Цифровые технологии

КриптоАРМ ГОСТ 3

Документация продукта

Релиз v3.7

Исходная документация на Trusted.ru

Редакция от 13.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Общие сведения

- О продукте ... 5
- Функции ... 7
- Описание ... 11
- Оценка ... 14
- Лицензирование ... 16

Начало работы с приложением

- Установка КриптоАРМ на Windows ... 19
- Установка КриптоАРМ на Linux ... 25
- Установка КриптоАРМ на macOS ... 35
- Установка КриптоПро CSP на Windows ... 43
- Установка КриптоПро CSP на macOS ... 44
- Установка КриптоПро CSP на Linux ... 46
- Установка лицензии КриптоАРМ ... 49
- Установка лицензии КриптоПро CSP ... 51
- Установка лицензии TSP и OCSP ... 53

Почта

- О почте ... 54
- Добавить аккаунт ... 57
- Отправка писем ... 60
- Просмотр писем ... 63
- Действия с письмами ... 64
- Подписать и отправить ... 69
- Настройки почты ... 73
- Уведомления ... 79
- Цепочки писем ... 81
- Статус письма ... 82
- Удаление и восстановление ... 83
- Удалить аккаунт ... 85
- Поиск писем ... 86
- Активный аккаунт ... 87

Документы

О документах ... 88
Профиль подписи ... 89
Информация о документе ... 92
Открыть документ ... 94
Удаление документов ... 95
Редактировать профиль ... 96
Удалить профиль ... 97
Смена профиля ... 98
Настройки профиля ... 99
Сертификат подписи ... 100
Сертификаты шифрования ... 102
Добавить в мастер ... 104
Показать в папке ... 105
Подписать документ ... 106
Зашифровать документ ... 113
Архивация ... 116
Расшифровать документ ... 117
Проверка подписи ... 119
Соподпись ... 122
Снять подпись ... 125
Групповые операции ... 126
Обратные операции ... 128
Результаты операций ... 130

Сертификаты

Установить сертификат ... 132
Сертификат из DSS ... 134
Запрос на сертификат ... 136
Самоподписанный сертификат ... 138
Корневые сертификаты ... 140
Импорт сертификатов ... 141
Список отзыва (CRL) ... 142
Экспорт личного ... 143
Экспорт сертификата ... 145

Ключевые контейнеры ... 146
Удалить сертификат ... 149
Действия с сертификатами ... 150

Контакты

Контакты ... 153
Добавить контакт ... 155
LDAP-книга ... 157
Информация о контакте ... 158
Связать сертификат ... 159
Редактировать контакт ... 161
Настройки LDAP ... 162
Смена книги ... 163
Удалить контакт ... 164
Восстановить контакт ... 165
Удалить LDAP ... 166
Поиск контакта ... 167
Группы контактов ... 168
vCard ... 170
CardDAV ... 171

Описание программы

О программе ... 172
Уведомления ... 173
Журнал событий ... 174

Дополнительные статьи

Index ... 177

Открыть статью на сайте

Описание

КриптоАРМ ГОСТ 3 Защищённая почта — отечественное программное решение, объединяющее функции почтового клиента и средства криптографической защиты информации. Программа предназначена для безопасного обмена электронными сообщениями и файлами с использованием шифрования и электронной подписи.

Решение позволяет организовать защищённый и юридически значимый электронный документооборот по электронной почте, обеспечивая конфиденциальность и целостность передаваемых данных.

Поддерживаемые платформы

Приложение работает на следующих операционных системах:

- Microsoft Windows
- macOS
- Linux
- Российские операционные системы (на базе Linux)

Совместимость

КриптоАРМ ГОСТ 3 Защищённая почта совместим с криптопровайдером СКЗИ:

- **КриптоПро CSP 5.0 R2 и выше**

Это обеспечивает работу с квалифицированной электронной подписью и ГОСТ-криптографией.

Основные возможности

Программа позволяет:

- подписывать электронные письма электронной подписью;
- шифровать содержимое писем и вложений;
- расшифровывать полученные защищённые сообщения;
- обмениваться конфиденциальной информацией через интернет-каналы связи.

Лицензирование

Функциональность зависит от типа лицензии:

КриптоАРМ ГОСТ 3

Позволяет:

- подписывать электронные документы;
- шифровать и расшифровывать файлы и документы;
- использовать приложение как стандартное средство работы с электронными документами.

КриптоАРМ ГОСТ 3 Защищённая почта

Дополнительно включает:

- использование приложения в качестве защищённого почтового клиента;
- подпись электронных писем;
- шифрование и расшифрование почтовых сообщений;
- обеспечение защищённого обмена email-сообщениями.

Таким образом, версия «Защищённая почта» расширяет базовый функционал КриптоАРМ ГОСТ 3, добавляя возможность работы непосредственно с электронной почтой в защищённом режиме.

Открыть статью на сайте

Функции

Функциональность

Операция	
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
	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 документами	работа с результатами выполнения операций с документами

Операция	
	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
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
	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	

Операция	
	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 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
	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

Операция	
	удаление сертификатов
	импорт сертификатов из DSS
	формирование отчёта действительности сертификата электронной подписи
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

Назначение и условия применения

КриптоАРМ ГОСТ 3 Защищённая почта — программное обеспечение, объединяющее функциональность почтового клиента и средства криптографической защиты информации. Приложение предназначено для защищённого обмена электронной корреспонденцией с использованием электронной подписи и шифрования.

Решение применяется для обмена конфиденциальными сообщениями между пользователями почтовых систем по стандартным почтовым протоколам:

- SMTP / SMTPS
- IMAP / IMAPS

Приложение обеспечивает:

- подготовку и отправку электронных писем;
- хранение и просмотр писем на локальном рабочем месте;
- криптографическую защиту содержимого писем и вложений.

Криптографические алгоритмы

Для защиты данных используются алгоритмы ГОСТ:

- ГОСТ 28147-89 (шифрование)
- ГОСТ Р 34.10-2012 (электронная подпись)
- ГОСТ Р 34.11-2012 (хеширование)
- ГОСТ Р 34.12-2015 / ГОСТ Р 34.12-2018 (блочные шифры)
- ГОСТ Р 34.13-2015 (режимы шифрования)

Приложение предназначено для создания и проверки электронной подписи, шифрования и расшифрования файлов посредством использования криптопровайдера КриптоПро CSP.

Криптопровайдер (Cryptography Service Provider, CSP) — это независимый модуль, позволяющий осуществлять криптографические операции с помощью функций CryptoAPI.

Поддерживаемые криптопровайдеры

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

Поддерживаемые ключевые носители

В приложении поддерживается работа с ключевыми носителями Рутокен, JaCarta, ESMART, АНГАРА через криптопровайдер КриптоПро CSP.

Лицензирование программного продукта

Для использования криптографических функций требуется лицензия.

Варианты лицензий

- **Временная лицензия** выдаётся пользователю, заполнившему форму на странице, для знакомства с продуктом сроком на 30 дней.
- **Годовая и бессрочная лицензии** приобретаются в интернет-магазине.

Для работы с криптографическими операциями только в разделе **Документы** (подписывать и расшифровывать электронные документы) необходима лицензия на **КриптоАРМ ГОСТ 3** или **КриптоАРМ ГОСТ 3 Защищённая почта**.

Для работы с криптографическими операциями в разделе **Почта** (подписывать, шифровать и расшифровывать электронные письма) и в разделе **Документы** (подписывать и расшифровывать электронные документы) необходима лицензия на **КриптоАРМ ГОСТ 3 Защищённая почта**.

Для работы приложения в качестве почтового клиента без использования функций подписи, шифрования и расшифрования писем и электронных документов лицензия на программу не требуется.

Системные требования

Для приложения сформулированы минимальные системные требования к конфигурации оборудования:

Процессор	Intel Pentium 4 или более поздний, который поддерживает SSE2
RAM	2 Гб
HDD	500 Мб

Поддерживаемые операционные системы

Клиентские:

- Microsoft Windows 7, 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
- Альт Рабочая станция 10
- Альт СП релиз 10
- РЕД ОС 8

- Роса «Хром» 12 Рабочая станция
- ОС «МСВСфера АРМ» 9
- AlterOS

Серверные:

- Windows Server 2016, 2019
- Ubuntu Server 20.04, 22.04
- CentOS 8
- Альт Сервер 10
- РЕД ОС «Сервер»
- РОСА Хром Сервер

> Следует учесть, что для работы необходима установка криптопровайдера КриптоПро CSP.

Открыть статью на сайте

Оценка приложения

В приложении предусмотрена возможность оставить оценку и отзыв. Это помогает улучшать продукт и учитывать пожелания пользователей.

Вы можете:

- поставить оценку приложению;
- оставить текстовый отзыв;
- указать контактные данные (по желанию);
- изменить уже отправленную оценку и отзыв.

Как оценить приложение

Чтобы оставить оценку:

1. На панели управления найдите иконку **Оценка приложения**.

   Она расположена рядом с кнопками управления окном:
   Свернуть, **Развернуть**, **Закрыть**.

2. Откройте форму оценки.

3. В появившемся окне доступны следующие поля:

   - оценка (обязательное поле);
   - отзыв о приложении (необязательно);
   - имя (необязательно);
   - e-mail (необязательно).

   Вы можете отправить только оценку без заполнения дополнительных полей.

4. Нажмите кнопку **Отправить**.

После отправки данные будут переданы разработчикам.

Как изменить оценку

Если вы уже отправили оценку, её можно изменить:

1. Нажмите на иконку **Оценка приложения**.
2. Откроется форма с ранее заполненными данными.
3. Нажмите кнопку **Изменить оценку**.

4. Внесите необходимые изменения:
    - скорректируйте оценку;
    - при необходимости измените текст отзыва и контактные данные.
5. Нажмите **Отправить** для сохранения изменений.

Примечание

Вы можете изменять оценку и отзыв неограниченное количество раз. Актуальной считается последняя отправленная версия.

Открыть статью на сайте

Лицензирование

Лицензии на **КриптоАРМ ГОСТ 3** различаются по времени действия и по функциональности.

Лицензии по времени действия

Для работы в приложении с криптографическими операциями необходима лицензия (временная, годовая или бессрочная).

- **Временная лицензия** выдаётся пользователю, заполнившему форму на странице, для знакомства с продуктом сроком на 30 дней.
- **Годовая и бессрочная лицензии** приобретаются в интернет-магазине.

Лицензии по функциональности

- лицензия на **КриптоАРМ ГОСТ 3** позволяет подписывать, шифровать и расшифровывать электронные документы, а также использовать приложение в качестве почтового клиента;
- лицензия на **КриптоАРМ ГОСТ 3 Защищённая почта** позволяет не только подписывать, шифровать и расшифровывать электронные документы, но и использовать приложение в качестве защищённого почтового клиента — подписывать, шифровать и расшифровывать сами почтовые сообщения.

Сравнение лицензий

Раздел «Почта»

Функция	КриптоАРМ ГОСТ 3	КриптоАРМ ГОСТ 3 Защищённая почта
Подключение аккаунтов (SMTP/SMTPS/IMAP/IMAPS)	✔	✔
Несколько почтовых аккаунтов	✔	✔
Работа с письмами (просмотр/отправка/получение)	✔	✔
Уведомления о письмах	✔	✔
Поиск и сортировка	✔	✔
Группировка писем в цепочки	✔	✔
Контакты из переписки	✔	✔

Функция	КриптоАРМ ГОСТ 3	КриптоАРМ ГОСТ 3 Защищённая почта
Подпись писем	❌	✔
Проверка подписи писем	❌	✔
Шифрование писем	❌	✔
Расшифрование писем	❌	✔

Раздел «Документы»

Функция	КриптоАРМ ГОСТ 3	Защищённая почта
Подпись документов	✔	✔
Проверка подписи	✔	✔
Шифрование / расшифрование	✔	✔
Комбинированные операции (подпись + шифрование и др.)	✔	✔
Подпись в DER / BASE64	✔	✔
Отсоединённая и присоединённая подпись	✔	✔
Архивирование (.zip)	✔	✔
Алгоритмы ГОСТ (28147-89, 34.12-2015, 34.13-2015)	✔	✔
Поддержка CAdES-T / CAdES-X Long Type 1	✔	✔
Соподпись	✔	✔
Шифрование для нескольких получателей	✔	✔

Раздел «Контакты»

Функция	КриптоАРМ ГОСТ 3	Защищённая почта
Локальная адресная книга	✔	✔
LDAP	✔	✔

Функция	КриптоАРМ ГОСТ 3	Защищённая почта
CardDAV	✔	✔
Импорт .vcf	✔	✔
Группы контактов	✔	✔
Отправка писем группе	✔	✔

Раздел «Сертификаты»

Функция	КриптоАРМ ГОСТ 3	Защищённая почта
Сертификаты ЭП	✔	✔
Ключевые контейнеры	✔	✔
Запросы на сертификаты	✔	✔
CRL (списки отзыва)	✔	✔
DSS сертификаты	✔	✔

КриптоАРМ API

Функция	КриптоАРМ ГОСТ 3	Защищённая почта
API-интерфейс	✔	✔

Итог

- **КриптоАРМ ГОСТ 3** — подходит для работы с электронными документами и базовыми криптографическими операциями.
- **КриптоАРМ ГОСТ 3 Защищённая почта** — расширяет функциональность, добавляя защищённую работу с электронной почтой.

Выбор лицензии зависит от задач пользователя: работа только с документами или полноценный защищённый почтовый обмен.

Открыть статью на сайте

Установка КриптоАРМ ГОСТ на Windows

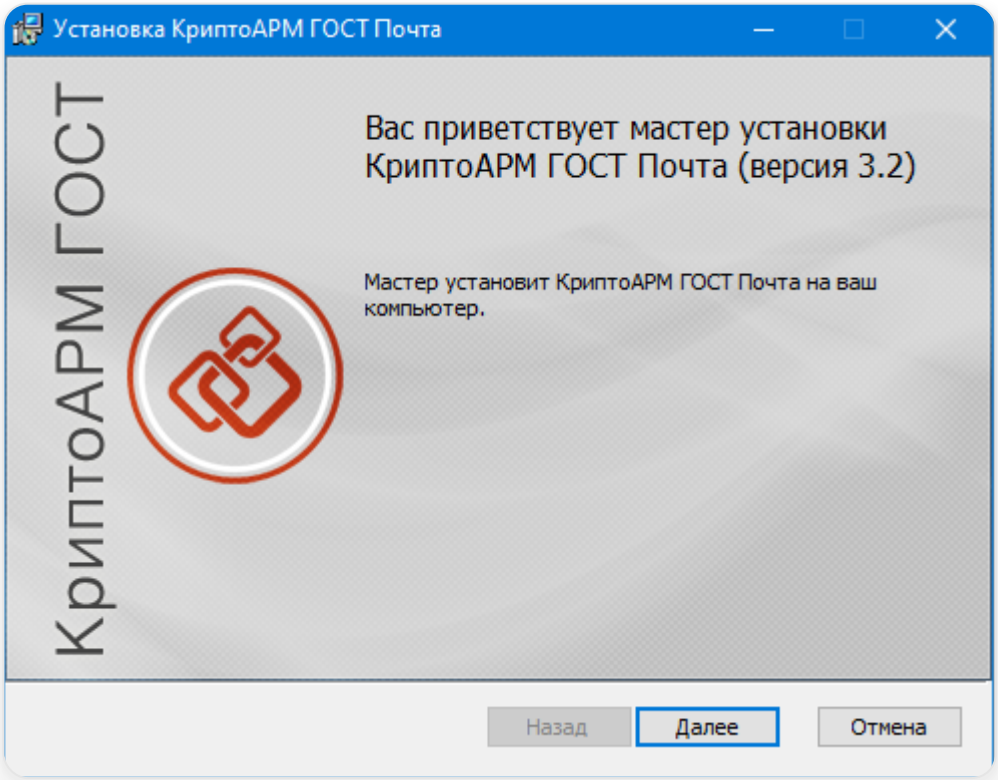
Важно! Дополнительно требуется установить:

- Распространяемые пакеты VS C++ 2013 (x64): https://www.microsoft.com/ru-RU/download/details.aspx?id=40784
- Распространяемые пакеты VS C++ 2019 (x64): https://support.microsoft.com/ru-ru/topic/%D0%BF%D0%BE%D1%81%D0%BB%D0%B5%D0%B4%D0%BD%D0%B8%D0%B5-%D0%BF%D0%BE%D0%B4%D0%B4%D0%B5%D1%80%D0%B6%D0%B8%D0%B2%D0%B0%D0%B5%D0%BC%D1%8B%D0%B5-%D0%B2%D0%B5%D1%80%D1%81%D0%B8%D0%B8-visual-c-%D0%B4%D0%BB%D1%8F-%D1%81%D0%BA%D0%B0%D1%87%D0%B8%D0%B2%D0%B0%D0%BD%D0%B8%D1%8F-2647da03-1eea-4433-9aff-95f26a218cc0

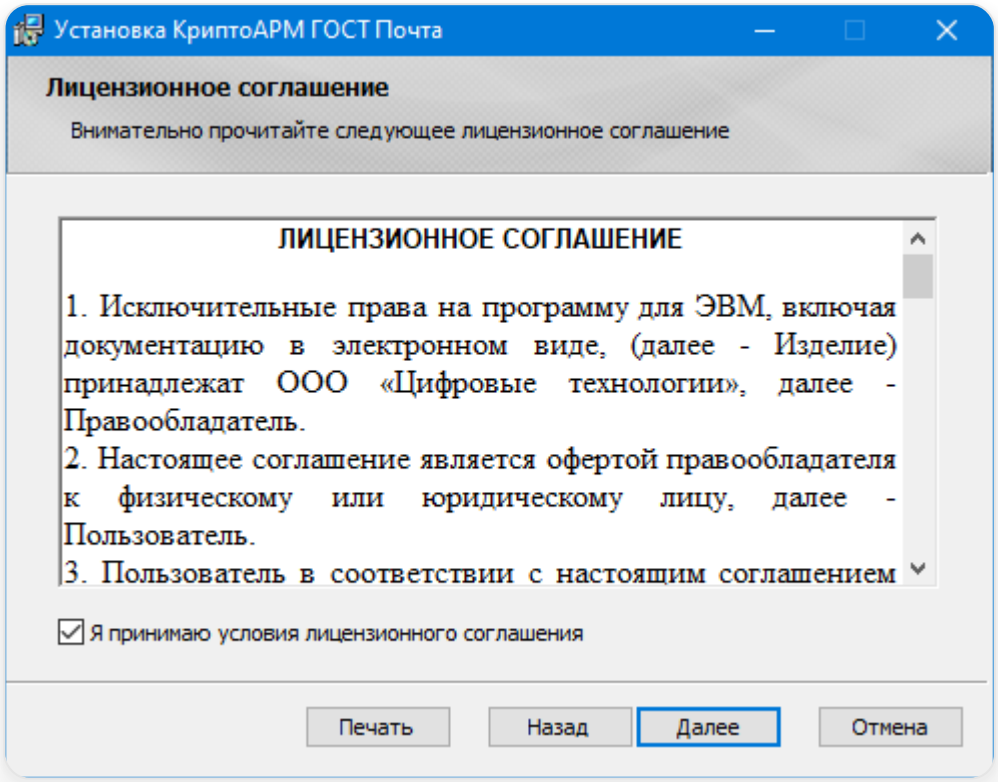
Для установки приложения **КриптоАРМ ГОСТ** на платформу **Microsoft Windows** предлагается дистрибутив под 64-битную платформу: **cryptoarm-gost-vx.x.x-win32-x64.msi**

Важно: для установки приложения нужны права администратора.

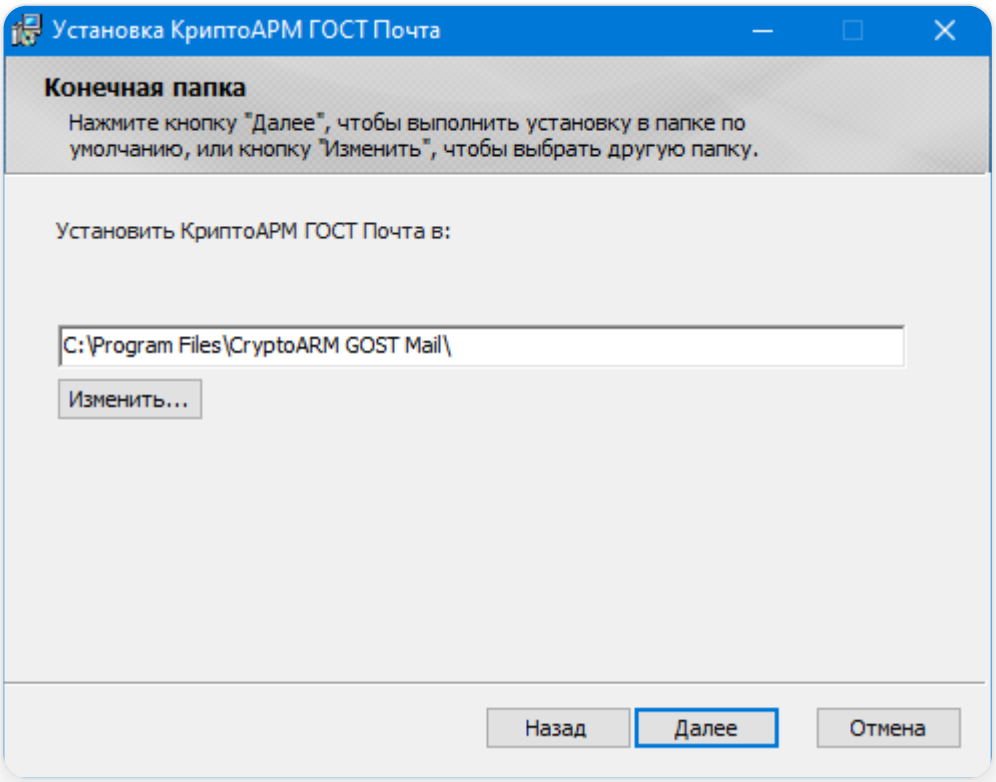
1. При запуске исполняемого файла открывается мастер установки приложения **КриптоАРМ ГОСТ**.



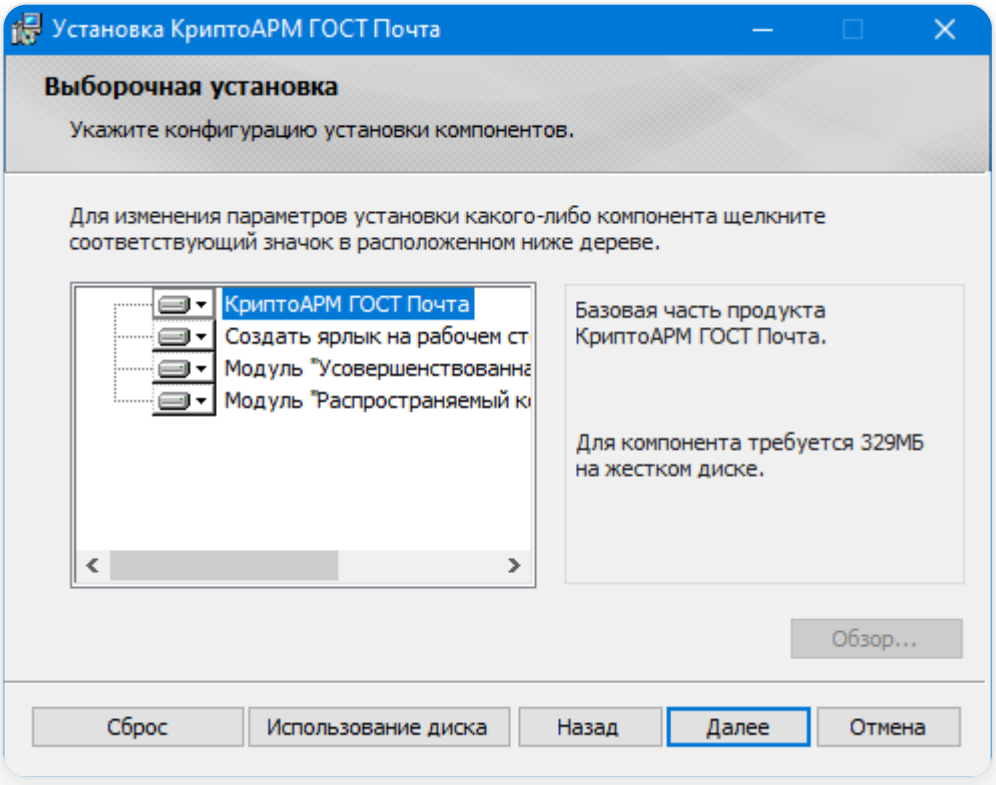
2. По кнопке **Далее** происходит переход на следующий шаг, где предлагается ознакомиться с условиями лицензионного соглашения. В случае согласия нужно **принять условия** и перейти к следующему шагу мастера, нажав кнопку **Далее**.



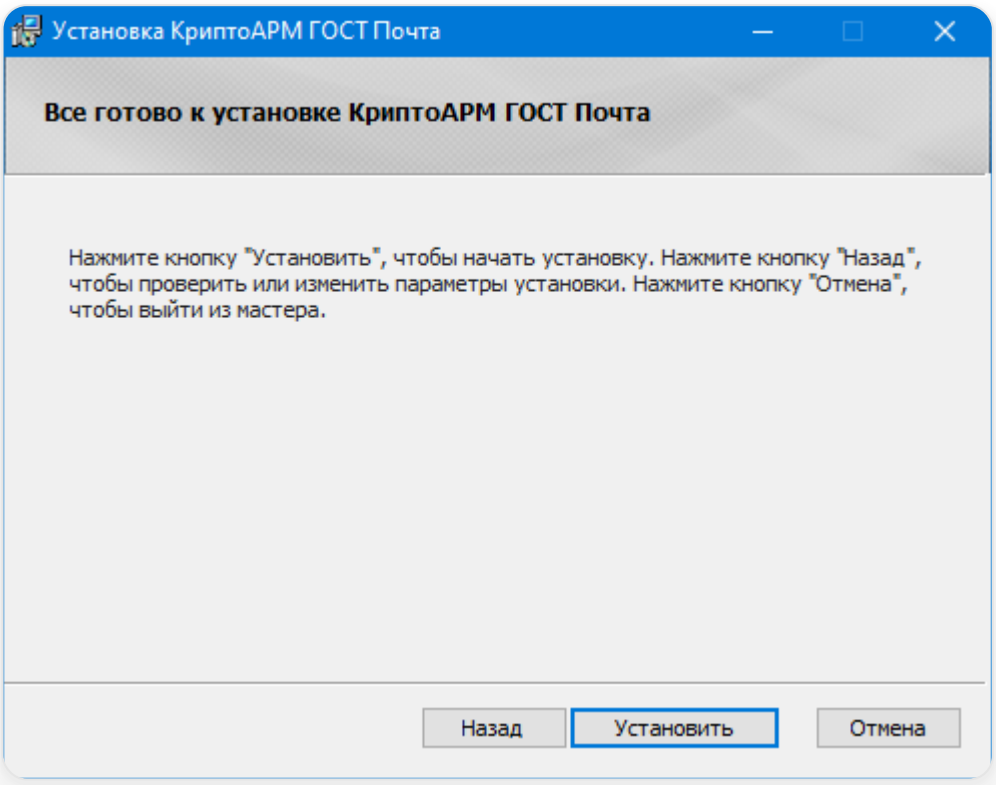
3. На следующем шаге мастера можно выбрать каталог для установки **КриптоАРМ ГОСТ** (по умолчанию приложение устанавливается в каталог `C:\Program Files\CryptoARM GOST Mail\`)).

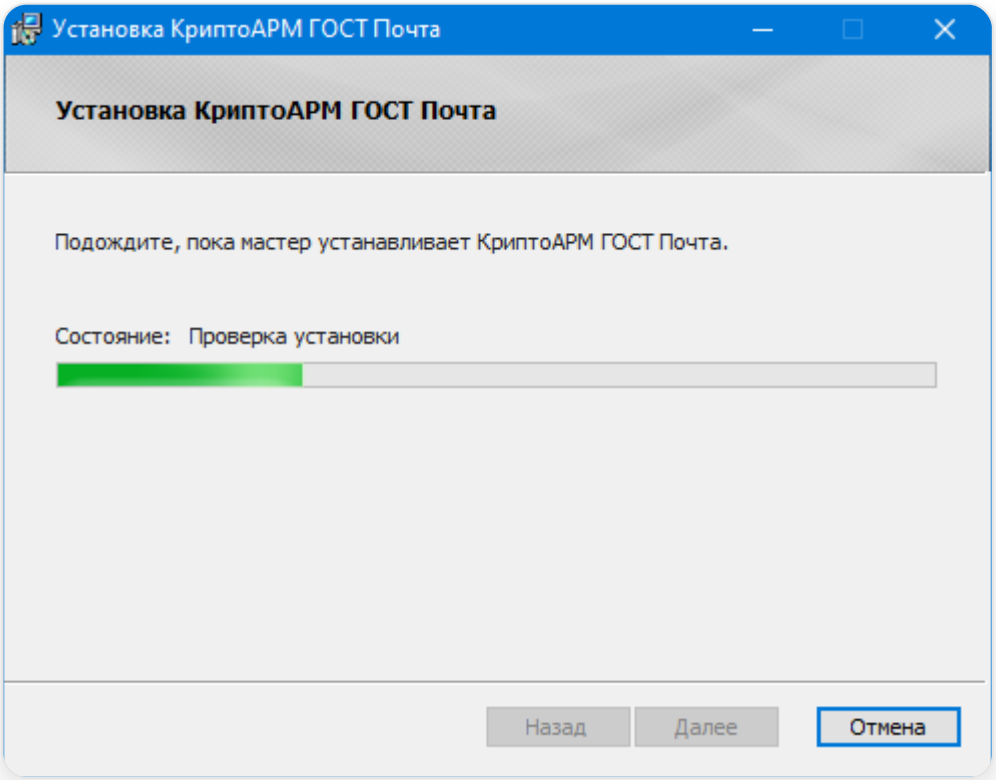


4. На шаге выборочной установки можно отключить создание ярлыка на рабочем столе и установку модулей для создания усовершенствованной подписи.

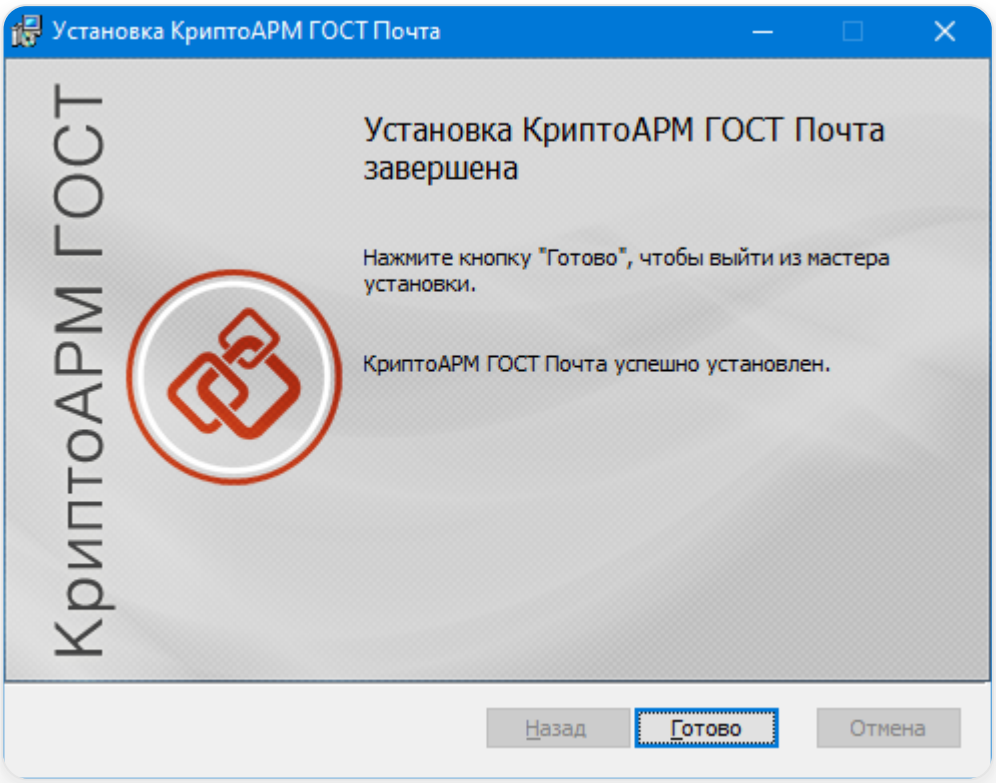


5. На заключительном шаге мастера по кнопке **Установить** выполняется установка. Нужны права администратора.





6. Закрыть окно установки, нажав **Готово**.



После успешной установки приложения в главном меню появится новая группа **КриптоАРМ ГОСТ**, которая содержит ярлык запуска приложения **КриптоАРМ ГОСТ** и ярлык запуска мастера удаления программы.

В указанном при установке каталоге (по умолчанию каталог `C:\Program Files\CryptoARM GOST Mail`) размещаются файлы приложения.

Открыть статью на сайте

Установка КриптоАРМ ГОСТ на Linux

Установка приложения **КриптоАРМ ГОСТ** на операционную систему **Linux** может быть выполнена в графическом режиме (через мастер установки пакетов), через терминал в режиме командной строки и обычной распаковкой из архива.

По умолчанию приложение устанавливается в каталог `/opt/cryptoarm_gost_3/`.

В режиме графической установки запустите на исполнение файл:

- **cryptoarm-gost-vx.x.x-x64.rpm** (где x.x.x – номер версии) для 64-разрядных ОС, основанных на **RPM**;
- **cryptoarm-gost-vx.x.x-x64.deb** (где x.x.x – номер версии) для 64-разрядных ОС, основанных на **DEB**.

Откроется пакетный менеджер, в котором нужно нажать **Установить**. Так как установка производится от имени администратора системы, то появится диалог ввода пароля администратора системы (`Root`).

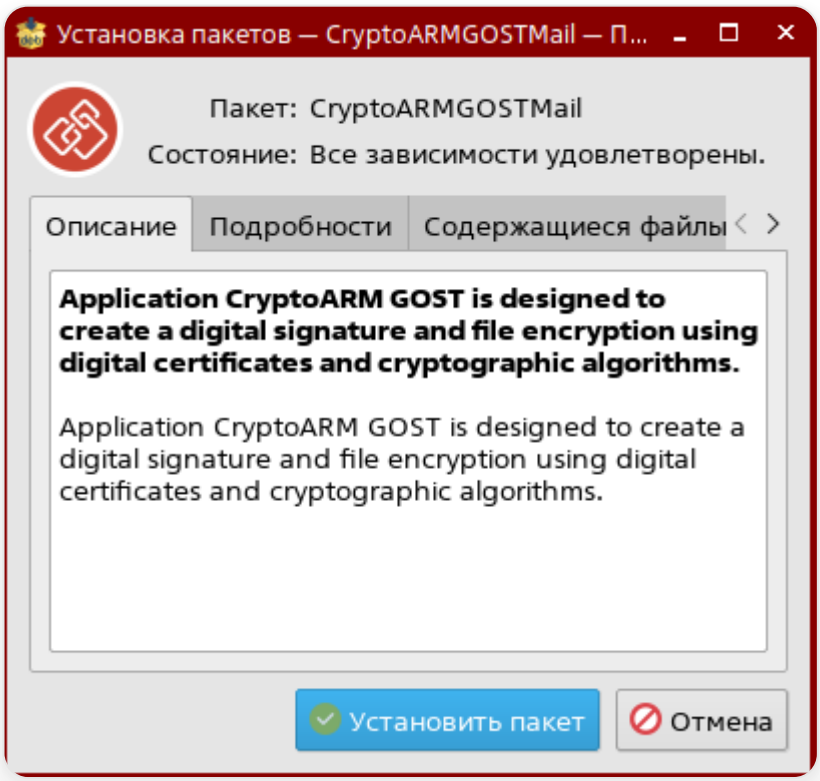
С помощью командной строки нужно запустить терминал и ввести команду:

- **sudo dpkg -i cryptoarm-gost-vx.x.x-x64.deb** — для ОС, основанных на **DEB**;
- **sudo rpm -i cryptoarm-gost-vx.x.x-x64.rpm** — для ОС, основанных на **RPM**;

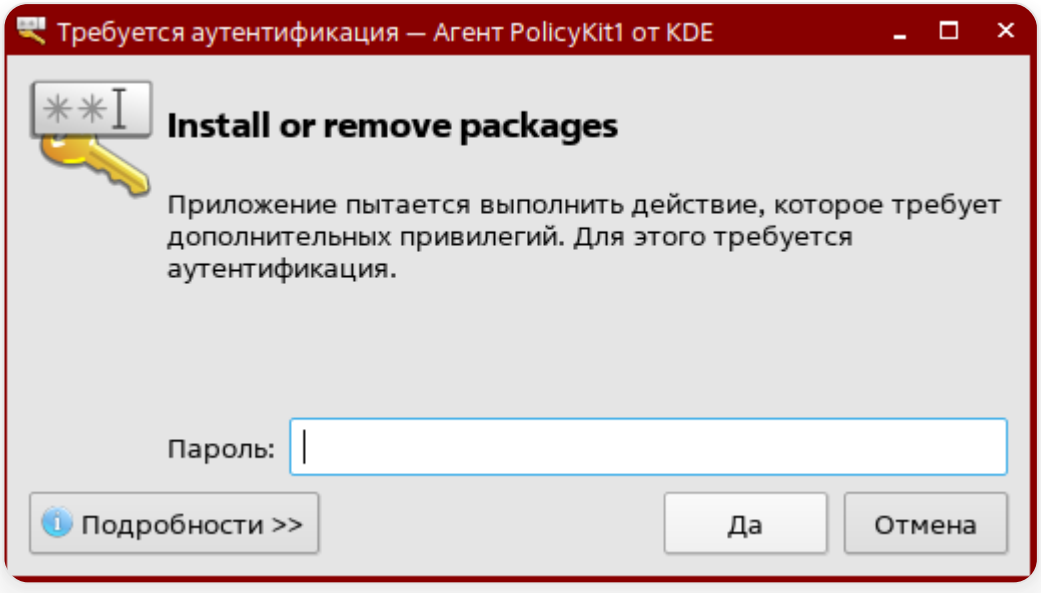
После установки приложения в меню появится ярлык **КриптоАРМ ГОСТ**.

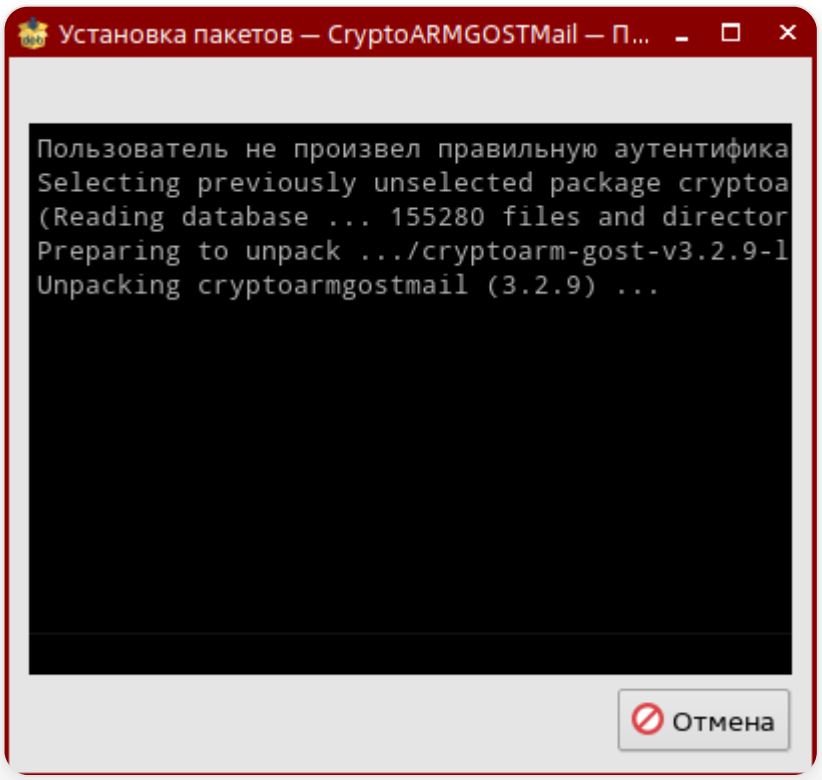
Графическая установка

1. На скачанный установочный файл дважды нажать левой кнопкой мыши. Откроется окно **Установка пакетов**, в котором нужно нажать **Установить пакет**.

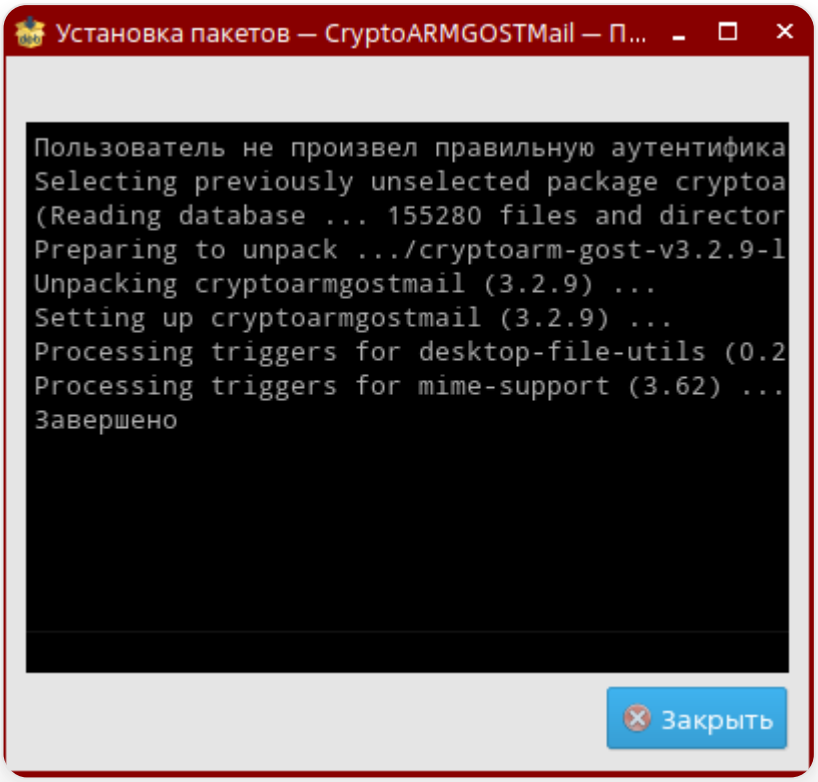


2. **Ввести** пароль системного администратора `root`. Начнётся установка пакетов.





3. После успешной установки программы на операционную систему нажать на **Закрыть**.

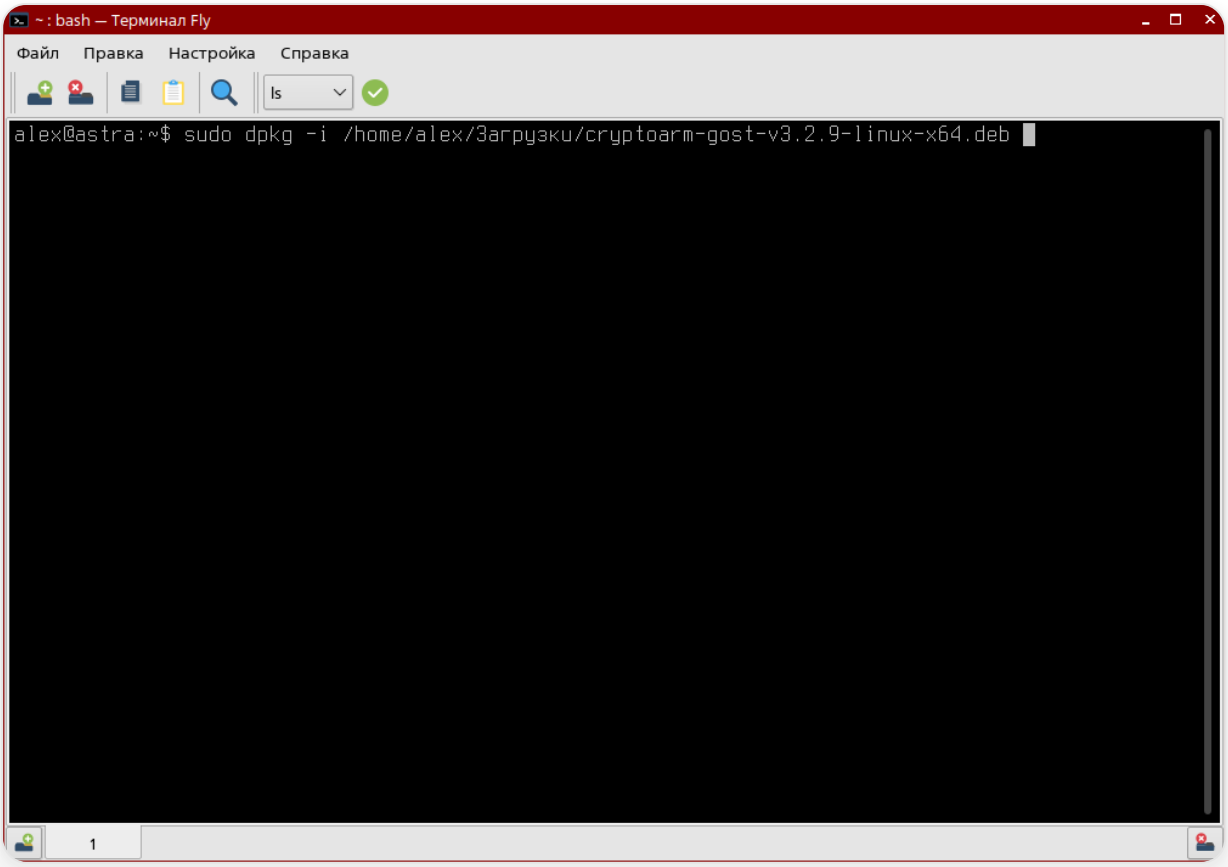


4. После установки приложения в меню появится ярлык **КриптоАРМ ГОСТ**.

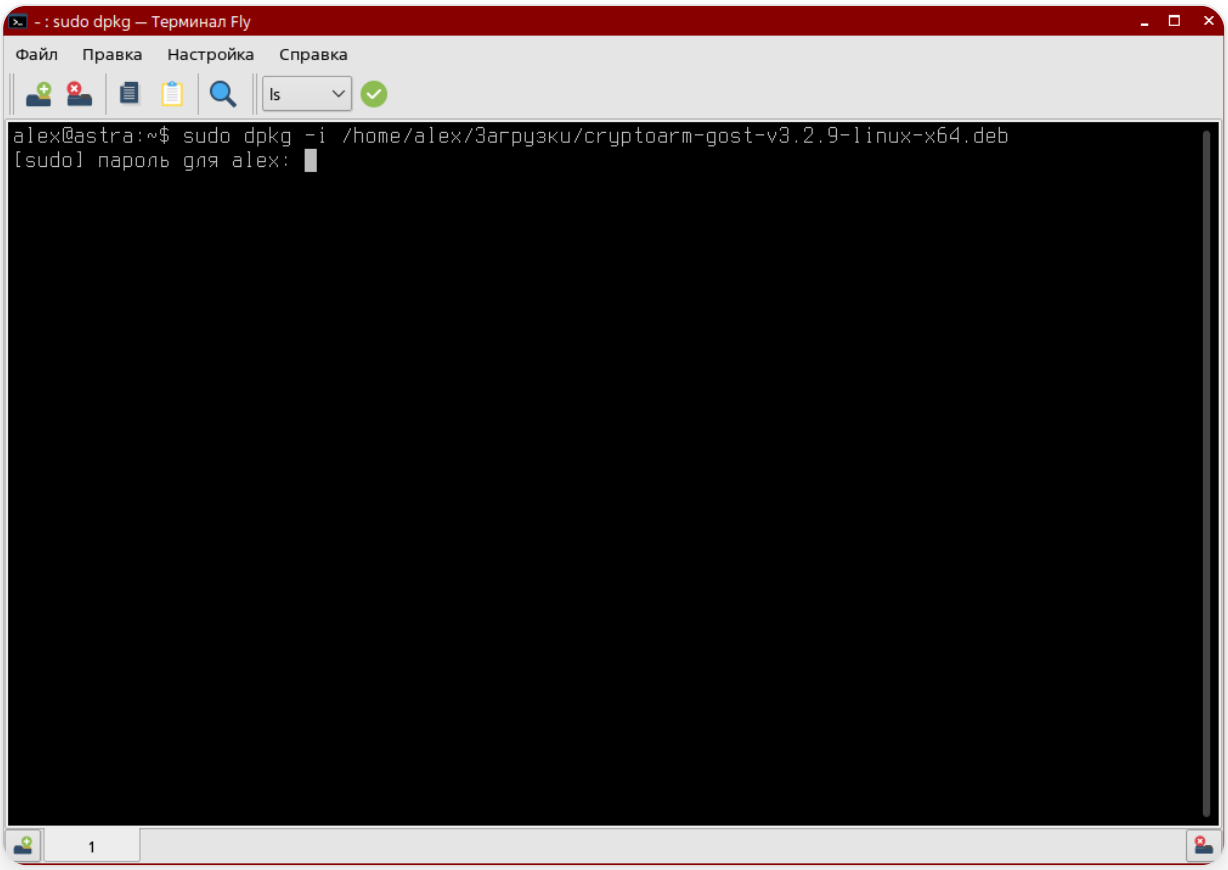
Установка через терминал

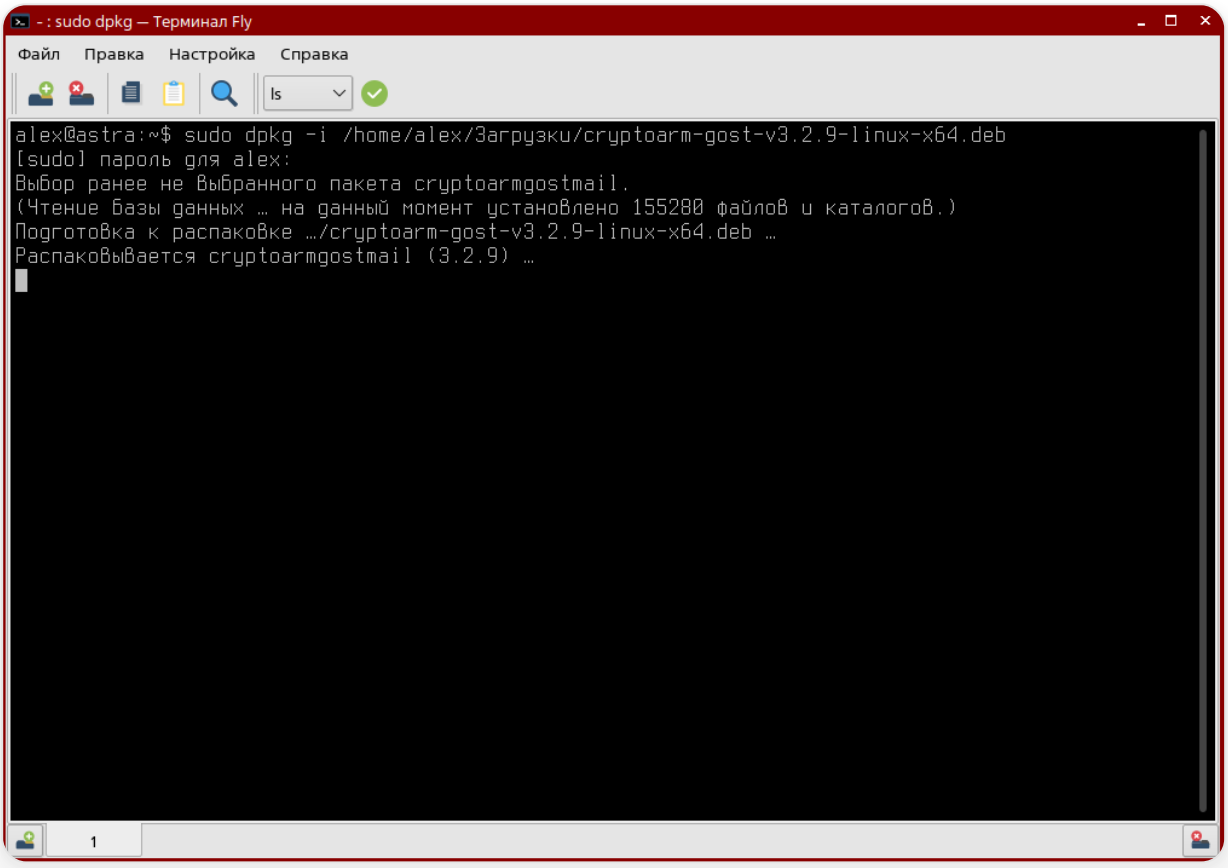
1. Для установки с помощью командной строки нужно запустить терминал и ввести команду:
   `sudo dpkb -i <путь\_к\_файлу/название_файла.deb>`

   Указать путь к установочному файлу и его название вручную или перетащить его в поле терминала.



2. Нажать **Enter**. Начинается 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

3. После установки приложения в меню появится ярлык **КриптоАРМ ГОСТ**.

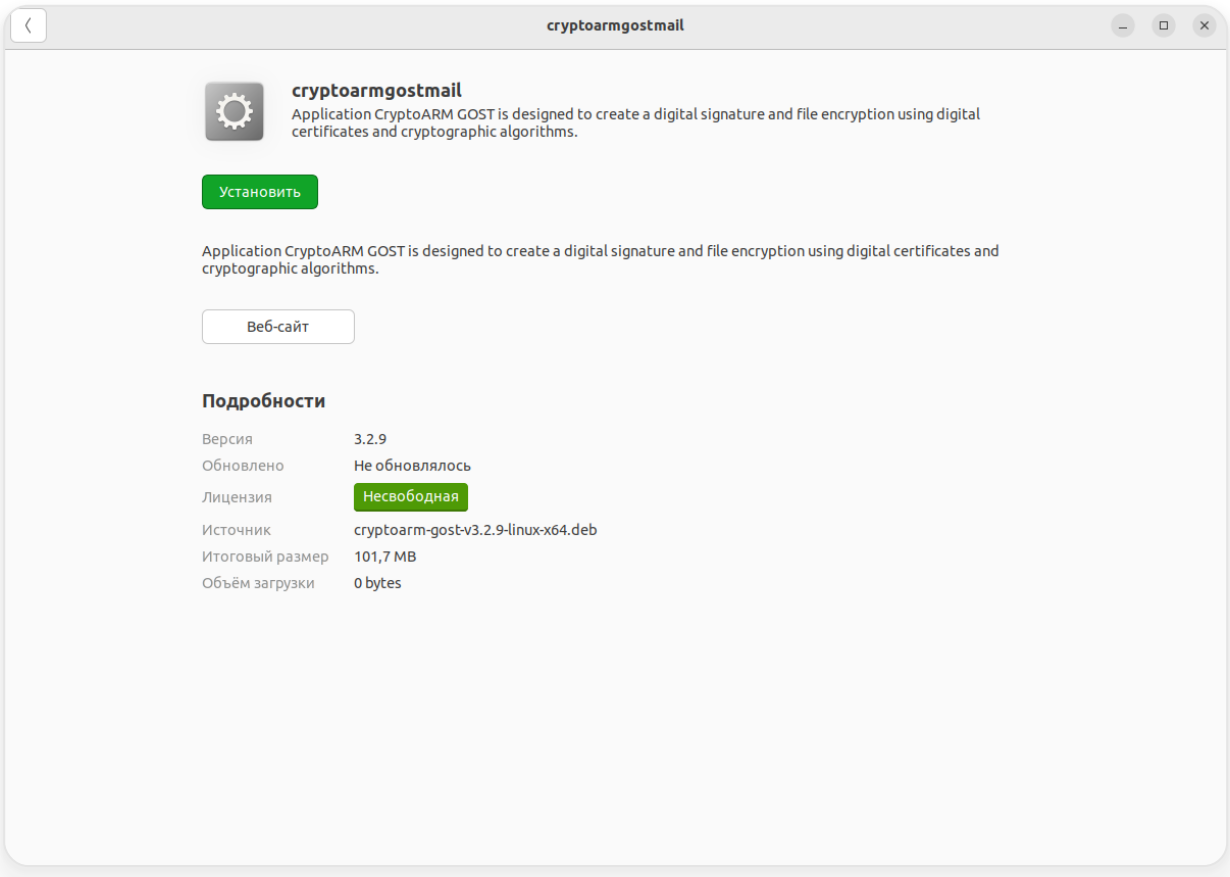
Установка КриптоАРМ ГОСТ на операционную систему Ubuntu

> **Важно!** Для Ubuntu 20.04 требуется установить дополнительно:

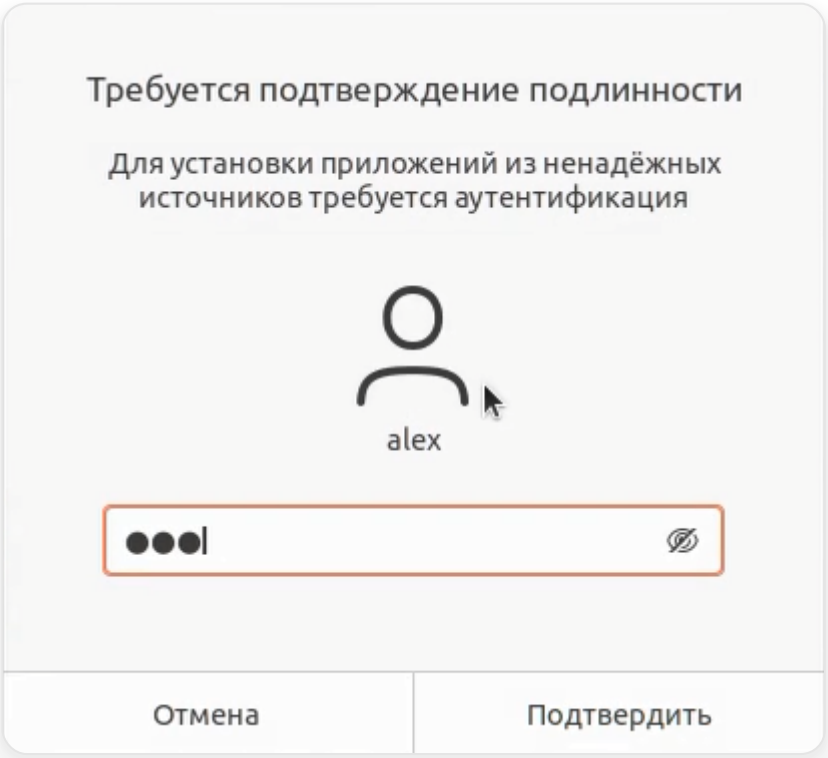
- `sudo apt install libtidy-dev`
- `sudo apt install libctemplate-dev`

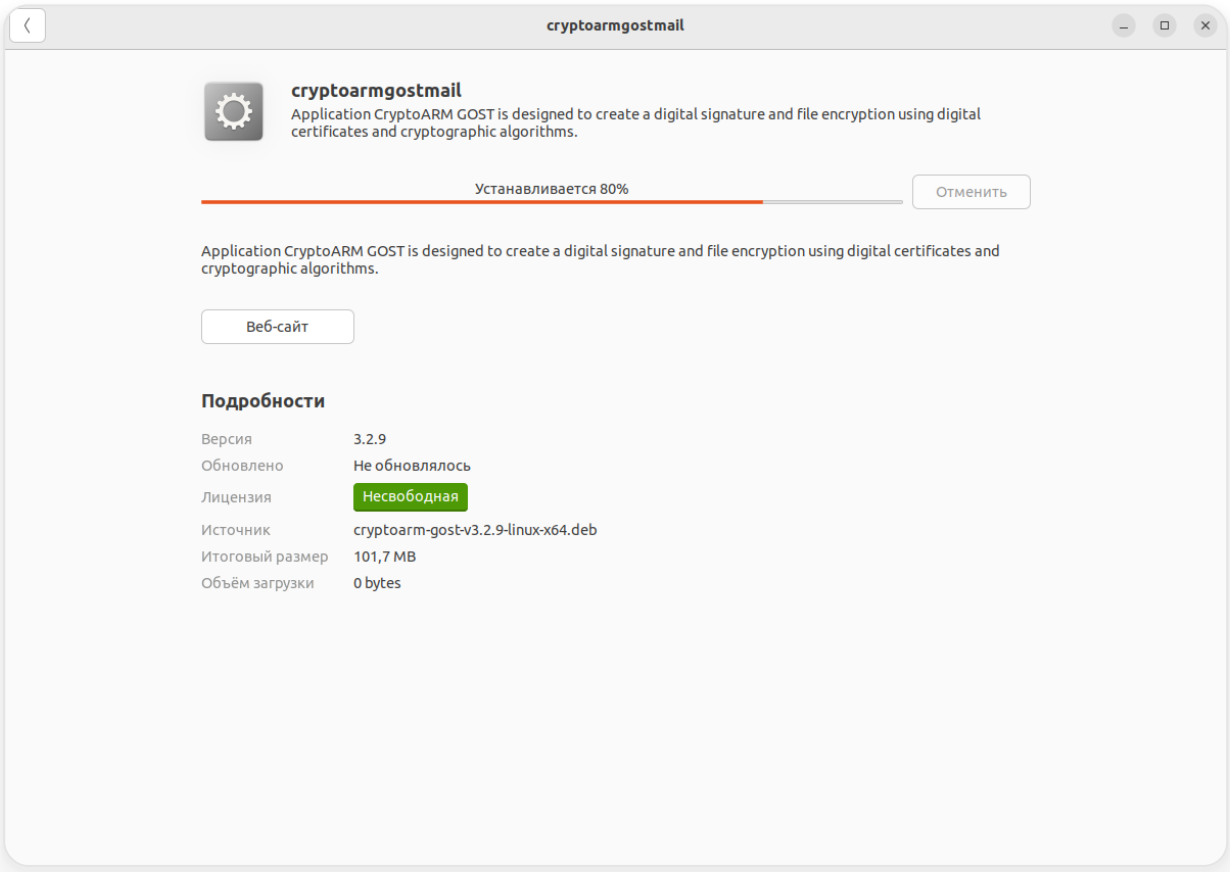
Графическая установка

1. На скачанный установочный файл дважды нажать левой кнопкой мыши. В открывшемся окне нажать на **Установить**.

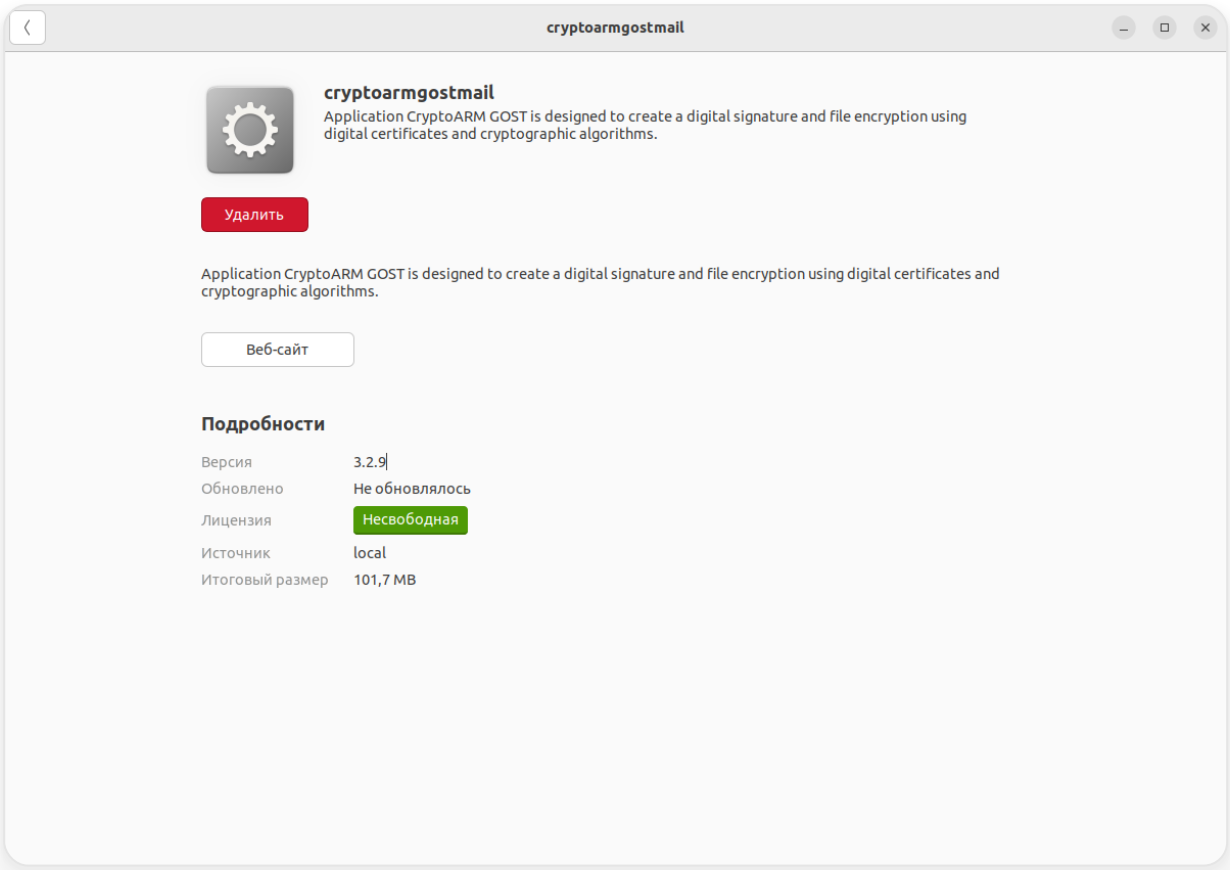


2. Ввести пароль системного администратора `root` и нажать **Подтвердить**. Начнётся установка.





3. Закрыть окно.

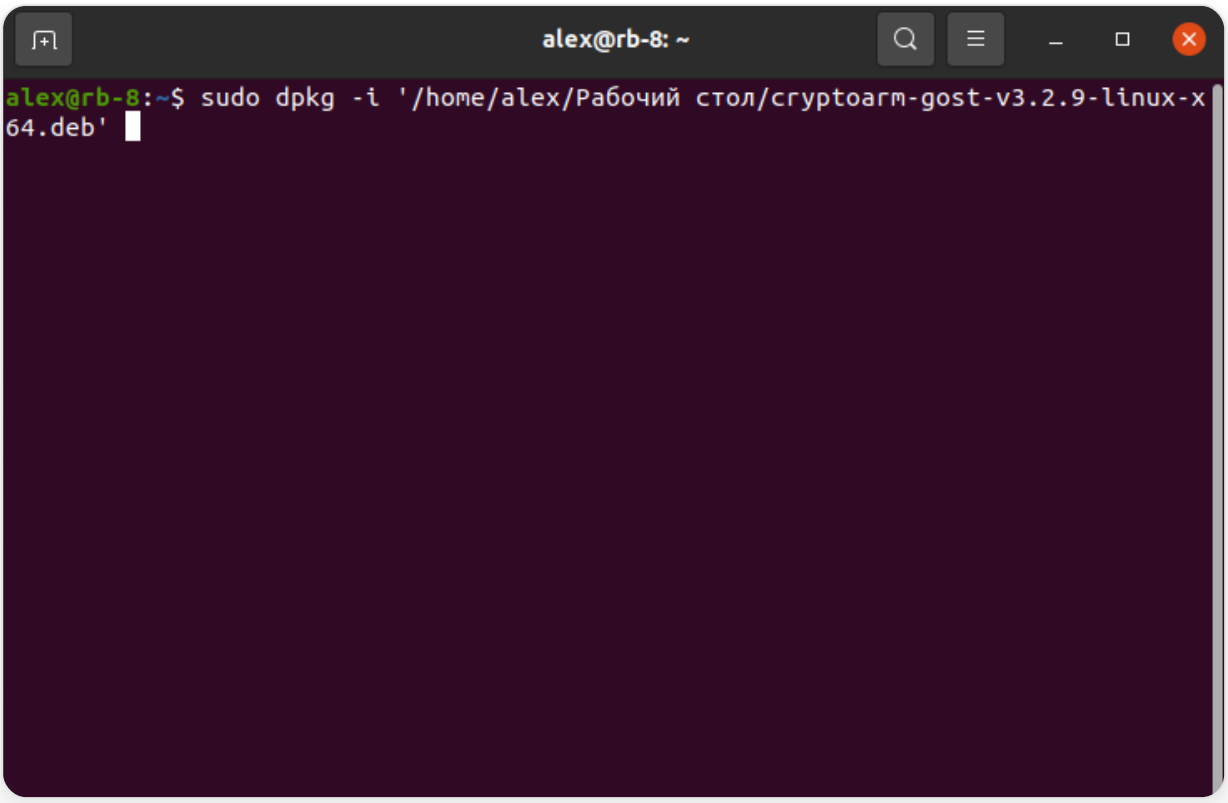


4. После установки приложения в меню появится ярлык **КриптоАРМ ГОСТ**.

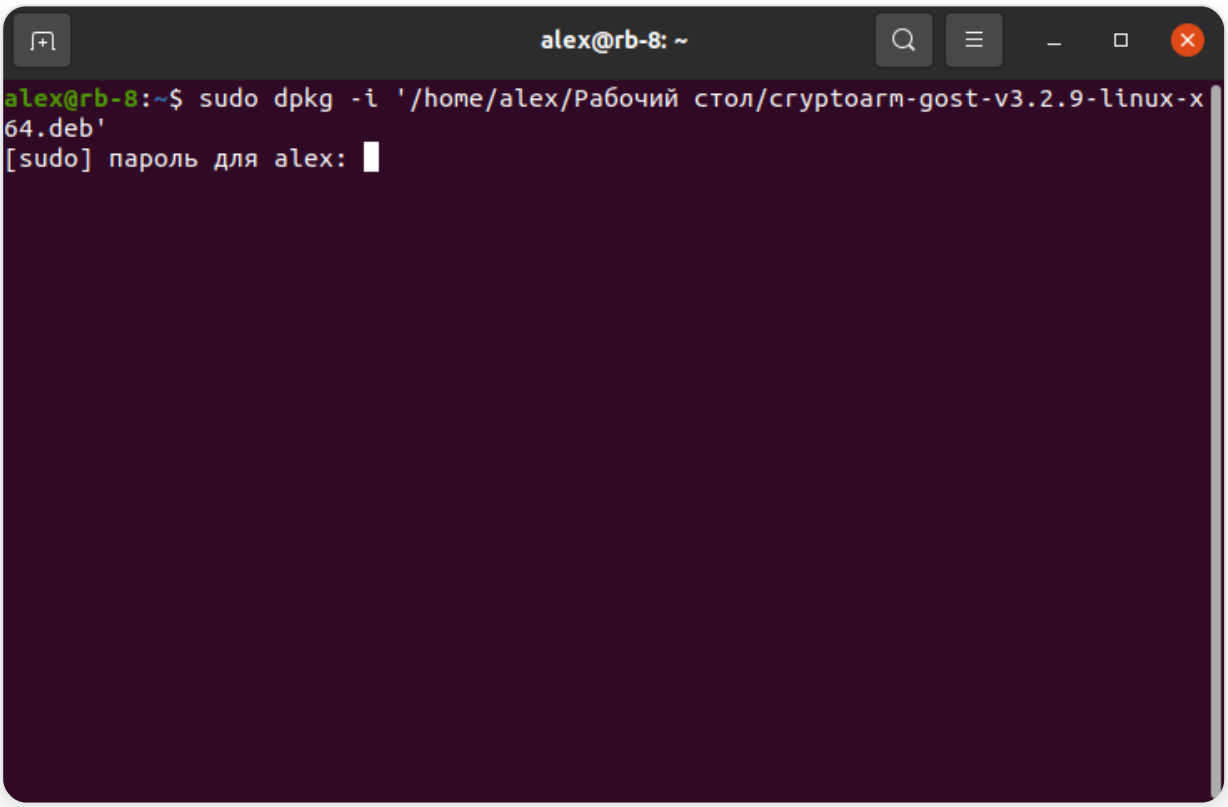
Установка через терминал

1. Для установки с помощью командной строки нужно запустить терминал и ввести команду:
   `sudo dpkb -i <путь\_к\_файлу/название_файла.deb>`

   Указать путь к установочному файлу и его название вручную или перетащить его в поле терминала.



2. **Ввести** пароль системного администратора root и нажать **Enter**. Начнётся установка пакетов.



3. После установки приложения в меню появится ярлык **КриптоАРМ ГОСТ**.

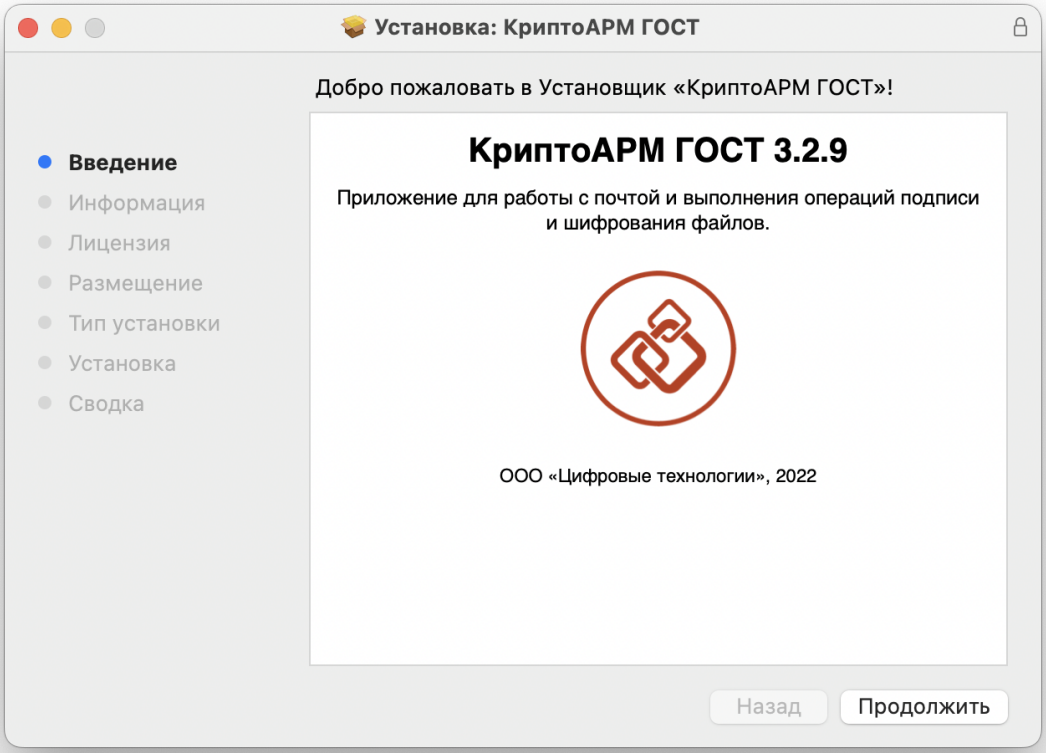
Открыть статью на сайте

Установка КриптоАРМ ГОСТ на macOS

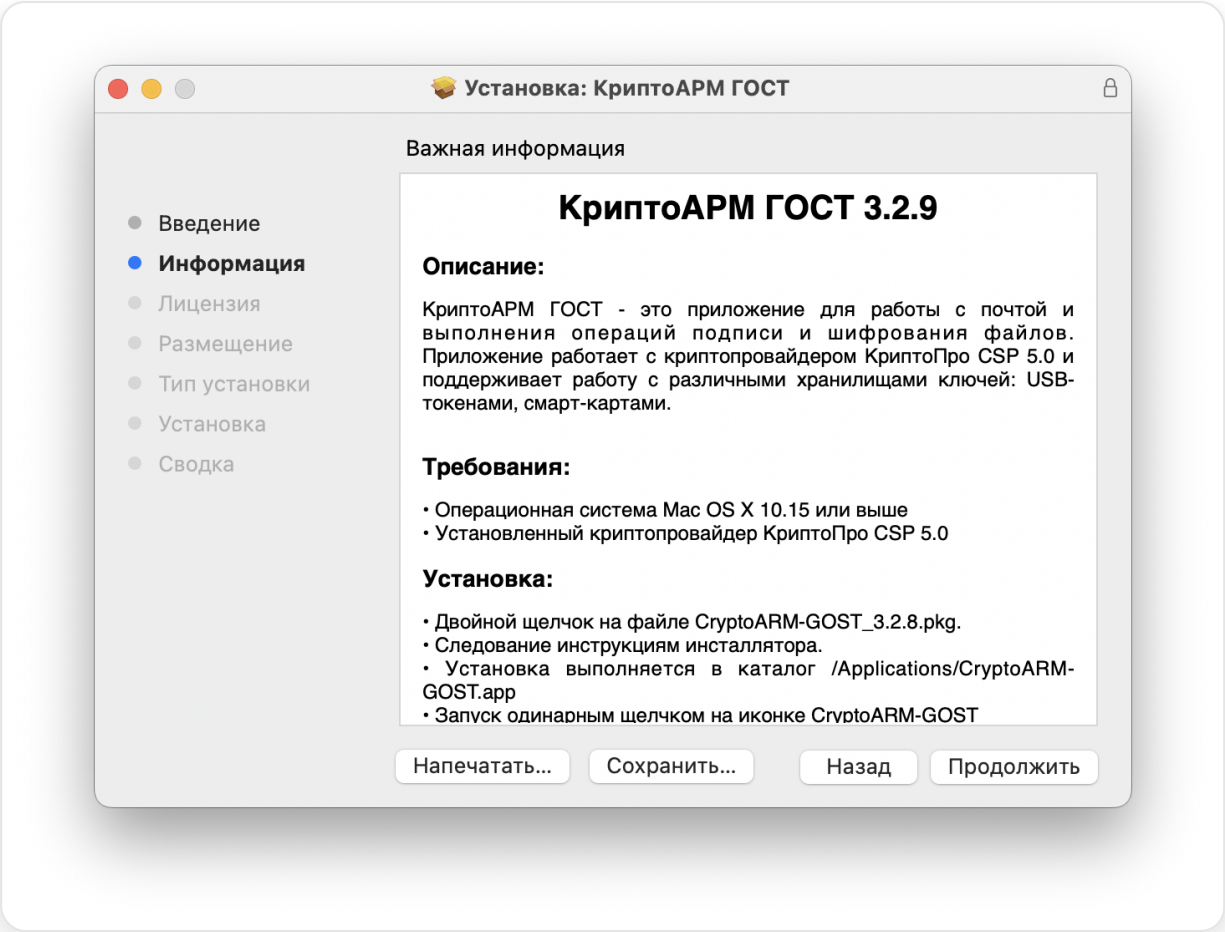
Дистрибутив приложения **КриптоАРМ ГОСТ** поставляется в упакованном виде, имеет формат `.dmg` и представляет собой образ диска, содержащий пакет установки **cryptoarm-gost-vx.x.x-x64.pkg,** описание приложения, каталог со скриптами удаления приложения.

1. Для установки пакета через графический интерфейс откройте двойным щелчком образ диска с дистрибутивом **cryptoarm-gost-vx.x.x-x64.dmg** (где x.x.x – номер версии).
2. Для установки программы **КриптоАРМ ГОСТ** запустите на исполнение файл **cryptoarm-gost-vx.x.x-64.pkg** (где x.x.x – номер версии).

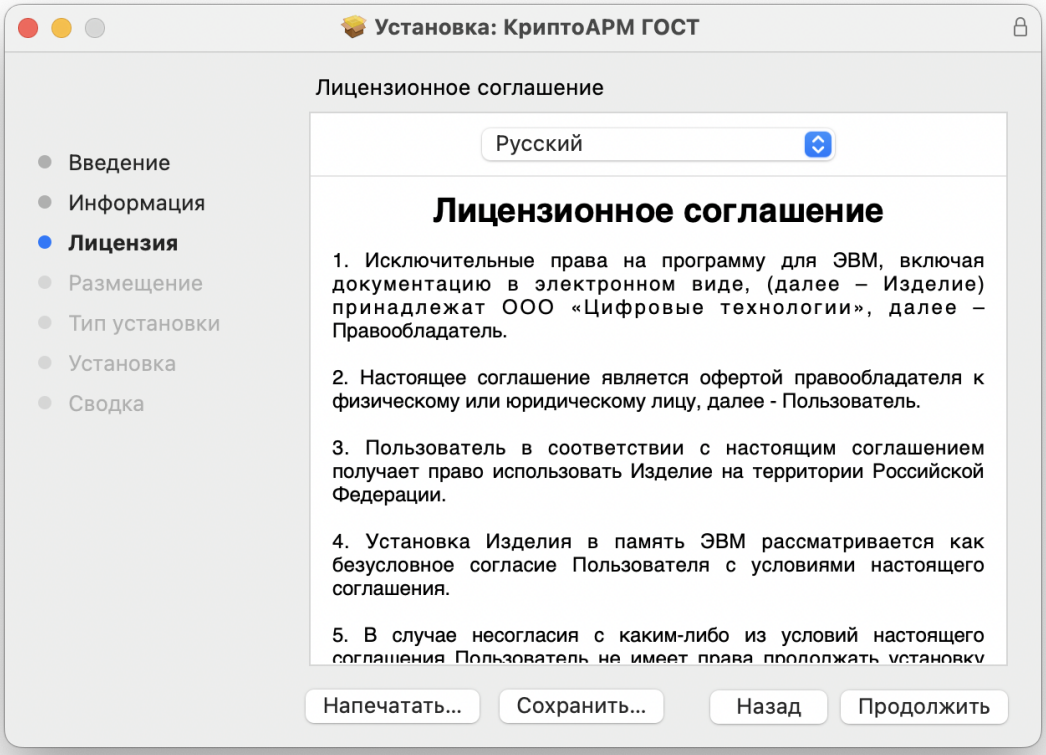
   Установочный пакет для приложения **КриптоАРМ ГОСТ** может поставляться вне образа диска. В таком случае нужно сразу запустить файл **cryptoarm-gost-vx.x.x-64.pkg** (где x.x.x – номер версии).
3. Откроется мастер установки **КриптоАРМ ГОСТ**. Для продолжения установки следует нажать кнопку **Продолжить**. На каждом шаге можно вернуться на предыдущий шаг нажатием **Назад**.



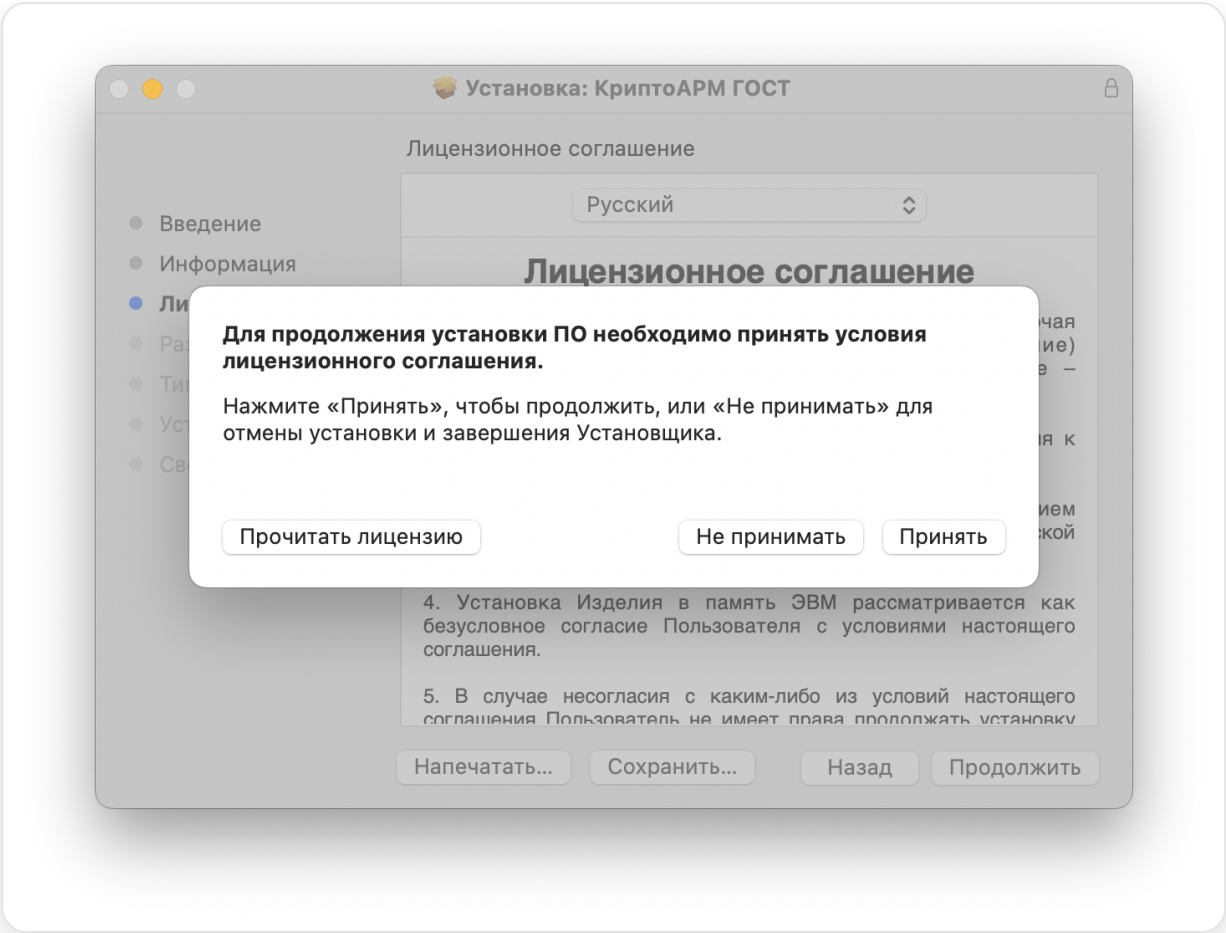
4. На следующем шаге предоставляется описание программы, которое можно распечатать или сохранить в файл. По кнопке **Продолжить** происходит переход на следующий шаг.



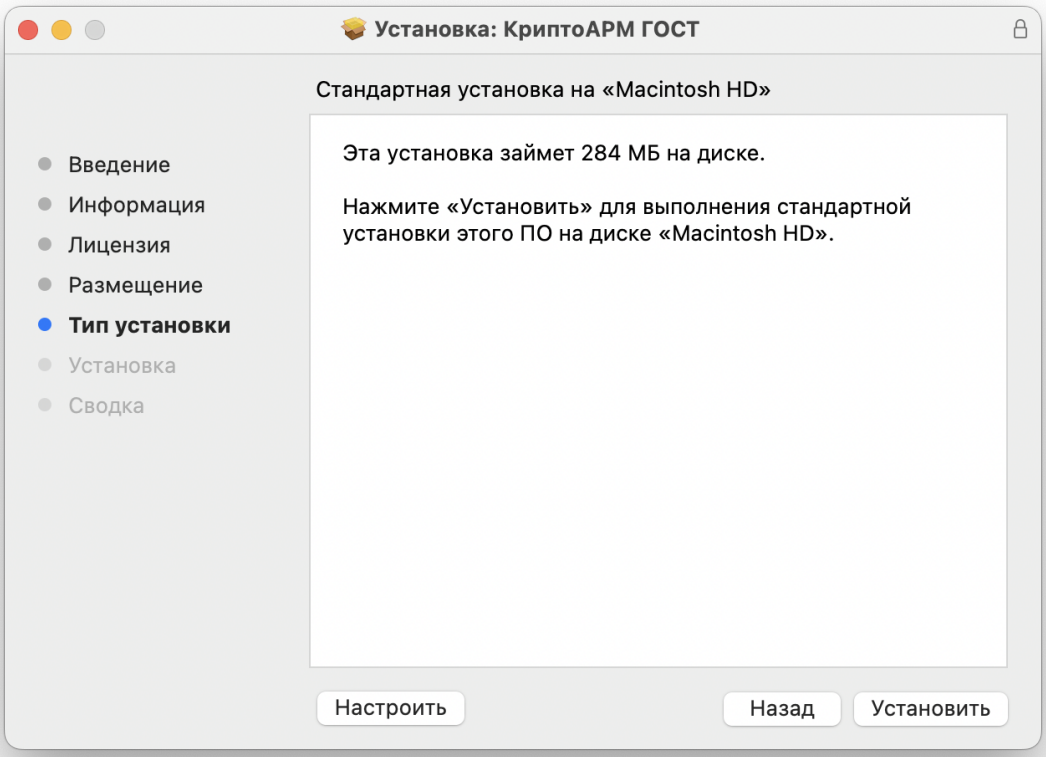
5. На этапе ознакомления с условиями лицензионного соглашения их можно распечатать или сохранить в файл.



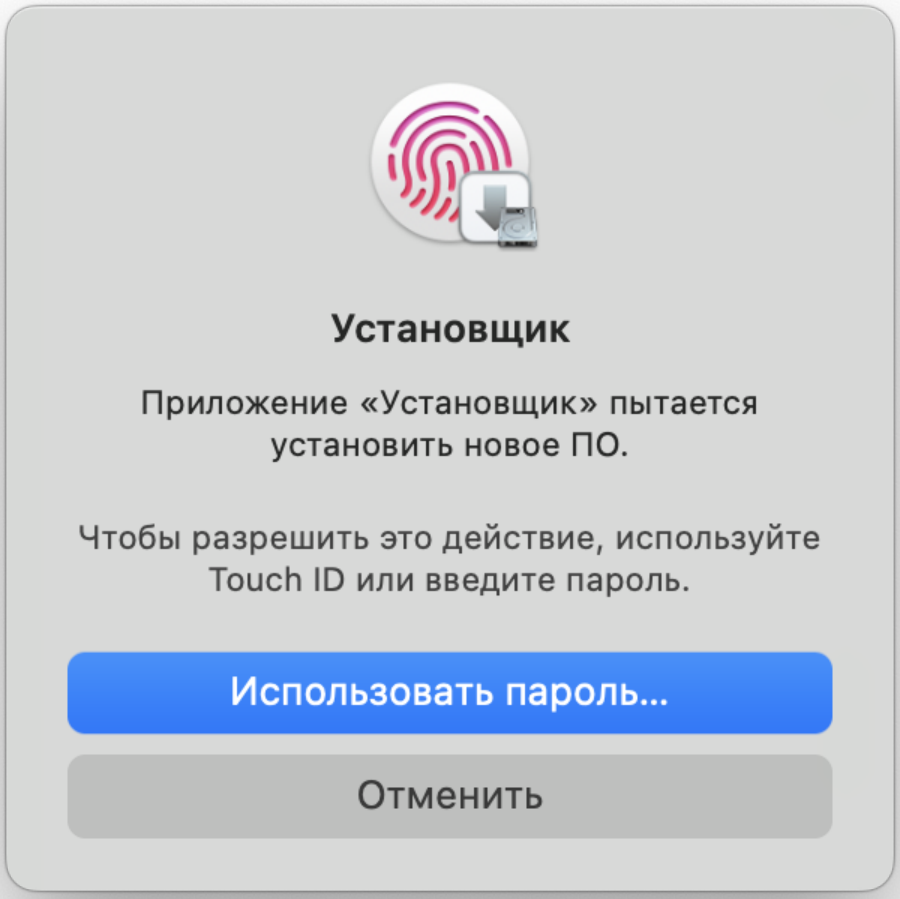
Принять условия лицензионного соглашения можно, нажав кнопку **Принять**. Установка продолжения продолжается. По кнопке **Не принимать** происходит отмена установки.

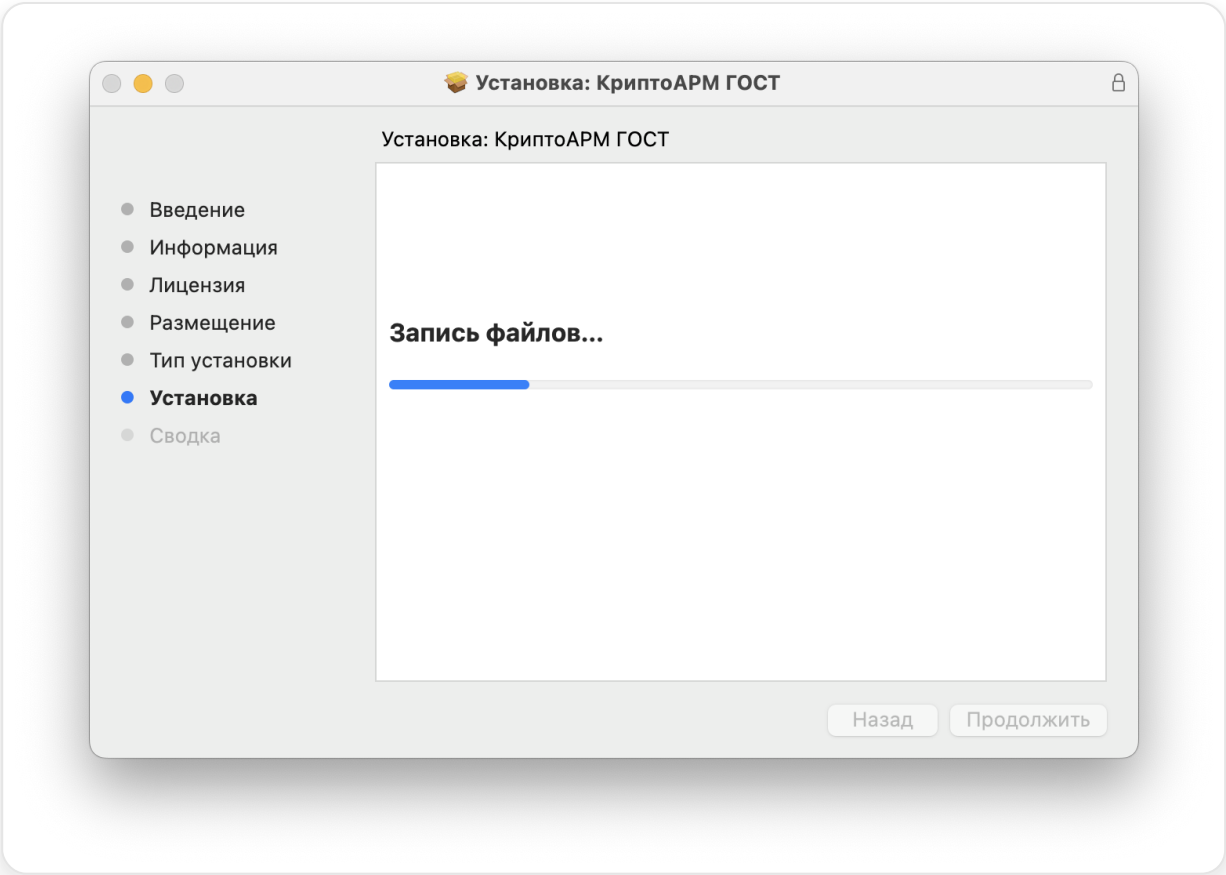


6. На последнем шаге мастера надо нажать кнопку **Установить** для завершения установки.

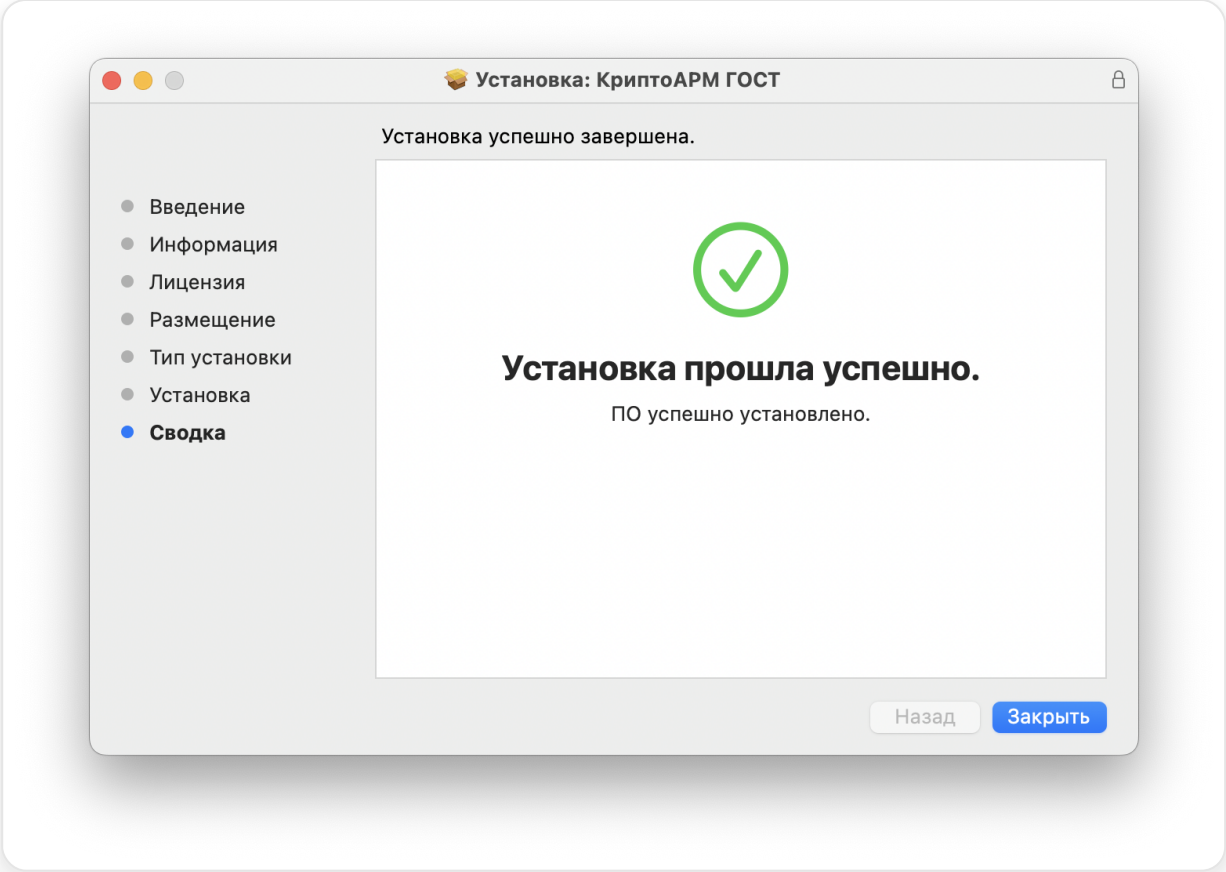


7. На запрос нужно **ввести** пароль администратора и нажать **Установить ПО**. Начнется установка программы на компьютер.


Установщик
Приложение «Установщик» пытается установить новое ПО.
Чтобы разрешить это действие, используйте Touch ID или введите пароль.
Использовать пароль...
Отменить



8. По окончании установки нужно нажать кнопку **Закрыть**.



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

Открыть статью на сайте

Установка КриптоПро CSP на Windows

КриптоПро CSP — криптопровайдер, необходимый для работы криптографических приложений и использования алгоритмов ГОСТ в операционной системе Windows.

Где скачать КриптоПро CSP

Скачать дистрибутив можно с официального сайта разработчика:

👉 https://www.cryptopro.ru/downloads

Важно перед установкой

Перед загрузкой и установкой необходимо:

- пройти регистрацию на сайте;
- принять лицензионное соглашение;
- выбрать нужную версию (актуальную или сертифицированную).

Регистрация требуется, так как КриптоПро CSP является средством криптографической защиты информации и распространяется с учётом требований законодательства.

Установка КриптоПро CSP

1. Перейдите на страницу загрузки и выберите **КриптоПро CSP**.
2. Авторизуйтесь или зарегистрируйтесь на сайте.
3. Скачайте установочный файл для Windows.
4. Запустите установщик.

При появлении запроса контроля учётных записей Windows (UAC) разрешите внесение изменений в систему.

Процесс установки

Установка выполняется автоматически:

- пользователь не участвует в процессе;
- все компоненты устанавливаются в стандартные каталоги системы;
- после завершения установка готова к использованию.

Открыть статью на сайте

Установка КриптоПро CSP на macOS

Скачать КриптоПро CSP можно с сайта разработчика — компании «КРИПТО-ПРО» — по ссылке.

На этом сайте понадобится пройти регистрацию, так как криптопровайдер является средством криптографической защиты информации, а значит его распространение подлежит учету в соответствующих государственных органах.

Выберите **КриптоПро CSP** и зарегистрируйтесь на сайте. **Согласитесь с лицензионным соглашением** и перейдите к загрузке.

Можно скачать актуальную или сертифицированную версию криптопровайдера для macOS.

После завершения загрузки двойным щелчком **распакуйте** загруженный файл macos-uni.tgz.

Войдите в распакованную папку. Установка ПО осуществляется от имени пользователя, имеющего права администратора: под учётной записью root или с использованием команды sudo.

СКЗИ КриптоПро CSP требует следующей последовательности установки: 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).

Запустите установку, выбрав в контекстном меню «Открыть».

В окне-предупреждении нажмите **Продолжить**.

Для установки следуйте указаниям мастера. **Ознакомьтесь** с лицензионным соглашением и продолжите установку, далее **Примите** условия лицензионного соглашения.

На следующем шаге выберете все установочные пакеты и нажмите **Продолжить — Установить**.

Введите имя и пароль пользователя, имеющего права администратора или учётной записи root. Начнется процесс установки.

По окончании установки **Закройте** установщик.

После первой установки КриптоПро CSP предоставляется временная лицензия на срок до 90 дней. Но если ранее программа уже устанавливалась или срок действия временной лицензии истек, то следует приобрести и установить лицензионный ключ.

Установка пакета для модулей TSP и OCSP

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

Скачать архив **Apple MacOS** по ссылке КриптоПро ЭЦП SDK 2.0 (требуется предварительная регистрация).

Установить 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.

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

Открыть статью на сайте

Установка КриптоПро CSP на Linux

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

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 https://www.cryptopro.ru/products/cades/downloads (требуется предварительная 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 https://drive.google.com/file/d/11Ts3wshs0-Fy7mc5NACKEb1x7fEu9oAy/view?usp=sharing

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 быть сообщение Operations done.

Открыть статью на сайте

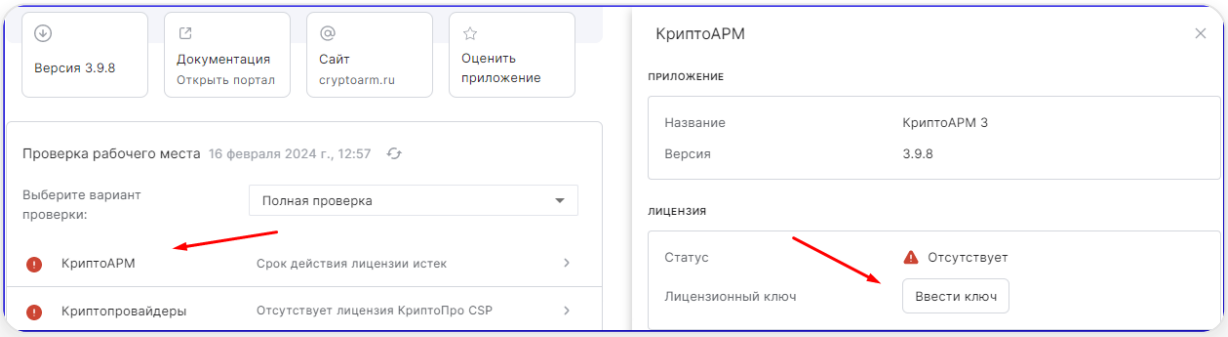
Установка лицензии КриптоАРМ ГОСТ

После установки приложения необходимо активировать лицензию, чтобы получить доступ к криптографическим функциям.

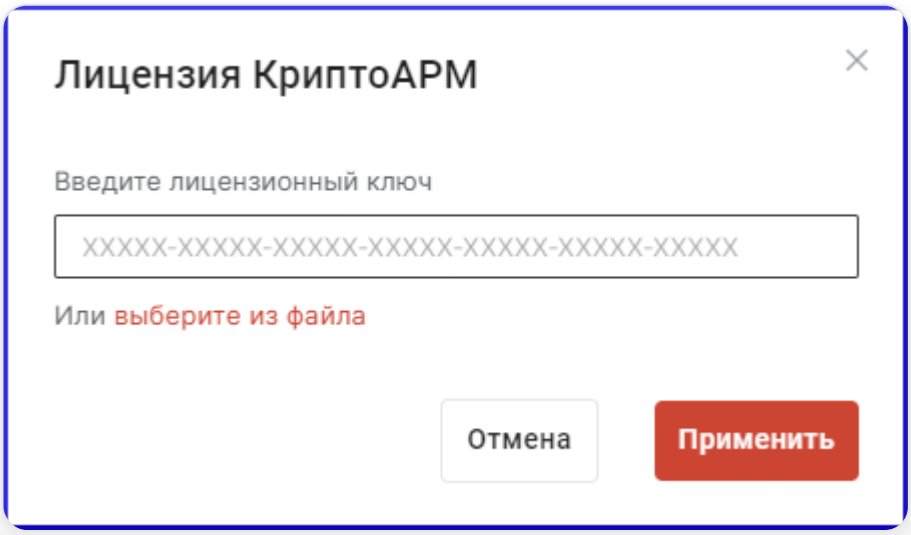
Как установить лицензию

Для установки лицензии на **КриптоАРМ ГОСТ**, необходимо выполнить следующие действия:

1. Перейти в раздел **Начальная страница**.
2. Нажать на кнопку с названием **КриптоАРМ** и в открывшемся боковом окне нажать на кнопку **Ввести ключ**.



3. В появившемся диалоговом окне ввести лицензионный ключ и нажать кнопку **Применить**.



Результат активации

После успешного ввода ключа:

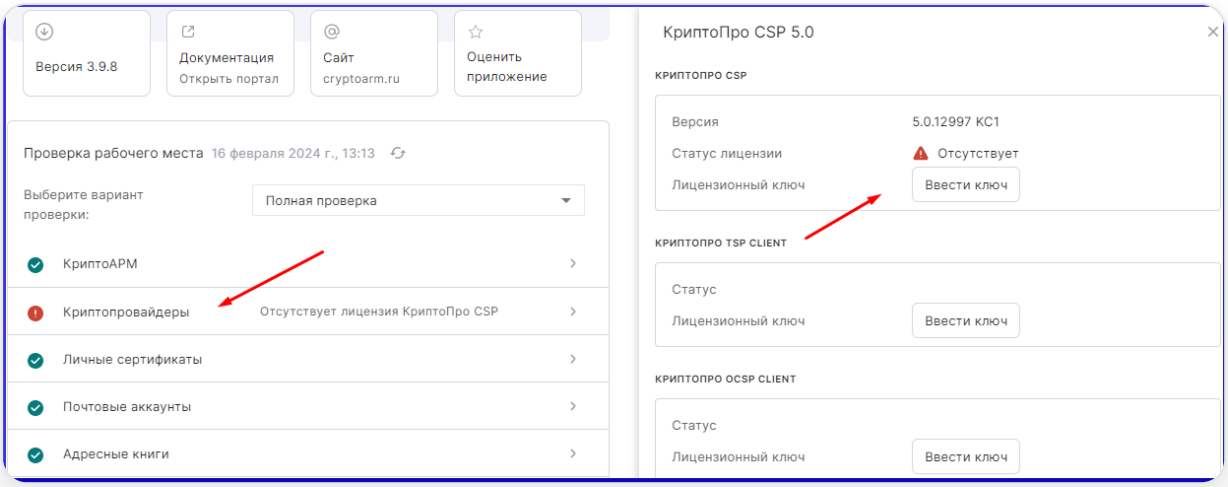
- статус лицензии обновляется;
- лицензия отображается как **Действительная**;
- становятся доступны все функции, предусмотренные вашей лицензией.

Открыть статью на сайте

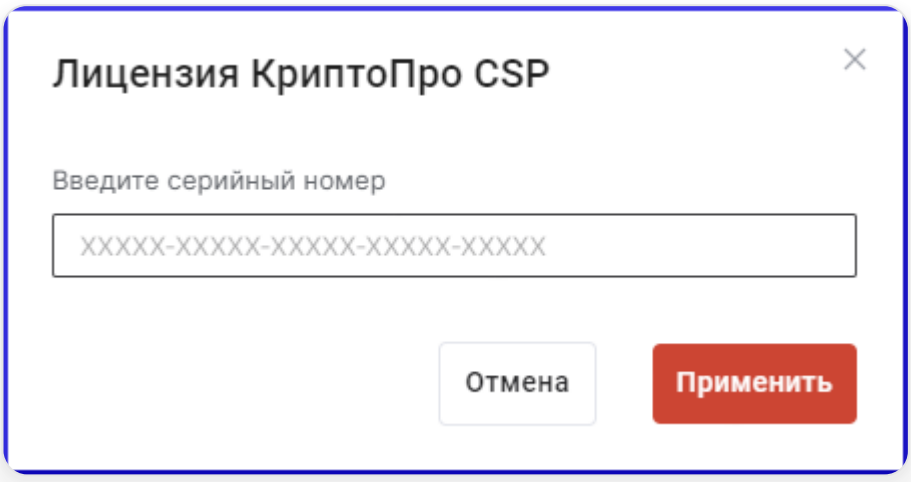
Установка лицензии КриптоПро CSP

Для установки лицензии на криптопровайдер КриптоПро CSP необходимо выполнить следующие действия:

1. Перейти в раздел **Начальная страница**
2. Нажать на кнопку с названием **Криптопровайдеры** и в открывшемся боковом окне нажать кнопку **Ввести ключ**



3. В появившемся диалоговом окне ввести лицензионный ключ и нажать кнопку **Применить**



Результат активации

После успешного ввода ключа:

- статус лицензии обновляется;

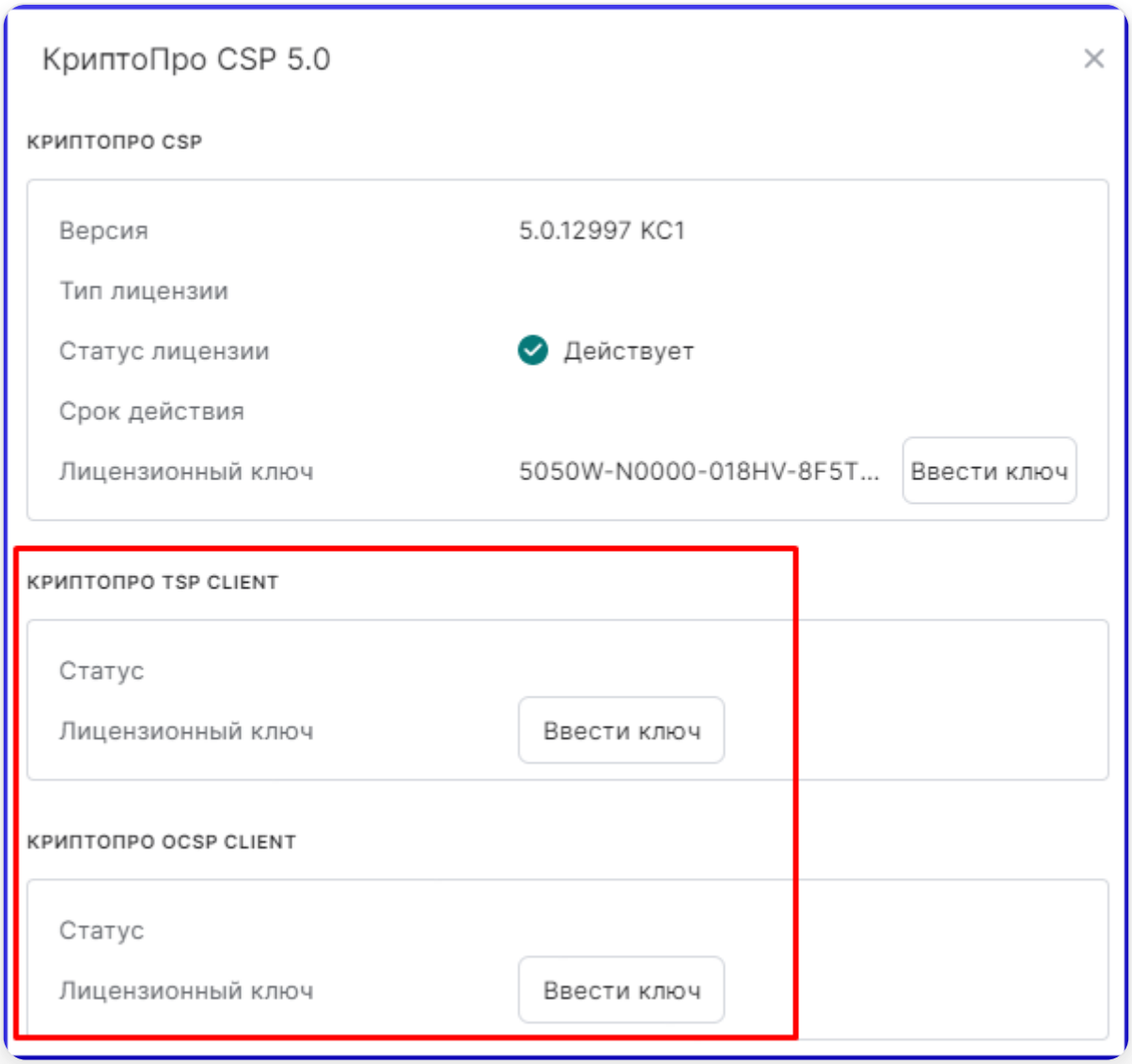
- лицензия отображается как **Действительная**;
- становятся доступны все функции, предусмотренные лицензией.

Открыть статью на сайте

Установка лицензии TSP и OCSP

Установка лицензионного ключа для модулей TSP и OCSP

Ввод лицензии на модули **TSP client** и **OCSP client** выполняется аналогично установке лицензии на **КриптоПро CSP** в боковом окне с информацией о криптопровайдерах



Открыть статью на сайте

Работа с почтой в КриптоАРМ ГОСТ

Работа с электронной почтой в **КриптоАРМ ГОСТ** начинается с раздела **Почта**. Здесь доступны функции подключения аккаунтов, управления письмами, папками, а также операции подписи и шифрования (в зависимости от лицензии).

Добавление почтового аккаунта

Чтобы начать работу:

1. Перейдите во вкладку **Почта**.
2. Нажмите кнопку добавления аккаунта в верхней части интерфейса.
3. Введите параметры почтового сервера.

После добавления аккаунта становится доступна структура папок и список писем.

Структура почтовых папок

После подключения аккаунта отображаются стандартные папки:

- **Все входящие** — письма всех подключённых аккаунтов
- **Входящие** — входящие письма текущего аккаунта (без спама)
- **Отправленные** — отправленные сообщения
- **Черновики** — сохранённые незавершённые письма
- **Корзина** — удалённые письма
- **Спам** — нежелательная почта

Если почтовый сервер содержит дополнительные папки, они также отображаются в списке.

Сохранённые письма

При удалении писем с сервера они могут сохраняться локально на устройстве. В этом случае создаётся папка:

- **Сохранённые письма**

В ней доступны следующие действия:

- открыть письмо
- удалить навсегда
- отметить прочитанным / непрочитанным

- переслать
- распечатать
- скачать
- удалить
- сохранить на сервер
- ответить

Общие действия с письмами

В списке писем доступны массовые операции:

- создание нового письма
- открытие письма в отдельной вкладке
- быстрый просмотр в боковой панели
- удаление писем (перемещение в корзину)
- отметка прочитано / непрочитано
- перемещение в папку
- обновление списка писем
- поиск и фильтрация писем

Дополнительные действия:

- удалить с сервера (с сохранением локальной копии)
- сохранить на сервер (восстановление письма на сервер)

Действия с отдельным письмом

При работе с конкретным письмом доступны:

- ответ
- ответить всем
- переслать
- распечатать
- скачать
- удалить
- удалить с сервера
- переместить в папку

Дополнительно (при наличии лицензии):

- **проверить подпись** — для подписанных писем
- **расшифровать** — для зашифрованных писем

Выбор почтового аккаунта

В верхнем правом углу раздела **Почта** доступен переключатель аккаунтов. Это позволяет быстро переключаться между несколькими подключёнными почтовыми ящиками.

Примечание

Доступность функций подписи и шифрования писем зависит от установленной лицензии **КриптоАРМ ГОСТ 3 Защищённая почта**.

Открыть статью на сайте

Как добавить почтовый аккаунт

КриптоАРМ ГОСТ поддерживает работу с популярными почтовыми сервисами, включая:

- Mail.ru
- Yandex
- Gmail
- Tegu
- iCloud
- CommuniGate Pro
- Microsoft Exchange

Чтобы начать работу с почтой, необходимо подключить почтовый аккаунт.

Добавление первого аккаунта

1. Перейдите в раздел **Почта**.
2. На правой боковой панели выберите **Добавить аккаунт**.
3. Заполните поля в новой вкладке добавления аккаунта.
4. Нажмите кнопку **Сохранить**.

> ⚠️ Для некоторых сервисов требуется создание **пароля для внешнего приложения**.

При успешном подключении добавленный аккаунт становится активным в приложении и отображается на правой боковой панели.

В списке писем отображаются все письма добавленного аккаунта с разделением по папкам.

Добавление следующего аккаунта

1. Перейдите в раздел **Почта**.
2. Откройте правую боковую панель и выберите **Добавить аккаунт**.
3. Заполните поля **Почтового аккаунта**.
4. Нажмите кнопку **Далее**.
5. Заполните поля **Дополнительно**.
6. Нажмите кнопку **Добавить**.

При успешном подключении в списке писем **Все входящие** отображаются письма всех добавленных аккаунтов.

Чтобы посмотреть письма добавленного аккаунта, нужно сделать его активным.
После этого в списке писем **Входящие** и вложенных папках отображаются все письма добавленного аккаунта.

Описание полей формы добавления аккаунта

Почтовый аккаунт

Учётные данные

Электронная почта — адрес добавляемой электронной почты. Обязательное поле.
Пароль — пароль к почтовому ящику. Обязательное поле.

Как получить пароль для внешнего приложения для почтового аккаунта:

- Яндекс.Почты;
- Gmail.com;
- Mail.ru.

Сервер входящей почты (IMAP)

- **Адрес сервера**: например `imap.gmail.com`, `imap.yandex.ru`
- **Порт**: `993`
- **Шифрование**:
  - без шифрования
  - SSL/TLS (рекомендуется)
  - SSL/TLS при обнаружении

Сервер исходящей почты (SMTP)

- **Адрес сервера**: например `smtp.gmail.com`, `smtp.yandex.ru`
- **Порт**: `465`
- **Шифрование**:
  - без шифрования
  - SSL/TLS (рекомендуется)
  - SSL/TLS при обнаружении
- **Логин** — может совпадать с email или быть его частью до символа `@`

Данные для серверов входящей и исходящей почты:

- Mail.ru;
- Yandex.ru;
- Gmail.com;
- Outlook.com;
- iCloud.

Дополнительно

- **Имя аккаунта** — имя почтового аккаунта, которое отображается в списке подключённых почтовых аккаунтов.

- **Забрать письма за** — в приложение загрузятся письма за указанный период (7 дней, 2 месяца, 3 месяца, за всё время).
- **Хранение почты** — настройки для хранения сообщений («Удалять оригиналы писем с почтового сервера», «Не удалять оригиналы писем с почтового сервера»). Письма могут быть удалены с сервера после загрузки на устройство. Для сохранения писем на сервере необходимо выбрать «Не удалять оригиналы писем с почтового сервера». По умолчанию выставлена настройка «Не удалять оригиналы писем с почтового сервера». Если активировать настройку «Удалять оригиналы писем с почтового сервера» и нажать кнопку «Добавить», то после подключения почтового аккаунта и получения всех писем оригиналы писем удаляются с почтового сервера. Все письма хранятся локально на устройстве и видны в папке «Сохранённые письма» общим списком.
- **Специальные папки** — настройка для создания локальных папок, которые будут отсутствовать на почтовом сервере. Для доступа к папкам с различных устройств необходимо выбрать «Локально и на сервере».

Если при подключении аккаунта возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку **События**. Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Ошибка аутентификации** — проверьте корректность пароля в настройках почты.
- **Ошибка синхронизации аккаунта** — в настройках почты проверьте корректность адреса электронной почты, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Как написать и отправить письмо

1. Перейдите в раздел **Почта**.
2. Подключите почтовый аккаунт, если он не был подключен.
3. На левой боковой панели нажмите кнопку **Новое сообщение**. Форма создания сообщения открывается в новой вкладке.

4. Выберите получателей («Кому», «Копия» или «Скрытая копия»).

   В поле установите курсор или начните вводить первые буквы имени/фамилии/адреса электронной почты. Открывается выпадающий список с контактами. Если подходящих контактов нет в списке, нажмите **Показать все контакты**. Открывается правая боковая панель со списком всех контактов, имеющих e-mail. Выберите контакт, нажав на него. Если у вас нет контактов, вы можете добавить контакты или просто ввести e-mail. Адреса получателей вводятся через запятую, точку с запятой, пробел. 5. Укажите тему. 6. Заполните содержимое письма.
   7. Для отправки сообщения нажмите кнопку **Отправить**.

Как оформить сообщение

Для оформления сообщения вы можете воспользоваться инструментами:

- 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).

Как работать с вложениями

Вы можете прикрепить один или несколько файлов с локального диска или выбрать из папки **Архив**.

Для добавления вложений нажмите кнопку **Прикрепить файл** и в выпадающем списке выберите место расположения вложения.

Файлы с компьютера — добавляет любые файлы с локального диска.

Из раздела Архив — позволяет выбрать файлы с локального диска из папки **Архив**.

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.

Вложение можно **Скачать** или открыть в мастере **Подпись и шифрование**, **Проверка и расшифрование**.

Сохранение черновика

Все изменения в новом сообщении автоматически сохраняются каждые 10 секунд в виде черновика.

Для перехода в раздел с черновиками выберите в левом меню стандартную папку **Черновики**.

Для черновиков вы можете выполнить следующие действия:

- **Открыть** — письмо открывается в режиме редактирования в новой вкладке. Вы можете дописать его и отправить.
- **Удалить** — черновик перемещается в папку **Корзина**.
- отметить **Прочитано/Не прочитано** выделенные письма;
- переместить **В папку** — переместить в выбранную папку писем;
- **Удалить с сервера** — удалить письмо с почтового сервера. Письмо будет доступно локально на компьютере.

Выбор подписи письма

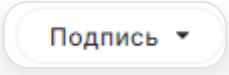
Вы можете создать подпись, которая будет автоматически подставляться в новое письмо при ответе или пересылке.

Подписи создаются в настройках почты.

По умолчанию в приложении задана дефолтная подпись с текстовкой **Отправлено из КриптоАРМ ГОСТ 3** 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.



Открывается список с подписями.

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

Если при отправке письма возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

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

Открыть статью на сайте

Просмотр письма в почте

Быстрый просмотр

Быстрый просмотр позволяет открыть письмо без перехода в новую вкладку.

Как открыть письмо

1. Перейдите в раздел **Почта**.
2. Выберите письмо в списке.
3. Нажмите иконку **Просмотр**.

Результат

Содержимое письма отобразится в правой боковой панели.

Просмотр в новой вкладке

Этот режим используется для более детального просмотра письма.

Как открыть письмо

1. Перейдите в раздел **Почта**.
2. Выберите письмо в списке.
3. Нажмите кнопку **Открыть** на верхней панели.

Результат

Письмо откроется в отдельной вкладке, где доступен полный функционал просмотра.

Открыть статью на сайте

Работа с письмами и вложениями

Как отвечать на письма и пересылать их

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. В правом верхнем углу нажмите на кнопку **Ответить** или **Ответить всем**.

Чтобы переслать письмо в правом верхнем углу нажмите на значок **Ещё** и выберите действие **Переслать**.

Форма письма открывается в новой вкладке.

Как просмотреть участников переписки

При чтении письма отображается информация с именем отправителя.

Участники переписки отображаются в поле **Кому**:

- если письмо пришло только вам, то отображается ваш e-mail адрес;
- если письмо пришло вам и кому-то еще, то для просмотра участников переписки нажмите кнопку **Еще**.

Для того чтобы скрыть список получателей, нажмите на кнопку **Скрыть**.

В поле CC отображаются все получатели поля Скрытая копия.

Как работать с вложениями во входящих письмах

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

1. Перейдите в раздел **Почта**.
2. Откройте письмо с вложениями.

Вы можете:

- Скачать все вложения одним архивом с помощью кнопки **Скачать все**.
- Открыть все вложения в одном из мастеров с помощью выпадающего меню **Открыть в**.

Вы можете посмотреть содержимое вложения, кликнув на него мышью. Документ открывается в программе по умолчанию. Если документ подписан электронной подписью и/или зашифрован, то открывается мастер обратных операций.

Открыв дополнительное меню, вы можете скачать вложение и открыть в мастерах.

Просмотр подписанных электронной подписью писем

ВАЖНО! Чтобы просматривать подписанные электронной подписью почтовые сообщения, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

Входящие письма, подписанные электронной подписью, отмечены иконкой:

- если сертификат подписи действительный;
- если сертификат недействительный.

Чтобы просмотреть детальную информацию о подписи сообщения и сертификате, наведите на иконку указатель мыши **Посмотреть свойства**. Во всплывающем окне будут видны сведения. Для просмотра сведений о владельце подписи (его персональные данные) и составе цепочки сертификации нужно нажать на кнопку **Подробнее**.

Отчёт о проверке электронной подписи можно **Распечатать**, **Обновить** и **Закрыть**.

Для недействительной подписи возможны причины:

- **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.

Вы можете обновить информацию о проверке подписи, выбрав на форме просмотра письма в меню **Еще** действие **Проверить подпись**.

Просмотр зашифрованных писем

> **ВАЖНО!** Чтобы просматривать зашифрованные почтовые сообщения, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.
>
> **ВАЖНО!** Для расшифрования зашифрованных почтовых сообщений необходима лицензия на **КриптоАРМ ГОСТ 3 Защищённая почта**.

Чтобы расшифровать письмо, нужно чтобы в **Личном хранилище** сертификатов у вас был установлен сертификат с закрытым ключом, которым будет осуществляться расшифрование.

Письма, зашифрованные отправителем, отмечены иконкой:

- если письмо расшифровано;
- если зашифровано, но невозможно расшифровать.

При наведении на иконку указателя мыши всплывает информация, что письмо зашифровано.

При открытии зашифрованного письма оно расшифровывается автоматически, если найден сертификат расшифрования и введен пароль к закрытому ключу.

Вы можете повторить расшифрование, если на форме просмотра письма в меню **Еще** выберите действие **Расшифровать** во всплывающем списке, которое отображается для зашифрованных писем.

Просмотр подписанных и зашифрованных писем

> **ВАЖНО!** Чтобы просматривать подписанные и зашифрованные почтовые сообщения, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.
>
> **ВАЖНО!** Для расшифрования зашифрованных почтовых сообщений необходима лицензия на **КриптоАРМ ГОСТ 3 Защищённая почта**.

Чтобы расшифровать письмо, нужно чтобы в **Личном хранилище** сертификатов у вас был установлен сертификат с закрытым ключом, которым будет осуществляться расшифрование.

Письма, подписанные и зашифрованные отправителем, отмечены иконкой:

- если письмо расшифровано;
- если зашифровано, но невозможно расшифровать.

При наведении на иконку указателя мыши всплывает информация, что письмо зашифровано.

При открытии зашифрованного письма оно расшифровывается автоматически, если найден сертификат расшифрования и введен пароль к закрытому ключу.

При наведении на иконку расшифрованного и подписанного письма отображается информация о подписи.

Как скачать письмо на компьютер

Письма можно скачивать на компьютер. Скачанное письмо можно прикрепить в виде файла к другому письму и отправить.

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на значок **Еще** и выберите действие **Скачать письмо** во всплывающем списке.

Письмо скачивается в формате EML.

Как распечатать письмо

1. Перейдите в раздел **Почта**.
2. Откройте письмо.
3. Нажмите на значок **Еще** и выберите действие **Распечатать** во всплывающем списке.

Просмотр цепочек писем

Если вы ведете активную переписку, включите группировку писем в цепочки.

В списке у таких писем отображается индикатор количества писем в цепочке.

Чтобы посмотреть любое письмо из цепочки, нажмите на строку с этим письмом в области просмотра письма.

Вы можете **Переслать все**, **Раскрыть все** письма цепочки (раскрывает или скрывает все письма в цепочке), **Распечатать**, выбрав в строке с темой действие.

Как переместить письмо в папку

1. Открыть раздел **Почта**.
2. Выделить письмо.
3. В верхней панели действий нажать **В папку**.
4. В правой боковой панели выбрать папку, в которую нужно переместить письмо.

Письмо перемещено в указанную папку.

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

Сортировка писем

Письма можно сортировать по отправителю (столбец **От**), по теме (столбец **Тема**), по дате (столбец **Дата**). Для этого нужно нажать на название столбца.

Открыть статью на сайте

Как отправить подписанное и зашифрованное сообщение

> **ВАЖНО!** Чтобы подписывать или зашифровывать почтовые сообщения, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.
>
> **ВАЖНО!** Для подписи, шифрования и расшифрования почтовых сообщений необходима лицензия на **КриптоАРМ ГОСТ 3 Защищённая почта**.

1. Перейдите в раздел **Почта**.
2. Подключите почтовый аккаунт, если он не был подключен.
3. На левой боковой панели нажмите кнопку **Новое сообщение**. Форма создания сообщения открывается в новой вкладке.
4. Выберите получателей («Кому», «Копия» или «Скрытая копия»).

   В поле установите курсор или начните вводить первые буквы имени/фамилии/адреса электронной почты. Открывается выпадающий список с контактами. Если подходящих контактов нет в списке, нажмите **Показать все контакты**. Открывается правая боковая панель со списком всех контактов, имеющих e-mail. Выберите контакт, нажав на него. Адреса получателей вводятся через запятую или точку с запятой.
5. Укажите тему.
6. Заполните содержимое письма.
7. Настройте добавление электронной подписи к письму и/или шифрование писем.
8. Для отправки сообщения нажмите кнопку **Отправить**.

Как настроить добавление электронной подписи к письму

Чтобы подписывать письма электронной подписью, нужно:

- установить в **Личное хранилище** сертификат с закрытым ключом;
- в настройках почты выбрать сертификат подписи из **Личного хранилища** сертификатов;
- включить подпись писем.

При отправке письма будут подписываться.

Как выбрать сертификат подписи

1. Откройте форму редактирования настроек почты и выберите раздел **Безопасность**.

2. В разделе **Сертификат подписи** нажмите **Выбрать сертификат**. Если сертификат выбран, его можно заменить.
3. В открывшейся правой боковой панели выберите сертификат подписи из списка, нажав на иконку сертификата. Сертификат добавляется в раздел **Сертификат подписи**. Если в правой боковой панели в списке нет сертификатов, то вы можете его импортировать, создать или установить.
4. После выбора сертификата закройте правую боковую панель.
5. Для фиксации изменений в настройках аккаунта нажмите кнопку **Сохранить**.

Как включить подпись писем

Настройку подписи писем вы можете включить при создании нового сообщения, выбрав опцию **Подписать** по кнопке **Безопасность**.

Вы можете настроить подпись писем по умолчанию для каждого нового письма. Для этого:

1. Откройте форму редактирования настроек почты и выберите вкладку **Безопасность**.
2. В разделе **Безопасность электронной почты** установите флаг **Добавлять электронную подпись к исходящим сообщениям**.
3. Для фиксации изменений в настройках аккаунта нажмите кнопку **Сохранить**. В таком случае в новом сообщение опция **Подписать** по кнопке **Безопасность** будет включена.

Как настроить шифрование письма и вложений

Чтобы шифровать письма и вложения нужно в получателях письма («Кому», «Копия» или «Скрытая копия») выбрать контакты, у которых добавлен сертификат, и включить шифрование писем.

Если письмо содержит вложения, то они будут зашифрованы вместе с письмом.

> **Как добавить сертификат к контакту** читайте в инструкции.

Как включить шифрование писем

Настройку шифрования писем вы можете включить при создании нового сообщения, выбрав опцию **Зашифровать** по кнопке **Безопасность**.

Вы можете настроить шифрование писем по умолчанию для каждого нового письма. Для этого:

1. Откройте форму редактирования настроек почты и выберите вкладку **Безопасность**.
2. В разделе **Безопасность электронной почты** установите флаг **Шифровать содержимое и вложения исходящих сообщений**.
3. Для фиксации изменений в настройках аккаунта нажмите кнопку **Сохранить**. В таком случае в новом сообщение опция **Зашифровать** по кнопке **Безопасность** будет включена.

Шифрование писем в свой адрес

Для шифрования писем в свой адрес необходимо:

1. Создать контакт с адресом своей электронной почты.
2. Привязать к созданному контакту свой сертификат электронной подписи.
3. В разделе **Почта** на левой боковой панели нажать кнопку **Новое сообщение**. Форма создания сообщения открывается в новой вкладке.
4. Выбрать получателей (созданный контакт).
5. Указать тему.
6. Заполнить содержимое письма.
7. Настроить шифрование писем.
8. Для отправки сообщения нажать кнопку **Отправить**.

Как настроить подпись и шифрование письма

Если вам требуется отправить подписанное электронной подписью и зашифрованное письмо:

- настройте **добавление электронной подписи к письму**.
- настройте **шифрование письма и вложений**.

> **Примечание:** если в списке получателей письма контакты или адреса электронной почты подсвечиваются красным цветом, проверьте, есть ли у этих получателей привязанные сертификаты.

Если при отправке письма возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Укажите получателей письма в полях Кому, Копия или Скрытая копия** — проверьте заполнение указанных полей.
- **Адреса user@aa не распознаны. Проверьте правильность ввода адресов** - проверьте электронные адреса получателей на корректность.
- **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.
- **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.

- **Один или несколько сертификатов отсутствуют** — проверьте наличие сертификатов у получателей, добавьте сертификаты к контактам и повторите отправку письма.
- **Не удалось отправить сообщение** — проверьте подключение к Интернету.

Открыть статью на сайте

Как настроить почту

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

Как перейти в настройки почты

1. Перейдите в раздел **Почта**.
2. Откройте правую боковую панель и в списке наведите курсор на почтовый аккаунт, настройки которого надо изменить.
3. Нажмите всплывающую иконку **Настройки**.

На боковой панели открывается форма просмотра настроек аккаунта.

Настройки почты состоят из вкладок:

- **Безопасность** — отображает параметры управления подписанными и зашифрованными сообщениями.
- **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.

Как редактировать настройки

1. В форме просмотра настроек аккаунта нажмите кнопку **Редактировать**. Форма редактирования открывается в новой вкладке.
2. Выберите одну из вкладок.
3. Внесите изменения.
4. После редактирования нужных параметров нажмите кнопку **Сохранить**.

Описание настроек безопасности

На форме редактирования настроек аккаунта выберите вкладку **Безопасность**.

Безопасность электронной 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 почты выбран сертификат подписи.

Сертификат подписи

Привязанный сертификат используется по умолчанию при подписи писем. Вы может выбрать только один сертификат подписи из хранилища личных сертификатов.

Если у вас нет личного сертификата, вы можете установить его, в том числе импортировав, или создать.

Отображать информацию об электронной подписи в исходящих письмах — при отправке подписанного письма информация о сертификате, его владельце и сроке действия автоматически добавляется в письмо и будет видно получателям писем, на устройствах которых не установлено приложение **КриптоАРМ ГОСТ 3 Защищённая почта**.

Шифрование исходящих писем

- **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.

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.

Описание настроек подключения почтового аккаунта

На форме редактирования настроек аккаунта выберите вкладку **Подключение**.

Вы можете редактировать все поля **Электронная почта**, **Пароль**, **Сервер входящей почты**, **Сервер исходящей почты**, **Имя аккаунта**, **Забрать письма за**, **Специальные папки**.

Редактирование имени не влияет на подключение.

При изменении адреса электронной почты список писем обновляется для нового адреса.

После смены пароля вы автоматически выйдете из аккаунта. Если вы ввели правильный пароль, письма аккаунта обновятся.

При увеличении периода, за который необходимо загрузить письма, в раздел **Почта** подгрузятся более старые сообщения.

При редактировании параметров **Сервер входящей почты**, **Сервер исходящей почты** письма подключенного аккаунта останутся в списке, но не будет синхронизации с почтовым сервером. Вы не увидите новых писем и не отправите свои.

Описание общих настроек

На форме редактирования настроек аккаунта выберите вкладку **Общие**.

Обработка сообщений

- Группировать письма в цепочки — при включенной опции письма группируются в цепочки по теме письма.
- Отображение изображений в письмах — если у вас низкая скорость интернет-соединения или вы хотите сэкономить трафик, отключите показ картинок по умолчанию.

  > **Примечание:** чтобы посмотреть изображения в письме, нажмите **Показать один раз** для отображения изображений в текущем письме или **Всегда показывать от ...** для постоянного отображения изображений от этого пользователя.

  Важно! не реализовано в текущей версии. Изображения в письмах отображаются всегда.
- **Отмечать как прочитанное при просмотре в области чтения** — при установленном флаге при быстром просмотре сообщения оно помечается как прочитанное.

Запрос уведомлений

- **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.

Отправка уведомлений о прочтении

- Всегда отправлять уведомления о прочтении для любого полученного сообщения.
- Никогда не отправлять уведомления о прочтении.
- Каждый раз спрашивать, следует ли отправить уведомление о прочтении.

Вы можете выбрать только одну опцию, настроив отправку/запрет на отправку уведомлений о прочтении письма.

Описание настроек подписи писем

На форме редактирования настроек аккаунта выберите вкладку **Подписи**.

Вы можете создать подпись, которая будет автоматически подставляться в новое письмо, а также при ответе или пересылке.

По умолчанию в приложении задана дефолтная подпись с текстовкой **Отправлено из КриптоАРМ ГОСТ 3** и ссылкой на магазин cryptoarm.ru.

Создание подписи

Создание новой подписи доступно по кнопке **Добавить**.

Укажите название и содержимое подписи.

При установке флага **По умолчанию** данная подпись будет добавлена в новое сообщение.

Флаг **Добавлять перед цитируемым текстом в ответных письмах** позволит добавить подпись сразу после текста ответа, а не в конце всех писем в цепочке.

Оформление подписи

Содержимое текста можно редактировать: выбрать стиль и размер шрифта, выделить текст курсивом, жирным, подчеркнутым, зачеркнутым.

Помимо текста вы можете вставить в подпись:

- Изображение. Формат изображения может быть .jpeg, .jpg, .png, .gif, максимальный размер — 1024x1024 пикселей, максимальный объем: 2 МБ.

- Ссылку.
  Для добавления ссылки выделите текст, нажмите кнопку **Добавить ссылку**, в появившемся окне укажите адрес ссылки.
  Вы можете удалить ссылку из подписи, выделив текст и нажав кнопку **Удалить ссылку**.

Удаление подписи

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

Сортировка писем

Правила обработки входящей почты позволяют сортировать входящие сообщения по папкам, пересылать письма на другой адрес и настраивать автоответчик.

Для сортировки писем необходимо:

1. нажать **Добавить правило**;
2. ввести название правила;
3. добавить условие;
4. указать выполняемое действие;
5. нажать **Создать**.

Можно выбрать следующие условия:

- от кого;
- кому;
- тема письма;
- содержание письма;
- дата получения;
- название вложения;
- статус;
- размер;
- ко всем входящим письмам.

Выбранные условия могут содержать/не содержать/совпадать/не совпадать с введённым значением.

Можно выполнить следующие действия:

- 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.

Созданные правила можно удалить по-отдельности или вместе, редактировать или переместить между собой.

Рассылка файлов

Данная настройка позволяет добавить автоматическую рассылку файлов в виде почтовых писем.

Для создания рассылки файлов необходимо:

1. нажать **Добавить рассылку**;
2. указать название рассылки;
3. выбрать папки для сканирования с устройства, из которых будут взяты файлы для рассылки. В рассылку попадут файлы только из корневой папки;
4. написать сопроводительное письмо, указав получателей, тему и текст;
5. при необходимости активировать функции **Отследить доставку письма** и **Запросить подтверждение о прочтении письма**;
6. дополнительно можно указать, что должно быть с файлами, которые были отправлены: файлы могут быть удалены с устройства либо перемещены в выбранную папку. Файлы, которые не удалось отправить, можно удалить, оставитьв исходной папке либо переместить в выбранную папку;
7. **Запустить рассылку активной** — сканирование папок запустится после сохранения рассылки при следующем обмене с почтовым сервером;
8. **Сохранить** настройки для рассылки.

Рассылки можно удалить по-отдельности или вместе, редактировать и переместить между собой.

Если при сохранении аккаунта возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Ошибка аутентификации** — проверьте корректность пароля в настройках почты.
- **Ошибка синхронизации аккаунта** — в настройках почты проверьте корректность адреса электронной почты, настройки сервера входящей и исходящей почты.

Открыть статью на сайте

Работа с уведомлениями о доставке и прочтении

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

Уведомление о прочтении подтверждает открытие отправленного сообщения.

Чтобы использовать уведомления о доставке и прочтении письма, нужно включить запрос уведомлений в настройках почты или при создании нового сообщения.

Как настроить уведомления о доставке и прочтении

1. Откройте форму создания нового сообщения.
2. Выберите опцию **Уведомить о доставке** и/или **Уведомить о прочтении** по кнопке **Уведомления**.

Как настроить уведомления о доставке и прочтении

1. Откройте форму редактирования настроек почты и выберите вкладку **Общие**.
2. В разделе **Запрос уведомлений** установите флаг **Запрашивать уведомление о доставке для всех исходящих сообщений** и/или **Запрашивать уведомление о прочтении для всех исходящих сообщений**.
3. Нажмите **Сохранить** для фиксации изменений в настройках аккаунта.

   В таком случае в новом сообщении опция **Запрашивать уведомление о доставке для всех исходящих сообщений** и/или **Запрашивать уведомление о прочтении для всех исходящих сообщений** по кнопке **Уведомления** будет включена.

Уведомления о доставке направляются отправителю автоматически почтовым сервисом при отправке письма на сервер адресата.

Как посмотреть результат уведомления о доставке и прочтении

Посмотреть результат уведомлений вы можете в папке **Отправленные**.

На панели с письмами отображается несколько статусов:

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

- Доставлено всем
- Доставлено не всем получателям.

Вы можете посмотреть детальную информацию о доставке/прочтении писем, кликнув курсором мыши на статусы.

Открыть статью на сайте

Группировка сообщений в цепочки

Вы можете выбрать, показывать ли каждое новое сообщение по отдельности или группировать переписку в цепочки.

Переписка группируется в цепочки, показывая новые ответы ниже предыдущих сообщений.

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

Как включить группировку писем в цепочки

1. Перейдите в раздел **Почта**.
2. Откройте форму редактирования настроек почты и выберите вкладку **Общие**.
3. В разделе **Обработка сообщений** установите флаг **Группировать письма в цепочки**.
4. Для фиксации изменений в настройках аккаунта нажмите **Сохранить**.

Для отключения группировки писем в цепочке выключите флаг **Группировать письма в цепочки**.

Открыть статью на сайте

Как отметить сообщение как прочитанное или непрочитанное

Чтобы не забыть прочитать сообщение позже, отметьте его как непрочитанное либо отметьте его как прочитанное, если оно не требует вашего внимания.

Как отметить письмо как прочитанное или непрочитанное

1. Перейдите в раздел **Почта**.
2. Выделите письмо в списке нажатием курсора.
3. В верхней панели действий с письмами нажмите кнопку **Прочитано** или **Не прочитано**.

Как отметить выделенные письма как прочитанные

1. Перейдите в раздел **Почта**.
2. Выберите письма, установив флаг для каждого письма, или выделите все письма, установив флаг в левом верхнем углу списка.
3. На верхней панели действий с письмами нажмите кнопку **Прочитано** или **Не прочитано**.

Открыть статью на сайте

Как удалять и восстанавливать письма

Удаленные сообщения хранятся в корзине.

Как удалить отдельное письмо

1. Перейдите в раздел **Почта**.
2. Выделите письмо в списке нажатием курсора.
3. В верхней панели действий с письмами нажмите на кнопку **Удалить**.

Как удалить одно письмо из цепочки

1. Откройте письмо.
2. Выберите письмо в цепочке, которое хотите удалить.
3. Нажмите на значок **Ещё** и нажмите во всплывающем списке действий кнопку **Удалить письмо**.

Как удалить несколько писем сразу

1. Перейдите в раздел **Почта**.
2. Установите флажки слева от писем.
3. В верхней панели нажмите на кнопку **Удалить**.

Как удалить все письма

1. Перейдите в раздел **Почта**.
2. Выберите все письма, активировав флаг **Выбрать все** с левой стороны на панели действий со списком писем.
3. На панели действий со списком писем нажмите кнопку **Удалить**.

Как посмотреть содержимое корзины

1. Перейдите в раздел **Почта**.
2. В левом боковом меню выберите **Корзина**.

Как очистить корзину

1. Перейдите в раздел **Почта**.
2. В левом боковом меню выберите **Корзина**.

3. Установите флажки напротив писем, которые хотите навсегда удалить, и нажмите **Удалить навсегда**.

Примечание: параметр **Удалить навсегда** доступен только в корзине. Чтобы удалить все сообщения в корзине, выделите все письма в корзине и нажмите на кнопку **Удалить навсегда** на панели действий.

Как восстановить удаленные письма

После переноса письма в корзину его можно восстановить.

1. Перейдите в раздел **Почта**.
2. В левом боковом меню выберите **Корзина**.
3. Установите флажки напротив писем, которые нужно восстановить.
4. В верхней панели нажмите на кнопку **В папку**.
5. В правом боковом меню выберите нужную папку.

Как удалить письмо с сервера

1. Перейдите в раздел **Почта**.
2. Выделите письмо в списке нажатием курсора.
3. В верхней панели действий с письмами нажмите на кнопку **Ещё — Удалить с сервера**.

Письмо удалено с сервера (его не видно при просмотре почтового аккаунта через браузер), но хранится локально на устройстве в папке **Сохранённые письма**.

Для удаления письма с устройства в папке **Сохранённые письма** выбрать письмо и нажать в верхней панели на кнопку **Удалить навсегда**.

Открыть статью на сайте

Как удалить почтовый аккаунт

1. Перейдите в раздел **Почта**.
2. Откройте правую боковую панель и в списке наведите курсор на почтовый аккаунт, который хотите удалить.
3. Нажмите всплывающую иконку **Настройки**.
4. На правой боковой панели в форме просмотра настроек аккаунта нажмите кнопку **Удалить**.
5. Подтвердите удаление.

В случае использования настройки «Не удалять оригиналы писем с почтового сервера» аккаунт удаляется. Письма и папки аккаунта удаляются из списка.

В случае использования настройки «Удалять оригиналы писем с почтового сервера» после подтверждения удаления проверяется наличие писем, удалённых с сервера. Если есть хотя бы одно такое письмо, то при удалении почтового аккаунта можно выбрать, сохранить или удалить такое письмо:

- **Нет, удалить** — все письма удаляются навсегда.
- **Да, сохранить** — все письма этого аккаунта сохраняются в папку Сохранённые письма, а аккаунт удаляется из списка подключённых аккаунтов.

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

Открыть статью на сайте

Поиск писем

1. Перейдите в раздел **Почта**.
2. Введите в поле поиска параметры поиска.

Критерии быстрого поиска

Быстрый поиск ведется:

- по имени отправителя;
- по имени получателей;
- по теме;
- по содержанию письма.

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**.

Критерии расширенного поиска

Расширенный поиск ведется:

- 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**.

Открыть статью на сайте

Переключение аккаунтов почты

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

Чтобы изменить активный аккаунт:

1. Перейдите в раздел **Почта**.
2. Для открытия правой боковой панели нажмите на выбранный активный аккаунт.
3. Наведите курсор на аккаунт, который хотите сделать активным, и нажмите на его иконку.

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

Открыть статью на сайте

Описание раздела «Документы»

Здесь представлен список документов специального каталога, который предназначен для сохранения архивной копии результатов выполнения операций. Документы данного списка расположены в папке пользователя в каталоге **\.Trusted\CryptoARM GOST 3\Documents**.

В левой боковой панели доступна возможность вызвать мастер **Подписи и шифрования** или **Проверки и расшифрования** для выполнения прямых и обратных операций с документами.

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

> **ВАЖНО!** Для подписи и расшифрования электронных документов необходима лицензия на КриптоАРМ ГОСТ 3 или на КриптоАРМ ГОСТ 3 Защищённая почта.

Работа с документами

Во вкладке **Архив** отображаются документы специального каталога, расположенного в вашей домашней папке в каталоге **\.Trusted\CryptoARM GOST 3\Documents**.

Вы можете добавить файлы в этот каталог через интерфейс приложения. Также в этой папке отображаются результаты выполнения операций (подписанные и (или) зашифрованные файлы).

Документы в эту папку вы всегда можете сохранить стандартными программами ОС.

Вы можете просмотреть содержимое документа, информацию о документе, удалить документы из списка, отправить в почтовом сообщении, перейти в папку расположения файла.

Также вы можете открыть выбранные документы в мастере **Подписи и шифрования** или **Проверки и расшифрования** для выполнения операций.

Во вкладке **Архив** или в мастере вы можете создавать и выбирать профили подписи, предназначенные для быстрого управления настройками операций.

ВАЖНО! Чтобы подписывать, проверять подпись, зашифровывать и расшифровывать документы, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

Открыть статью на сайте

Как создать профиль подписи

Чтобы оперативно выполнять операции, вы можете устанавливать специальные профили — шаблоны, индивидуальные настройки.

Для каждой ситуации можно создать и использовать собственный профиль для выполнения операций подписи, архивирования, шифрования. Для обмена документами с бухгалтером вы можете установить и использовать один профиль, с партнерами — второй, с клиентами — третий.

Создать профиль вы можете в разделе **Документы** — **Архив**, в мастере прямых или обратных операций или в разделе **Сертификаты**.

Как создать профиль из раздела Документы

1. Выберите в **Меню** раздел **Документы**.
2. Откройте правую боковую панель и выберите **Добавить профиль подписи**.
3. Заполните поля профиля.
4. Нажмите кнопку **Сохранить**.

Как создать профиль в мастере прямых или обратных операций

1. Перейдите в мастер **Подписи и шифрования** или **Проверки и расшифрования**.
2. Откройте правую боковую панель и выберите **Добавить профиль подписи**.
3. Заполните поля профиля.
4. Нажмите кнопку **Сохранить**.

Как создать профиль из раздела Сертификаты

1. Открыть раздел **Сертификаты**, хранилище **Личные сертификаты**.
2. В списке личных сертификатов выделите сертификат.
3. В верхней панели действий откройте дополнительное меню и выберите **Создать профиль подписи**.
4. В новой вкладке создания профиля выберите операцию **Подпись** и сертификат подписи. Заполните другие поля.
5. Нажмите кнопку **Сохранить**.

Описание полей профиля

- **Имя профиля** — обязательное для заполнения (название заполнено по умолчанию);
- **Операции** — подпись, архивирование, шифрование. Выделите нужные операции;

- **Сохранение результатов** — вы можете задать путь для сохранения результатов операций. Если параметр не задан, то файлы сохраняются рядом с исходными. Так же вы можете сохранить копию файла, полученного в результате операции, в папке **Архив**, установив флаг **Создавать копию файлов в Архиве**. Файлы данного каталога отображаются в папке **Архив**.

В зависимости от выбранных параметров в окне создания профиля станут доступны дополнительные поля.

- **Операция Подпись**.

  Доступные поля:

- **Сертификат подписи** — для выбора доступны личные сертификаты с привязкой к закрытому ключу;

- **Стандарт подписи** — CAdES-BES для создания классической подписи, CAdES-T для создания подписи со штампом времени, CAdES-X Long Type 1 для усовершенствованной подписи, CAdES-A для длительного хранения. При выборе стандартов CAdES-T, CAdES-X Long Type 1, CAdES-A или при включении штампов времени требуется заполнить поле **Служба штампов времени (TSP)**.
- **Кодировка подписи** — сохранение подписи в одной из двух кодировок BASE64 или DER.
- **Вид подписи** — присоединённая или отсоединённая.
- **Формат файла подписи** — выбор расширения для подписываемых документов в форматах .sig, .p7s, .sgn, .sign, .bin.
- **Штамп времени на подпись** – предназначен для создания подписи со штампом времени на подпись. При включении опции требуется заполнить поле **Служба штампов времени (TSP)**. Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Штамп времени на подписанные данные** – предназначен для создания подписи со штампом времени на данные. При включении опции требуется заполнить поле **Служба штампов времени (TSP)**. Данная опция доступна только при установленном модуле КриптоПро TSP Client.
- **Служба штампов времени (TSP)** — адрес службы штампов времени, который можно узнать у поставщика услуг. Например, услуги службы штампов времени могут предоставлять Удостоверяющие центры.
- **Служба онлайн статусов (OCSP)** — адрес службы OCSP. Поле отображается, если выбран стандарт подписи CAdES-X Long Type 1. Данное поле не обязательно для заполнения, чаще адрес прописан в самом сертификате, которым создается подпись.

- **Использовать прокси-сервер** – если при подключении к службам TSP или OCSP используется прокси-сервер, то установка флага активирует его настройки: Адрес прокси-сервера, Логин, Пароль, которые можно узнать у системного администратора.

- **Операция архивирование**.
  Для данной операции нет дополнительных настроек.

- **Операция Шифрование**.

  Доступные поля:

- **Сертификат шифрования** — для выбора доступны личные сертификаты, сертификаты других пользователей и контакты, у которых есть привязка к сертификату.

- **Алгоритм шифрования** – файл шифруется по одному из алгоритмов: ГОСТ 28147-89, ГОСТ Р 34.12-2015 Магма, ГОСТ Р 34.12-2015 Кузнечик. Данный параметр доступен для выбора только начиная с версии КриптоПро CSP 5.0.11635.
- **Кодировка файлов** — сохранение зашифрованного файла в одной из двух кодировок BASE64 или DER.
- **Удалить исходные файлы после шифрования** — исходные файлы в случае успешного завершения операции удаляются из файловой системы.

Открыть статью на сайте

Как просмотреть информацию о документе

Просмотреть информацию о документе вы можете в разделе **Документы** — вкладка **Архив**, в мастере прямых или обратных операций.

Просмотр информации о простом или зашифрованном документе

1. Перейдите в раздел **Документы** — вкладка **Архив**.
2. Выделите документ в списке цветом.
3. Нажмите на иконку просмотра .

В области быстрого просмотра отображается информация о документе — тип, размер, даты создания и изменения, каталог расположения файла.

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

При нажатии на кнопку **Обновить** обновляется информация о документе.

Просмотр информации о подписанном документе

1. Перейдите во вкладку **Архив**.
2. Выделите подписанный документ в списке (с расширением .sig).
3. Нажмите на иконку просмотра.

В области быстрого просмотра на разных вкладках отображается информация о подписи и о документе.

Информация о подписи:

- общий статус (действительность подписи);
- информация о подписи (кто и когда подписал документ);
- свойства подписи (стандарт подписи, дата и время подписания);
- информация о подписчике;
- информация об издателе;
- данные о сертификате (до какой даты действителен, алгоритм подписи);
- состав цепочки сертификации.

Информация о документе: тип, размер, каталог расположения файла, даты создания и изменения.

> **ВАЖНО!** Чтобы просматривать информацию о подписи подписанных документов, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

При нажатии на кнопку **Обновить** обновляется информация о документе.

При нажатии на кнопку **Печать** формируется **Отчёт о проверке электронной подписи** в формате .pdf, который можно распечатать или скачать на устройство (протокол проверки подписи).

Если при просмотре информации о документе возникла ошибка, она выводится как уведомление в правом верхнем углу. Вы можете ее посмотреть, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

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.

Открыть статью на сайте

Как открыть документ для просмотра

Документ для просмотра открывается в программе, которая ассоциирована с его расширением.

Для подписанных или зашифрованных документов открывается оригинал.

ВАЖНО! Чтобы просматривать подписанные и зашифрованные документы, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

При открытии зашифрованного документа происходит расшифрование, поэтому в хранилище личных сертификатов должен быть сертификат с закрытым ключом, в адрес которого производилось шифрование.

Открыть документ вы можете в разделе **Документы** — вкладка **Архив**, в мастере прямых или обратных операций.

1. Перейдите в раздел **Документы** — вкладка **Архив**.
2. Выделите документ в списке.
3. Нажмите на кнопку **Открыть** на верхней панели.

Если при открытии документа возникла ошибка, она выводится как уведомление в правом верхнем углу. Вы можете ее посмотреть, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **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.

Открыть статью на сайте

Как удалить документ

Документы можно удалить во вкладке **Архив**, тогда они удаляются из файловой системы.

Также можно удалить в мастере **Подписи и шифрования** или **Проверки и расшифрования**, тогда происходит очищение списка без удаления из файловой системы.

Как удалить документ

1. Перейдите к списку документов.
2. Выделите документ в списке нажатием курсора.
3. В верхней панели нажмите на кнопку **Удалить**.

Как удалить несколько документов сразу

1. Перейдите к списку документов.
2. Установите флажки слева от документов.
3. В верхней панели нажмите на кнопку **Удалить**.

Как удалить все документы

1. Перейдите к списку документов.
2. Выберите все документы, установив флажок в левом верхнем углу.
3. В верхней панели нажмите на кнопку **Удалить**.

> **Важно!**: При удалении во вкладке **Архив** файлы удаляются из файловой системы. При удалении из **Мастера** документы из файловой системы не удаляются.

Открыть статью на сайте

Как редактировать профиль подписи

1. Перейдите во вкладку **Архив** или в мастер **Подпись и шифрование** или **Проверка и расшифрование**.
2. Для открытия правой боковой панели нажмите на выбранный активный профиль.
3. Наведите курсор на профиль, который хотите изменить, и нажмите на иконку **Настройки**.
4. На правой боковой панели в форме просмотра настроек профиля нажмите кнопку **Редактировать**.
5. Отредактируйте поля профиля.
6. Нажмите **Сохранить**.

Открыть статью на сайте

Как удалить профиль подписи

1. Перейдите во вкладку **Архив** или в мастер **Подпись и шифрование** или **Проверка и расшифрование**.
2. Для открытия правой боковой панели нажмите на выбранный активный профиль.
3. Наведите курсор на профиль, который хотите удалить, и нажмите на иконку **Настройки**.
4. На правой боковой панели в форме просмотра настроек профиля нажмите кнопку **Удалить**.

Профиль удаляется.

Нельзя удалить профиль, выбранный по умолчанию.

Открыть статью на сайте

Как переключаться между профилями подписи

Вы можете выбирать различные профили подписи в зависимости от операций, которые нужно выполнить.

1. Перейдите во вкладку **Архив** или в мастер **Подпись и шифрование** или **Проверка и расшифрование**.
2. Для открытия правой боковой панели нажмите на выбранный активный профиль.
3. Наведите курсор на профиль, который хотите сделать активным, и нажмите на его иконку.

Профиль становится активным.

Параметры, заданные в выбранном профиле, применяются в **Настройках операции** в мастере **Подписи и шифрования**.

Всегда есть выбранный активный профиль.

Открыть статью на сайте

Как посмотреть настройки профиля подписи

1. Перейдите во вкладку **Архив** или в мастер **Подпись и шифрование** или **Проверка и расшифрование**.
2. Для открытия правой боковой панели нажмите на выбранный активный профиль.
3. Наведите курсор на профиль, настройки которого хотите посмотреть, и нажмите на кнопку **Настройки**.

Вы можете переключаться по вкладкам профиля для просмотра информации о настройках выбранных операций.

Открыть статью на сайте

Как выбрать сертификат подписи

Чтобы подписывать документы электронной подписью, необходимо в профиле подписи или в настройках операции в мастере **Подписи и шифрования** выбрать сертификат из хранилища **Личные**, у которого есть привязка к закрытому ключу.

Для выбора сертификата подписи в **Профиле подписи** перейдите на форму создания или редактирования профиля и выберите в нем операцию **Подпись**.

Для выбора сертификата подписи в **Настройках операции** в мастере **Подписи и шифрования** перейдите в мастер из вкладки **Архив** и выберите в верхней панели операцию **Подписать**.

Как выбрать сертификат подписи

1. В поле **Сертификат подписи** нажмите **Выбрать сертификат**.
2. Для настроек операций выберите сертификат из выпадающего списка. Если подходящего сертификат нет, то нажмите **Показать все сертификаты**.

   Далее, или, если выбор сертификата происходит в профиле подписи, то на правой боковой панели в списке сертификатов наведите курсор на сертификат, который хотите выбрать, и нажмите на его иконку.
3. Сертификат появляется в поле **Сертификат подписи**.
4. Закройте правую боковую панель.
5. Сохраните изменения.

Как изменить сертификат подписи в профиле подписи

1. Перейдите на форму создания или редактирования профиля подписи.
2. В поле **Сертификат подписи** нажмите на иконку редактирования у сертификата.
3. На правой боковой панели в списке сертификатов наведите курсор на сертификат, который хотите выбрать, и нажмите на его иконку. Сертификат изменяется в поле **Сертификат подписи** профиля. Выбор сертификат можно отменить, повторно нажав на его иконку.
4. Закройте правую боковую панель.
5. Сохраните изменения.

Как изменить сертификат подписи в настройках операции в мастере Подписи и шифрования

1. Перейдите в мастер **Подписи и шифрования** и выберите операцию **Подписать**.
2. В поле **Сертификат подписи** нажмите на иконку удаления у сертификата.
3. В пустом поле **Сертификат подписи** нажмите **Выбрать сертификат**.

4. Выберите сертификат из выпадающего списка. Если подходящего сертификат нет, то нажмите **Показать все сертификаты**.

   На правой боковой панели в списке сертификатов наведите курсор на сертификат, который хотите выбрать, и нажмите на его иконку.

5. Сертификат появляется в поле **Сертификат подписи**.

> **Примечание:** при выборе недействительного сертификата отображается предупреждение.

Как удалить сертификат подписи из профиля подписи

1. Откройте форму создания или редактирования профиля.
2. В поле **Сертификат подписи** нажмите на иконку удаления у сертификата или в поле **Сертификат подписи** нажмите на иконку редактирования у сертификата, на правой боковой панели в списке сертификатов нажмите на иконку уже выбранного сертификата.

Сертификат удаляется из поля **Сертификат подписи** профиля.

Как удалить сертификат подписи из настроек операций

1. Перейдите в мастер **Подписи и шифрования**.
2. В поле **Сертификат подписи** нажмите на иконку удаления у сертификата.

Поле **Сертификат подписи** очищается.

Открыть статью на сайте

Как выбрать сертификаты шифрования

Чтобы шифровать документы, необходимо в профиле подписи или в настройках операции в мастере **Подписи и шифрования** выбрать сертификаты шифрования из хранилища **Личные** и **Других пользователей** и/или контакты, у которых есть привязанный сертификат.

Для выбора сертификатов шифрования в **Профиле подписи** перейдите на форму создания или редактирования профиля и выберите в нем операцию **Шифрование**.

Для выбора сертификатов шифрования в **Настройках операции** в мастере **Подписи и шифрования** перейдите в мастер из вкладки **Архив** и выберите в верхней панели операцию **Зашифровать**.

Как выбрать сертификаты шифрования

1. В поле **Сертификаты шифрования** нажмите **Выбрать сертификаты**.
2. Для настроек операций выберите сертификат из выпадающего списка. Возможен выбор нескольких сертификатов. Если подходящего сертификата нет, то нажмите **Показать все сертификаты**.

   Далее, или, если выбор сертификата происходит в профиле подписи, то на правой боковой панели на вкладке **Сертификаты** отображаются сертификаты получателей, а на вкладке **Контакты** — контакты с привязанными сертификатами, в адрес которых будет зашифрован документ. Для выбора наведите курсор на сертификат или контакт и нажмите на его иконку. Сертификаты или контакты появляются в поле **Сертификат шифрования** профиля.
3. При необходимости закройте правую боковую панель после выбора всех сертификатов.

Как добавить сертификаты шифрования в профиле подписи

1. Откройте форму создания или редактирования профиля подписи.
2. В поле **Сертификат шифрования** нажмите на **Выбрать сертификаты**.
3. На правой боковой панели на вкладке **Сертификаты** отображаются сертификаты получателей, а на вкладке **Контакты** — контакты с привязанными сертификатами, в адрес которых будет зашифрован документ. Для выбора наведите курсор на сертификат или контакт и нажмите на его иконку.
   Сертификаты или контакты появляются в поле **Сертификат шифрования** профиля.
4. Закройте правую боковую панель после выбора.

Как добавить сертификаты шифрования в настройках операций мастера Подписи и шифрования

1. Перейдите в мастер **Подписи и шифрования** и выберите операцию **Зашифровать**.
2. В поле **Сертификат шифрования** нажмите на **Выбрать сертификат**.
3. Выберите сертификат из выпадающего списка. Если подходящего сертификат нет, то нажмите **Показать все сертификаты**. На правой боковой панели на вкладке **Сертификаты** отображаются сертификаты получателей, а на вкладке **Контакты** — контакты с привязанными сертификатами, в адрес которых будет зашифрован документ. Для выбора наведите курсор на сертификат или контакт и нажмите на его иконку. Сертификаты или контакты появляются в поле **Сертификаты шифрования** профиля. Возможен множественный выбор.
4. При необходимости закройте правую боковую панель после выбора.

Примечание: при выборе недействительного сертификата отображается предупреждение.

Как удалить сертификат шифрования в профиле подписи

1. Откройте форму создания или редактирования профиля подписи.
2. В поле **Сертификаты шифрования** нажмите на иконку удаления у сертификата или в разделе **Сертификаты шифрования** нажмите на **Выбрать сертификаты**, на правой боковой панели на вкладке **Сертификаты** в списке сертификатов нажмите на иконку уже выбранного сертификата или на вкладке **Контакты** — на уже выбранный контакт.
3. Сертификат или контакт удаляется из поля **Сертификаты шифрования** профиля.

Как удалить сертификат шифрования в настройках операций мастера Подписи и шифрования

1. Перейдите в мастер **Подписи и шифрования**.
2. В поле **Сертификаты шифрования** нажмите на иконку удаления сертификата.
3. Сертификат или контакт удаляется из поля **Сертификаты шифрования**.

Открыть статью на сайте

Как добавить документы в мастер

Принцип добавления документов в мастер **Подписи и шифрования** и **Проверки и расшифрования** идентичен.

Перейти в мастер можно через левое боковое меню или через кнопку **Добавить в**. При этом при переходе по кнопке в мастер в список документов для операции добавляется выделенный цветом документ из списка документов вкладки **Архив**.

Добавление из Архива

1. Перейдите в раздел **Документы** — вкладка **Архив**.
2. Выделите документы в списке и перейдите в мастер **Подпись и шифрование** или **Проверка и расшифрование**. Если вы хотите открыть пустой мастер, то не выбирайте документы и перейдите в мастер **Подпись и шифрование** или **Проверка и расшифрование**.
3. Если в списке нет документов, то нажмите **Добавить из Архива** в области формирования списка. Если документы уже добавлены в список, то нажмите кнопку **Из Архива** на панели действий.
4. В открывшейся правой боковой панели нажмите на иконку документа, который хотите добавить. Документ добавляется в список. При повторном нажатии на иконку документ удаляется из списка.
5. После выбора всех документов закройте правую боковую панель, нажав кнопку **Закрыть**.

Добавление из файлового менеджера

1. Перейдите в раздел **Документы** — мастер **Подпись и шифрование** или **Проверка и расшифрование**.
2. Добавьте документы одним из следующих способов:
   - перетащите документы или папки с документами из файлового менеджера в область формирования списка файлов. При перетаскивании папки файлы добавляются одноуровневым списком.
   - нажмите кнопку **Загрузить с компьютера** и в файловом менеджере выберите необходимые документы.

Открыть статью на сайте

Как посмотреть расположение документа

Принцип работы с документами в мастерах **Подписи и шифрования** и **Проверки и расшифрования** и в разделе **Документы** идентичен.

1. Перейдите в мастер, где в списке есть документы.
2. Выделите документ нажатием курсора.
3. В верхней панели откройте дополнительное меню и нажмите кнопку **Показать в папке**.

При множественном выборе документов данная опция недоступна.

Открыть статью на сайте

Как подписать документ

Важно перед началом

Перед подписанием документов убедитесь, что выполнены следующие условия:

> ⚠️ Установлен криптопровайдер **КриптоПро CSP**
> ⚠️ У вас есть действующая лицензия **КриптоАРМ ГОСТ 3** или **КриптоАРМ ГОСТ 3 Защищённая почта**

Подготовка к подписи

Для выполнения подписи необходимо:

- установить сертификат с закрытым ключом в хранилище **Личное**;
- убедиться, что сертификат доступен в системе;
- при необходимости настроить профиль подписи.

Где выполняется подпись

Подписание документов выполняется в разделе:

Документы → Подпись и шифрование

Вы можете добавлять файлы:

- перетаскиванием (drag-and-drop);
- через кнопку **Загрузить с компьютера**;
- через вкладку **Архив**.

Способы подписания документа

В КриптоАРМ ГОСТ доступно несколько способов подписи:

- с использованием профиля подписи (рекомендуется);
- с ручной настройкой параметров;
- с использованием специализированных стандартов подписи (CAdES);
- с использованием DSS-сертификатов.

Подписание с использованием профиля

Профиль подписи — это заранее сохранённый набор настроек.

Создайте профиль подписи, в котором заданы настройки подписи.

1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подписи и шифрования**.
3. Выберите профиль подписи, в котором заданы настройки подписи. При выборе профиля в мастере автоматически заполняются **Настройки операций**, **Сертификат подписи**, каталоги сохранения результатов подписи.
4. Добавьте документы в список.
5. Нажмите кнопку **Выполнить**.

Подписание с ручной настройкой

Если вы хотите изменить параметры подписи, не изменяя настройки в профиле, то воспользуйтесь настройками в открытом мастере.

1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подписи и шифрования**.
3. Включите на верхней панели операцию **Подписать**. В **Настройках операций** становятся доступны параметры подписи.
4. Установите параметры подписи (вид, кодировку, стандарт, формат файла подписи), выберите сертификат подписи и настройте каталоги сохранения подписанных файлов.
5. Для операции подписи можно выбрать только один сертификат из категории **Личные**, у которого есть привязка к закрытому ключу. Для этого:
   - нажмите на поле **Сертификат подписи**;
   - в развернувшемся списке выберите сертификат.
     Если в списке нет подходящего сертификата, то нажмите **Показать все сертификаты** и в открывшейся боковой панели выберите нужный сертификат.
6. Добавьте документы в список.
7. Нажмите кнопку **Выполнить**.

Подпись с использованием DSS-сертификата

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.

Подпись со штампом времени (TSP)

Служба штампов времени используется для простановки штампов времени на документы. Данные, защищенные электронной подписью Службы, содержат надежную информацию о времени существования электронного документа. Штампы времени используются для привязки факта существования каких-либо данных ко времени.

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

1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подписи и шифрования**.
3. Создайте профиль подписи или выберите в настройках операции с включенной опцией **Подпись** следующие параметры подписи:

   - стандарт — **CAdES-BES**, вид, кодировку, формат файла подписи, выберите сертификат подписи и настройте каталоги сохранения подписанных файлов;
   - включите опцию **Штамп времени на подпись**, если требуется поставить штамп на подпись;
   - включите опцию **Штамп времени на подписываемые данные**, если требуется поставить штамп на данные;
   - заполните в поле **Служба штампов времени (TSP)** адрес службы, который можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: `\<протокол\>://\<сервер\>[:порт][/путь]`. В качестве протокола может быть указан "http" и "https".

- **Использовать прокси-сервер** — если при подключении к службе TSP используется прокси-сервер, то установка флага активирует его настройки: **Адрес прокси-сервера, Логин, Пароль,** которые можно узнать у системного администратора.

4. Добавьте документы в список.

5. Нажмите кнопку **Выполнить**.

Подпись CAdES-T

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

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

1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подписи и шифрования**.

3. Создайте профиль подписи или выберите в настройках операции с включенной опцией **Подпись** следующие параметры подписи:

   - **стандарт — CAdES-T**, вид, кодировку, формат файла подписи, выберите сертификат подписи и настройте каталоги сохранения подписанных файлов;
   - опция **Штамп времени на подпись** автоматически активируется;
   - опция **Штамп времени на подписываемые данные** недоступна для активации;
   - заполните в поле **Служба штампов времени (TSP)** адрес службы, который можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: `\<протокол\>://\<сервер\>[:порт][/путь]`. В качестве протокола может быть указан "http" и "https".
   - **Использовать прокси-сервер** — если при подключении к службе TSP используется прокси-сервер, то установка флага активирует его настройки: **Адрес прокси-сервера, Логин, Пароль,** которые можно узнать у системного администратора.

4. Добавьте документы в список.

5. Нажмите кнопку **Выполнить**.

Усовершенствованная подпись 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.

Вы можете создать усовершенствованную подпись только при наличии установленных модулей **TSP Client** и **OCSP Client** и лицензий на них.

1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подписи и шифрования**.
3. Создайте профиль подписи или выберите в настройках операции с включенной опцией **Подпись** следующие параметры подписи:
   - стандарт — **CAdES-X Long Type 1**, вид, кодировку, формат файла подписи, выберите сертификат подписи и настройте каталоги сохранения подписанных файлов;
   - заполните в поле **Служба штампов времени (TSP)** адрес службы, который можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: `\<протокол\>://\<сервер\>[:порт][/путь]`. В качестве протокола может быть указан "http" и "https".
   - при необходимости заполните поле **Служба онлайн статусов (OCSP)** — адрес службы OCSP. Данное поле не обязательно для заполнение, чаще всего адрес прописан в самом сертификате, которым создается подпись.
   - **Использовать прокси-сервер** — если при подключении к службе TSP используется прокси-сервер, то установка флага активирует его настройки: **Адрес прокси-сервера, Логин, Пароль,** которые можно узнать у системного администратора.
4. Добавьте документы в список.
5. Нажмите кнопку **Выполнить**.

Архивная подпись 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.

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

1. Перейдите в раздел **Документы**.
2. Откройте мастер **Подписи и шифрования**.
3. Создайте профиль подписи или выберите в настройках операции с включенной опцией **Подпись** следующие параметры подписи:
   - стандарт — **CAdES-A**, вид, кодировку, формат файла подписи, выберите сертификат подписи и настройте каталоги сохранения подписанных файлов;
   - опция **Штамп времени на подпись** автоматически активируется;

- заполните в поле **Служба штампов времени (TSP)** адрес службы, который можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Формат адреса: `\<протокол\>://\<сервер\>[:порт][/путь]`. В качестве протокола может быть указан "http" и "https";
- при необходимости заполните поле **Служба онлайн статусов (OCSP)** — адрес службы OCSP. Чаще всего адрес прописан в самом сертификате, которым создается подпись.
- **Использовать прокси-сервер** — если при подключении к службе TSP используется прокси-сервер, то установка флага активирует его настройки: **Адрес прокси-сервера, Логин, Пароль,** которые можно узнать у системного администратора.

4. Добавьте документы в список.

5. Нажмите кнопку **Выполнить**.

Результат выполнения операции

На вкладке **Подпись и шифрование** отображаются ход и результаты выполнения операции.

При успешном выполнении операции подписанные файлы сохраняются в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан.

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

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

Вы можете посмотреть информацию о подписи, выделив документ в списке и нажав иконку просмотра.

Действия с файлами после выполнения операции:

- **Открыть** — файл откроется в соответствующей программе;
- **Сохранить в Архив** — результат операции будет сохранён в специальную папку на устройстве и будет отображаться во вкладке **Архив** раздела **Документы**;
- **Добавить в Подпись и шифрование / Проверка и расшифрование** — результат операции будет добавлен в мастер **Подпись и шифрование** или **Проверка и расшифрование**;
- **Промежуточные файлы** — откроется список промежуточных файлов (оригинал документов).

Если какие-то документы не удалось подписать, то операция считается выполненной с ошибками. Вы можете посмотреть, какие файлы подписались успешно, а какие с ошибками.

Ошибки при операции выводятся как уведомления. Вы можете их посмотреть, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

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

Открыть статью на сайте

Как зашифровать документ

Важно перед началом

Перед шифрованием документов убедитесь, что:

> ⚠️ Установлен криптопровайдер **КриптоПро CSP**
> ⚠️ Настроены сертификаты получателей (контакты или хранилище сертификатов)

Подготовка сертификатов

Для выполнения шифрования необходимо, чтобы сертификаты получателей были доступны системе.

Вы можете использовать:

- сертификаты из хранилища **Другие пользователи**;
- сертификаты, привязанные к **контактам**;
- сертификаты из раздела **Личные** (в отдельных сценариях).

Где выполняется шифрование

Шифрование выполняется в мастере:

Документы → Подпись и шифрование

Вы можете добавить файлы:

- перетаскиванием (drag-and-drop);
- через вкладку **Архив**;
- через кнопку добавления документов.

Способы шифрования документов

В КриптоАРМ ГОСТ доступны два основных способа:

- с использованием профиля шифрования (рекомендуется);
- с ручной настройкой параметров.

Шифрование с использованием профиля

Профиль шифрования — это заранее сохранённые настройки, которые ускоряют работу.

1. Перейдите во вкладку **Архив**.
2. Выберите в списке документы, которые нужно зашифровать, или ничего не выбирайте, если хотите добавить документы из системы.
3. Перейдите в мастер **Подписи и шифрования** через левое боковое меню или с помощью кнопки **Добавить в**.
4. Выберите профиль, в котором заданы настройки шифрования. При выборе профиля в мастере автоматически заполняются **Настройки операций**, **Сертификаты шифрования**, каталоги сохранения зашифрованных файлов.
5. При необходимости добавьте документы в список.
6. Нажмите кнопку **Выполнить**.

Шифрование с ручной настройкой

Если вы хотите изменить параметры шифрования, не изменяя настройки в профиле, то воспользуйтесь настройками в открытом мастере.

1. Перейдите во вкладку **Архив**.
2. Выберите в списке документы, которые нужно зашифровать, или ничего не выбирайте, если хотите добавить документы из системы.
3. Перейдите в мастер **Подписи и шифрования** через левое боковое меню или с помощью кнопки **Добавить в**.
4. Включите на верхней панели операцию **Зашифровать**. В **Настройках операций** становятся доступны параметры шифрования.
5. Установите параметры шифрования (алгоритм, кодировку, удаление исходных файлов после шифрования), выберите сертификаты шифрования и настройте каталоги сохранения зашифрованных файлов. При шифровании допускается выбор нескольких сертификатов из категории **Личные** и **Других пользователей** и **Контактов**, у которых есть привязанные сертификаты. Для этого нажмите на поле **Сертификаты шифрования**, в развернувшемся списке выберите сертификаты и/или контакты. Если в списке нет подходящих сертификатов, то нажмите **Показать все сертификаты** и в открывшейся боковой панели на соответствующих вкладках выберите нужные сертификаты и/или контакты.
6. При необходимости добавьте документы в список.
7. Нажмите кнопку **Выполнить**.

Результат выполнения операции

На вкладке **Подпись и шифрование** отображаются ход и результаты выполнения операции.

При успешном выполнении операции зашифрованные файлы сохраняются в заданном каталоге, если выбран каталог для сохранения результатов. Или рядом с исходным файлом, если каталог не задан.

Если установлен флаг **Создать копию в Архиве**, то копия зашифрованного файла сохраняется в папке пользователя. Файлы из данного каталога доступны в разделе **Документы** — вкладка **Архив**.

Если в параметрах шифрования была выбрана опция **Удалить файлы после шифрования**, то в результате операции будут только полученные зашифрованные файлы; промежуточные файлы и оригиналы документов удаляются.

Действия с файлами после выполнения операции:

- **Открыть** — файл откроется в соответствующей программе после ввода пароля на контейнер;
- **Сохранить в Архив** — результат операции будет сохранён в специальную папку на устройстве и будет отображаться во вкладке **Архив** раздела **Документы**;
- **Добавить в Подпись и шифрование / Проверка и расшифрование** — результат операции будет добавлен в мастер **Подпись и шифрование** или **Проверка и расшифрование**;
- **Промежуточные файлы** — откроется список промежуточных файлов (оригинал документов).

Если какие-то документы не удалось зашифровать, то операция считается выполненной с ошибками. Вы можете посмотреть, какие файлы зашифрованы успешно, а какие с ошибками.

Ошибки при операции выводятся как уведомления. Вы можете их посмотреть, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

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

Открыть статью на сайте

Как архивировать документы

Архивировать документы вы можете в мастере **Подписи и шифрования**.

Вы можете архивировать любые произвольные документы, загрузив их с помощью drag-and-drop либо выбрать документы из раздела.

Для архивирования документов дополнительные настройки не нужны, можно выбрать каталог сохранения архива и сохранение копии во вкладку **Архив**.

1. Перейдите в раздел **Документы** — вкладка **Архив**.
2. Выберите в списке документы, которые нужно заархивировать, или ничего не выбирайте, если хотите добавить документы из системы.
3. Нажмите **Подпись и шифрование**.
4. Включите на верхней панели операцию **Архивировать**.
5. Добавьте документы в список.
6. При необходимости выберите каталог сохранения архива, опцию сохранения копии в **Архив**.
7. Нажмите кнопку **Выполнить**.

Результат выполнения операции

При успешном выполнении операции документ отображается в мастере **Результаты операции**.

Документ сохраняется в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с первым добавленным файлом, если каталог не задан.

Если вы добавили для архивирования документы из разных каталогов, то при выполнении операции вам надо выбрать каталог для сохранения документов.

Если установлен флаг **Создать копию в Архив**, то копия созданных документов сохраняется в папке пользователя. Файлы из данного каталога доступны во вкладке **Архив**.

Чтобы каждый раз не задавать операцию в мастере подписи и шифрования, вы можете настроить профиль с архивированием и каталогами сохранения результатов и выбирать его.

Открыть статью на сайте

Как расшифровать документ

Важно перед началом

Перед расшифрованием убедитесь, что:

> ⚠️ Установлен криптопровайдер **КриптоПро CSP**
> ⚠️ У вас есть лицензия **КриптоАРМ ГОСТ 3** или **КриптоАРМ ГОСТ 3 Защищённая почта**
> ⚠️ В хранилище есть сертификат с закрытым ключом, использованный при шифровании

Какие файлы можно расшифровать

В приложении можно расшифровать файлы:

- с расширением **.enc**;
- зашифрованные в **КриптоАРМ ГОСТ** или совместимых системах;
- содержащие сертификат получателя, совпадающий с вашим.

Как расшифровать документ

1. Перейдите во вкладку **Архив**.
2. Выберите в списке документы, которые нужно расшифровать, или ничего не выбирайте, если хотите добавить документы из системы.
3. Перейдите в мастер **Проверка и расшифрование** через левое боковое меню или с помощью кнопки **Добавить в**.
4. При необходимости добавьте документы в список.
5. Нажмите кнопку **Выполнить**.

На вкладке **Проверка и расшифрование** отображаются ход и результаты 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**.

Действия с файлами

Вы можете:

- **Открыть** — файл откроется в соответствующей программе после ввода пароля на контейнер;
- **Сохранить на компьютере / в Архив** — результат операции можно сохранить на устройство в определённую пользователем папку или в специальную папку на устройстве (файл будет отображаться во вкладке **Архив** раздела **Документы**);
- **Добавить файлы с компьютера / из Архива** — в мастер **Проверка и расшифрование** будет добавлен файл, указанный пользователем;
- **Добавить в Подпись и шифрование / Проверка и расшифрование** — результат операции будет добавлен в мастер **Подпись и шифрование** или **Проверка и расшифрование**;
- **Отправить** — откроется новое письмо с вложением в виде файлов, которые были в окне результатов операции;
- **Удалить** — выбранные файлы удалятся из окна мастера **Проверка и расшифрование**.

Если какие-то документы не удалось расшифровать, то операция считается выполненной с ошибками. Вы можете посмотреть, какие файлы расшифрованы успешно, а какие с ошибками.

Ошибки при операции выводятся как уведомления. Вы можете их посмотреть, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

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

Открыть статью на сайте

Как проверить подпись документа

> **ВАЖНО!** Чтобы проверять подпись документов, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

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

> **Примечание:** для корректной проверки подписи у вас должны быть установлены корневой и промежуточные сертификаты подписанта документа.

Как посмотреть информацию о подписи документа во вкладке Архив

1. Перейдите во вкладку **Архив**.
2. Выделите в списке подписанный документ (с расширением .sig, .p7s, .sgn, .sign, .bin или XMLDSig).
3. Нажмите на иконку просмотра .
4. На правой боковой панели отображается информация о свойствах подписи и о документе.

Как посмотреть информацию о подписи документа в мастерах

1. Перейдите во вкладку **Архив**.
2. Выберите в списке файлы, подпись которых нужно проверить, или ничего не выбирайте, если хотите добавить файлы из системы.
3. Перейдите в мастер **Проверка и расшифрование** через левое боковое меню или с помощью кнопки **Добавить в**.
4. При необходимости добавьте документы в список.
5. Выделите один подписанный файл (с расширением .sig, .p7s, .sgn, .sign, .bin или XMLDSig).
6. Нажмите на иконку просмотра.
7. На правой боковой панели отображается информация о свойствах подписи и о документе.

Статус проверки подписи списка документов

1. Перейдите во вкладку **Архив**.
2. Выберите в списке файлы, подпись которых нужно проверить, или ничего не выбирайте, если хотите добавить файлы из системы.
3. Перейдите в мастер **Проверка и расшифрование** через левое боковое меню или с помощью кнопки **Добавить в**.
4. При необходимости добавьте документы в список.
5. В списке документов отображается общий статус проверки подписи, который дублируется в виде иконок: подпись действительна, подпись недействительна, не удалось проверить подпись.
6. Для более подробной информацию подписи откройте информацию о файле.

Как посмотреть информацию о подписи документа с соподписями

Если документ подписан несколькими подписями (имеет соподписи), то для просмотра конкретной подписи в правой боковой панели в информации о подписи выберите подпись из списка.

Как посмотреть информацию о подписи документа с штампами времени

Если документ подписан подписью со штампом времени, то для просмотра параметров штампа:

1. Разверните информацию, нажав на иконку .
2. Выберите в выпадающем списке тип штампа времени.

Как посмотреть информацию об усовершенствованной подписи

Если документ подписан усовершенствованной подписью, то для просмотра сведений о штампах времени в усовершенствованной подписи:

1. Разверните информацию, нажав на иконку .
2. Выберите в выпадающем списке тип штампа времени.

Также в информации о подписи вы можете посмотреть информацию о OCSP ответе усовершенствованной подписи.

Если при проверке отсоединённой подписи исходный файл не будет найден автоматически, то возникнет уведомление об этом, которое вы можете посмотреть, нажав на иконку .

Для выбора исходного файла в правой боковой панели нажмите **Указать путь к файлу**. Откроется файловый менеджер для выбора.

Действия с файлами

Вы можете:

- **Открыть** — файл откроется в соответствующей программе;
- **Сохранить на компьютере / в Архив** — результат операции можно сохранить на устройство в определённую пользователем папку или будет сохранён в специальную папку на устройстве и будет отображаться во вкладке **Архив** раздела **Документы**;
- **Добавить файлы с компьютера / из Архива** — в мастер **Проверка и расшифрование** будет добавлен файл, указанный пользователем;
- **Добавить в Подпись и шифрование / Проверка и расшифрование** — результат операции будет добавлен в мастер **Подпись и шифрование** или **Проверка и расшифрование**;
- **Отправить** — откроется новое письмо с вложением в виде файлов, которые были в окне результатов операции;
- **Удалить** — выбранные файлы удалятся из окна мастера **Проверка и расшифрование**.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

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

Открыть статью на сайте

Как добавить соподпись

Соподпись — это дополнительная электронная подпись, которая добавляется к уже подписанному документу. Она позволяет подтвердить документ повторно другим сертификатом или пользователем.

Важно перед началом

Перед добавлением соподписи убедитесь, что:

> ⚠️ Установлен криптопровайдер **КриптоПро CSP**
> ⚠️ В системе установлен сертификат с закрытым ключом (хранилище **Личное**)

Какие файлы можно использовать

Для добавления соподписи используются файлы:

- с расширением **.sig**;
- уже подписанные документы;
- файлы с отсоединённой или присоединённой подписью.

Общая логика соподписи

При добавлении соподписи:

- новая подпись добавляется к существующей;
- исходный файл не изменяется;
- формируется расширенная цепочка подписей.

Соподпись с использованием профиля

1. Перейдите во вкладку **Архив**.
2. Выберите в списке уже подписанные документы, к которым нужно добавить подпись, или ничего не выбирайте, если хотите добавить документы из системы.
3. Перейдите в мастер **Подписи и шифрования** через левое боковое меню или с помощью кнопки **Добавить в**.
4. Выберите профиль подписи, в котором заданы настройки подписи. При выборе профиля в мастере автоматически заполняются **Настройки операций**, **Сертификат подписи**, каталоги сохранения результатов подписи.
5. При необходимости добавьте документы в список.

6. Нажмите кнопку **Выполнить**.

Соподпись с ручной настройкой

Если вы хотите изменить параметры подписи, не изменяя настройки в профиле, то воспользуйтесь настройками в открытом мастере.

1. Перейдите во вкладку **Архив**.
2. Выберите в списке документы с расширением .sig, к которым нужно добавить подпись, или ничего не выбирайте, если хотите добавить документы из системы.
3. Перейдите в мастер **Подписи и шифрования** через левое боковое меню или с помощью кнопки **Добавить в**.
4. Включите на верхней панели операцию **Подписать**. В **Настройках операций** становятся доступны параметры подписи.
5. Установите параметры подписи (стандарт и использование штампов времени) и настройте каталоги сохранения подписанных файлов.

6. Для операции подписи можно выбрать только один сертификат из категории **Личные**, у которого есть привязка к закрытому ключу. Для этого:

   - нажмите на поле **Сертификат подписи**;
   - в развернувшемся списке выберите сертификат.

   Если в списке нет подходящего сертификата, то нажмите **Показать все сертификаты** и в открывшейся боковой панели выберите нужный сертификат.

7. При необходимости добавьте документы в список.

8. Нажмите кнопку **Выполнить**.

Результат выполнения операции

На вкладке **Подпись и шифрование** отображаются ход и результаты выполнения операции.

При успешном выполнении операции подписанные файлы сохраняются в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан. Если установлен флаг **Создать копию в Архиве**, то копия подписанных документов сохраняется в специальную папку, файлы которой доступны во вкладке **Архив**.

Если какие-то документы не удалось подписать, то операция считается выполненной с ошибками. Вы можете посмотреть, какие файлы подписались успешно, а какие с ошибками.

Ошибки при операции выводятся как уведомления. Вы можете их посмотреть, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Не удалось открыть файл** — добавленные в мастер документы были удалены или по какой то причине не доступны.
- **Не удалось подписать файл** — ошибка в адресе службы штампов времени, если подпись со штампом или усовершенствованная. Ошибка подключения к прокси-серверу.
- **Не удалось подписать файл** — ошибки, связанные с истекшими лицензиями КриптоПро TSP Client, OCSP Client, КриптоПро CSP.
- **Не удалось найти исходный файл для подписи** — в мастер добавлен файл с отсоединённой подписью без исходного документа. Чтобы выполнить соподпись в данной ситуации, перед подписанием скопируйте оригинал документа в папку с файлом подписи (названия фалов должно совпадать) или выберите исходный файл в правой боковой панели, нажав **Указать путь к файлу**.

Открыть статью на сайте

Как снять подпись с документа

> **ВАЖНО!** Чтобы снять подпись, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

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

1. Перейдите в раздел **Документы** — вкладка **Архив**.
2. Выберите в списке файлы, подпись с которых нужно снять, или ничего не выбирайте, если хотите добавить файлы из системы.
3. Перейдите в мастер **Проверка и расшифрование** через левое боковое меню или с помощью кнопки **Добавить в**.
4. При необходимости, добавьте документы в список.
5. Нажмите кнопку слева от файла, с которого надо снять подпись .

На вкладке **Проверка и расшифрование** отображаются ход и результаты выполнения операции.

При успешном снятии подписи полученные оригиналы документов сохраняются во временной папке и удаляются после выполнения другой операции. Вы можете сохранить полученные документы на компьютер или в папку Архив, нажав **Сохранить** и выбрав действие в меню **На компьютере** или **В Архив**.

Если с каких-то документов не удалось снять подпись, то операция считается выполненной с ошибками. Вы можете посмотреть, с каких документов подпись снята успешно, а с каких с ошибками.

Ошибки при операции выводятся как уведомления. Вы можете их посмотреть, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

1. **Нельзя снять откреплённую подпись с файла** — при открепленной 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.

Открыть статью на сайте

Как выполнять прямые групповые операции

Прямые групповые операции в **КриптоАРМ ГОСТ** позволяют выполнять подпись, архивирование и шифрование за одну операцию. Это будут прямые групповые операции. Они выполняются в мастере **Подпись и шифрование**.

Что можно выполнять одновременно

В мастере **Подпись и шифрование** доступны следующие комбинации:

- **Подпись + архивирование** — документ подписывается и упаковывается в архив;
- **Подпись + шифрование** — документ подписывается и защищается шифрованием;
- **Архивирование + шифрование** — документ архивируется и шифруется;
- **Подпись + архивирование + шифрование** — полный цикл защиты документа.

Важно перед началом

Перед выполнением операций убедитесь, что:

> ⚠️ Установлен криптопровайдер **КриптоПро CSP**
> ⚠️ Есть лицензия **КриптоАРМ ГОСТ 3** или **КриптоАРМ ГОСТ 3 Защищённая почта**
> ⚠️ Настроены сертификаты для подписи и шифрования

Как выполнить групповую операцию

1. Откройте мастер **Подписи и шифрования**. Перейти в мастер вы можете из раздела **Документы** через левое боковое меню или с помощью кнопки **Добавить в**.
2. Добавьте документы в список одним из способов:
    - перетащите документы или папки с документами из файлового менеджера в область формирования списка файлов. При перетаскивании папки файлы добавляются одноуровневым списком.
    - нажмите кнопку **Загрузить с компьютера** для пустого списка файлов или кнопку **Добавить файл** на панели действий, а затем в файловом менеджере выберите необходимые документы.
    - нажмите **Добавить из Архива** для пустого списка или кнопку **Из Архива** на панели действий, если в списке документы уже добавлены.

3. Выберите профиль подписи, в котором заданы операции и настройки операций. При выборе профиля в мастере автоматически заполняются **Настройки операций**, каталоги сохранения результатов операций. Или включите на верхней панели необходимые операции. В зависимости от этого в **Настройках операций** становятся доступны дополнительные параметры.

4. Заполните необходимые параметры операций. Настройки операций в мастере не изменяют настройки в выбранном профиле подписи.
5. Нажмите кнопку **Выполнить**.

На вкладке **Подпись и шифрование** отображаются ход и результаты выполнения операций.

При успешном выполнении операций файлы сохраняются в заданном каталоге, если выбран каталог для сохранения результатов, или рядом с исходным файлом, если каталог не задан. Если установлен флаг **Создать копию в Архиве**, то копия документов сохраняется во вкладку **Архив** и в специальный каталог на устройстве.

Если какие-то документы не удалось обработать, то операция считается выполненной с ошибками. Вы можете посмотреть, какие файлы обработаны успешно, а какие с ошибками.

Ошибки при операциях выводятся как уведомления. Вы можете их посмотреть, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

> **Примечание:** при групповой операции подпись и шифрование, если в настройках подписи выбрана отделенная подпись, то в результате создается архив, содержащий исходный файл и файл подписи, который потом шифруется.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

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

Открыть статью на сайте

Как выполнять обратные групповые операции

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

> **ВАЖНО!** Чтобы проверять подпись и расшифровывать документы, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.
>
> **ВАЖНО!** Для расшифрования зашифрованных электронных документов необходима лицензия на ПО КриптоАРМ ГОСТ 3 или на ПО КриптоАРМ ГОСТ 3 Защищённая почта.

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

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

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

По итогам расшифрования и разархивирования автоматически раскрывается первый уровень вложенности.

Если вам требуется получить исходный документ, необходимо перейти на уровень ниже, нажав на кнопку слева от файла.

В этом случае появится текстовка совершаемой операции — «Расшифрован», «Разархивирован», «Результат проверки подписи». И по итогу выполнения операции в раскрывшейся панели станет доступным исходный документ.

Для просмотра информации о подписи выделите один документ в списке и нажмите на иконку просмотра.

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

1. Откройте мастер **Проверки и расшифрования**. Перейти в мастер вы можете из раздела **Документы** через левое боковое меню или с помощью кнопки **Добавить в**.

2. Добавьте документы в список одним из способов:
    - перетащите документы или папки с документами из файлового менеджера в область формирования списка файлов. При перетаскивании папки и файлы добавляются одноуровневым списком;
    - нажмите кнопку **Загрузить с компьютера** для пустого списка файлов или кнопку **Добавить файлы** на панели действий, а затем в файловом менеджере выберите необходимые документы;
    - нажмите **Добавить из Архива** для пустого списка или кнопку **Добавить файлы** на панели действий, если в списке документы уже добавлены.
3. Нажмите кнопку **Выполнить**.

На вкладке **Проверка и расшифрование** отображаются ход и результаты выполнения операций.

При успешном выполнении операций полученные документы сохраняются во временной папке и удаляются после выполнения другой операции. Вы можете сохранить полученные документы на компьютер или в папку Архив, нажав **Сохранить** и выбрав действие в меню **На компьютере** или **В Архив**.

Если какие-то документы не удалось обработать, то операция считается выполненной с ошибками. Вы можете посмотреть, какие файлы обработаны успешно, а какие с ошибками.

Ошибки при операции выводятся как уведомления. Вы можете их посмотреть, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Не удалось открыть файл** — добавленные в мастер документы были удалены или по какой-то причине не доступны, добавлен пустой файл (с нулевым размером).
- **Не удалось расшифровать файл** — не найден сертификат для расшифрования.
- **Не удалось расшифровать файл** — ошибки, связанные с истекшей лицензией КриптоПро CSP.
- **Нельзя снять откреплённую подпись с файла** — при открепленной подписи оригинал документа и так находится в отдельном файле.

Открыть статью на сайте

Как работать с результатами операций

При нажатии на кнопку **Выполнить** в мастере **Подпись и шифрование** или при добавлении файлов в мастер **Проверка и расшифрование** происходит переход к ходу выполнения операций.

Во время выполнения операции на верхней панели отображается прогресс-бар и название операции, которая должна быть в итоге выполнена.

По итогу выполнения операций отображается общий статус:

- **Операция выполнена успешно** и прогресс-бар залит зеленым цветом;
- **Операция выполнена с ошибками** и прогресс-бар залит красным цветом.

Действия с документами результатов

Для результатов операций доступны действия на панели инструментов:

- **Открыть** — файл открывается с помощью программы по умолчанию.
- **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.

Вы можете посмотреть информацию о выделенном цветом документе, нажав иконку просмотра .

Отображение результатов проверки подписи

В результатах операции мастера **Подписи и шифрования** в списке не отображается общий статус проверки подписи документов. Вы можете посмотреть только информацию о подписи, выделив один подписанный документ.

Чтобы в списке отображался общий статус проверки подписанных документов, нужно добавить их в мастер **Проверки и расшифрования**. В таком случае в списке отображается общий статус проверки подписи: подпись действительна, подпись недействительна, не удалось проверить подпись.

Отображение результатов при возникновении ошибок операций

Если не выполнены какие-либо операции с документами, то уведомления об ошибках отображаются в верхнем правом углу экрана. Вы можете их посмотреть, нажав иконку, где цифрой обозначается количество ошибок.

Если по каким-то причинам операция не выполнилась для всех файлов, то в списке останутся оригиналы документов, сгруппированные в раздел **Не успешно**.

Если для документов выполнилась часть операций, то для просмотра полученных промежуточных файлов нажмите кнопку **Промежуточные файлы**.

Если операция выполнилась частично, то результаты разделяются на выполненные **Успешно** и **Не успешно**.

Для просмотра полученных промежуточных файлов нажмите кнопку **Промежуточные файлы**.

Открыть статью на сайте

Как установить личный сертификат

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

Если у вас сертификат и закрытый ключ находятся в контейнере **.pfx**, то воспользуйтесь инструкцией по установке сертификата из файла **.pfx**.

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

Перед импортом личного сертификата убедитесь, что у вас установлен криптопровайдер КриптоПро CSP.

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

Как установить сертификат из ключевого контейнера

Примечание: возможно, понадобится установка драйверов для токена.

Данный способ возможен, если сертификат присутствует в контейнере. Иначе функция установки 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**. Открывается список контейнеров.
4. В списке выделите контейнер.
5. Нажмите кнопку **Установить**.
6. При необходимости введите пароль к ключевому контейнеру.

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

Как установить сертификат с закрытым ключом из файла .pfx

1. Выберите раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в правой части окна.
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 личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

Как установить сертификат с привязкой к ключевому контейнеру

1. Выберите раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в правой части окна.
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 личное хранилище и отображается в списке. Теперь вы можете подписывать и расшифровывать документы этим сертификатом.

Если при импорте возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Открыть статью на сайте

Как создать подключение к сервису DSS

Для установки сертификата из DSS надо сначала создать подключение к 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.
4. Нажмите кнопку **Подключить**.
5. Если у вас 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**. Вы можете установить флаг **Запоминать пароль до выхода из приложения**, чтобы каждый раз не вводить пароль для подключения при работе с сертификатом DSS. Если пароль не задан, то данный шаг пропускается.
6. Если у вас в личном кабинете DSS в настройках стоит подтверждение аутентификации по SIM-карте или с помощью мобильного приложения, то на следующем шаге появляется информационное окно с ожиданием подтверждения операции на телефоне. **Подтвердите** операцию на телефоне. Если идентификация настроена не с помощью телефона, то данный шаг пропускается.

При успешной аутентификации сертификат DSS автоматически помещается в хранилище **Личные сертификаты**.

Сертификаты DSS в списке отмечаются иконкой облачного контейнера .

Важно! Для того чтобы сертификат был действительный, у вас должны быть должны быть установлены корневые сертификаты УЦ и актуальный список отзыва сертификатов (COC).

Если при подключении к сервису возникают ошибки, они выводятся как уведомления. Вы можете их посмотреть, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Не удалось подключиться к серверу DSS** — неверный логин или пароль — проверьте правильность заполнения данных.
- **Не удалось подключиться к серверу DSS** — проверьте правильность ввода адресов серверов, доступ к сети Интернет.

Открыть статью на сайте

Как создать запрос на сертификат

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

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в правой части окна и в открывшемся списке действий выберите **Создать запрос**.
3. Форма создания запроса на сертификат открывается в новой вкладке.
4. **Выберите** папку для сохранения файла запроса. Если папка не выбрана, файл запроса сохранится в папку пользователя.
5. **Выберите** шаблон сертификата, открыв правую боковую панель со списком шаблонов. Можно выбрать шаблон из списка или выбрать пользовательский шаблон. Для этого нужно **Загрузить шаблон** в формате .json. Для получения инструкции по заполнению шаблона пишите на электронную почту support@trusted.ru. Импортированные шаблоны можно удалить.
6. **Загрузите данные из XML** — позволяет автоматически заполнить поля в запросе с помощью загрузки файлов XML. Данные в полях можно редактировать.
7. Заполните поля раздела **Сведения о владельце**. Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.
8. Перейдите в раздел **Параметры ключа**.

   В данном разделе вы можете задать:

   - 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. После заполнения всех полей нажмите кнопку **Сохранить**.
10. Выберите ключевой носитель для хранения контейнера (реестр, диск, токен), если требуется.
11. На запрос системы **установите** пароль на данный контейнер и **подтвердите** его.

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 во вкладке **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.

Если создании запроса возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Открыть статью на сайте

Как создать самоподписанный сертификат

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

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

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в правой части окна и в открывшемся списке действий выберите **Создать запрос**.
3. Форма создания запроса на сертификат открывается в новой вкладке.
4. При необходимости выберите шаблон сертификата, открыв правую боковую панель со списком шаблонов.
5. В правом верхнем углу установите флаг **Создать самоподписанный сертификат**.
6. Заполните поля раздела **Сведения о владельце**.
   Набор полей меняется в зависимости от выбранного на предыдущем шаге шаблона.
7. Перейдите в раздел **Параметры ключа**.

   В данном разделе вы можете задать:

   - 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).
8. После заполнения всех полей нажмите кнопку **Сохранить**.
9. **Выберите** ключевой носитель для хранения контейнера (реестр, диск, токен), если требуется.
10. На запрос системы **установите** пароль на данный контейнер и **подтвердите** его.

На основе указанных данных формируется самоподписанный сертификат.

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

Если создании сертификата возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Открыть статью на сайте

Как установить корневой и промежуточный сертификаты

Установить корневой или промежуточный сертификат вы можете во вкладке **Удостоверяющие центры** в разделе **Сертификаты**.

1. Перейдите в раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат** в правой части окна и в открывшемся списке действий выберите **Импорт из файла**.
3. В файловом менеджере выберите файл сертификата.
4. Подтвердите запрос на установку сертификата.
5. На запрос ввода пароля администратора введите его и подтвердите.

> **Примечание:** при импорте корневых и промежуточных сертификатов могут быть запрошены права администратора.

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

Если при импорте возникает ошибка, она выводится как уведомление в правом верхнем углу.

Вы можете посмотреть уведомления, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Вы можете импортировать корневой и промежуточный сертификат из любого раздела, выбрав в окне с предупреждением **Поместить в рекомендуемое хранилище Удостоверяющие центры** и нажав **Применить**. В таком случае сертификат установится в подходящее хранилище.

Открыть статью на сайте

Как импортировать сертификат другого пользователя

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

1. Выберите раздел **Сертификаты**.
2. Нажмите кнопку **Добавить сертификат**.
3. Выберите из списка кнопку **Импорт из файла**.
4. В файловом менеджере выберите файл сертификата.

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

Если при импорте возникает ошибка, она выводится как уведомление в правом верхнем углу.

Вы можете посмотреть уведомления, нажав на иконку.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Вы можете импортировать сертификат без закрытого ключа из любого раздела, выбрав в окне с предупреждением **Поместить в рекомендуемое хранилище Другие пользователи** и нажав **Применить**. В таком случае сертификат установится в подходящее хранилище.

Открыть статью на сайте

Как установить список отзыва сертификатов

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

1. Выберите раздел **Сертификаты**.
2. Выберите вкладку **Списки отзыва**.
3. На панели действий нажмите кнопку **Импорт из файла**.
4. В файловом менеджере выберите файл списка отзыва (файл с расширением **.crl**).

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

Если при импорте возникает ошибка, она выводится как уведомление в правом верхнем углу.

Вы можете посмотреть уведомления, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Чтобы список отзыва был действительный, нужно в раздел **Удостоверяющие центры** установить сертификат, выпустивший COC.

Открыть статью на сайте

Как экспортировать личный сертификат

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

Экспортируйте сертификат с закрытым ключом, если вам нужно:

- сохранить копию сертификата и связанного с ним закрытого ключа;
- удалить сертификат и его закрытый ключ с устройства и установить на другое устройство.

Как экспортировать 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. Введите пароль к ключевому контейнеру или нажмите **Отмена**. Если пароль не задан, то данный шаг пропускается.
6. В выпадающем списке выберите **Не экспортировать закрытый ключ**. Выбор может быть заблокирован, если ключ не экспортируемый.
7. Выберите тип кодировки `BASE64` или `DER`.
8. Нажмите кнопку **Выполнить**.
9. В файловом менеджере задайте путь к файлу сертификата и имя файла.

Как экспортировать сертификат с закрытым ключом в контейнер pfx

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** в верхней панели действий.
5. Введите пароль к ключевому контейнеру. Если пароль не задан, то данный шаг пропускается.
6. В выпадающем списке выберите **Экспортировать закрытый ключ**. Выбор заблокирован, если ключ не экспортируемый.
7. Задайте пароль к файлу **.pfx**.
8. Нажмите **Выполнить**.
9. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Если при экспорте возникает ошибка, она выводится как уведомление в правом верхнем углу.

Вы можете посмотреть уведомления, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Открыть статью на сайте

Как экспортировать сертификат другого пользователя

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

1. Выберите раздел **Сертификаты**.
2. Выберите хранилище **Других пользователей** или **Удостоверяющие центры**.
3. В списке выделите сертификат.
4. Нажмите кнопку **Экспортировать** на панели действий.
5. Выберите тип кодировки `BASE64` или `DER`.
6. Нажмите кнопку **Выполнить**.
7. В файловом менеджере задайте путь к файлу сертификата и имя файла.

При успешном выполнении операции сертификат экспортируется в файл.

Если при экспорте возникает ошибка, она выводится как уведомление в правом верхнем углу.

Вы можете посмотреть уведомления, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Открыть статью на сайте

Как работать с ключевыми контейнерами

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

Как посмотреть сертификат в контейнере

1. При необходимости подключите ключевой носитель к устройству.
2. Выберите раздел **Сертификаты**.
3. Выберите хранилище **Ключи**. Открывается список контейнеров.
4. В списке выделите контейнер.
5. Нажмите на иконку просмотра .

В правой боковой панели отображается информация о сертификате в контейнере. Если выводится надпись «В контейнере отсутствуют сертификаты», значит, контейнер не содержит сертификат и его стоит импортировать.

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**. Открывается список контейнеров.
4. В списке выделите контейнер.
5. Нажмите на иконку просмотра .
6. В правой боковой панели нажмите на кнопку **Печать**.

Как протестировать контейнер

> **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**. Открывается список контейнеров.
4. В списке выделите контейнер.
5. Нажмите на иконку просмотра .
6. В правой боковой панели нажмите на кнопку **Протестировать**.
7. 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**. Открывается список контейнеров.
4. В списке выделите контейнер.
5. Нажмите кнопку **Установить**.
6. При необходимости введите пароль к ключевому контейнеру.

Сертификат установлен в личное хранилище.

Как удалить контейнер

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

1. Выберите раздел **Сертификаты**.
2. Выберите хранилище **Ключи**. Открывается список контейнеров.
3. В списке выделите контейнер.
4. Нажмите кнопку **Удалить**.
5. 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

Вы можете обновить список контейнеров, нажав иконку **Обновить**.

Открыть статью на сайте

Как удалить сертификаты

1. Выберите раздел **Сертификаты**.
2. Выберите хранилище, из которого необходимо удалить сертификат.
3. В списке выделите сертификат.
4. Нажмите кнопку **Удалить**.
5. Подтвердите удаление.

Сертификат будет успешно удален из хранилища.

Если сертификат удалить не получается, то возникает ошибка. Ошибки при операции выводятся как уведомления. Вы можете их посмотреть, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

> **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.

Открыть статью на сайте

Действия с разными категориями сертификатов

Перейти в раздел **Сертификаты** вы можете через левое основное меню.

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.

Обновление списка сертификатов происходит по нажатию иконки **Обновить**.

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** — позволяет создать профиль 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

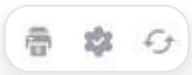
Для ключевых контейнеров вы можете выполнить следующие действия:

- **Установить** — для установки сертификата из контейнера в категорию Личных;
- **Удалить** — для удаления контейнера (**Удаленный контейнер восстановлению не подлежит!**);
- 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.



Открыть статью на сайте

Описание раздела Контакты

Данный раздел предназначен для управления контактами.
Контакты могут быть локальными, добавленными из адресной книги LDAP, добавленными из адресной книги по протоколу CardDAV или импортированными в формате vCard.

Смена книг доступна на правой боковой вкладке.

В левой боковой панели вы можете переключится между папками. Если активной выбрана книга **Контакты**, то доступны папки:

- **Все контакты** — содержит локальные и добавленные контакты;
- **Контакты** — содержит локальные контакты;
- **Группы** — содержит каталог групп разного уровня вложенности и контакты в них;
- **Корзина** — содержит удаленные контакты. При удалении контакты помещаются в корзину, из которой вы их можете удалить совсем.

Если подключена и выбрана активной адресная книга LDAP, то в левом меню доступны папки:

- **Все контакты** — содержит локальные контакты и контакты LDAP;
- **Контакты** — контакты адресной книги LDAP;
- **Корзина** — содержит удаленные локальные контакты. Контакты LDAP удалить нельзя.
- **Папки LDAP** — в виде списка. При наведении на папку LDAP отображается информация о расположении. При выборе папки отображаются контакты LDAP данной папки.

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 ГОСТ.

- **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**.

Открыть статью на сайте

Как добавить локальный контакт

Вы можете создавать контакты для хранения имен, адресов электронной почты, номеров телефонов и других данных. При вводе получателя нового письма этот контакт появиться в списке для выбора.

Вы можете привязать сертификат к контакту для шифрования писем в его адрес.

Создание контакта из раздела контактов

1. Перейдите в раздел **Контакты**.
2. Нажмите кнопку **Новый контакт** в левом меню.
3. Выберите **Создать контакт**.
4. Заполните поля.
5. Нажмите кнопку **Сохранить**.

Создание контакта из раздела сертификатов

1. Перейдите в раздел **Сертификаты**.
2. Выберите хранилище сертификатов **Других пользователей**.
3. Выделите сертификат в списке.
4. На верхней панели действий нажмите кнопку **Создать контакт**. Форма создания контакта открывается в новой вкладке. Данные контакта заполнены доступными данными из сертификата.
5. Заполните необходимые поля.
6. Нажмите кнопку **Сохранить**.

При успешном выполнении операции созданный контакт появляется в списке контактов.

Вы можете редактировать и удалять контакты.

Описание полей формы добавления контакта

Поля сгруппированы по вкладкам **Данные контакта** и **Сертификат**.

Поля раздела **Данные контакта**:

- 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.

Также контакт можно добавить в группу контактов.

Открыть статью на сайте

Как подключить адресную книгу LDAP

Вы можете подключить несколько адресных книг LDAP для работы с контактами.

1. Перейдите в раздел **Контакты**.
2. Откройте правую боковую панель, нажав в правом верхнем углу на выбранную адресную книгу.
3. Выберите **Добавить подключение LDAP**.
4. Заполните поля.
5. Нажмите кнопку **Сохранить**.

При успешном подключении в список **Все контакты** добавляются контакты адресной книги LDAP.

При выборе активной адресной книги LDAP в левом боковом меню отображаются папки LDAP.

Описание полей формы подключения адресной книги

- Название каталога LDAP — произвольное название для адресной книги.
- Сведения о сервере — имя сервера и порт.
- Данные для входа в систему — имя пользователя и пароль.
- База поиска — по умолчанию или другая.
- Параметры сервера — время ожидания, не возвращать более чем N результатов, фильтр поиска и база поиска.
- Параметры синхронизации — частота обновления каталога.

Если при подключении адресной книги возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку .

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Не удалось подключиться к LDAP** — проверьте правильность заполнения полей имя сервера и порт. Проверьте имя пользователя и пароль.

Открыть статью на сайте

Как посмотреть информацию о контакте

Быстрый просмотр

1. Перейдите в раздел **Контакты**.
2. Выделите контакт в списке нажатием курсора.
3. Нажмите кнопку **Просмотреть** .

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.

Открыть статью на сайте

Как привязать сертификат к контакту

Чтобы шифровать документы в адрес контакта, нужно привязать сертификат к контакту.

Данная функция доступна только для локальных контактов.

Вы можете привязать сертификат из уже установленных сертификатов или из файла.

> **ВАЖНО!** Чтобы привязать сертификат, у вас на рабочем месте должен быть установлен криптопровайдер КриптоПро CSP.

Как привязать сертификат из установленных сертификатов

Вы можете привязать сертификат из хранилища **Личные сертификаты** и сертификатов **Других пользователей**.

Если у вас в хранилище нет сертификатов, вы можете импортировать сертификат или выполнить привязку сертификата из файла.

1. Откройте форму создания или редактирования контакта.
2. Нажмите кнопку **Добавить сертификат** — **Из раздела Сертификаты**.
3. В правой боковой панели выберите сертификат, который будет привязан к контакту, нажав на иконку сертификата. Возможен множественный выбор. Сертификат автоматически добавляется в список привязанных сертификатов, доступный на вкладке **Сертификат** контакта.
4. Закройте боковую панель после выбора нужных сертификатов.
5. Нажмите кнопку **Сохранить**.

Как привязать сертификат из файла

Если у вас нет сертификатов в хранилище **Личные сертификаты** и сертификатов **Других пользователей**, вы можете выполнить привязку сертификата из файла. Сертификат установится в хранилище сертификатов **Других пользователей**.

1. Откройте форму создания или редактирования контакта.
2. Нажмите кнопку **Добавить сертификат** — **Из файла**.
3. Выберите файл сертификата в файловом менеджере. Сертификат добавляется в список привязанных сертификатов, доступный на вкладке **Сертификат** контакта.
4. Нажмите кнопку **Сохранить**.

Как привязать сертификат к контакту из раздела сертификатов

1. Перейдите в раздел **Сертификаты**.
2. Выберите категорию **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.

Открыть статью на сайте

Как редактировать локальный контакт

Вы можете редактировать только локальные контакты. Контакты LDAP доступны только для просмотра.

1. Перейдите в раздел **Контакты**.
2. Выделите контакт в списке, который вы хотите изменить.
3. Нажмите кнопку **Редактировать** в верхней панели.
4. Измените нужные поля.
5. Нажмите кнопку **Сохранить**.

Открыть статью на сайте

Как редактировать настройки адресной книги LDAP

1. Перейдите в раздел **Контакты**.
2. Откройте правую боковую панель, нажав в правом верхнем углу на выбранную адресную книгу.
3. Наведите курсор на книгу LDAP, которую хотите изменить, и нажмите на иконку **Настройки**.
4. На правой боковой панели в форме просмотра настроек адресной книги нажмите кнопку **Редактировать**.
5. В новой вкладке **Редактирование адресной книги** отредактируйте нужные поля.
6. Нажмите кнопку **Сохранить**.

При успешном подключении контакты адресной книги LDAP обновятся.

Если при обновлении подключения адресной книги возникает ошибка, она выводится как уведомление в правом верхнем углу. Вы можете посмотреть уведомления, нажав на иконку

.

Для просмотра подробного описания ошибки или отправки в техническую поддержку нажмите кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

ВОЗМОЖНЫЕ УВЕДОМЛЕНИЯ:

- **Не удалось подключиться к LDAP** — проверьте правильность заполнения полей имя сервера и порт. Проверьте имя пользователя и пароль.

Открыть статью на сайте

Как переключаться между адресными книгами

Вы можете переключаться между локальными контактами и подключенными адресными книгами LDAP и CardDAV.

1. Перейдите в раздел **Контакты**.
2. Откройте правую боковую панель, нажав в правом верхнем углу на выбранную адресную книгу.
3. Наведите курсор на книгу, которую хотите сделать активной, и нажмите на ее иконку.

Локальные контакты, контакты LDAP и CardDAV отображаются в папке **Все контакты**.

В папке **Контакты** отображаются контакты выбранной адресной книги.

При выборе активной адресной книги LDAP в левом боковом меню отображаются папки LDAP.

Открыть статью на сайте

Как удалять локальные контакты

Удаленные контакты хранятся в корзине.

Вы можете удалить только локальные контакты. Контакты адресной книги LDAP недоступны для редактирования и удаляются при удалении адресной книги.

Как удалить отдельный контакт

1. Перейдите в раздел **Контакты**.
2. Выделите контакт в списке нажатием курсора.
3. В верхней панели нажмите на кнопку **Удалить**.

Как удалить несколько контактов сразу

1. Перейдите в раздел **Контакты**.
2. Установите флажки слева от контактов.
3. В верхней панели нажмите на кнопку **Удалить**.

Как удалить все контакты

1. Перейдите в раздел **Контакты**.
2. Выберите все контакты, установив флажок в левом верхнем углу.
3. В верхней панели нажмите на кнопку **Удалить**.

Как очистить корзину

1. Перейдите в раздел **Контакты**.
2. В левом боковом меню выберите **Корзина**.
3. Установите флажки напротив контактов, которые хотите навсегда удалить, и нажмите кнопку **Удалить навсегда**.

> **Примечание:** параметр **Удалить навсегда** доступен только в корзине.

Чтобы удалить все контакты в корзине, выделите все контакты в корзине и нажмите на кнопку **Удалить навсегда** на панели действий.

Открыть статью на сайте

Как восстановить удалённые контакты из корзины

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 нужно восстановить.
4. В верхней панели нажмите на кнопку **Восстановить**.

Открыть статью на сайте

Как удалить адресную LDAP

1. Перейдите в раздел **Контакты**.
2. Откройте правую боковую панель, нажав в правом верхнем углу на выбранную адресную книгу.
3. Наведите курсор на книгу LDAP, которую хотите удалить, и нажмите на кнопку **Настройки**.
4. На правой боковой панели в форме просмотра книги нажмите кнопку **Удалить**.
5. Подтвердите удаление.

Адресная книга удаляется. Удаляются все загруженные из нее контакты.

Открыть статью на сайте

Поиск контакта

1. Перейдите в раздел **Контакты**.
2. В поисковой строке введите параметры поиска.

Поиск возможен по следующим значениям: ФИО, e-mail, номер телефона.

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.

Как создать группу контактов

Группу контактов можно создать несколькими способами.

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).

Созданная группа будет видна во вкладке **Контакты**.

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

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 новая 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.

Как редактировать группу

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.

Как написать 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**.

Как удалить группу контактов

1. Открыть раздел **Контакты**.
2. Нажать на контекстное меню нужной группы контактов.
3. Выбрать **Удалить**.
4. Подтвердить удаление группы, её подгрупп и контактов.

Открыть статью на сайте

Поддержка vCard

vCard — текстовый формат для обмена электронными контактными данными. Обычно файл vCard имеет расширение .vcf.

Как импортировать контакты в формате vCard

1. Открыть раздел **Контакты**.
2. Выбрать **Новый контакт** — **Импортировать vCard**.
3. Выбрать файл, указать адресную книгу и группу. Также можно **Создать адресную книгу**.
4. **Импортировать**, если контакты должны быть в адресной книге или **Создать и импортировать**, если адресная книга была создана при импорте контактов.

В **Уведомлениях** будет указано, сколько контактов из скольки было импортировано и были ли найдены контакты со схожими данными, которые можно **Объединить** или **Пропустить**.

После импорта во вкладке **Все контакты** будут видны все локальные и импортированные контакты.

Если импортированные контакты были добавлены в иную адресную книгу, то для их просмотра необходимо переключиться между адресными книгами (в правой боковой панели сделать активной нужную адресную книгу).

Открыть статью на сайте

Как добавить адресную книгу по протоколу CardDAV

CardDAV — это протокол адресной книги, предназначенный для предоставления пользователям доступа к данным на сервере.

Как добавить адресную книгу по протоколу CardDAV

1. Открыть раздел **Контакты**.
2. Открыть правое боковое меню с адресными книгами.
3. Нажать на **Добавить учётную запись CardDAV**.
4. В открывшейся вкладке заполнить данные.
5. **Сохранить**.

Поля формы добавления адресной книги по протоколу CardDAV

1. Название адресной книги.
2. Сведения о сервере: адрес сервиса.
3. Вход в систему: имя пользователя (e-mail) и пароль (для добавления адресной книги необходимо создать пароль для приложения CardDAV в настройках почтового сервиса).
4. Параметры синхронизации: порядок синхронизации (в обе стороны, с сервиса на устройство или с устройства на сервис) и интервал обновления (частота синхронизации адресной книги с почтовым сервисом; возможны варианты обновления никогда, раз в 5/30/60 минут и раз в сутки).
5. Сохранять новые локальные контакты в учётную запись CardDAV.

Открыть статью на сайте

Описание раздела «О программе»

В раздел **О программе** программы вы можете перейти, выбрав в меню пункт **КриптоАРМ ГОСТ Версия 3.x.x**.

В данном разделе содержится информация о правообладателе (ООО «Цифровые технологии»), указан адрес сайта и e-mail для обращения в техническую поддержку.

Сведения о системе вы можете сохранить в файл или отправить по почте. В таком случае открывается почтовый клиент, заданный по умолчанию в ОС. Эти данные нужны для последующей отправки в техническую поддержку при возникновении вопросов по работе программы.

Во вкладках **Лицензия КриптоАРМ ГОСТ** и **Лицензия КриптоПро CSP** представлена информация о продукте, статусе лицензии (действительна), версии программы, сроке работы и разработчике программы.

Здесь необходимо вводить лицензию для работы с КриптоАРМ ГОСТ 3 и криптопровайдером КриптоПро CSP.

Приобрести лицензии можно, нажав на кнопку **Купить лицензию**.

Дополнительно представлены вкладки **Лицензия КриптоПро TSP** и **Лицензия КриптоПро OCSP**, в которых указана информация о продукте и возможность **Ввести** или **Купить** лицензию.

Открыть статью на сайте

Как работать с уведомлениями

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 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 иконку или закрыть вкладку .

Вы можете просмотреть подробное описание ошибки, нажав кнопку **Перейти в журнал** в правой боковой панели списка уведомлений.

Открыть статью на сайте

Как работать с журналом событий

Общее описание

Информация о событиях, происходящих в рамках приложения, записывается в журнал событий.

Вы можете 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** и **Ошибка**.

Информация включает в себя все сообщения, информирующие о действиях, например, операция подписи, экспорт сертификата, синхронизация почты.

Ошибка сообщает об ошибках в работе приложения.

Вы можете 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.

Вы можете скопировать ее для отправки в техническую поддержку, нажав кнопку **Скопировать** .

Сохранение выделенных событий в файл

Вы можете сохранить выбранные в списке события в файл.

1. Выделите с помощью флагов нужные события.
2. На верхней панели действий нажмите 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 кнопку **Отправить**. Открывается вкладка нового сообщения с прикрепленным файлом журнала в формате .log.

Печать событий

Вы можете распечатать подробную информацию о выбранных в списке событий.

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

Параметры журнала

Вы можете настроить размер журнала и уровни логирования.

1. На панели действий нажмите 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 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

Вы можете посмотреть события из архивного журнала.

1. На панели действий нажмите 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.

Показать в папке

Вы можете перейти к расположению файла событий, нажав в дополнительном меню кнопку **Показать в папке**.

Сортировка и фильтрация

Вы можете сортировать список сообщений 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 кнопку **Открыть фильтр**.

Вы можете 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

- КриптоАРМ ГОСТ
- электронная подпись
- шифрование данных
- защищённая почта author: "Команда КриптоАРМ" date: 2026-05-50 updated: 2025-05-05

КриптоАРМ ГОСТ 3

КриптоАРМ ГОСТ 3 — это российская программа, сочетающая в себе функции почтового клиента и программы для подписания и шифрования информации.

КриптоАРМ ГОСТ 3 замещает такие почтовые клиенты, как MS Outlook, The Bat и др. и может использоваться в качестве клиента для почтовых серверов МойОфис Почта, Р7-Офис, Communigate PRO, Tegu, VK Mail.

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

КриптоАРМ ГОСТ 3 применяется для:

- подачи электронных документов в государственные органы;
- шифрования информации ограниченного доступа (персональные данные, коммерческая тайна);
- организации электронного документооборота и обмена неформализованными электронными документами между контрагентами, филиалами и работниками.

Лицензирование КриптоАРМ ГОСТ 3:

- лицензия на ПО **КриптоАРМ ГОСТ 3 Защищённая почта** позволяет подписывать, шифровать и расшифровывать электронные письма и документы, то есть использовать приложение в качестве защищённого почтового клиента и в качестве программы для подписи и шифрования документов;
- лицензия на ПО **КриптоАРМ ГОСТ 3** позволяет подписывать и расшифровывать электронные документы, а также использовать приложение в качестве почтового клиента.