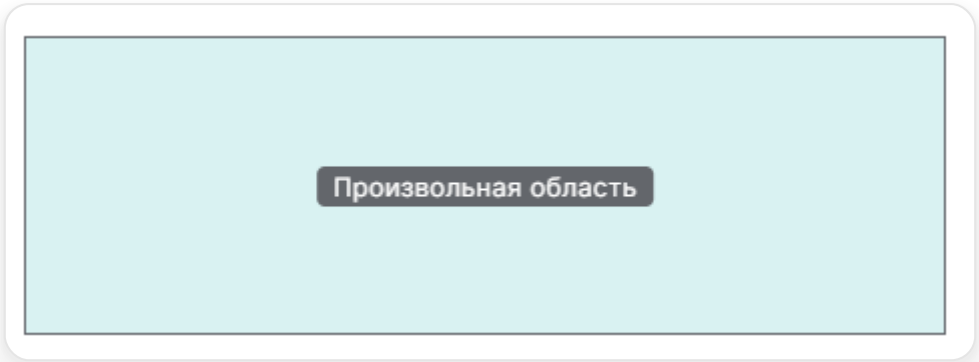
Как разместить произвольную область

Произвольная область – это область для графического изображения или текста. В области можно разместить свой комментарий, статус или отметку о конфиденциальности документа.

1. Нажмите кнопку **Добавить область** в блоке **Добавьте произвольную область**.
2. На странице документа появятся пунктирные направляющие. При наведении курсора мыши на пересечении направляющих отобразится схематичный прямоугольник.
3. Наведите курсор мыши в место размещения штампа на странице документа и кликните левой кнопкой мыши. В этом случае размер области будет соответствовать размеру схематичного прямоугольника. Для того, чтобы задать собственный размер области, наведите курсор мыши в место размещения штампа и, зажав левую кнопку мыши, разметьте область нужного размера.

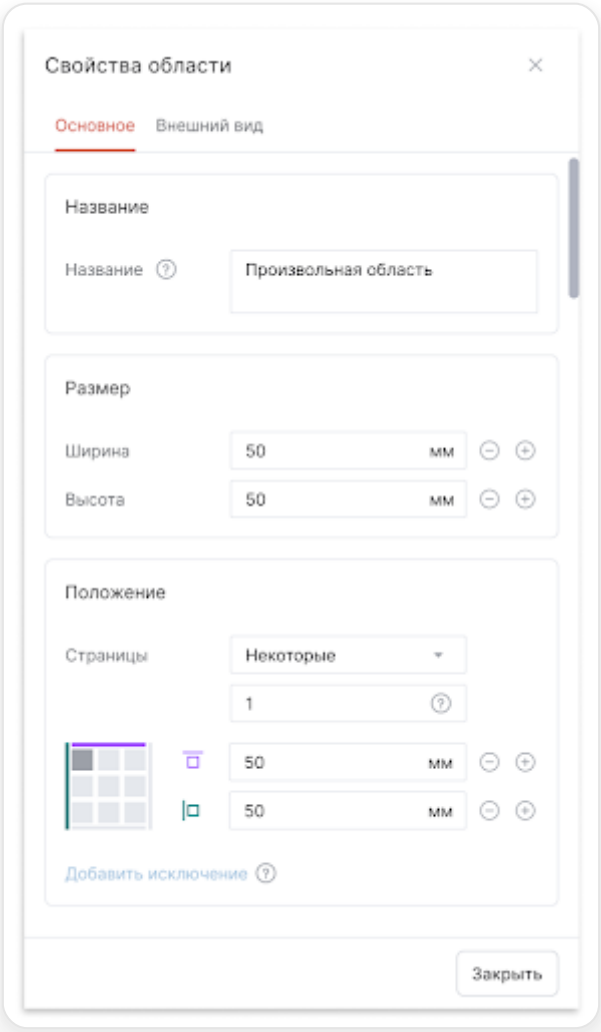


Важно. После разметки в области для штампа будет отображен лейбл с названием области. Лейбл носит информационный характер и не будет отображаться после настройки внешнего вида штампа.



Как изменить размер и положение произвольной области

1. Нажмите на кнопку **Свойства** в блоке **Добавьте произвольную область**. Откроется правая боковая панель **Свойства области**.
2. В блоке **Название** укажите новое название для области.
3. В блоке **Размер** укажите новые значения ширины и высоты области в миллиметрах.
4. В блоке **Положение** настройте страницы расположения области, способ выравнивания области на странице и укажите новые значения для отступов от края страницы. Если на некоторых страницах документа требуется поместить штамп в другом месте, то можно использовать настройку Добавить исключение.
5. Закройте панель с настройкой положения области по кнопке **Закрыть**.



Как удалить произвольную область

Чтобы удалить произвольную область из документа нажмите на кнопку **Удалить** в блоке **Добавьте произвольную область**.

Важно. Нельзя удалить произвольную область в подписанном документе.

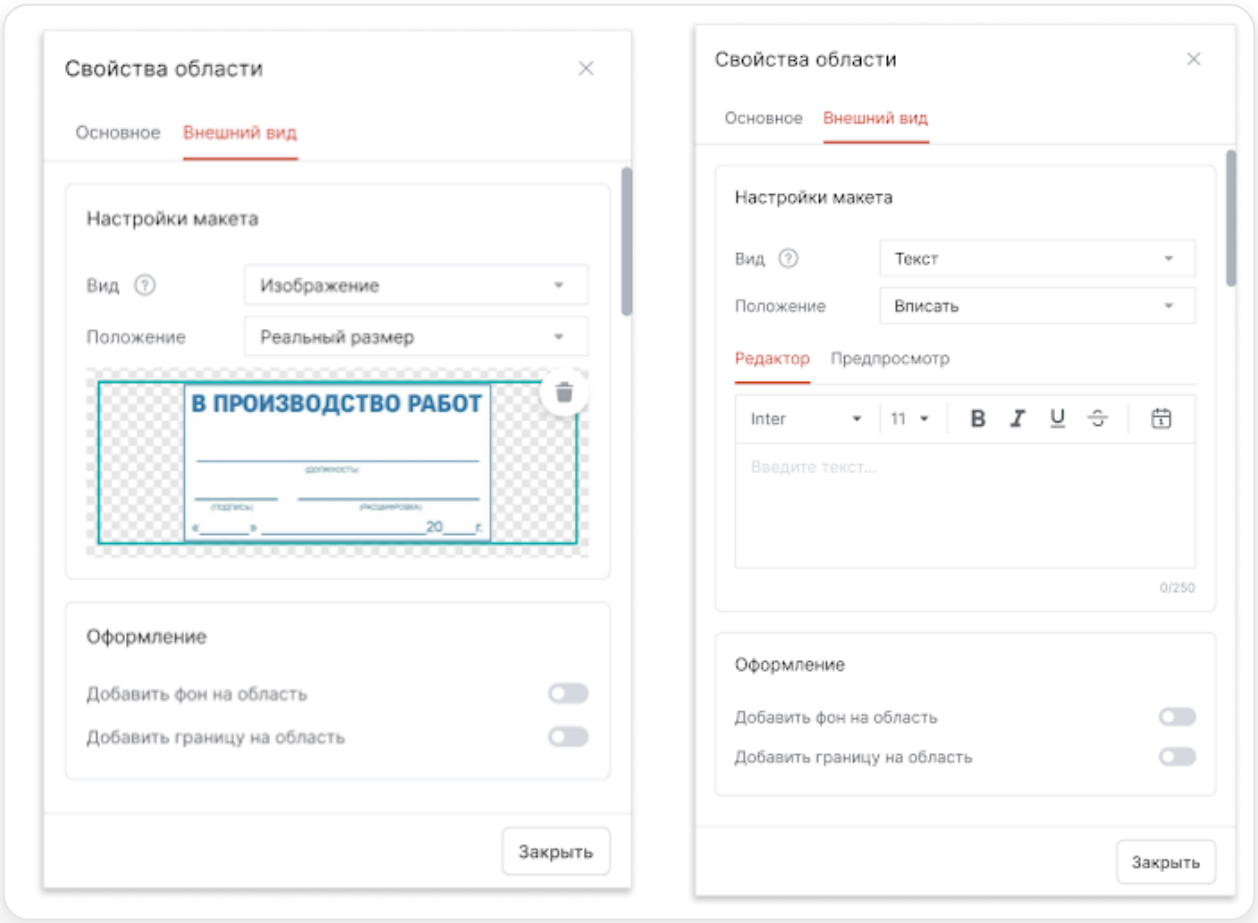
Как настроить оформление произвольной области

Примечание. В произвольную область можно загрузить любое изображение или напечатать текст.

1. Разместите область на странице документа.
2. Нажмите на кнопку **Свойства** в блоке **Добавьте произвольную область**.
3. В появившейся правой боковой панели перейдите на вкладку **Внешний вид**.
4. 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.

5. 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.
6. Настройте прозрачность контента произвольной области и отображение границы и фона штампа в блоке **Оформление**.



Настройка сохранения результата

Для подписанного документа можно настроить каталог для сохранения результата.

Для этого в блоке **Сохранение** результатов необходимо выбрать вариант сохранения:

1. **Папка с исходным документом**. В таком случае подписанный файл сохраняется рядом с исходным файлом. Настройка выбрана по умолчанию.
2. **Сохранить в папку...** При выборе опции становится доступно поле для выбора каталога. Для автоматического сохранения результата операции в папке **«Архив»** нужно активировать настройку **Создать копию в папке «Архив»**.

Выполнение операции

Перед выполнением операции происходит проверка на корректность заполнения настроек и возможность выполнения.

При успешном выполнении операции новый файл сохраняется в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан. Происходит запись события в **Журнал событий**.

Подписанный документ открывается в режиме просмотра и проверки подписи.

Ошибки, которые могут возникнуть при выполнении операции, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Если были внесены изменения в настройки подписи, то по кнопке **Назад** или при нажатии на кнопку **Отмена** в правой боковой панели возникает окно с предупреждением. Настроенные параметры подписи не запоминаются программой, если ранее не были сохранены в **Профиль подписи**.

Открыть статью на сайте

Сертификация PDF-документа

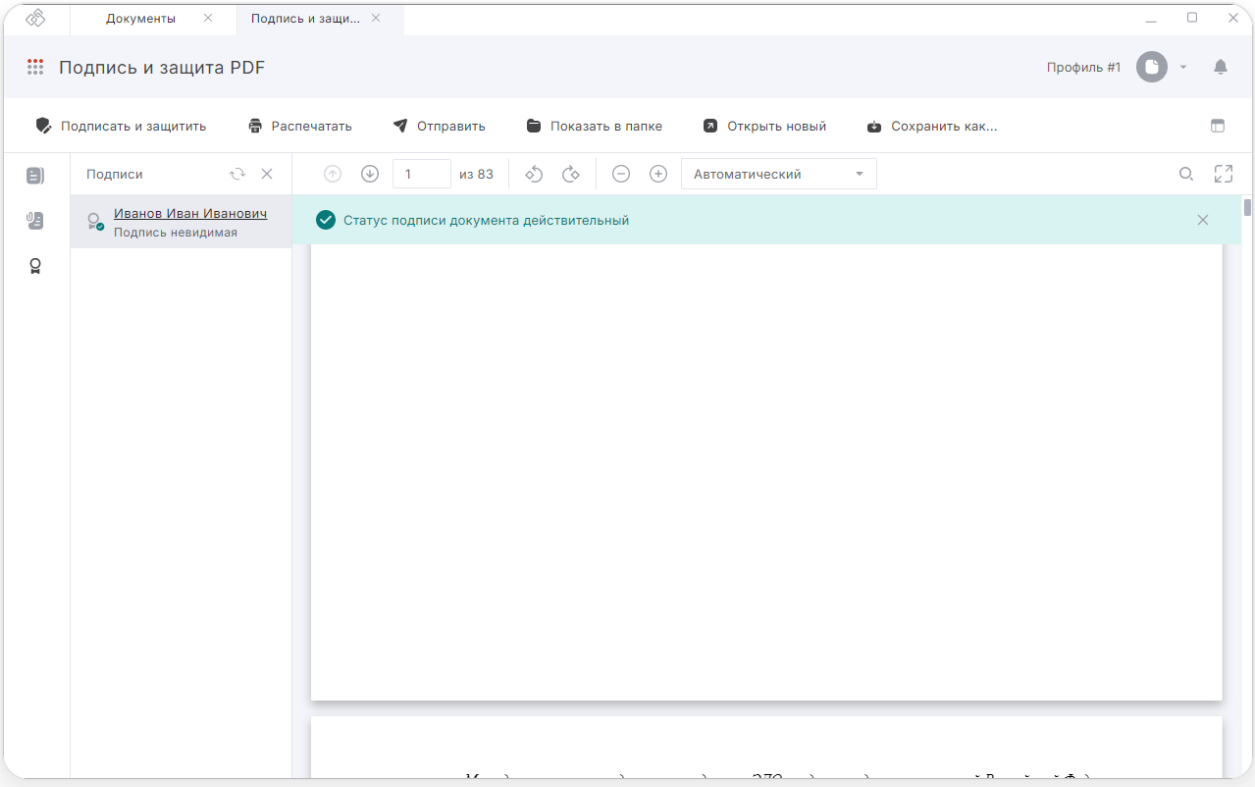
Сертификация позволяет защитить PDF-документ от изменений путем его подписания электронной подписью, с указанием типа изменений, разрешенных для документа. В приложении при сертификации разрешается заполнение размеченных областей для подписантов и для произвольной области. При сертификации выполняется обязательная конвертация документа в формат PDF/A-2b. Подробнее.

Важно. Сертификация доступна только для неподписанных документов.

Как сертифицировать документ PDF

1. Загрузите PDF-документ.
2. Нажмите кнопку **Подписать и защитить** на панели действий.
3. Укажите настройки подписи, перечисленные в Подпись PDF-документа.
4. Нажмите кнопку **Выполнить**.

При успешном выполнении операции новый файл сохраняется в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан. Документ открывается в режиме просмотра и проверки подписи.



Открыть статью на сайте

Конвертация PDF-документа

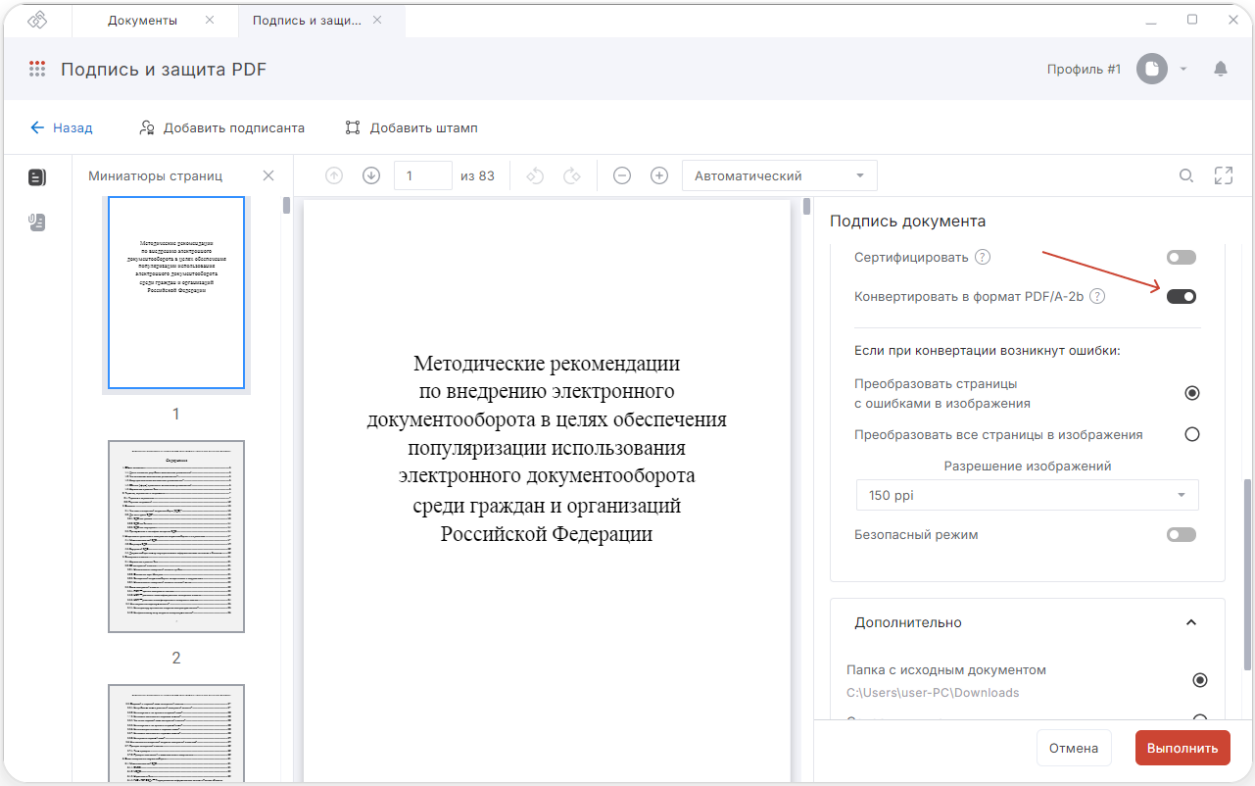
При конвертации документа в формат PDF/A-2b происходит удаление скриптов, форм и прочие элементов, влияющие на безопасность и целостность документа.

Важно:

- Конвертация выполняется только вместе с подписью документа.
- Конвертация доступна только для неподписанных документов.

Как конвертировать документ PDF

1. Загрузите PDF-документ.
2. Нажмите кнопку **Подписать и защитить** на панели действий.
3. Укажите настройки подписи, перечисленные в Подпись PDF-документа.
4. Активируйте настройку **Конвертировать в PDF/A-2b** в блоке **Защитите документ**.
5. При возникновении ошибок в ходе конвертации можно настроить вариант действий с документом:
   - Преобразовать страницы с ошибками в изображения (выставлено по умолчанию).
   - Преобразовать все страницы в изображения.
   - Остановить операцию и сообщить об ошибке.
6. Укажите каталог для сохранения результата операции.
7. Нажмите кнопку **Выполнить**.



При успешном выполнении операции новый файл сохраняется в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан. Документ открывается в режиме просмотра и проверки подписи.

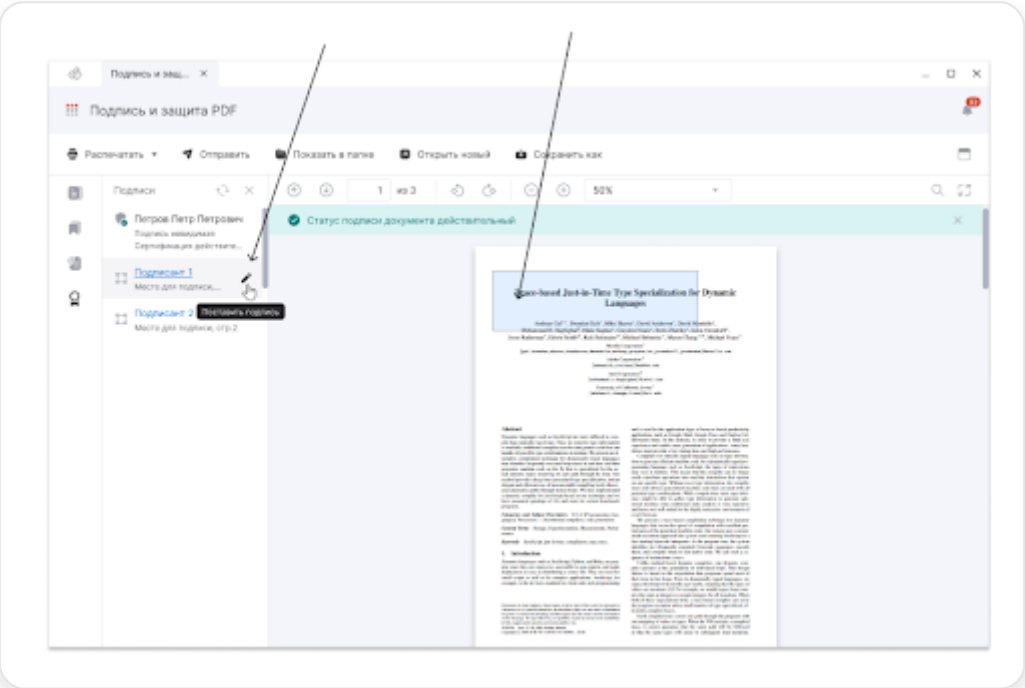
Открыть статью на сайте

Подпись PDF-документа в существующую разметку

Если подписанный документ содержит свободные размеченные области для подписантов, то можно поставить подпись в любую из этих свободных областей.

1. Загрузите PDF-документ.
2. Наведите курсор мыши на область в боковом меню и нажмите на кнопку **Поставить подпись**, либо кликните по области на странице документа.
3. В открывшейся правой боковой панели:
   - Выберите сертификат подписи.
   - Настройте стандарт подписи.
   - При необходимости настройте оформление произвольной области.
4. Укажите каталог для сохранения результата операции.
5. Нажмите кнопку **Выполнить**.

При успешном выполнении операции новый файл сохраняется в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан. Документ открывается в режиме просмотра и проверки подписи.

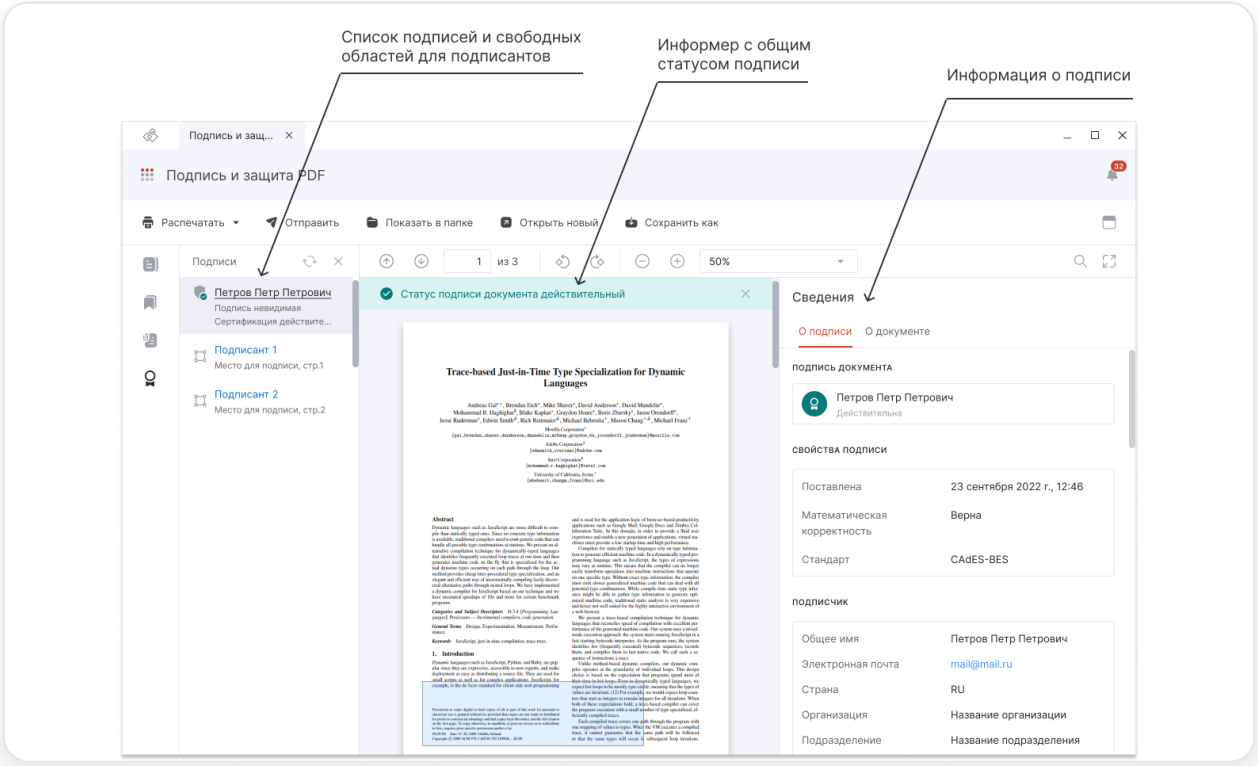


Открыть статью на сайте

Проверка подписи PDF-документа

Общий статус подписи отображается в виде информера в области просмотра документа.

Список подписей PDF-документа и свободных областей для подписантов выводятся в боковом меню.



Для просмотра подробной информации о подписи необходимо выделить подпись в списке бокового меню и нажать кнопку **Подробно** в строке с подписью или на панели действий.

Важно. Если в документе статус подписи недействительный из-за недействительности сертификата, то следует проверить построение цепочки сертификатов и, если потребуется, установить недостающие сертификаты. Подробнее в инструкции Установка корневого и промежуточного сертификатов.

Открыть статью на сайте

Выполнение операций в командной строке или терминале

В данном разделе описана инструкция по выполнению криптографических операций с помощью командной строки (для Windows) и терминала (для Unix-подобных операционных систем).

Важно. Прежде чем подписывать документы, убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP. Также для подписи документов необходима лицензия на КриптоАРМ и КриптоПро CSP.

Для выполнения команд в консоли необходимо придерживаться определенного синтаксиса при написании команды.

- `-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.

Все команды и параметры пишутся через пробел.

Важно. Перед вводом команды необходимо указать путь до исполняемого файла. После указания пути до исполняемого файла необходимо поставить пробел, затем вводить команды.

В зависимости от ОС путь до исполняемого файла может отличаться:

- В ОС Windows: `"C:\Program Files\CryptoARM 6\cryptoarm6.exe"`.
- В Unix-подобных ОС семейства Linux: `/opt/cryptoarm6/cryptoarm6`.
- На ОС MacOS: `/Applications/cryptoarm6.app/Contents/MacOS/cryptoarm6`.

Подпись

sign или **sig**

Команда позволяет выполнить операцию подписи файла или нескольких файлов. Если в исходном файле указать уже подписанный документ, то будет добавлена еще одна подпись к файлу.

Пример

```
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

Команда	Описание
`--cert <serial>`	Серийный номер сертификата подписи
`--standard <type>`	Расширение создаваемого файла подписи (choices: "CAdES-T", "CAdES-A", "CAdES-XLT1", "CAdES-BES", default: "CAdES-BES")
`--detached`	Отделённая подпись
`--save-copy`	Сохранение копии результата в Архиве
`--pin <pin-code>`	ПИН код ключа сертификата подписи
`--enc <DER|BASE-64>`	Кодировка в которой будет сохранён подписанный файл, DER или BASE-64 (default: "DER")
`--ext <sig|p7s|sgn|sign|bin>`	Адрес службы TSP. Для Windows нужно указывать URL в одинарных кавычках. Пример: `--tsp 'https://example.com/tsp/tsp.srf'`
`--ocsp <ocsp-addr>`	Адрес службы OCSP. Для Windows нужно указывать URL в одинарных кавычках. Пример: `--ocsp 'https://example.com/ocsp/ocsp.srf'`
`--proxy <proxy-address>`	Служба прокси с указанным адресом
`--proxy-port <port>`	Порт для службы прокси
`--proxy-login <login>`	Пароль для службы прокси
`--proxy-password <password>`	Пароль для службы прокси
`-f, --force`	Автоматическое согласие на использование недействительного сертификата (использование не рекомендуется)
`--logcrypto`	Включает лог trusted-crypto
`--source-file <source-file-name>`	Путь к файлу для подписи
`--source-folder <source-folder>`	Путь к папке в которой нужно подписать все файлы
`--signed-file-path <file-path-name>`	Путь к файлу в который будет сохранена созданная подпись
`--folder-save-signed <folder-to-save-signed>`	Путь к папке в которую будут сохранены подписанные файлы

Команда	Описание
`-h, --help`	Вывод справки команды

Шифрование

encrypt или **enc**

Команда позволяет выполнить шифрование одного или нескольких файлов в адрес одного или нескольких сертификатов.

Пример

```
encrypt --cert &lt;серийный номер сертификата> [--enc DER|BASE64] [--alg &lt;alg-oid>] [--delete-source]  [--save-copy]  [--ext &lt;encrypted file extension>] --source-file &lt;путь к файлу>|--source-folder &lt;путь к папке>  --encrypted-file-path &lt;путь к файлу с новым именем для сохранения результата>|--folder-save-encrypted &lt;путь к папке для сохранения результата>
```

Описание команды

Команда	Описание
`--cert, <serial...>`	Серийный номер сертификата подписи
`--alg <alg-oid>`	OID алгоритма шифрования (default: "1.2.643.2.2.21")
`--delete-source`	Удаление исходного файла после шифрования
`--save-copy`	Сохранение копии результата в Архиве
`--ext <enc|p7m|p7e|pem>`	Расширение создаваемого шифрованного файла (default: "enc")
`--enc <DER|BASE-64>`	Кодировка шифруемого файла, DER или BASE-64 (default: "DER")
`--logcrypto`	Включает лог trusted-crypto
`-f, --force`	Автоматическое согласие на использование недействительных сертификатов (использование не рекомендуется)
`--source-file <path-file>`	Путь к файлу для шифрования
`--encrypted-file-path <path-file>`	Путь к файлу в который будет сохранён результат шифрования
`--folder-save-encrypted <path-folder>`	Путь к папке в которую будут сохранены результаты шифрования

Команда	Описание
`--source-folder <path-folder>`	Путь к папке в которой нужно зашифровать все файлы
`-h, --help`	Вывод справки команды

Расшифрование

decrypt или **dec**

Команда позволяет выполнить расшифрование одного или нескольких зашифрованных файлов.

Пример

```
decrypt [-pin <PIN>] [-save-copy] <source-file-name>|<source-folder> <encrypted-file-path>|
<folder-to-save-decrypted>
```

Описание команды

Команда	Описание
`--save-copy`	Сохранение копии результата в Архиве
`-logcrypto`	Включает лог trusted-crypto
`--pin <pin-code>`	Пин-код ключа расшифрования
`--source-file <path-file>`	Путь к файлу для расшифрования
`--source-folder <path-folder>`	Путь к папке в которой нужно расшифровать все файлы
`--decrypted-file-path <path-file>`	Путь к файлу в который будет сохранён результат расшифрования
`--folder-save-decrypted <path-folder>`	Путь к папке в которую будут сохранены результаты расшифрования
`-h, --help`	Вывод справки команды

Проверка подписи

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.

Примеры

```
verify [-save-report|-r [<report-file>]] <source-file-name>|<source-folder>
```

```
verify_ts [-save-report|-r [<report-file>]] <source-file-name>|<source-folder>
```

Пример. Проверить подпись файлов в папке C:\Foldername с сохранением отчета о проверке в формате pdf в папку с проверяемыми файлами.

```
"C:\Program Files\CryptoARM 6\cryptoarm6.exe" ver --source-folder C:\Foldername -r-pdf
```

Описание команды

Команда	Описание
`-r-pdf`	Сохранение отчета о проверке в формате pdf в папку с проверяемым файлом
`--save-report-pdf [report-folder]`	Сохранение отчета о проверке в формате pdf в указанную папку
`-r-json`	Сохранение отчета о проверке в json формате в папку с проверяемым файлом
`--save-report-json [report-file-path]`	Сохранение отчета о проверке в json формате в указанную папку
`--document <original-file>`	Путь до исходного файла для откреплённой подписи
`--logcrypto`	Включает лог trusted-crypto
`--source-file <source-file-path>`	Путь к файлу подписи для проверки
`-source-folder <source-folder-path>`	Путь к папке в которой нужно проверить все подписи
`-h, --help`	Вывод справки команды

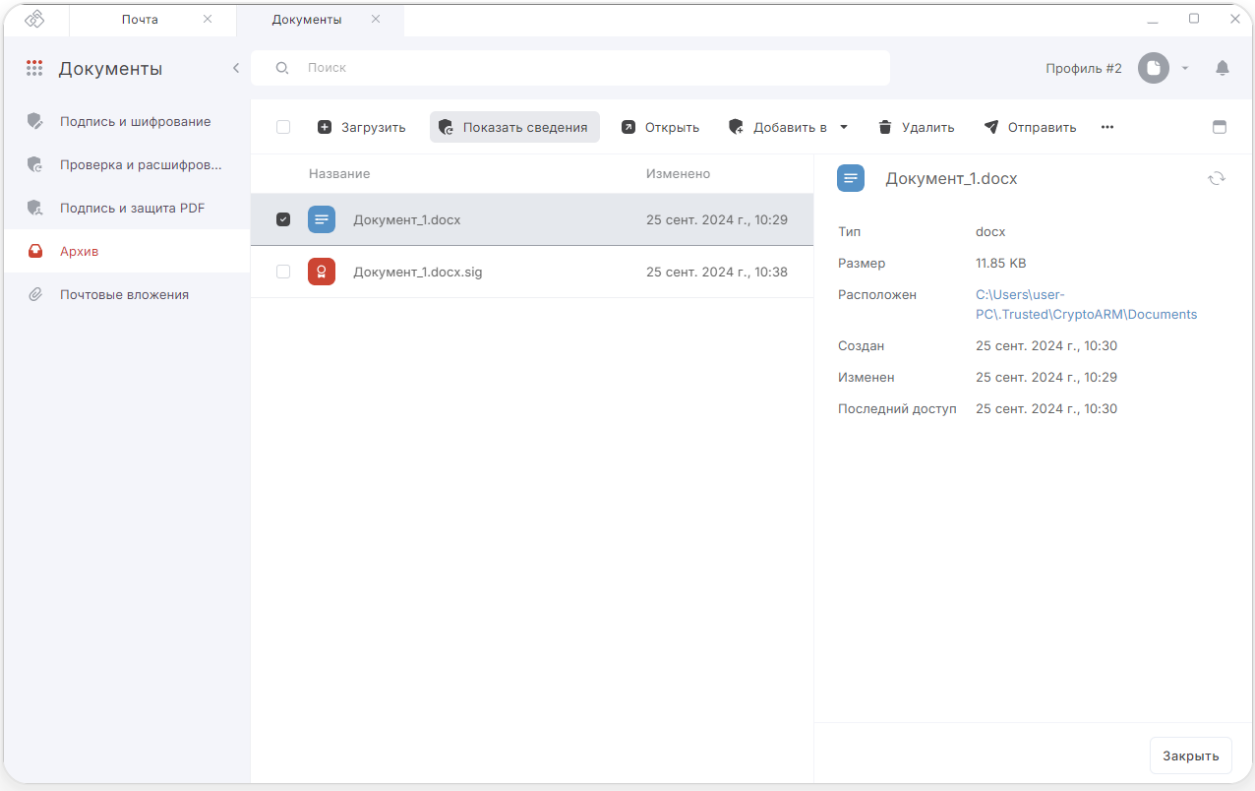
Открыть статью на сайте

Просмотр информации о документе

В приложении КриптоАРМ можно просмотреть информацию о документе и его подписях не только в мастере «Проверка и расшифрование», но и в мастере «Подпись и шифрование», а также в папках «Архив» и «Почтовые вложения».

Как открыть сведения о документе

1. Выделите документ в списке документов:
    - В папке «Архив» или «Почтовые вложения»,
    - В мастере «Подпись и шифрование» или «Проверка и расшифрование».
2. Нажмите на кнопку **Показать сведения** на панели действий или кнопку **Подробно**.
3. Появится область для просмотра.
4. Нажмите на вкладку **О документе**, если документ содержит подпись или является машиночитаемой доверенностью. Для остальных документов сведения отображаются сразу при открытии области.



При нажатии на ссылку пути расположения файла открывается каталог расположения документа в файловом менеджере.

Как открыть сведения о подписи документа

В приложении доступна проверка подписи для файлов расширением .sig, .p7s, .sgn, .sign, .bin.

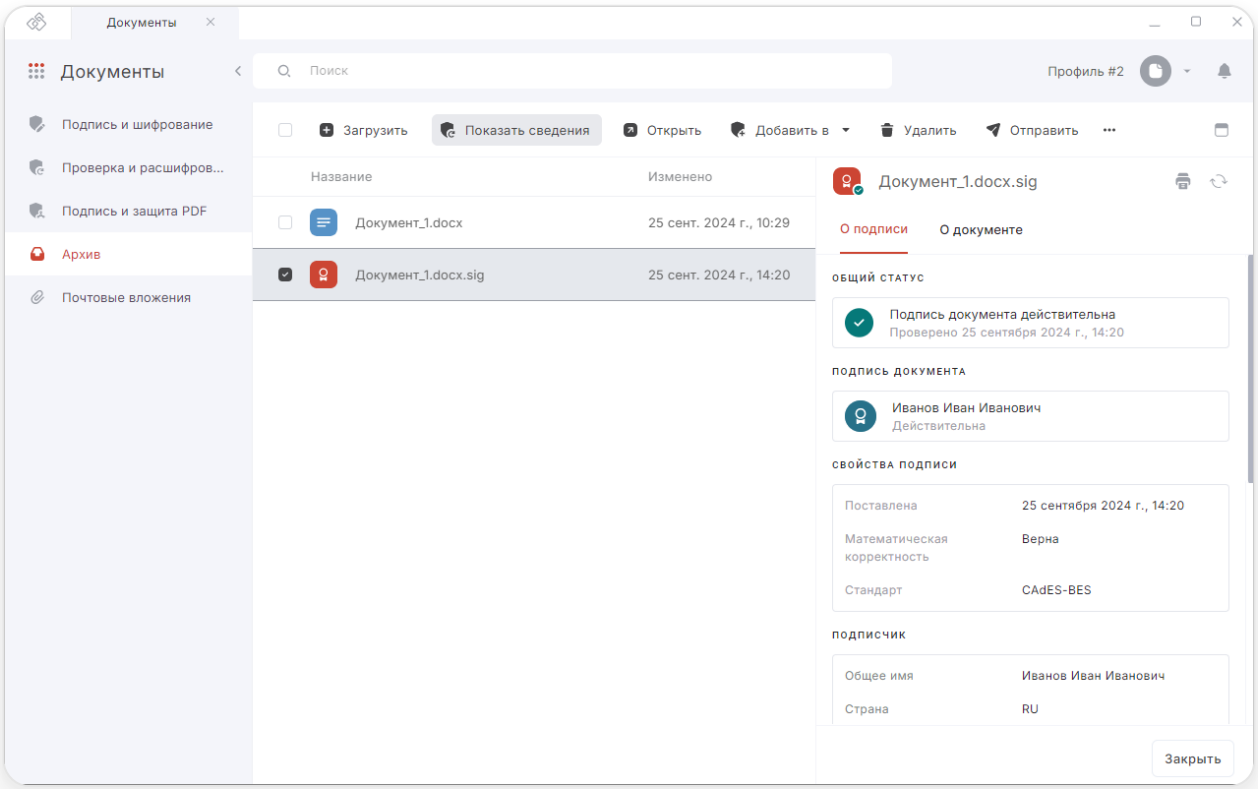
Важно. Перед проверкой убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP.

Примечание. Чтобы проверка подписи прошла успешно, необходимо установить корневой и промежуточные сертификаты для сертификата подписанта.

1. Выделите подписанный документ в списке документов:
    - В папке «Архив» или «Почтовые вложения»,
    - В мастере «Подпись и шифрование» или «Проверка и расшифрование».
2. Нажмите на кнопку **Показать сведения** на панели действий или кнопку **Подробно**.
3. Появится область для просмотра.

В области справа на вкладке **О подписи** будут выведны сведения о подписи документа.

Примечание. Для проверки открепленной подписи необходимо указать путь к подписанному файлу.



Как обновить сведения о подписи документа в «Архиве»

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

1. Выполните шаги из инструкции Как открыть сведения о подписи документа.
2. В области просмотра со сведениями о подписи нажмите на кнопку **Обновить**.

Сведения о подписи будут обновлены.

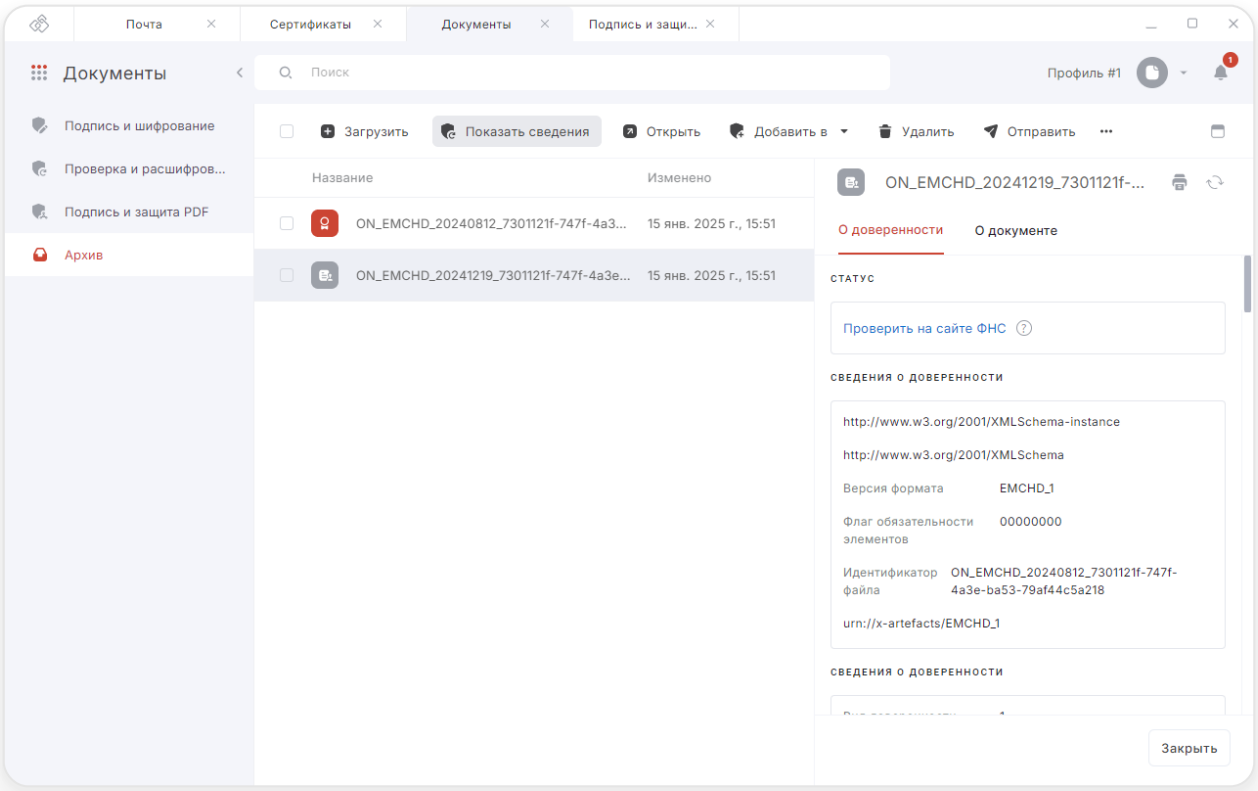
Как распечатать сведения о подписи документа в «Архиве»

1. Выполните шаги из инструкции Как открыть сведения о подписи документа.
2. В области просмотра со сведениями о подписи нажмите на кнопку **Печать**.
3. Откроется окно с отчетом о проверке электронной подписи.

Отчет можно распечатать или скачать на устройство.

Как посмотреть печатную форму МЧД

1. Выделите файл МЧД с расширением .xml в списке документов:
    - В папке «Архив» или «Почтовые вложения»,
    - В мастере «Подпись и шифрование» или «Проверка и расшифрование».
2. Нажмите на кнопку **Показать сведения** на панели действий или кнопку **Подробно**.
3. Появится область для просмотра.
4. В области просмотра будет выведена визуализация МЧД.



Как распечатать МЧД

1. Выполните шаги из инструкции Как посмотреть печатную форму МЧД.
2. В области просмотра со сведениями о МЧД нажмите на кнопку **Печать** .
3. Откроется окно с печатной формой МЧД.

МЧД можно распечатать или скачать на устройство.

Как проверить статус МЧД

1. Выполните шаги из инструкции Как посмотреть печатную форму МЧД.
2. В блоке **Статус** нажмите на кнопку **Проверить на сайте ФНС**.

В браузере по умолчанию откроется сайт ФНС со статусом доверенности.

Возможные уведомления

Ошибки, которые могут возникнуть при просмотре сведений, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Не удалось найти исходный файл для подписи — данное сообщение возникает, если при отсоединённой подписи не найден исходный документ. На правой боковой панели нажмите **Указать путь к файлу** для выбора исходного документа или скопируйте исходный документ в папку с файлом подписи. В таком случае необходимо, чтобы названия исходного файла и файла подписи совпадали.

Инструкции по теме

1. Как проверить подпись документа.
2. Как посмотреть уведомления.

Открыть статью на сайте

Просмотр документа

Документ открывается в программе, которая ассоциирована с его расширением.

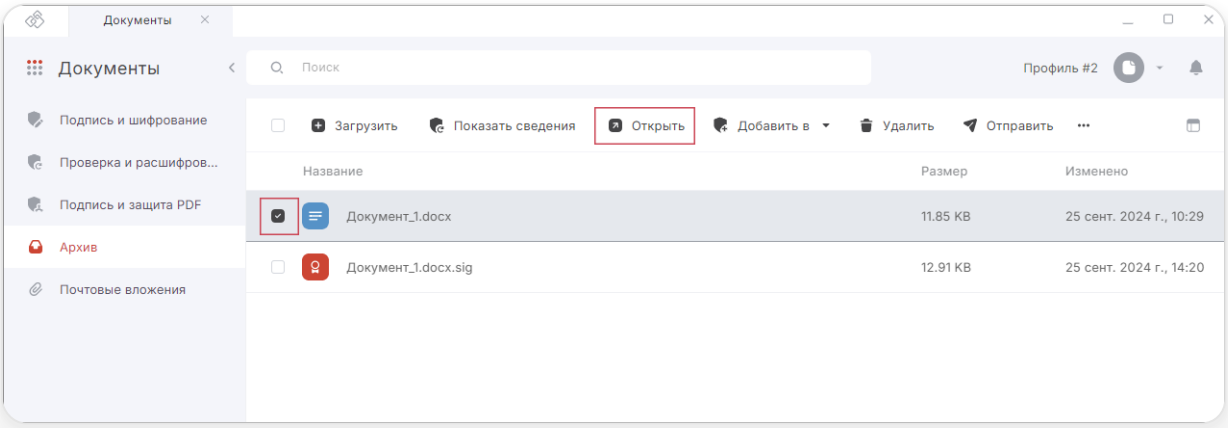
Для подписанных или зашифрованных документов открывается оригинал.

Важно. Перед тем как просматривать подписанные и зашифрованные документы, убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP.

При открытии зашифрованного документа происходит расшифрование, поэтому в хранилище «Личные сертификаты» должен быть установлен сертификат с закрытым ключом, в адрес которого производилось шифрование.

Как открыть документ

1. Выделите документ в списке и нажмите **Открыть**:
    - В папке **Архив** или **Почтовые вложения** раздела **Документы**,
    - В мастере **Подпись и шифрование**,
    - В мастере **Проверка и расшифрование**.
2. Документ будет открыт в программе, которая ассоциирована с его расширением



Возможные уведомления

Ошибки, которые могут возникнуть при просмотре документа, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

- **Не удалось найти исходный файл для подписи** — данное сообщение возникает, если при отделенной подписи не найден исходный документ. На правой боковой панели нажмите **Указать путь к файлу** для выбора исходного документа или скопируйте исходный документ в папку с файлом подписи. В таком случае необходимо, чтобы названия исходного файла и файла подписи совпадали.
- **Не удалось расшифровать файл** — данное сообщение возникает, если при просмотре документа не найден сертификат расшифрования.

Инструкции по теме

1. Как посмотреть информацию о документе.
2. Как посмотреть уведомления.

Открыть статью на сайте

Удаление документа

Документы, хранящиеся в папке «Архив», можно удалить. При этом они будут удалены из файловой системы.

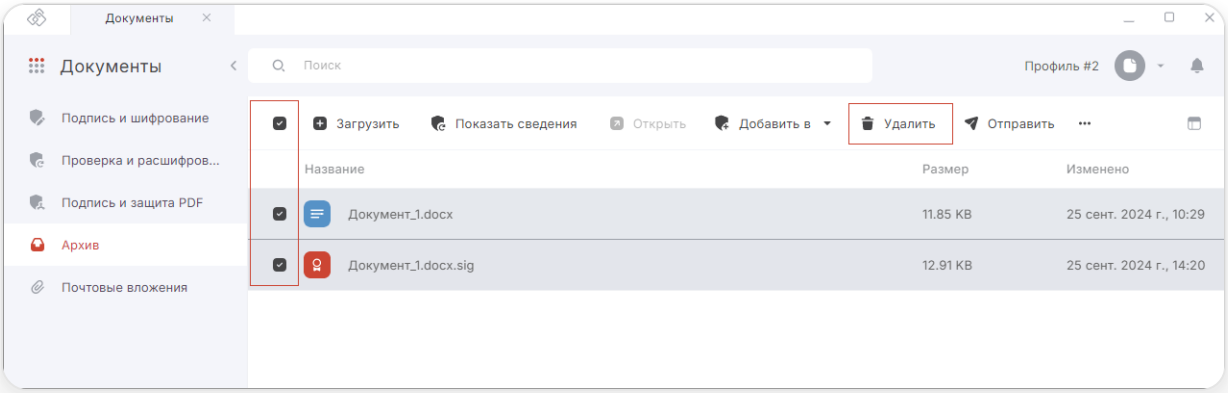
Примечание. Если вы удаляете документы в мастере «Подпись и шифрование» или «Проверка и расшифрование», список будет очищен, но документы останутся в системе.

Как удалить документ из «Архива»

1. Перейдите в раздел **Документы** → папка **Архив**.
2. Нажмите на панель с документом в списке.
3. Нажмите на кнопку **Удалить**, размещенную на панели действий.
4. Подтвердите действие в модальном окне.

Как удалить несколько документов из «Архива»

1. Перейдите в раздел **Документы** → папка **Архив**.
2. Отметьте флажками документы, которые нужно удалить.
3. Нажмите на кнопку **Удалить**, размещенную на панели действий.
4. Подтвердите действие в модальном окне.



Открыть статью на сайте

Добавление в мастер

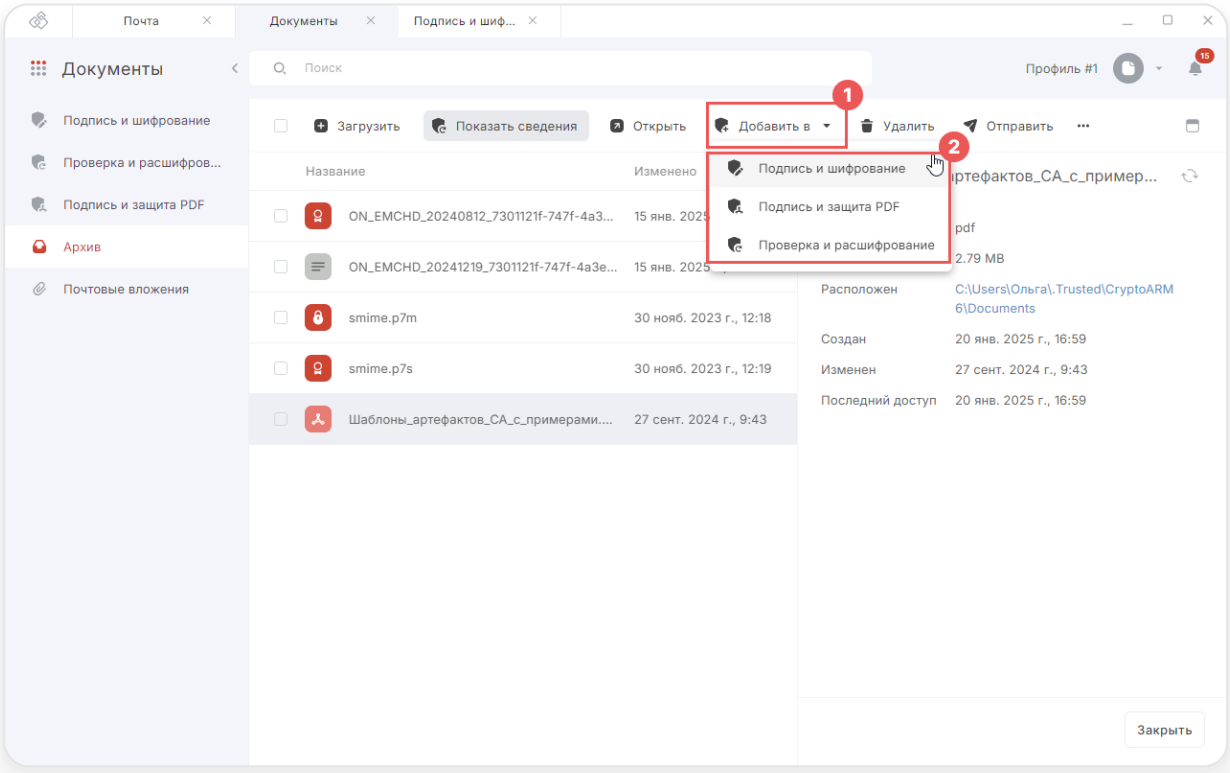
Документы, хранящиеся в папке «Архив», можно открыть в одном из мастеров:

- Подпись и шифрование,
- Проверка и расшифрование,
- Подпись и защита PDF (доступно для документов с расширением PDF).

Как добавить в мастер документ из «Архива»

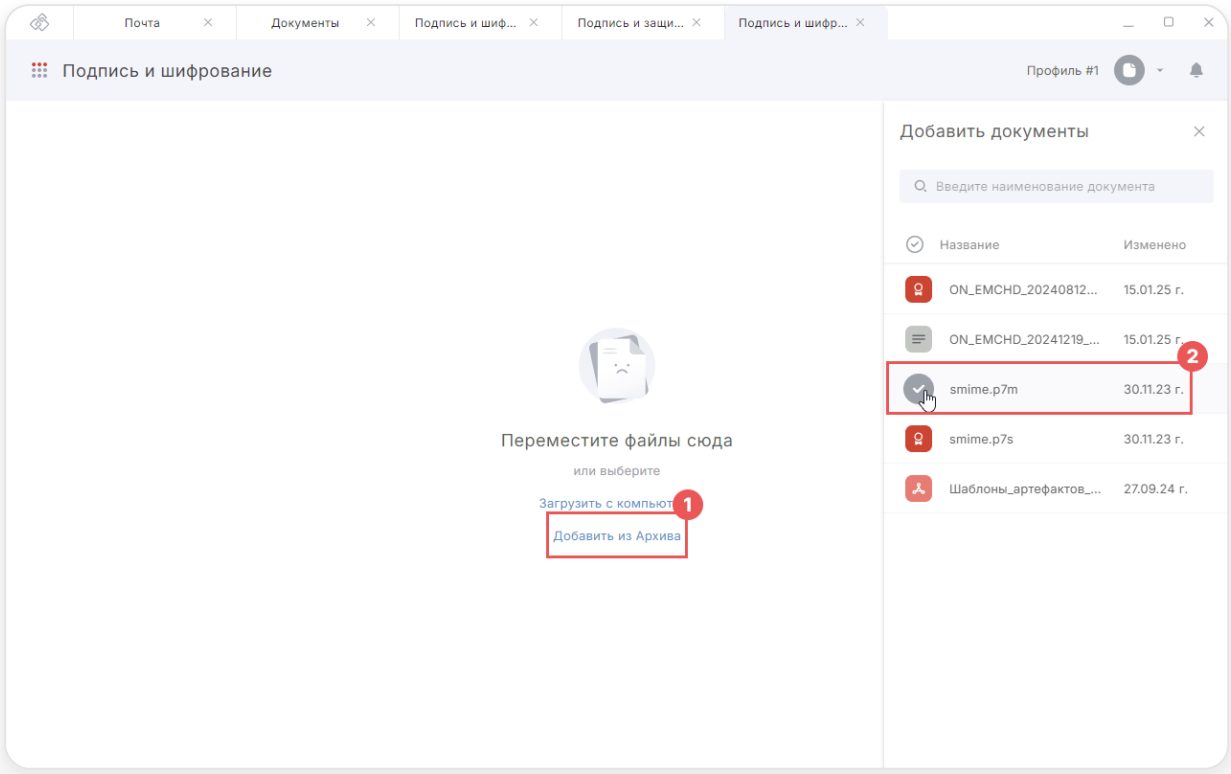
Первый способ

1. Перейдите в раздел **Документы** → папка **Архив**.
2. Нажмите на панель с документом в списке.
3. Нажмите на кнопку **Добавить в**, размещенную на панели действий.
4. Откроется меню со списком матсеров, доступных для выбранного документа:
    - Подпись и шифрование,
    - Проверка и расшифрование,
    - Подпись и защита PDF (доступно для документов с расширением PDF)
5. Выберите мастер, в котором необходимо открыть документ.



Второй способ

1. Перейдите в раздел **Документы**.
2. В левом боковом меню нажмите на **Подпись и шифрование** или **Проверка и расшифрование**.
3. Откроется окно мастера.
4. Нажмите на кнопку **Добавить из Архива**, размещенную в центре окна.
5. Откроется окно со списком документов, сохраненных в папке «Архив».
6. Установите флаги напротив документов, которые необходимо добавить в мастер.



Документы будут добавлены в мастер.

Инструкции по теме

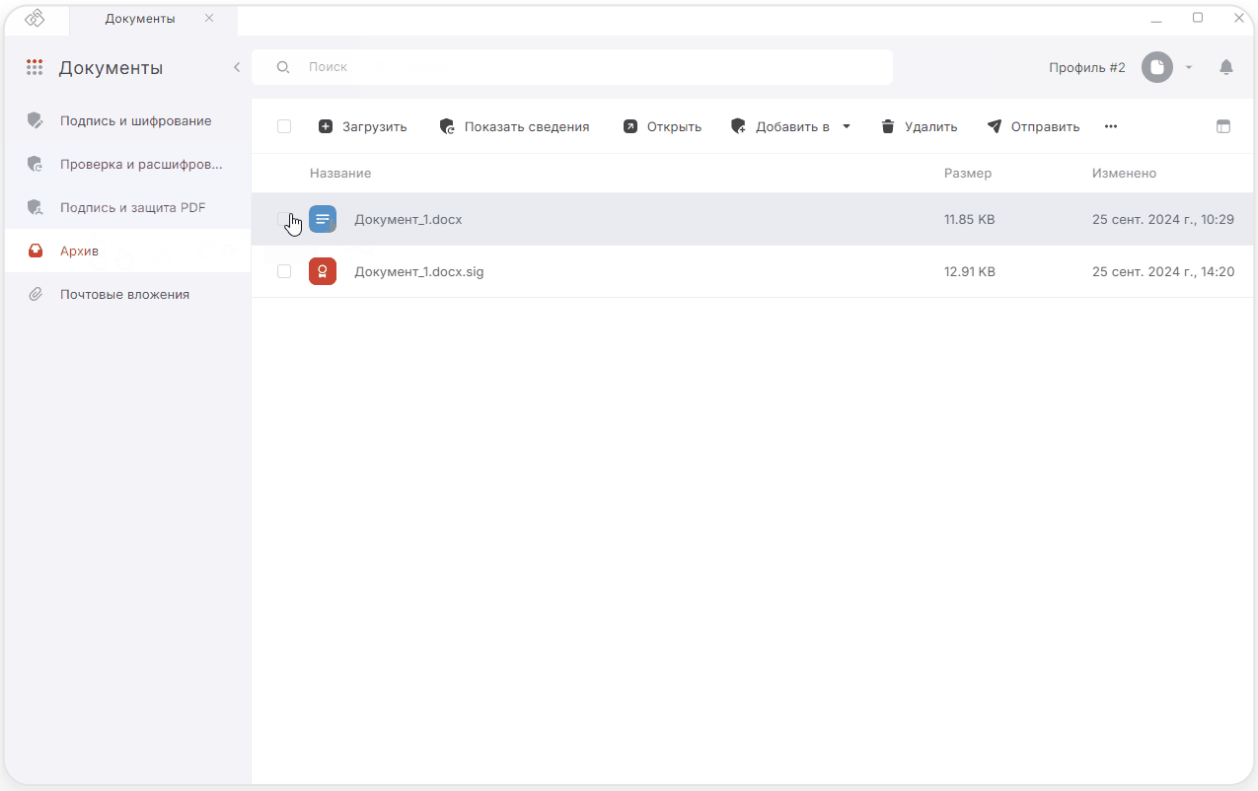
1. Как подписать документ.
2. Как зашифровать документ.
3. Как расшифровать документ.
4. Как снять подпись с документа.

Открыть статью на сайте

Как открыть папку с файлом на компьютере

Как открыть папку с файлом, который сохранен в «Архиве»

1. Перейдите в раздел **Документы** → папка **Архив**.
2. Нажмите на панель с документом в списке.
3. Нажмите на кнопку **Показать в папке**, размещенную на панели действий.
4. Откроется системная папка с файлом.

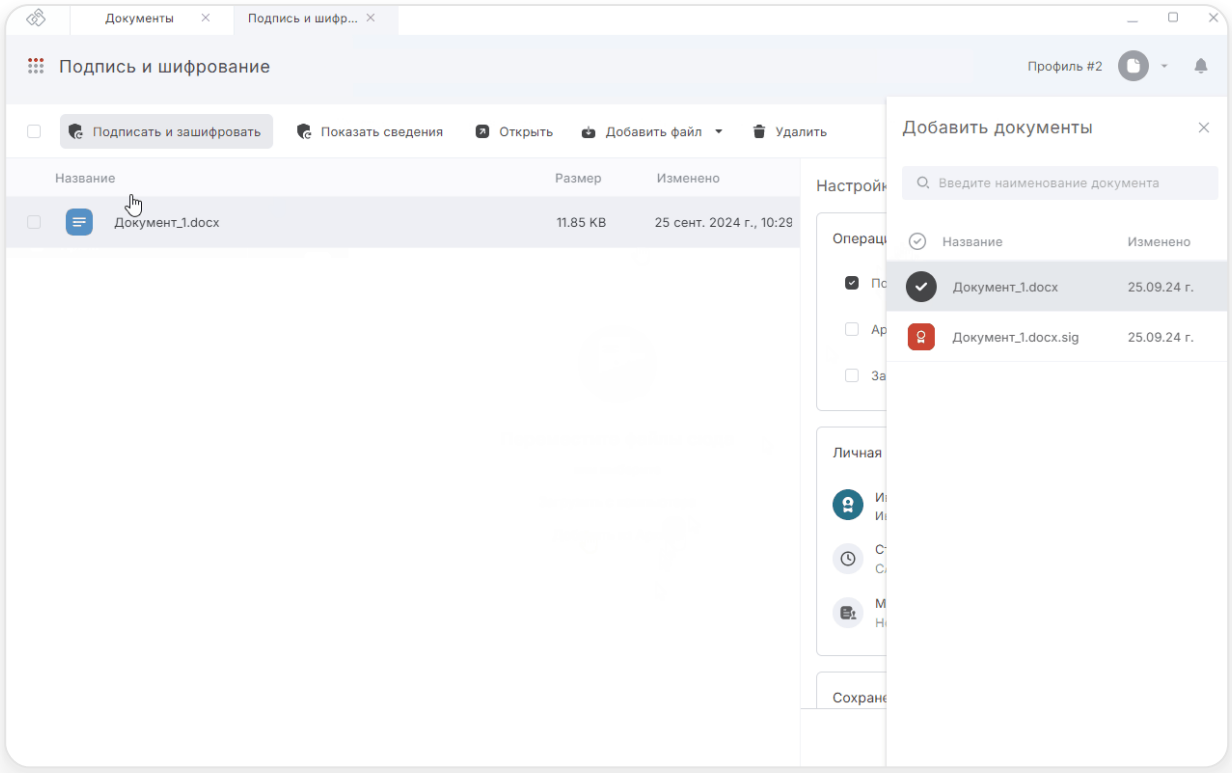


Статичный кадр демонстрации. Открыть анимацию

Как открыть папку с файлом, который добавлен в мастер

1. Откройте мастер **Подпись и шифрование** или **Проверка и расшифрование**.
2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Нажмите на кнопку **Показать в папке**, размещенную на панели действий.
4. Появится область просмотра справа от списка документов.

5. В открывшемся боковом окне, нажмите на кнопку расположения файла.



Статичный кадр демонстрации. Открыть анимацию

При множественном выборе документов данная опция недоступна.

Инструкции по теме

1. Как добавить документы в мастер.
2. Как посмотреть информацию о документе.

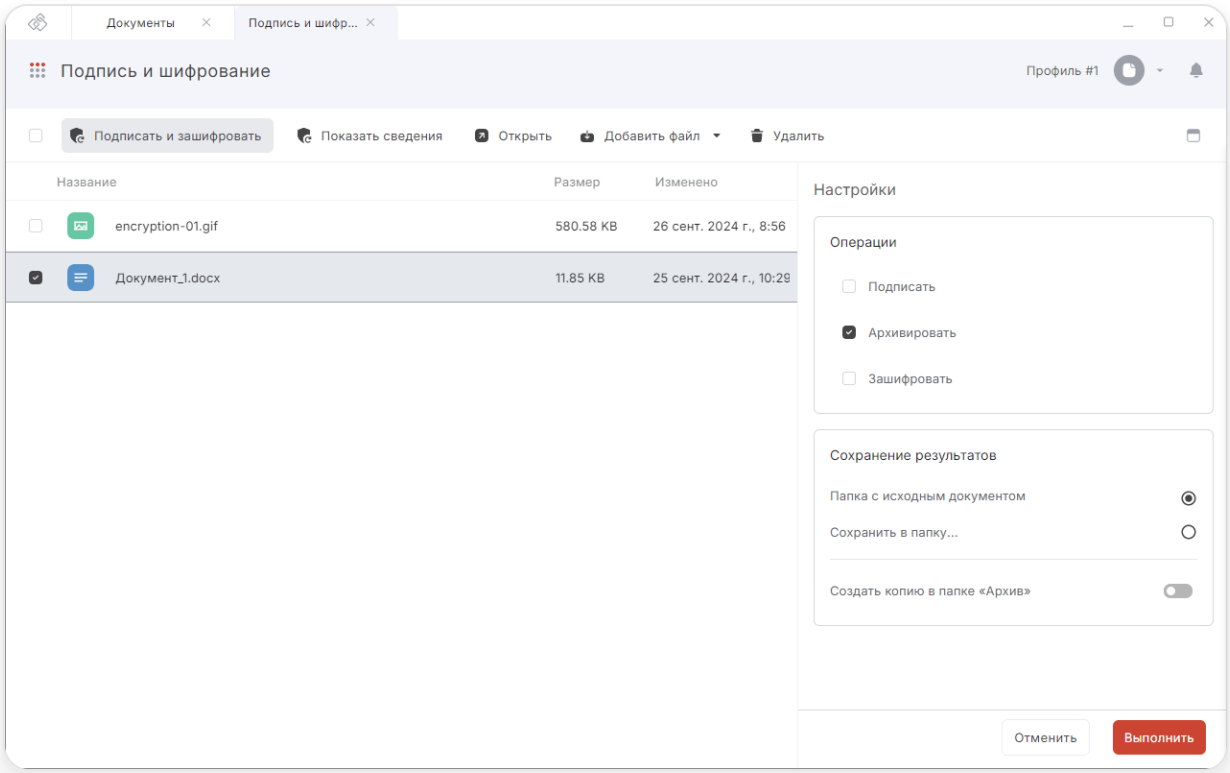
Открыть статью на сайте

Архивирование документов

Для архивирования документов не требуется дополнительных настроек. Вы можете выбрать каталог для сохранения архива и настроить сохранение копии в папке «Архив».

Как создать архив с документами

1. Откройте мастер **Подписи и шифрования** одним из способов:
    - Нажмите **Подпись и шифрование** в левом боковом меню раздела **Документы**,
    - Вызовите действие **Добавить в** → **Подпись и шифрование** для файла в папке «Архив», результатах операции или в разделе «Почта».
2. Добавьте документы в список с помощью drag-and-drop или кнопок **Загрузить с компьютера**, **Добавить из Архива**.
3. Укажите настройки, либо выберите профиль подписи с сохраненными настройками. Настройки мастера автоматически перезаполняются при выборе профиля.
    - В блоке **Операции** выберите **Архивировать**,
    - В блоке **Сохранение результатов** укажите настройки сохранения результатов операции. Если вы хотите архивировать документы из разных каталогов, то вам необходимо выбрать каталог для сохранения результатов.
4. Нажмите кнопку **Выполнить**.
5. Подтвердите действие в модальном окне.



Результат выполнения операции

Во время выполнения операции в нижней части окна появляется панель с индикатором выполнения и кнопкой «Отмена». Операции происходят с документами последовательно. Если вы нажмёте на кнопку «Отмена», операция будет приостановлена на том документе, с которым производилась операция на момент отмены.

Если операция прошла успешно, подписанные файлы будут сохранены в каталоге, который был указан в настройках мастера. Если каталог не указывался, то результаты будут размещены рядом с исходным файлом.

Если установлен флаг **Создать копию в Архиве**, то копия подписанных документов сохраняется в специальную папку, документы которой доступны в разделе **Документы → вкладка Архив**.

Инструкции по теме

1. Как добавить документы в мастер.
2. Как создать профиль подписи.
3. Как переключаться между профилями подписи.
4. Как посмотреть уведомления.
5. Действия с результатами операций.

Открыть статью на сайте

Описание раздела

Раздел **Сертификаты** предназначен для управления сертификатами.

Категории сертификатов

Для сертификатов доступны следующие категории:

- **Личные** — содержит ваши личные сертификаты с привязкой к закрытому ключу.
- **Других пользователей** — содержит все сертификаты других пользователей и контактов, предназначены для шифрования в адрес этих сертификатов.
- **Удостоверяющие центры** — содержит доверенные корневые и промежуточные сертификаты.
- **Списки отзыва**.
- **Запросы** — содержит созданные пользователем запросы на сертификат.
- **Ключи** — содержит список доступных ключевых контейнеров, расположенных в системе и на отчуждаемых носителях.

На верхней панели вы можете выбрать действия с сертификатом, которые зависят от выбранной категории.

Действия с личными сертификатами

Для личных сертификатов вы можете выполнить следующие действия:

- **Открыть** — для получения сведений о сертификате, его составе и пути сертификации;
- **Экспортировать** — для экспорта сертификата в файл;
- **Создать профиль подписи** — для создания профиля подписи, в котором в настройках будет выбрана операция подписи и сертификат подписи;
- **Удалить** — для удаления сертификата;
- Просмотреть сведения о сертификате в правой боковой панели.

Действия с сертификатами других пользователей

Для сертификатов других пользователей вы можете выполнить следующие действия:

- **Открыть** — для получения сведений о сертификате, его составе и пути сертификации;
- **Экспортировать** — для экспорта сертификата в файл;
- **Привязать к контакту** — позволяет добавлять сертификат к контакту для шифрования почтовых сообщений, отправляемых в адрес контакта;
- **Создать контакт** — для создания контакта, у которого будет привязан выбранный сертификат;
- **Удалить** — для удаления сертификата;

- просмотреть сведения о сертификате в правой боковой панели.

Действия с сертификатами удостоверяющих центров

Для сертификатов удостоверяющих центров вы можете выполнить следующие действия:

- **Открыть** — для получения сведений о сертификате, его составе и пути сертификации;
- **Экспортировать** — для экспорта сертификата в файл;
- **Удалить** — для удаления сертификата;
- просмотреть сведения о сертификате в правой боковой панели.

Действия со списками отзыва сертификатов (COC)

Для списков отзыва сертификатов вы можете выполнить следующие действия:

- **Импорт из файла** — для установки COC из файла;
- **Экспортировать** — для экспорта COC в файл;
- **Удалить** — для удаления COC;
- просмотреть сведения о списке отзыва в правой боковой панели.

Действия с запросами на сертификат

Для запросов на сертификат вы можете выполнить следующие действия:

- **Создать запрос** — для генерации запроса на сертификат или самоподписанного сертификата;
- **Показать в папке** — открывается файловый менеджер с расположением файла запроса;
- **Отправить** — для отправки файла запроса в новом почтовом сообщении;
- **Экспортировать** — для экспорта запроса в файл. Запрос экспортируется как сертификат;
- **Удалить** — для удаления запроса;
- просмотреть сведения о запросе в правой боковой панели.

Действия с ключами

Для ключевых контейнеров вы можете выполнить следующие действия:

- **Установить** — для установки сертификата из контейнера в категорию «Личных»;
- **Удалить** — для удаления контейнера;
- просмотреть сведения о сертификате в контейнере в правой боковой панели.

Действия при просмотре информации о сертификате

При просмотре сведений о сертификате или запросе в правой боковой панели доступны действия:

- **Печать** — для печати информации о сертификате.
- **Протестировать** — для тестирования контейнера закрытого ключа. Данная функция доступна только для сертификатов или запросов, у которых есть привязка к закрытому ключу.
- **Обновить** — для обновления информации о сертификате. 

Обновление списка сертификатов

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Обновить**, размещенную рядом с заголовокм раздела.

Поиск по сертификатами

Чтобы найти определенный сертификат:

1. Перейдите в раздел **Сертификаты**.
2. В поисковой строке введите параметры поиска.
3. Нажмите Enter.

Поиск возможен по следующим значениям: по общему имени, по серийному номеру и отпечатку.

Инструкции по теме

1. Как установить личный сертификат.
2. Как установить сертификат из DSS.
3. Как создать запрос на сертификат.
4. Как установить корневой и промежуточный сертификаты.
5. Как работать с ключевыми контейнерами.

Открыть статью на сайте

Установка личного сертификата

Важно. Прежде чем импортировать личный сертификат, убедитесь, что на вашем компьютере установлен криптопровайдер КриптоПро CSP.

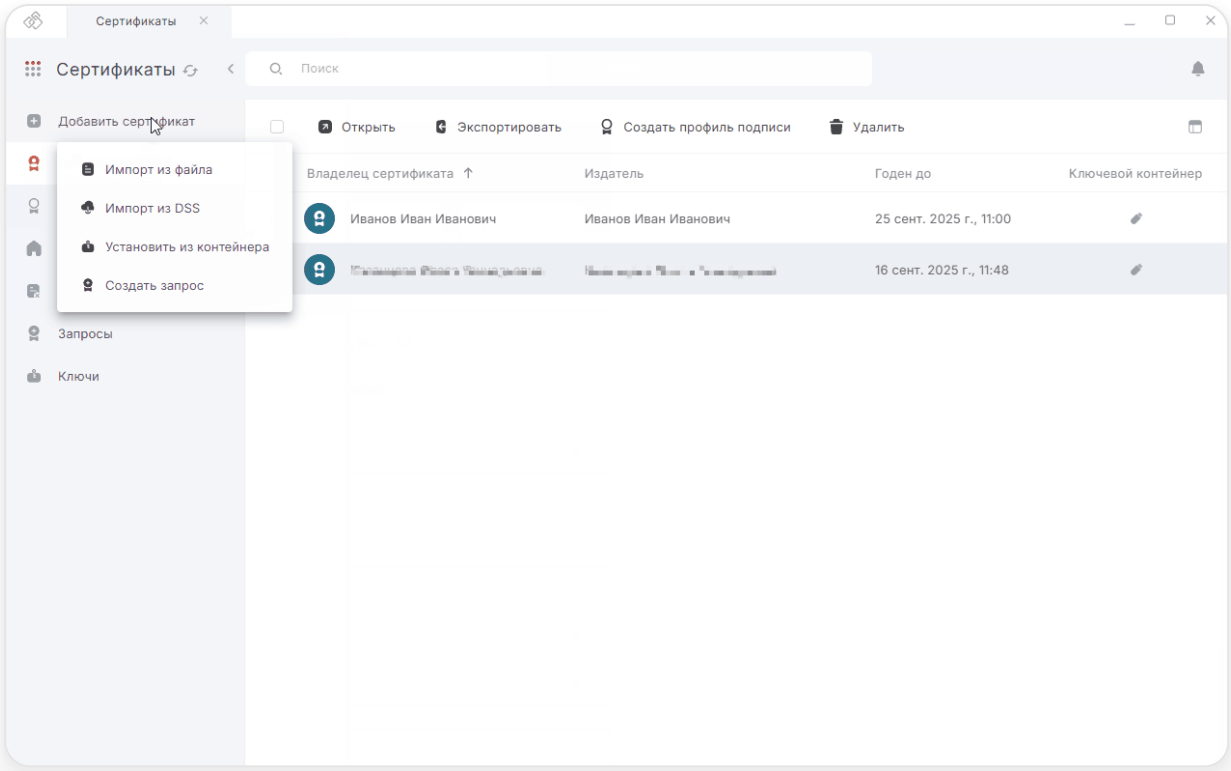
Примечание. Чтобы статус сертификата был действительный, в приложении должны быть установлены корневые сертификаты удостоверяющего центра и актуальный список отзыва сертификатов.

Установка сертификата из ключевого контейнера

В некоторых случаях требуется установка драйверов для токена.

Этот способ установки доступен, если в контейнере имеется сертификат. В противном случае функция будет недоступна.

1. При необходимости подключите токен к устройству.
2. Выберите раздел **Сертификаты**.
3. Выберите раздел **Ключи**. Или нажмите кнопку **Добавить сертификат** в правой части окна и в открывшемся списке действий выберите **Установить из контейнера**.
4. Откроется список контейнеров.
5. Выделите контейнер в списке.
6. Нажмите кнопку **Установить**.
7. При необходимости введите пароль к ключевому контейнеру.

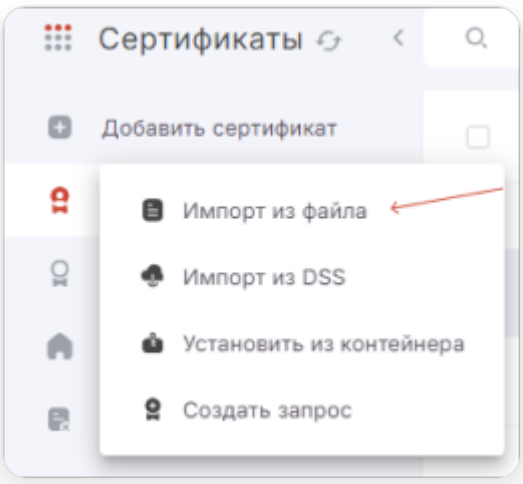


Статичный кадр демонстрации. Открыть анимацию

Сертификат установлен в хранилище «Личные сертификаты».

Установка сертификата с закрытым ключом из файла .pfx

1. Выберите раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в левом боковом меню.
3. В открывшемся списке действий выберите **Импорт из файла**.



4. В файловом менеджере выберите файл сертификата .pfx.

5. Введите пароль к контейнеру pfx.
6. Задайте новый пароль к ключевому контейнеру.

Сертификат установлен в хранилище «Личные сертификаты».

Установка сертификата с привязкой к ключевому контейнеру

1. Выберите раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в левом боковом меню.
3. В открывшемся списке действий выберите **Импорт из файла**.
4. В файловом менеджере выберите файл сертификата .cer или .crt.
5. Введите пароль к ключевому контейнеру, если требуется.

Сертификат установлен в хранилище «Личные сертификаты».

Возможные ошибки

Ошибки, которые возникают при установке сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как установить корневой и промежуточный сертификаты.
2. Как импортировать список отзыва сертификатов (COC).
3. Как посмотреть уведомления.

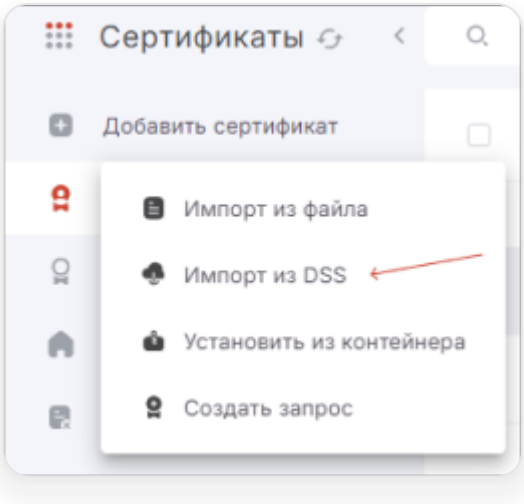
Открыть статью на сайте

Установка сертификата из DSS

Для установки сертификата из DSS необходимо создать подключение к сервису DSS.

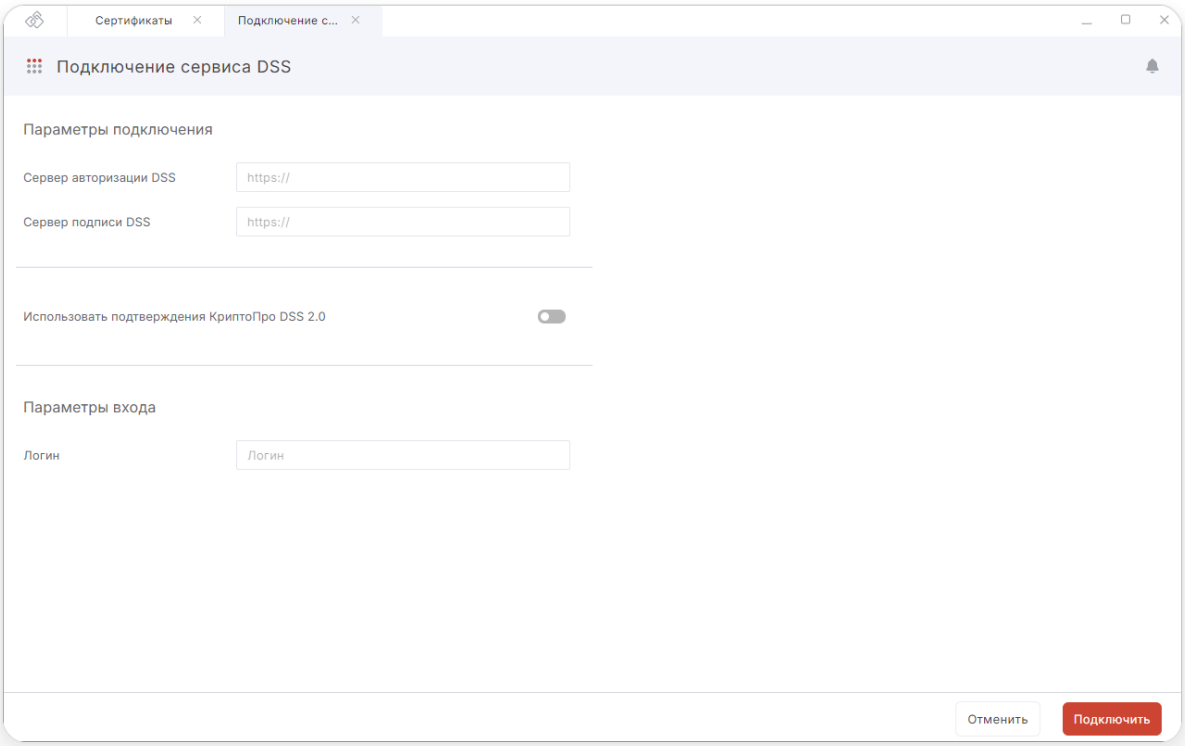
Как создать подключение к сервису DSS

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в левом боковом меню.
3. В открывшемся списке действий выберите **Импорт из DSS**.



4. Заполните поля:
   - **Название подключения** — любое название (может состоять из латинских букв, цифр и знака подчеркивания);
   - **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 КриптоПро DSS 2.0;

- **Логин** — ваш логин для доступа к сертификату.



5. Нажамите **Подключить**.

6. 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.

7. 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 отличаются иконкой облачного контейнера .

Важно. Чтобы статус сертификата был действительный, должны быть установлены корневые сертификаты УЦ и актуальный список отзыва сертификатов (COC).

Возможные уведомления

Ошибки, которые возникают при установке сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

1. **Не удалось подключиться к серверу DSS: неверный логин или пароль** — проверить правильность заполнения данных.
2. **Не удалось подключиться к серверу DSS** — проверить правильность ввода адресов серверов, доступ к сети Интернет.

Инструкции по теме

1. Как установить корневой и промежуточный сертификаты.
2. Как импортировать список отзыва сертификатов (COC).

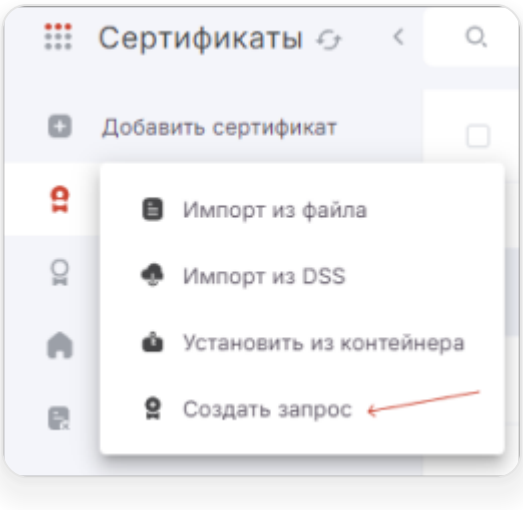
Открыть статью на сайте

Создание запроса

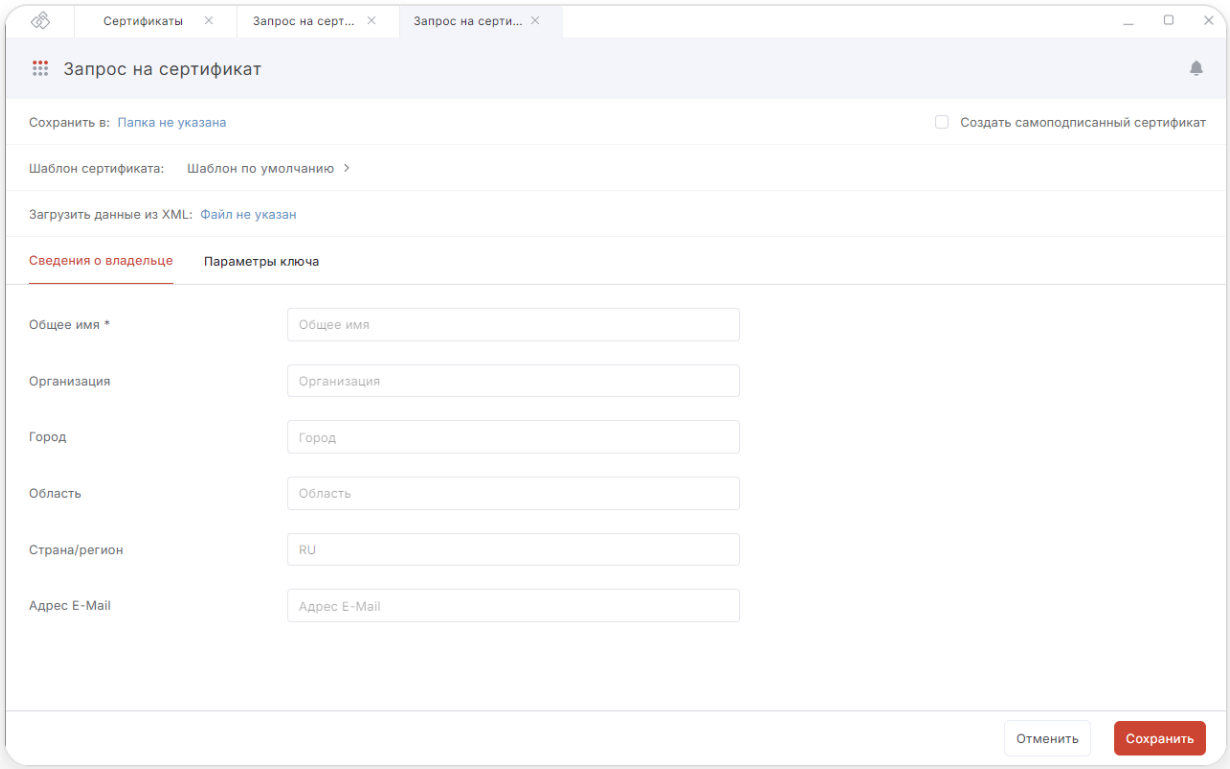
Запрос на сертификат — это электронный документ, который содержит информацию для получения сертификата электронной подписи в Удостоверяющем центре.

Как создать запрос на сертификат

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в правой части окна и в открывшемся списке действий выберите **Создать запрос**.



3. Откроется форма создания запроса.



4. Выберите папку для сохранения файла запроса. Если папка не выбрана, файл запроса сохранится в папку: C:\Users\Username\.Trusted\CryptoARM 6\Requests.

5. Выберите шаблон сертификата. Можно выбрать шаблон из списка или загрузить собственный в формате .json.

6. Заполните данные в запросе одним из способов:

    - Загрузите данные из XML — позволяет автоматически заполнить поля в запросе с помощью загрузки файлов XML.
    - Укажите вручную.

7. Заполните поля вкладки **Сведения о владельце**. Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.

8. Выставите настройки вкладки **Параметры ключа**.

    - идентификация заявителя;
    - алгоритм ключа;
    - назначение ключа;
    - название ключевого контейнера — создан на основе нового ключевого набора, но вы можете задать свое имя или оставить созданное автоматически;
    - флаг **Пометить ключи как экспортируемые** — данная опция позволит экспортировать сертификат вместе с закрытым ключом для переноса на другое устройство;
    - использование ключа;
    - назначение сертификата (EKU).

9. Нажмите **Сохранить**.

10. Выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
11. При необходимости установите пароль на контейнер.

На основе указанных данных формируется запрос на сертификат.

При успешной генерации запрос сохраняется в файл <CN сертификата><алгоритм ><дата генерации>.req в заданной папке и отображается в папке **Запросы** раздела **Сертификаты**.

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

Ошибки, которые возникают при создании запроса, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как установить корневой и промежуточный сертификаты.
2. Как импортировать список отзыва сертификатов (COC).
3. Как установить личный сертификат.
4. Как создать самоподписанный сертификат.
5. Как посмотреть уведомления.

Открыть статью на сайте

Создание самоподписанного сертификата

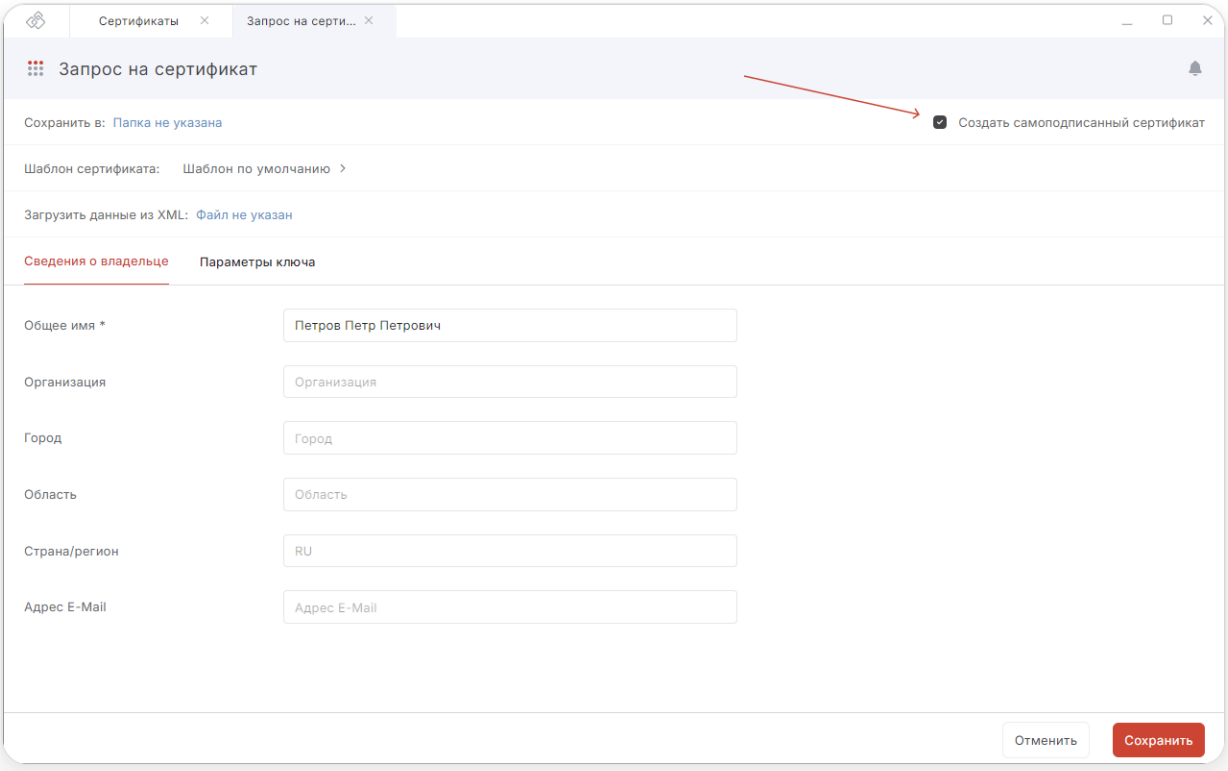
Самоподписанный сертификат – сертификат, изданный самим пользователем, без обращения к Удостоверяющему центру.

Самоподписанный сертификат является одновременно личным и корневым (устанавливается в хранилище «Личный сертификаты» и «Доверенные корневые центры сертификации»).

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

Как создать самоподписанный сертификат

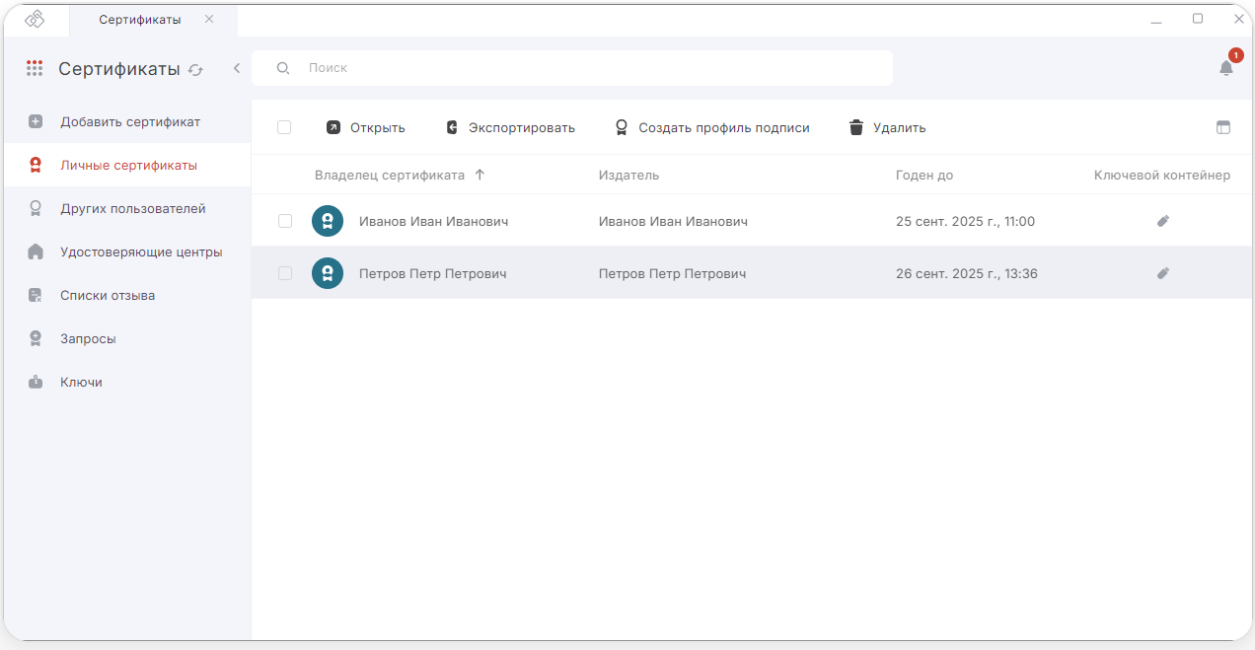
1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в левом боковом меню.
3. В открывшемся списке действий выберите **Создать запрос**.
4. Откроется форма создания запроса на сертификат.
5. Выберите шаблон сертификата.
6. В правом верхнем углу установите флаг **Создать самоподписанный сертификат**.



7. Заполните поля раздела **Сведения о владельце**. Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.
8. Выставите настройки вкладки **Параметры ключа**.
    - идентификация заявителя;
    - алгоритм ключа;
    - назначение ключа;
    - название ключевого контейнера — создан на основе нового ключевого набора, но вы можете задать свое имя или оставить созданное автоматически;
    - установить флаг **Пометить ключи как экспортируемые** — данная опция позволит экспортировать сертификат вместе с закрытым ключом для переноса на другое устройство;
    - использование ключа;
    - назначение сертификата (EKU).
9. Нажмите **Сохранить**.
10. Выберите ключевой носитель для хранения контейнера (реестр, диск, токен).
11. При необходимости установите пароль на контейнер.

На основе указанных данных формируется самоподписанный сертификат.

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



При генерации самоподписанного сертификата запрос на сертификат не создается.

Чтобы самоподписанный сертификат был действительным, нужно импортировать его в раздел **Удостоверяющие центры**. Для этого сначала необходимо сертификат экспортировать в файл без закрытого ключа, а потом импортировать в раздел УЦ. Подробнее в инструкции Установка корневого и промежуточного сертификатов.

Ошибки, которые возникают при создании сертификата, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как экспортировать сертификат.
2. Как установить корневой и промежуточный сертификаты.
3. Как импортировать список отзыва сертификатов (COC).
4. Как создать запрос на сертификат.
5. Как посмотреть уведомления.

Открыть статью на сайте

Установка корневого и промежуточного сертификатов

Корневой сертификат — это 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.

Сертификаты, выданные удостоверяющим центром, называются промежуточными.

Чтобы проверить статус сертификатов, необходимо установить в приложении все сертификаты, участвующие в цепочке сертификации.

Примечание. При импорте корневых и промежуточных сертификатов могут быть запрошены права администратора.

Как установить корневой или промежуточный сертификат

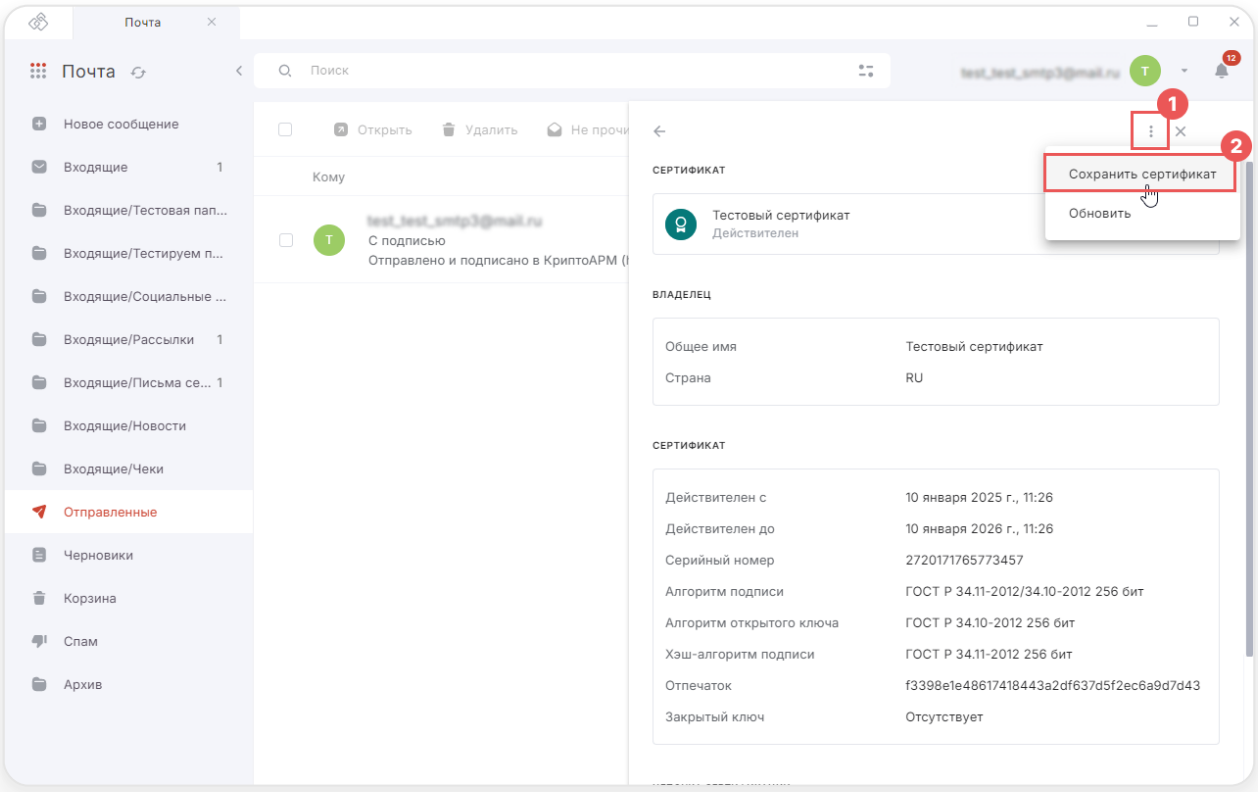
1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в левом боковом меню.
3. В открывшемся меню действий выберите **Импорт из файла**.
4. Откроется окно файлового менеджера.
5. Выберите файл сертификата.
6. Подтвердите запрос на установку сертификата.

При успешном импорте сертификат появится в хранилище сертификатов **Удостоверяющие центры**.

Как установить корневой или промежуточный при проверке подписи документа

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование**. Подробнее в инструкции Проверка подписи документа.
2. Откройте область просмотра со сведениями о подписи.
3. В блоке **Цепочка сертификации** нажмите на сертификат.
4. Откроются сведения о сертификате.
5. Вызовите меню действий по кнопке **Еще**.
6. Нажмите на **Сохранить сертификат**.

При успешном импорте сертификат появится в хранилище сертификатов **Удостоверяющие центры**.



Возможные ошибки

Ошибки, которые возникают при установке сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как импортировать список отзыва сертификатов (CRL).
2. Как посмотреть уведомления.

Открыть статью на сайте

Установка сертификатов других пользователей

Для шифрования документов, адресованных другому пользователю, вам потребуется его сертификат.

Импорт сертификата, который был отправлен вам другим пользователем, происходит в хранилище сертификатов **Других пользователей**. Он нужен для шифрования документов в адрес этого сертификата. Такой сертификат импортируется без закрытого ключа.

Примечание. Чтобы статус сертификата был действительный, у вас должны быть установлены корневые сертификаты удостоверяющих центров и актуальный список отзыва сертификатов.

Как установить сертификат другого пользователя из файла

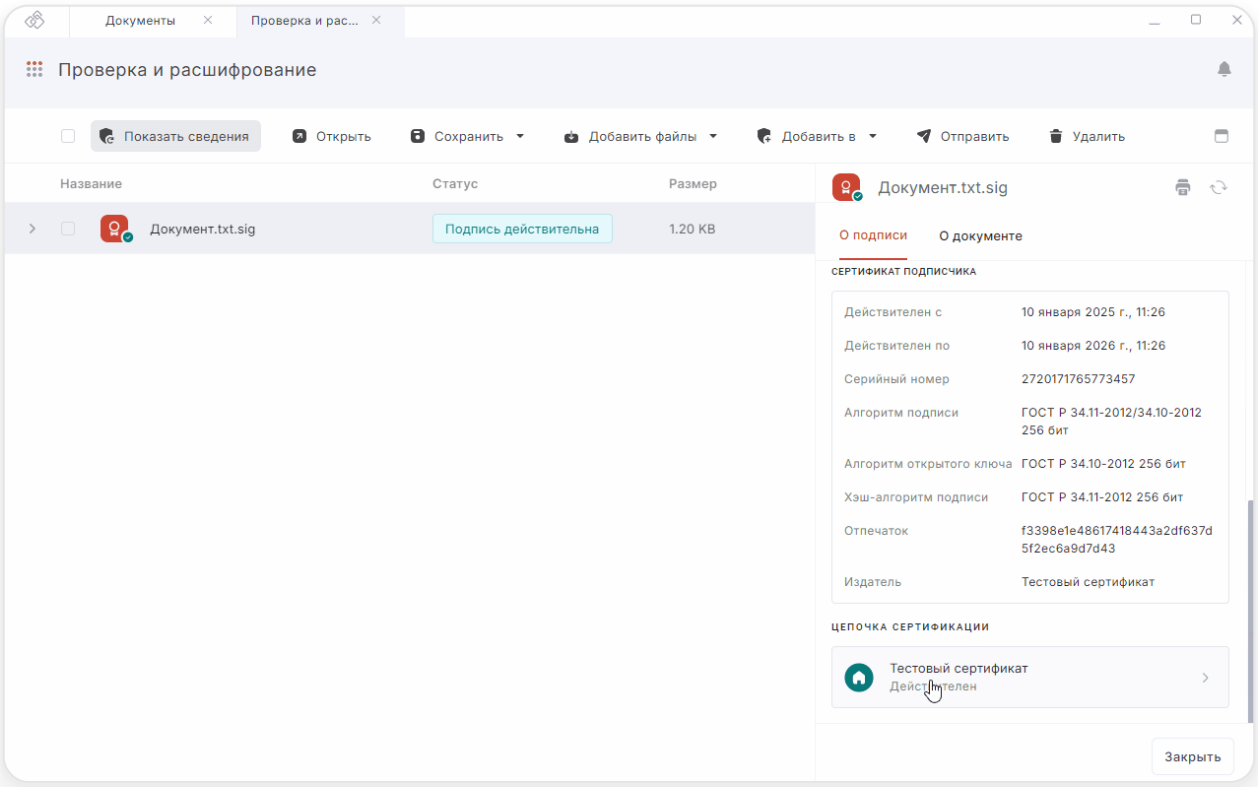
1. Выберите раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в левом боковом меню.
3. В открывшемся меню действий выберите **Импорт из файла**.
4. Откроется окно файлового менеджера.
5. Выберите файл сертификата.
6. Подтвердите запрос на установку сертификата.

При успешном импорте сертификат появится в списке хранилища сертификатов **Других пользователей**.

Как установить сертификат другого пользователя при проверке подписи документа

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование**. Подробнее в инструкции Проверка подписи документа.
2. Откройте область просмотра со сведениями о подписи.
3. В блоке **Цепочка сертификации** нажмите на сертификат подписанта.
4. Откроются сведения о сертификате.
5. Вызовите меню действий по кнопке **Еще**.
6. Нажмите на **Сохранить сертификат**.

Сертификат будет успешно сохранен в хранилище сертификаты «Других пользователей».

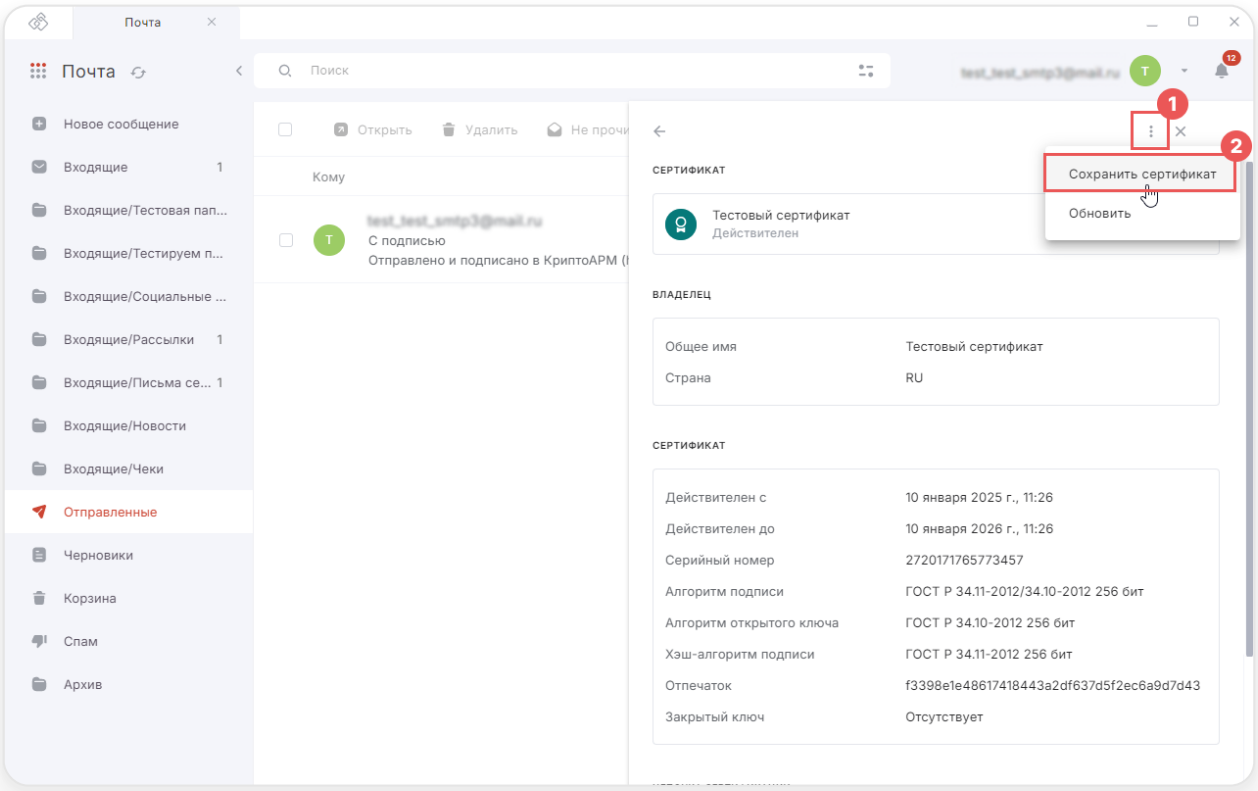


Статичный кадр демонстрации. Открыть анимацию

Как установить сертификат другого пользователя при проверке подписи письма

1. Откройте сведения о подписи письма. Подробнее в инструкции Как открыть сведения о подписи письма.
2. В блоке **Цепочка сертификации** нажмите на сертификат подписанта.
3. Откроются сведения о сертификате.
4. Вызовите меню действий по кнопке **Еще**.
5. Нажмите на **Сохранить в «Сертификатах»**.

Сертификат будет успешно сохранен в хранилище сертификаты «Других пользователей».



Сертификат будет успешно сохранен в хранилище сертификаты «Других пользователей».

Возможные ошибки

Ошибки, которые возникают при установке сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как установить корневой и промежуточный сертификаты.
2. Как импортировать список отзыва сертификатов (COC).
3. Как посмотреть уведомления.

Открыть статью на сайте

Установка списка отзыва

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

Как установить список отзыва

1. Выберите раздел **Сертификаты**.
2. Выберите группу **Списки отзыва**.
3. Нажмите кнопку **Добавить сертификат** в левом боковом меню.
4. В открывшемся меню действий выберите **Импорт из файла**.
5. Откроется окно файлового менеджера.
6. Выберите файл сертификата.
7. Подтвердите запрос на установку сертификата.

При успешном импорте COC отображается в разделе **Списки отзыва**.

Ошибки, которые возникают при установке сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Чтобы список отзыва был действительный, нужно в раздел **Удостоверяющие центры** установить сертификат, выпустивший этот список. Подробнее в инструкции Установка корневого и промежуточного сертификатов.

Инструкции по теме

1. Как установить корневой и промежуточный сертификаты.
2. Как посмотреть уведомления.

Открыть статью на сайте

Экспорт личного сертификата

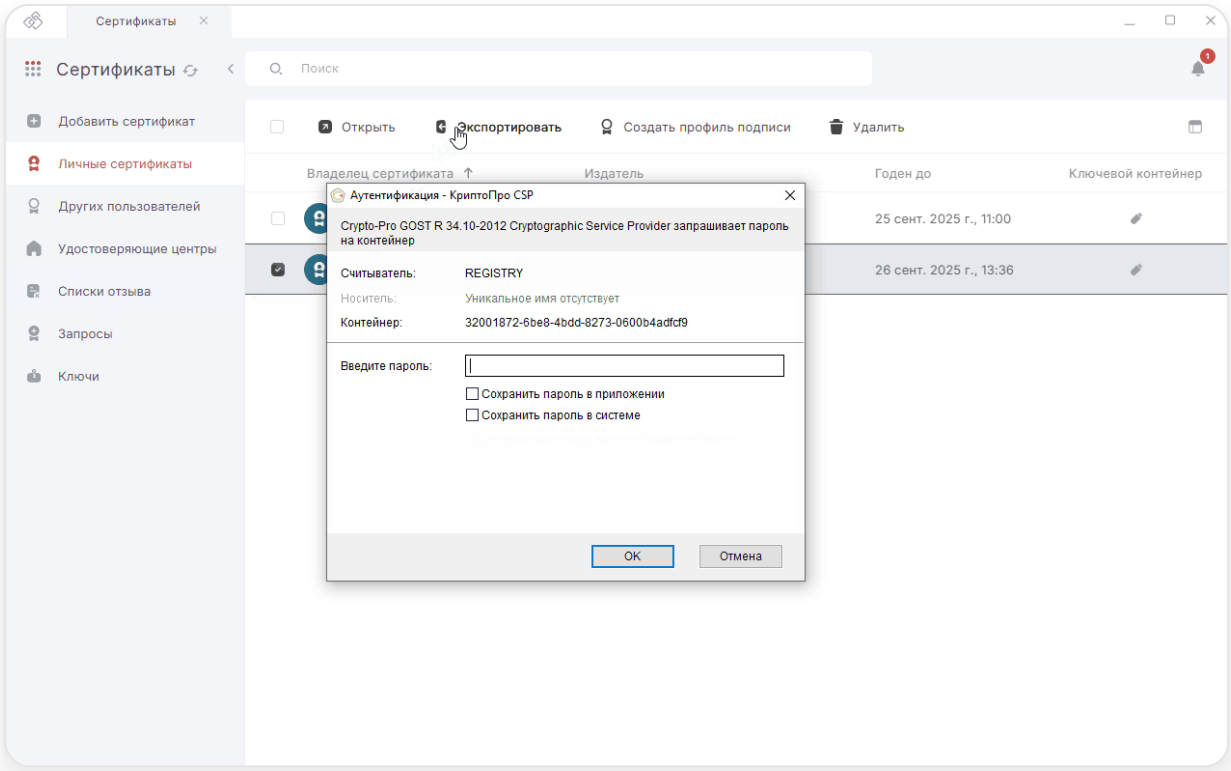
Для обмена шифрованными данными с другими пользователями необходимо экспортировать сертификат без закрытого ключа.

Экспорт сертификата с закрытым ключом выполняется в случае, если требуется перенести сертификат и его закрытый ключ на другое устройство, либо требуется сохранить копию сертификата вместе с закрытым ключом.

Важно. Вы можете экспортировать сертификат вместе с закрытым ключом, если ключ имеет флаг «экспортируемый». В противном случае эта функция недоступна.

Как экспортировать личный сертификат без закрытого ключа

1. Выберите раздел **Сертификаты**.
2. Выберите вкладку **Личные сертификаты**.
3. В списке выделите личный сертификат.
4. Нажмите кнопку **Экспортировать** на панели действий.
5. При необходимости введите пароль к ключевому контейнеру или нажмите **Отмена**. Если пароль не задан, то данный шаг пропускается.
6. Откроется окно **Экспорт сертификата**.
    - Выберите **Не экспортировать закрытый ключ**. Выбор может быть заблокирован, если ключ не экспортируемый.
    - Выберите тип кодировки BASE64 или DER.
7. Нажмите кнопку **Выполнить**.
8. В файловом менеджере задайте путь к файлу сертификата и имя файла.



Статичный кадр демонстрации. Открыть анимацию

Как экспортировать личный сертификат с закрытым ключом

Важно. Вы можете экспортировать сертификат вместе с закрытым ключом, если ключ имеет флаг «экспортируемый». В противном случае эта функция недоступна.

1. Выберите раздел **Сертификаты**.
2. Выберите вкладку **Личные сертификаты**.
3. В списке выделите личный сертификат.
4. Нажмите кнопку **Экспортировать** на панели действий.
5. При необходимости введите пароль к ключевому контейнеру или нажмите **Отмена**. Если пароль не задан, то данный шаг пропускается.
6. Откроется окно **Экспорт сертификата**.
    - Выберите **Экспортировать закрытый ключ**. Выбор экспорта закрытого ключа может быть заблокирован, если ключ не экспортируемый.
    - Выберите тип кодировки BASE64 или DER.
7. Укажите пароль от PFX-контейнера.
8. Нажмите кнопку **Выполнить**.
9. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Ошибки, которые возникают при экспорте сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как посмотреть уведомления.
2. Как экспортировать сертификат.
3. Как установить личный сертификат.
4. Как импортировать сертификаты других пользователей.

Открыть статью на сайте

Экспорт сертификата

Как экспортировать сертификат другого пользователя, корневой или промежуточный из файла

Примечание. Сертификаты других пользователей, корневые и промежуточные сертификаты экспортируются без закрытого ключа.

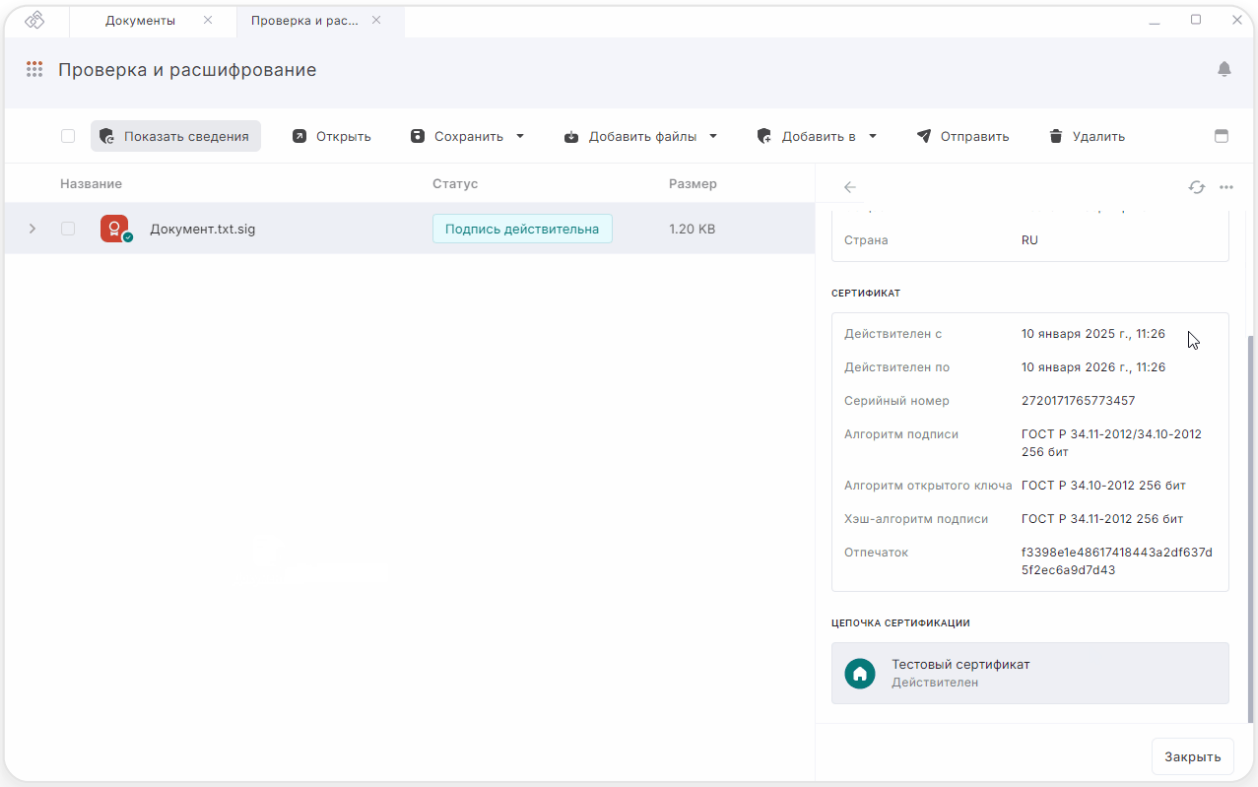
1. Выберите раздел **Сертификаты**.
2. Выберите вкладку **Личные сертификаты**.
3. В списке выделите личный сертификат.
4. Нажмите кнопку **Экспортировать** на панели действий.
5. Откроется окно **Экспорт сертификата**.
6. Выберите тип кодировки BASE64 или DER.
7. Нажмите кнопку **Выполнить**.
8. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Как экспортировать сертификат при проверке подписи документа

1. Выполните проверку подписи документа в мастере **Проверка и расшифрование**. Подробнее в инструкции Проверка подписи документа.
2. Откройте область просмотра со сведениями о подписи.
3. В блоке **Цепочка сертификации** 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 экспорт и нажмите **Выполнить**.
9. Укажите путь для сохранения файла с сертификатом в окне файлового менеджера.

При успешном выполнении операции сертификат экспортируется в файл.



Статичный кадр демонстрации. Открыть анимацию

Возможные ошибки

Ошибки, которые возникают при экспорте сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как посмотреть уведомления.
2. Как экспортировать личный сертификат.
3. Как импортировать сертификаты других пользователей.

Открыть статью на сайте

Удаление сертификата

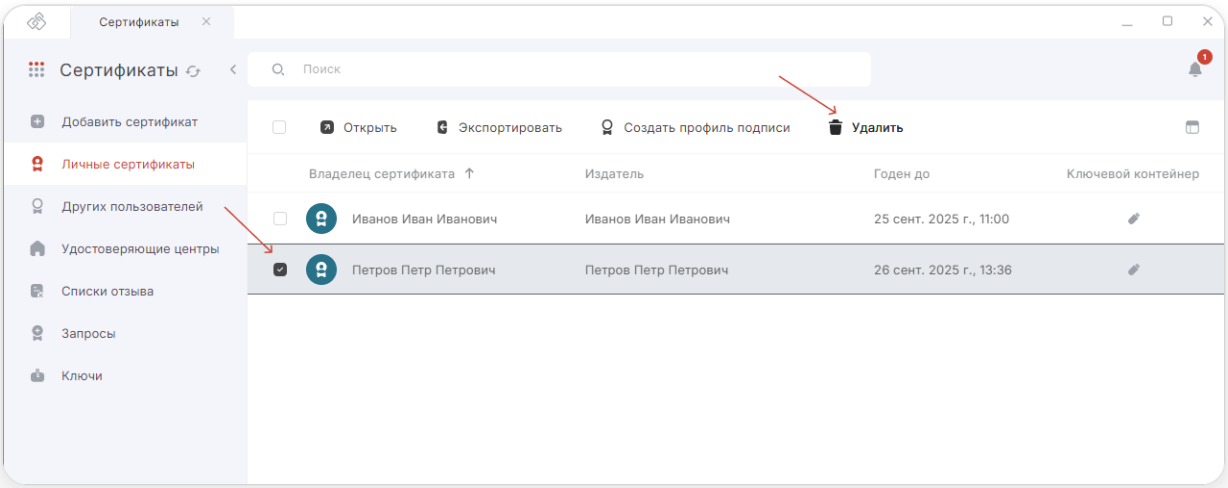
Как удалить сертификат

1. Выберите раздел **Сертификаты**.
2. Выберите хранилище, из которого необходимо удалить сертификат.
3. Выделите сертификат 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**.

   Важно. Не рекомендуется удалять контейнер закрытого ключа, так как он не подлежит восстановлению.

5. Подтвердите удаление.



Сертификат будет успешно удален из хранилища.

Ошибки, которые возникают при удалении сертификатов, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Инструкции по теме

1. Как посмотреть уведомления.
2. Как работать с ключевыми контейнерами.

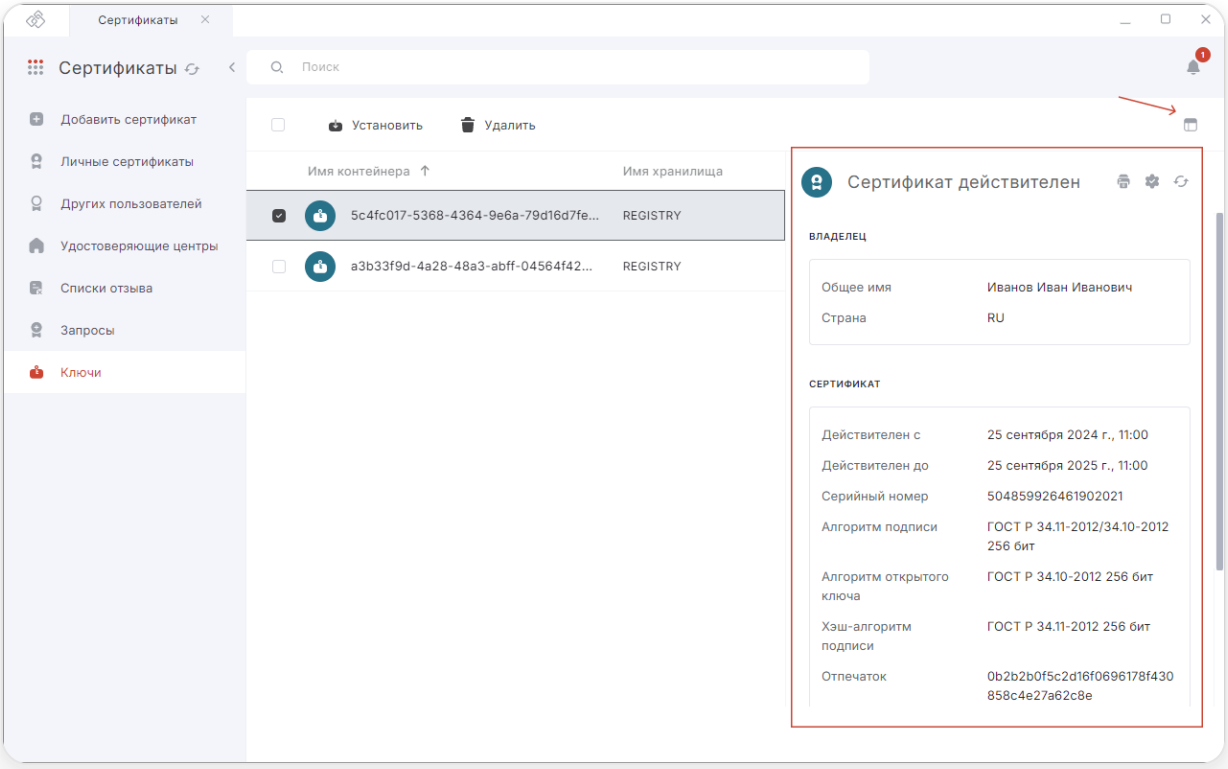
Открыть статью на сайте

Действия с ключевыми контейнерами

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

Как просмотреть сертификат в контейнере

1. При необходимости подключите ключевой носитель к устройству.
2. Выберите раздел **Сертификаты**.
3. Выберите хранилище **Ключи**. Откроется список контейнеров.
4. Выделите контейнер в списке.
5. Нажмите на иконку просмотра .
6. В боковой панели справа от списка отобразится информация о сертификате в контейнере. Если выводится надпись «В контейнере отсутствуют сертификаты», значит, контейнер не содержит сертификат.



Для сертификата в контейнере доступны **действия**:

- **Печать** — для печати информации о сертификате.
- **Протестировать** — для тестирования контейнера закрытого ключа.

- **Обновить** — для обновления информации о сертификате.



Как распечатать информацию о сертификате в контейнере

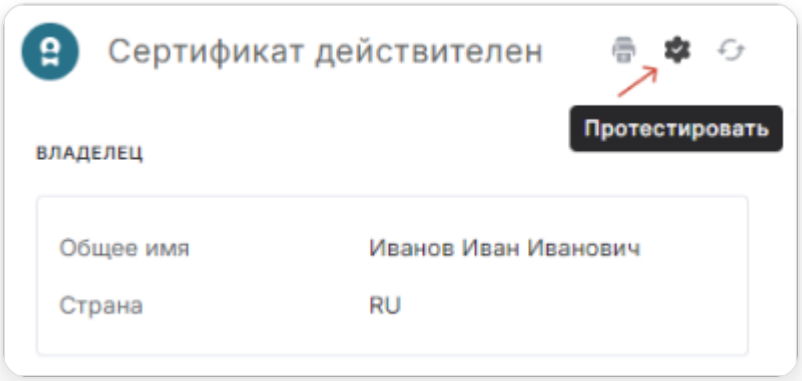
Примечание. Данная функция доступна только для контейнеров, в которых есть сертификат.

1. При необходимости подключите ключевой носитель к устройству.
2. Выберите раздел **Сертификаты**.
3. Выберите хранилище **Ключи**. Откроется список контейнеров.
4. Выделите контейнер в списке.
5. Нажмите на иконку просмотра .
6. В боковой панели справа от списка отобразится информация о сертификате в контейнере. Если выводится надпись «В контейнере отсутствуют сертификаты», значит, контейнер не содержит сертификат.
7. Нажмите на кнопку **Печать**.

Как проверить наличие контейнера закрытого ключа

Примечание. Данная функция доступна только для контейнеров, в которых есть сертификат.

1. При необходимости подключите ключевой носитель к устройству.
2. Выберите раздел **Сертификаты**.
3. Выберите хранилище **Ключи**. Откроется список контейнеров.
4. Выделите контейнер в списке.
5. Нажмите на иконку просмотра .
6. В боковой панели справа от списка отобразится информация о сертификате в контейнере. Если выводится надпись «В контейнере отсутствуют сертификаты», значит, контейнер не содержит сертификат.
7. В правой боковой панели нажмите на кнопку **Протестировать**.



8. При необходимости введите пароль к ключевому контейнеру.

В правой боковой панели отображается информационное сообщение о результатах тестирования контейнера.

Как установить сертификат из ключевого контейнера

Примечание. Данная функция доступна только для контейнеров, в которых есть сертификат.

1. При необходимости подключите ключевой носитель к устройству.
2. Выберите раздел **Сертификаты**.
3. Выберите хранилище **Ключи**. Откроется список контейнеров.
4. Выделите контейнер в списке.
5. Нажмите кнопку **Установить**.
6. При необходимости введите пароль к ключевому контейнеру.

Сертификат установлен в хранилище «Личные сертификаты».

Как удалить контейнер

Важно. Удаленный контейнер не подлежит восстановлению! Вам придется перевыпускать сертификат.

1. При необходимости подключите ключевой носитель к устройству.
2. Выберите раздел **Сертификаты**.
3. Выберите хранилище **Ключи**. Откроется список контейнеров.
4. Выделите контейнер в списке.
5. Нажмите кнопку **Удалить**.
6. Подтвердите удаление.

Если во время удаления был установлен флаг **Удалить связанный с контейнером сертификат**, то сертификат удалится из хранилища **Личные сертификаты**.

Как обновить список контейнеров

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Обновить**, размещенную рядом с заголовокм раздела.

Инструкции по теме

1. Как установить личный сертификат.

Открыть статью на сайте

Описание раздела

Раздел **Контакты** предназначен для управления адресными книгами и контактами.

- Как создать контакт
- Как импортировать контакт из файла vCard
- Как подключить адресную книгу LDAP
- Как подключить адресную книгу ALD Pro
- Как подключить адресную книгу по протоколу CardDAV
- Как привязать к контакту сертификат

Действия с контактами

В списке контактов вы можете выполнить следующие действия с контактами:

- **Создать** новый контакт, импортировать vCard, создать группу.
- **Открыть** информацию о выделенном контакте в новой вкладке.
- **Открыть** информацию о выделенном контакте для быстрого просмотра в правой боковой панели.
- **Написать** письмо выбранным контактам. Открывается вкладка с новым сообщением, где в поле Кому подставляются выбранные контакты или контакт. Доступна для контактов, у которых заполнено поле e-mail.
- **В группу** — добавить в группу контактов.
- **Редактировать** — открывается вкладка с формой редактирования контакта. Данная функция доступна только для локальных контактов; если вы выбрали контакт из LDAP, то кнопка заблокирована.
- **Поиск дубликатов** — открывается вкладка с поиском дубликатов локального контакта по e-mail среди контактов активной адресной книги.
- **Экспортировать** — данные о контакте (контактах) экспортируются в файл формата .vcf, которые можно импортировать, например, в КриптоАРМ 6.
- **Отправить контакт** — откроется окно редактирования нового письма, в котором приложением будет сформированный файл формата .vcf.
- **Удалить** контакт. Удаленный контакт помещается в **Корзину**. Данная функция доступна только для локальных контактов. Если вы выбрали контакт из LDAP, то кнопка заблокирована.
- **Найти** контакт по ФИО, e-mail или номеру телефона.

Поиск дубликатов

При нажатии на **Поиск дубликатов** в верхней панели действий открывается вкладка с поиском дубликатов локального контакта по e-mail среди контактов активной адресной книги. Поиск осуществляется по e-mail.

Для поиска дубликатов нужно нажать на **Поиск дубликатов**. В открывшейся вкладке будет показан результат поисков:

- **Не найдено контактов со схожими данными** — в списке контактов отсутствуют контакты с одинаковыми электронными адресами.
- **Найдено контактов со схожими данными (N)** — в списке контактов найдены контакты с одинаковыми электронными адресами.

Найденные контакты можно **Пропустить** или **Объединить**:

- **Пропустить** — при новом поиске дубликатов данные контакты не будут выводиться в результатах поиска.
- **Объединить** — все контакты объединяются в один контакт, который был создан первым (или до импорта адресной книги), с добавлением недостающей информации (если такая есть). Его можно **Открыть**, чтобы **Написать** или **Удалить**.

Настройка колонок

При нажатии на кнопку **Настроить колонки** откроется окно выбора столбцов:

- электронная почта;
- мобильный номер телефона;
- городской номер телефона;
- должность;
- организация;
- отдел;
- дата рождения;
- регион;
- город;
- адрес;
- индекс.

При нажатии на названия соответствующие столбцы будут появляться или исчезать в главном окне вкладки **Контакты**.

Инструкции по теме

1. Как добавить локальный контакт.
2. Как добавить адресную книгу LDAP.
3. Как переключаться между адресными книгам.
4. Как посмотреть информацию о контакте.
5. Как удалять локальные контакты.
6. Как отправлять электронные письма.

Открыть статью на сайте

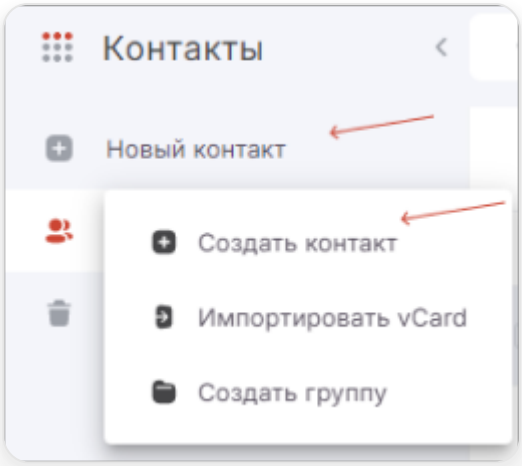
Добавление контакта

Вы можете создавать контакты для хранения имен, адресов электронной почты, номеров телефонов и других данных. При вводе получателя нового письма этот контакт появится в списке для выбора.

Вы можете привязать сертификат к контакту для шифрования писем в его адрес.

Как создать контакт

1. Перейдите в раздел **Контакты**.
2. Нажмите на кнопку **Новый контакт** в боковом меню слева.
3. Выберите **Создать контакт**.



4. Заполните данные о контакте.
5. Добавьте фото контакта. Подробнее о фото в инструкции Добавление фото к контакту.
6. Нажмите кнопку **Сохранить**.

Как создать контакт из сертификата

1. Перейдите в раздел **Сертификаты**.
2. Выберите хранилище сертификатов **Других пользователей**.
3. Выделите сертификат в списке.
4. На верхней панели действий нажмите **Создать контакт**.
5. Откроется форма создания контакта с данными, заполненными на основании сертификата.
6. Заполните данные о контакте.
7. Добавьте фото контакта. Подробнее о фото в инструкции Добавление фото к контакту
8. Нажмите **Сохранить**.

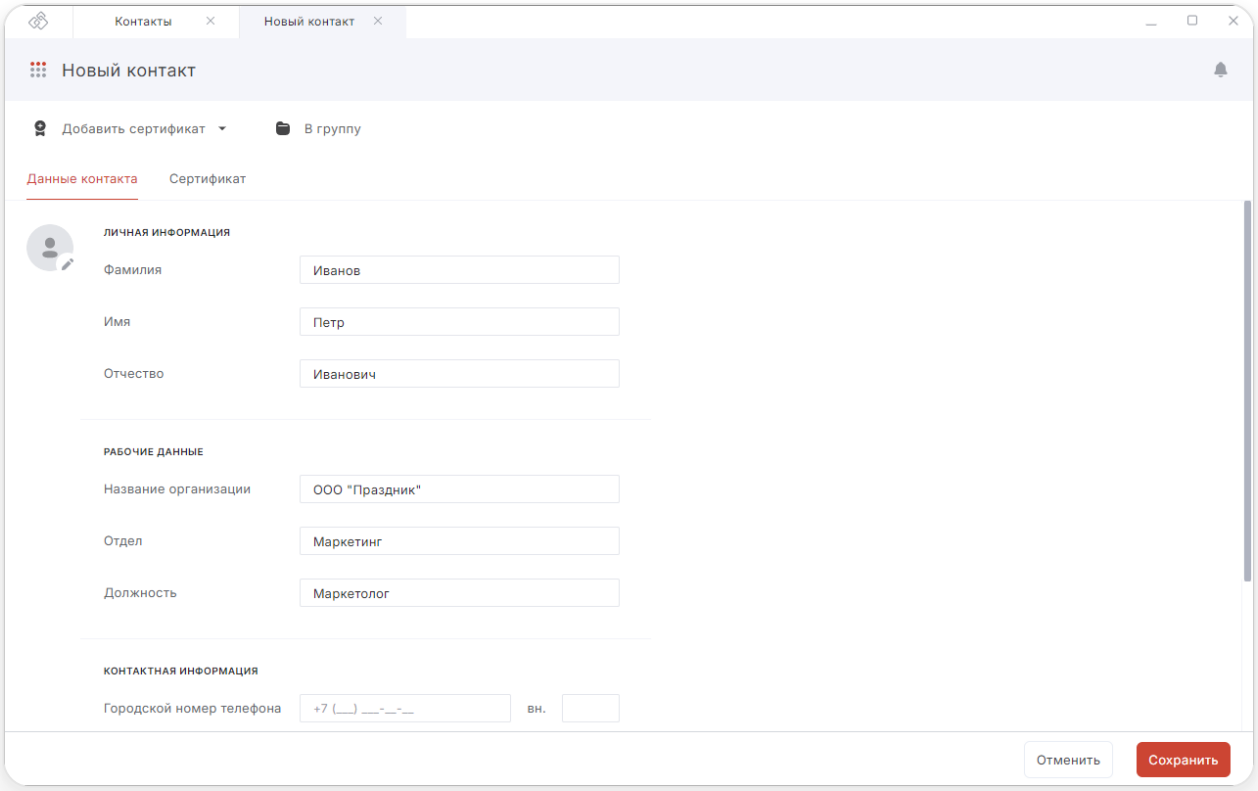
При успешном выполнении операции созданный контакт появляется в списке контактов.

Описание полей формы добавления контакта

Поля сгруппированы по вкладкам **Данные контакта** и **Сертификат**.

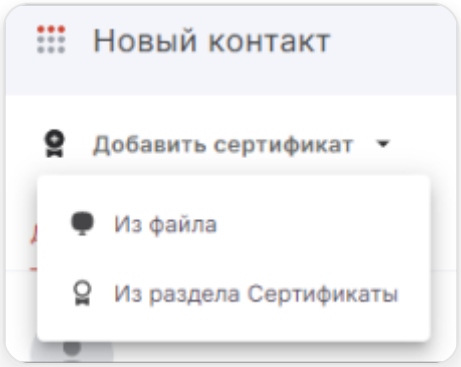
Поля раздела **Данные контакта**:

- фото;
- личная информация: фамилия, имя, отчество;
- рабочие данные: название организации, отдел, должность;
- контактная информация: городской номер телефона, мобильный номер телефона, e-mail;
- дополнительная информация: день рождения, адрес, примечание.



Кнопка **Добавить** добавляет дополнительное поле. Доступна для полей: мобильный номер телефона и адрес электронной почты.

В разделе **Сертификат** отображается список привязанных к контакту сертификатов.



Инструкции по теме

1. Как привязать сертификат к контакту.
2. Как удалять локальные контакты.
3. Как редактировать локальные контакты.
4. Как добавить адресную книгу LDAP.

Открыть статью на сайте

Просмотр информации о контакте

Быстрый просмотр

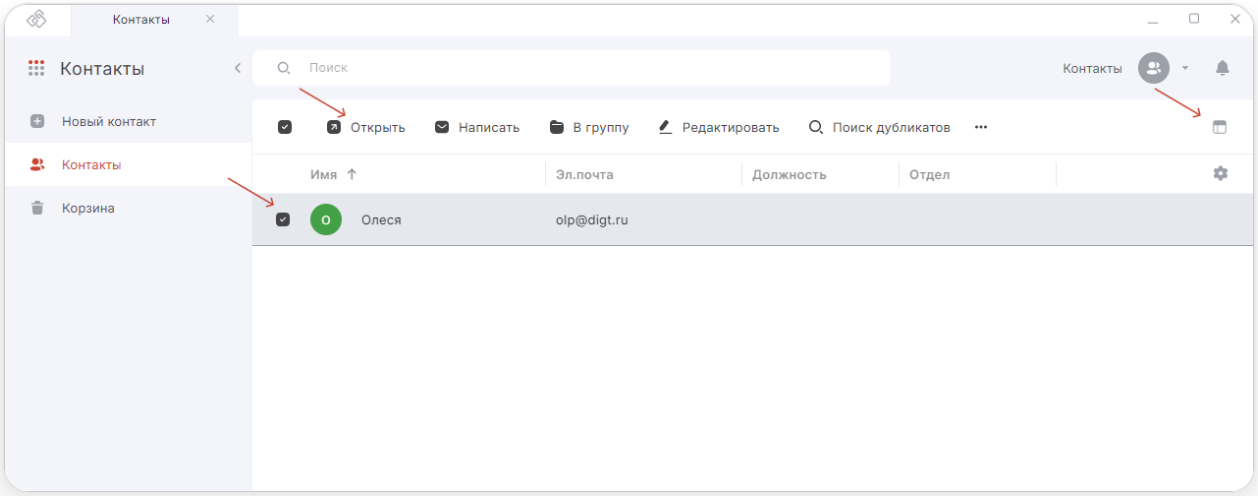
1. Перейдите в раздел **Контакты**.
2. Нажмите на панель с контактом в списке контактов.
3. Нажмите кнопку **Просмотреть** .
4. Справа от списка контактов откроется панель со сведениями о контакте.

Область просмотра контакта отображается в правой боковой панели.

Просмотр в новой вкладке

1. Перейдите в раздел **Контакты**.
2. Выделите контакт в списке нажатием курсора.
3. На верхней панели нажмите кнопку **Открыть**.

Информация о контакте открывается для просмотра в новой вкладке.



Вы можете написать письмо контакту и удалить контакт.

Инструкции по теме

1. Как редактировать локальный контакт.
2. Как переключаться между адресными книгами.

Открыть статью на сайте

Привязка сертификата к контакту

Чтобы шифровать документы в адрес контакта, нужно привязать сертификат к контакту.

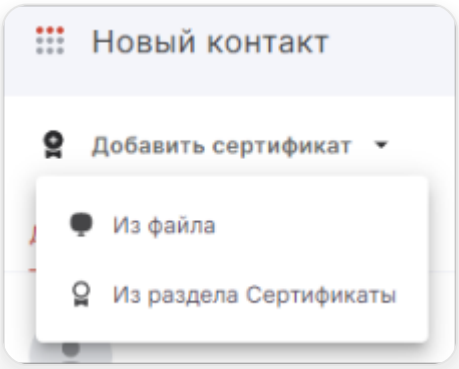
Примечание. Данная функция доступна только для локальных контактов.

Важно. Чтобы привязать сертификат, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

Как привязать к контакту сертификат, установленный в приложении

Для привязки к контакту доступны сертификаты из хранилищ **Личные сертификаты** и **Других пользователей**.

1. Откройте форму создания или редактирования контакта.
2. Нажмите кнопку **Добавить сертификат** → **Из раздела Сертификаты**.



3. Откроется окно со списком сертификатов из хранилищ **Личные сертификаты** и **Других пользователей**.
4. Выберите сертификат, нажав на иконку сертификата. Возможен множественный выбор. После выбора сертификат автоматически добавится в список сертификатов контакта.
5. После выбора закройте окно со списком сертификатов.
6. Нажмите кнопку **Сохранить**.

Как привязать к контакту сертификат из файла

Если у вас нет сертификатов в хранилищах **Личные сертификаты** и **Других пользователей**, вы можете выполнить привязку сертификата из файла.

1. Откройте форму создания или редактирования контакта.

2. Нажмите кнопку **Добавить сертификат — Из файла**.
3. Откроется окно файлового менеджера.
4. Выберите файл с сертификатом.
5. После выбора сертификат автоматически добавится в список сертификатов контакта.
6. Нажмите кнопку **Сохранить**.

Как привязать к контакту сертификат в разделе «Сертификаты»

1. Перейдите в раздел **Сертификаты**.
2. Выберите хранилище сертификаты **Других пользователей**.
3. Выделите сертификат в списке.
4. На верхней панели действий нажмите кнопку **Привязать к контакту**.
5. В правой боковой панели из списка выберите контакт, к которому будет привязан сертификат.

Сертификат успешно привязан к контакту.

Инструкции по теме

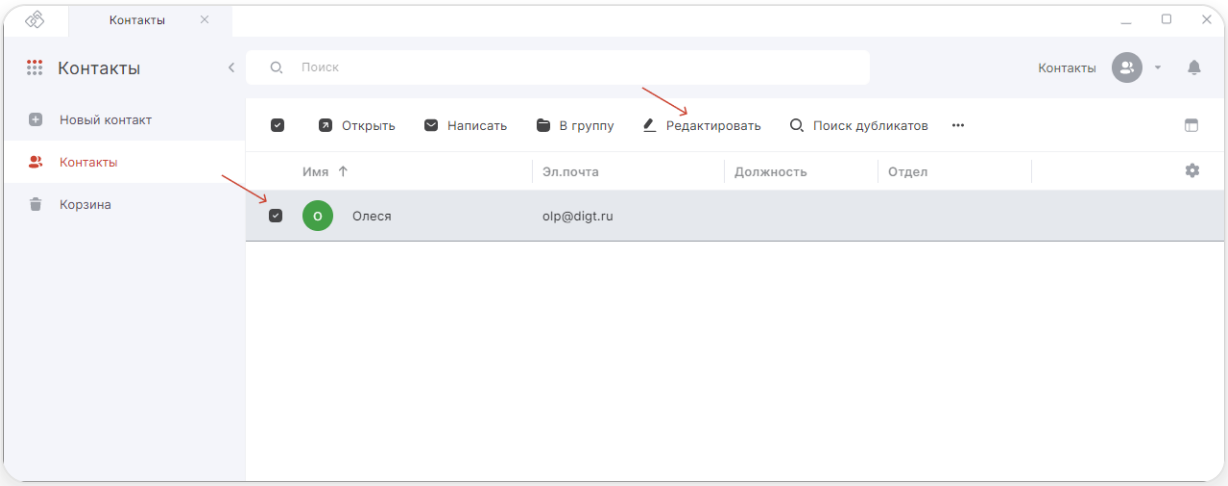
1. Как добавить локальный контакт.
2. Как редактировать локальный контакт.
3. Как импортировать сертификаты других пользователей.

Открыть статью на сайте

Редактирование контакта

Примечание. Для редактирования доступны только локальные контакты.

1. Перейдите в раздел **Контакты**.
2. Выделите в списке контакт, данные которого необходимо отредактировать.
3. Нажмите кнопку **Редактировать** в верхней панели.



4. Внесите изменения в данные и фото контакта. Подробнее об изменении фото в инструкции Добавление фото к контакту.
5. Нажмите кнопку **Сохранить**.

Инструкции по теме

1. Как добавить локальный контакт.
2. Как привязать сертификат к контакту.

Открыть статью на сайте

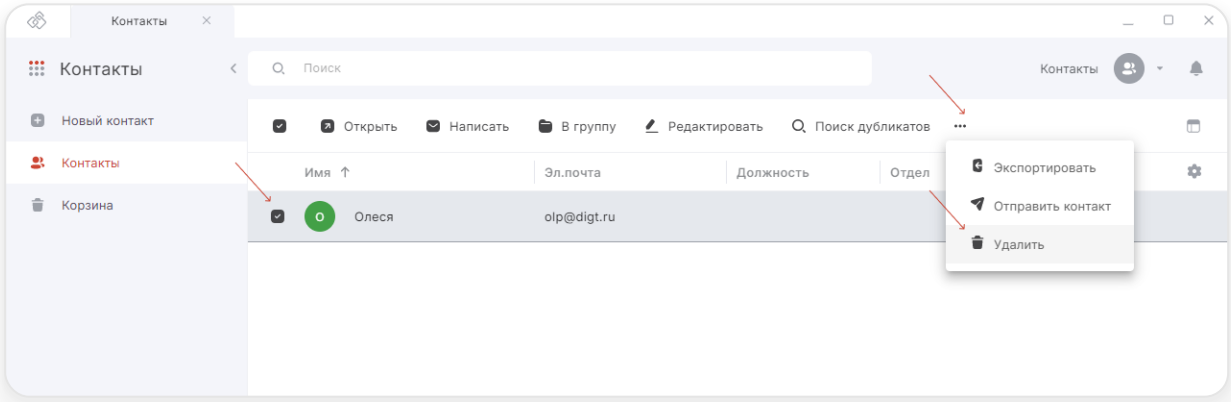
Удаление локальных контакта

Удаленные контакты хранятся в группе «Корзина».

Удалить можно только локальные контакты. Контакты из подключенных адресных книг LDAP и ALD Pro будут удалены при удалении самой адресной книги.

Как удалить контакт

1. Перейдите в раздел **Контакты**.
2. Нажмите на панель с контактом в списке.
3. В верхней панели нажмите на кнопку **Удалить**.



Как удалить несколько контактов

1. Перейдите в раздел **Контакты**.
2. Установите флажки слева от контактов, которые необходимо удалить.
3. В верхней панели нажмите на кнопку **Удалить**.

Как удалить контакт из «Корзины»

1. Перейдите в раздел **Контакты**.
2. В левом боковом меню выберите **Корзина**.
3. Установите флажки слева от контактов, которые необходимо навсегда удалить.
4. Нажмите **Удалить навсегда**.

Чтобы очистить «Корзину», установите флажки для всех контактов в списке и нажмите на кнопку **Удалить навсегда** на панели действий.

Инструкции по теме

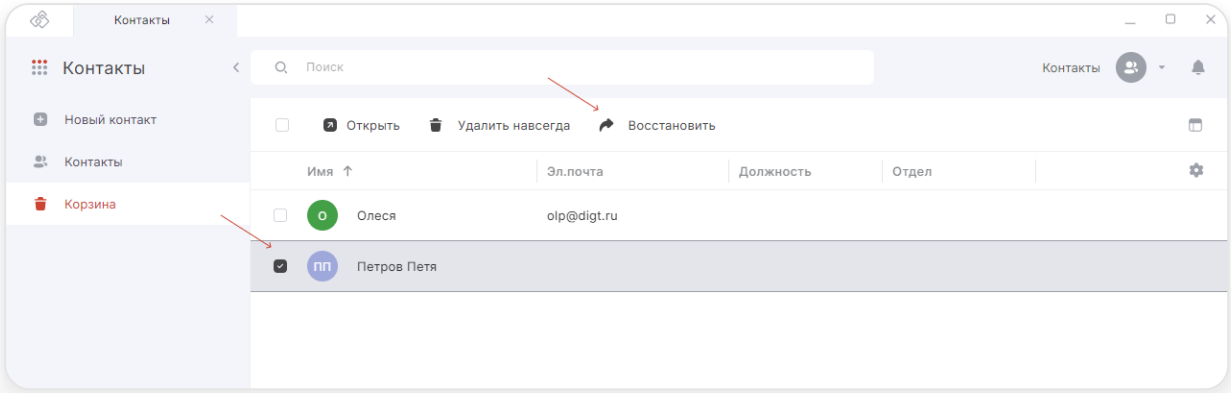
1. Как восстановить удаленные контакты из корзины.
2. Как удалить адресную книгу LDAP.

Открыть статью на сайте

Восстановление удаленных контактов

После переноса контакта в «Корзину» его можно восстановить.

1. Перейдите в раздел **Контакты**.
2. В левом боковом меню выберите **Корзина**.
3. Установите флажки напротив контактов, которые необходимо восстановить.
4. В верхней панели нажмите на кнопку **Восстановить**.



Открыть статью на сайте

Поиск контакта

Чтобы найти определенный контакт:

1. Перейдите в раздел **Контакты**.
2. В поисковой строке введите параметры поиска.

Поиск возможен по следующим значениям: ФИО, e-mail, номер телефона.

Инструкции по теме

1. Как добавить адресную книгу LDAP.
2. Как добавить локальный контакт.
3. Как посмотреть информацию о контакте.

Открыть статью на сайте

Группа контактов

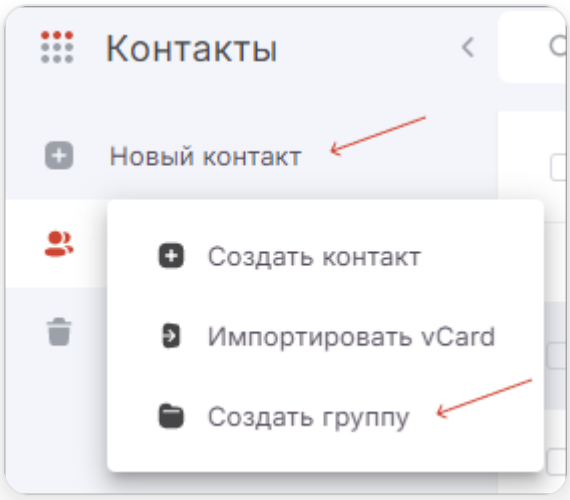
Группа контактов позволяет разделить все контакты по тем или иным признакам. Контакты распределяются по группам по желанию пользователя. Можно создавать несколько уровней вложенности.

Создание группы контактов

Группу контактов можно создать несколькими способами.

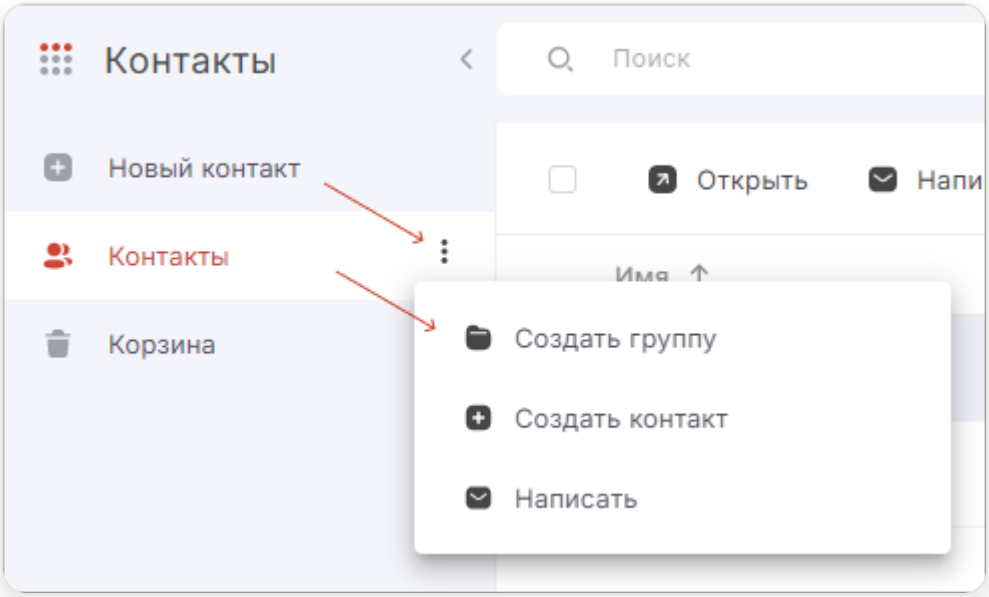
Первый способ:

1. Открыть раздел **Контакты**.
2. Нажать на **Новый контакт** → **Создать группу**.
3. В открывшемся окне указать название группы и уровень вложенности (в **Контакты** или в ранее созданную группу).



Второй способ:

1. Открыть раздел **Контакты**.
2. Нажать на контекстное меню вкладки **Контакты** → **Создать группу**.
3. В открывшемся окне указать название группы и уровень вложенности (в **Контакты** или в ранее созданную группу).



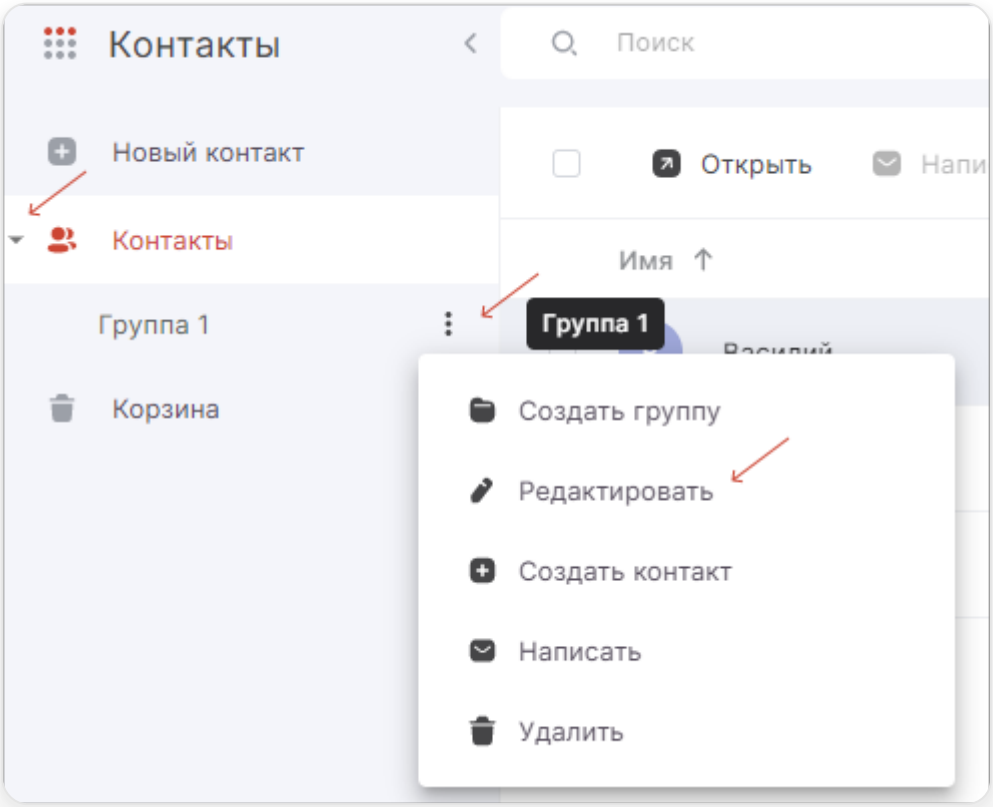
Действия с группой контактов

Доступны следующие действия для группы контактов:

1. **Создать группу** — откроется окно создания группы контактов с назначенным уровнем вложенности.
2. **Редактировать** — можно изменить название группы и уровень вложенности.
3. **Создать контакт** — откроется окно создания контакта с назначенной вложенностью в выбранную группу.
4. **Написать** — откроется вкладка нового сообщения с электронными адресами получателей, которые состоят в данной группе.
5. **Удалить** — откроется окно подтверждения удаления группы.

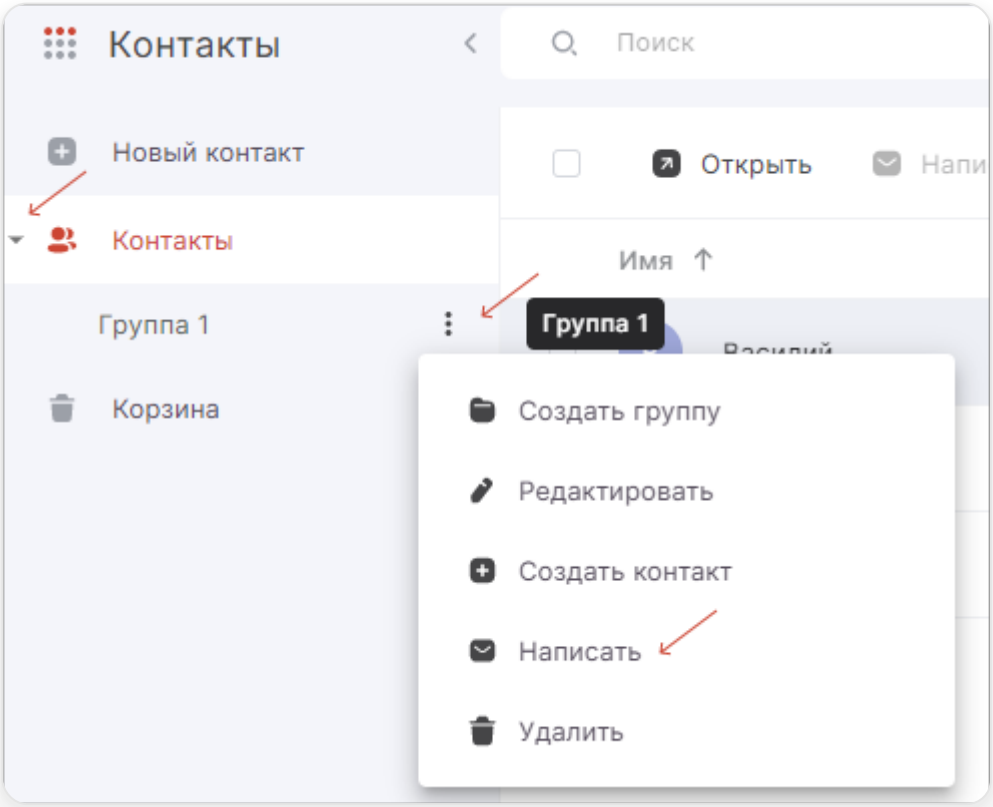
Редактирование группы

1. Открыть раздел **Контакты**.
2. Нажать на контекстное меню нужной группы контактов.
3. Выбрать **Редактировать**.
4. Изменить название и (или) уровень вложенности группы.
5. **Сохранить** изменения.



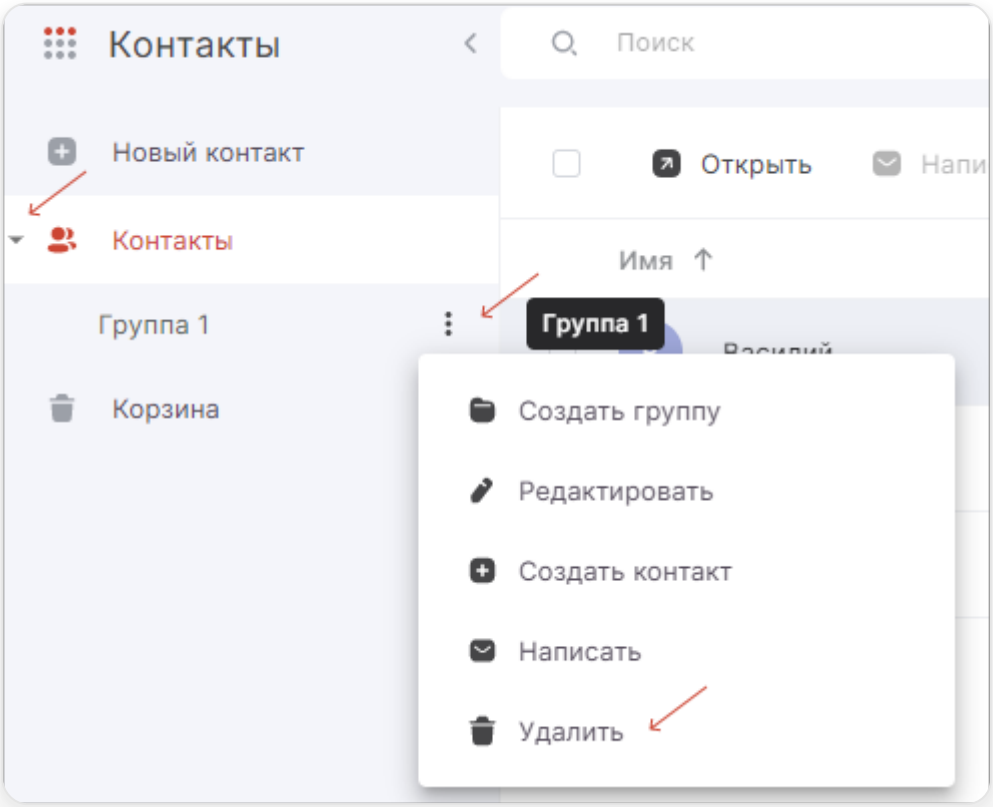
Отправка писем контактам одной группы

1. Открыть раздел **Контакты**.
2. Нажать на контекстное меню нужной группы контактов.
3. Выбрать **Написать**.
4. Написать письмо.
5. Нажать на **Отправить**.



Удаление группы контактов

1. Открыть раздел **Контакты**.
2. Нажать на контекстное меню нужной группы контактов.
3. Выбрать **Удалить**.
4. Подтвердить удаление группы, её подгрупп и контактов.


Контакты
Поиск
Новый контакт
Открыть
Напи
Контакты
Имя
Группа 1
Группа 1
Василий
Корзина
Создать группу
Редактировать
Создать контакт
Написать
Удалить

Открыть статью на сайте

Добавление фото к контакту

Для каждого контакта вы можете загрузить фотографию с компьютера или выбрать аватар с сервиса Gravatar. Тогда в разделе **Почта** и **Документы** вы будете видеть не только имя контакта, но и изображение, которое для него установили.

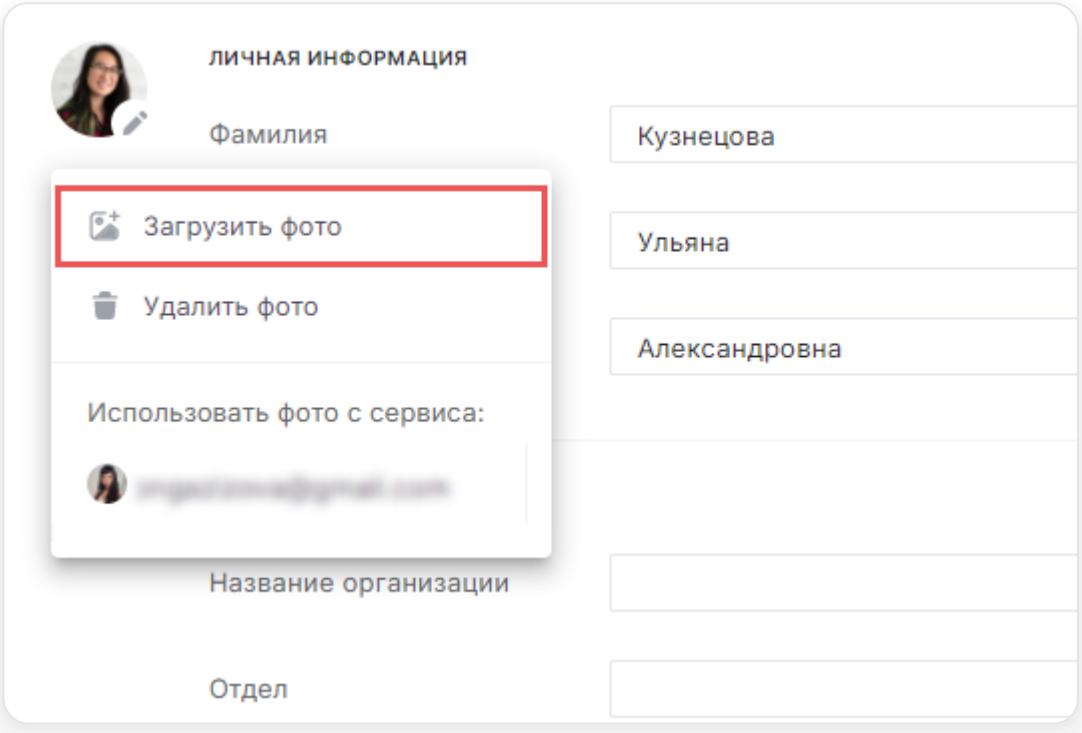
Gravatar — сервис, позволяющий интернет-пользователям хранить свой аватар на специальном сервере.

Важно. Адрес электронной почты, сохраненный в контакте, должен совпадать с адресом пользователя, зарегистрированным на сервисе Gravatar. Если адреса не совпадают, то аватар отображаться не будет.

Примечание. При экспорте контакта с привязанным фото в формате .vcf, фото экспортируется вместе с контактом. При импорте контакта с привязанным фото в формате .vcf фото импортируется вместе с контактом. Подробнее про поддержку vCard.

Как загрузить фото контакта

1. Перейдите в раздел **Контакты**.
2. Откройте форму редактирования контакта. Как открыть форму редактирования.
3. Нажмите на аватар контакта.
4. Откроется меню действий с аватаром контакта.
5. Выберите **Загрузить фото**.



6. Откроется окно файлового менеджера.
7. Укажите путь к файлу с фото. Доступны для выбора файлы в формате jpg (jpeg), gif, png, bmp размером не более 2mb.
8. Нажмите **Сохранить** в форме редактирования контакта.

Фотография будет прикреплена к контакту и станет его аватаркой. Она будет доступна во всех разделах приложения, где используется этот контакт.

Как установить фото контакта из сервиса Gravatar

1. Перейдите в раздел **Контакты**.
2. Откройте форму редактирования контакта. Как открыть форму редактирования.
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 будет прикреплена к контакту и станет его аватаркой. Она будет доступна во всех разделах приложения, где используется этот контакт.

Как удалить фото контакта

1. Перейдите в раздел **Контакты**.
2. Откройте форму редактирования контакта. Как открыть форму редактирования.
3. Нажмите на аватар контакта.
4. Откроется меню действий с аватаром контакта.
5. Выберите действий **Удалить фото**.

Открыть статью на сайте

Добавление адресной книги LDAP

В приложении КриптоАРМ поддерживается импорт контактов и синхронизации информации о них из адресной книги LDAP.

Описание полей формы подключения

Название поля	Описание
Название адресной книги	Произвольное название, которое будет отображаться в приложении
Имя сервера	Адрес сервера
Порт	Порт для подключения к серверу
Имя пользователя	Учетная запись для подключения к серверу
Пароль	Пароль для учетной записи
Время ожидания	Время ожидания ответа сервера
Не возвращать более чем	Количество записей, возвращаемых сервером. Для серверов, которые настроены для постраничной передачи данных.
Фильтр поиска	Фильтр поиска учетных записей. По умолчанию фильтр отключен.
База поиска	DN контейнера, в котором будет выполняться поиск записей
Автообновление каталога	Настройка синхронизации данных с сервером. По умолчанию автообновление отключено.

Как добавить адресную книгу LDAP

Шаг 1. Настройка LDAP

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.

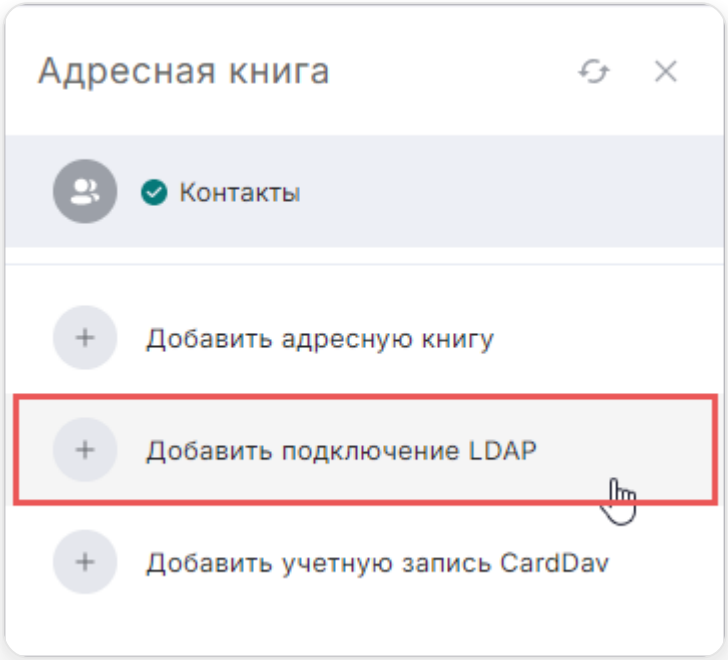
3. Сервер LDAP должен быть доступен по сети с компьютера, на котором работает почтовый клиент. Если данный сервер находится за NAT или он закрыт брандмауэром, то необходимо обеспечить доступ по следующим портам:

   - 389 tcp или udp. Незащищенный доступ к активному каталогу.
   - 636 tcp или udp. Доступ с защитой SSL.

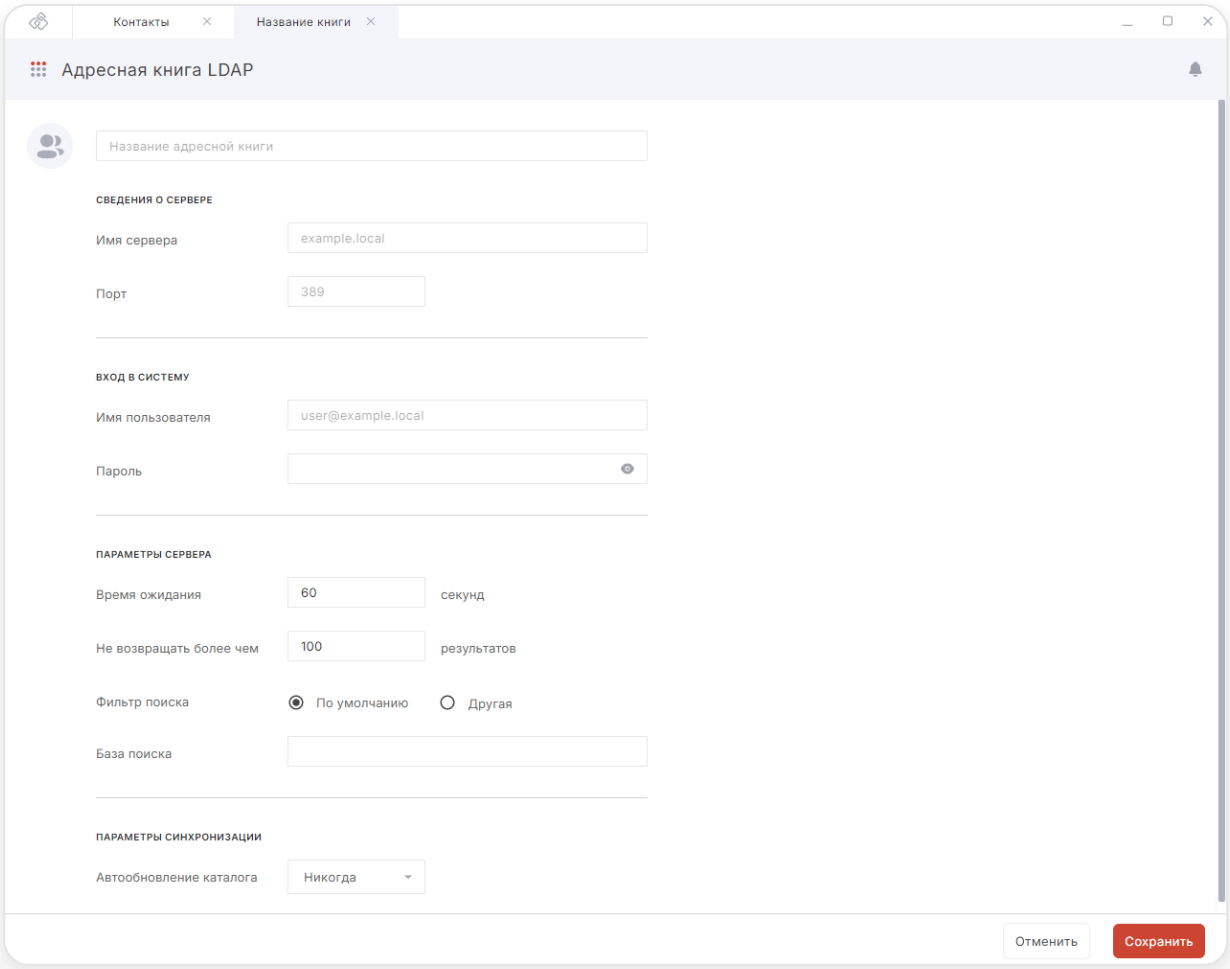
   Достаточно открыть и использовать один из данных портов, желательно 636.

Шаг 2. Создание подключения в КриптоАРМ

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Выберите **Добавить подключение LDAP**.



4. Откроется форма добавления адресной книги.



5. Укажите настройки подключения.
6. Нажмите **Сохранить**.

После подключения в списке адресных книг появится новая книга.

Чтобы просмотреть контакты адресной книги, необходимо переключиться на неё. Подробнее в инструкции Переключение между адресными книгами.

Возможные ошибки

Ошибки, которые возникают при подключении адресной книги, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

- Не удалось подключиться к LDAP — проверьте правильность заполнения полей **Имя сервера** и **Порт**. Проверьте **Имя пользователя** и **Пароль**.

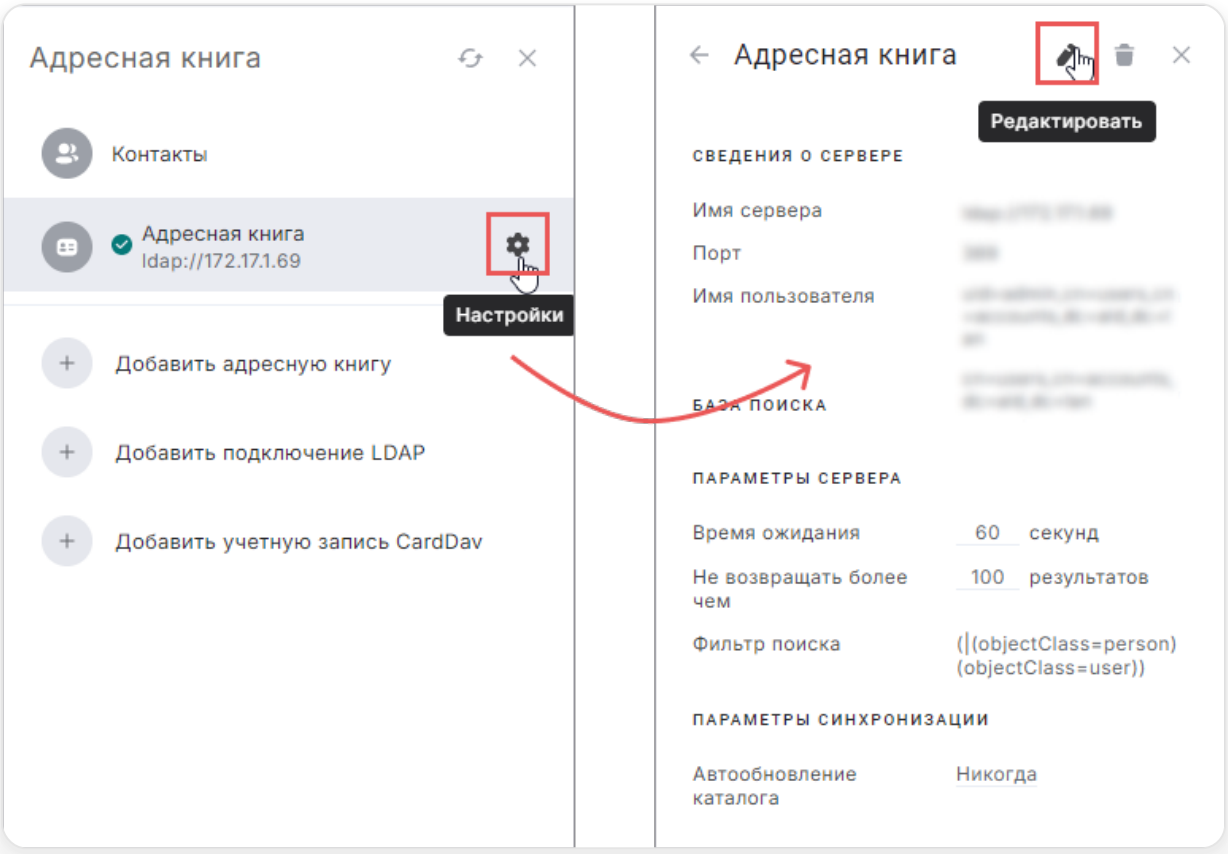
Инструкции по теме

1. Как переключаться между адресными книгами.
2. Как редактировать адресную книгу LDAP.
3. Как удалить адресную книгу LDAP.
4. Как посмотреть информацию о контакте.
5. Как посмотреть уведомления.

Открыть статью на сайте

Редактирование настроек адресной книги LDAP

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки**.
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Редактировать**.



7. Откроется форма для редактирования настроек адресной книги.
8. Внесите изменения и нажмите кнопку **Сохранить**.

При успешном подключении контакты адресной книги LDAP обновятся.

Возможные ошибки при подключении

Ошибки, которые возникают при подключении адресной книги, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

- Не удалось подключиться к LDAP — проверьте правильность заполнения полей **Имя сервера** и **Порт**. Проверьте **Имя пользователя** и **Пароль**.

Инструкции по теме

1. Как удалить адресную книгу LDAP.
2. Как посмотреть информацию о контакте.
3. Как посмотреть уведомления.

Открыть статью на сайте

Удаление адресной книги LDAP

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки**.
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Удалить**.
7. Подтвердите действие в модальном окне.

Адресная книга удаляется. Удаляются все ее контакты.

Инструкции по теме

1. Как добавить адресную книгу LDAP.
2. Как посмотреть информацию о контакте.

Открыть статью на сайте

Адресная книга ALD Pro

ALD Pro — это 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» как альтернатива западному решению — Microsoft Active Directory для централизованного управления и администрирования ИТ-инфраструктуры.

В приложении КриптоАРМ поддерживается импорт контактов и синхронизации информации о них из адресной книги ALD Pro.

Описание полей формы подключения

Название поля	Описание
Название адресной книги	Произвольное название, которое будет отображаться в приложении
Имя сервера	Адрес сервера
Порт	Порт для подключения к серверу
Имя пользователя	Учетная запись для подключения к серверу
Пароль	Пароль для учетной записи
Время ожидания	Время ожидания ответа сервера
Не возвращать более чем	Количество записей, возвращаемых сервером. Для серверов, которые настроены для постраничной передачи данных.
Фильтр поиска	Фильтр поиска учетных записей. По умолчанию фильтр отключен.
База поиска	DN контейнера, в котором будет выполняться поиск записей
Автообновление каталога	Настройка синхронизации данных с сервером. По умолчанию автообновление отключено.

Как подключить адресную книгу ALD Pro

Шаг 1. Настройка ALD Pro

1. Создайте в ALD Pro 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 ALD Pro 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:

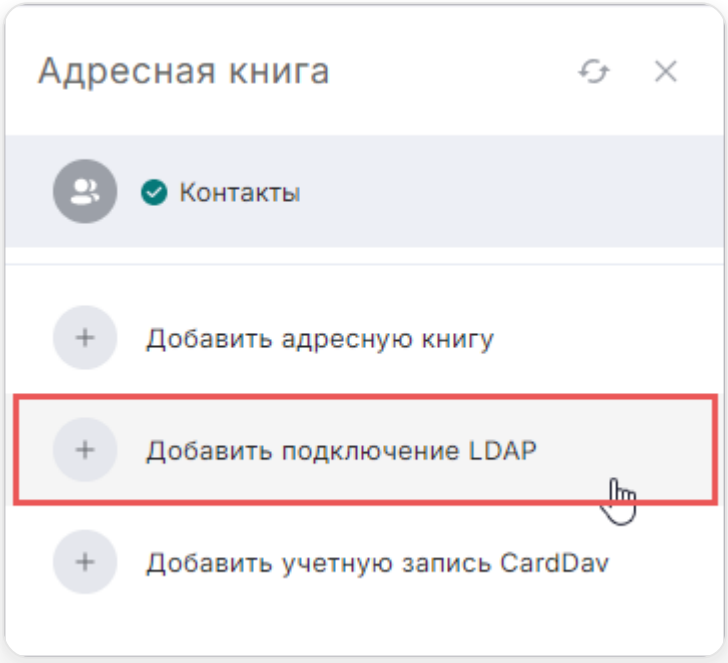
   - 389 tcp или udp. Незащищенный доступ к активному каталогу.
   - 636 tcp или udp. Доступ с защитой SSL.

   Достаточно открыть и использовать один из данных портов, желательно 636.

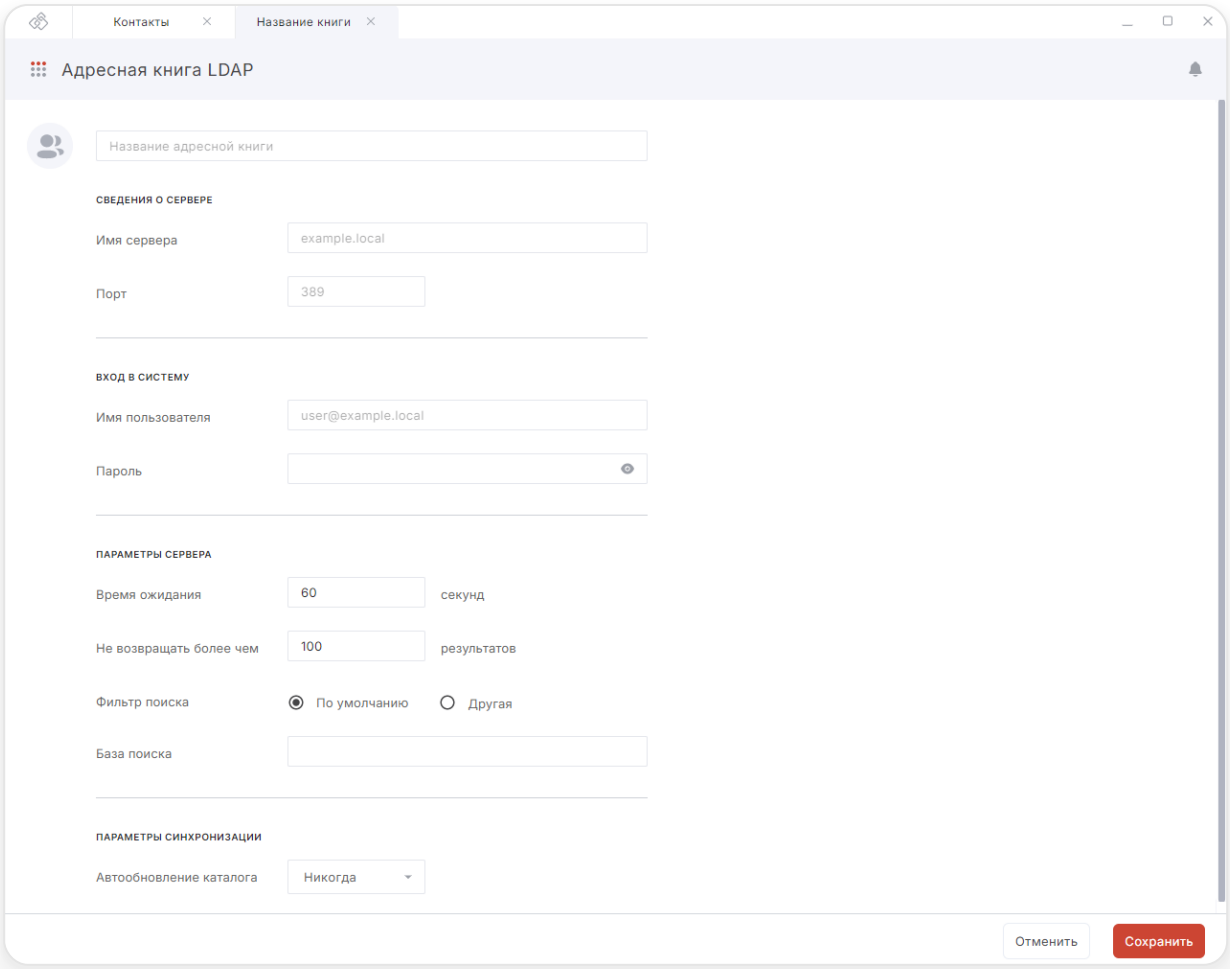
Шаг 2. Создание подключения в КриптоАРМ

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.

3. Выберите **Добавить подключение LDAP**.



4. Откроется форма добавления адресной книги.



5. Укажите настройки подключения.
6. Нажмите **Сохранить**.

После подключения в списке адресных книг появится новая книга.

Чтобы просмотреть контакты адресной книги, необходимо переключиться на неё. Подробнее в инструкции Переключение между адресными книгами.

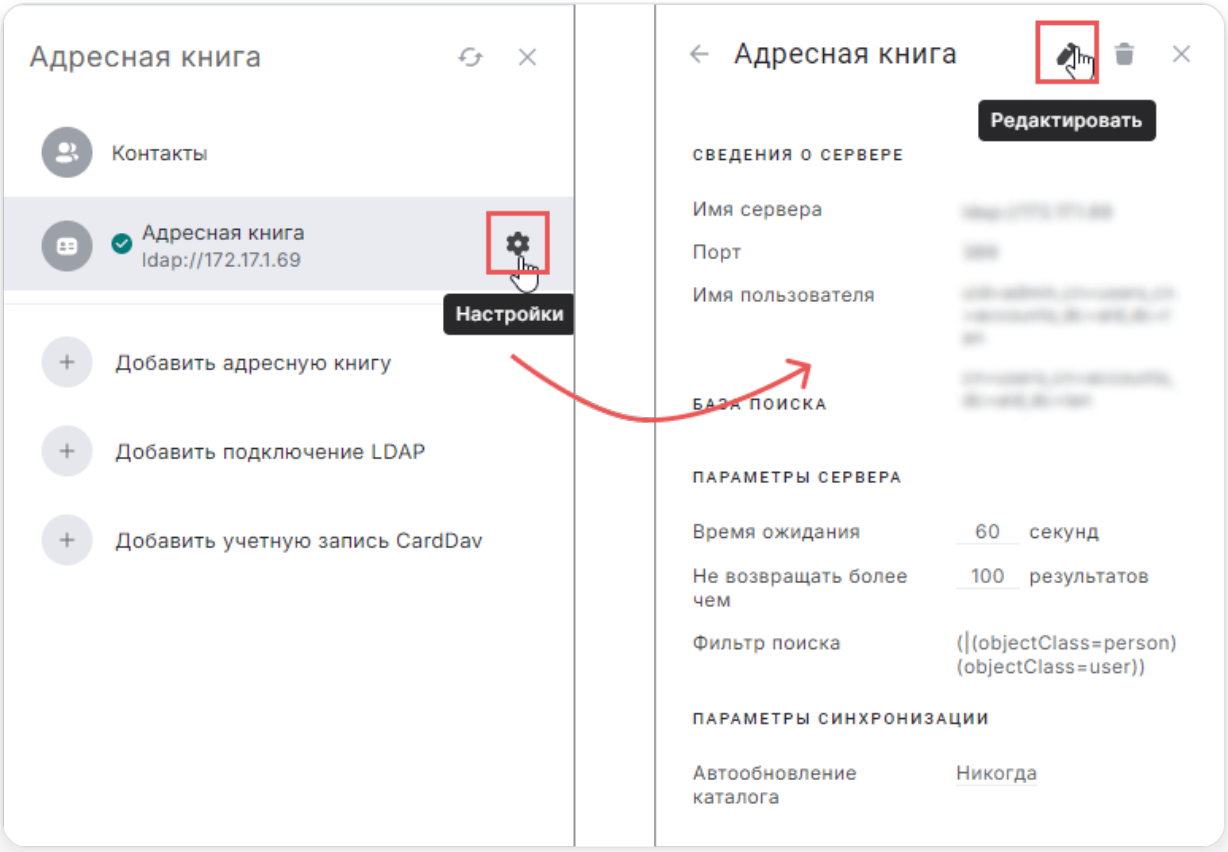
Возможные ошибки при подключении

Ошибки, которые возникают при подключении адресной книги, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

- Не удалось подключиться к LDAP — проверьте правильность заполнения полей **Имя сервера** и **Порт**. Проверьте **Имя пользователя** и **Пароль**.

Как отредактировать настройки адресной книги ALD Pro

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки**.
5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Редактировать**.



7. Откроется форма для редактирования настроек адресной книги.
8. Внесите изменения и нажмите кнопку **Сохранить**.

Как удалить адресную книгу ALD Pro

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Наведите курсор на панель с профилем, настройки которого необходимо отредактировать.
4. Нажмите на кнопку **Настройки**.

5. Откроется окно с предпросмотром настроек.
6. Нажмите на кнопку **Удалить**.
7. Подтвердите действие в модальном окне.

Открыть статью на сайте

Адресная книга CardDAV

В приложении КриптоАРМ поддерживается подключение адресной книги по протоколу CardDAV.

CardDAV — это протокол адресной книги, предназначенный для предоставления пользователям доступа к данным на сервере.

Описание полей формы подключения

Название поля	Описание
Название адресной книги	Произвольное название, которое будет отображаться в приложении
Адрес сервера	Адрес сервера, на котором размещена книга
Имя пользователя	Учетная запись для подключения к серверу
Пароль	Пароль для учетной записи
Интервал обновления	Частота синхронизации адресной книги с почтовым сервисом. По умолчанию «Никогда»
Порядок синхронизации	По умолчанию выстaлено значение «В обе стороны»
Сохранять новые контакты в учетную запись CardDAV	По умолчанию настройка неактивна

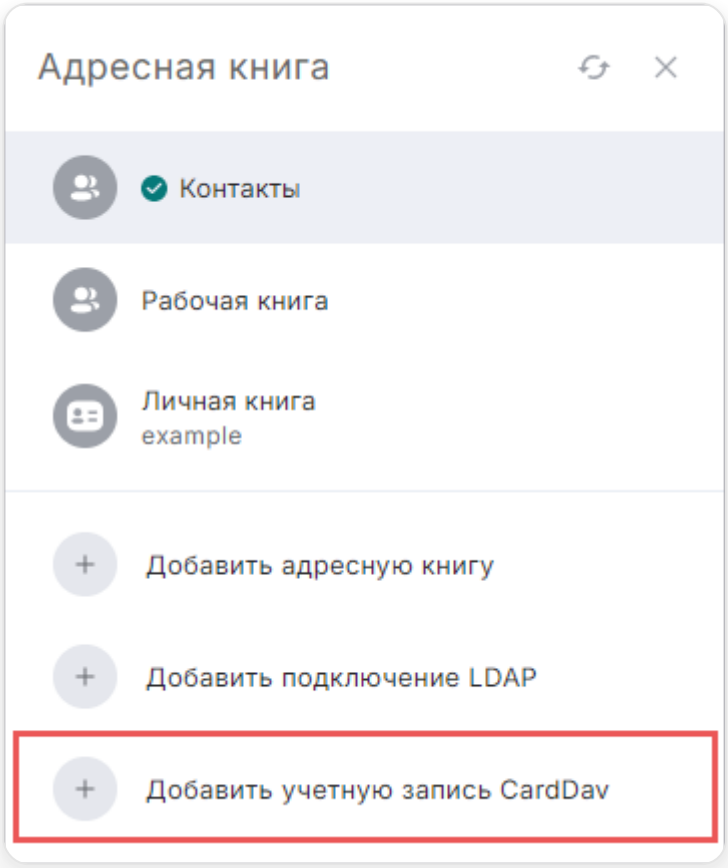
Как добавить адресную книгу по протоколу CardDAV

Шаг 1. Создание пароля

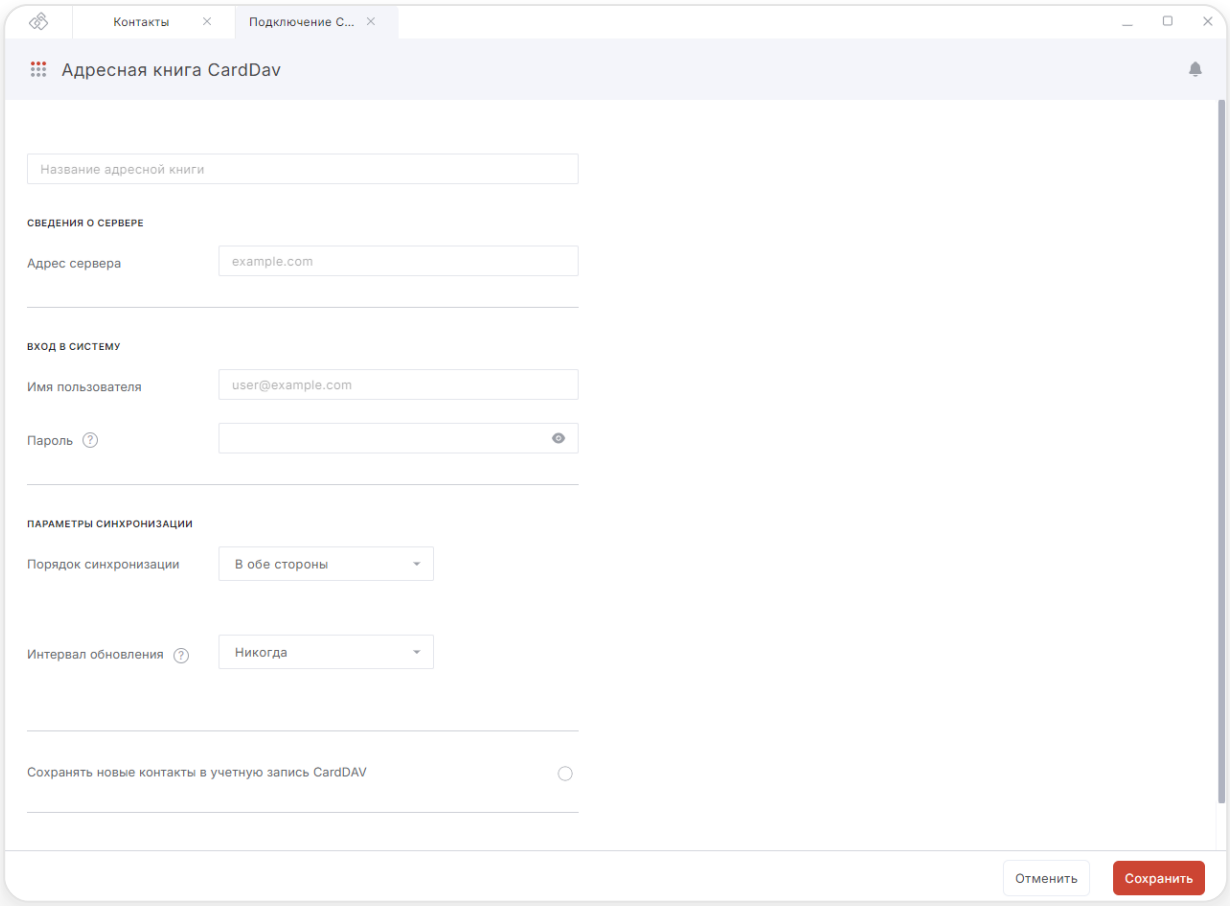
В качестве пароля может выступать обычный пароль или специальный пароль приложения, который необходимо создать в настройках сервиса, на котором размещена адресная книга.

Шаг 2. Создание подключения в КриптоАРМ

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Выберите **Добавить учётную запись CardDAV**.



4. Откроется форма добавления адресной книги.



5. Укажите настройки подключения.

6. Нажмите **Сохранить**.

После подключения в списке адресных книг появится новая книга.

Чтобы просмотреть контакты адресной книги, необходимо переключиться на неё. Подробнее в инструкции Переключение между адресными книгами.

Ошибки, которые возникают при подключении адресной книги, выводятся в виде уведомлений в правом верхнем углу. Чтобы просмотреть уведомления, нажмите на кнопку в виде колокольчика. Откроется окно со списком уведомлений. Для просмотра подробного описания ошибки перейдите в Журнал по соответствующей кнопке в окне со списком уведомлений.

Открыть статью на сайте

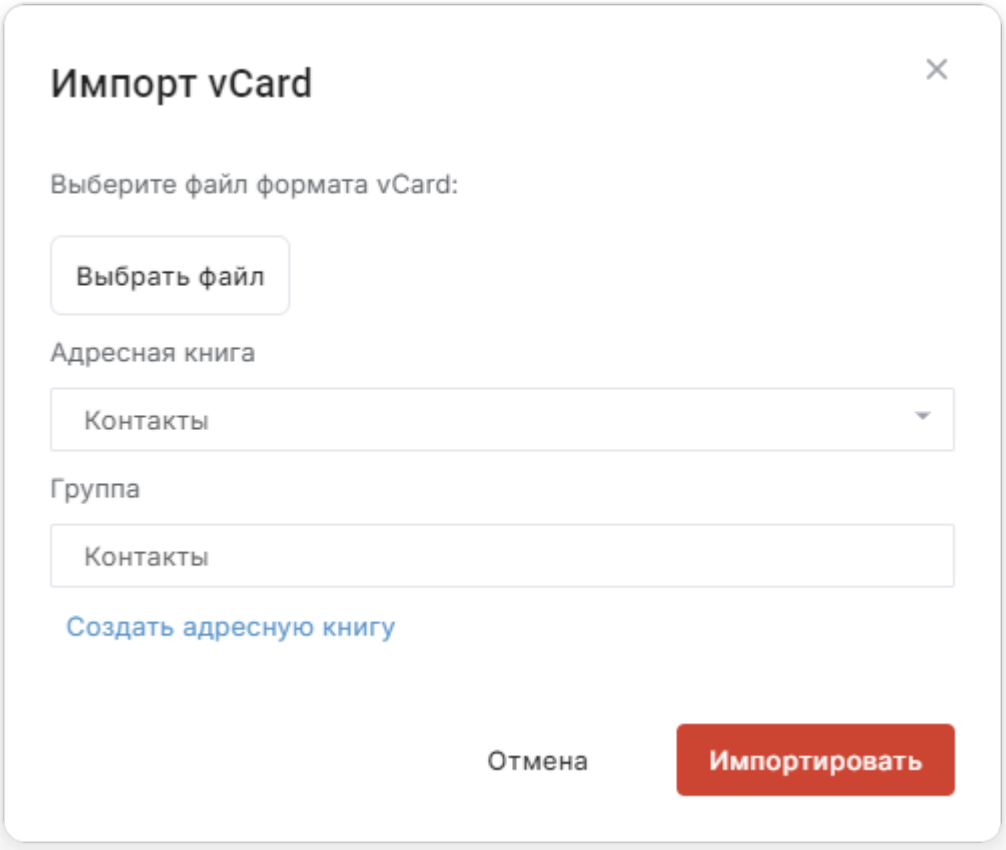
Импорт контактов vCard

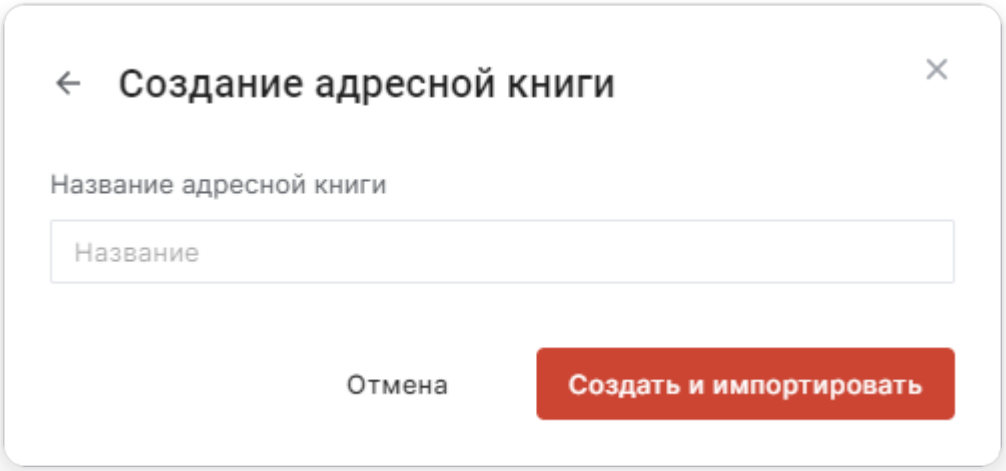
В приложении КриптоАРМ поддерживается формат виртуальной карточки vCard.

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.

Как импортировать контакты из файла vCard

1. Откройте раздел **Контакты**.
2. В левом боковом меню нажмите **Новый контакт** → **Импортировать vCard**.
3. Откроется окно **Импорт vCard**.
    - Нажмите **Выбрать файл**. Откроется окно 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.





4. Нажмите **Импортировать**.

Будет запущен процесс импорта. Дождитесь окончания операции.

После окончания операции будет выведено уведомление с количеством импортированных контактов.

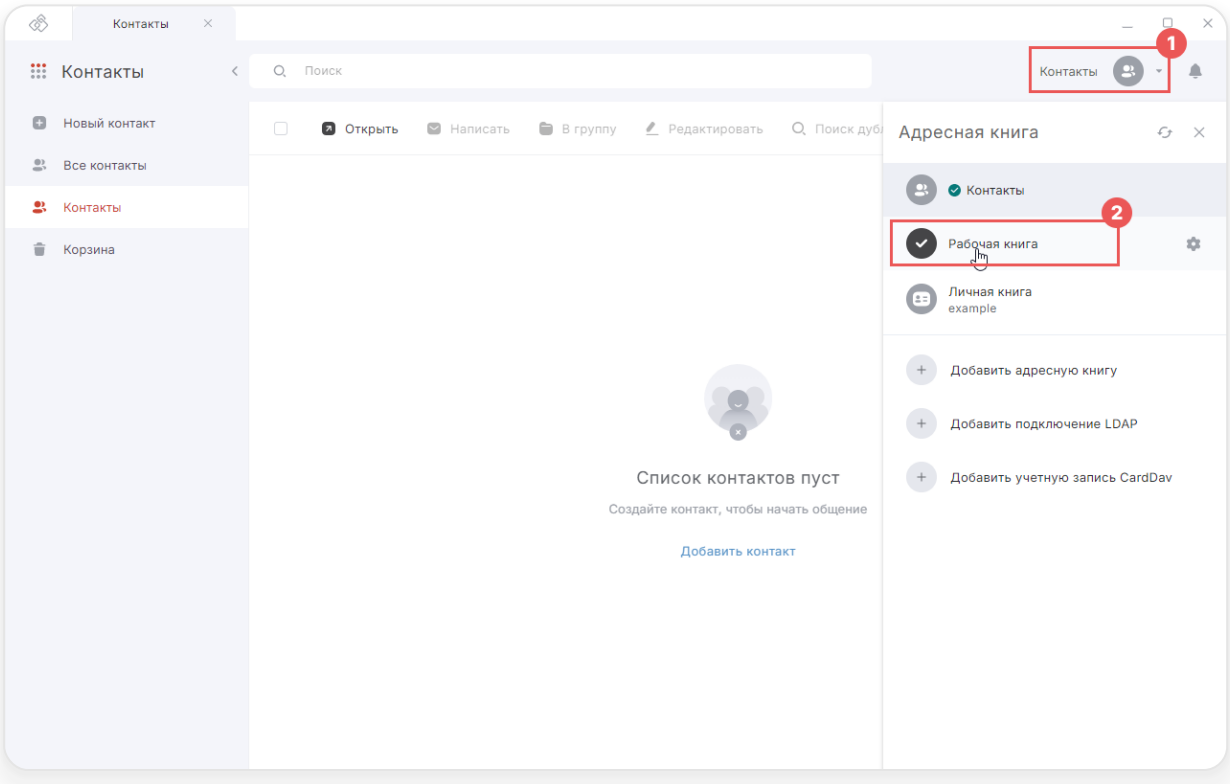
Открыть статью на сайте

Переключение между адресными книгами

В разделе **Контакты** отображаются контакты активной адресной книги.

Чтобы переключиться на другую книгу:

1. Перейдите в раздел **Контакты**.
2. Откройте окно со списком адресных книг. Для этого нажмите на название активной адресной книги в верхнем правом углу окна.
3. Нажмите на панель с книгой, которую хотите просмотреть.



Инструкции по теме

1. Как добавить адресную книгу LDAP.
2. Как добавить локальный контакт.
3. Как посмотреть информацию о контакте.

Открыть статью на сайте

Работа с уведомлениями

Уведомления

Все ошибки при работе с приложением отображаются в виде уведомлений.

Всплывающее уведомление отображается в верхнем правому углу экрана.

Текст уведомления показывается в течение 5 секунд. Вы можете закрыть уведомление раньше, нажав на кнопку **Закрыть**.

При клике на всплывающее уведомление открывается правая боковая панель с уведомлениями.

Также правая боковая панель открывается при нажатии на иконку, где цифрой обозначено количество новых уведомлений на вкладке. 

Уведомления в правой боковой панели разделены на два вида: события текущей вкладки и **Другие** события, которые возникли в приложении, но открытых вкладок для отображения этих уведомлений нет.

Новые уведомления выделяются жирным шрифтом.

Вы можете очистить все уведомления вкладки, нажав на иконку  или закрыть вкладку.

Вы можете просмотреть подробное описание ошибки, нажав на кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Инструкции по теме

1. Как работать с журналом событий.

Открыть статью на сайте

Работа с журналом событий

Общее описание

Информация о событиях, происходящих в рамках приложения, записывается в журнал событий.

Можно перейти в журнал, нажав в левой верхней панели на кнопку **События — Перейти в журнал**.

При возникновении уведомления нажать кнопку **Перейти в журнал** в правой боковой панели списка уведомлений. 

События в журнале разделяются по уровням логирования:

- **Информация** включает в себя все сообщения, информирующие о действиях, например, операция подписи, экспорт сертификата, синхронизация почты.
- **Ошибка** сообщает об ошибках в работе приложения.

Можно обновить события в журнале, нажав кнопку **Обновить**.

Просмотр подробной информации события

Для просмотра подробной информации о событии выделите запись в списке журнала и нажмите иконку просмотра.

В правой боковой панели отображается подробная информация.

Можно скопировать ее для отправки в техническую поддержку, нажав на кнопку **Скопировать**. 

Сохранение выделенных событий в файл

Вы можете сохранить выбранные в списке события в файл. Для этого:

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

Выделенные события сохраняются в созданный файл .log.

Отправка выделенных событий вложением в письме

Можно отправить информацию из журнала событий письмом из программы.

Для этого выделите с помощью флагов события и нажмите на кнопку **Отправить**.

Открывается вкладка нового сообщения с прикрепленным файлом журнала в формате .log.

Печать событий

Чтбы распечатать подробную информацию о выбранных в списке событий, выполните следующие действия:

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

Параметры журнала

В программе можно настроить размер журнала и уровни логирования. Для этого:

1. На панели действий нажмите на кнопку **Параметры журнала**.
2. В разделе общих настроек на вкладке **Параметры журнала событий** задайте размер журнала и уровень логирования. Общие параметры, такие как имя, расположение, даты создания и изменения, недоступны для редактирования и являются информационными. Максимальный размер журнала — 5 МБ.
3. Нажмите на кнопку **Сохранить** для применения изменений.

При достижении максимального размера файла создается новый журнал без перезаписи старого. Старый журнал становится архивным.

Вы можете в параметрах журнала перейти к расположению файла событий, нажав на ссылку поля **Расположен**.

Загрузка архивного журнала

Можно посмотреть события из архивного журнала. Для этого:

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

Архивная копия открывается в новой вкладке.

Для событий архивного журнала доступны:

- сохранение в файл;
- отправка вложением в письме;
- печать.

Просмотр расположения файла событий

Вы можете перейти к расположению файла событий, нажав в дополнительном меню на кнопку **Показать в папке**.

Сортировка и фильтрация

Список сообщений можно в журнале по любому из столбцов. По умолчанию журнал отсортирован по дате, начиная от последнего события.

Для фильтрации журнала используется строка поиска.

Вы можете воспользоваться быстрым поиском по символьному совпадению, тогда в журнале останутся только записи, удовлетворяющие запросу.

Для более детальной фильтрации вы можете задать параметры. Для этого в строке поиска нажмите на кнопку **Открыть фильтр**.

Можно задать следующие **параметры:**

- **Дата** — диапазон дат;
- **Приложение** — раздел, в котором возникло событие;
- **Уровень логирования**;
- **Содержит текст** — ключевые слова в сообщении.

Фильтр применяется после нажатия на кнопку **Поиск** в параметрах.

Отменить примененный фильтр вы можете, нажав в строке поиска иконку .

Открыть статью на сайте

Общее описание

КриптоАРМ поддерживает API с двумя возможными точками вызова локальное приложение на рабочем месте и web-приложение (сервис).

При вызове операции через API КриптоАРМ будет запущен 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:

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
`mail`	действия с электронными письмами

Сценарий выполнения команд (для взаимодействия с web-приложениями)

1. Пользователь заходит на портал (web-приложение).
2. Выбирает объекты (например список документов) и действие (например подпись).
3. Портал генерирует и отображает (или сразу переходит) ссылку с протоколом **cryptoarm://**
4. Если КриптоАРМ не запущен, то запускается. Затем обращается к порталу за JSON с набором параметров, нужных для выполнения конкретной операции. JSON генерируется на сервере, где располагается web-приложение.
5. Полученный JSON обрабатывается и в зависимости от команды выполняются нужные дополнительные запросы к web-приложению.
6. Пользователь подтверждает саму запрошенную операцию (остальной функционал приложения блокируется).
7. Результаты отправляются на сервер.

Сценарий выполнения команд (для взаимодействия с локальным приложением)

1. Пользователь открывает стороннее приложение, в котором есть поддержка КриптоАРМ API.
2. Выбирает объекты (например список документов) и действие (например подпись).
3. Приложение генерирует объект (JSON) и передает на исполнение параметром в КриптоАРМ.
4. Если КриптоАРМ не запущен, то запускается. Затем обращается к порталу за JSON с набором параметров, нужных для выполнения конкретной операции. JSON генерируется на сервере, где располагается web-приложение.
5. Полученный JSON обрабатывается.
6. Пользователь подтверждает саму запрошенную операцию (остальной функционал приложения блокируется).
7. Результаты сохраняются в локальную папку, переданную в параметрах операции.

Формат ссылки для web КриптоАРМ API

```
cryptoarm://<command>/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `?id=<id>` - обязательный параметр. Идентификатор транзакции.

Формат ссылки для локального варианта КриптоАРМ API

Вариант 1:

```
cryptoarm://<command>/<URI>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URI>` - путь к файлу JSON с параметрами, нужными для выполнения команды

Вариант 2:

```
cryptoarm://<command>/<JSON>
```

- `cryptoarm://` - зарегистрированный протокол

- `<command>` - выполняемая команда
- `<JSON>` - JSON с параметрами, нужными для выполнения команды

Открыть статью на сайте

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

Не используются.

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

Ключ	Тип	Описание
data	string/Object	Необязательное поле. Может содержать дополнительные сведения об ошибке.

HTTP-коды

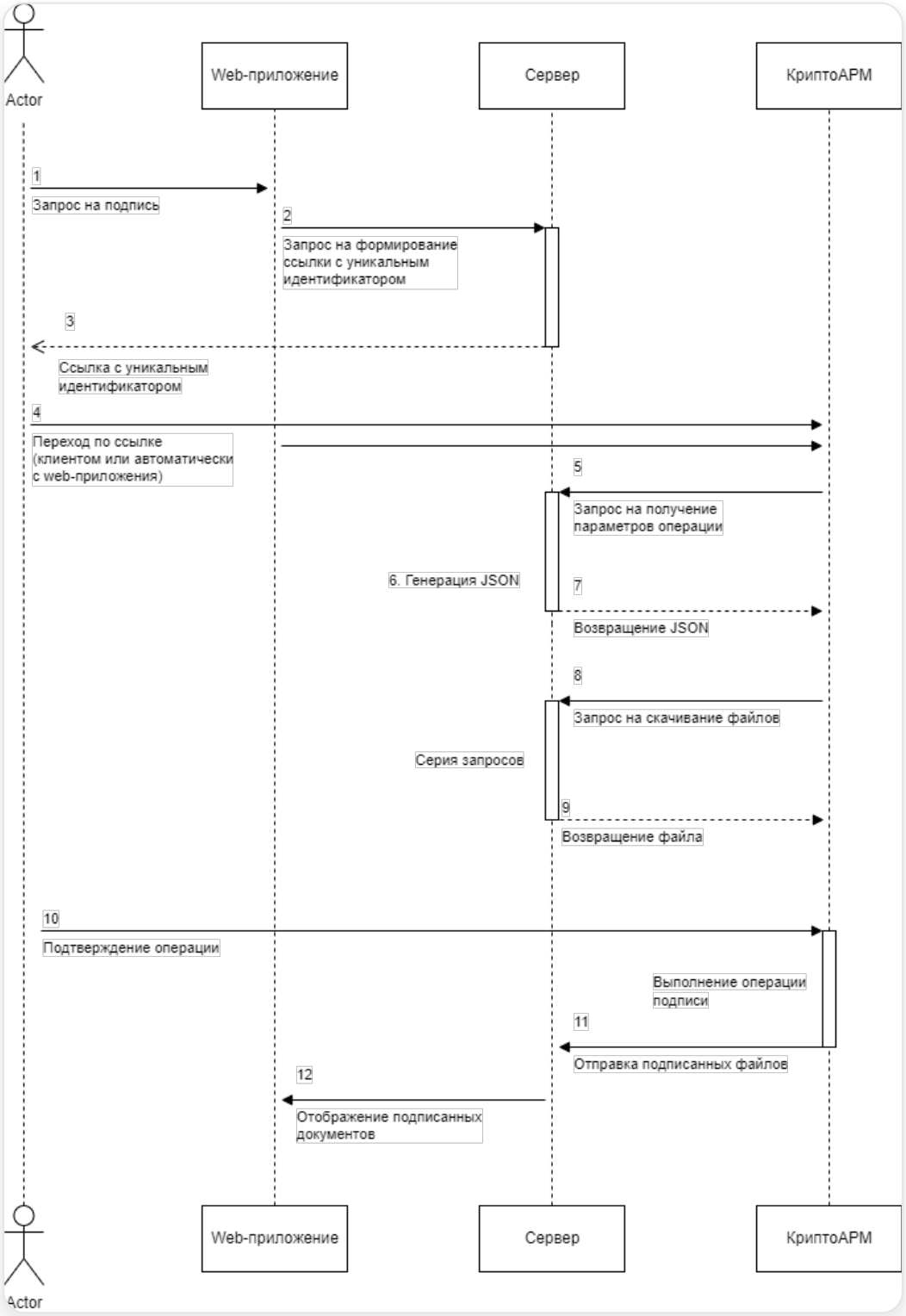
Код	Ошибка	Описание
200	OK	И для ответов, и для ошибок
204	No Response	Для пустых запросов (нотификация)
405	Method Not Allowed	Метод не доступен
415	Unsupported Media Type	Если `Content-Type` не application/json

Открыть статью на сайте

Описание

Команда `signAndEncrypt` (подпись и шифрование) используется для запроса на подпись документа или пакета документов. Может использоваться в качестве аутентификатора.

> **Внимание**
>
> Выполнение операции требует действующей лицензии на КриптоАРМ.


Actor
Web-приложение
Сервер
КриптоАРМ
1
Запрос на подпись
2
Запрос на формирование ссылки с уникальным идентификатором
3
Ссылка с уникальным идентификатором
4
Переход по ссылке (клиентом или автоматически с web-приложения)
5
Запрос на получение параметров операции
6. Генерация JSON
7
Возвращение JSON
8
Запрос на скачивание файлов
Серия запросов
9
Возвращение файла
10
Подтверждение операции
Выполнение операции подписи
11
Отправка подписанных файлов
12
Отображение подписанных документов
Actor
Web-приложение
Сервер
КриптоАРМ

Открыть статью на сайте

Формат ссылки

Для выполнения команды `signAndEncrypt` должна быть сформирована ссылка вида:

```
cryptoarm://<command>/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `<command>` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `?id=<id>` - обязательный параметр. Идентификатор транзакции.

Пример:

```
cryptoarm://signAndEncrypt/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Открыть статью на сайте

Общее

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.

Открыть статью на сайте

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. Подробнее в разделе Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ISignAndEncryptParameters`	Объект со сведениями о параметрах операции подписи

Ключ	Значение	Описание
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. Подробнее в разделе Формат ссылки
appName?	string	Необязательный параметр. Используется только для локального API. Если значение передано, то КриптоАРМ отобразит это название в окне подтверждения операции как название стороннего приложения.
apiKey?	string	Необязательный параметр. Используется только для локального API. Если значение передано, то КриптоАРМ отобразит это значение в окне подтверждения операции как проверочный код.

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": {
        "operation": [
            "SIGN",
            "ARCHIVE",
            "ENCRYPT"
        ],
        "props": {
            "headerText": "Подпись документов cryptoarm.ru",
            "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": ""
                }
            ],
            "extra": {
                "token": "9c7101f7-9c47-4481-b4da-a6a497abde08",
                "signType": "1",
                "signStandart": "1"
            },
            "uploader": "http://localhost:8080/upload"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Открыть статью на сайте

Отправка результата прямых операций

После того, как пользователь выберет нужные сертификаты КриптоАРМ выполняет операцию. Полученные файлы отправляется POST-запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат 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

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.outDirectResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "directResults": [
          {
            "id": 2
        "out": "MIIWgQYJKoZIhvcNAQcCoIIWcjCCFm4CA…cN/aHmA="
          }
        ]
    }
}
```

Открыть статью на сайте

Отправка результата обратных операций

Результаты отправляется POST-запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.outReverseResults`	Используемый метод. Всегда `signAndEncrypt.outReverseResults`.
params	Объект типа `IReverseResults`	Сведения о результатах обратной операции

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.outReverseResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "reverseResults": [
          {
            "out": "MIIWgQYJKoZIhvcNAQcCoIIWcjCCFm4CA…cN/aHmA="
          }
        ]
    }
}
```

Открыть статью на сайте

Отправка результата проверки подписи

Результаты проверки подписи отправляется POST запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`signAndEncrypt.verifySignResults`	Используемый метод. Всегда `signAndEncrypt.verifySignResults`.
params	Объект типа `IVerifySignResults`	Сведения о проверке подписи

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "signAndEncrypt.verifySignResults",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "verifyResults": [
          {
            "id": 2,
            "status": false,
            "signers": [
              {
                "hash": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV",
                "issuerFriendlyName": "Минкомсвязь России",
                "issuerName": "Минкомсвязь России",
                "subjectFriendlyName ": "Минкомсвязь России",
                "subjectName": "Минкомсвязь России",
                "status": true
              }
             ]
          }
        ]
    }
}
```

Открыть статью на сайте

Интерфейс ISignAndEncryptParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string[]	Тип операции. Доступные значения типов (комбинировать различные типы нельзя): `ISignAndEncryptOperationDirect`, `ISignAndEncryptOperationReverse`, `ISignAndEncryptOperationVerify`
props	`ISignAndEncryptOperationProps`	Параметры операции

Открыть статью на сайте

Тип ISignAndEncryptOperationDirect

Возможные прямые операции.

Значение	Описание
SIGN	Подпись
ARCHIVE	Архивирование
ENCRYPT	Шифрование

Открыть статью на сайте

Тип ISignAndEncryptOperationReverse

Возможные обратные операции.

Значение	Описание
UNSIGN	Снятие подписи
DECRYPT	Расшифрование
UNZIP	Разархивирование

Открыть статью на сайте

Тип ISignAndEncryptOperationVerify

Проверка подписи.

Значение	Описание
VERIFYSIGN	Проверка подписи

Открыть статью на сайте

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://
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`. Перед отправкой результатов операции на сервер, они будут упакованы в архив.
extra	Объект типа `IExtra`	Настройки операции
localResultParams	Объект типа `ILocalResultParams`	Необязательное свойство. Используется только для локального API. Указывает пути для сохранения результатов.

Открыть статью на сайте

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.

Открыть статью на сайте

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	Необязательный параметр. Возможные значения: 0 - присоединенная подпись, 1 - отсоединённая подпись.
signStandart?	number	Необязательный параметр. Стандарт подписи. Возможные значения: 0 - CMS, 1 - CAdES-X Long Type 1, 2 - CAdES-T, 3 - CAdES-A.
signEncoding?	number	Необязательный параметр. Кодировка. Возможные значения: 0 – BASE-64, 1 – DER.
timestampOnSign?	string	Необязательный параметр. Штамп времени на подпись. Возможные значения: True - будет добавлен штамп времени, False – не будет добавлен штамп времени.
timestampOnData?	string	Необязательный параметр. Штамп времени на подписываема данные. Возможные значения: True - будет добавлен штамп времени, False – не будет добавлен штамп времени.
encryptEncoding?	number	Необязательный параметр. Кодировка. Возможные значения: 0 – BASE-64, 1 – DER.
encryptAlgorithm?	number	Необязательный параметр. Алгоритм шифрования. Возможные значения: 0 – ГОСТ 28147-89, 1 – ГОСТ 34.12-2015 Магма, 2 – ГОСТ 34.12-2015 Кузнечик.
token?	string	

Свойство	Тип	Описание
		Необязательный параметр. Токен, который будет использоваться при скачивании файлов с сервиса (параметр запроса).
tspURL?	string	Необязательный параметр. Адрес службы штампов времени.
ocspURL?	string	Необязательный параметр. Адрес службы актуальных статусов.
encryptCertificates?	string[]	Необязательный параметр. Сертификаты шифрования.
signCertificate?	Объект типа: `{«x509»:string}`	Необязательный параметр. Сертификат подписчика или параметры для поиска сертификата подписчика.
signatureExtension?	string	Необязательный параметр. Расширение для подписанного файла.
separateArchivesForSignResults?	boolean	Необязательный параметр. Создавать пакет (архив) для каждого подписываемого файла.
isAddStampToPdf?	boolean	Необязательный параметр. Добавить печатную форму для PDF-файлов.
signStampAppearance?	`ISignStampAppearance`	Необязательный параметр. Параметры штампа PDF.
signStamp?	`IPdfMarkedArea`	Необязательный параметр. Расположение и размер области под штамп.
printReport?	boolean	Необязательный параметр. Создавать отчет о проверке подписи в pdf формате.

Открыть статью на сайте

Интерфейс IDirectResults

Объекты данного типа описывают результаты прямой операции.

Свойство	Тип	Описание
id	string	Используется идентификатор, который указан в ссылке на операцию (Формат ссылки).
status	string	Статус выполнения операции. В случае успеха «Completed».
directResults	`IDirectResultOut[]`	Массив результатов прямых операций

Открыть статью на сайте

Интерфейс IDirectResultOut

Объекты данного типа содержат результаты прямой операции для файла.

Свойство	Тип	Описание
id	string	Необязательный параметр. Идентификатор исходного файла. Если включено архивирование, то данный параметр не используется, т.к. выходной файл один для всех исходных.
out	string	Результат операции в BASE-64
signers?	`ISignerStatus[]`	Необязательный параметр. Сведения о подписчиках.
signValid?	boolean	Необязательный параметр. Общий статус подписи. Учитывается статус всех подписей файла.
outSignStamp	boolean	Необязательный параметр. Результат проверки подписи в pdf формате.

Открыть статью на сайте

Интерфейс IReverseResults

Объекты данного типа описывают результаты обратной операции.

Свойство	Тип	Описание
id	string	Используется идентификатор, который указан в ссылке на операцию (Формат ссылки).
reverseResults	`IReverseResultOut[]`	Массив результатов обратных операций

Открыть статью на сайте

Интерфейс IReverseResultOut

Объекты данного типа описывают результаты обратной операции.

Свойство	Тип	Описание
id	string	Необязательный параметр. Идентификатор исходного файла.
out	string	Результат операции в BASE-64

Открыть статью на сайте

Интерфейс IVerifySignResults

Объекты данного типа описывают результаты проверки подписи.

Свойство	Тип	Описание
id	string	Используется идентификатор, который указан в ссылке на операцию (Формат ссылки).
status	string	Статус выполнения операции. В случае успеха « Completed».
verifySignResults	`IVerifySignResult[]`	Массив результатов проверки

Открыть статью на сайте

Интерфейс IVerifySignResult

Объекты данного типа описывают результаты проверки подписи.

Свойство	Тип	Описание
id	string	Идентификатор исходного файла
signValid	boolean	Общий статус проверки подписи
signers	`ISignerStatus[]`	Информация о подписчиках документа

Открыть статью на сайте

Интерфейс ISignerStatus

Объекты данного типа описывают сведения о подписчиках.

Свойство	Тип	Описание
signerCertificate	`ICertificateInfo`	Сведения о сертификате подписчика
isValid	boolean	Статус подписи
signingTime	string	Время подписи

Открыть статью на сайте

Интерфейс ILocalResultParams

Объекты данного типа используется только в параметрах локального API.

Содержат пути для сохранения результатов операций.

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 файл или сохранять в один JSON, один файл.

Открыть статью на сайте

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. Возможные значения: «all» – штамп на всех страницах, «last» – штамп на последней странице, «some» – штамп на некоторых страницах.
pageNumbers?	string	Необязательный параметр. Страница или диапазон страниц. Пример: «3» или «1-7».

Открыть статью на сайте

Интерфейс IMockupSettings

Интерфейс `IMockupSettings` описывает параметры внешнего вида штампа.

Свойство	Тип	Описание
position	string	Положение штампа внутри области. Возможные значения: «fitArea» – вписать, «actualSize» – реальный размер, «fitMockup» – подогнать область под макет.
addBackground	boolean	Определяет, будет ли добавлен фон на область
addBorders	boolean	Определяет, будет ли добавлена граница на область
logotype?	boolean	Необязательный параметр. Использовать или нет логотип для штампа.

Открыть статью на сайте

Интерфейс IRequisitesSettings

Интерфейс `IRequisitesSettings` описывает содержимое (реквизиты) штампа подписи.

Свойство	Тип	Описание
position	string	Реквизиты в штампе. Возможные значения: «default» – штамп без дополнительных областей под реквизиты, «left» – штамп с дополнительными реквизитами слева, «right» – штамп с дополнительными реквизитами справа, «leftAndRight» – штамп с дополнительными реквизитами слева и справа.
centralDisplayType	string	Внешний вид штампа. Определяет доступность настроек дополнительных реквизитов. Возможные значения: «byGost» – внешний вид по ГОСТ, «arbitrary» – произвольно.
central	`IPdfCertRequisite[]`	Массив значений реквизитов, для добавления в центральную часть штампа
left	`IPdfCertRequisite[]`	Массив значений реквизитов, для добавления в левую часть штампа
right	`IPdfCertRequisite[]`	Массив значений реквизитов, для добавления в правую часть штампа

Открыть статью на сайте

Интерфейс IPdfCertRequisite

Интерфейс `IPdfCertRequisite` описывает свойства для реквизита штампа.

Свойство	Тип	Описание
title	string	Заголовок
dataKey?	string	Необязательный параметр. Указывает название поля сертификата, значение которого будет использовано. Если в сертификате нет указанного поля, то значение будет «Не указано».
isEditable	boolean	Указывает, доступно ли редактирование поля пользователем. Если false, то значение должно быть передано в поле editedValue или взято из сертификата по значению dataKey.
editedValue?	string	Необязательный параметр. Значение реквизита, которое будет использовано, если не указано свойство dataKey.
editedValueCharLimit?	number	Необязательный параметр. Определяет максимальную длину строки.

Открыть статью на сайте

Интерфейс IPdfMarkedArea

Интерфейс `IPdfMarkedArea` описывает параметры для расположения области штампа PDF (координаты и размеры).

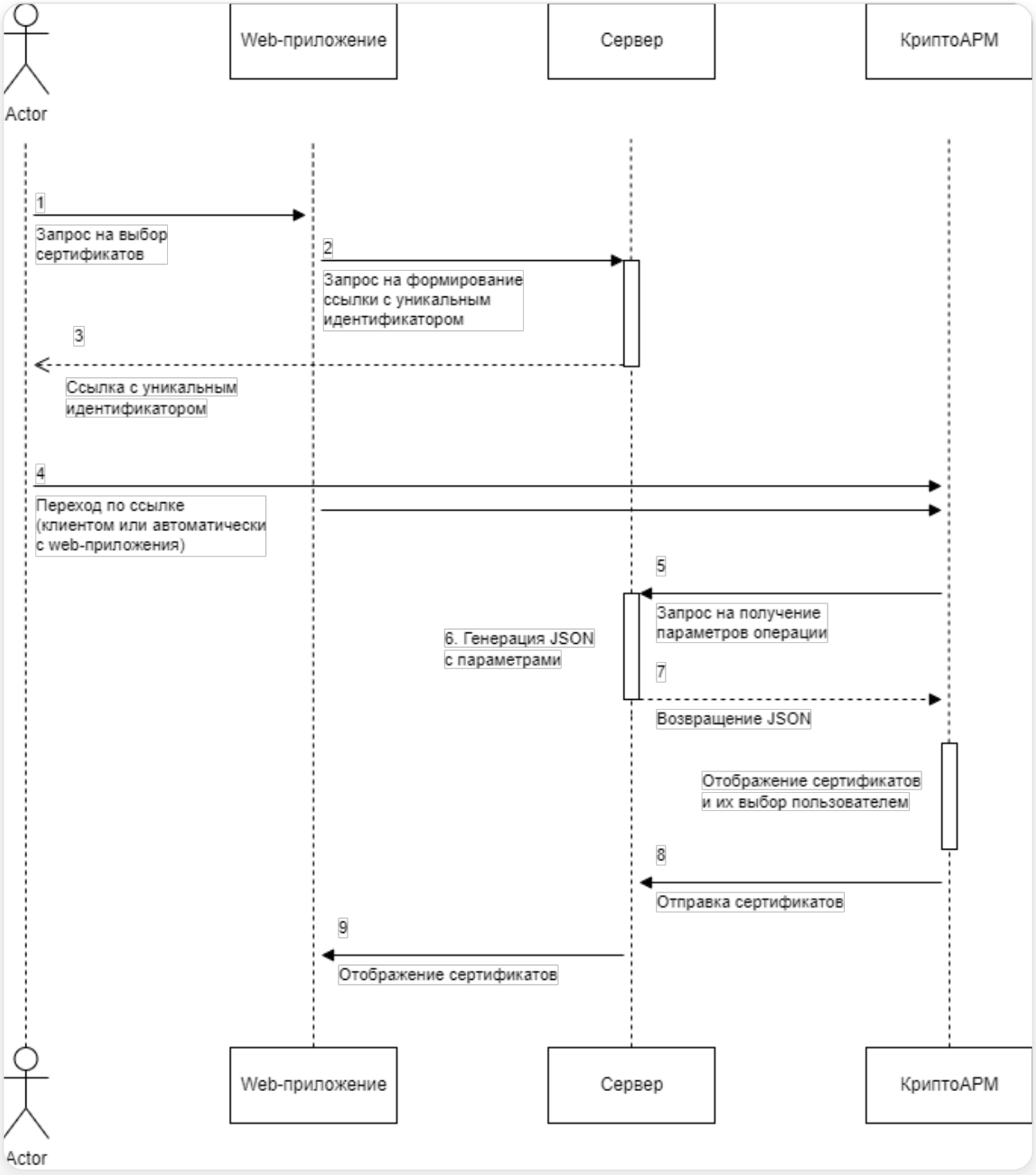
Свойство	Тип	Описание
height	number	Высота области под штамп
width	number	Ширина области под штамп
horizontalPadding	number	Отступ от левого края документа
verticalPadding	number	Отступ от правого края документа

Открыть статью на сайте

Описание

Команда `certificates` используется для: экспорта сертификата или списка сертификатов, а импорта сертификата в локальное хранилище, просмотра информации о сертификате.

Схема взаимодействия (экспорт сертификатов):



Открыть статью на сайте

Формат ссылки

Для выполнения команды `certificates` должна быть сформирована ссылка вида:

```
cryptoarm://certificates/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `certificates` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://certificates/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Открыть статью на сайте

Общее

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.

Открыть статью на сайте

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. Подробнее в разделе Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
     }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`ICertificatesParameters`	Объект со сведениями о параметрах операции

Ключ	Значение	Описание
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. Подробнее в разделе Формат ссылки

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 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": "information",
        "props": {
            "certificateBase64": "MIIFFDCCBMGgAwIBAgIQT...4VVkDWbX/n4="
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Открыть статью на сайте

Отправка сертификата

При экспорте сертификатов результат отправляются на сервер. После того, как пользователь выберет нужный сертификат КриптоАРМ отправляет запрос, содержащий выбранные элементы (base64 без заголовков). Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.base64`	Используемый метод. Всегда `certificates.base64`.
params	`ICertificateBase64Params`	Параметры, содержащие объект сертификата

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.base64",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "certificateBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/n4=",
        "friendlyName": "Минкомсвязь России"
    }
}
```

Открыть статью на сайте

Отправка списка сертификатов

При экспорте сертификатов результат отправляются на сервер. Если параметры `ICertRequestParameters` содержат поле «multy» со значением «true», то пользователю в КриптоАРМ будет разрешён множественный выбор сертификатов. После того, как пользователь выберет нужные сертификаты и нажмет кнопку «Готово», КриптоАРМ отправляет запрос, содержащий выбранные элементы (base64 без заголовков). Используются нотификации (уведомления), для которых не используется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.base64`	Используемый метод. Всегда `certificates.base64`.
params	`ICertificateBase64Params`	Параметры, содержащие объект сертификата

```
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=",
                "friendlyName": "Минкомсвязь России"
            },
            {
                "certificateBase64": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV...4VVkDWbX/
n4=",
                "friendlyName": "Головной удостоверяющий центр"
            }
        ]
    }
}
```

Открыть статью на сайте

Отправка сведений о сертификате

После того, как пользователь выберет нужный сертификат КриптАРМ отправляет запрос, содержащий выбранные элементы (base64 без заголовков). Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certificates.information`	Используемый метод. Всегда `certificates.information`.
params	Объект типа `ICertificateInfo`	Сведения о сертификате

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.information",
    "params": {
        "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
        "hash": "MIIFFDCCBMGgAwIBAgIQTm1HiybyfWV",
        "issuerFriendlyName": "Минкомсвязь России",
        "issuerName": "Минкомсвязь России",
        "subjectFriendlyName ": "Минкомсвязь России",
        "subjectName": "Минкомсвязь России",
        "status": true
    }
}
```

Открыть статью на сайте

Интерфейс ICertificatesParameters

Объекты данного типа описывают параметры команды запроса на получение сертификат.

Свойство	Тип	Описание
operation	string	Тип операции импорт, экспорт, информация. Доступные значения: “import”, “export”, “information”
props	`ICertificatesOperationProps`	Параметры операции

Открыть статью на сайте

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 имен хранилищ. Если не задан, то используется значение MY (личные сертификаты).
multy?	boolean	Необязательный параметр. Разрешен ли множественный выбор. По умолчанию false.
certificateBase64?	string	Необязательный параметр. Сертификат в формате X.509 закодированный в Base64.

Открыть статью на сайте

Интерфейс ICertificateBase64Params

Объекты данного типа описывают параметры запроса для метода `certificates.base64`.

Свойство	Тип	Описание
id	string	Идентификатор транзакции
certificateBase64	string	Сертификат в формате X.509 закодированный в Base64
friendlyName	string	Дружественное имя сертификата

Открыть статью на сайте

Интерфейс ICertificateInfo

Объекты данного типа описывают объекты, содержащие свойства сертификата.

Свойство	Тип	Описание
hash	string	SHA1 отпечаток
issuerFriendlyName	string	Дружественное имя издателя (CN)
issuerName	string	Имя издателя
notAfter	string	Дата окончания действия сертификата
notBefore	string	Дата начала действия сертификата
rootCAMinComSvyaz	boolean	Флаг, обозначающий 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.

Открыть статью на сайте

Интерфейс ICertificateIdentityInfos

Объекты данного типа описывают объекты, содержащие параметры сертификата, позволяющие только идентифицировать его.

Свойство	Тип	Описание
id	string	Идентификатор транзакции
hash	string	SHA1 отпечаток
rootCAMinComSvyaz	boolean	Флаг, обозначающий является ли владельцем корневого сертификата цепочки “Минкомсвязь России”
status	boolean	Статус сертификата. Проверяется вся цепочка.
pubKeyAlg	string	OID алгоритма открытого ключа сертификата

Открыть статью на сайте

Интерфейс КриптоАРМ при выборе и отправке сертификатов

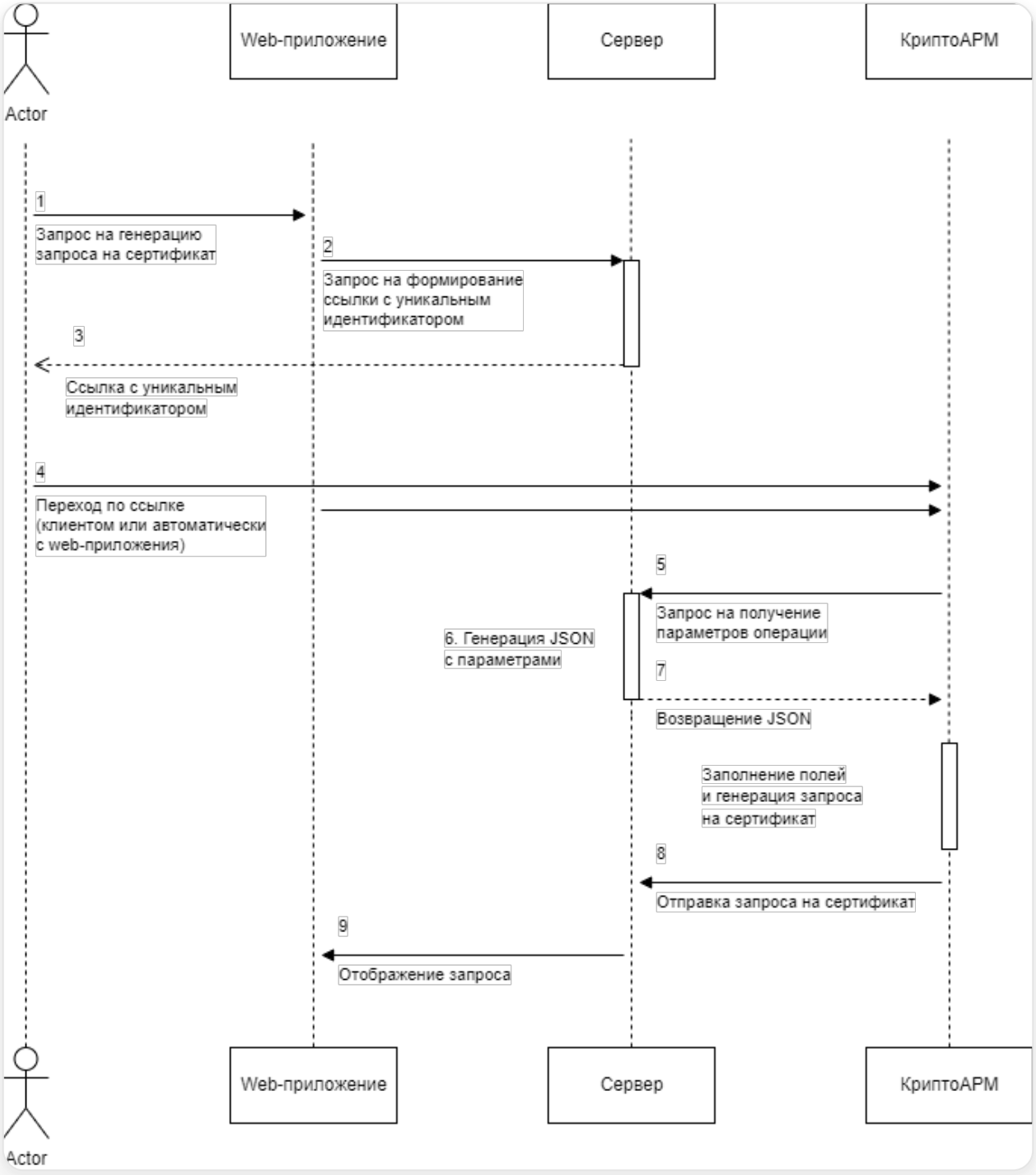
При выполнении команды запроса на сертификаты, не относящийся к процедуре интерфейс блокируется. Пользователю доступны: выбор сертификатов. Доступны две кнопки: «Готово» и «Отмена». После выполнения команды, приложение будет свернуто в системный трей.

Открыть статью на сайте

Описание

Команда `certrequests` используется для: генерации запроса на сертификат по шаблону или экспорт запросов.

Схема взаимодействия (экспорт сертификатов):



Открыть статью на сайте

Формат ссылки

Для выполнения команды `certrequests` должна быть сформирована ссылка вида:

```
cryptoarm://certificates/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `certrequests` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://certrequests/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Открыть статью на сайте

Общее

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.

Открыть статью на сайте

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. Подробнее в разделе Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "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

Ключ	Значение	Описание
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. Подробнее в разделе Формат ссылки

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": {
        "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"
        }
    }
}
```

Открыть статью на сайте

Отправка запроса на сертификат

После генерации запроса, он будет отправлен на сервер. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`certrequests.base64`	Используемый метод. Всегда `certrequests.base64`.
params	`ICertificaterequestBase64Param`	Параметры, содержащие объект сертификата

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"
    }
}
```

Открыть статью на сайте

Интерфейс ICertrequestsParameters

Объекты данного типа описывают параметры команды.

Свойство	Тип	Описание
operation	string	Тип операции: генерация запроса на сертификат. Значение типа: `CertrequestsOperation
props	`ICertrequestsOperationGenerateProps`	Параметры операции

Открыть статью на сайте

Тип CertrequestsOperation

Возможные операции с запросами на сертификат.

Значение	Описание
GENERATE	Генерация запроса на сертификат

Открыть статью на сайте

Интерфейс ICertrequestsOperationGenerateProps

Объекты данного типа описывают дополнительные свойства операции.

Свойство	Тип	Значение	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина: 40 символов.	headerText?
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина: 120 символов.	descriptionText?
templateType	string	JSONTemplate или CertificateTemplate	В качестве шаблона используется JSON типа IJSONTemplate или в качестве шаблона используется сертификат
template	`IJSONTemplate` или `ICertificateTemplate`	Шаблон для генерации запроса на сертификат	

Открыть статью на сайте

Интерфейс ICertificatesParameters

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
Extensions	`IRequestExtension`	Расширения
MarkExportable	boolean	Определяет экспортируемость ключей

Открыть статью на сайте

Интерфейс IRDN

Свойство	Тип	Описание
Oid	string	Описание шаблона
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 массива `SettingsValues`
ProhibitChange	boolean	Флаг указывающий, что поле не может быть изменено
ProhibitEmpty	boolean	Флаг указывающий, что поле должно быть непустым

Открыть статью на сайте

Интерфейс IRequestExtension

Свойство	Тип	Описание
KeyUsage	`IKeyUsage[]`	Описание шаблона
ExtendedKeyUsage	`IExtendedKeyUsage[]`	Наименование OID

Открыть статью на сайте

Интерфейс IKeyUsage

Свойство	Тип	Описание
Name	string	Наименование OID
LocalizedName	string	Локализованное наименование OID
DefaultValue	boolean	Значение по умолчанию
ProhibitChange	boolean	Флаг указывающий, что поле не может быть изменено

Открыть статью на сайте

Интерфейс IExtendedKeyUsage

Свойство	Тип	Описание
Name	string	Наименование OID
LocalizedName	string	Локализованное наименование OID
DefaultValue	boolean	Значение по умолчанию
ProhibitChange	boolean	Флаг указывающий, что поле не может быть изменено

Открыть статью на сайте

Интерфейс ICertificatesParameters

Объекты данного типа используются для генерации запроса на сертификат, где запрос формируется по сертификату.

Свойство	Тип	Описание
certificateBase64	string	Сертификат в формате X.509 закодированный в Base64

Открыть статью на сайте

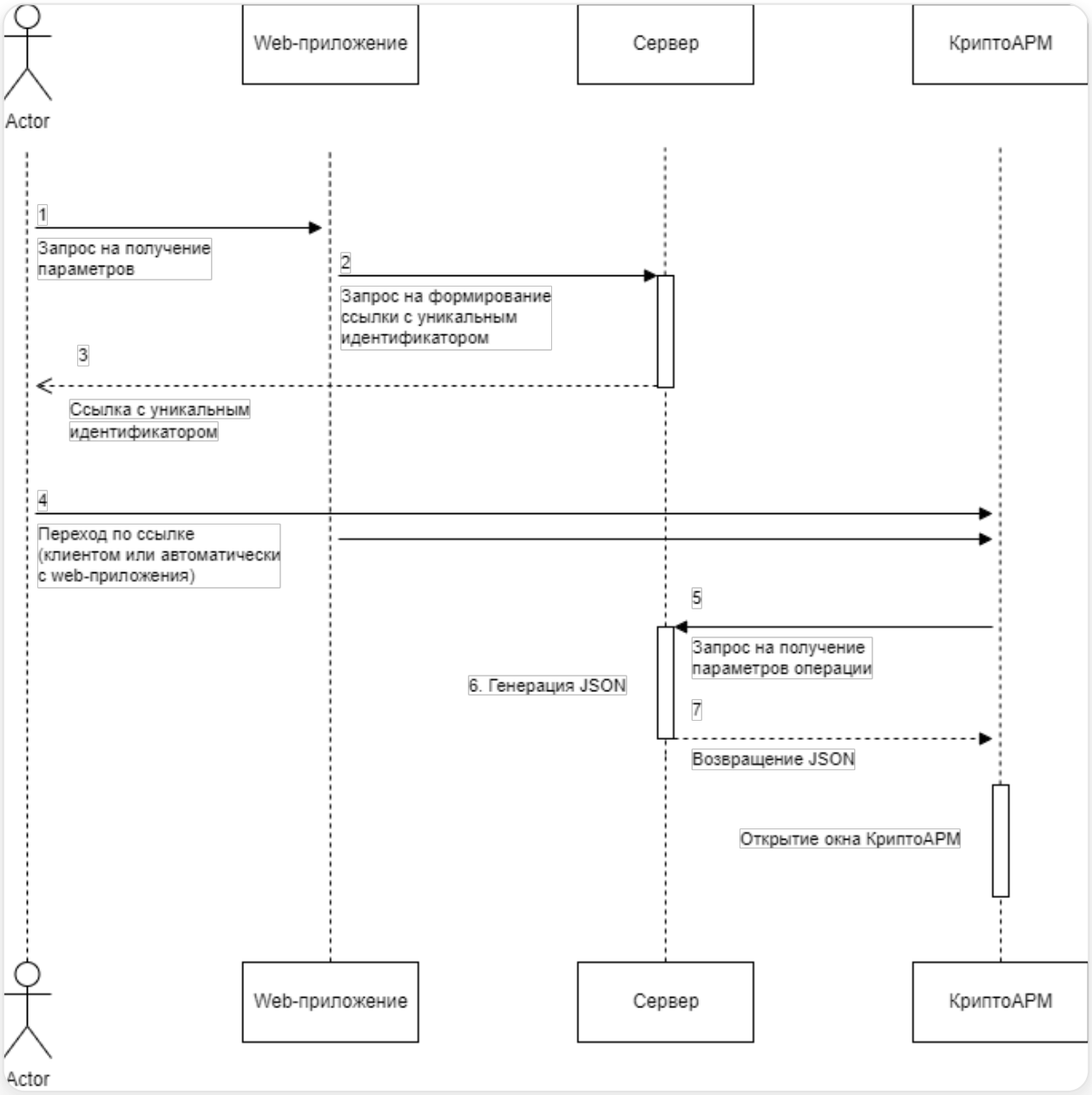
Интерфейс ICertificaterequestBase64Params

Свойство	Тип	Описание
id	string	Идентификатор транзакции
certificaterequestBase64	string	Запрос в формате X.509 закодированный в Base64
friendlyName	string	Дружественное имя субъекта

Открыть статью на сайте

Описание

Команда `diagnostics` используется для диагностики рабочего места пользователя. Схема взаимодействия:ката или списка сертификатов, а импорта сертификата в локальное хранилище, просмотра информации о сертификате.



Открыть статью на сайте

Формат ссылки

Для выполнения команды `diagnostics` должна быть сформирована ссылка вида:

```
cryptoarm://diagnostics/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `diagnostics` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://diagnostics/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Открыть статью на сайте

Общее

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.

Открыть статью на сайте

Получение параметров операции

После получения команды `diagnostics` КриптоАРМ отправляет запрос на получение параметров операции.

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. Подробнее в разделе Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "certificates.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

Ключ	Значение	Описание
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. Подробнее в разделе Формат ссылки

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": {
        "operation": ["CSP_ENABLED", "LICENSES", "VERSIONS"],
        "props": {
            "headerText": "Диагностика cryptoarm.ru",
            "descriptionText":
"Выполняется диагностика рабочего места для работы на портале"
        }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Открыть статью на сайте

Отправка сведений о рабочем месте

Полученные сведения отправляется POST запросом. Используются нотификации (уведомления), для которых не требуется ответ сервера.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`diagnostics.information`	Используемый метод. Всегда `diagnostics.information`.
params	`IDiagnosticsInformation`	Сведения о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
  "jsonrpc": "2.0",
  "method": "diagnostics.information",
  "params": {
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "CSP_ENABLED": true,
    "LICENSES": {
      "csp": {
        "status": true,
      },
      "cryptoarm": {
        "status": true,
        "type": "temporary",
        "expiration": "1591689487056",
      }
    },
    "VERSIONS": {
      "csp": "5.0.11753",
      "cryptoarm": "2.5.2",
    }
  }
}
```

Открыть статью на сайте

Интерфейс IDiagnosticsParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string	Тип операции. Доступные значения типа: `IDiagnosticOperation
props	`IDiagnosticsOperationProps`	Параметры операции

Открыть статью на сайте

Тип IDiagnosticOperation

Возможные операции.

Значение	Описание
SYSTEMINFORMATION	Сведения о системе
CSP_ENABLED	Наличие КриптоПро CSP
CADES_ENABLED	Доступность CADES
VERSIONS	Версии используемых компонентов (КриптоАРМ, КриптоПро)
PROVIDERS	Список криптопровайдеров
LICENSES	Статус лицензий
PERSONALCERTIFICATES	Наличие личных сертификатов

Открыть статью на сайте

Интерфейс IDiagnosticsOperationProps

Интерфейс `IDiagnosticsOperationProps` 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

Интерфейс IDiagnosticsInformation

Объекты данного типа описывают объекты, содержащие сведения о рабочем месте.

Свойство	Тип	Описание
id	string	Идентификатор транзакции
API_VERSION	string	Версия поддерживаемого КриптоАРМ API
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[]`	Сведения о личных сертификатах (только идентификаторы)

Открыть статью на сайте

Интерфейс ISystemInformation

Объекты данного типа содержат сведения о системе пользователя.

Свойство	Тип	Описание
type	string	Тип системы. Возможные значения: 'Linux', 'Darwin' и 'Windows_NT'
arch	string	Архитектура операционной системы. Возможные значения: 'arm', 'arm64', 'ia32', 'mips', 'mipsel', 'ppc', 'ppc64', 's390', 's390x', 'x32', и 'x64'
platform	string	Имя платформы. Возможные значения: 'aix', 'darwin', 'freebsd', 'linux', 'openbsd', 'sunos', и 'win32'
packageType?	string	Необязательный параметр. Тип поддерживаемого пакета (инсталлятора). Возможные значения: ‘msi’, ‘pkg’, ‘rpm’ или ‘deb’

Открыть статью на сайте

Интерфейс IVersions

Объекты данного типа содержат сведения о версиях.

Свойство	Тип	Описание
csp	string	Версия КриптоПро CSP
cryptoarm	string	Версия КриптоАРМ

Открыть статью на сайте

Интерфейс IProviders

Объекты данного типа описывают доступность ГОСТ-провайдеров.

Свойство	Тип	Описание
GOST2012_256	boolean	ГОСТ 2012-256
GOST2012_512	boolean	ГОСТ 2012-512

Открыть статью на сайте

Интерфейс ILicenses

Объекты данного типа описывают статусы лицензии КриптоАРМ и КритпоПро CSP.

Свойство	Тип	Описание
csp	`ILicenseInfo`	Сведения о лицензии на КриптоПро CSP
cryptoarm	`ILicenseInfo`	Сведения о лицензии на КриптоАРМ

Открыть статью на сайте

Интерфейс ILicenseInfo

Объекты данного типа описывают сведения о лицензии компонента.

Свойство	Тип	Описание
status	boolean	Действительна или нет лицензия
type	`LicenseType`	Тип лицензии
expiration?	string	Необязательный параметр. Дата истечения лицензии для трилальных лицензий или подписок (в формате UTC).

Открыть статью на сайте

LicenseType Enum

Данное перечисление описывает возможные типы лицензий.

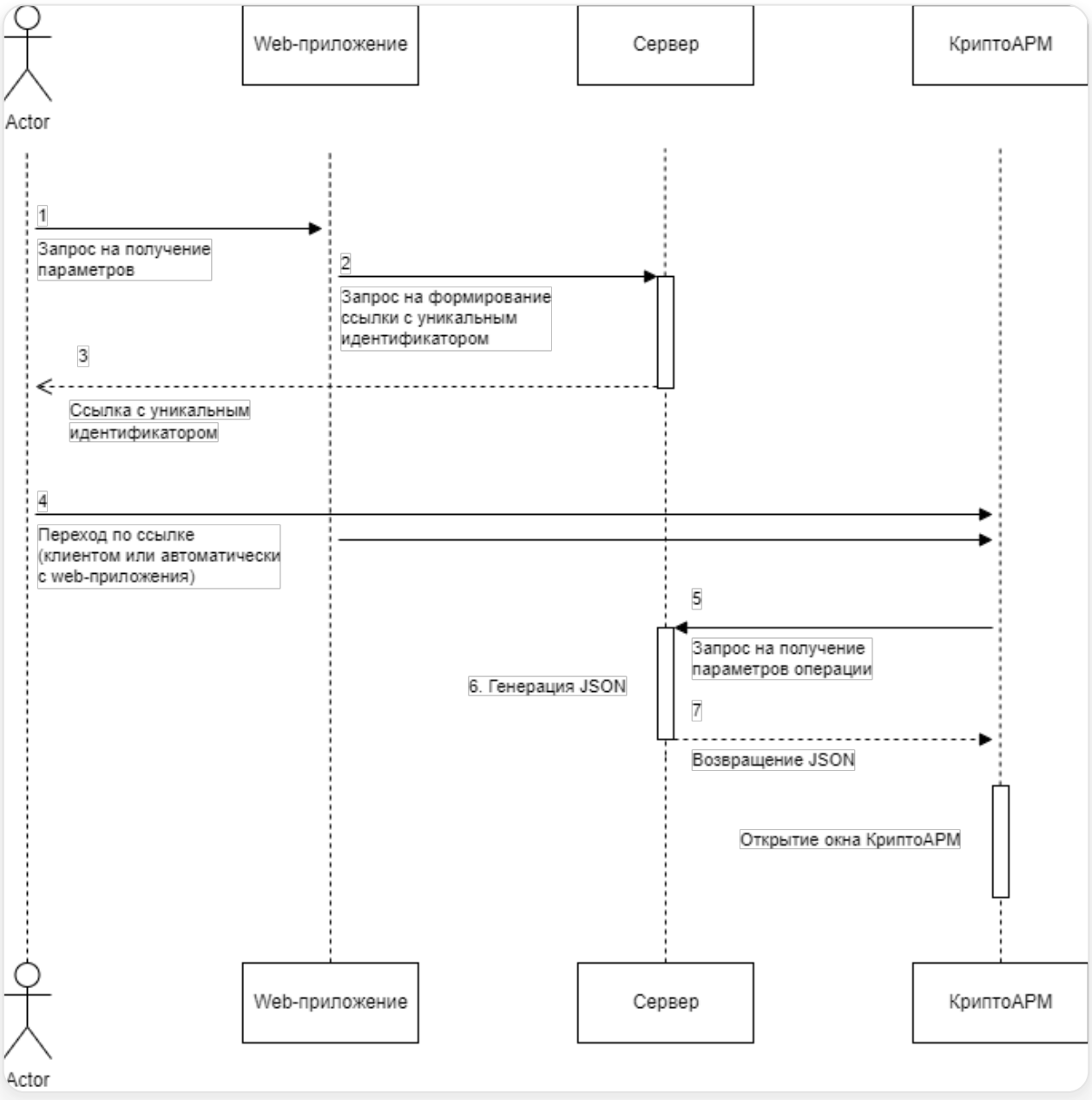
Значение	Описание
Permanent	Постоянная
Subscription	Подписка
Daily	Дневная
Trial	Триальная

Открыть статью на сайте

Описание

Команда `startView` используется для открытия конкретного окна приложения КриптоАРМ.

Схема взаимодействия:



Открыть статью на сайте

Формат ссылки

Для выполнения команды `startView` должна быть сформирована ссылка вида:

```
cryptoarm://startView/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `startView` - выполняемая команда
- `<URL>` - ссылка на получение JSON с параметрами, нужными для выполнения команды
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://startView/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Открыть статью на сайте

Общее

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.

Открыть статью на сайте

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. Подробнее в разделе Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "startView.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IStartViewParameters`	Объект со сведениями о параметрах операции

Ключ	Значение	Описание
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. Подробнее в разделе Формат ссылки

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"
}
```

Открыть статью на сайте

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, “CERTIFICATES_MY” - окно Сертификаты/Личные сертификаты, “CERTIFICATES_ADDRESS_BOOK” - окно Сертификаты/Другие пользователи, “CERTIFICATES_CA” - окно Сертификаты/ Промежуточные, “CERTIFICATES_ROOT” - окно Сертификаты/Корневые, “CONTACTS” - окно Контакты, “KEYS” - окно Сертификаты/ Список контейнеров, “ABOUT” и “DIAGNOSTIC” - окно О программе (Настройки).
props	`IStartViewOperationProps`	Параметры операции

Открыть статью на сайте

Интерфейс IStartViewOperationProps

Интерфейс `IStartViewOperationProps` описывает параметры операции.

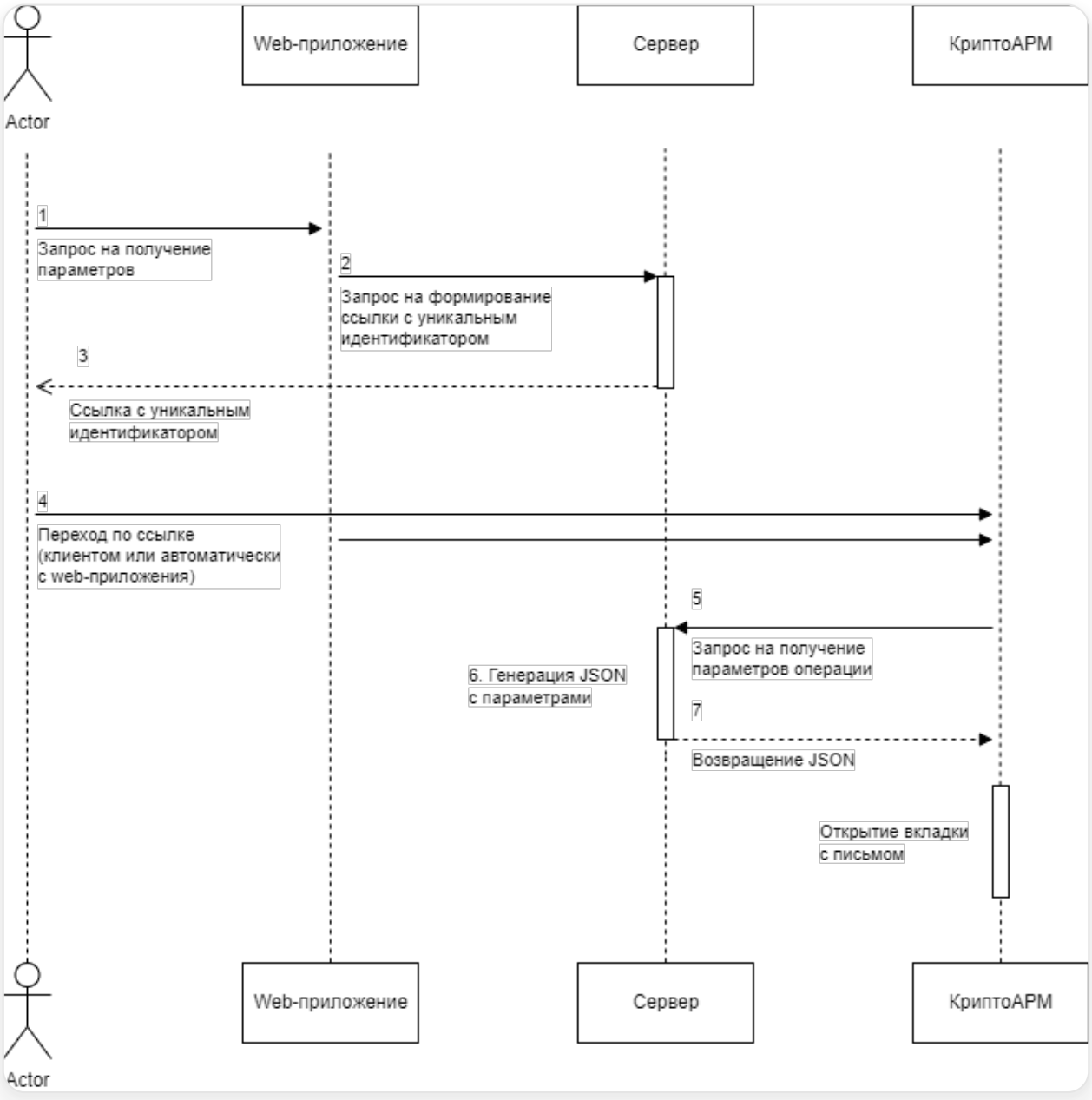
Свойство	Тип	Описание
headerText?	string	Необязательный параметр. Используется для отображения в заголовке окна. Максимальная длина - 40 символов.
descriptionText?	string	Необязательный параметр. Используется для отображения в сведениях об операции. Максимальная длина - 120 символов.

Открыть статью на сайте

Описание

Команда `mail` используется для действий с электронными письмами в КриптоАРМ.

Схема взаимодействия:



Открыть статью на сайте

Формат ссылки

Для выполнения команды `mail` должна быть сформирована ссылка вида:

```
cryptoarm://mail/<URL>/?id=<id>
```

- `cryptoarm://` - зарегистрированный протокол
- `mail` - выполняемая команда
- `<URL>` - ссылка, на которую КриптоАРМ будет слать запросы
- `id` - уникальный идентификатор транзакции

Пример:

```
cryptoarm://mail/https://example.com/json?id=2c48eb32-a0a8-405c-ade9-eed130605cba
```

Открыть статью на сайте

Общее

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.

Открыть статью на сайте

Получение параметров операции

После получения команды `mail` КриптоАРМ отправляет запрос на получение параметров операции.

Формат запроса

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
method	`mail.parameters`	Используемый метод. Всегда `mail.parameters`.
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. Подробнее в разделе Формат ссылки
diagnostic	`IDiagnosticInformaton`	Диагностическая информация о рабочем месте

Пример:

```
Content-Type: application/json
Content-Length: ...
Accept: application/json
{
    "jsonrpc": "2.0",
    "method": "mail.parameters",
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba",
    "diagnostic": {
    }
}
```

Формат ответа

Ключ	Значение	Описание
jsonrpc	«2.0»	Версия JSON-RPC протокола. Всегда «2.0».
result	`IMailParameters`	Объект со сведениями о параметрах операции

Ключ	Значение	Описание
id	Уникальный идентификатор	Используется идентификатор, который указан в ссылке на операцию. Подробнее в разделе Формат ссылки

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": {
        "operation": "SEND",
        "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": ""
                },
                {
                    "name": "file4.pdf",
                    "url": "http://localhost:8080/public/files/file4.pdf",
                    "id": 4,
                    "urlDetached": ""
                }
           ],
           "sign": false,
           "encrypt": false,
           "deliveryReport": false,
           "readReport": false
           }
      }
    },
    "id": "2c48eb32-a0a8-405c-ade9-eed130605cba"
}
```

Открыть статью на сайте

Интерфейс IMailParameters

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
operation	string	Тип операции. Доступные значения: «SEND» – открыть новое сообщение (черновик) с переданными параметрами, «OPEN» – открыть для чтения сообщение eml.
props	`IMailOperationProps`	Параметры операции

Открыть статью на сайте

Интерфейс IMailOperationProps

Объекты данного типа описывают вид операции и её параметры.

Свойство	Тип	Описание
eml?	`IFile`	Необязательный параметр. Параметры для получения eml файла.
mailProps?	`IMailProps`	Необязательный параметр. Свойства для нового сообщения.
extra?	Объект типа `IExtra`	Необязательный параметр. Настройки операции. Для команды `mail` это свойство может содержать token, для скачивания eml с сервера.

Открыть статью на сайте

Интерфейс IMailProps

Объекты данного типа описывают параметры операции 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)
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

Открыть статью на сайте

Часто задаваемые вопросы

О продукте

- Возможности КриптоАРМ
- Какие криптопровайдеры поддерживаются
- Какие типы ключевых носителей поддерживаются
- Какие системные требования нужны
- Как отправить отзыв о КриптоАРМ
- Как узнать какая версия КриптоАРМ установлена
- Как изменить раздел при запуске

Начало работы

- Как скачать и установить КриптоАРМ на Windows
- Как скачать и установить КриптоАРМ на Linux
- Как скачать и установить КриптоАРМ на macOS
- Как скачать и установить КриптоПро CSP на Windows
- Как скачать и установить КриптоПро CSP на Linux
- Как скачать и установить КриптоПро CSP на macOS
- Как установить сертификат из ключевого контейнера
- Как установить сертификат из файла .pfx
- Как установить сертификат из DSS
- Как создать самоподписанный сертификат
- Как получить квалифицированную электронную подпись
- Как установить корневой или промежуточный сертификат
- Как установить сертификат другого пользователя

Лицензирование

- Как узнать статус лицензии КриптоАРМ
- Как узнать статус лицензии КриптоПро CSP
- Как ввести лицензионный ключ КриптоАРМ
- Как ввести лицензионный ключ КриптоПро CSP

Проверка рабочего места

- Как запустить проверку рабочего места
- Как скачать или отправить отчет о системе

Подпись и шифрование

- Как подписать файл
- Как подписать файл со штампом времени
- Как подписать файл усовершенствованной подписью
- Как подписать файл со архивным штампом времени
- Как подписать pdf-файл со штампом
- Как сертифицировать pdf-файл
- Как создать печатную форму со штампом для pdf-файлов
- Как зашифровать файл

Проверка и расшифрование

- Как расшифровать файл
- Как проверить подпись файла
- Как снять подпись с файла

МЧД

- Как посмотреть визуализацию МЧД
- Как распечатать МЧД
- Как проверить статус МЧД

Почтовые настройки

- Как добавить почтовый аккаунт:
  - почта Mail,
  - Яндекс почта,
  - Gmail,
  - Outlook,
  - iCloud,
  - Rambler.
- Как открыть настройки аккаунта
- Как изменить пароль в аккаунте
- Как настроить подпись и шифрование исходящих писем
- Как привязать сертификат подписи к аккаунту
- Как создать подпись (в конце письма)
- Как настроить отображение информации о сертификате в подписи (в конце письма)
- Как настроить автоответчик
- Как настроить пересылку писем в другой ящик

Адресные книги

- Как подключить адресную книгу LDAP
- Как подключить адресную книгу ALDPro
- Как добавить адресную книгу по протоколу CardDAV

Работа с письмами

- Как отправить подписанное и зашифрованное письмо
- Как отправить письмо с уведомлением о доставке и прочтении
- Как проверить подпись письма
- Как расшифровать письмо
- Как узнать доставлено ли письмо
- Как узнать прочитано ли письмо
- Как открыть письмо в формате .eml
- Как расшифровать письмо в формате.p7m
- Как проверить подпись письма с вложением smime.p7s

Открыть статью на сайте

Глоссарий

Сертификаты

Термин	Определение
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

Термин	Определение
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 квалифированных 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

Термин	Определение
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.

Термин	Определение
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.

Термин	Определение
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

Термин	Определение
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.

Термин	Определение
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

API КриптоАРМ

Руководство содержит описание API приложения КриптоАРМ.