Цифровые технологии

КриптоАРМ 5

Документация продукта

Релиз 5.x · историческое руководство

Исходная документация на CryptoARM.ru

Редакция от 25.11.2026

Правообладатель и разработчик
ООО «Цифровые технологии»

Содержание

Содержание 6

Общие сведения

- Где скачать дистрибутив КриптоАРМ и как его выбрать? 9
- Как установить КриптоАРМ? 10
- Где купить лицензию на КриптоАРМ ? 13
- Временная лицензия и срок ее действия 14
- Проверка наличия ГОСТ - криптопровайдера 15
- Установка лицензии 16
- Удаление КриптоАРМ 20

Параметры программы

- Интерфейс программы 21
- Общие настройки 28
- Режим "Квалифицированная подпись" 33
- Параметры прокси-сервера 37
- Упрощенный режим работы 38

Управление профилями

- Операции с профилями 40
- Общие параметры профиля 47
- Настройки операции подписи 49
- Настройки операции шифрования 53
- Настройки операции расшифрования 56
- Настройки управления интерфейсом 57
- Настройки использования политик сертификатов 59
- Настройки верификации сертификатов 62
- Настройки службы штампов времени TSP 65
- Настройки службы актуальных статусов OCSP 67
- Настройки каталогов хранения файлов 69

Операции с сертификатами

- Проверка сертификата на квалифицированность 71
- Как получить новый сертификат? 73

Как создать самоподписанный сертификат? ... 74
Импорт (установка) сертификата ... 79
Хранение сертификатов ... 84
Как проверить статус сертификата? ... 85
Работа с квалифицированными сертификатами ... 93
Просмотр информации о сертификате ... 96
Фильтрация и сортировка сертификатов ... 100
Печать сертификата ... 102
Экспорт сертификата ... 103
Удаление сертификата ... 105

Операции с запросами на сертификат

Как создать запрос на получение сертификата ... 106
Просмотр информации о запросах, фильтрация и сортировка запросов в списке ... 111
Как создать запрос на аннулирование сертификата ... 114

Операции со списками отзыва сертификатов

Установка списка отзывов в хранилище ... 119
Просмотр информации о списках ... 121
Фильтрация и сортировка списков отзыва ... 122
Экспорт и удаление списков отзыва ... 124

Операции со списками доверенных сертификатов и криптопровайдерами

Как создать список доверенных сертификатов? ... 125
Установка списка в хранилище ... 128
Просмотр информации о списке ... 130
Фильтрация и сортировка списка ... 131
Экспорт и удаление списка ... 133
Операции с криптопровайдерами ... 134

Операции со справочниками назначений сертификата и ключевыми носителями

Создание нового назначения ... 139
Просмотр свойств назначения ... 142
Импорт, экспорт и удаление назначения ... 143
Операции с ключевыми носителями ... 145

Работа с программой

Как подписать электронный документ? ... 147

Добавление заверяющей подписи ... 156
Как добавить соподпись (параллельную подпись)? ... 163
Как проверить электронную подпись? ... 169
Снятие и проверка подписи ... 173
Как зашифровать данные? ... 174
Как расшифровать данные ? ... 181
Как подписать и зашифровать электронный документ ... 185
Как расшифровать и проверить подпись на электронном документе? ... 193
Как просмотреть зашифрованный документ? ... 198
Как получить штамп в службе штампов времени? ... 199
Как просмотреть штамп времени? ... 200

Часто задаваемые вопросы

Ошибка пакета Windows installer ... 204
Ошибка в ходе установки сборки ... 205
Внутренняя ошибка 2739 ... 207
Не удалось открыть подраздел: UNKNOWN/Components ... 208
Координатор установщика Windows ... 209
Ошибка построения пути сертификации ... 210
Ошибка сохранения данных ... 212
Некорректный формат лицензии ... 213
Ошибка исполнения функции (0x0000065b) ... 214
Указан неправильный алгоритм (0x80090008) ... 215
Предупреждение «Нет полного доверия к сертификату подписи» или «Подпись математически корректна, но нет полного доверия к сертификату подписи» ... 217
Ошибка установки свойства в контекст сертификата (0x80092004) ... 219
Выбранный вами сертификат не действителен, продолжить его использование? ... 220
Отказано в доступе. (0x80090010) ... 221
Не найден используемый криптопровайдер. Возможно он не установлен, запрещен или не поддерживается. ... 223
Носитель ключевого контейнера не поддерживается данной лицензией (0x80070057) ... 224
КриптоАРМ зависает (не отвечает) в момент выбора сертификата подписи ... 225
Отсутствует личный сертификат для расшифрования ... 228
Неизвестный криптографический алгоритм. (0x80091002) ... 230
Неправильное значение индекса. (0x80091008) ... 232

Error initialize resource dll, неизвестная ошибка 234

Данные настройки для этого продукта повреждены. Обратитесь в службу поддержки. (0x0000064a) 235

Отсутствует список аккредитованных УЦ 237

Внутренняя ошибка (CSP). (0x80090020) 240

Установка сертификатов из файла p7b и cer 241

При установке следующих сертификатов возникли ошибки 249

Не поддерживается безопасное удаление файлов с атрибутом "сжатый" 250

В URL (сетевом адресе) указан неподдерживаемый протокол (0x00002ee6) 251

Исходные оглавления

Операции с сертификатами 252

Операции со справочниками назначений сертификата и ключевыми носителями 253

Управление профилями 254

Параметры программы 255

Операции с запросами на сертификат 256

Операции со списками отзыва сертификатов 257

Операции со списками доверенных сертификатов и криптопровайдерами 258

Часто задаваемые вопросы 259

Работа с программой 261

Общие сведения 262

Открыть статью на сайте

Содержание

Общие сведения

- Где скачать дистрибутив КриптоАРМ и как его правильно выбрать?
- Как установить КриптоАРМ?
- Где купить лицензию на КриптоАРМ?
- Временная лицензия и срок ее действия
- Проверка наличия ГОСТ - криптопровайдера
- Установка лицензии
- Удаление программы

Параметры программы

- Интерфейс программы
- Общие настройки
- Режим "Квалифицированная подпись"
- Параметры прокси-сервера
- Интерактивный режим

Управление профилями

- Операции с профилями
- Общие параметры профиля
- Настройки операции подписи
- Настройки операции шифрования
- Настройки операции расшифрования
- Настройки управления интерфейсом
- Настройки использования политик сертификатов
- Настройки верификации сертификатов
- Настройки службы штампов времени TSP
- Настройки службы актуальных статусов OCSP
- Настройки каталогов хранения файлов

Операции с сертификатами

- Проверка на квалифицированность
- Как получить новый сертификат?
- Как создать самоподписанный сертификат?
- Импорт (установка) сертификата
- Хранение сертификатов
- Как проверить статус сертификата?
- Работа с квалифицированными сертификатами
- Просмотр информации о сертификате
- Фильтрация и сортировка сертификатов
- Печать сертификата

- Экспорт сертификата
- Удаление сертификата

Операции с запросами на сертификат

- Как создать запрос на получение сертификата
- Просмотр информации о запросах, фильтрация и сортировка запросов в списке
- Как создать запрос на аннулирование сертификата

Операции со списками отзыва сертификатов

- Установка списка отзывов в хранилище
- Просмотр информации о списках
- Фильтрация и сортировка списков отзыва
- Экспорт и удаление списков отзыва

Операции со списками доверенных сертификатов и криптопровайдерами

- Как создать список доверенных сертификатов?
- Установка списка в хранилище
- Просмотр информации о списке
- Фильтрация и сортировка списка
- Экспорт и удаление списка
- Операции с криптопровайдерами

Операции со справочниками назначений сертификата и ключевыми носителями

- Создание нового назначения
- Просмотр свойств назначения
- Импорт, экспорт и удаление назначения
- Операции с ключевыми носителями

Работа с программой

- Как подписать электронный документ?
- Добавление заверяющей подписи
- Как добавить соподпись (параллельную подпись)?
- Как проверить электронную подпись?
- Снятие и проверка подписи
- Как зашифровать данные?
- Как расшифровать данные?
- Как подписать и зашифровать электронный документ?
- Как расшифровать и проверить подпись на электронном документе?
- Как просмотреть зашифрованный документ?
- Как получить штамп в службе штампов времени?
- Как просмотреть штамп времени?

Часто задаваемые вопросы

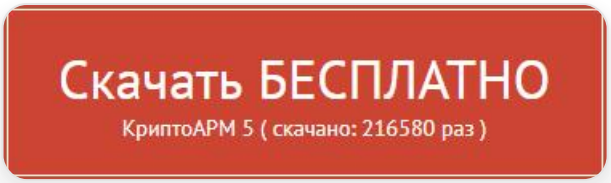
- Ошибка пакета Windows installer

- Ошибка в ходе установки сборки
- Внутренняя ошибка 2739
- Не удалось открыть подраздел: UNKNOWN/Components
- Координатор установщика Windows
- При установке следующих сертификатов возникли ошибки.
- Ошибка построения пути сертификации.
- Ошибка сохранения данных.
- Некорректный формат лицензии.
- Ошибка исполнения функции (0x0000065b)
- Указан неправильный алгоритм (0x80090008)
- Предупреждение «Нет полного доверия к сертификату подписи»
- Ошибка установки свойства в контекст сертификата (0x80092004)
- Выбранный вами сертификат не действителен, продолжить его использование?
- Отказано в доступе. (0x80090010)
- Не найден используемый криптопровайдер. Возможно он не установлен, запрещен или не поддерживается.
- Носитель ключевого контейнера не поддерживается данной лицензией (0x80070057)
- КриптоАРМ зависает (не отвечает) в момент выбора сертификата подписи
- Отсутствует личный сертификат для расшифрования
- Неизвестный криптографический алгоритм. (0x80091002)
- Неправильное значение индекса. (0x80091008)
- Error initialize resource dll, неизвестная ошибка
- Данные настройки для этого продукта повреждены. Обратитесь в службу поддержки. (0x0000064a)
- Отсутствует список аккредитованных УЦ
- Внутренняя ошибка (CSP). (0x80090020)
- Установка сертификатов из файла p7b и cer

Открыть статью на сайте

Где скачать дистрибутив КриптоАРМ и как его выбрать?

КриптоАРМ - программа для защиты электронных документов. Используется для создания и проверки электронной подписи (в т.ч. усиленной квалифицированной электронной подписи), шифрования и расшифрования файлов, генерации ключей электронной подписи, создания самоподписанных сертификатов.



Нажмите на кнопку Скачать БЕСПЛАТНО для загрузки программы. При первой установке на рабочем месте активируется бесплатный период сроком на 14 дней.

КриптоАРМ Старт - бесплатная версия, в которой для создания электронной подписи и шифрования применяются встроенные криптопровайдеры ОС Windows. Включена проверка ГОСТ подписи при наличии СКЗИ КриптоПро CSP.

КриптоАРМ Стандарт Плюс - базовая версия, предназначенная для подписи и шифрования электронных документов. Поддерживает российские ГОСТ алгоритмы подписи и шифрования, внешние ключевые носители (usb-токены, смарт-карты).

КриптоАРМ Терминал - серверная версия (для установки на серверных ОС). Поддерживает работу в режиме терминального сервера, предоставляющего централизованный доступ пользователям локальной сети к программе на сервере.

СКЗИ КриптоАРМ 5 - сертифицированная версия, соответствующая требованиям № 63-ФЗ «Об электронной подписи». Дополнительно требуется приобрести дистрибутив на CD с формуляром, и СКЗИ КриптоПро CSP 4.0

При первой установке на рабочем месте автоматически устанавливается полнофункциональная версия программы «КриптоАРМ Стандарт Плюс» сроком на четырнадцать дней. После истечения этого срока программа перейдет в режим Старт, что заметно снизит ее возможности.

Приобрести лицензионный ключ на любую версию «КриптоАРМ» можно в нашем интернет-магазине круглосуточно, семь дней в неделю.

Важно отметить, что при повторных установках программы «КриптоАРМ» на одном и том же рабочем месте, бесплатный период использования уже не может быть активирован.

Открыть статью на сайте

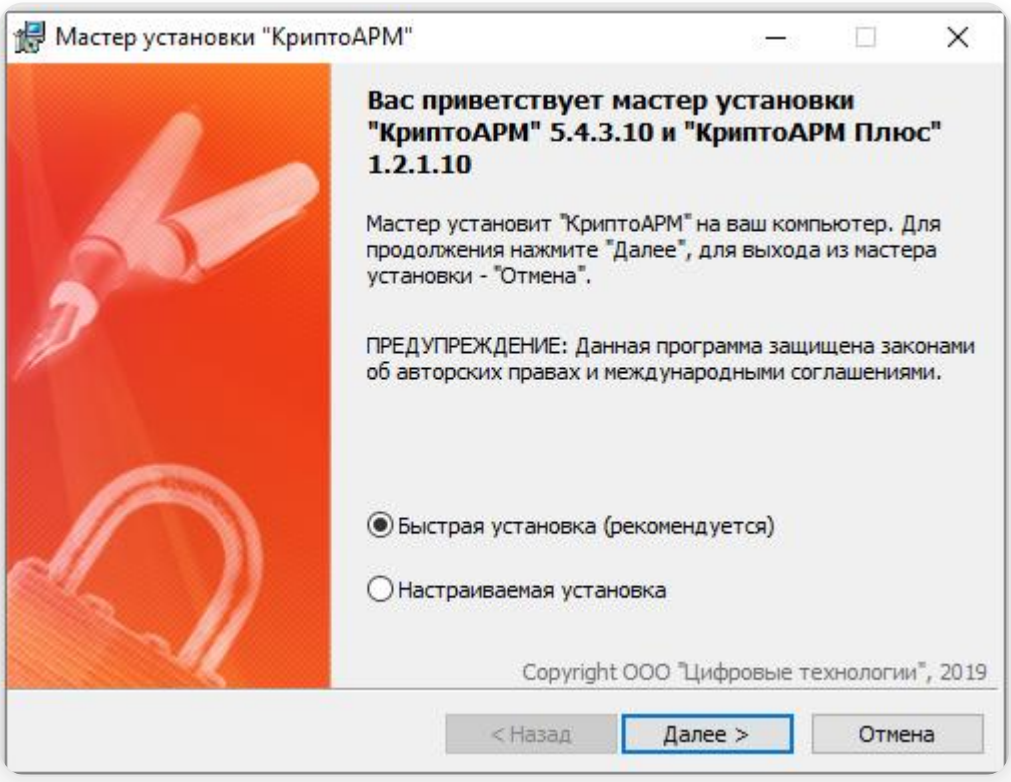
Как установить КриптоАРМ?

Установка программы «КриптоАРМ» должна осуществляться пользователем, имеющим права Администратора системы.

1. Для установки программы «КриптоАРМ» запустите на исполнение файл **Trusted- Desktop x.x.exe** (где x.x. – номер версии). Откроется мастер установки «КриптоАРМ».

2. На этом шаге выберите вариант установки:

   - **Быстрая установка** (рекомендуется).
     Быстрая установка программы, включает все дополнительные компоненты. Требует наибольшего объема места на диске.
   - **Настраиваемая установка**
     Установка с выбором дополнительных компонентов (модулей к программе). Рекомендуется для опытных пользователей.

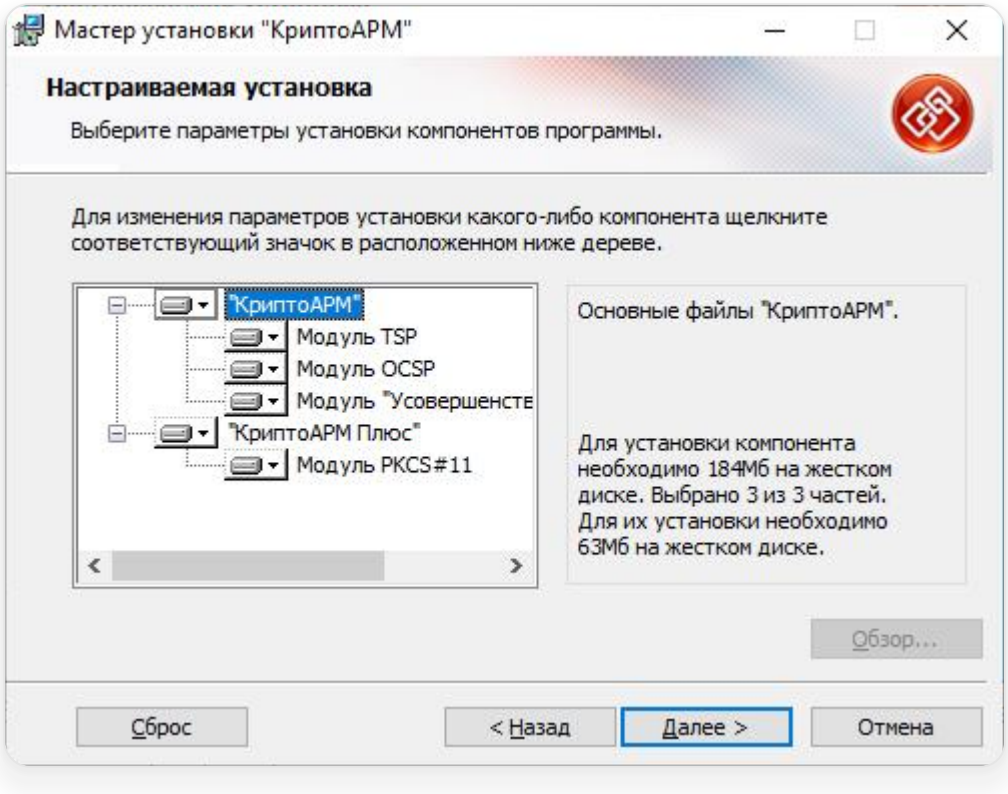


3. Нажмите **Далее** для продолжения установки (или **Отмена** для выхода из мастера установки).

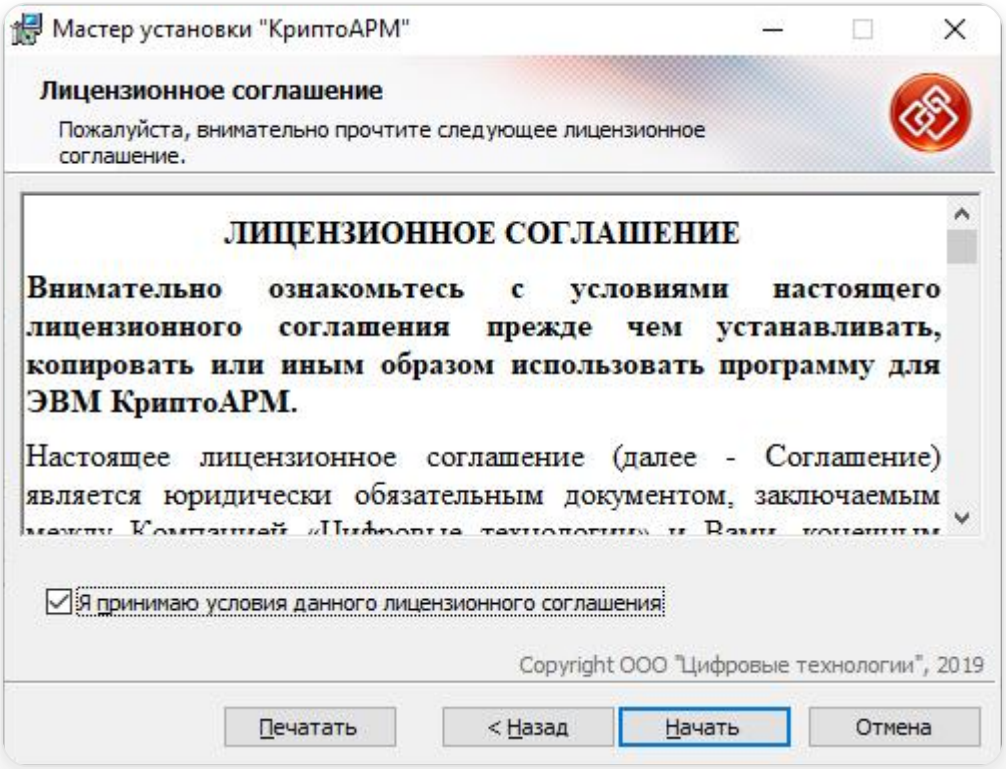
4. Следующий шаг зависит от того, какой вид установки вы выбрали.

   При выборе **быстрой установки** вы сразу переходите на следующий шаг установки.
   При выборе **настраиваемой установки** вы можете указать:

- какие из модулей нужно установить
- директорию на вашем компьютере, куда приложение будет установлено.



5. Ознакомьтесь с условиями лицензионного соглашения, в случае согласия отметьте соответствующий пункт и нажмите **Начать**.



6. Начнется установка программы на компьютер.

7. По окончании установки нажмите кнопку **Готово**. Для завершения установки перезагрузите компьютер.

8. После установки программы
   - в меню **Пуск - Программы** появится группа «КриптоАРМ», которая содержит меню вызова главного окна программы «КриптоАРМ», документации пользователя и программиста в формате PDF и меню мастера удаления программы.
   - в указанном при установке каталоге (по умолчанию в каталоге Program Files) будут созданы подкаталоги Digt\Trusted\Desktop.

	Программа «КриптоАРМ» распространяется с уже введенным ключом временной лицензии, которая начинает действовать с момента установки и запуска программы. Более подробно о временной лицензии и сроке ее действия можно узнать в соответствующей главе.

Открыть статью на сайте

Где купить лицензию на КриптоАРМ ?

Купить программу «КриптоАРМ» вы можете:

- Непосредственно в компании "Цифровые технологии".
  Для покупки товаров нажмите на кнопку **Магазин** в верхней части сайта cryptoarm.ru. Ознакомьтесь с инструкцией как оформить заказ или позвоните по телефону +7 (8362) 33-70-50. Если у вас возникнут вопросы, то вы можете написать на sales@cryptoarm.ru или задать их менеджеру в онлайн-чате, доступном в правом нижнем углу сайта.
- У официальных партнеров компании "Цифровые технологии" (ИТ-разработчики, удостоверяющие центры, системные интеграторы, интернет-магазины). Полный список региональных компаний-партнеров и их контактную информацию вы найдете на сайте в разделе "Партнеры".

Открыть статью на сайте

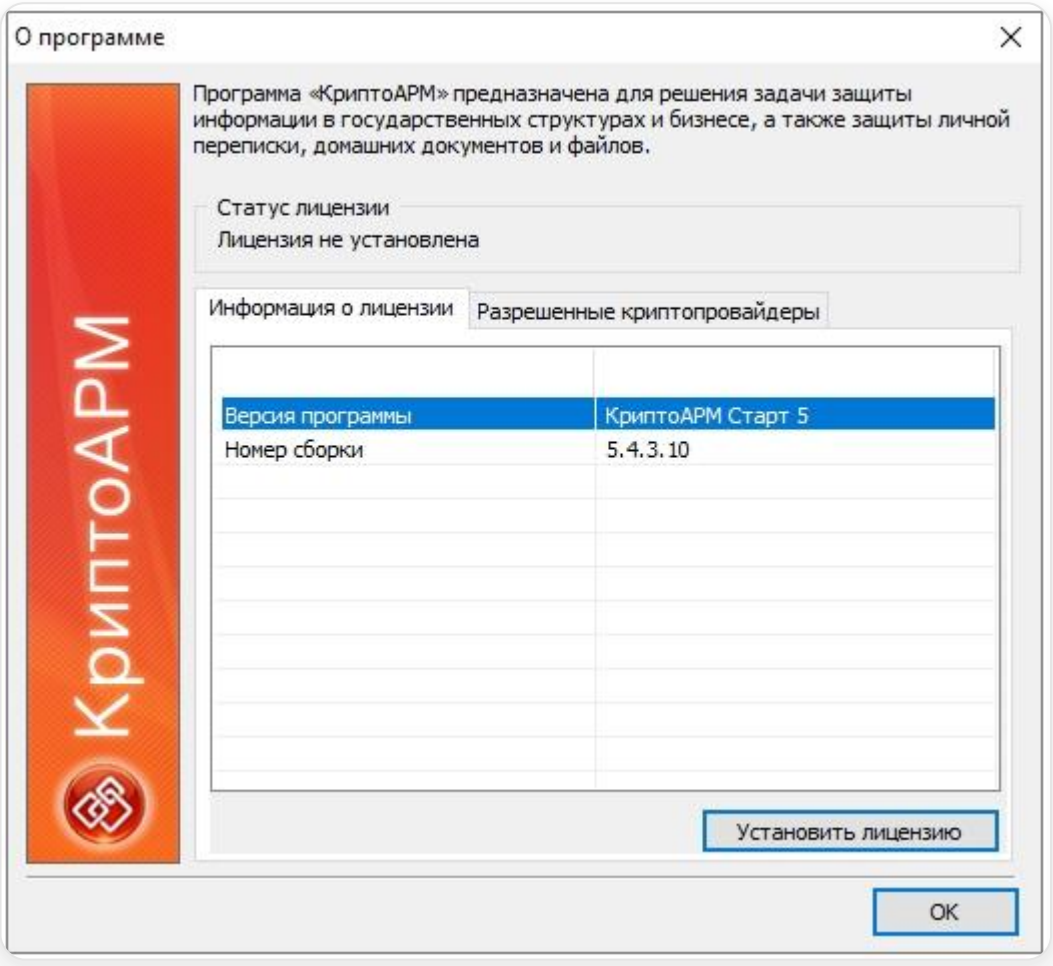
Временная лицензия и срок ее действия

Чтобы упростить первые шаги по изучению программы “КриптоАРМ” не требуется запрашивать временную лицензию.

В течение 14 дней с момента установки “КриптоАРМ” работает в режиме “Стандарт Плюс” с максимальным набором функциональных возможностей.

Ознакомительная версия НЕ для коммерческого использования. По истечении 14 дней программа автоматически переключается на версию “Старт”, которая имеет ряд ограничений по сравнению с полнофункциональной версией.

Для перехода на другую версию достаточно просто приобрести и установить специальную лицензию. Переустанавливать программу при этом не требуется.



Открыть статью на сайте

Проверка наличия ГОСТ - криптопровайдера

При каждом запуске программы «КриптоАРМ» осуществляется проверка установленных в системе криптопровайдеров, использующих в своей работе алгоритмы ГОСТ. Если криптопровайдеры не обнаружены, то появляется соответствующее предупреждение.

Вы можете настроить отображение данного предупреждения в настройках параметров программы во вкладке "Общие"



Криптопровайдеры, использующие алгоритмы ГОСТ, необходимы для полноценной работы.

Открыть статью на сайте

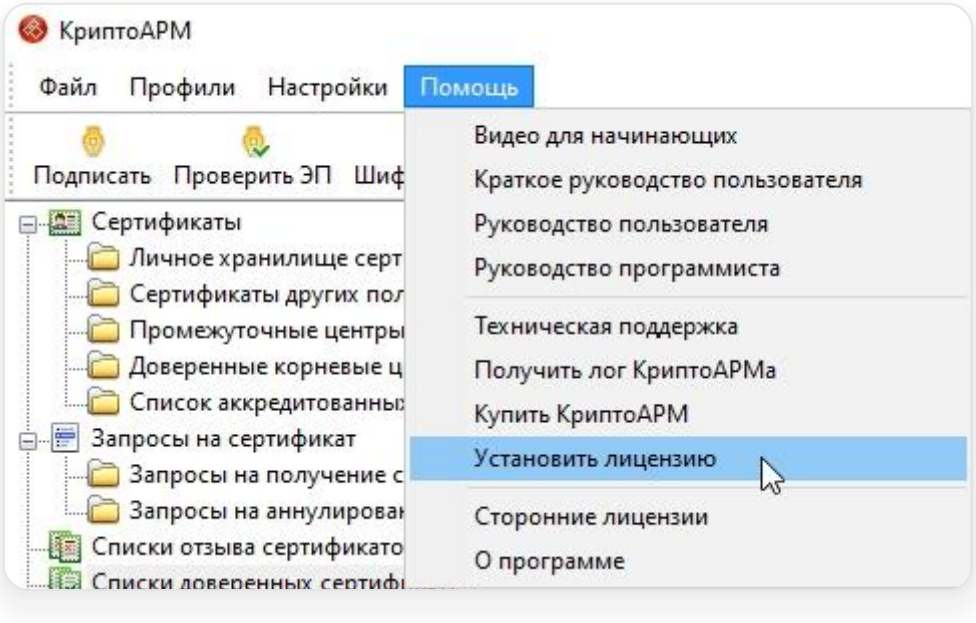
Установка лицензии

Версия «КриптоАРМ Старт» не требует регистрации и время ее использования не ограничено. Версии «КриптоАРМ Стандарт» и «КриптоАРМ Стандарт Плюс» требуют ввода лицензионного ключа. Как приобрести лицензию к программе «КриптоАРМ», читайте в инструкции "Где скачать КриптоАРМ и как его выбрать?"

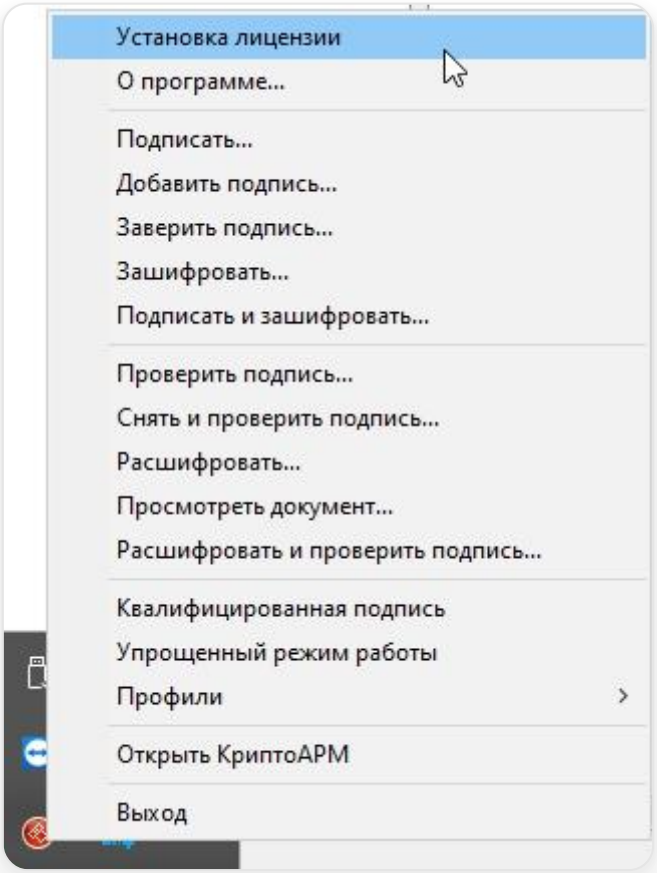
Регистрация продукта должна осуществляться пользователем, имеющим права администратора системы.

Зарегистрировать программу «КриптоАРМ» (установить лицензию к программе) вы можете следующими способами:

- через главное окно (**Помощь - Установить лицензию**)

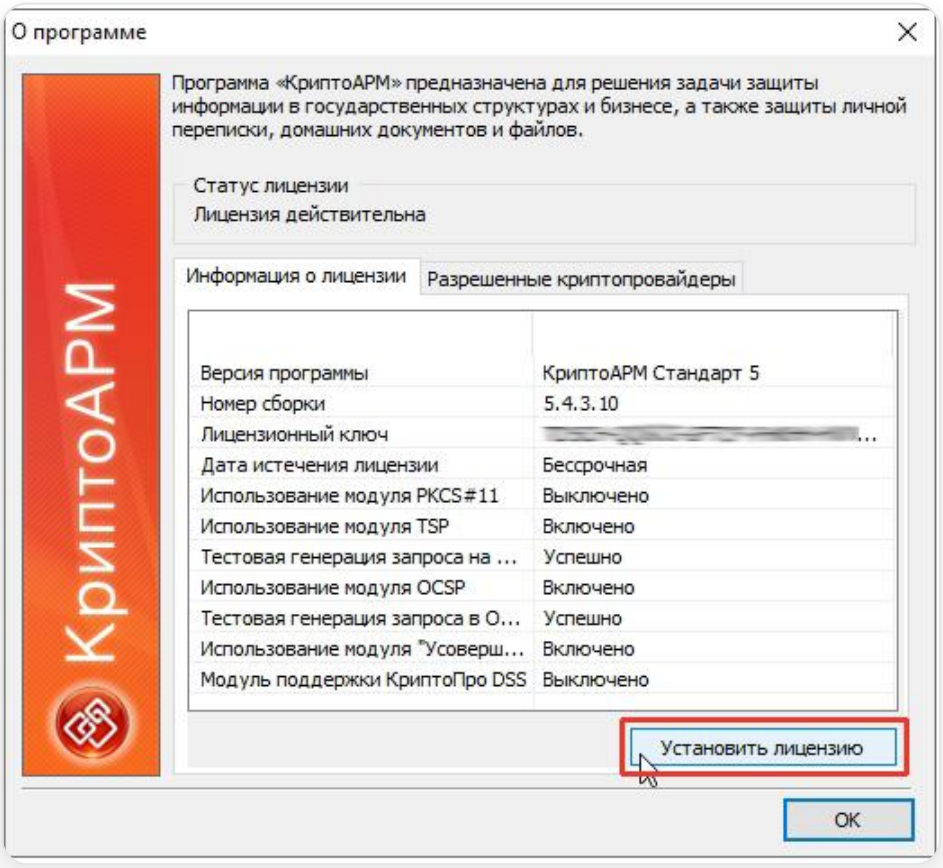


- через значок на панели задач (**Установка лицензии**)

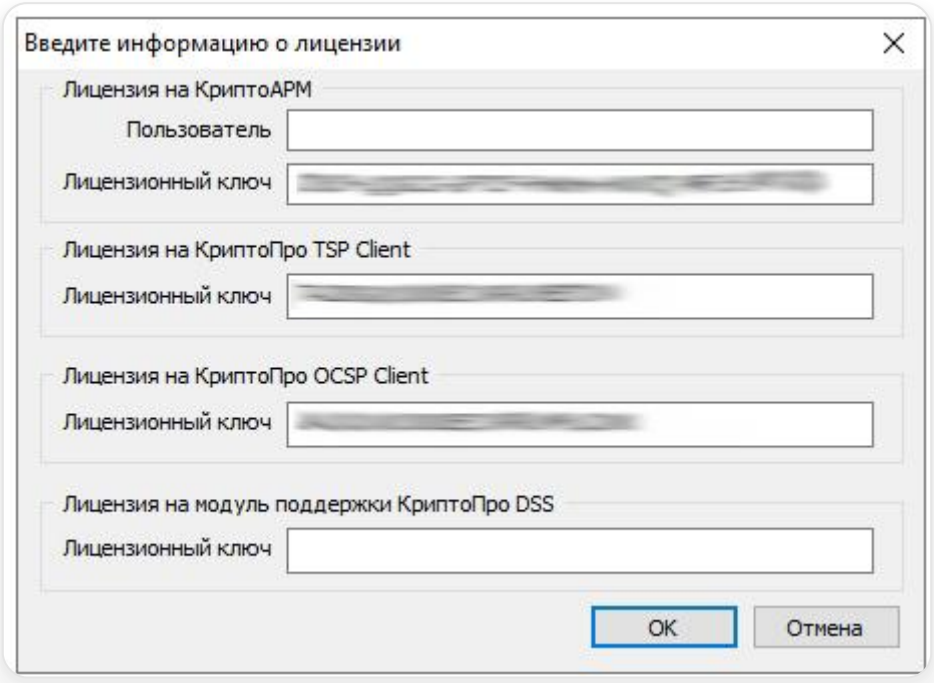


Чтобы зарегистрировать программу, выполните следующие шаги:

Шаг 1. В окне **О программе** нажмите на кнопку **Установить лицензию**:



Шаг 2. Доступ к функциональности программы «КриптоАРМ» и его модулям регулируется лицензиями. Введите информацию согласно выданной вам лицензии:



При успешной регистрации программы «КриптоАРМ» возникнет сообщение об этом.

В закладке **Информация о лицензии** отображается информация в соответствии с используемой лицензией на программу «КриптоАРМ»:

- версия продукта
- номер сборки дистрибутива программы
- серийный номер лицензии
- имя пользователя программы
- организация, которую представляет пользователь
- адрес электронной почты пользователя
- использование дополнительных модулей
- другие

	При работе с Модулем TSP проверяется статус лицензии на программное обеспечение «КриптоПро TSP Client».
	При работе с Модулем OCSP проверяется статус лицензии на программное обеспечение «КриптоПро OCSP Client».
	При использовании лицензии к комплекту «КриптоАРМ СтандартPRO» автоматически включаются лицензии на модули TSP и OCSP.

Открыть статью на сайте

Удаление КриптоАРМ

Удалить программу «КриптоАРМ» можно следующими способами:

- с помощью программы установки и удаления «КриптоАРМ»;
- стандартными средствами операционной системы Windows.

Для удаления «КриптоАРМ» стандартными средствами Windows:

1. Нажмите на кнопку **Пуск**, в главном меню Windows активизируйте команду **Настройка - Панель управления**.
2. Откроется окно **Панель управления**: активизируйте ярлык **Установка и удаление программ**.
3. Откроется одноименное окно, в котором перечислены программы, установленные на компьютере.
4. Выберите в списке программу «КриптоАРМ»: нажмите на кнопку **Удалить** и подтвердите решение об удалении.
5. Ход процесса удаления будет отображаться в виде индикатора прогресса в специальном окне. По завершении процесса программа «КриптоАРМ» будет удалена с компьютера и из списка элементов **Установленные программы**.

Для удаления «КриптоАРМ» с помощью программы установки:

1. Запустите на исполнение файл **TrustedDesktop x.x.exe** из дистрибутива программы. Откроется мастер установки «КриптоАРМ». Нажмите кнопку **Далее**.
2. Откроется окно, в котором выберите операцию **Удалить**:
3. Возникнет сообщение с предложением выполнить процедуру удаления: нажмите на кнопку **Удалить**.
4. Начнется удаление программы «КриптоАРМ». Ход процесса отображается в виде индикатора прогресса.
5. После завершения этого процесса возникнет сообщение с информацией о том, что программа удалена. Нажмите на кнопку **Готово**.



Для завершения процедуры удаления необходимо выполнить перезагрузку компьютера.

Открыть статью на сайте

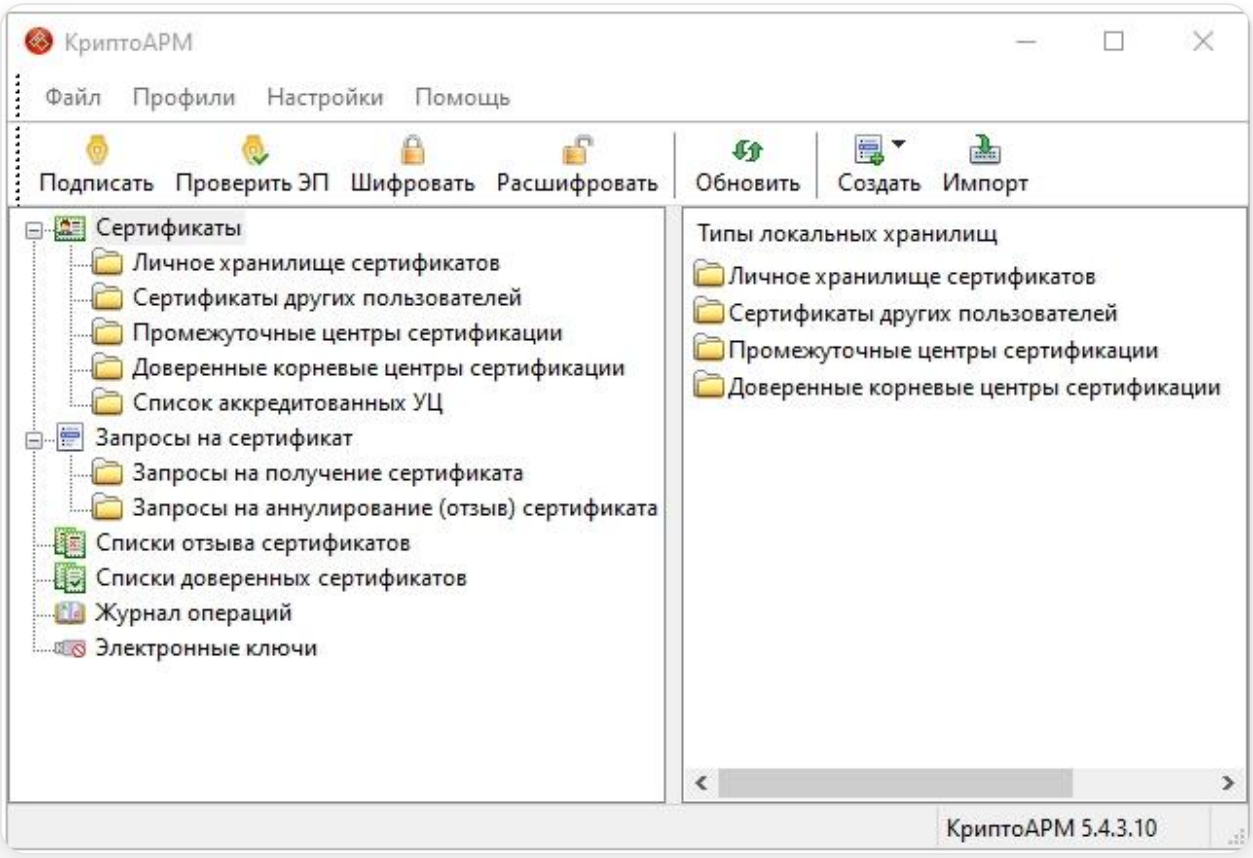
Интерфейс программы

Вы можете работать с программой «КриптоАРМ», выбрав наиболее удобный для вас вариант:

- Главное окно программы: предназначено для выполнения криптоопераций, а также управления криптопровайдерами, сертификатами и настройками программы
- Значок на панели задач, который имеет контекстное меню с полным перечнем операций.
- Проводник Windows (контекстное меню файла)

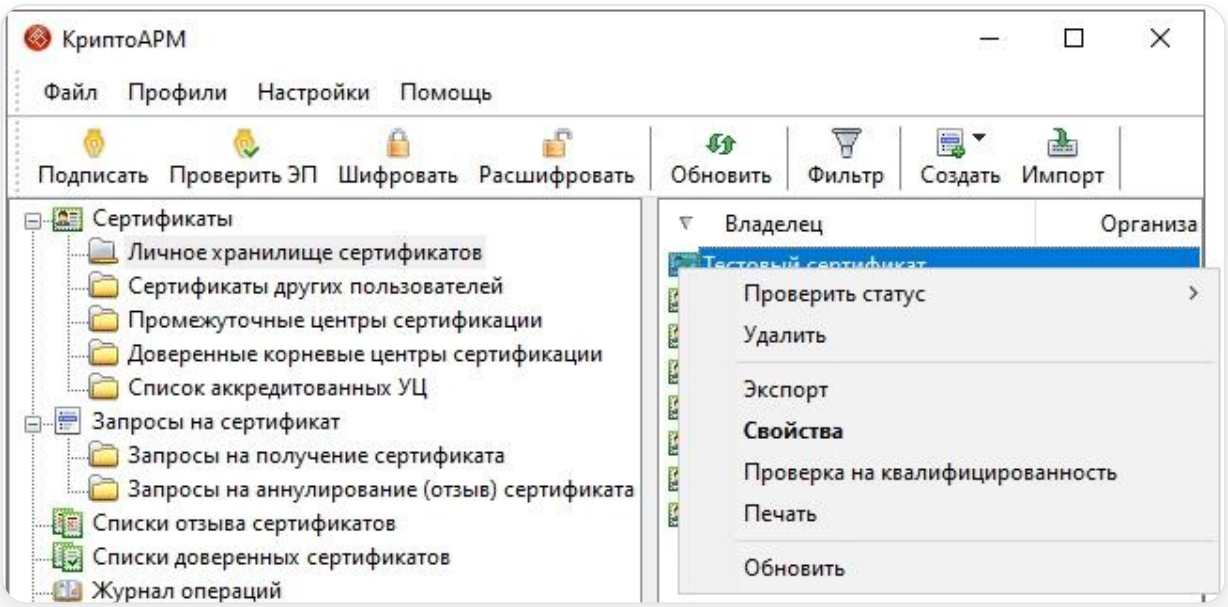
Главное окно программы

В левой части главного окна расположено дерево объектов, которое включает в себя основные разделы: «Сертификаты», «Запросы на сертификат», «Списки отзыва сертификатов», «Списки доверенных сертификатов» и «Электронные ключи». В правой части главного окна отображаются объекты, входящие в разделы дерева из левой его части:

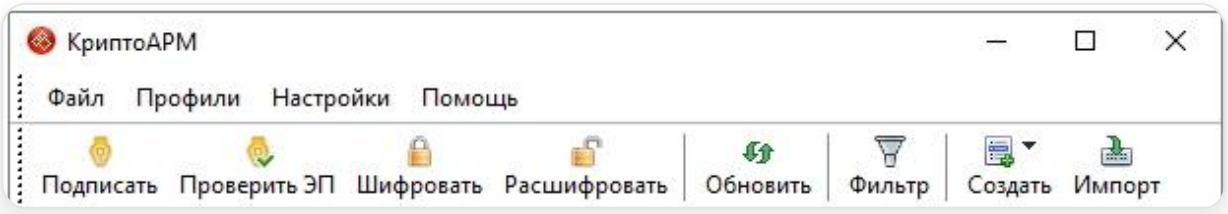


Вы можете работать с сертификатами, списками, выполнять криптооперации несколькими способами:

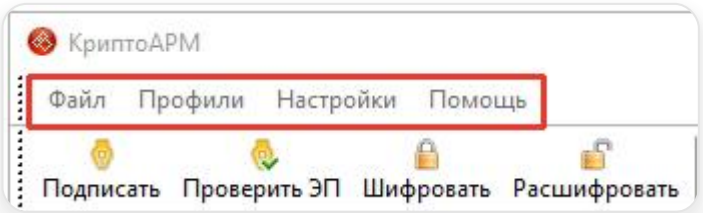
- Непосредственно в самих папках дерева, используя **контекстное меню** (открывается правой клавишей мыши на объекте/пустом поле):



- с помощью **специальных значков**, размещенных над деревом папок на специальной панели:

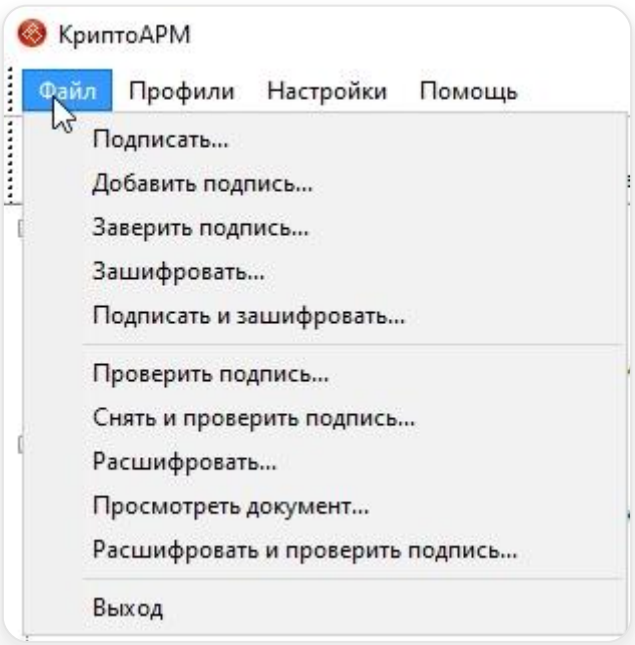


- через **верхнюю панель** главного окна:

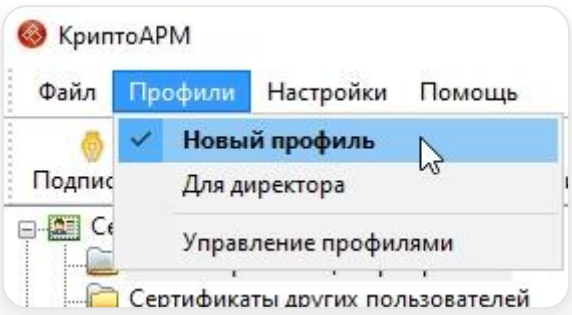


Возможности верхней панели главного окна

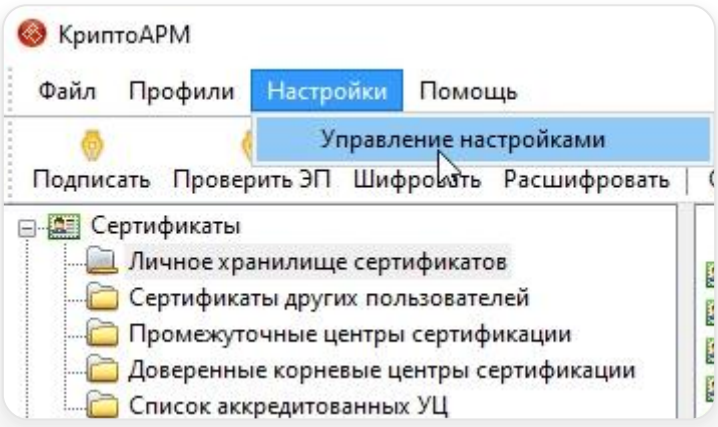
«Файл». Здесь вы можете выбрать нужную вам операцию.



«Профили». Меню для выбора профиля (индивидуальной настройки) по умолчанию и управления профилями. Профиль по умолчанию отмечен жирным шрифтом.

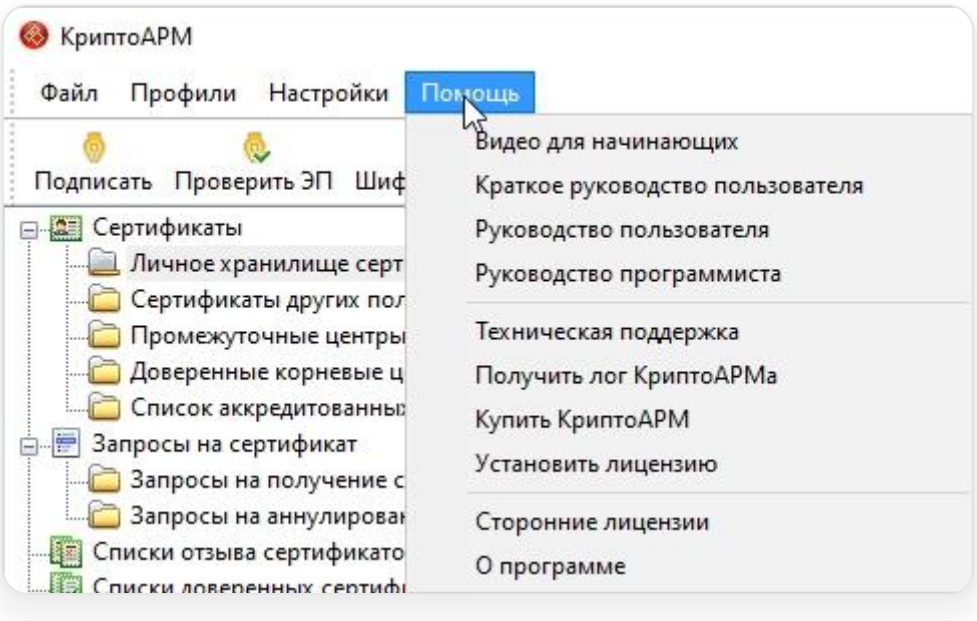


«Настройки». Меню для управления общими настройками программы.



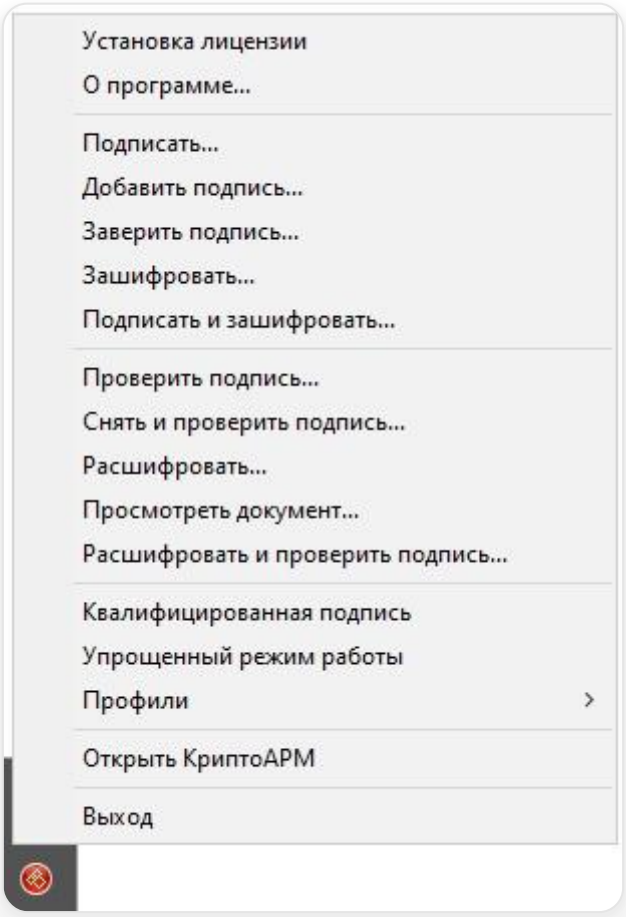
«Помощь». Меню, в котором вы можете открыть краткое или полное руководство пользователя, руководство программиста, перейти на веб страницу технической поддержки

или интернет-магазина, получить лог программы, установить лицензию и просмотреть информацию о программе.



КриптоАРМ на панели задач

Вы можете работать с программой «КриптоАРМ» через уведомление на панели задач. В настройках программы вы можете указать, чтобы «КриптоАРМ» присутствовал на панели задач в правом нижнем углу экрана компьютера для быстрого выполнения криптографических операций.



При двойном щелчке на значке «КриптоАРМ» открывается главное окно программы.

Используя значок уведомления на панели задач, вы можете:

- установить лицензию к программе «КриптоАРМ»
- просмотреть информацию о программе «КриптоАРМ»
- подписывать файлы и проверять корректность подписи
- шифровать и расшифровывать файлы
- устанавливать пошаговый режим выполнения криптоопераций и режим «Квалифицированная подпись»
- выбирать настройки для выполнения криптоопераций
- работать через «КриптоАРМ» с рабочими каталогами (папки **Входящие/Исходящие**)
- переходить к работе с программой в главном окне

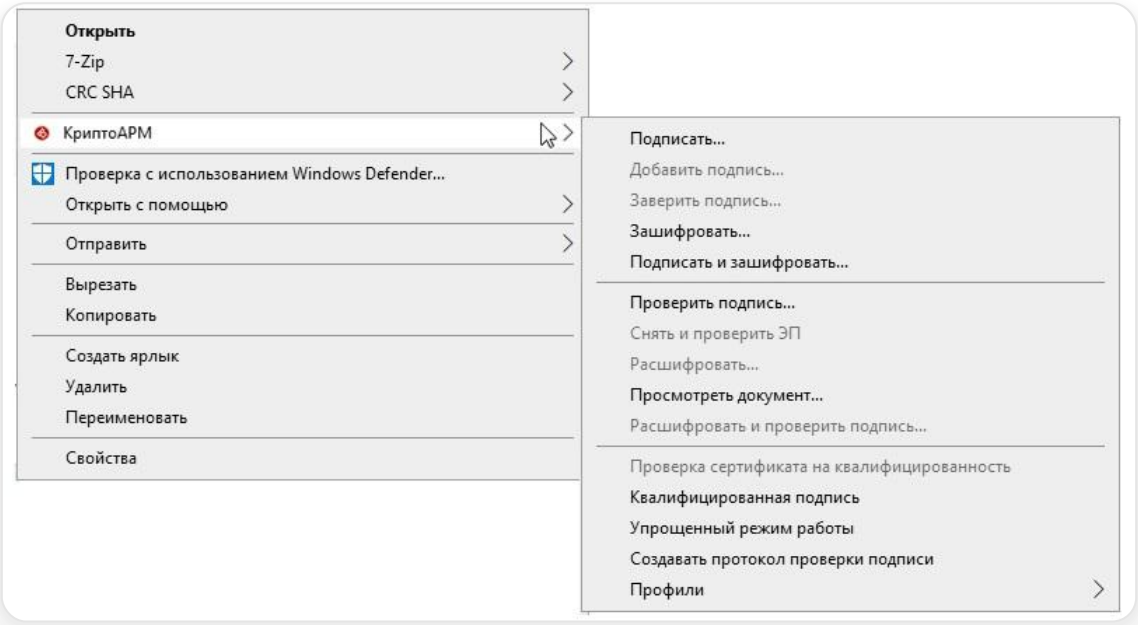
Для выполнения операций через панель задач:

1. Откройте программу «КриптоАРМ» (**Пуск > Программы > «КриптоАРМ»**)
2. Значок «КриптоАРМ» появится в правом углу на панели задач
3. Правой клавишей мыши откройте контекстное меню и выберите нужную операцию.

4. Далее следуйте шагам Помощника выбранной операции.

Через контекстное меню файла

Вы можете работать с программой «КриптоАРМ» в Проводнике Windows через контекстное меню файла:



Этот вариант позволяет быстро и удобно выполнять основные операции с электронными данными:

- подписать электронной подписью
- проверить корректность подписи
- зашифровать
- расшифровать файлы
- одновременно зашифровать и подписать данные
- одновременно расшифровать данные и проверить корректность электронной подписи
- установить режимы выполнения криптоопераций: «Упрощенный», «Квалифицированная подпись»
- проверить является ли сертификат квалифицированным
- выбрать настройку для выполнения криптоопераций

Для выполнения операций в Проводнике Windows:

- Откройте в Проводнике папку, где находится файл, для которого необходимо выполнить операцию(зашифровать, подписать и т.п.).

- Правой клавишей мыши откройте контекстное меню файла или сразу нескольких файлов и выберите нужную операцию.
- Далее следуйте шагам Помощника выбранной операции.
  В случае если вы выбрали для операции сразу несколько файлов, они будут обработаны последовательно.

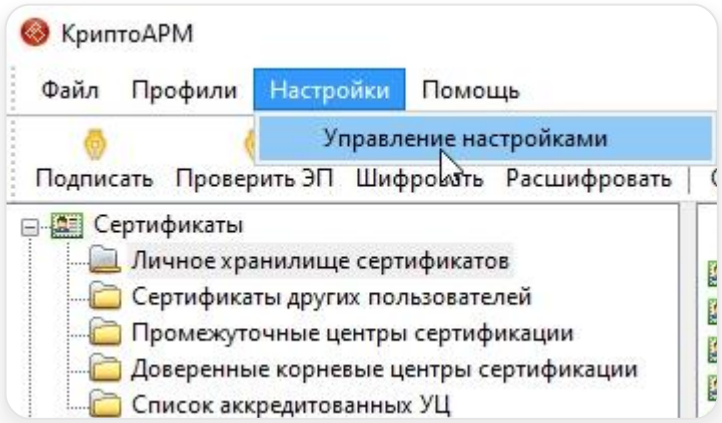
Открыть статью на сайте

Общие настройки

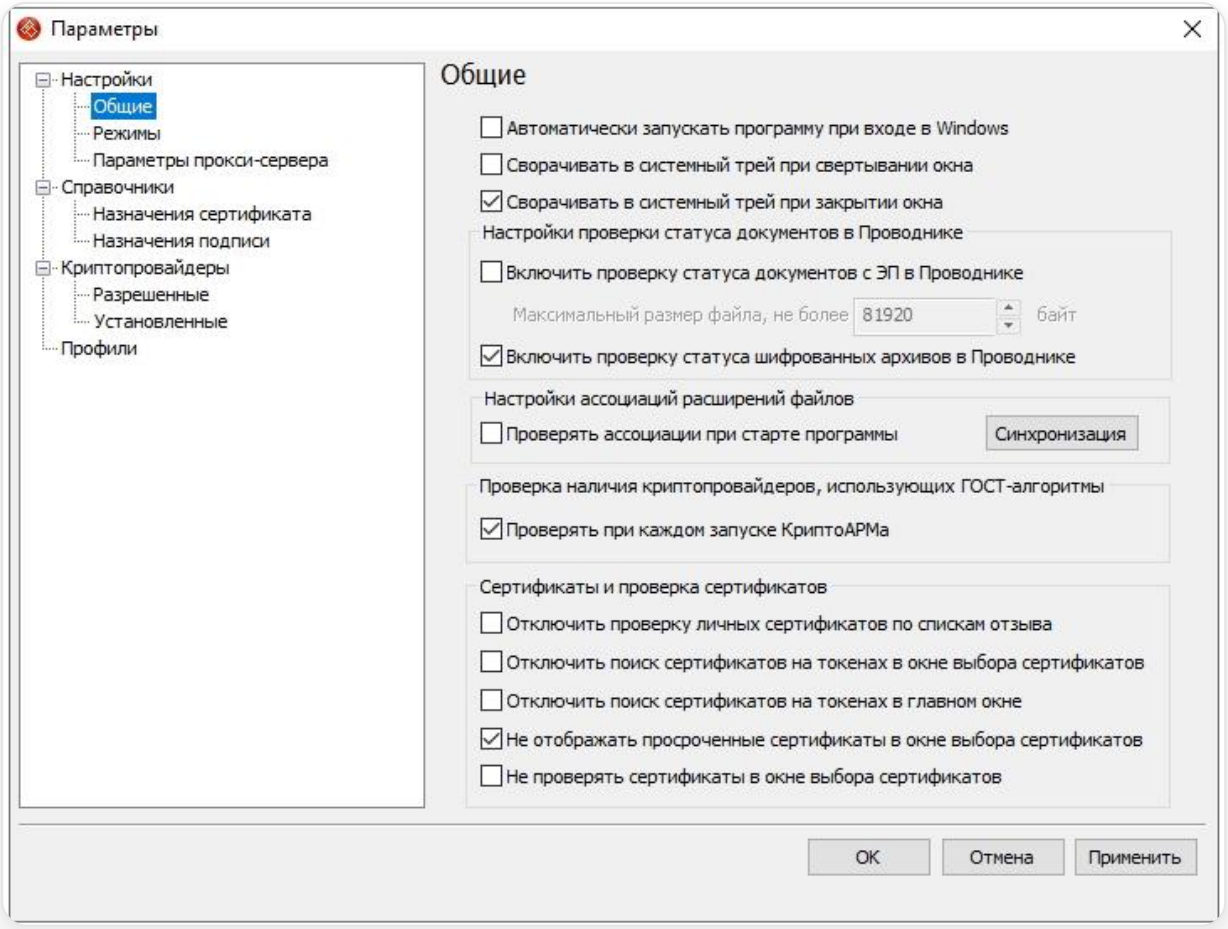
Настроить базовые параметры программы вы можете через главное окно программы.

Для этого выполните следующие шаги:

1. На верхней панели главного окна откройте меню **Настройки - Управление настройками**:



2. В окне **Параметры** найдите закладку **Настройки - Общие**:

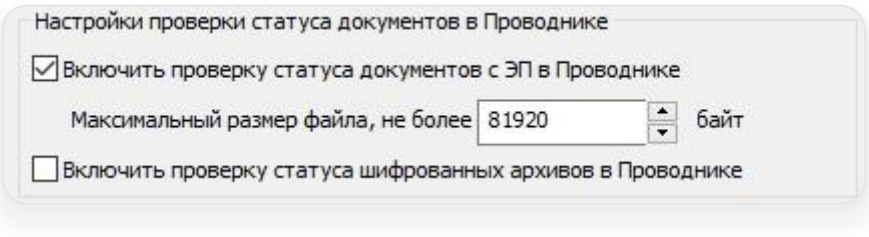


3. В окне вы можете настроить:

> - Автоматический запуск программы при входе в Windows;
> - Сворачивание главного окна программы в системный трей (панель задач) при свёртывании/ закрытии окна;
> - Проверку статуса документов в Проводнике Windows;
> - Ассоциации расширений файлов;
> - Проверку наличия криптопровайдеров, использующих алгоритмы ГОСТ;
> - Проверку сертификатов.

Настройка проверки статуса документов в Проводнике

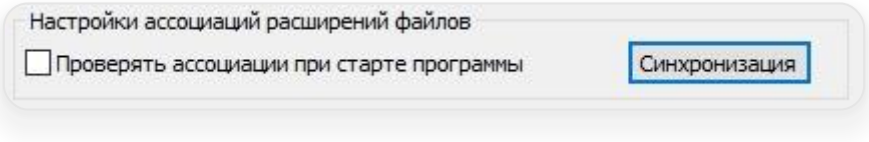
Зачастую проверка статуса документа, подписанного электронной подписью, занимает слишком много времени из-за очень большого размера проверяемого файла. Вы можете ограничить указать максимальный размер для проверяемых файлов и, тем самым, сократите свое время на обработку файлов. Для этого поставьте галочку напротив строки включить проверку статуса документов с ЭП в Проводнике и укажите предельный (максимальный) размер проверяемых файлов.



	Иногда автоматическая проверка статуса подписанных или зашифрованных документов может работать некорректно. Дело в том, количество overlays в операционной системе Windows ограничено 15-ю элементами. Если у вас установлено много программ, которые используют элементы overlays для отображения информации, то элементы приложения «КриптоАРМ» могут просто не попасть в это количество и соответственно не отображаться.

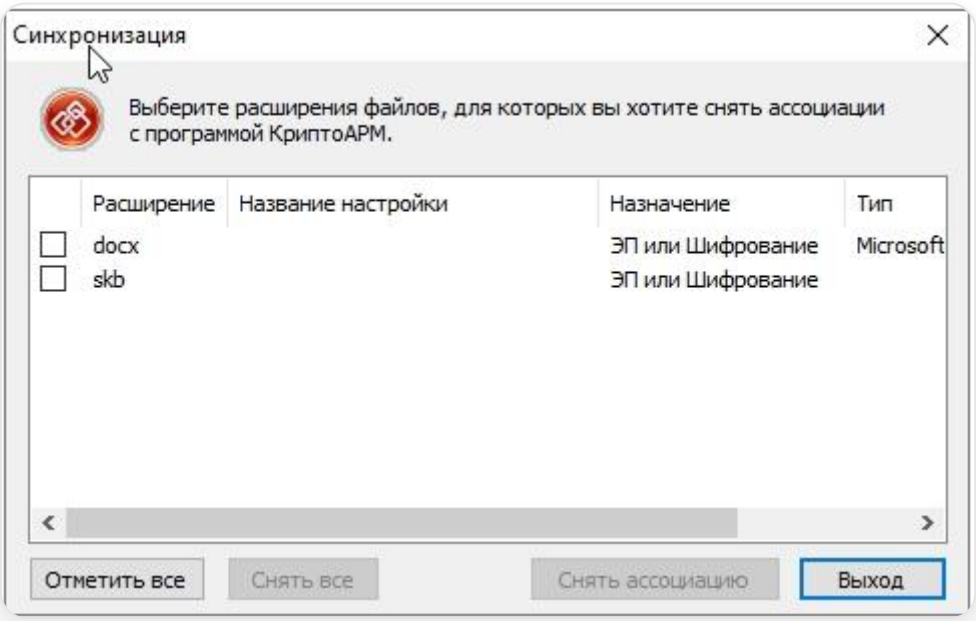
Настройка ассоциаций расширений файлов

Вы самостоятельно можете настраивать/ менять/ дополнять список файловых расширений (напр., *.sig), имеющих ассоциацию с программой «КриптоАРМ». Для просмотра и редактирования списка На верхней панели главного окна откройте меню **Сервис - Параметры программы - Общие** и нажмите на кнопку **Синхронизация**.



В окне **Сихронизация** содержится подробная информация об установленных ранее ассоциациях:

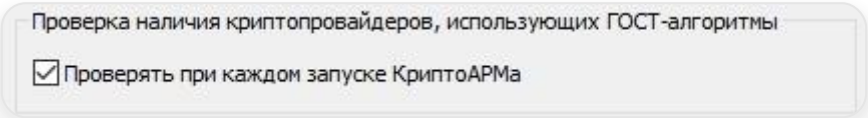
- «Расширение» - название расширения для файла.
- «Название настройки» - настройка, в которой по умолчанию выбрано данное расширение.
- «Назначение» - назначение файлов с указанным расширением в программе «КриптоАРМ».
- «Тип» - определяемый Windows тип файла.



Кнопка **Снять ассоциацию** позволяет выборочно снять (удалить) ассоциацию с файловых расширений. Чтобы снять ассоциацию с программой «КриптоАРМ» у всего списка файловых расширений, нажмите на кнопку **Отметить все** и затем **Снять все**. Восстановить ассоциацию для расширений, которые указаны в настройках, можно в самой настройке, нажав кнопку **Установить ассоциацию**. Подробнее об этом читайте в главе Настройки операции подписи.

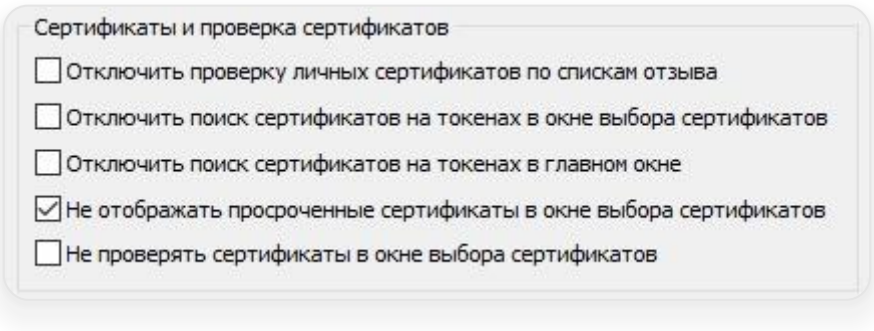
Настройка проверки наличия криптопровайдеров, использующих алгоритмы ГОСТ

При каждом запуске КриптоАРМ проверяет, установлен ли в системе криптопровайдер с поддержкой алгоритмов ГОСТ. Если такой криптопровайдер не будет обнаружен, КриптоАРМ покажет предупреждение. Если использование такого криптопровайдера не предполагается, предупреждение можно отключить, сняв галочку «Проверять при каждом запуске КриптоАРМ».



Настройка проверки сертификатов

Начиная с версии 5.3, КриптоАРМ проверяет личные сертификаты по спискам отзыва только если эта проверка выполняется пользователем вручную. При необходимости автоматическую проверку можно включить сняв галочку «Отключить проверку личных сертификатов по спискам отзыва».



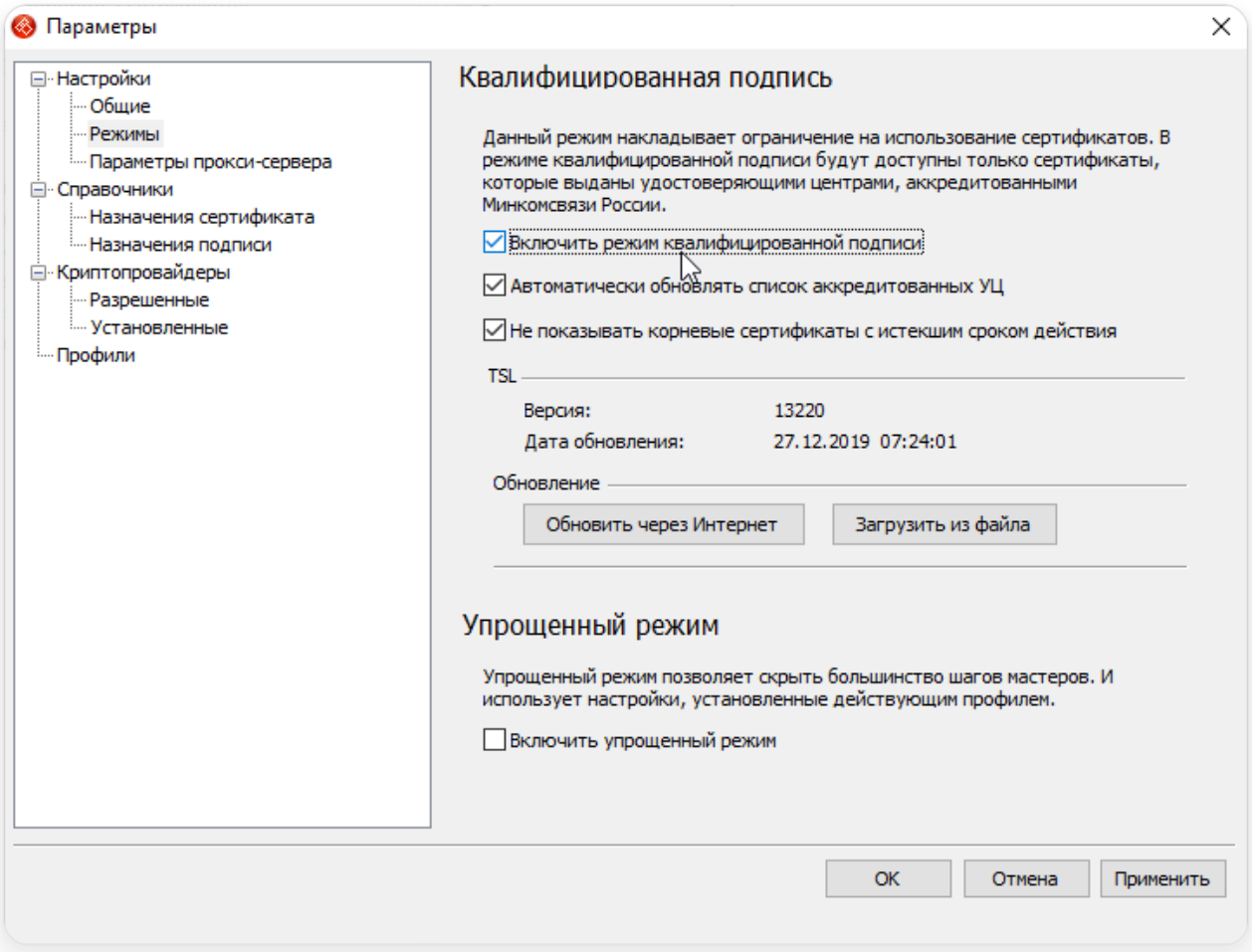
Галочка «Отключить поиск сертификатов на токенах в окне выбора сертификатов» позволяет не выполнять поиск сертификатов на отчуждаемых носителях. Это позволяет немного ускорить работу окна в случае, если не предполагается использование отчуждаемых носителей. При установке этой галочки в окне выбора сертификатов будут отображаться только сертификаты из хранилища личных сертификатов.

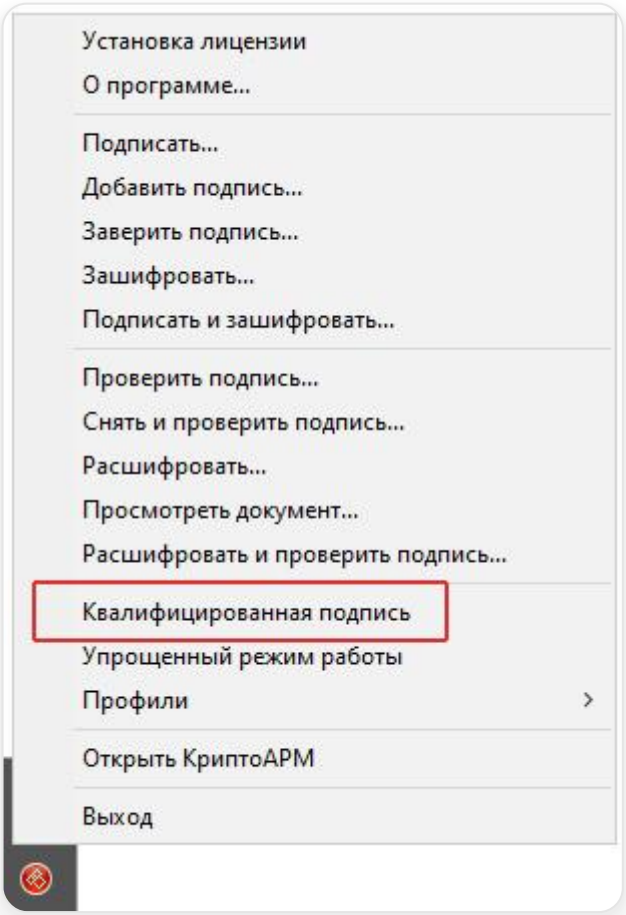
Открыть статью на сайте

Режим "Квалифицированная подпись"

Данный режим накладывает специальное ограничение на работу с цифровыми сертификатами. При включении данного режима вам станут доступны только сертификаты от удостоверяющих центров, аккредитованных Минкомсвязи Российской Федерации. В качестве фильтра используется актуальный список аккредитованных УЦ, размещаемый на портале Госуслуг.

Настроить режим «Квалифицированная подпись» вы можете на верхней панели инструментов в меню **Настройки > Управление настройками > Режимы**:





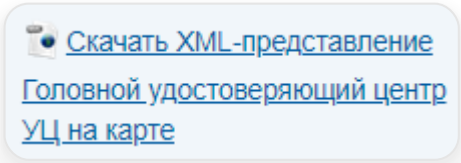
Быстро включить/отключить режим вы можете:

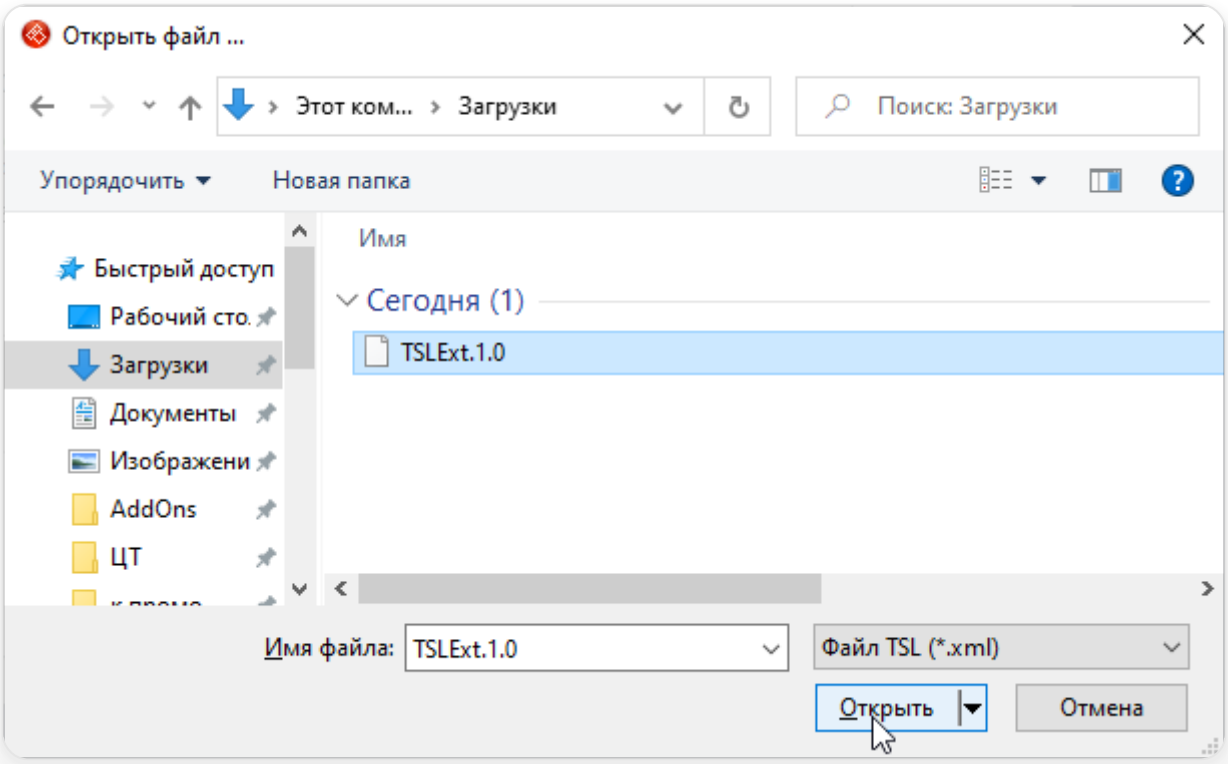
- через контекстное меню программы на панели задач
- через контекстное меню любого файла

Список аккредитованный УЦ постоянно обновляется. Удобнее настроить автоматическое обновление списка аккредитованных удостоверяющих центров, чтобы не обновлять каждый раз вручную. Для этого установите флаг напротив строки **Автоматически обновлять список аккредитованных УЦ**.

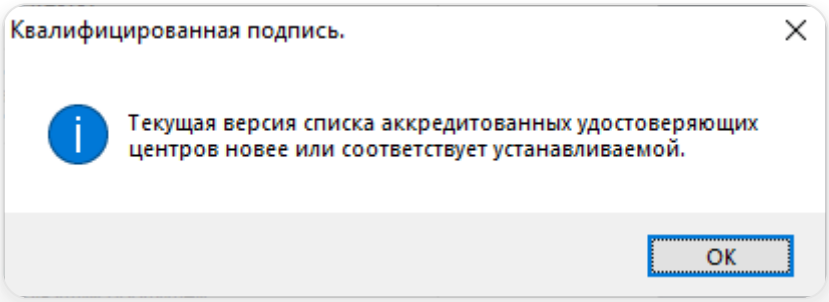
Обновить данный список (TSL) вы можете в любой момент. В верхнем меню главного окна откройте **Сервис > Параметры программы > Режимы** и выберите вариант обновления списка:

- Обновить через Интернет: вариант удобно использовать при стабильном быстром интернет-канале;
- Загрузить из файла: если доступ к интернету затруднен/отсутствует, рекомендуем скачать список в виде файла с портала Минкомсвязи («Скачать XML представление») и установить вручную. Файл TSL имеет формат *.xml.

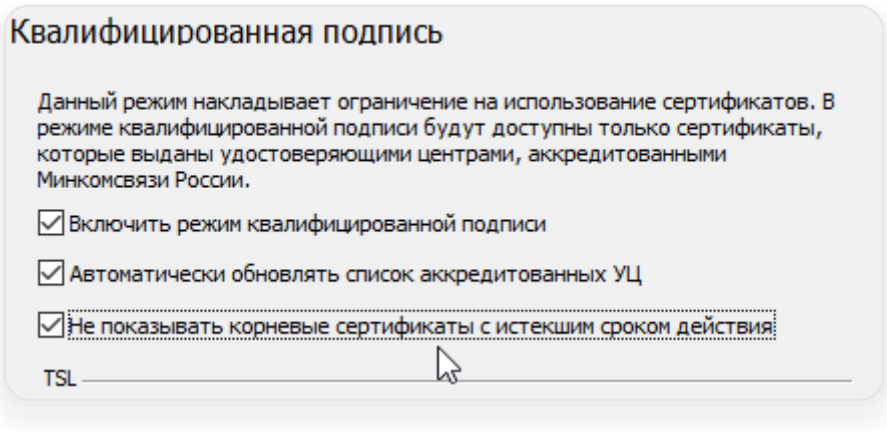




«КриптоАРМ» обновит список. Если установленный на ваш компьютер список по прежнему актуален, то программа сообщит об этом:



Для удобства работы со списками корневых сертификатов вы можете **отключить показ корневых сертификатов с истекшим сроком действия**.



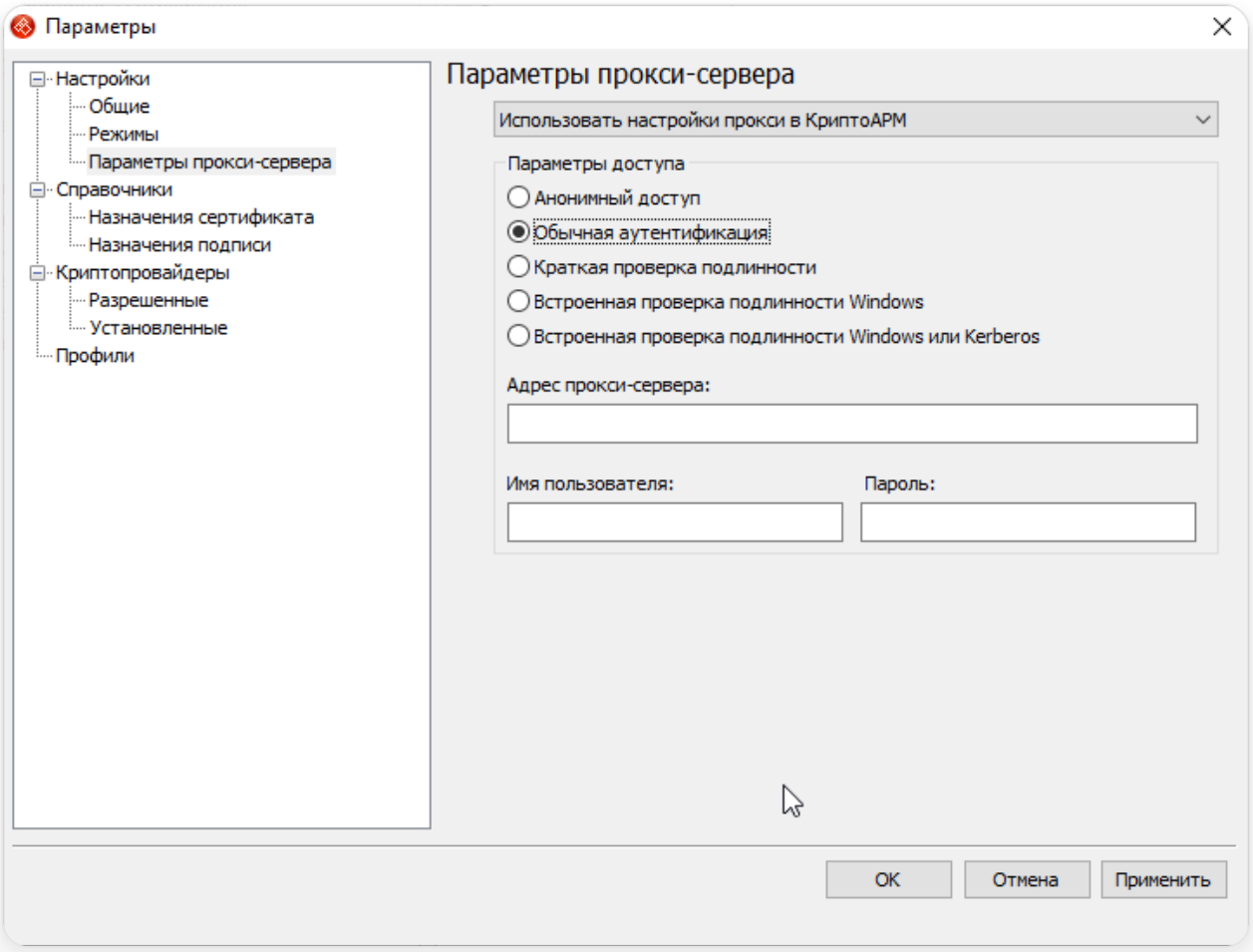
Дополнительную информацию о работе с квалифицированными сертификатами вы узнаете в одноименной главе.

Открыть статью на сайте

Параметры прокси-сервера

Программе «КриптоАРМ» для полноценной работы требуется подключение к сети Интернет, что позволяет оперативно загружать списки отзыва сертификатов и списки аккредитованных УЦ.

Если выход в сеть ограничен прокси-сервером, то вы можете настроить параметры доступа.



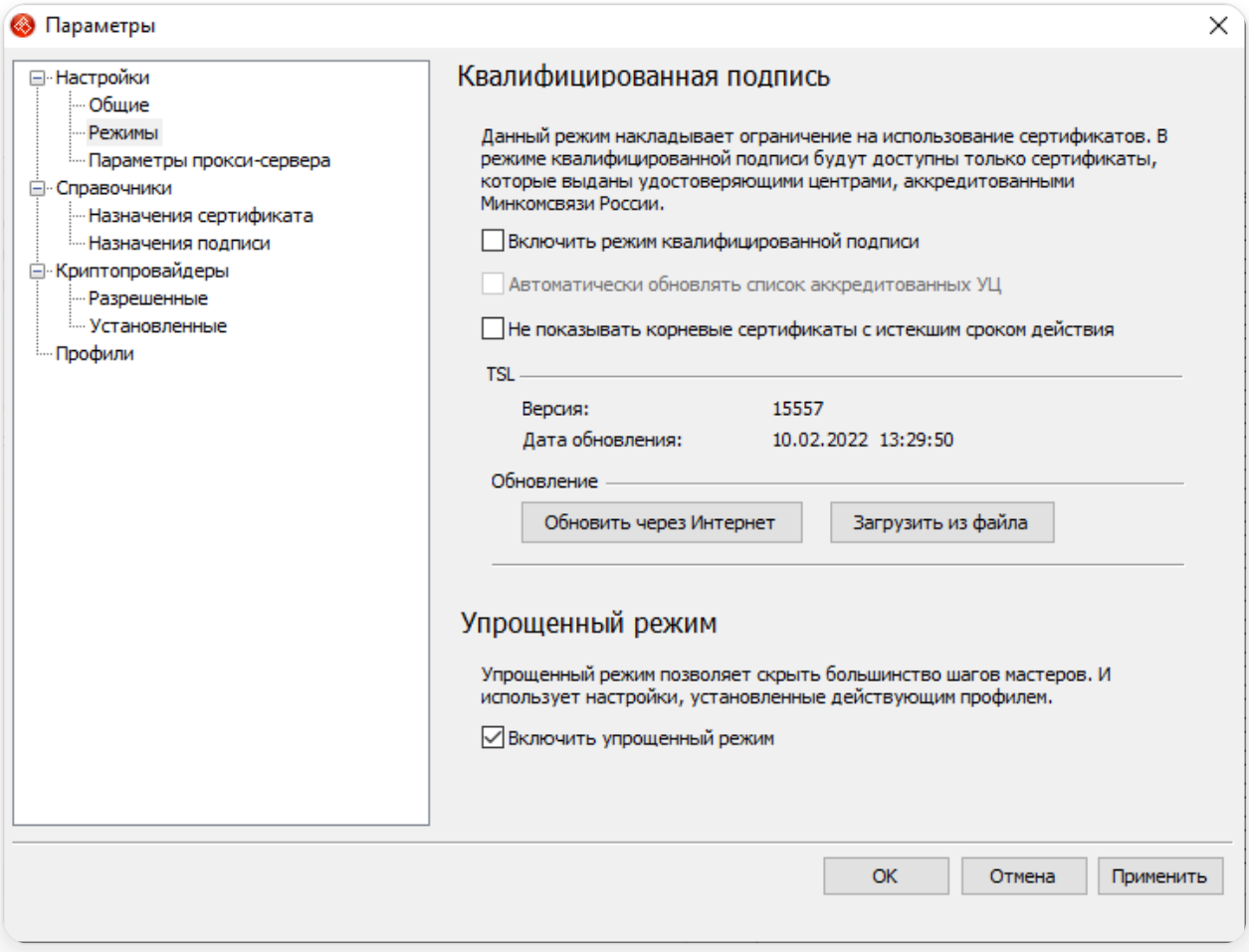
Детали настройки параметров доступа вы можете узнать у системного администратора.

Открыть статью на сайте

Упрощенный режим работы

Режим позволяет выполнять типовые криптооперации «в один клик», скрывая большинство шагов. При упрощенном режиме программа использует в качестве шаблона ту настройку, которая установлена "по умолчанию". В этом случае во время операции программой запрашивается ввод только тех параметров, которые не указаны в данной настройке. Остальные шаги операции выполняются программой автоматически согласно указанным в настройке параметрам.

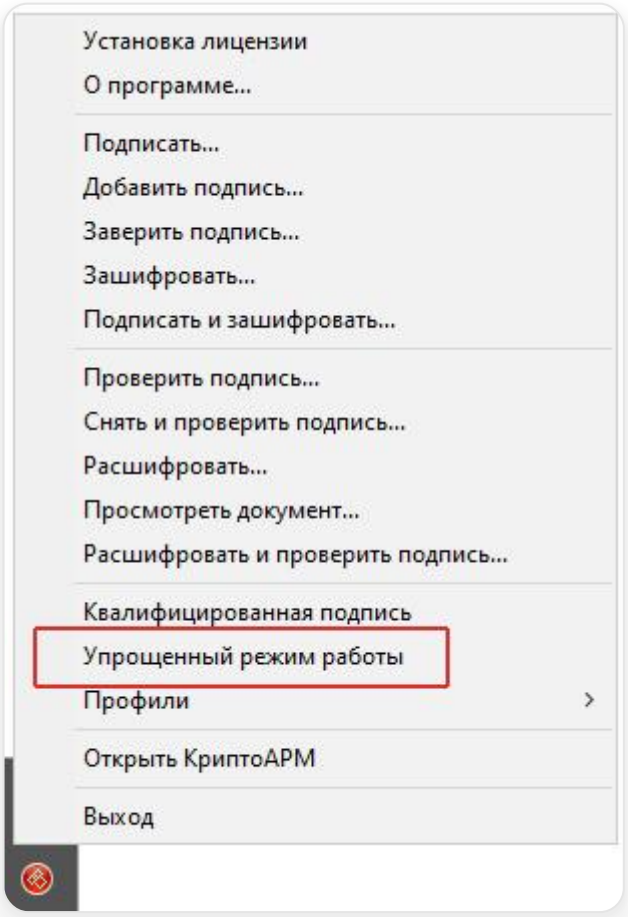
Включить «упрощенный режим» вы можете на верхней панели инструментов в меню **Настройки - Управление настройками - Режимы**. Для установки упрощенного режима используйте флаг **Включить упрощенный режим**.



При отключении данного режима во время выполнения операции вам будут доступны ВСЕ шаги Мастера для указания необходимых параметров вручную.

Быстро включить/отключить режим вы можете:

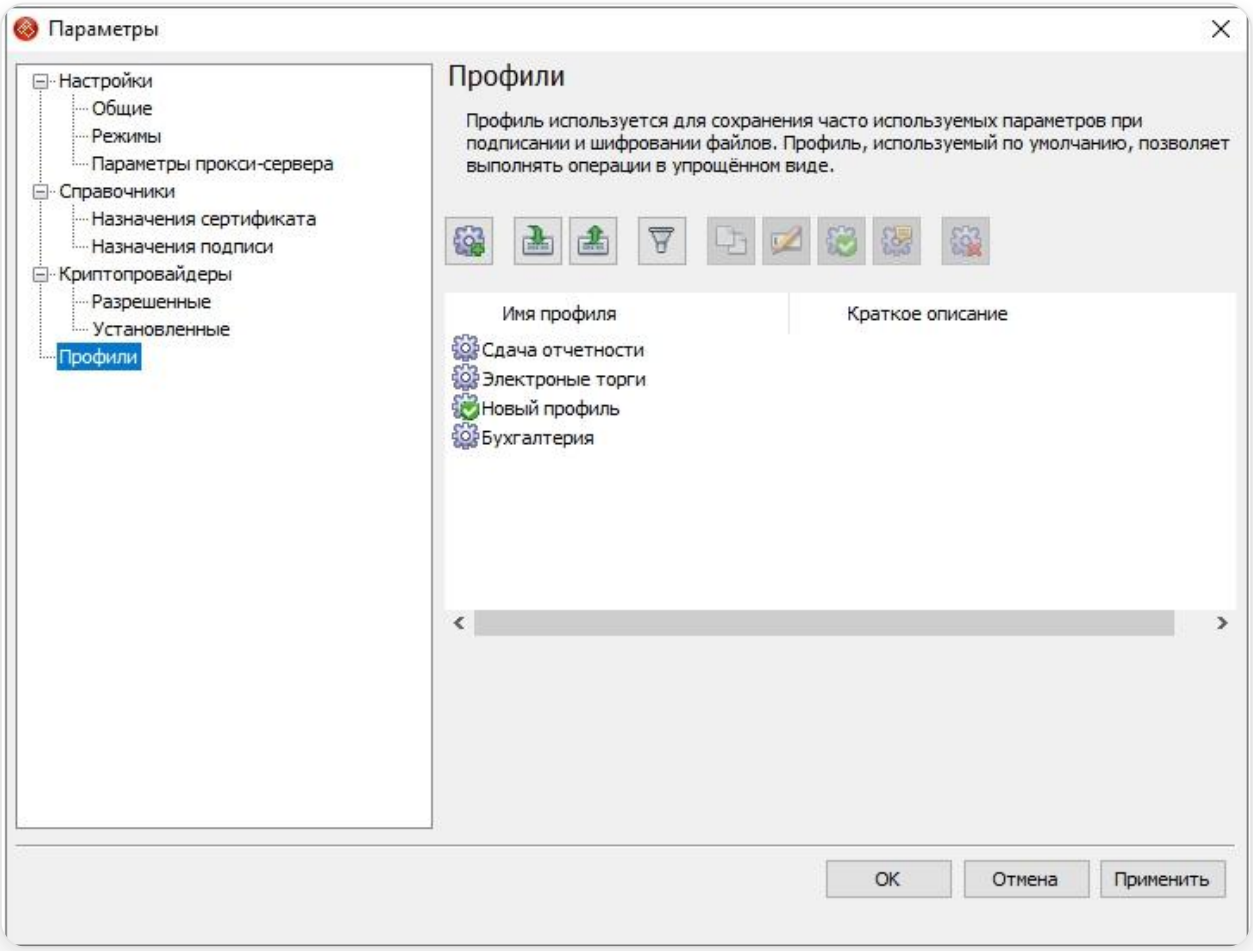
- через контекстное меню программы на панели задач
- через контекстное меню любого файла


Установка лицензии
О программе...
Подписать...
Добавить подпись...
Заверить подпись...
Зашифровать...
Подписать и зашифровать...
Проверить подпись...
Снять и проверить подпись...
Расшифровать...
Просмотреть документ...
Расшифровать и проверить подпись...
Квалифицированная подпись
Упрощенный режим работы
Профили
Открыть КриптоАРМ
Выход

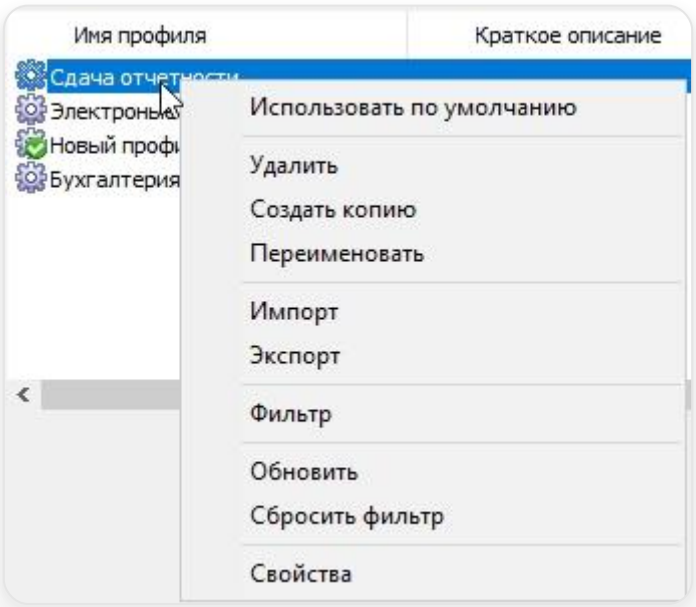
Открыть статью на сайте

Операции с профилями

Чтобы оперативно выполнять криптооперации, вы можете устанавливать специальные профили (шаблоны, индивидуальные настройки). Для каждой ситуации можно создать и использовать собственный профиль для выполнения криптографических операций, работы с сертификатами и т.п.



Работа с настройками выполняется через панель инструментов в меню **Настройки - Управление настройками - Профили** либо **Профили - Управление профилями**. Для вас доступно контекстное меню (правой клавишей мыши на настройке/пустом поле):



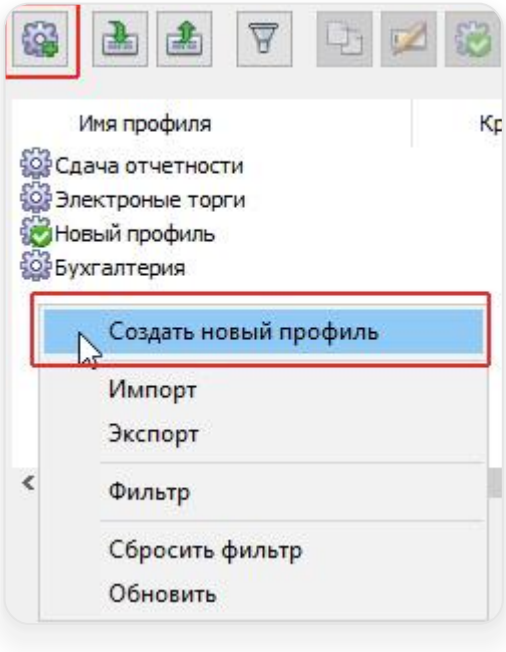
Еще один вариант работы с настройками – специальные значки:



1 – Создать профиль
2 – Импортировать профиль
3 – Экспортировать профиль
4 – Фильтровать профили по определенному параметру
5 – Создать копию профиля
6 – Переименовать профиль
7 – Установить профиль по умолчанию
8 – Просмотреть/изменить свойства профиля
9 – Удалить профиль

Создание нового профиля

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями** и вызовите контекстное меню правой клавишей мыши. Выберите пункт **Создать новый профиль**:



Откроется окно **Параметры настройки**. В создаваемом профиле вы можете установить следующие параметры:

- общие параметры (название, описание и т.п.)
- параметры подписи
- параметры шифрования
- параметры расшифрования
- параметры управления интерфейсом пользователя
- параметры использования политик сертификатов
- параметры верификации сертификатов
- параметры работы с TSP-службой (Службой штампов времени)
- параметры работы с OCSP-службой (Службой актуальных статусов)

2. Сохраните указанные параметры настройки (кнопка **Применить**).

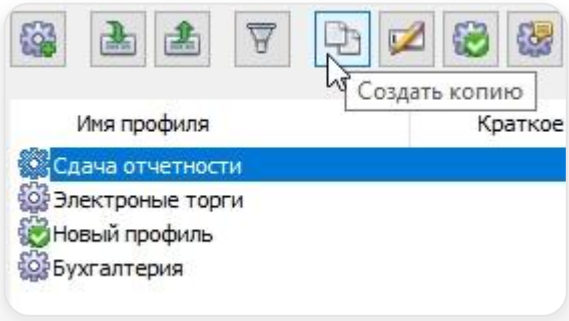
3. Созданная настройка отобразится в списке настроек.

Переименование профиля

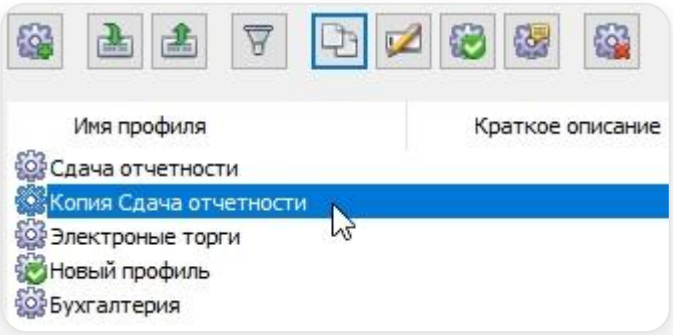
1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Из списка выберите профиль, который необходимо переименовать, и с помощью контекстного меню или спец.значка на панели инструментов выберите пункт **Переименовать**.
2. Введите новое имя для указанного профиля.
3. Профиль будет переименован.

Создание копии профиля

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Из списка выберите профиль, копию которого необходимо создать. С помощью контекстного меню или спец.значка на панели инструментов выберите пункт **Создать копию**.



2. В списке появится новый профиль под названием "Копия (название копируемого профиля)". Он включает все параметры того профиля, который была скопирован:

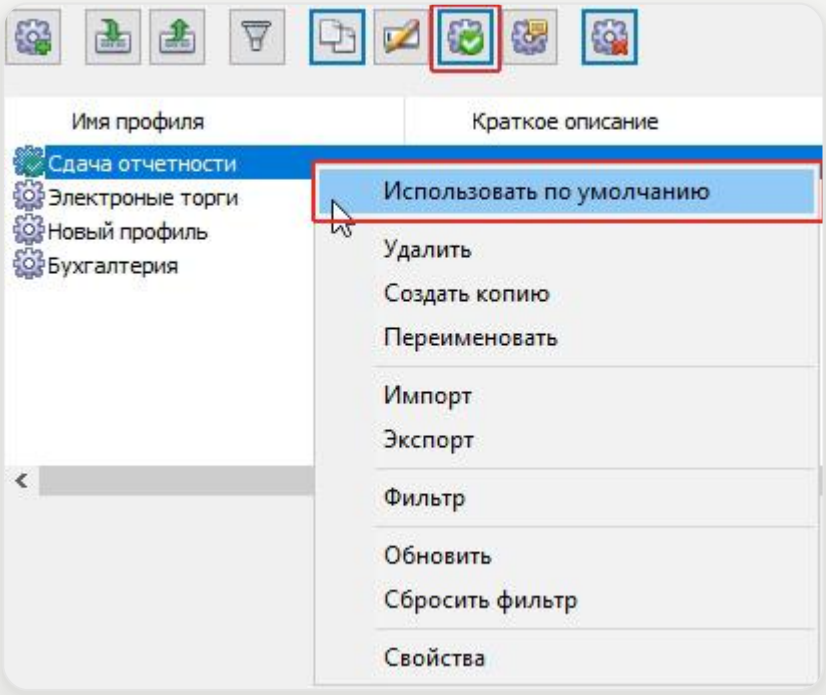


Установка профиля по умолчанию

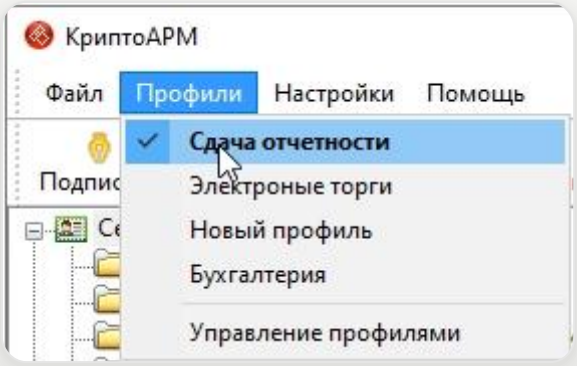
Вы можете установить один из используемых вами профилей как "используемый по умолчанию" (он будет использоваться автоматически, когда не выбран ни один из профилей).

Чтобы установить профиль по умолчанию:

> 1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. В контекстном меню профиля, который планируете использовать по умолчанию, или на панели инструментов выберите пункт **Использовать по умолчанию**:



2. При этом указанный профиль будет установлен как "Профиль по умолчанию".
    - Профиль, установленный по умолчанию, обозначается пиктограммой:
    - В общем списке профиль, используемый по умолчанию, выделен жирным шрифтом:



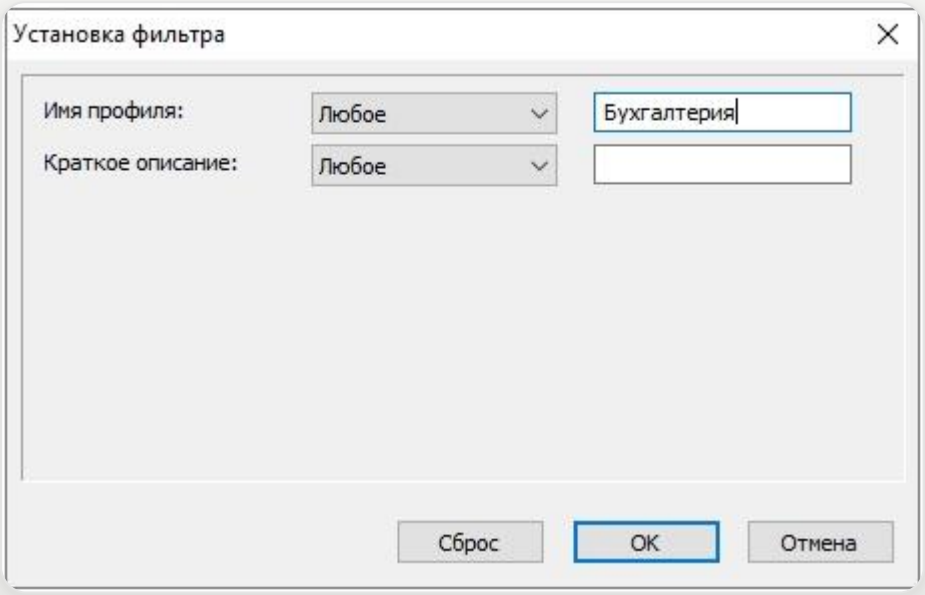
Фильтрация профилей

Вы можете фильтровать профили в списке последующим параметрам:

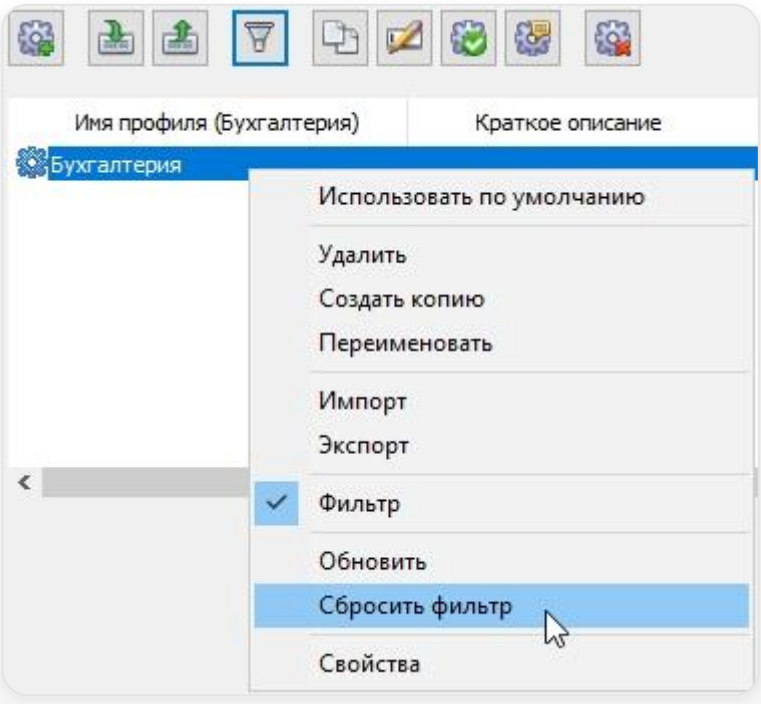
- имя настройки
- краткое описание

Чтобы отфильтровать настройки:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**, в контекстном меню или на панели инструментов выберите пункт **Фильтр**.
2. В окне **Установка фильтра** укажите параметры, по которым необходимо отобрать профили «КриптоАРМ»:



3. Список профилей будет отфильтрован по указанным вами параметрам.
4. Вернуться к исходному списку профилей вы можете, сбросив фильтр:



Экспорт профиля

При обновлении или переустановке программы «КриптоАРМ» рекомендуется экспортировать используемые в работе профили выполнения операций в XML-формат.

Чтобы экспортировать настройку в файл:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**, выберите профиль, который необходимо экспортировать. В контекстном меню объекта или на панели инструментов выберите пункт **Экспорт**
2. В окне проводника введите имя экспортируемого файла с настройкой
3. Указанный профиль будет экспортирована в файл в формате *.xml. При экспорте нескольких профилей, будет создаваться один *.xml файл, содержащий все экспортируемые профили.

Импорт профиля

При обновлении или переустановке программы «КриптоАРМ» вы можете импортировать ранее сохраненные в XML-формате профили выполнения операций.

Чтобы импортировать файл с профилем:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Правой клавишей мыши откройте контекстное меню или на панели инструментов выберите пункт **Импорт.**
2. В окне проводника выберите файл с профилем в формате .xml
3. В список профилей будет импортирован указанная вами профиль.

Удаление профиля

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**, выберите профиль, который необходимо удалить. В контекстном меню объекта или на панели инструментов выберите пункт **Удалить**
2. На запрос системы подтвердите свое решение.
3. Указанный профиль будет удален из списка.

Открыть статью на сайте

Общие параметры профиля

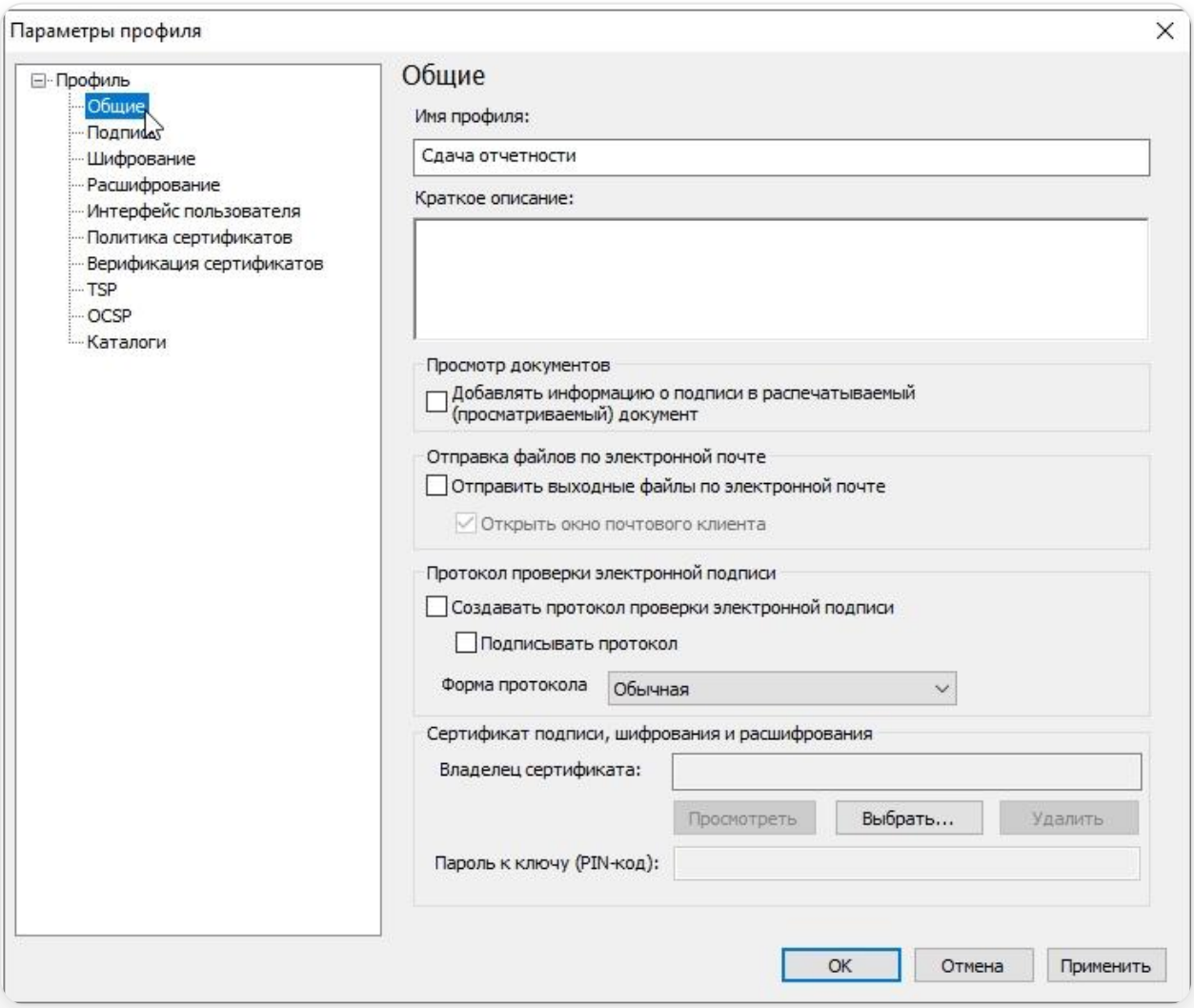
С раздела «Общие» начинается создание любого профиля. Здесь вы указываете имя нового профиля и его краткое описание, можете настроить отправку подписанных/зашифрованных данных по электронной почте и др.

В разделе «Общие» и укажите:

- Имя профиля,
- Краткое описание профиля (для чего будет использоваться профиль),
- Требуется ли добавлять информацию о подписи в распечатываемый (просматриваемый) документ,
- Следует ли отправлять выходные данные по электронной почте,
- Сертификат, который будет использоваться для подписания, шифрования и расшифрования данных (кнопка **Выбрать**). Указанный сертификат при необходимости можно удалить из настроек (кнопка **Удалить**), а также просмотреть общую и детальную информацию о нем (кнопка **Просмотреть**).
- Пароль к ключу (PIN-код).



Эту опцию мы советуем использовать крайне осторожно, только в тех ситуациях, когда хочется избавиться от ручного ввода пин-кода, даже с учетом понижения уровня защищенности. Помните: хранение пароля к закрытому ключу в профиле может быть небезопасным.

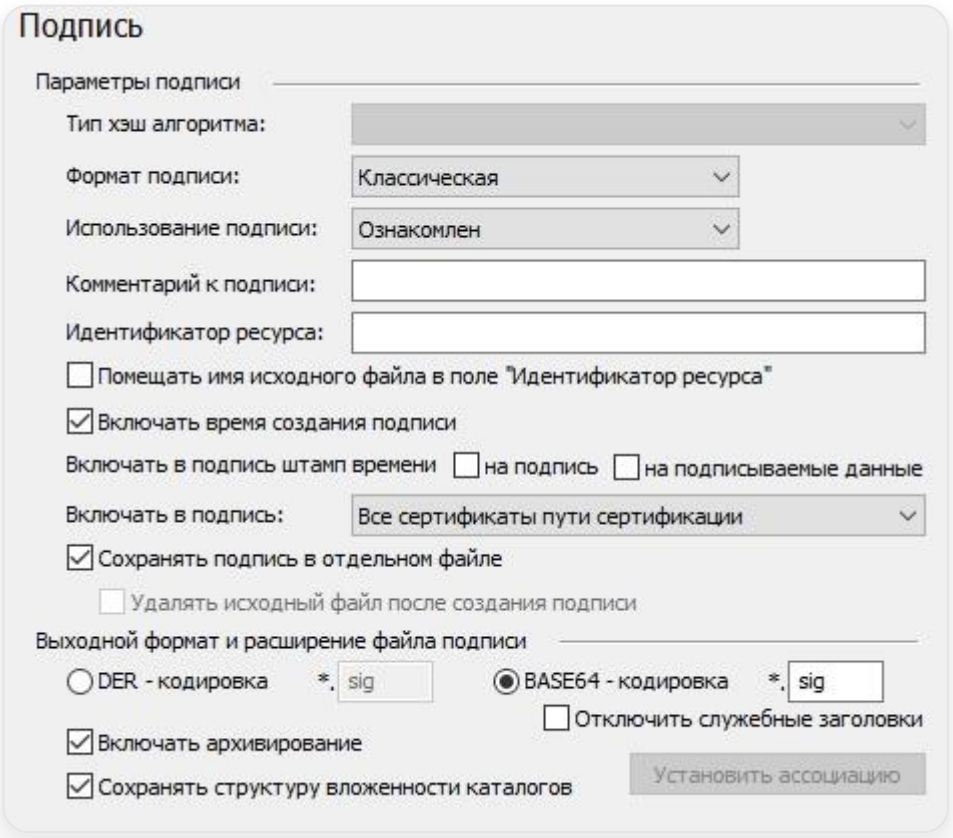

Параметры профиля
Профиль
Общие
Подписи
Шифрование
Расшифрование
Интерфейс пользователя
Политика сертификатов
Верификация сертификатов
TSP
OCSP
Каталоги
Общие
Имя профиля:
Сдача отчетности
Краткое описание:
Просмотр документов
Добавлять информацию о подписи в распечатываемый (просматриваемый) документ
Отправка файлов по электронной почте
Отправить выходные файлы по электронной почте
Открыть окно почтового клиента
Протокол проверки электронной подписи
Создавать протокол проверки электронной подписи
Подписывать протокол
Форма протокола
Обычная
Сертификат подписи, шифрования и расшифрования
Владелец сертификата:
Просмотреть
Выбрать...
Удалить
Пароль к ключу (PIN-код):
OK
Отмена
Применить

Открыть статью на сайте

Настройки операции подписи

Для установки параметров подписи в настройке выполните следующие шаги:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстном меню файла или на панели инструментов: выберите пункт **Профили**.
2. Откройте ту настройку, в которой необходимо установить/изменить параметры. В окне **Параметры настройки** откройте раздел **Подпись**.



3. Укажите параметры электронной подписи:
   - **Тип хэш-алгоритма**, на основе которого будет создаваться электронная подпись (выберите из выпадающего списка). Список зависит от того, какой криптопровайдер вы используете для работы
   - **Формат подписи:**классическая или усовершенствованная

> - **классическая**
>   Содержимое ключей и сертификатов позволяет установить авторство электронного документа, однако в используемом сегодня формате ЭП не фиксируется время её создания и статус сертификата открытого ключа на

момент подписи (действителен, отозван, приостановлен). Это затрудняет процедуру доказательства подлинности электронной подписи.

- **усовершенствованная**
  Усовершенствованная электронная подпись. Предназначена для разрешения споров между подписывающей и проверяющей сторонами, которые могут возникать в отдаленном будущем, даже годы спустя момента их создания.

- **Использование подписи:** «ознакомлен», «подписано», «согласовано» и т.п. (выберите из выпадающего списка). О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.

- **Комментарий к подписи.** Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").

- **Идентификатор ресурса.** Под идентификатором ресурса понимается:

  - путь до исходного, подписываемого файла (на компьютере или в Интернете, где находится данный файл)
  - имя файла (указывается для того, чтобы в случае изменения имени файла получатель подписанного документа смог определить первоначальное его название).

- **Включить время создания подписи.** При установке флага - в файл подписи будет включено время подписи.

- **Включить штамп времени** на подписываемые данные и/или на саму электронную подпись

  - **на подписываемые данные**
    При установке этого флага в файл электронной подписи будет включен штамп времени на исходные данные. Штамп времени на документе удостоверяет время создания документа для последующего разрешения конфликтов, связанных с использованием электронного документа. Эта возможность способствует обеспечению неотказуемости от подписи.
    Наличие штампа времени в подписанном документе позволяет продлевать срок действия электронной подписи. Например, такой штамп удостоверяет, что подпись была создана до того, как сертификат ключа подписи был аннулирован(отозван). Таким образом, даже после отзыва сертификата останется возможность использовать данный отозванный сертификат для проверки электронных подписей, созданных до момента отзыва. Подобная проблема актуальна для всех систем электронного документооборота.

  - **на подпись**
    При установке этого флага в файл электронной подписи будет включен штамп времени на создаваемую электронную подпись.

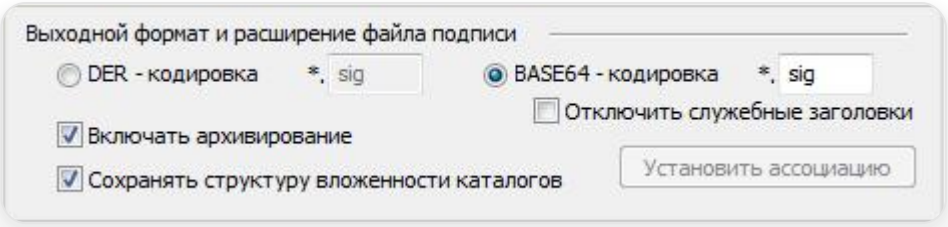
	Флаг доступен только при установленной лицензии на модуль TSP.

- **Включать в подпись:**

  - только сертификат владельца: режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
  - путь сертификации без корневого сертификата: в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
  - все сертификаты пути сертификации: в атрибуты подписи добавляется вся цепочка сертификатов, в том числе, и корневой сертификат;
  - не включать сертификаты в подпись: в атрибуты подписи не включаются сертификаты.

- **Сохранить подпись в отдельном файле.**
  При установке флага будет создана электронная подпись, отделенная от подписываемых данных (отдельным файлом). Удобна в том случае, когда вы отправляете документ человеку, который не использует «КриптоАРМ» и ему важна не столько подпись, сколько сами данные.
  При отсутствии флага - будет сформирована электронная подпись, включающая в себя файл с исходными данными (в этом случае документ и ЭП будут храниться вместе). Такая подпись называется совмещенной.

4. Установите параметры выходного формата и расширение файла подписи:



- **Кодировка и расширение;**

  - **DER encoded binary X.509**
    Платформенно-независимый метод хранения сертификатов. Может использоваться для их передачи между компьютерами. Расширения подписанного файла *.sig, *.p7s.
  - **- Base64 encoded X.509**
    Вариант кодирования, разработанный для использования совместно с S/MIME (безопасным протоколом электронной почты). Файл использует ASCII-символы, благодаря чему может пройти неповрежденным через все почтовые шлюзы.

> Для этого варианта кодирования вы можете указать флаг **Отключить служебные заголовки** (в этом случае в файле подписи не будут использоваться заголовки, указывающие начало и окончание блока с подписанными данными. Заголовки необходимы для того, чтобы можно было выполнять проверку ЭП более ранними версиями программы «КриптоАРМ»).

- **Включить архивирование;**

  Вы можете указать требуется ли заархивировать подписанные файлы

- **Сохранять структуру вложенности каталогов;**

  В архиве можно сохранять структуру вложенности каталогов.

  При развертывании корпоративной системы электронного документооборота для подписанных файлов можно установить специальные расширения, отличные от стандартных. Чтобы при работе с программой «КриптоАРМ» эти файлы обрабатывались, необходимо занести новые расширения в список так называемых «ассоциаций»:

  - Добавьте необходимое расширение и нажмите на кнопку **Установить ассоциацию**.
  - Для снятия ассоциации с расширения нажмите на кнопку **Снять ассоциации**.

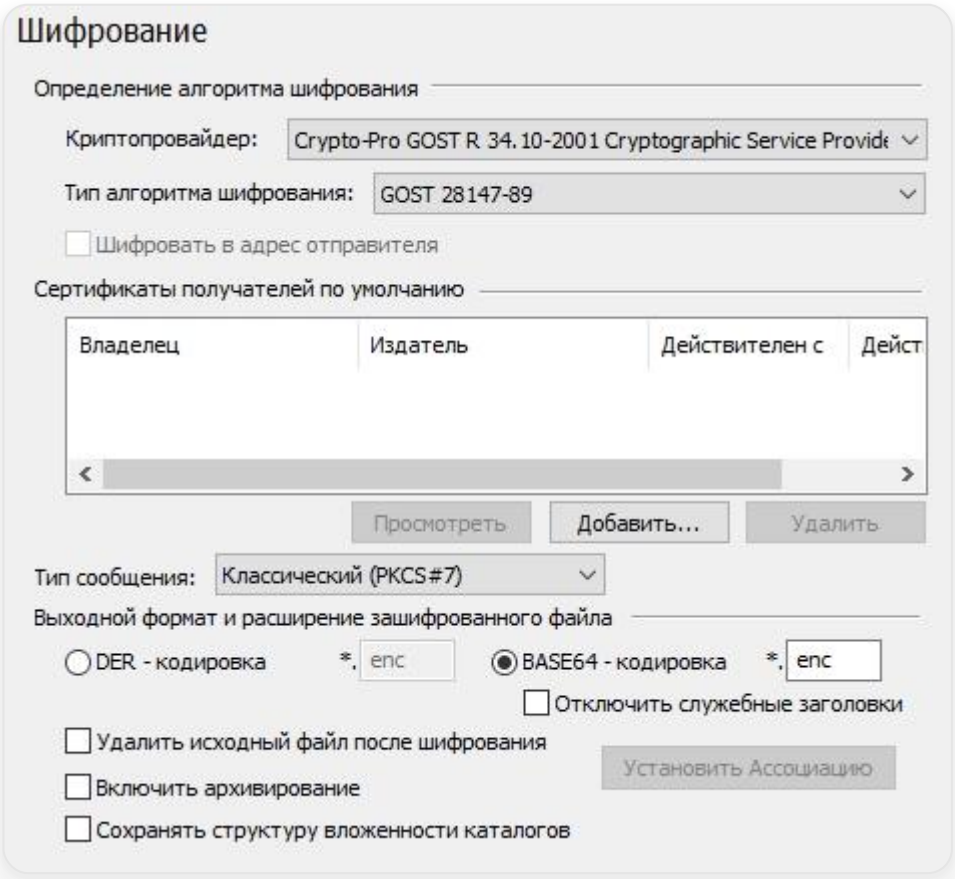
Настроив все необходимые параметры подписи, сохраните внесенные изменения (кнопка **Применить** или **ОК**).

Открыть статью на сайте

Настройки операции шифрования

Для установки параметров шифрования в профиле выполните следующие шаги:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстном меню файла или на панели инструментов: выберите пункт **Профили**.
2. Откройте профиль, в котором необходимо установить/изменить параметры шифрования. В окне **Параметры настройки** откройте раздел **Шифрование**.
3. Укажите параметры шифрования:



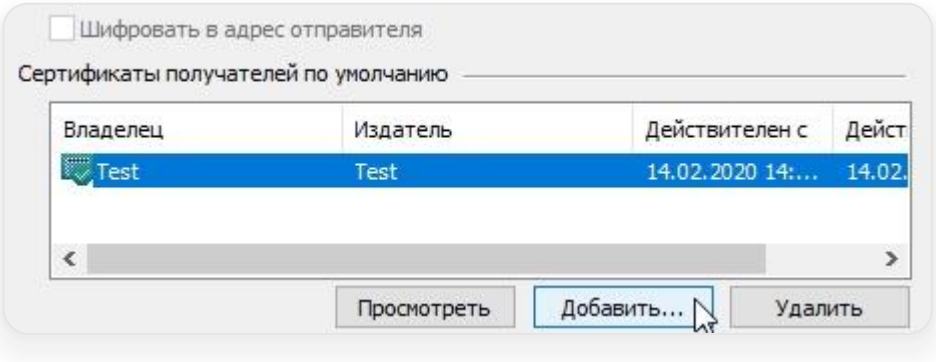
В выпадающем списке укажите **Криптопровайдер**, который должен использоваться при шифровании данных, и **тип алгоритма шифрования**(в зависимости от используемого криптопровайдера);

	Необходимость выбора криптопровайдера обусловлена тем, что не все криптопровайдеры совместимы. Например, нельзя одновременно

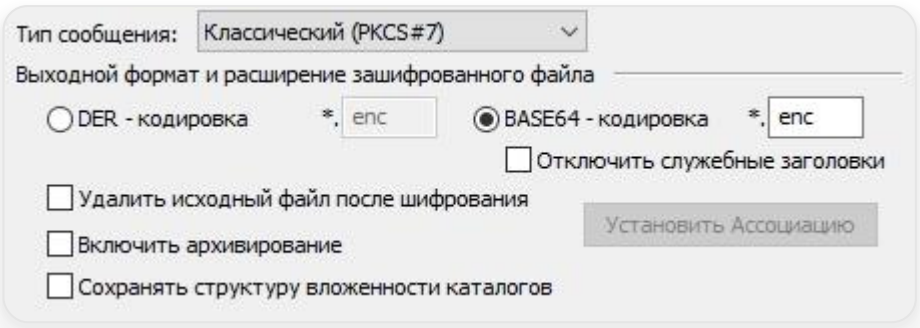
	зашифровать в адрес ключей (сертификатов), созданных на «КриптоПро CSP» и Microsoft Base Cryptographic Provider v1.0.
	В случае использования криптопровайдера «SafeSign CSP Version 1.0» рабочим алгоритмом шифрования является только RC4.

Чтобы иметь возможность впоследствии расшифровать зашифрованный файл, установите флаг **Шифровать в адрес отправителя**. В этом случае ваш сертификат шифрования попадет в список сертификатов получателей по умолчанию.

В окне **Сертификаты получателей по умолчанию** укажите сертификаты, которые будут использоваться настройкой по умолчанию для шифрования данных (кнопка **Добавить**). Вы можете указать личные сертификаты, так и сертификаты других пользователей.



Вы можете настроить выходные форматы данных, которые будут использоваться по умолчанию для шифрования данных в этой настройке:



- **Кодировка и расширение (например, *.enc, *.p7m, *.pem)**

Для формата в BASE64-кодировке вы можете указать флаг **Отключить служебные заголовки** (в этом случае в файле подписи не будут использоваться заголовки, указывающие начало и окончание блока с подписанными данными. Заголовки необходимы для того, чтобы можно было выполнять проверку ЭП более ранними версиями программы «КриптоАРМ»).

Регистрация дополнительных расширений файлов, которые должны ассоциироваться с программой «КриптоАРМ». При развертывании системы электронного документооборота для зашифрованных файлов можно установить специальные расширения, отличные от стандартных. Чтобы при работе с программой «КриптоАРМ» эти файлы корректно обрабатывались, необходимо занести новые расширения в список так называемых «ассоциаций». Добавьте необходимое расширение и нажмите на кнопку **Установить ассоциацию**. Для снятия ассоциации с расширения используйте кнопку **Снять ассоциации**.

- **Удалить исходные файлы после выполнения операции.**
  В этом случае исходный файл, выбранный пользователем для шифрования, будет удален после успешного завершения операции.

- **Включить архивирование.**
  Вы можете указать, требуется ли заархивировать зашифрованные файлы.

- **Сохранять структуру вложенности каталогов.** В этом случае архив зашифрованных файлов будет иметь ту же структуру каталогов/папок, что была до шифрования.

Настроив все необходимые параметры шифрования, сохраните внесенные изменения (кнопка **Применить** или **ОК**).

Открыть статью на сайте

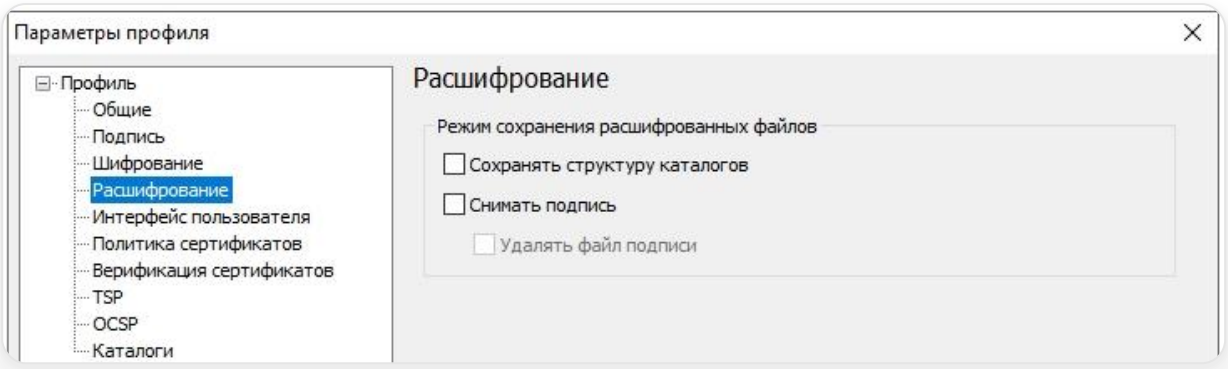
Настройки операции расшифрования

Для установки параметров расшифрования:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстном меню файла или на панели инструментов: выберите пункт **Профили**.

2. Откройте профиль, в котором необходимо установить/изменить параметры. В окне **Параметры настройки** откройте раздел **Расшифрование**.

3. Укажите параметры расшифрования: требования к сохранению расшифрованных данных.



Сохранять исходную структуру каталогов при расшифровании. В этом случае при расшифровании будет сохраняться та же структура каталогов/папок, что была в зашифрованном пакете.

Снимать электронную подпись с документа и **удалять файл подписи**.

4. Настроив все необходимые параметры расшифрования, сохраните внесенные изменения (кнопка **Применить**).

Открыть статью на сайте

Настройки управления интерфейсом

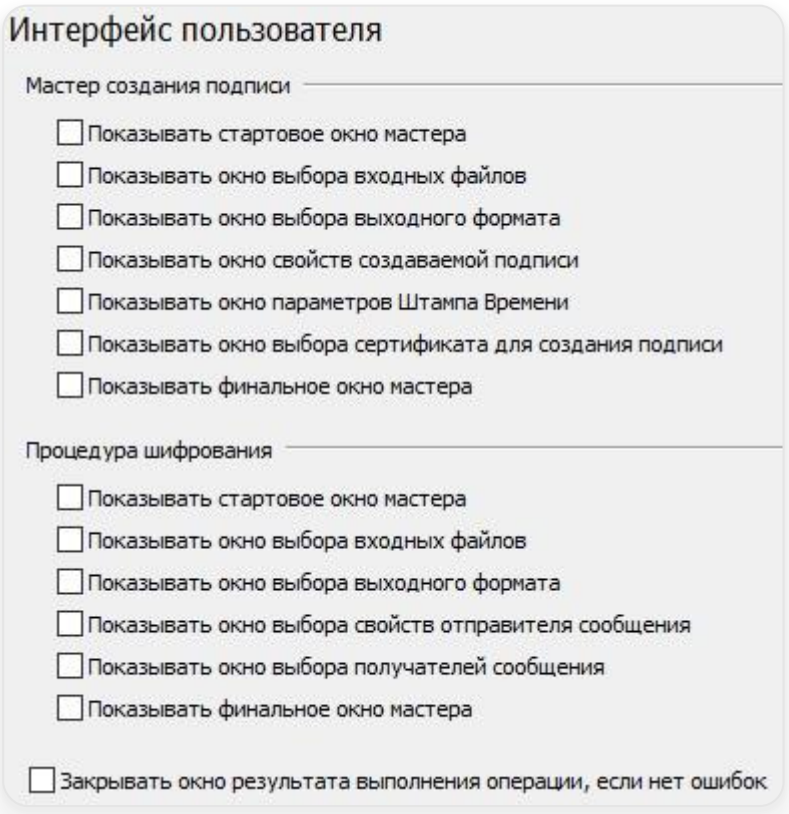
Для установки параметров пользовательского интерфейса выбранной настройки, выполните следующие шаги:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстном меню файла или на панели инструментов: выберите пункт **Профили**.

2. Откройте профиль, в которой необходимо установить/ изменить параметры. В окне **Параметры настройки** откройте раздел **Интерфейс пользователя**.

3. В этом разделе вы можете индивидуально настроить пользовательский интерфейс для операций создания электронной подписи и шифрования. Установите флаги напротив полей, описывающих **те элементы интерфейса, которые должны показываться при выполнении криптоопераций**:

   - Стартовое окно мастера (для подписи и шифрования);
   - Окно выбора списка входных файлов (для подписи и шифрования);
   - Окно выбора выходного формата (для подписи и шифрования);
   - Окно свойств создаваемой подписи (для подписи);
   - Окно параметров Штампа Времени (для подписи);
   - Окно выбора сертификата для создания подписи (для подписи);
   - Окно выбора свойств отправителя сообщения (для шифрования);
   - Окно выбора получателя сообщения (для шифрования);
   - Финальное окно мастера (для подписи и шифрования).



Вы можете настроить ход операции таким образом, что при отсутствии ошибок в результате выполнения операции финальное окно будет автоматически закрываться - для этого установите флаг напротив строки **Закрывать окно результата выполнения операции, если нет ошибок**.

10. Настроив необходимые параметры интерфейса пользователя, сохраните внесенные изменения (кнопка **Применить**).

Открыть статью на сайте

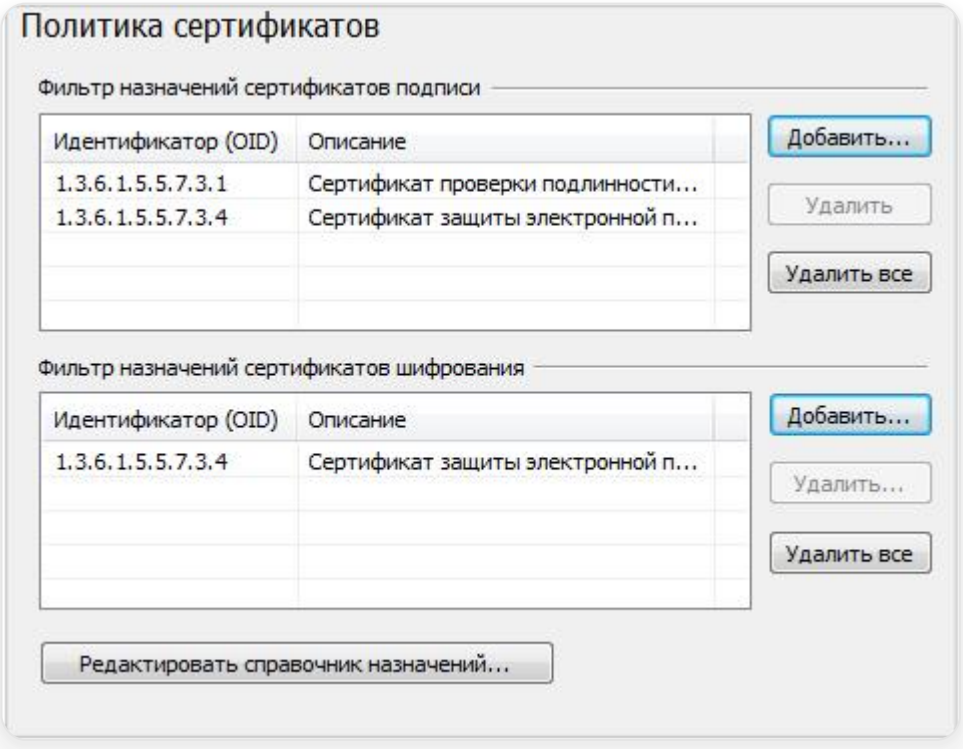
Настройки использования политик сертификатов

Вы можете настроить фильтры сертификатов подписи и шифрования по их назначениям, если этого требует политика организации, а также редактировать справочник назначений сертификатов.

	Детали настройки справочника назначений вы можете узнать у вашего системного администратора.

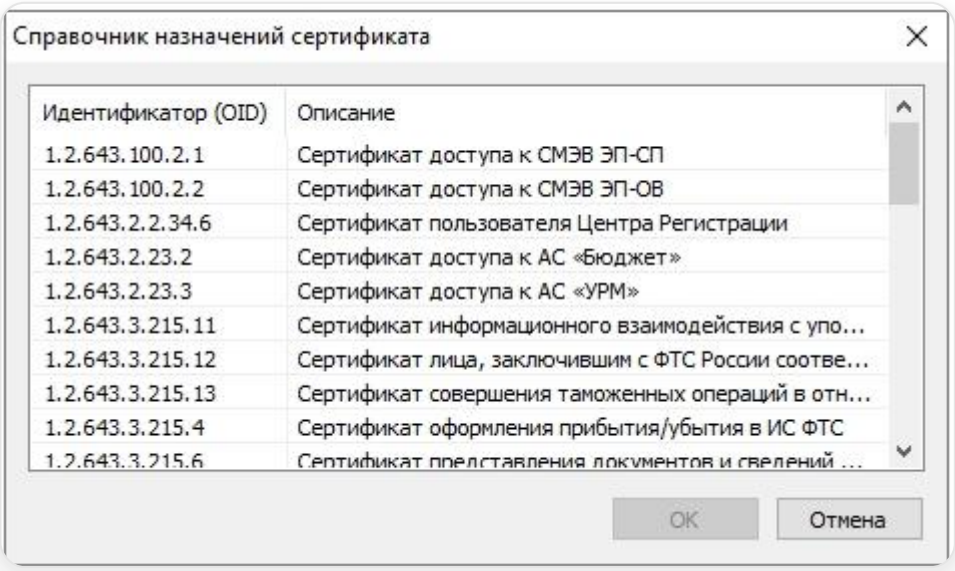
Для настройки параметров политики сертификатов, выполните следующие шаги:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстном меню файла или на панели инструментов: выберите пункт **Профили**.
2. Откройте профиль, в котором необходимо установить параметры. В окне **Параметры настройки** откройте раздел **Политика сертификатов**. В этом окне вы можете настроить фильтры назначений сертификатов подписи и шифрования, а также редактировать справочник назначений.

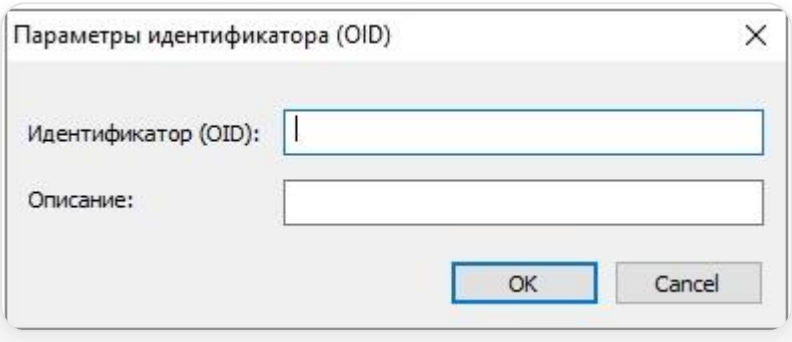


3. Для формирования фильтра необходимо предварительно занести требуемые назначения сертификатов в справочник. Если в настройке установлен фильтр сертификатов для конкретной операции, то в окне выбора сертификата для выполнения этой операции будут доступны только те сертификаты, которые определены в соответствии с установленным фильтром.

4. Выбор идентификаторов (OID) осуществляется из справочника назначений (кнопка **Добавить**). Изначально справочник заполнен некоторыми значениями.



5. Чтобы добавить новый OID в справочник, необходимо нажать на кнопку **Редактировать справочник назначений**. Появится форма редактирования справочника назначений сертификата.
   - для добавления нового идентификатора нажмите на кнопку **Добавить**. Откроется окно ввода параметров политики. Введите идентификатор (OID) и его описание. В справочник назначений добавится новая запись;



   - изменить параметры идентификатора можно, выбрав в списке необходимый OID и нажав на кнопку **Изменить**. Откроется окно **Параметры идентификатора**, в котором внесите требуемые изменения;
   - для удаления OID из справочника нажмите на кнопку **Удалить**, кнопка Удалить все позволяет удалить весь список OID данного справочника;

- вы также можете импортировать OID в формате .xml в справочник (кнопка **Импорт**) или экспортировать имеющийся в справочнике OID (кнопка **Экспорт**);

6. Установив параметры политики сертификатов, сохраните внесенные изменения (кнопка **Применить**).

Открыть статью на сайте

Настройки верификации сертификатов

Для установки параметров верификации сертификатов выбранной настройки, выполните следующие шаги:

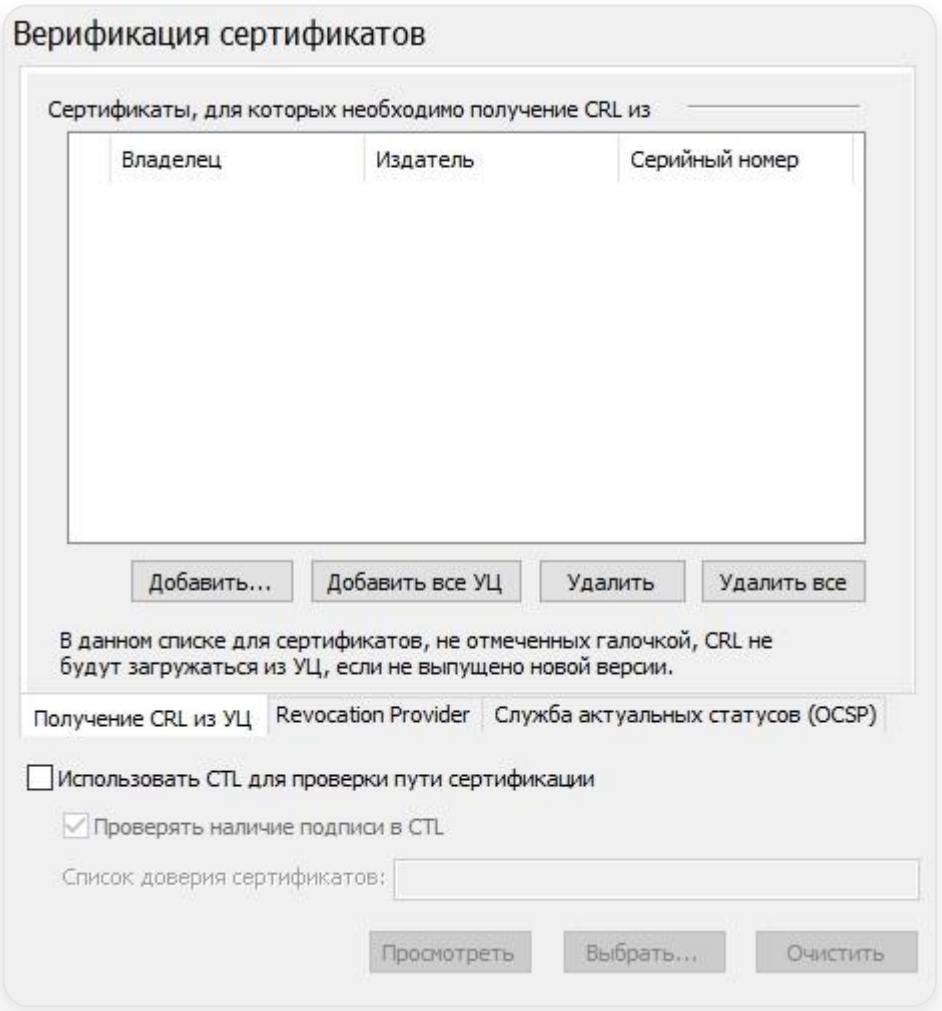
1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстное меню файла или на панели инструментов: выберите пункт **Профили**.

2. Откройте профиль, в котором необходимо установить/ изменить параметры. В окне **Параметры настройки** откройте раздел **Верификация сертификатов**.
   Вы можете установить настройку для проверки статуса сертификатов четырьмя способами:

   - на основе полученного из удостоверяющего центра актуального списка отзыва сертификатов;
   - через Revocation Provider;
   - с помощью Службы актуальных статусов (OCSP);
   - с помощью списка доверенных сертификатов.

   Откройте закладку, соответствующую выбранному вами типу проверки, и занесите сертификаты, которые требуется проверять именно этим способом:

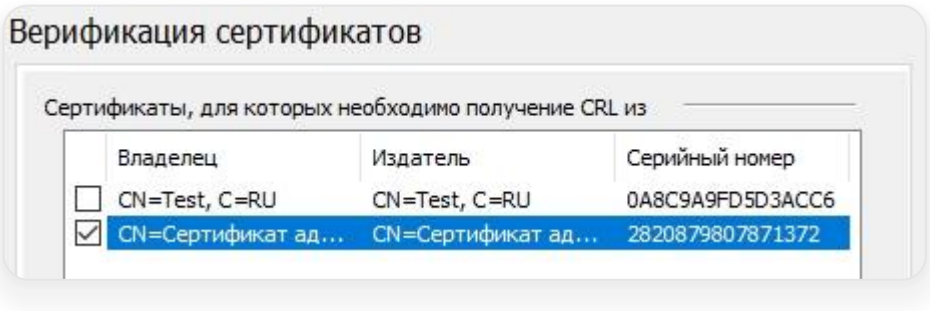
   - получение CRL из УЦ (получение списка отозванных сертификатов из удостоверяющего центра);
   - Revocation Provider;
   - Служба актуальных статусов (OCSP)



Чтобы проверять статусы сертификатов (личных и других пользователей) способами «Получение COC из УЦ» или «Revocation Provider» для всех Удостоверяющих центров (корневые сертификаты которых установлены в хранилище Доверенные корневые центры сертификации), нажмите на кнопку **Добавить все УЦ**.

Вы можете удалить из списка выбранные сертификаты, выделив их и нажав на кнопку **Удалить**. Если вы хотите удалить весь список сертификатов, нажмите кнопку **Удалить все**.

На вкладке **Получение CRL из УЦ** рядом с каждым выбранным сертификатом расположена галочка. Если она установлена, COC будет всегда загружаться из удостоверяющего центра. Если же галочка убрана, то COC будет подгружаться только в том случае, если на сервере выпущена новая версия COC или его срок действия истек.



«КриптоАРМ» узнаёт о выпуске нового COC по дате планового обновления, указанного в самом списке отзыва. Если список будет выпущен внепланово (раньше срока), то его обновление необходимо будет запустить вручную. Узнать о том, как обновить COC из УЦ, можно в разделе Операции с сертификатами.

	Детали настройки справочника назначений вы можете узнать у вашего системного администратора.

Если необходимо проверить сертификат с помощью списка доверенных сертификатов (CTL), отметьте в настройках "Использовать CTL для проверки пути сертификации".

Из хранилища сертификатов необходимо Выбрать списки доверенных сертификатов. Если хранилище пусто, то с помощью кнопки **Импорт** установите список. Вы можете удалить выбранный ранее список доверия, нажав на **Очистить**.

1. Настроив необходимые параметры, сохраните внесенные изменения (кнопка **Применить**).

Открыть статью на сайте

Настройки службы штампов времени TSP

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

Для настройки параметров штампа времени, выполните следующие шаги:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстное меню файла или на панели инструментов: выберите пункт **Профили**.

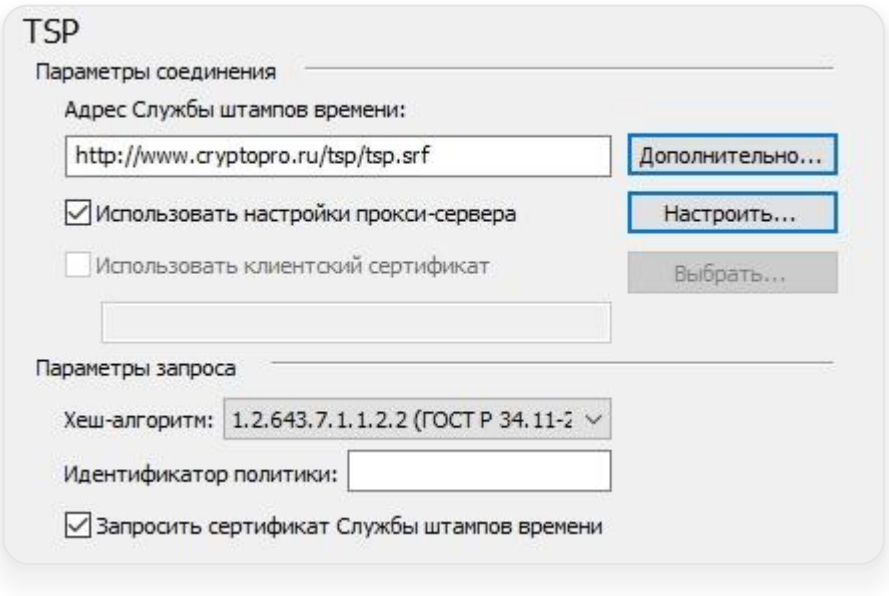
2. Откройте профиль, в котором необходимо установить/ изменить параметры. В окне **Параметры настройки** откройте раздел **TSP**, в котором укажите параметры соединения со Службой штампов времени и параметры запроса:

   Адрес Службы штампов времени

   Формат адреса: <протокол>://<сервер>[:порт][/путь]. В качестве протокола вы можете указать "http" и "https". Адрес службы штампов времени можно узнать у поставщика услуги. Например, услуги службы штампов времени могут предоставлять удостоверяющие центры. Так же это может быть сторонняя служба которой вы и ваши контрагенты доверяете.

   - настройки прокси-сервера, если при подключении к службе OCSP используется прокси-сервер
   - клиентский сертификат, если доступ к службе OCSP выполняется по цифровым сертификатам (чтобы активировать режим выбора клиентского сертификата, в строке с адресом сервера должен быть указан протокол "https").

   Параметры запроса



	Детали настройки параметров работы со Службой вы можете узнать у системного администратора.

3. Установив параметры штампа времени, сохраните внесенные изменения (кнопка **Применить**).

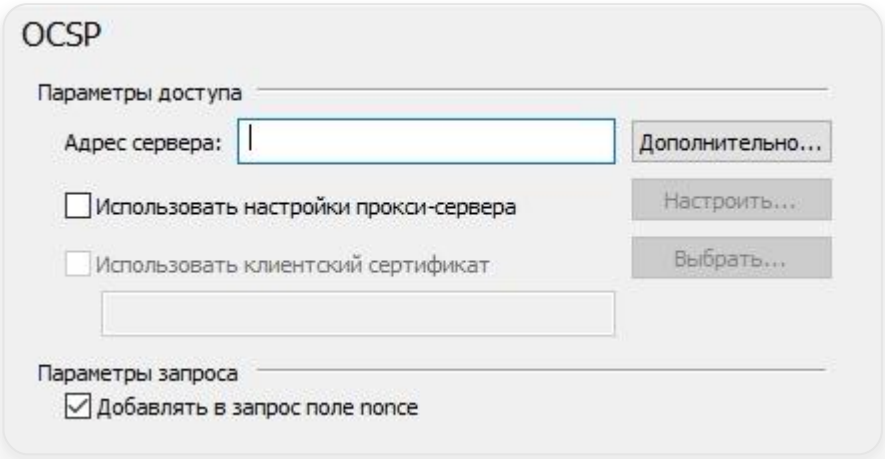
Открыть статью на сайте

Настройки службы актуальных статусов OCSP

С помощью Службы актуальных статусов сертификатов вы можете в онлайн-режиме проверять статус сертификатов на основе протокола OCSP (Online Certificate Status Protocol).

Для настройки параметров доступа к службе:

1. На верхней панели главного окна откройте пункт меню **Профили - Управление профилями**. Это же вы можете сделать через контекстном меню файла или на панели инструментов: выберите пункт **Профили**.
2. Откройте профиль, в котором необходимо установить/ изменить параметры. В окне **Параметры настройки** откройте раздел OCSP, в котором укажите параметры соединения со Службой актуальных статусов:



- **адрес сервера**
  Формат адреса: <протокол>://<сервер>[:порт][/путь]. В качестве протокола вы можете указать "http" и "https".
- **настройки прокси-сервера**, если при подключении к службе OCSP используется прокси-сервер Формат адреса: <протокол>://<сервер>[:порт]. В качестве протокола вы можете указать "http" и "https".
- **клиентский сертификат**, если доступ к службе OCSP выполняется по цифровым сертификатам (чтобы активировать режим выбора клиентского сертификата, в строке с адресом сервера должен быть указан протокол "https").

	Детали настройки параметров работы со Службой вы можете узнать у системного администратора.

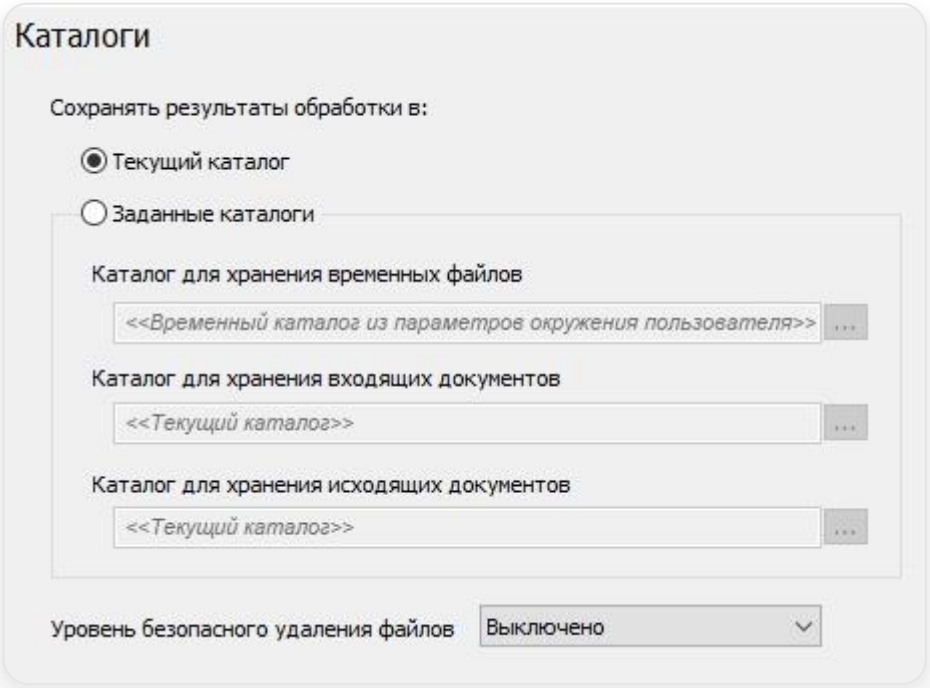
4. Установив параметры доступа к Службе, сохраните внесенные изменения (кнопка **Применить**).

Открыть статью на сайте

Настройки каталогов хранения файлов

Вы можете установить собственные каталоги для хранения файлов, а также уровень безопасного удаления файлов. Для этого выполните следующие шаги:

1. На верхней панели главного окна откройте пункт меню **Профили > Управление профилями**. Это же вы можете сделать через контекстное меню файла или на панели инструментов: выберите пункт **Профили**.
2. Откройте профиль, в котором необходимо установить/ изменить параметры. В окне **Параметры настройки** откройте раздел **Каталоги**.



В этом подкаталоге вы можете установить место, куда будут сохраняться рабочие файлы (входящие, временные, исходящие), **в текущем каталоге** или **в специально отведенных для этого каталогах**.

- **Каталоги для хранения временных файлов;**

  Эта настройка позволяет установить для временных файлов собственный каталог пользователя вместо системного.

  На этот каталог можно установить права доступа только для пользователей, работающих с данной настройкой. Это ограничит несанкционированный доступ к временным данным, которые могут содержать конфиденциальную информацию.

По умолчанию используется системный каталог. Обычно это "c:\Documents and Settings\<имя пользователя>\Local Settings\Temp\".

- Указать специальные **Каталоги для хранения входящих документов**, в которых будут храниться исходные документы, полученные в результате проведения операции Снятия и проверки электронной подписи.
- Указать специальные **Каталоги для хранения исходящих документов**, в которых будут храниться исходные документы, полученные в результате проведения операции Снятия и проверки электронной подписи.
- Здесь же вы можете настроить уровень безопасного удаления файлов.

  При обычном удалении с жесткого диска, файл помечается как удаленный, и занимаемое им место освобождается. Но при этом сами данные файла остаются на диске, и, в силу особенности строения файловых систем, эти данные еще можно извлечь с диска.

  Чтобы избежать такого восстановления, перед удалением файл можно перезаписать случайными данными. Такой файл невозможно восстановить обычными программными средствами. Также можно сделать несколько проходов перезаписи, что значительно усложнит восстановление или сделает его невозможным даже специальными программными средствами.

  Настройка уровня безопасного удаления задает количество проходов перезаписи случайными данными, перед удалением временных файлов, созданных программой «КриптоАРМ» при операциях с подписанными и шифрованными данными.

Можно выбрать четыре уровня безопасного удаления:

- **Выключено** - перезапись случайными данными не будет производиться.
- **Низкий** - Перед удалением будет произведена однократная перезапись случайными данными.
- **Средний** - Перед удалением будет произведена семикратная перезапись случайными данными.
- **Высокий** - Перед удалением перезапись случайными данными будет произведена тридцать пять раз.

	Скорость обработки файлов большого объема может уменьшиться при включении Высокого уровня удаления

Установив параметры работы с каталогами, сохраните внесенные изменения (кнопка **Применить**).

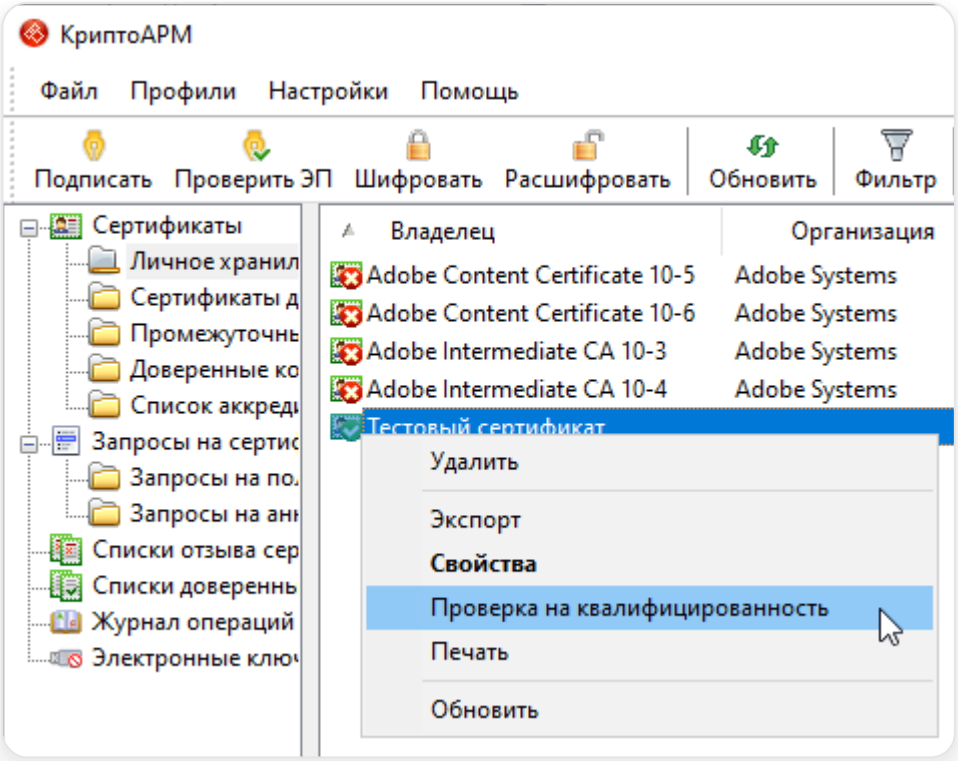
Открыть статью на сайте

Проверка сертификата на квалифицированность

Программа «КриптоАРМ» имеет возможность проверять сертификаты на соответствие требованиям приказа ФСБ РФ от 27.12.2011 №795 «Об утверждении Требований к форме квалифицированного сертификата ключа проверки электронной подписи».

Проверку сертификата можно осуществить через:

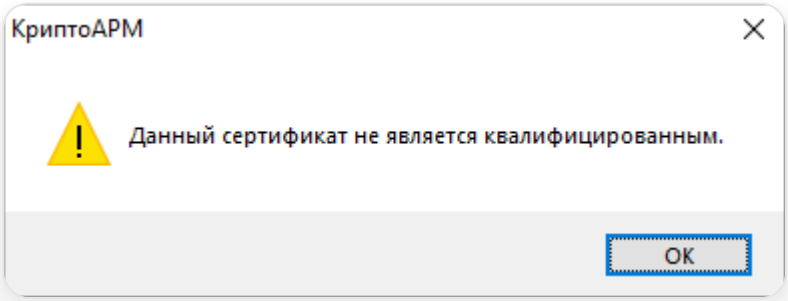
1. **контекстное меню в главном окне программы** (такая проверка только для сертификатов, установленных в хранилище)



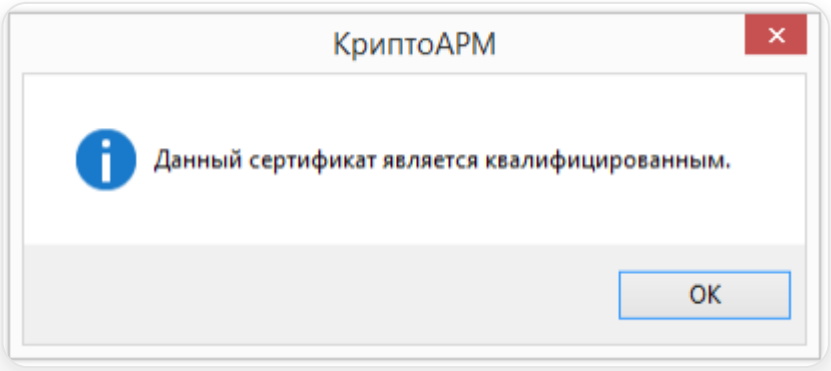
2. **контекстное меню Проводника** (проверка для сертификатов, не установленных в хранилище)

Результаты проверки сертификата:

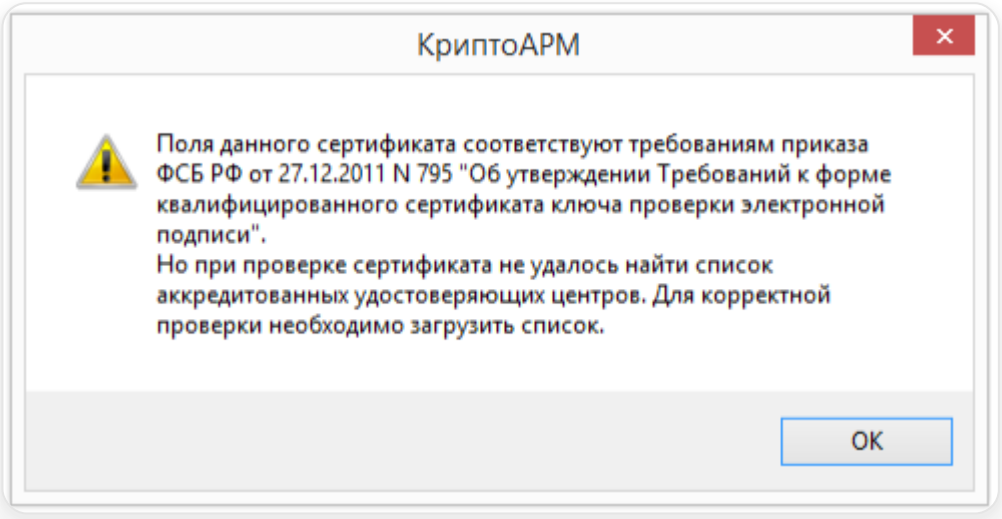
- Сертификат не прошел проверку, то есть не является квалифицированным;



- Сертификат полностью прошёл проверку и соответствует требованиям, предъявляемым к квалифицированному сертификату ключа проверки электронной подписи;



- Проверка сертификата на квалифицированность прошла не полностью. Не удалось построить полный путь сертификации по списку аккредитованных удостоверяющих центров (TSL). Для корректного завершения проверки, необходимо установить TSL. Подробнее о загрузке списка аккредитованных удостоверяющих центров вы можете почитать в главе "Квалифицированная подпись".



Открыть статью на сайте

Как получить новый сертификат?

Получение нового сертификата выполняется в соответствии с регламентом работы, определенным Центром регистрации (плановая смена ключей и сертификатов) при внеплановой смене ключей и сертификатов (отзыв ранее действующего сертификата).

Получить новый сертификат вы можете на основании поданного в Удостоверяющий центр запроса на сертификат. В процессе создания запроса производится генерация ключей и запись их на ключевой носитель.

О том, как создать запрос на сертификат читайте в разделе Операции с запросами на сертификат.

Центр регистрации передает запрос на получение нового сертификата в Центр сертификации, где и происходит формирование сертификата. Выпущенный сертификат устанавливается пользователем в хранилище сертификатов своего рабочего места (на компьютер).

В процессе установки сертификата также автоматически производится его запись на ключевой носитель. В дальнейшем данный сертификат может быть повторно установлен на рабочее место пользователя (например, при потере сертификата в результате сбоя компьютера или операционной системы) или на другое рабочее место (в случае перехода пользователя на другое рабочее место). В этом случае сертификат с ключевого носителя устанавливается с помощью программы «КриптоАРМ».

Открыть статью на сайте

Как создать самоподписанный сертификат?

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

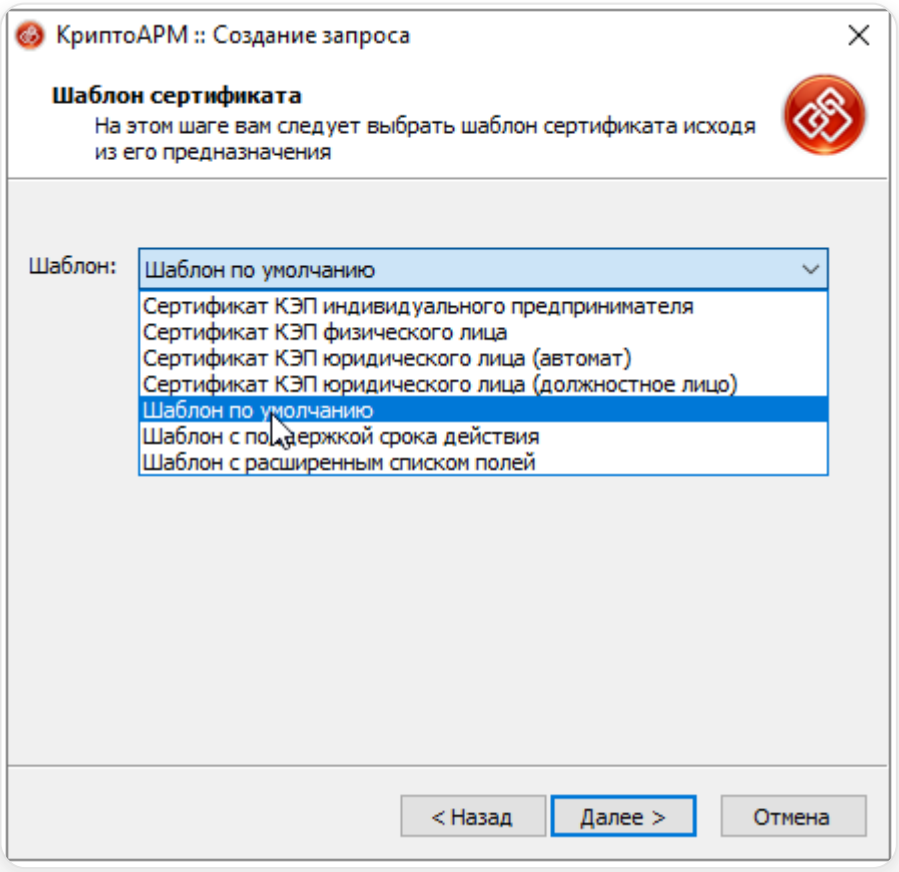
Самоподписанные сертификаты используются для обмена зашифрованными или подписанными документами между людьми, доверяющими друг другу, например, друзьями, коллегами. Обменявшись такими сертификатами между собой, они могут пересылать друг другу подписанные и зашифрованные электронные данные, не беспокоясь при этом, что информация может быть перехвачена, искажена и использована против их интересов.



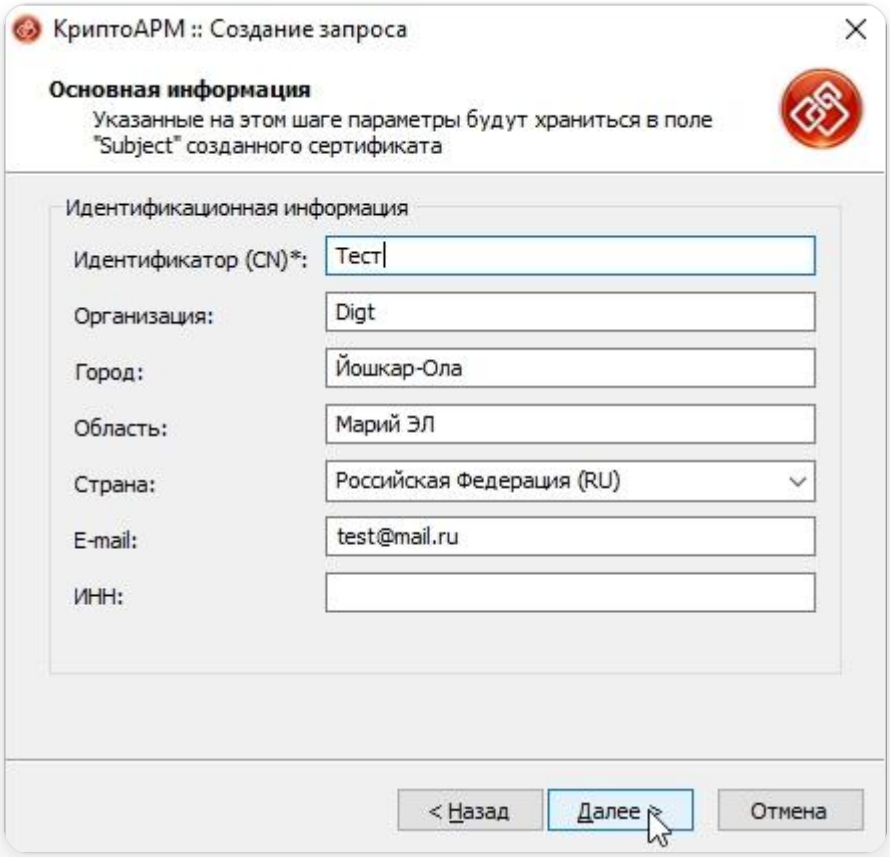
Важно помнить, что использование самоподписанных сертификатов не позволяет решать конфликтные ситуации, возникающие при обмене конфиденциальными данными, с помощью суда.

Для создания самоподписанного сертификата, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Сертификаты**. Вызовите правой клавишей мыши контекстное меню и выберите пункт **Создать > Самоподписанный сертификат**. Откроется Мастер создана самоподписанного сертификата.
2. На первом шаге ознакомьтесь с порядком и требованиями создания самоподписанного сертификата. Нажмите **Далее**.
3. На следующем шаге из выпадающего списка выберите шаблон сертификата:

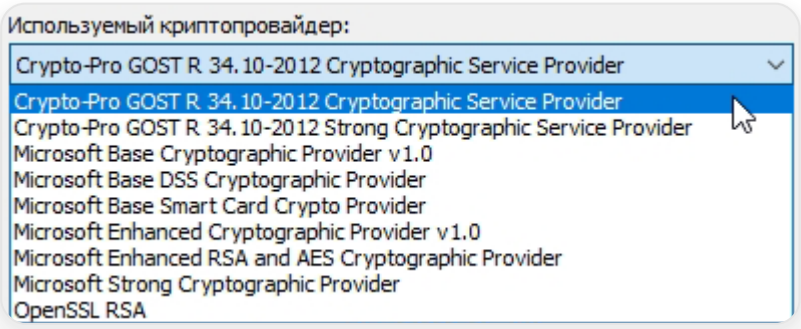


4. Укажите идентификационную информацию о владельце будущего сертификата, в зависимости от того, какой шаблон вы выбрали на предыдущем шаге.

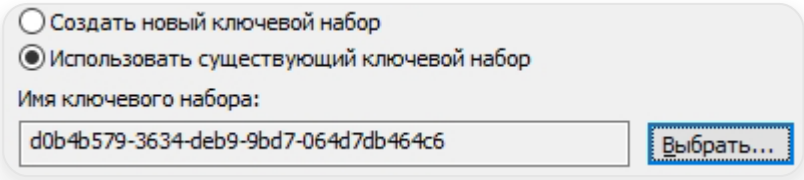


	Поля отмеченные знаком «*» являются обязательными для заполнения.
	Обратите внимание, если вы указываете ИНН юридического лица, номер всегда должен начинаться с «00», например 007707049388.
	СНИЛС указывается без пробелов и знаков «-», например, 07306654534.

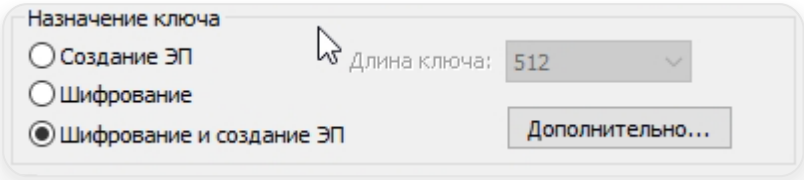
5. В открывшемся окне **Параметры ключа** в выпадающем списке выберите укажите следующие настройки:
    - Используемый криптопровайдер.



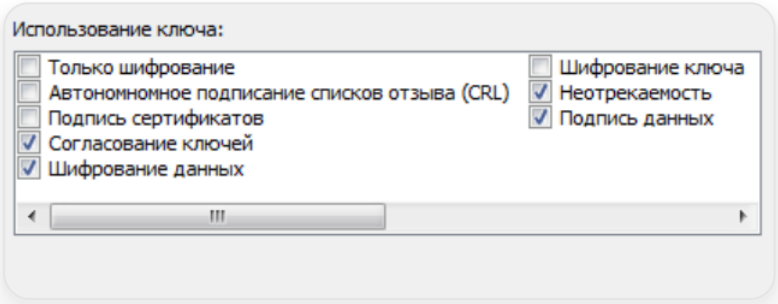
- Выберите вариант создания ключевого набора.
  - **Создать ключевой набор -** сертификат будет создан на основе нового ключевого набора.
  - **Использовать существующий ключевой набор** – выберите ключевой набор, который будет использован при создании сертификата, из списка существующих (кнопка **Выбрать**).



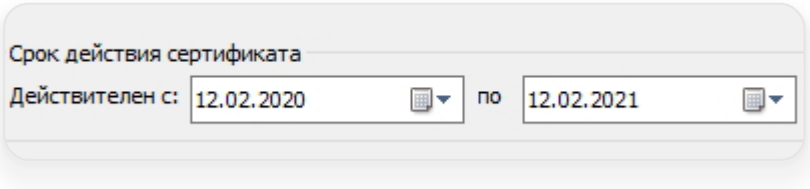
- Установите переключатель напротив необходимого Назначения ключа сертификата.



- Вы также можете выбрать дополнительное назначение ключа, нажав на кнопку **Дополнительно**. В списке назначений использования ключа выберите необходимое:

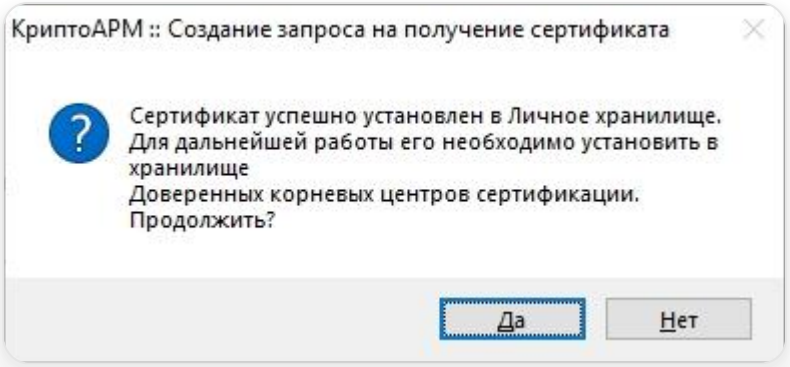


В разделе **Срок действия сертификата** автоматически проставляется дата, с которой сертификат действителен (текущее системное время) и дата, по которую сертификат действителен (1 год вперед от текущего времени). Эти даты вы можете отредактировать.



- Укажите необходимую **Длину ключа**. Чем длиннее ключ, тем он надежнее.
- **Пометить ключи как экспортируемые**. Если вы отметите этот флаг, то сможете проводить экспорт сертификата вместе с закрытыми ключами.

7. На основе указанных данных будет сформирован самоподписанный сертификат открытого ключа. После завершения операции возникнет окно с информацией о ее результатах. Нажмите **Готово**.
8. На запрос системы установите пароль на носитель и подтвердите его.
9. На запрос системы установить ли самоподписанный сертификат в хранилище Доверенных корневых центром сертификации, нажмите на кнопку **Да**.



Открыть статью на сайте

Импорт (установка) сертификата

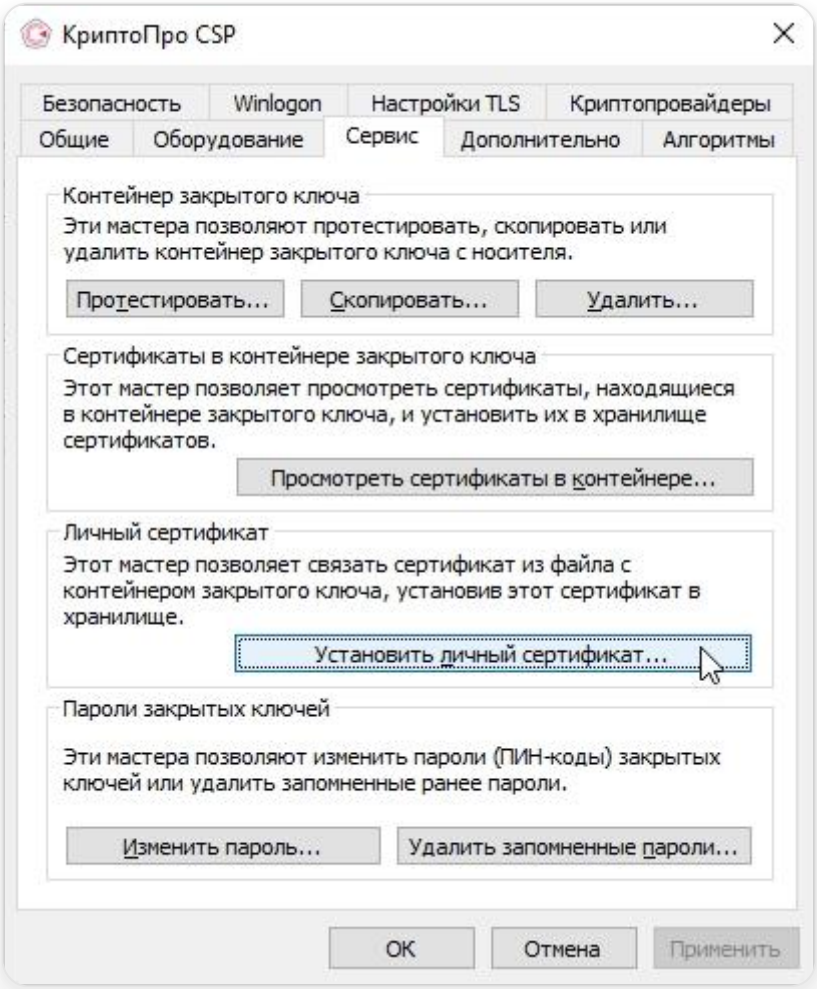
Импорт сертификатов может понадобиться для выполнения следующих задач:

- Установка сертификата, который был отправлен вам другим пользователем, компьютером или центром сертификации;
- Восстановление поврежденного или утерянного сертификата, заархивированного ранее;
- Установка сертификата и связанного с ним закрытого ключа с компьютера, на котором владелец сертификата его использовал ранее.

Первичная установка в хранилище личного сертификата ГОСТ может выполняться как средствами криптопровайдера «КриптоПро CSP», так и средствами программы «КриптоАРМ».

Внимание! В меню КриптоАРМ выберите Настройки - Управление настройками - режимы и выключите режим квалифицированной подписи.

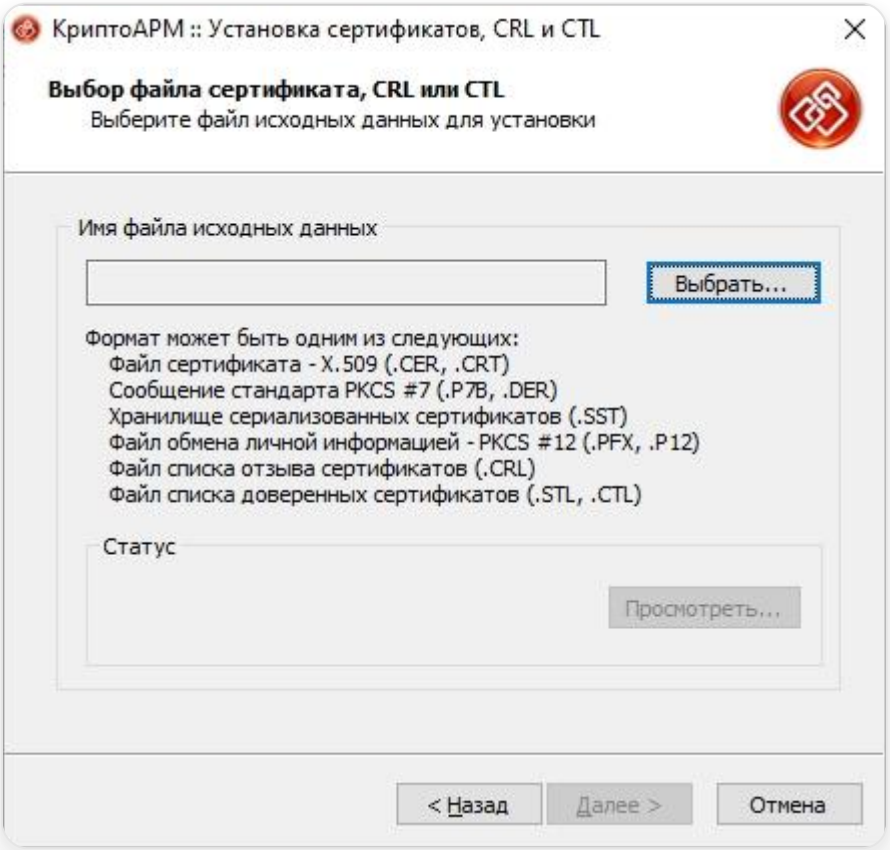
Установка личного сертификата средствами «КриптоПро CSP» осуществляется непосредственно в окне криптопровайдера «КриптоПро CSP», закладка «Сервис».



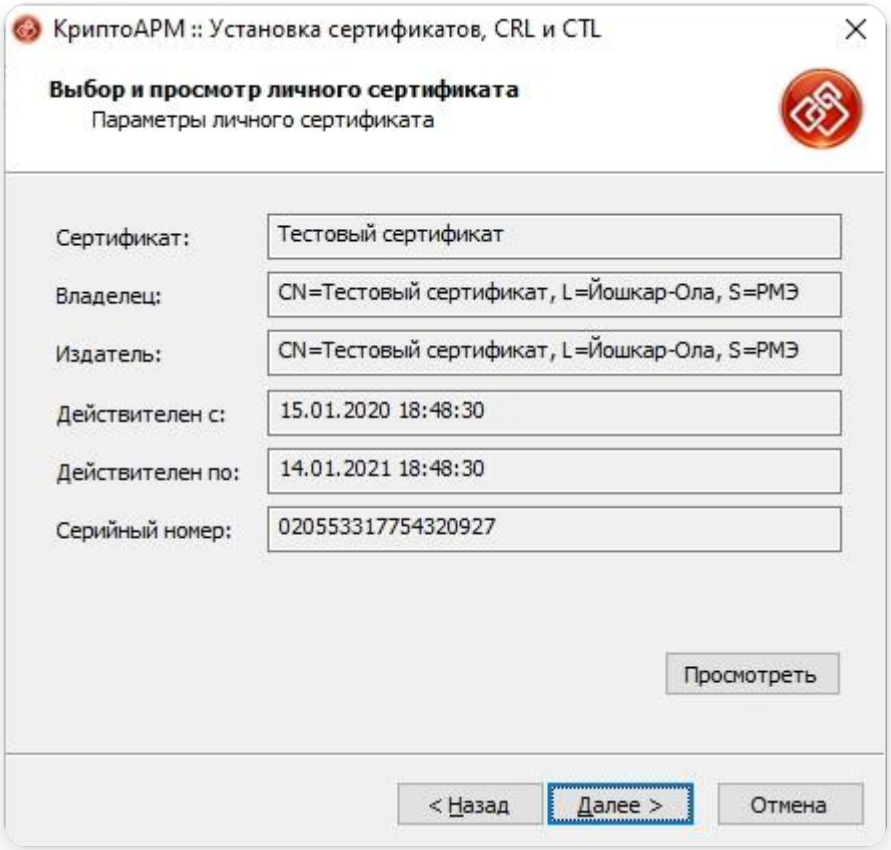
Установка личного сертификата средствами программы «КриптоАРМ»

Чтобы установить сертификат с помощью «КриптоАРМ», выполните следующие шаги:

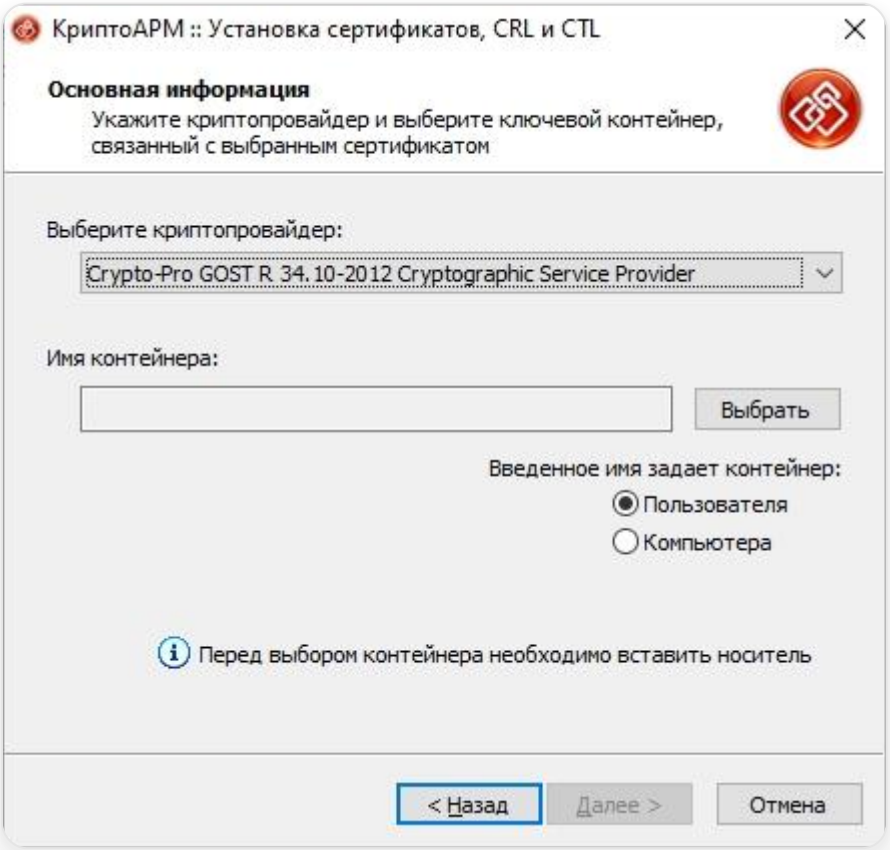
1. В главном окне в разделе Сертификаты выберите хранилище, куда необходимо импортировать сертификат. В контекстном меню раздела или на панели инструментов выберите пункт **Импорт**.
2. Откроется стандартный Мастер установки сертификата, позволяющий установить цифровой сертификат в хранилище для дальнейшего использования. Ознакомьтесь с порядком выполнения операции.
3. Если вы устанавливаете личный сертификат, в этом же окне установите флаг напротив строки **Установить личный сертификат**. Кроме того, вы можете установить флаг **Поместить сертификат в контейнер** (в этом случае в ключевом контейнере будет храниться не только ключевая пара, но и сам сертификат).
4. В следующем окне укажите файл, содержащий импортируемый сертификат. Система позволяет импортировать сертификаты следующих форматов:
   - Файл сертификата X.509 (.CER, CRT)
   - Сообщение стандарта PKCS #7 (. P7B, .DER)
   - Хранилище сериализованных сертификатов (.SST) – несколько сертификатов, объединенных в один файл.
   - Файл обмена личной информацией – PKCS #12



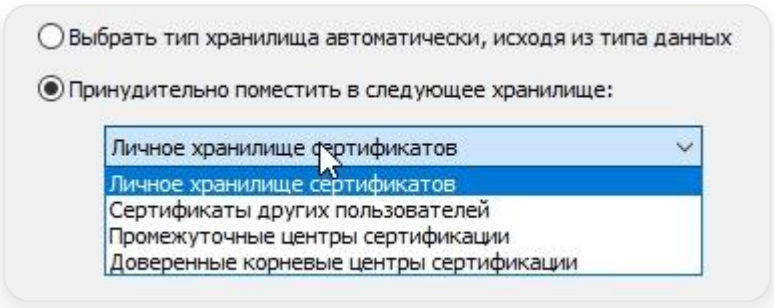
5. Если вы устанавливаете личный сертификат, на следующем этапе откроется окно, содержащее информацию о нем (данные о владельце и издателе сертификата, срок действия и серийный номер):



6. Если на первом этапе вы установили флаг **Поместить сертификат в контейнер**, откроется окно, в котором вам нужно
   - Выбрать криптопровайдер;
   - Выбрать из списка имя ключевого контейнера (перед этим вставьте ключевой носитель, на котором храниться данный контейнер);
   - Укажите, что введенное имя задает контейнер пользователя.



7. Если на первом шаге вы не установили флаг **Установить личный сертификат**, то система вам предложит указать хранилище, в котором будет храниться импортируемый сертификат:
   - Автоматический (тип хранилища выбирается системой);
   - Для ручного выбора хранилища, в выпадающем меню выберите необходимое хранилище.



3. После завершения операции возникнет сообщение об успешном импорте сертификата.

Открыть статью на сайте

Хранение сертификатов

Программа «КриптоАРМ» в качестве хранилищ использует поддерживаемые криптопровайдером типы, а также стандартные хранилища сертификатов, входящих в операционную систему Windows.

Название хранилища сертификатов	Описание хранилища
Личное хранилище сертификатов	Личные сертификаты, используемые вами и связанные с вашими закрытыми ключами.
Сертификаты других пользователей	Сертификаты пользователей, с которыми вы обмениваетесь шифрованными или подписанными данными.
Промежуточные центры сертификации	Сертификаты промежуточных центров сертификации.
Доверенные корневые центры сертификации	Автоматически подписанные сертификаты от центра сертификации, которые неявным образом являются доверенными. Здесь хранятся сертификаты, изданные сторонними удостоверяющими центрами, Microsoft, а также вашей организацией (если организация располагает собственным сервером сертификатов). Хранилище также содержит самоподписанные сертификаты.
Доверенные издатели сертификатов	Сертификаты доверенных издателей сертификатов.

Открыть статью на сайте

Как проверить статус сертификата?

Использование сертификата можно условно разделить на два этапа

- проверка статуса сертификата
- если статус «действителен», использование сертификата для выполнения криптографических операций.

Каждый раз при обращении к сертификату программа «КриптоАРМ» проверяет его статус. Существует несколько типов проверки статуса сертификатов:

> 1. По локальному списку отзыва сертификатов (COC)
> 2. По списку отозванных сертификатов из удостоверяющего центра
> 3. С использованием Revocation Provider
> 4. В OCSP службе
> 5. С помощью списка доверенных сертификатов
> 6. В режиме «Квалифицированная подпись»

Статус сертификата проверяется по следующим параметрам:

Параметры проверки	Пояснение
Проверка срока действия сертификата	Проверяется, истек или нет срок действия цифрового сертификата
Проверка корректности электронной подписи выдавшего сертификат Удостоверяющего центра	Для заверения вашего личного цифрового сертификата используется электронная подпись Удостоверяющего центра, в котором вы получили свой сертификат. Чтобы статус вашего сертификата был "Действителен", необходимо иметь установленный корневой сертификат и актуальный список отзыва сертификатов.
Построение цепочки (до корневого сертификата УЦ)	Доверие к личному сертификату пользователя определяется на основе цепочки сертификатов. Начальным элементом цепочки является корневой сертификат УЦ, хранящийся в хранилище **Доверенные корневые центры сертификации**.
Проверка действительности сертификата по спискам отзыва сертификатов	По умолчанию при работе с сертификатами в «КриптоАРМ» их статус проверяется по COC, установленному в хранилище **Промежуточные центры сертификации**. Но также возможно выполнить проверку сертификата по **COC, полученному из УЦ**, или с помощью **Revocation Provider**.

	Начиная с версии 5.3, статус отзыва не проверяется для личных сертификатов пользователя
С помощью списка доверенных сертификатов	Чтобы проверить статус сертификата с помощью списка доверенных сертификатов необходимо отметить "Использовать CTL для проверки пути сертификации" в настройках по умолчанию в разделе Параметры верификации сертификатов".

Возможны 3 статуса действительности сертификатов, выданных УЦ:

	"действителен"
	"недействителен"
	"неизвестен"

Сертификат является действительным, если:

1. Подпись Удостоверяющего центра под сертификатом корректна.
2. Срок действия сертификата не истек.
3. Сертификат используется для тех целей, для которых был создан.
4. Сертификат не отозван и его действие не приостановлено.

Чтобы проверить статус сертификата:

1. В дереве элементов главного окна выберите раздел **Сертификаты**. Откройте нужное вам хранилище, в котором выберите сертификат для проверки.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус**
   - По локальному списку отзыва сертификатов (списку, установленному в хранилище **Списки отзыва сертификатов**);
   - По списку отзыва из Удостоверяющего центра (в онлайн-режиме по локальной сети);
   - С использованием Revocation Provider;
   - Проверить в OCSP службе.

При проверке статуса сертификата могут возникнуть следующие сообщения:

Сообщение	Пояснение
Истёк срок действия сертификата	Сертификат, которым подписаны данные, просрочен
Невозможно построить цепочку для сертификата	Невозможно построить цепочку сертификатов от клиентского сертификата до сертификата доверенного УЦ
Произошла ошибка при обновлении COC	

	Настройки системы безопасности не предполагают обновлений СОС; библиотека CPCRLUpdate.dll отсутствует или не зарегистрирована
Произошла ошибка при открытии хранилища	Нет прав доступа к хранилищу сертификатов
СОС найден, однако возник сбой при его обработке	СОС хранится в неизвестном формате
СОС найден, однако он нуждается в обновлении	Дата обновления СОС истекла, необходимо обновить СОС в УЦ, для того чтобы сертификат бы действительным
Ошибка при сопоставлении СОС и сертификата	Ошибка в процессе поиска клиентского сертификата в последнем выпущенным УЦ СОС
Сертификат содержится в СОС	Сертификат недействителен (отозван в УЦ по какой-либо причине и занесен в СОС);

	Чтобы упростить процедуру проверки статуса сертификата, вы можете в настройках выполнения операций указать параметры проверки сертификатов. Для выбранных сертификатов в процессе работы всегда автоматически будет использоваться указанный вами способ проверки.

Проверка статуса сертификата по локальному СОС

«КриптоАРМ» поддерживает способ проверки статуса цифрового сертификата по локальному списку отзыва сертификатов (СОС), периодически обновляемого Удостоверяющим центром согласно Регламенту данного УЦ.

Чтобы проверить статус сертификата, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Сертификаты** - нужное вам хранилище, в котором выберите сертификат (или группу сертификатов) для проверки.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус - по локальному СОС**.

Статусы сертификатов

Статус	Пояснение
 "действителен"	Выполняются все условия действительности сертификата
 "недействителен"	Срок действия сертификата истек: • Есть непросроченный СОС и в нем находится указанный сертификат • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП

	• Не удалось получить СОС из УЦ (если выполняется обязательная проверка по СОС, полученному из УЦ)
 "неизвестен"	Статус, возможный только для сертификатов, которым не требуется проверка по СОС, полученному из УЦ: • отсутствует СОС • СОС просрочен

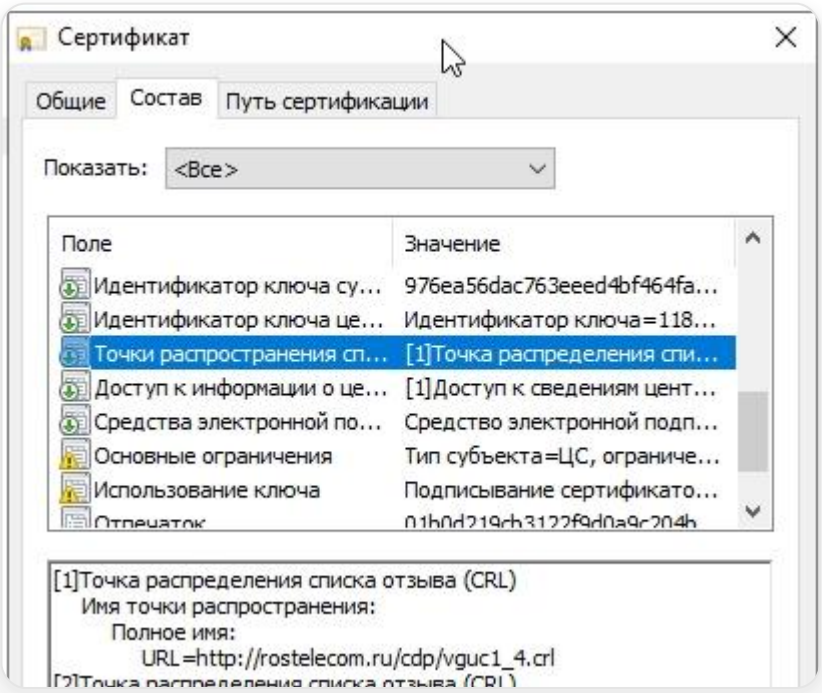
Возможные ошибки обновления списка отозванных сертификатов (СОС)

Ошибка	Объяснение
0x80092004 (Cannot find object or property.)	• Не найден издатель проверяемого сертификата. • Файл СОС не соответствует проверяемому сертификату.
0x80092007 (The specified certificate is self signed.)	Проверяемый сертификат - самоподписанный. Нет смысла проверять самоподписанный сертификат по СОС, т.к. СОС подписывается тем же самым самоподписанным сертификатом.

Проверка статуса сертификата по СОС из УЦ

«КриптоАРМ» позволяет проверять статус цифрового сертификата в режиме получения (и их участия в процедурах проверок) СОС в онлайн режиме из CDP и/или сетевого справочника системы.
Для использования возможности получения СОС из УЦ необходимо соблюдение следующих условий:

1. В проверяемом сертификате должно присутствовать расширение **«Точка распространения СОС / CRL Distribution Point (CDP)»**. При этом если значений (URL’ов) в расширении несколько, то программа «КриптоАРМ» будет пытаться скачать СОС по всем адресам до первого успешного скачивания. Поддерживаются часто используемые протоколы - "ftp", "http" и "file".



2. По одной из точек распространения COC (оптимально, если по первой) можно скачать COC с помощью веб-браузера, например Microsoft Internet Explorer. При этом, не вводя никакой дополнительной информации (имени пользователя, пароля, перехода по ссылкам). Протестировать можно следующим образом:
   - закрыть все окна Internet Explorer (т.к. они могут хранить параметры доступа к серверу);
   - запустить Internet Explorer и вставить в поле адреса URL из точки распространения COC;
   - нажать Enter, после чего Internet Explorer должен сразу предложить сохранить скачанный файл COC;
   - сохранить COC в файл и открыть его проводником Windows (должна без ошибок открыться форма просмотра COC).

Чтобы проверить статус сертификата:

- В дереве элементов главного окна выберите раздел **Сертификаты** - нужное вам хранилище, в котором выберите сертификат (или группу сертификатов) для проверки.
- В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус - по COC из УЦ**.

Статус	Пояснение
"действителен"	Выполняются все условия действительности сертификата
"недействителен"	• Срок действия сертификата истек • Есть непросроченный COC и в нем находится указанный сертификат • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП

"неизвестен"	Статус, возможный только для сертификатов, которым не требуется проверка по СОС, полученному из УЦ: • отсутствует СОС • СОС просрочен • не удалось получить СОС из УЦ

Возможные ошибки обновления СОС

Ошибка	Объяснение
0x800C0005	Ошибка скачивания СОС по сети, например, файл не найден или нет доступа.
0x80092004 (Cannot find object or property.)	• Не найден издатель проверяемого сертификата. • Файл СОС не соответствует проверяемому сертификату.
0x80092007 (The specified certificate is selfsigned.)	Проверяемый сертификат - самоподписанный. Нет смысла проверять самоподписанный сертификат по СОС, т.к. СОС подписывается тем же самым самоподписанным сертификатом

Проверка статуса сертификата с помощью Revocation Provider

При работе с сертификатами в «КриптоАРМ» их статус можно проверить с помощью Revocation Provider (если на компьютере пользователя установлен «КриптоПро Revocation Provider»).

Чтобы проверить статус сертификата:

1. В дереве элементов главного окна выберите раздел **Сертификаты** - нужное вам хранилище, в котором выберите сертификат (или группу сертификатов) для проверки.
2. В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус - с использованием Revocation Provider**.

Статус	Пояснение
"действителен"	Выполняются все условия действительности сертификата
"недействителен"	• Срок действия сертификата истек • Из OCSP Службы получен ответ "Сертификат отозван" или сертификат включен в список отзыва, опубликованный УЦ (в зависимости от типа Revocation Provider: Microsoft или «КриптоПро») • Не строится цепочка сертификации

	• Сертификат имеет некорректную ЭП
 "неизвестен"	Статус, возможный только для сертификатов, которым не требуется проверка по СОС, полученному из УЦ: • отсутствует СОС • СОС просрочен • не удалось получить СОС из УЦ

Проверка статуса сертификата в OCSP службе

«КриптоАРМ» поддерживает способ проверки статуса цифрового сертификата в OCSP службе (при установленной лицензии на модуль OCSP). При проверке статуса сертификата по OCSP формируется запрос в службу OCSP и его отправка по адресу, прописанному в сертификате или указанному в настройках групповых политик.
Если сертификат не имеет атрибута, содержащего адрес службы OCSP, то параметры доступа к службе берутся из текущей установленной по умолчанию настройке.
Если сертификат содержит адрес службы или несколько адресов, то параметры доступа в служб (такие как настройки прокси-сервера или сертификат аутентификации) берутся из OCSP профиля. При этом программа будет повторно пытаться получить OCSP ответ для каждого адреса OCSP до тех пор, пока не будет получен ответ со статусом (сертификат действителен или сертификат недействителен).
Если ни по одному из адресов, указанных в сертификате, не был получен ответ со статусом сертификата, то проверяется статус сертификата в службе, адрес которой указан в настройке.

Чтобы проверить статус сертификата:

- В дереве элементов главного окна выберите раздел Сертификаты - нужное вам хранилище, в котором выберите сертификат (или группу сертификатов) для проверки.
- В контекстном меню объекта или на панели инструментов выберите пункт **Проверить статус - В службе OCSP**.

Статус	Пояснение
 "действителен"	Выполняются все условия действительности сертификата
 "недействителен"	• Срок действия сертификата истек • Из OCSP Службы получен ответ "Сертификат отозван" • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП
 "неизвестен"	Ошибка доступа к службе OCSP

Проверка сертификата с помощью списка доверенных сертификатов

Чтобы проверить статус сертификата:

1. Необходимо отметить "Использовать CTL для проверки пути сертификации" в настройке верификации сертификатов.
2. После произведенных действий все сертификаты, корневой сертификат которых не включен в список доверенных сертификатов, станут недействительными.

Статус	Пояснение
"действителен"	Выполняются все условия действительности сертификата
"недействителен"	• Срок действия сертификата истек • Есть непросроченный COC, и в нем находится указанный сертификат • Не строится цепочка сертификации • Сертификат имеет некорректную ЭП • Не удалось получить COC из УЦ (если выполняется обязательная проверка по COC, полученному из УЦ)
"неизвестен"	Ошибка доступа к службе OCSP

Открыть статью на сайте

Работа с квалифицированными сертификатами

Для многих сегодня становится проблемой гарантировать, что получаемые электронные документы подписаны действительно квалифицированной электронной подписью. Для решения этой задачи мы ввели технологию, которая позволяет с точностью определять, является ли сертификат подписи квалифицированным или нет.

Режим «Квалифицированная подпись»

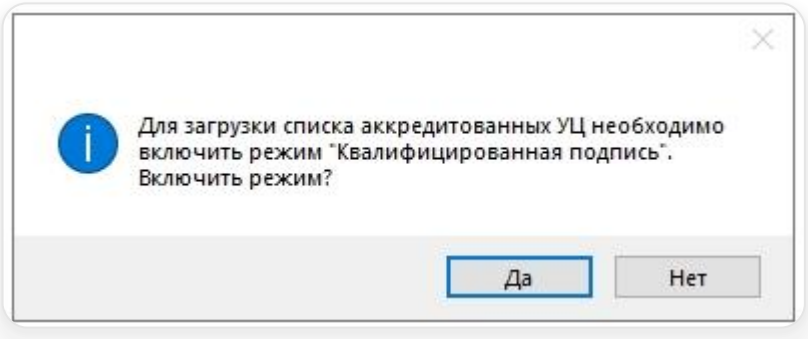
Для работы исключительно с квалифицированными сертификатами вам достаточно включить в программе «КриптоАРМ» режим «Квалифицированная подпись».

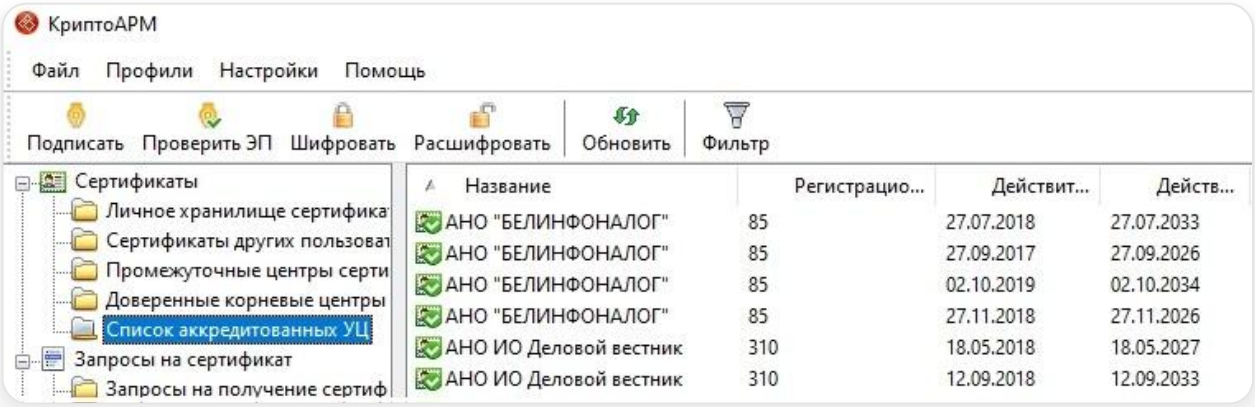
При включенном режиме Квалифицированная подпись вам станут доступны только сертификаты, которые выданы аккредитованными удостоверяющими центрами и соответствуют требованиям к форме квалифицированного сертификата. То есть только квалифицированные сертификаты ключа проверки электронной подписи. Все остальные сертификаты скрываются. Проверка сертификатов, которыми подписаны электронные документы, выполняется также при включенном режиме.

Просмотр списка аккредитованных удостоверяющих центров

На портале Уполномоченного федерального органа в области электронной подписи Минкомсвязи размещается актуальный список аккредитованных удостоверяющих центров. Именно этот список используется программой «КриптоАРМ» в качестве фильтра при работе с электронной подписью. Список отображается в отдельной папке **Список аккредитованных УЦ**.

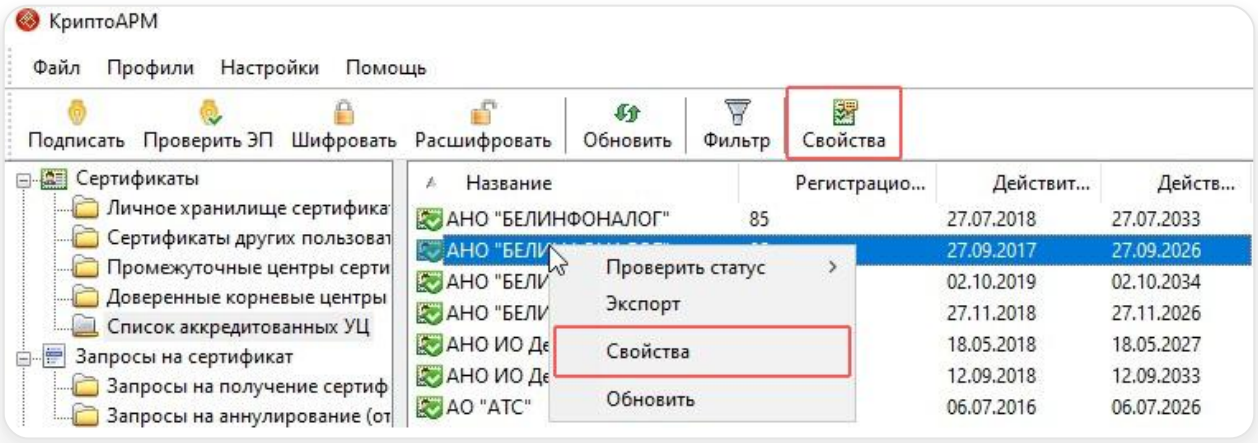
Чтобы загрузить актуальный список аккредитованных УЦ, предварительно включите режим «Квалифицированная подпись» (**Сервис - Параметры программы - Режимы**).





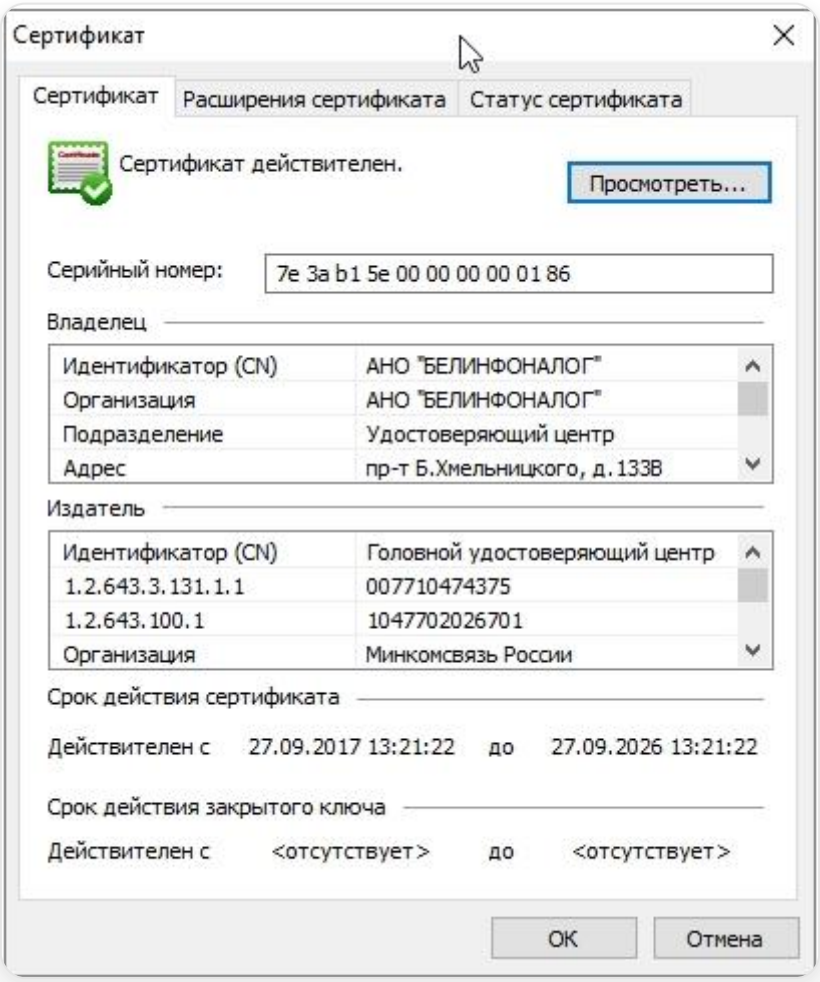
Вы можете просмотреть подробную информацию о корневом сертификате каждого удостоверяющего центра в списке.

Для этого найдите строку с названием нужного вам удостоверяющего центра и в контекстном меню объекта (либо на панели инструментов главного окна) выберите пункт **Свойства**.



Откроется окно **Сертификат**, в котором вы можете узнать подробную информацию о сертификате:

- серийный номер, владелец, издатель, срок действия сертификата и закрытого ключа (закладка **Сертификат**),
- расширения сертификата: использование ключа, политики сертификата и др. (закладка **Расширения сертификата**),
- общий статус проверки полного пути сертификации (закладка **Статус сертификата**)


Сертификат
Сертификат
Расширения сертификата
Статус сертификата
Сертификат действителен.
Просмотреть...
Серийный номер:
7e 3a b1 5e 00 00 00 00 01 86
Владелец
Идентификатор (CN)
АНО "БЕЛИНФОНАЛОГ"
Организация
АНО "БЕЛИНФОНАЛОГ"
Подразделение
Удостоверяющий центр
Адрес
пр-т Б.Хмельницкого, д.133В
Издатель
Идентификатор (CN)
Головной удостоверяющий центр
1.2.643.3.131.1.1
007710474375
1.2.643.100.1
1047702026701
Организация
Минкомсвязь России
Срок действия сертификата
Действителен с 27.09.2017 13:21:22 до 27.09.2026 13:21:22
Срок действия закрытого ключа
Действителен с <отсутствует> до <отсутствует>
OK
Отмена

Открыть статью на сайте

Просмотр информации о сертификате

Для просмотра информации о сертификате выполните следующие шаги:

1. Выберите необходимый из списка и дважды щелкните по нему мышью, либо вызовите правой клавишей мыши контекстное меню и выберите пункт **Свойства**.

2. Откроется окно **Сертификат** для просмотра подробной информации о сертификате.
   В окне сертификат вам будут доступны 3 закладки:
   - Сертификат;
   - Расширения сертификата;
   - Статус сертификата.

4. В закладке **Сертификат** доступна следующая информация:
   - Статус сертификата;
   - Серийный номер сертификата;
   - Сведения о владельце сертификата;
   - Сведения об издателе сертификата;

5. Срок действия сертификата (с какого и до какого периода действителен сертификат).

6. В закладке **Расширения сертификата** доступна следующая информация:
   - Варианты использования ключа;
   - Политики сертификата;
   - Средства электронной подписи и УЦ издателя.

4. В закладке **Статус сертификата** отображен общий статус проверки полного пути сертификации. В этой закладке вы можете проверять статус сертификата.

   Информацию о сертификате вы также можете просмотреть через стандартное окно просмотра свойств сертификата Windows. Для этого в окне просмотра информации о сертификате в закладке **Сертификат** нажмите на кнопку **Сертификат**, либо в закладке **Статус сертификата - Просмотреть**.

   Откроется стандартное окно просмотра свойств сертификата Windows. Окно содержит три закладки: Общие, Состав, Путь сертификации.

   В закладке **Общие** дается базовая информация о сертификате.

   В закладке **Состав** даны более подробные сведения о сертификате: представлен перечень атрибутов сертификата и их значения. В таблице перечислены основные сведения о составе сертификата:

В закладке **Путь сертификации** отображается место сертификата в цепочке доверия (или сертификационный путь) - от корневого сертификата Удостоверяющего центра до просматриваемого сертификата.

Удостоверяющим центрам, сертификаты которых хранятся в хранилище доверенных корневых центров сертификации, оказывается по умолчанию большое доверие. Это позволяет всем выпущенным ими сертификатам наследовать доверие от ЦС. Если в сертификационном пути присутствует только один сертификат, то такие сертификаты называются самоподписанными. Все корневые ЦС имеют такие сертификаты.

В нижней части окна отображается информация о владельце сертификата, статусе сертификата и подробности о статусе.

Информация о сертификате также доступна в финальном окне всех криптографических операций.

Сведения о сертификате	Поля	Значение полей
Поля v1	Версия	Номер версии протокола x.509
	Серийный номер	Уникальный серийный номер, присвоенный сертификату центром сертификации. Серийный номер уникален для всех сертификатов, выданных определенным центром сертификации
	Алгоритм подписи	Алгоритм хеширования, который центр сертификации использует для электронной подписи сертификата
	Издатель	Сведения о центре сертификации, выдавшем данный сертификат
	Действителен с	Начальная дата срока действия сертификата
	Действителен по	Конечная дата срока действия сертификата
	Субъект	Имя лица или центра сертификации, которым выдан сертификат. Если центр сертификации находится на сервере члена домена организации, это будет отличительное имя в организации. В ином случае это

		может быть полное имя и адрес электронной почты или другой идентификатор.
	Открытый ключ	Длина и тип открытого ключа, связанного с сертификатом
Расширения	Улучшенный ключ	Назначения, для которых сертификат может быть использован
	Идентификатор ключа субъекта	Обеспечивает идентификацию сертификатов, включающих конкретный открытый ключ
	Идентификатор ключа центра сертификатов	Обеспечивает идентификацию открытого ключа, связанного с закрытым ключом, который используется для подписи удостоверяющим центром сертификата
	Точки распространения списка отзыва сертификата (coc)	«Криптоарм» позволяет проверять статус цифрового сертификата в режиме получения coc в онлайн режиме из cdp. Для того чтобы проверять статус сертификата подобным образом, в сертификате должно присутствовать расширение «точка распространения coc / crl distribution point (cdp)». При этом если значений (url'ов) в расширении несколько, то программа «Криптоарм» будет пытаться скачать coc по всем адресам до первого успешного скачивания. Поддерживаются часто используемые протоколы: "ftp", "http" и "file"
	Доступ к информации о центрах сертификации	Предоставляет информацию о ЦС, которым выдан просматриваемый сертификат: 1. поле содержит информацию о списке корневых сертификатов центра сертификации (url) 2. адреса ocsp служб
	Использование ключа	Варианты использования закрытого ключа (например, цифровая подпись,

		неотрекаемость, шифрование ключей, шифрование данных и др.)
Критические расширения	Использование ключа	Варианты использования закрытого ключа
Свойства	Алгоритм отпечатка	Алгоритм хеширования, который генерирует сводку данных (или отпечаток) для электронных подписей
	Отпечаток	Сводка данных (или отпечаток) для электронных подписей

Открыть статью на сайте

Фильтрация и сортировка сертификатов

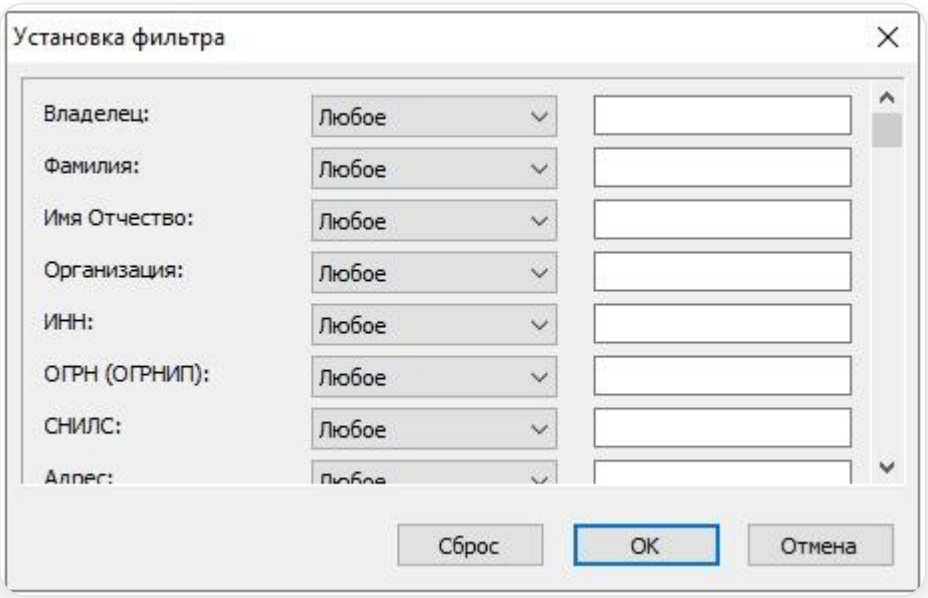
Фильтрация сертификатов

Вы можете фильтровать сертификаты в списке по следующим параметрам:

- Владелец
- Фамилия
- Имя Отчество
- Организация
- ИНН
- ОГРН (ОГРНИП)
- СНИЛС
- Адрес
- Издатель
- Электронная почта
- Серийный номер
- Дата, с которой сертификат действителен
- Дата, по которую сертификат действителен.
- Населенный пункт
- Регион
- Страна
- Электронная почта
- Серийный номер
- Отпечаток (sha1)

Чтобы отфильтровать сертификаты в списке:

1. В разделе **Сертификаты** выберите папку с тем типом сертификатов, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**.
2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать сертификаты:



3. Список сертификатов будет отфильтрован по указанным вами параметрам.
4. Вернуться к исходному списку сертификатов вы можете, сбросив фильтр.

Сортировка сертификатов в списке

В программе «КриптоАРМ» реализована возможность сортировать цифровые сертификаты в списке.

Сортировка может выполняться по следующим параметрам:

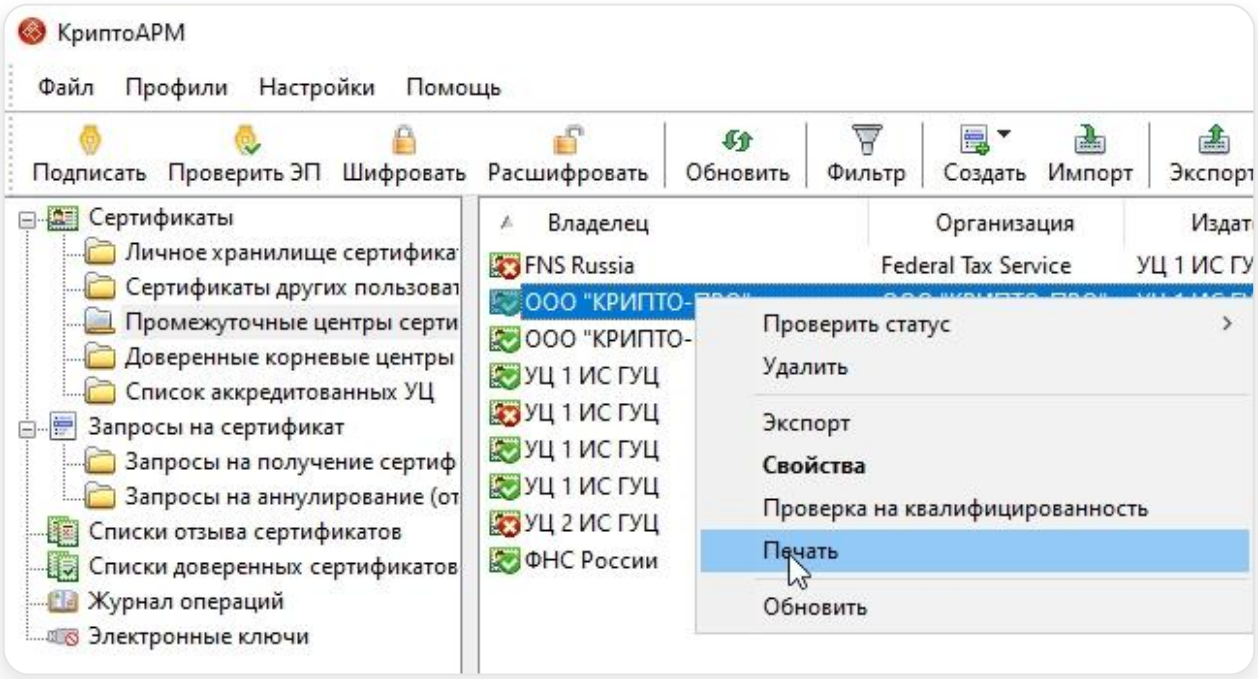
- Владелец
- Фамилия
- Имя Отчестсво
- Организация
- ИНН

Открыть статью на сайте

Печать сертификата

Для печати сертификата выполните следующие шаги:

- Откройте хранилище сертификатов, выберите необходимый сертификат (или группу сертификатов), в контекстном меню объекта или на панели инструментов выберите пункт **Печать**.



- В новом окне браузера Microsoft Internet Explorer будет сформирована печатная форма сертификата.
- Для вывода на печать формы сертификата на панели инструментов браузера нажмите на кнопку **Печать**.

Открыть статью на сайте

Экспорт сертификата

Программа «КриптоАРМ» позволяет экспортировать сертификат из хранилища в файл.

Экспорт сертификата может понадобиться для выполнения следующих задач:

- Архивирование сертификата;
- Архивирование сертификата и связанного с ним закрытого ключа;
- Копирование сертификата для использования на другом компьютере;
- Удаление сертификата и его закрытого ключа с компьютера владельца сертификата для установки на другом компьютере

Когда сертификат экспортируется, он копируется из хранилища сертификатов в файл, использующий стандартный формат хранения сертификатов.

Для экспорта сертификата, выполните следующие шаги:

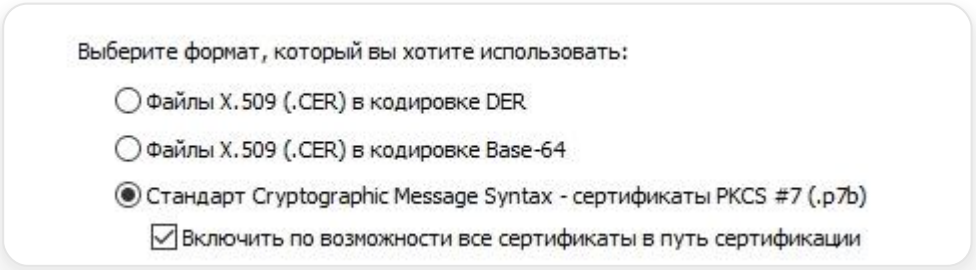
1. В дереве элементов главного окна выберите раздел **Сертификаты**. Откроется список хранилищ сертификатов. Выберите хранилище, в котором содержится сертификат для экспортирования.

2. В правой панели главного окна выделите с сертификат (или группу сертификатов), который необходимо экспортировать, в контекстном меню объекта или на панели задач выберите пункт **Экспорт**. Если экспортируемый сертификат – ГОСТ, введите пароль для доступа к ключевому контейнеру.

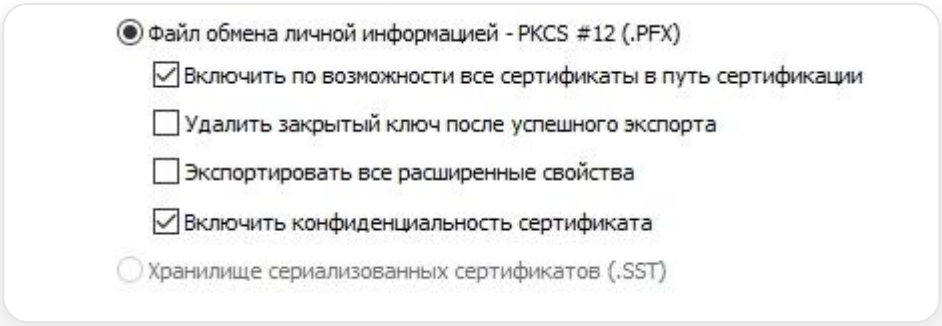
3. Откроется стандартный диалог **Мастер экспорта сертификатов**. Ознакомьтесь с порядком экспорта сертификатов и нажмите на кнопку **Далее**.

4. Вы можете экспортировать закрытый ключ вместе с сертификатом. Для этого поставьте переключатель напротив пункта **Да, экспортировать закрытый ключ**. В случае выбора пункта **Нет, не экспортировать закрытый ключ** будет произведена операция экспорта только сертификата (и его открытого ключа). Если при создании запроса на сертификат вы не пометили ключи как "экспортируемые", то вы сможете экспортировать сертификат (без закрытого ключа). В этом случае переключатель **Да, экспортировать закрытый ключ** будет заблокирован.

5. Если вы экспортируете только сертификат (без закрытого ключа), то в следующем окне выберите следующие форматы экспортируемого файла:
   - Файлы в DER-кодировке X.509 (.CER)
   - Файлы в Base64-кодировке X.509 (.CER)
   - Стандарт Cryptographic Message Syntax - сертификаты PKCS #7 (.p7b)



6. Если вы экспортируете сертификат с закрытым ключом, то вам будет доступен только один формат экспортируемого файла - файл обмена личной информацией - PKCS#12 (.PFX). При этом вы имеете возможность:
   - включить по возможности все сертификаты в путь сертификата;
   - включить усиленную защиту (требуется IE 5.0, NT 4.0 SP4 или выше);
   - удалить закрытый ключ после успешного экспорта.



7. Для обеспечения безопасности следует защитить закрытый ключ паролем.

8. Укажите имя экспортируемого файла и путь экспорта.

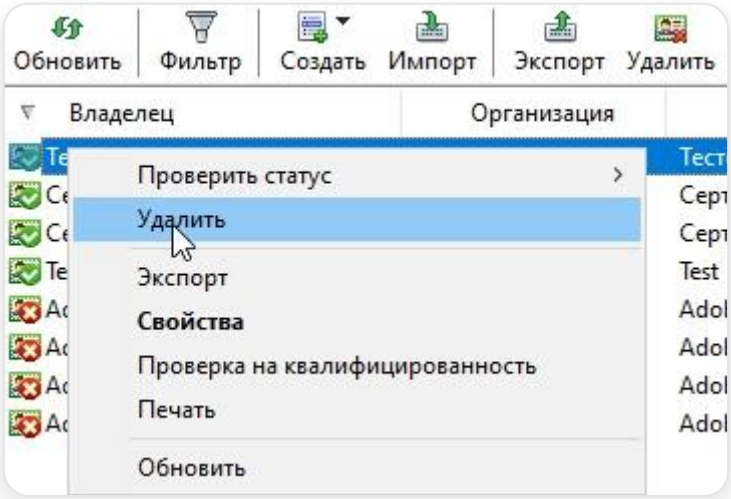
9. По окончании операции возникнет сообщение об успешном экспорте сертификата.

Открыть статью на сайте

Удаление сертификата

Чтобы удалить сертификат:

1. В дереве элементов главного окна выберите раздел **Сертификаты**. Откроется список хранилищ сертификатов.
2. Выберите хранилище, из которого необходимо удалить сертификат.
3. В правой панели главного окна выделите строку с сертификатом (или группу сертификатов), который необходимо удалить, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить**.
4. Подтвердите решение удалить сертификат.
5. Сертификат будет успешно удален из хранилища



Открыть статью на сайте

Как создать запрос на получение сертификата

С помощью программы «КриптоАРМ» вы можете создавать запросы следующих типов:

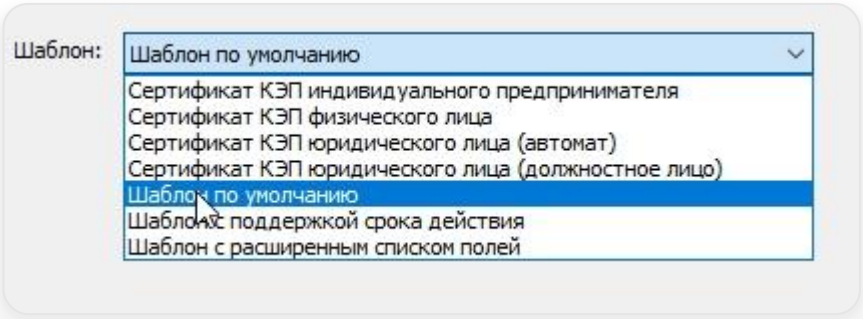
- запрос на получение сертификата
- запрос на отзыв сертификата

Запрос на получение сертификата

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

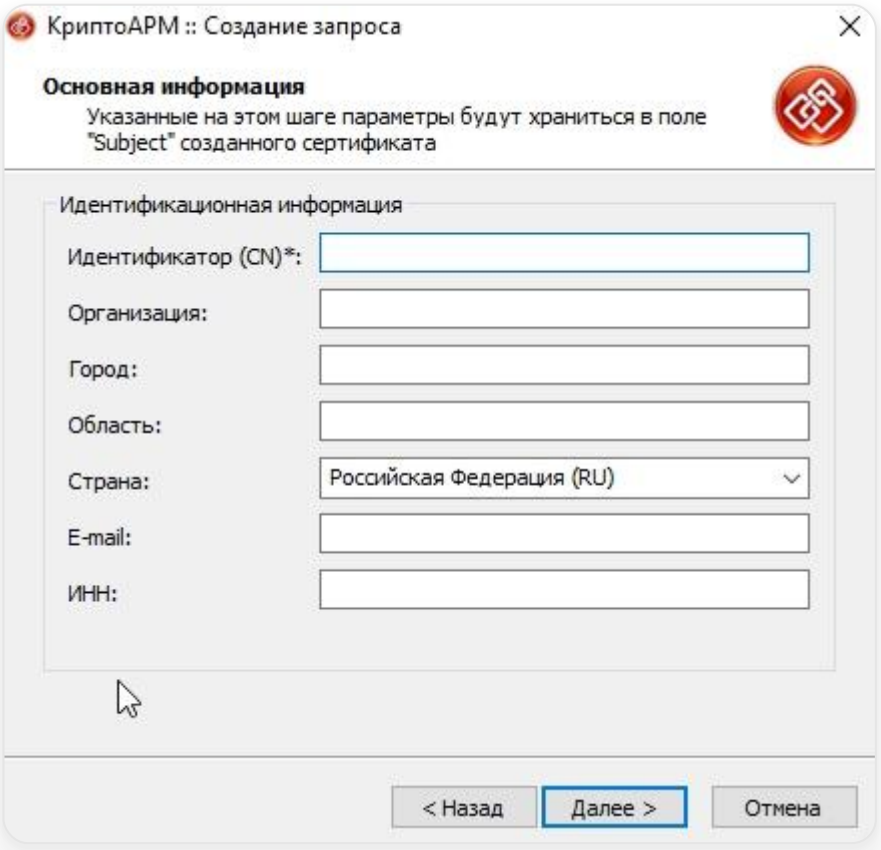
Для создания запроса на получение сертификата в УЦ:

1. В дереве элементов главного окна выберите раздел **Запросы**. Вызовите правой клавишей мыши контекстное меню и выберите пункт **Создать > Запрос на сертификат**.
2. Откроется стандартный Мастер создания запроса. Ознакомьтесь с порядком и требованиями создания запроса на получение сертификата.
3. На следующем шаге из выпадающего списка выберите шаблон сертификата:



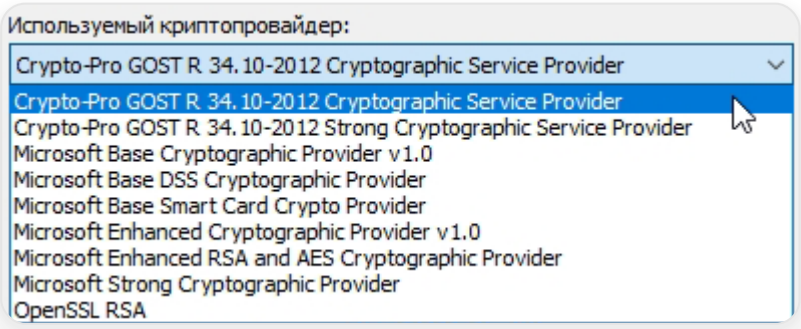
- шаблон по умолчанию
  При создании запроса на сертификат по «шаблону по умолчанию» необходимо ввести базовую информацию о владельце: **Идентификатор, Организация, Город, Область, Страна, E-Mail и ИНН;**
- шаблон с расширенным списком полей
  При создании запроса на сертификат по «шаблону с расширенным списком полей» дополнительно к базовой информации добавляется следующая: **Должность, Подразделение, Регион, Населенный пункт, Адрес**

4. Откроется окно **Основная информация**, в котором, согласно выбранному на предыдущем шаге шаблону, необходимо указать идентификационную информацию о владельце будущего сертификата:



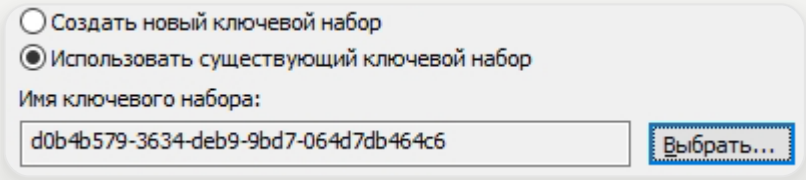
	Поля отмеченные знаком «*» являются обязательными для заполнения.
	Обратите внимание, если вы указываете ИНН юридического лица, номер всегда должен начинаться с «00», например 007707049388.
	СНИЛС указывается без пробелов и знаков «-», например, 07306654534.

5. В окне **Параметры ключа** укажите следующие настройки:
   - Криптопровайдер, который будет использован при создании сертификата.

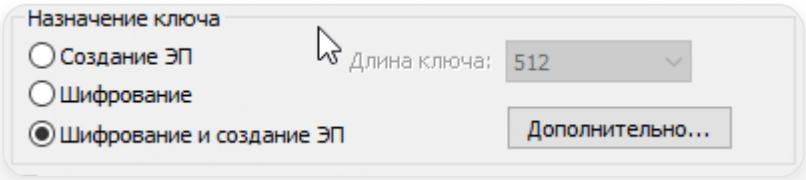


- Вариант создания ключевого набора.

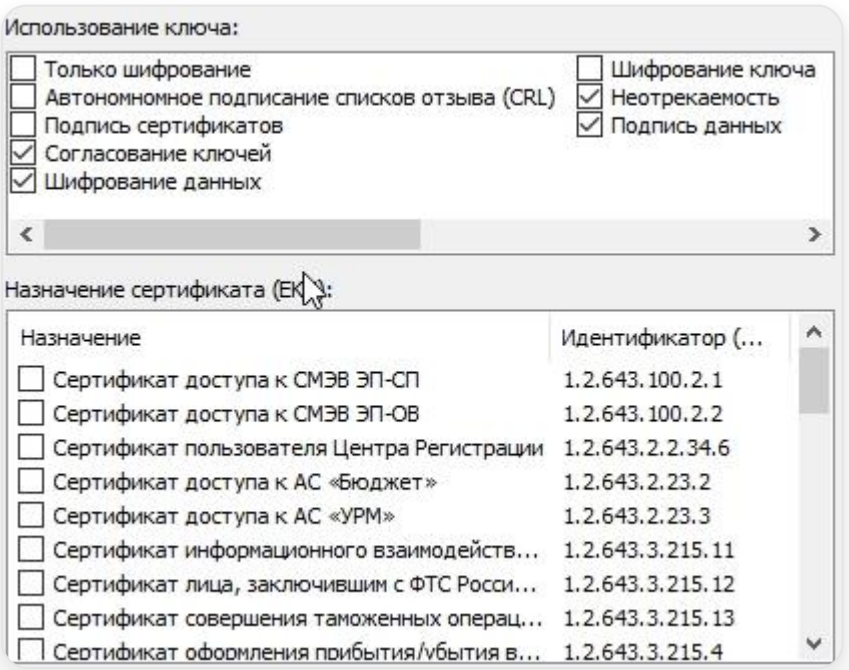
  - Создать ключевой набор сертификат будет создан на основе нового ключевого набора.
  - Использовать существующий ключевой набор – выберите ключевой набор, который будет использован при создании сертификата, из списка существующих (кнопка Выбрать).



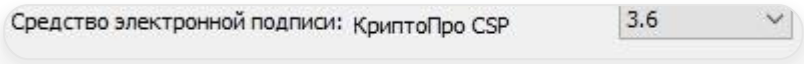
- Установите переключатель напротив необходимого **Назначения ключа** сертификата.



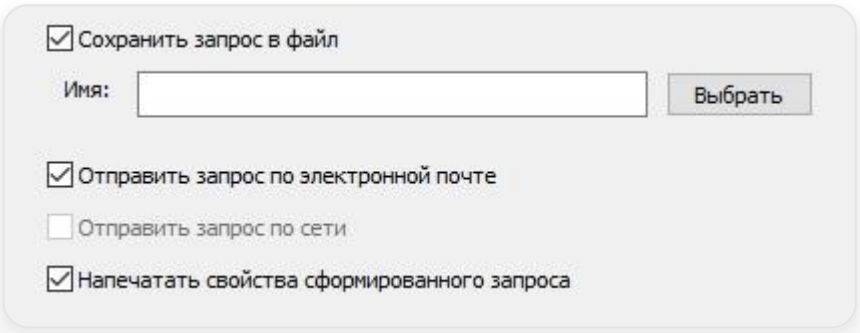
- Вы также можете выбрать дополнительное назначение ключа, нажав на кнопку **Дополнительно**. В списке назначений использования ключа и назначений сертификата (EKU) выберите необходимое:



- Укажите необходимую **Длину ключа**. Чем длиннее ключ, тем он надежнее.
- **Пометить ключи как экспортируемые.** Если вы отметите этот флаг, то сможете проводить экспорт сертификата вместе с закрытыми ключами
- Если для создания запроса был выбран шаблон квалифицированной электронной подписи, то необходимо будет указать в зависимости от выбранного криптопровайдера версию средства электронной подписи владельца.



6. Укажите, каким образом вы хотите отправить запрос на обработку:



- на отчуждаемом ключевом носителе, предварительно сохранив запрос в файл;
- по электронной почте:
  Для этого на следующем шаге укажите тему письма, e-mail и комментарии к письму.

	**Outlook** Если для отправки электронных писем вы используете программу Outlook, то сначала вам будет предложено подтвердить отправку письма. При этом отправка письма не выполняется, если программа не запущена, а будет выполнена только после запуска Outlook.

	**The Bat!** В отличие от Outlook, программа сначала запускается, а потом просит подтвердить отправку письма

- в онлайн-режиме (через веб-службу ЦС)
  Укажите адрес веб-службы УЦ (IP-адрес или URL-адрес) и сертификат корневого Удостоверяющего центра.

4. На основе указанных данных будет сформирован запрос на сертификат открытого ключа. После завершения операции возникнет окно с информацией о ее результатах.
5. Для ГОСТ сертификата выберите ключевой носитель, куда должен быть сохранен сформированный запрос (Реестр, дискета, USB брелок).
6. На запрос системы установите пароль на данный носитель и подтвердите его.

Открыть статью на сайте

Просмотр информации о запросах, фильтрация и сортировка запросов в списке

Просмотр информации о запросе

Вы можете просматривать следующую информацию о созданных вами запросах:

- Данные о самом запросе (дата создания запроса, данные по планируемой операции - созданию, отзыву, а также комментарий)
- Данные о сертификатах
  - о сертификате, над которым выполняется операция;
  - о сертификате подписчика запроса.

  Чтобы просмотреть информацию о запросе в УЦ:

  1. В разделе **Запросы на сертификат** выберите папку с тем типом запроса, который необходимо просмотреть. В контекстном меню выберите пункт **Свойства**.
  2. В открывшемся окне вы сможете просмотреть подробную информацию
     - о запросе, переданном в УЦ;
     - о сертификате, относительно которого был сформирован запрос;
     - о сертификате подписчика запроса.

Вы также можете просматривать информацию о запросах в финальном окне всех криптографических операций.

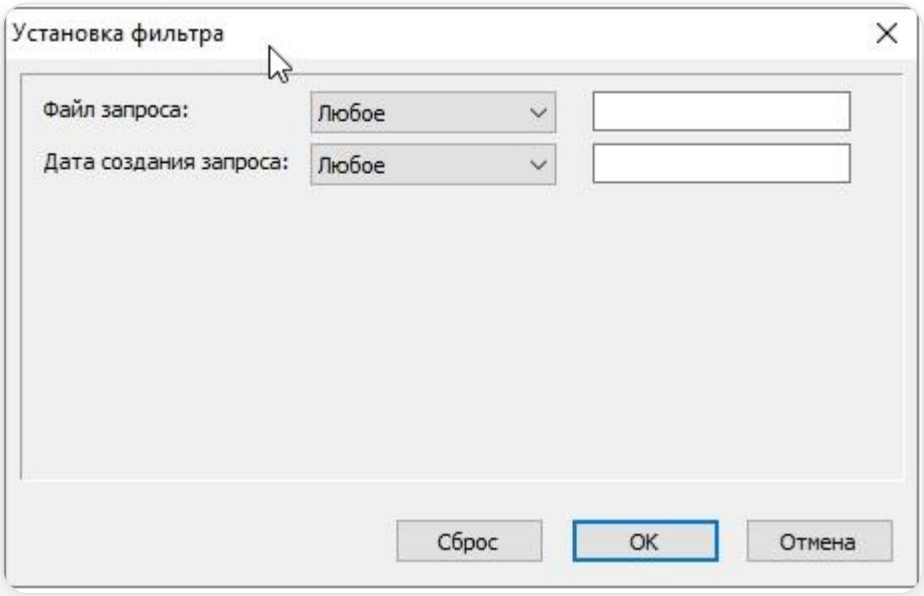
Фильтрация запросов

Вы можете фильтровать запросы в списке по следующим параметрам:

- файл запроса (название)
- дата создания запроса

Чтобы отфильтровать запросы в списке:

1. В разделе **Запросы на сертификат** выберите папку с тем типом запросов, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**.
2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать запросы:

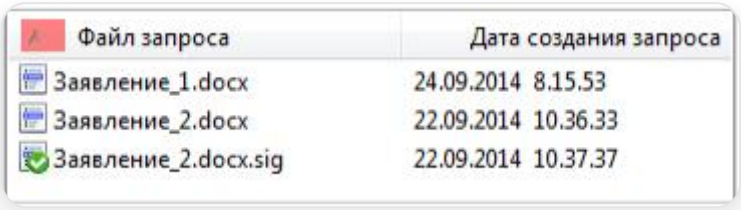


3. Список запросов будет отфильтрован по указанным вами параметрам.
4. Вернуться к исходному списку запросов вы можете, сбросив фильтр.

Сортировка запросов в списке

В программе «КриптоАРМ» реализована возможность сортировать запросы в удостоверяющей центр в списке. Сортировка может выполняться по следующим параметрам:

- файл запроса
- дата создания запроса



Печать запроса

Для печати запроса выполните следующие действия:

1. В разделе **Запросы на сертификат** выберите папку с тем типом запросов, которые необходимо отфильтровать. В контекстном меню выберите пункт, в контекстном меню объекта или на панели задач выберите пункт **Печать**.
2. Откроется документ в формате MS Word и предложено преобразовать в формат *.pdf.

Удаление запроса

Для удаления запроса на сертификат:

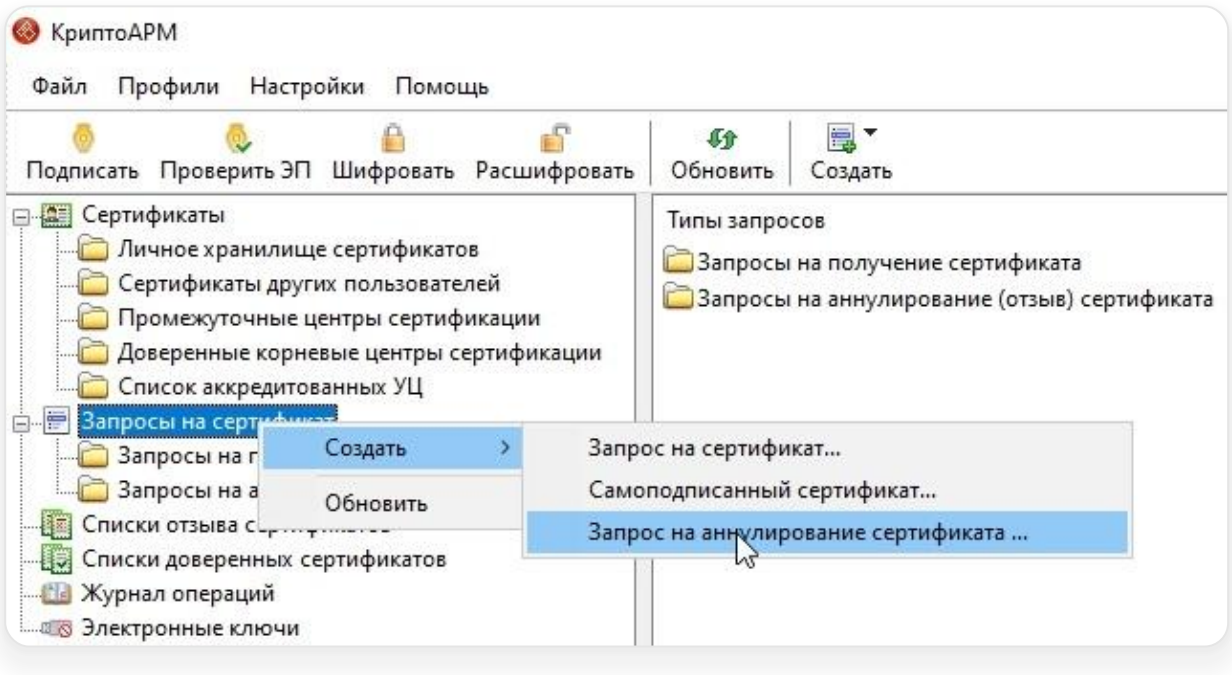
1. В дереве элементов главного окна выберите раздел **Запросы на сертификат > Запросы на получение сертификата/аннулирование (отзыв) сертификата**. В правой панели главного окна выделите строку с запросом на сертификат (или группу запросов на сертификат), который необходимо удалить, в контекстное меню объекта или на панели инструментов выберите пункт **Удалить**.
2. Подтвердите решение удалить запрос на сертификат.
3. Запрос будет удален из хранилища.

Открыть статью на сайте

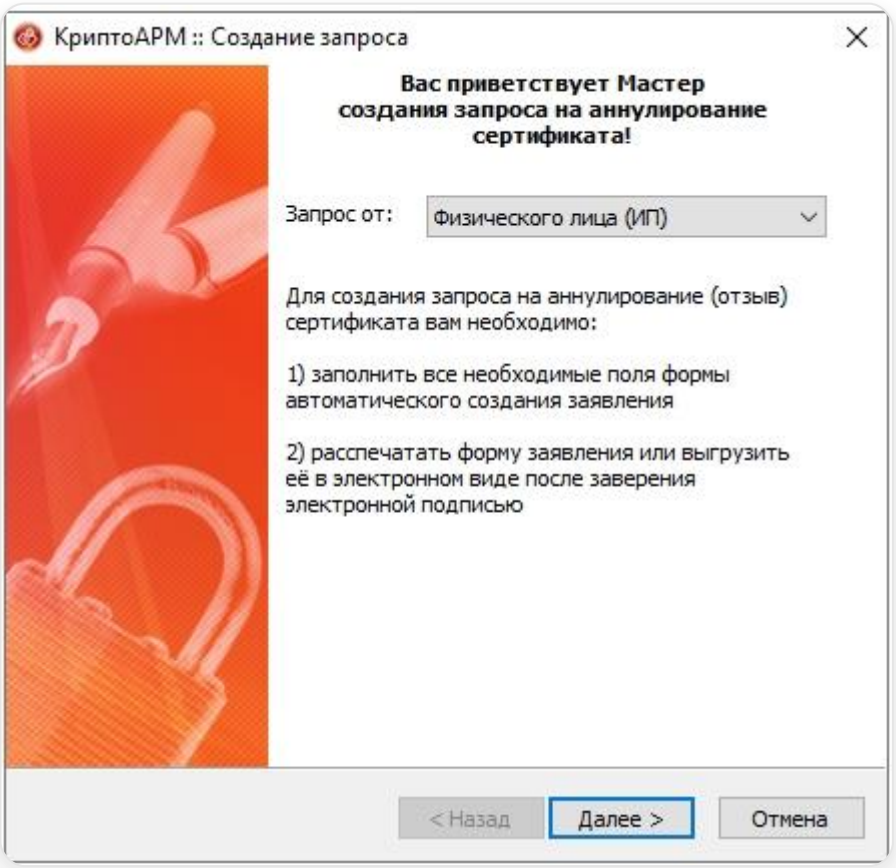
Как создать запрос на аннулирование сертификата

Создать запрос подобного типа вы можете двумя способами:

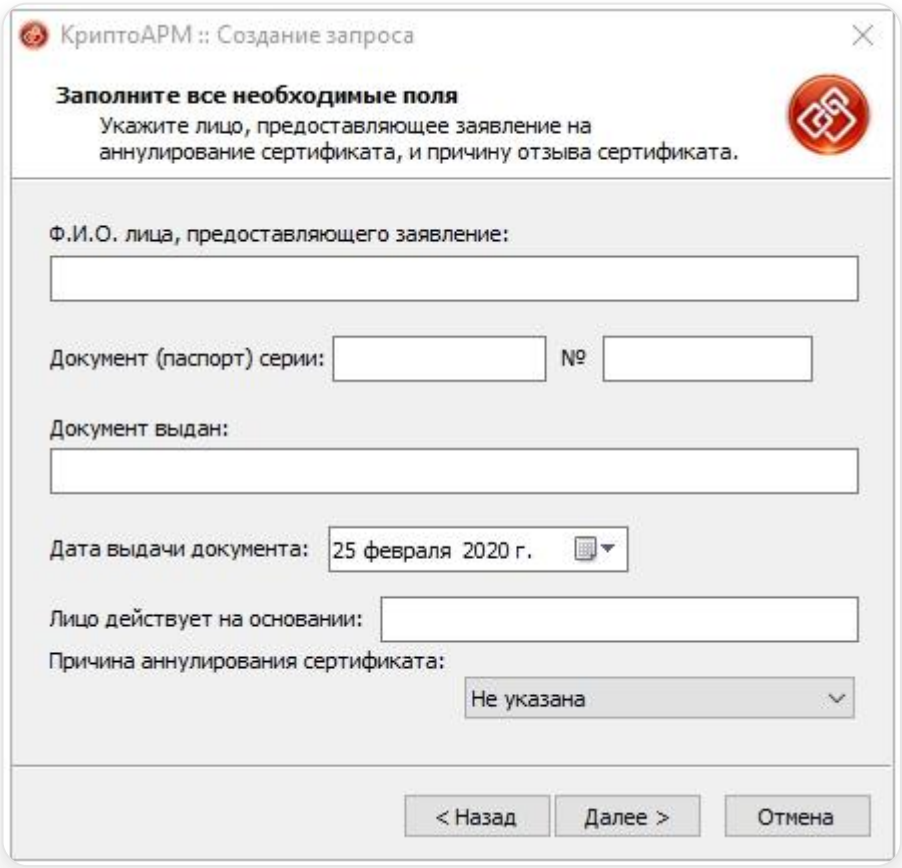
- В разделе **Сертификаты**, в контекстном меню сертификата пункт **Создать > Запрос на аннулирование сертификата**;
- В разделе **Запросы на сертификат**, в контекстном меню раздела пункт **Создать > Запрос на аннулирование сертификата**:



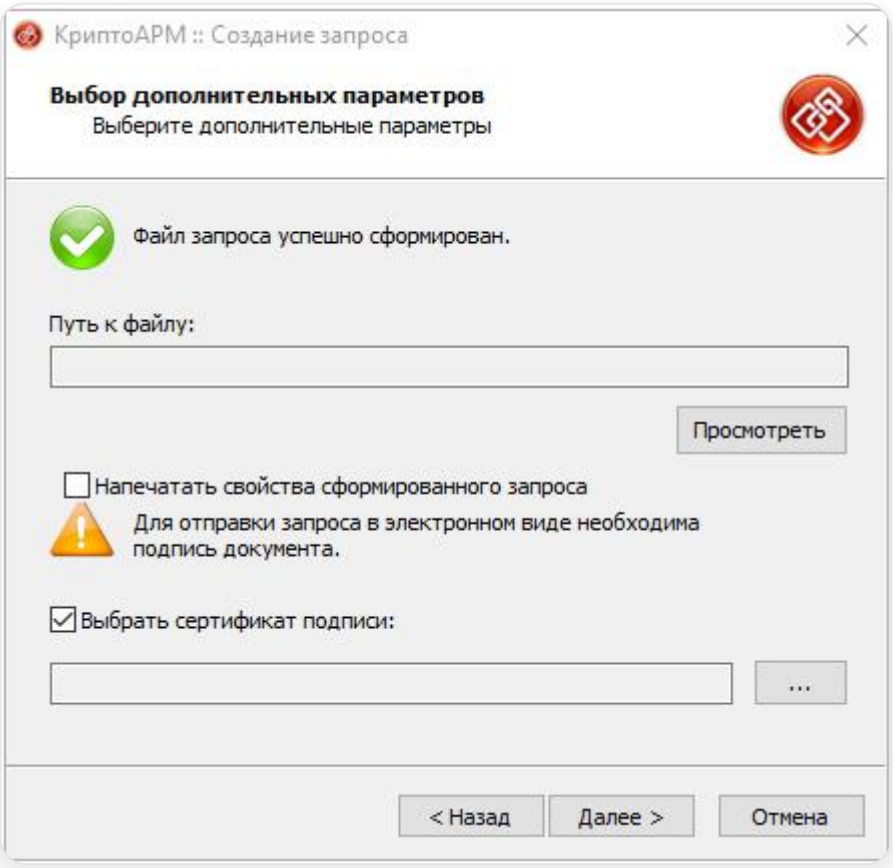
1. Откроется мастер создания запроса. Ознакомьтесь с порядком формирования запроса. На первом шаге вам потребуется указать, от кого выполняется запрос на отзыв: от физического лица (ИП) или юридического лица.



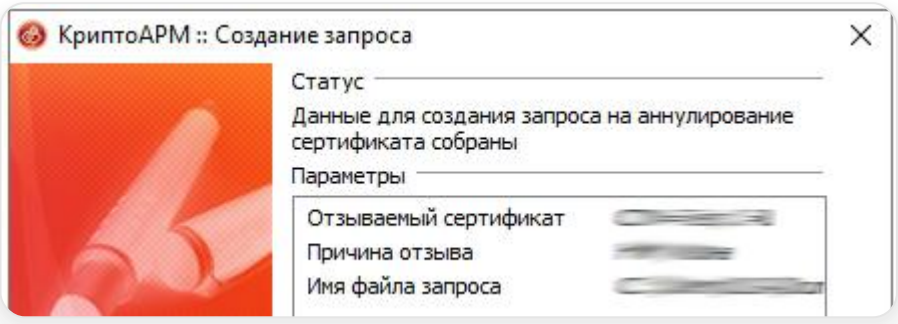
2. Выберите личный сертификат, который необходимо отозвать.
3. На следующем шаге заполните информацию о лице, предоставляющем заявление на аннулирование сертификата, и причину отзыва сертификата (ее можно выбрать из списка):



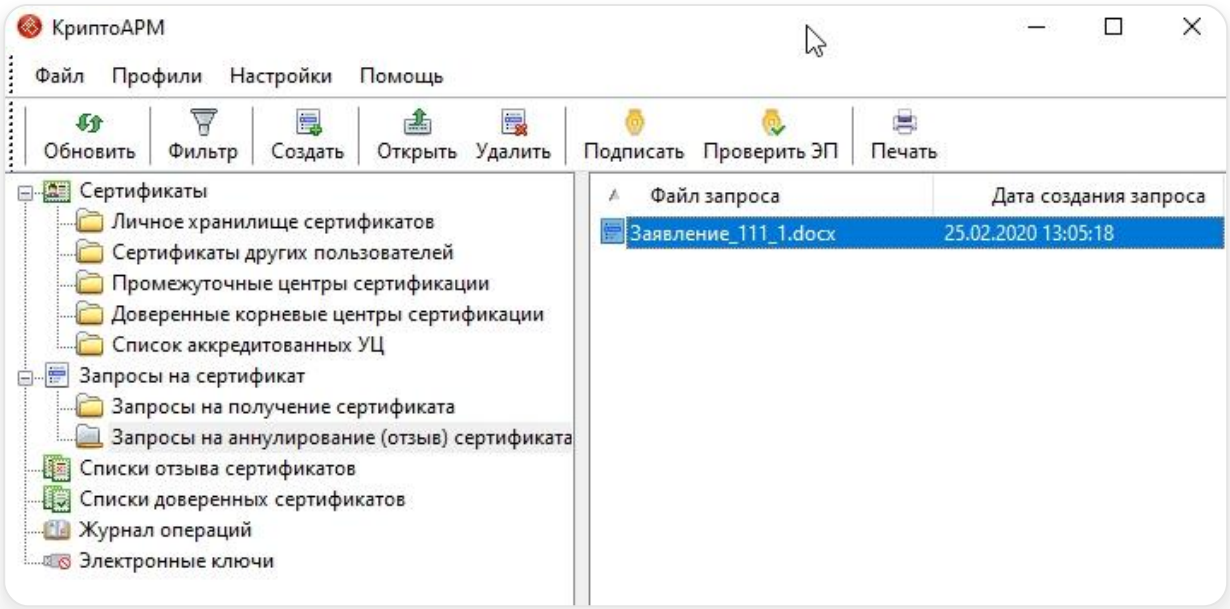
4. Укажите дополнительные параметры запроса: путь для сохранения файла и сертификат подписи, которым будет подписан запрос:



5. На основе указанных данных будет сформирован запрос на отзыв сертификата. После завершения операции возникнет окно с информацией о ее результатах:



6. Сформированный запрос и отделенная электронная подпись к файлу запроса отобразятся в разделе **Запросы на аннулирование (отзыв) сертификата**:


КриптоАРМ
Файл
Профили
Настройки
Помощь
Обновить
Фильтр
Создать
Открыть
Удалить
Подписать
Проверить ЭП
Печать
Сертификаты
Личное хранилище сертификатов
Сертификаты других пользователей
Промежуточные центры сертификации
Доверенные корневые центры сертификации
Список аккредитованных УЦ
Запросы на сертификат
Запросы на получение сертификата
Запросы на аннулирование (отзыв) сертификата
Списки отзыва сертификатов
Списки доверенных сертификатов
Журнал операций
Электронные ключи
Файл запроса
Дата создания запроса
Заявление_111_1.docx
25.02.2020 13:05:18

Открыть статью на сайте

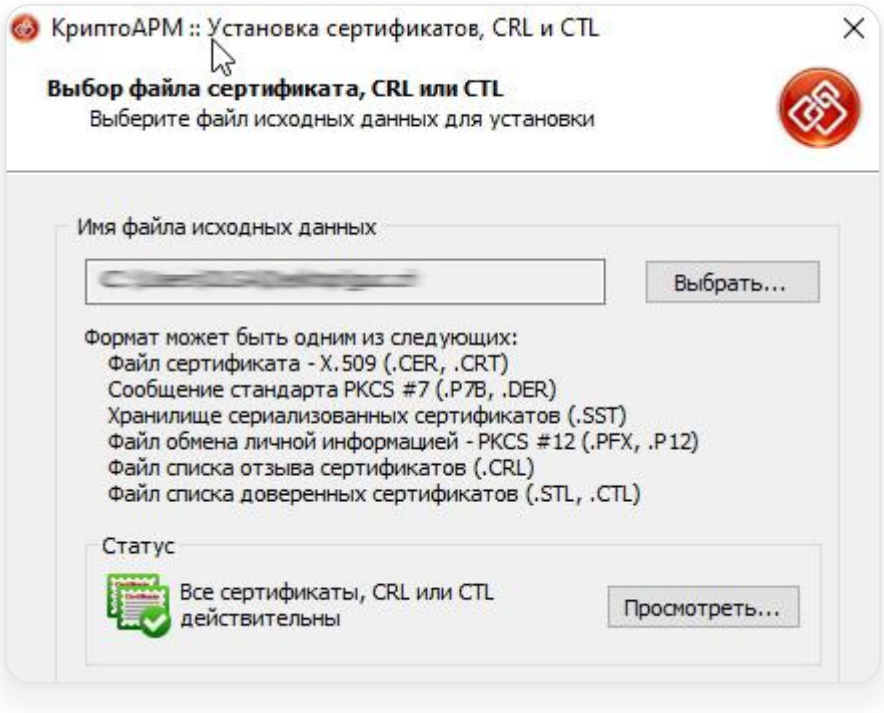
Установка списка отзывов в хранилище

Список отозванных сертификатов можно найти на сайте удостоверяющего центра, выпустившего сертификат, а также есть возможность скачать его по ссылке из состава сертификата. Для этого понадобится открыть сертификат в личном хранилище КриптоАРМ нажатием левой клавиши мыши. Далее кнопка **Просмотреть**, вкладка **Состав**. Здесь понадобится найти строчку **Точки распространения списков отзыва** и скопировать любую из представленных в нижнем окне ссылок клавишами **Ctrl+C**, вставить в адресную строку браузера клавишами **Ctrl+V и** нажать **Enter**.

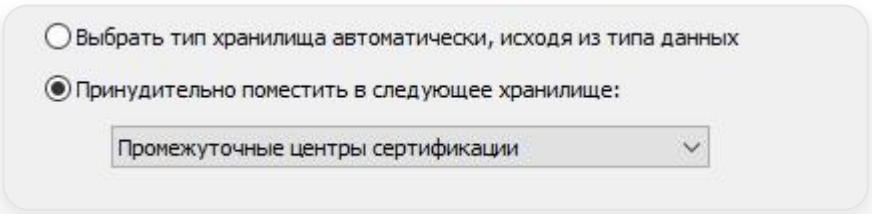
Для установки списка в хранилище СОС, необходимо выполнить операцию импорта списка.

Для того чтобы импортировать список отзыва, выполните следующие шаги:

1. В дереве элементов главного окна выберите раздел **Списки отзыва сертификатов**.
2. В контекстное меню объекта (пункт **Редактировать** или контекстное меню на самом разделе) или на панели инструментов выберите пункт **Импорт**.
3. Откроется стандартный диалог Мастер установки сертификата и СОС.
4. Выберите импортируемый файл СОС в формате .crl:



5. Укажите хранилище, куда будет импортирован список отзыва сертификатов.
   Списки отзыва сертификатов всегда необходимо устанавливать в системное хранилище **Промежуточные центры сертификации**, так как система PKI работает только с СОС из хранилища Промежуточных ЦС.



6. После завершения операции возникнет сообщение об успешном импорте СОС.

Открыть статью на сайте

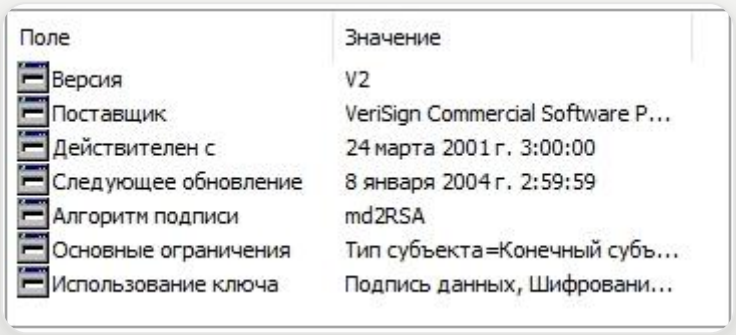
Просмотр информации о списках

В правой панели главного окна доступна базовая информация о списках отзыва:

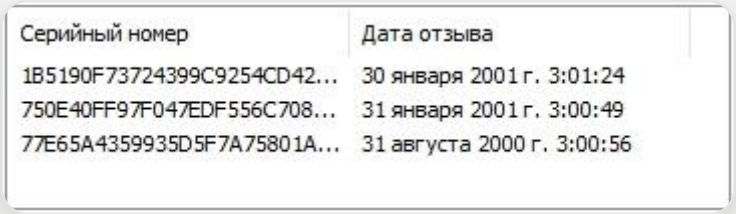
- Имя субъекта, выпустившего СОС (издатель);
- Срок истечения действия СОС (действителен с / действителен по).

Для просмотра детальной информации о Списке отзыва сертификатов, выполните следующие шаги:

1. Выберите необходимый СОС из списка, в контекстном меню объекта или на панели задач выберите пункт **Свойства**.
2. Откроется форма с информацией о Списке отзыва сертификатов (СОС):
   - В закладке **Общие** содержится общая информация о просматриваемом списке отзыва:



   - В закладке **Список отзыва** дается подробная информация о каждом сертификате, входящем в просматриваемый список



Открыть статью на сайте

Фильтрация и сортировка списков отзыва

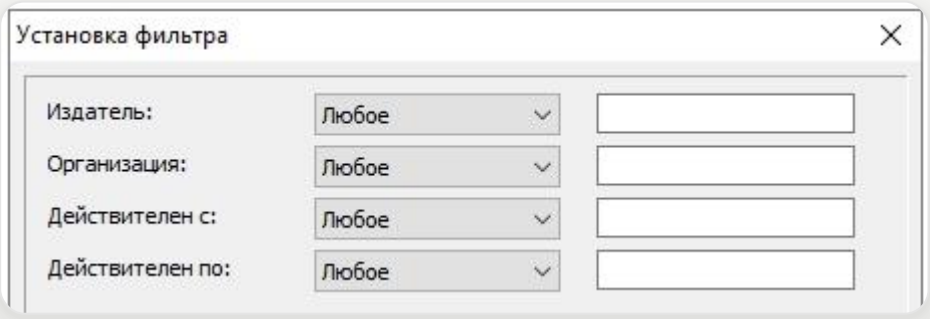
Фильтрация списков отзыва

Вы можете фильтровать СОС в списке по следующим параметрам:

- Издатель;
- Организация;
- Дата, с которой СОС действителен;
- Дата, по которую СОС действителен.

Чтобы отфильтровать списки отзыва сертификатов:

1. В разделе **Списки отзыва сертификатов** выберите папку с тем типом списков, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**.
2. В окне Установка фильтра установите параметры, по которым необходимо отобрать СОС:



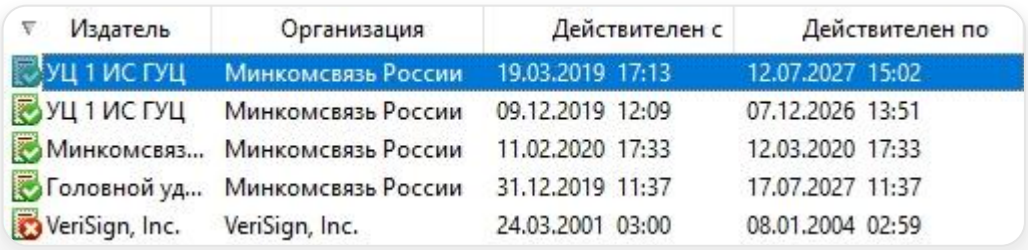
3. Список СОС будет отфильтрован по указанным вами параметрам.
4. Вернуться к исходному списку вы можете, сбросив фильтр.

Сортировка списков отзыва

В программе «КриптоАРМ» реализована возможность сортировать списки отзыва сертификатов.

Сортировка может выполняться по следующим параметрам:

- имя издателя списка отзыва;
- дата, с которой действителен список;
- дата, по которую действителен список;



Издатель	Организация	Действителен с	Действителен по
УЦ 1 ИС ГУЦ	Минкомсвязь России	19.03.2019 17:13	12.07.2027 15:02
УЦ 1 ИС ГУЦ	Минкомсвязь России	09.12.2019 12:09	07.12.2026 13:51
Минкомсвяз...	Минкомсвязь России	11.02.2020 17:33	12.03.2020 17:33
Головной уд...	Минкомсвязь России	31.12.2019 11:37	17.07.2027 11:37
VeriSign, Inc.	VeriSign, Inc.	24.03.2001 03:00	08.01.2004 02:59

Открыть статью на сайте

Экспорт и удаление списков отзыва

Экспорт списков отзыва

Программа позволяет экспортировать списки отзыва сертификатов (COC) в хранилище.

Чтобы экспортировать список отзыва:

1. В дереве элементов главного окна выберите раздел **Списки отзыва сертификатов**.
2. В правой панели главного окна выделите COC (или группу COC), который необходимо экспортировать, в контекстном меню объекта или на панели задач выберите пункт **Экспорт**.
3. Откроется стандартный диалог Мастер экспорта сертификатов, позволяющий выбрать экспортируемый файл COC.
4. Введите имя файла **Списка отзыва сертификата**.
5. В заключение возникнет сообщение об успешном экспорте COC.

Удаление списков отзыва

Система позволяет удалять списки отзыва сертификатов (COC) из хранилища.

Чтобы удалить список отзыва:

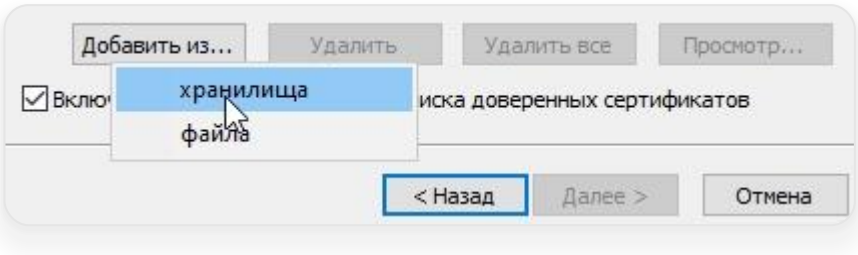
1. В дереве элементов главного окна выберите раздел **Списки отзыва сертификатов**.
2. В правой панели главного окна выделите строку со списком отзыва сертификатов (или группу COC), который необходимо удалить, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить**.
3. Подтвердите решение удалить список отзыва.
4. В случае подтверждения список отзыва сертификатов будет удален из хранилища.

Открыть статью на сайте

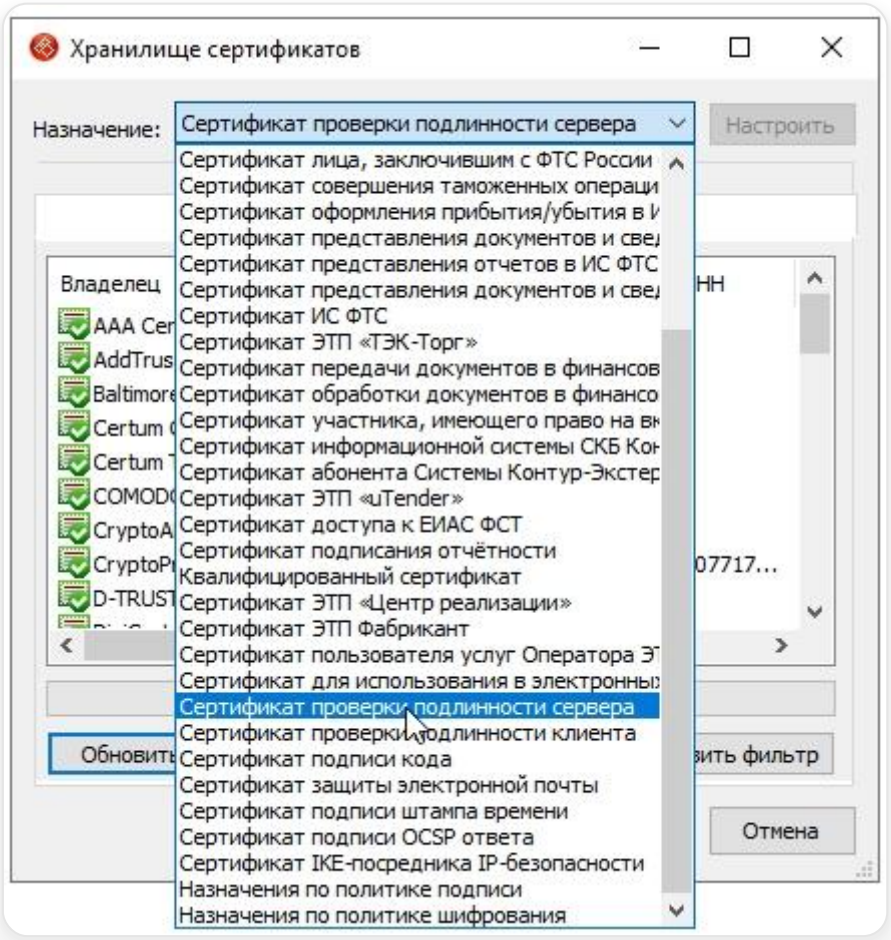
Как создать список доверенных сертификатов?

Чтобы создать список доверенных сертификатов:

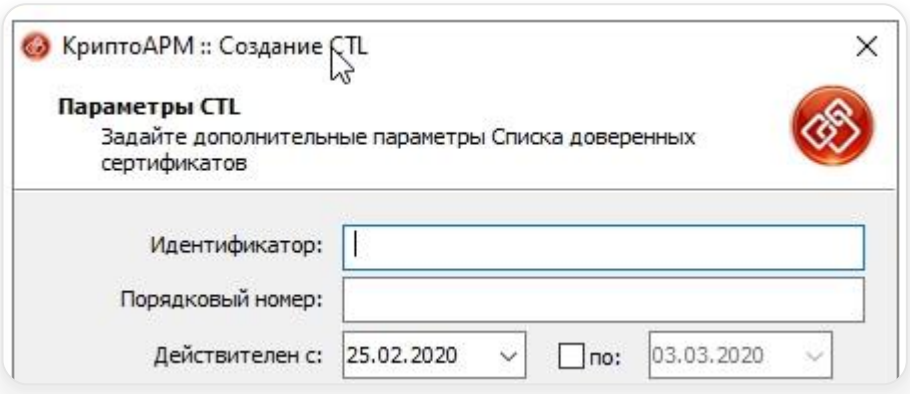
- В дереве элементов главного окна выберите раздел **Списки доверенных сертификатов**.
- В контекстное меню объекта (пункт **Редактировать** или контекстное меню на самом разделе) или на панели инструментов выберите пункт **Создать**.
- Откроется Мастер создания списка доверенных сертификатов (СДС). Ознакомьтесь с порядком и требованиями для создания списка.
- Из хранилища или файла выберите сертификаты УЦ, к которым должно осуществляться доверие:



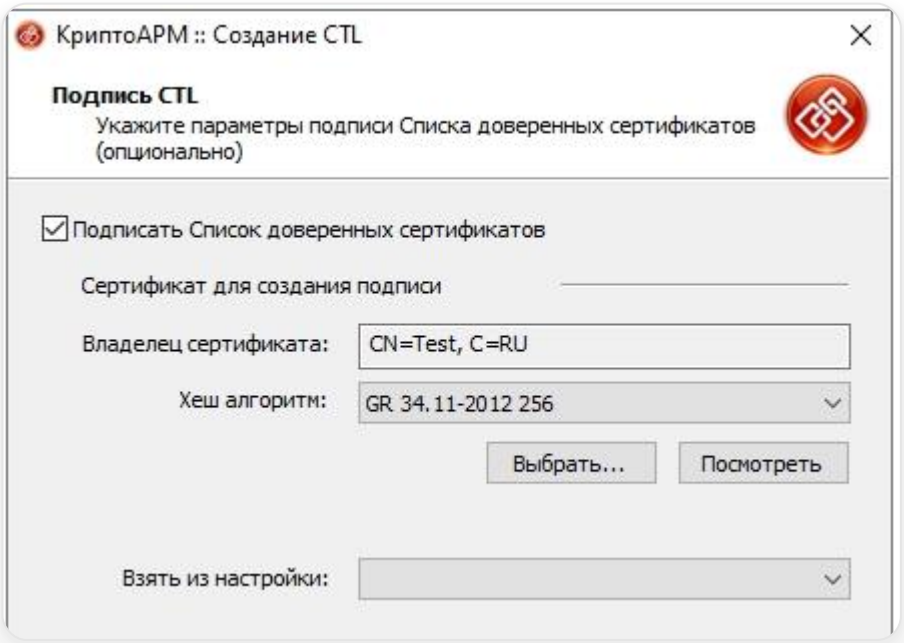
Для упрощения поиска сертификатов «КриптоАРМ» позволяет фильтровать сертификаты в списке по их назначению.



- Далее заполните дополнительные параметры списка доверенных сертификатов: идентификатор, порядковый номер, время действия списка доверия и область использования сертификатов в списке (идентификатор и описание).



- При необходимости вы можете подписать создаваемый список доверенных сертификатов электронной подписью. Для этого поставьте флаг напротив строки **Подписать Список доверенных сертификатов**. При этом станет доступен раздел, где вы сможете указать параметры подписи Списка доверенных сертификатов или взять параметры из готовой настройки подписи.



- После сбора данных нажмите **Готово** для завершения мастера создания СДС.

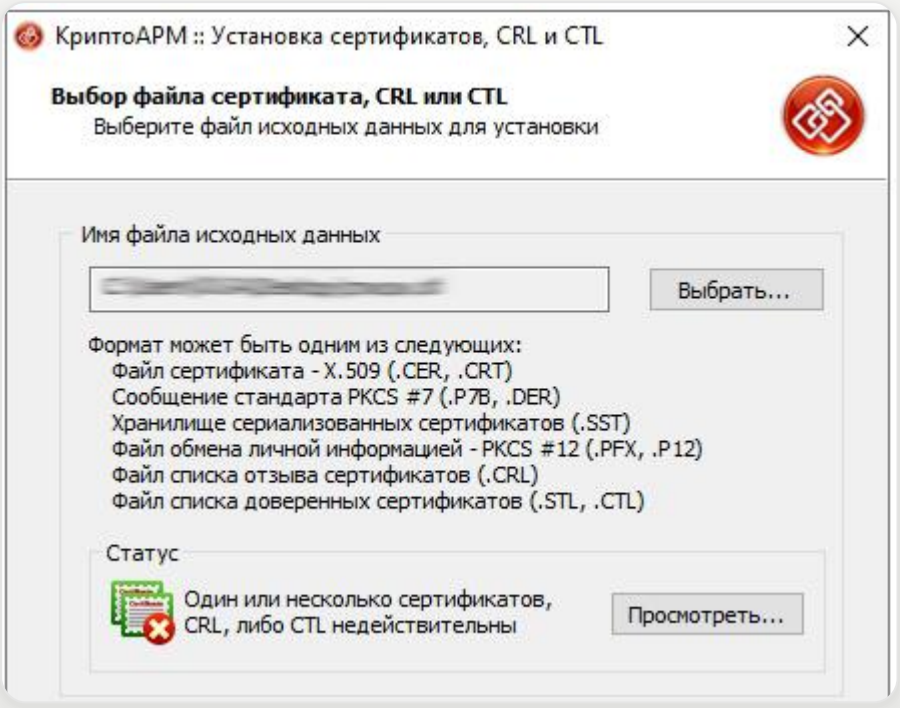
Открыть статью на сайте

Установка списка в хранилище

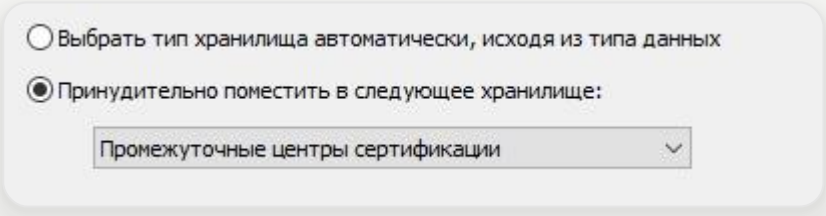
Для установки списка в хранилище, необходимо выполнить операцию импорта списка.

Чтобы импортировать список:

1. В дереве элементов главного окна выберите раздел Списки доверенных сертификатов.
2. В контекстном меню объекта (пункт Редактировать или контекстное меню на самом разделе) или на панели инструментов выберите пункт Импорт.
3. Откроется стандартный диалог Мастер установки сертификата и СОС.
4. Выберите импортируемый файл СДС (в формате. stl):



5. Укажите хранилище, куда будет импортирован список доверенных сертификатов.



Списки доверенных сертификатов всегда необходимо устанавливать в системное хранилище **Промежуточные центры сертификации.**

6. После завершения операции возникнет сообщение об успешном импорте СДС.

Открыть статью на сайте

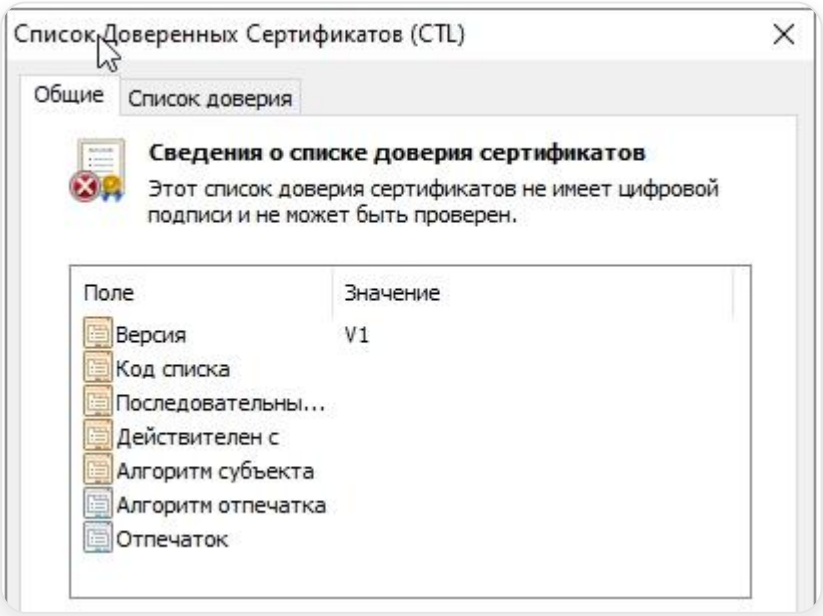
Просмотр информации о списке

В правой панели главного окна доступна базовая информация о списках доверенных сертификатов:

- Идентификатор;
- Срок действия СДС (действителен с / действителен по);
- Области применения;
- Сертификат подписи.

Для просмотра подробной информации о **Списке доверенных сертификатов**, выполните следующие шаги:

1. Выберите необходимый СДС из списка, в контекстном меню объекта или на панели задач выберите пункт **Свойства**:
2. Откроется форма с информацией о **Списке доверенных сертификатов**:
   - В закладке **Общие** содержится общая информация о просматриваемом списке:



   - В закладке **Список доверия** дается подробная информация о каждом сертификате, входящем в просматриваемый список.

Открыть статью на сайте

Фильтрация и сортировка списка

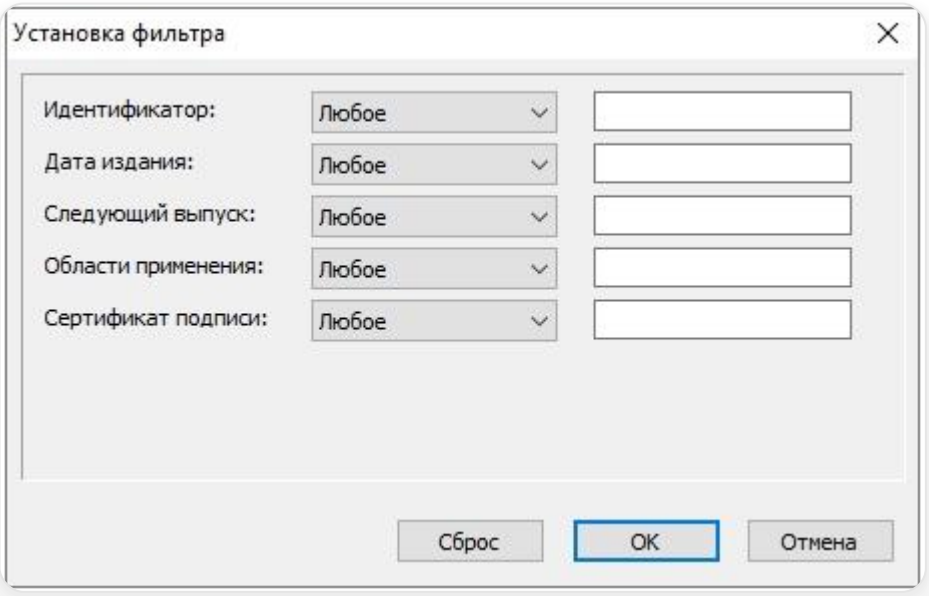
Фильтрация списка

Вы можете фильтровать списки доверенных сертификатов (СДС) по следующим параметрам:

- издатель;
- дата, с которой СДС действителен;
- дата, по которую СДС действителен;
- идентификатор использования;
- область применения;
- сертификат подписи.

Чтобы отфильтровать списки доверенных сертификатов:

1. В разделе **Списки доверенных сертификатов** выберите папку с тем типом списков, которые необходимо отфильтровать. В контекстном меню выберите пункт **Фильтр**
2. В окне **Установка фильтра** установите параметры, по которым необходимо отобрать СДС:



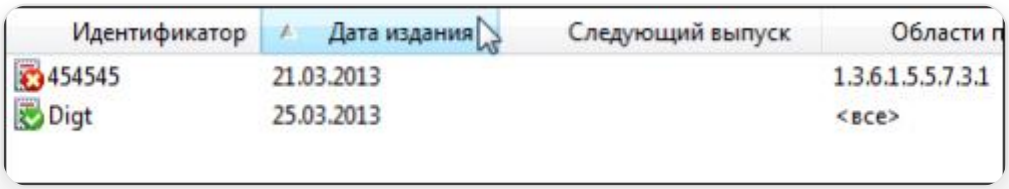
3. Список СДС будет отфильтрован по указанным вами параметрам.
4. Вернуться к исходному списку вы можете, сбросив фильтр.

Сортировка списков

В программе «КриптоАРМ» реализована возможность сортировать списки доверенных сертификатов в общем списке.

Сортировка может выполняться по следующим параметрам:

- Идентификатор (имя издателя списка отзыва);
- Дата издания (дата, с которой действителен список);
- Следующий выпуск (дата, по которую действителен список);
- Области применения (идентификатор использования);
- Сертификат подписи.



Открыть статью на сайте

Экспорт и удаление списка

Экспорт списков

Программа позволяет экспортировать списки доверенных сертификатов (СДС) в хранилище.

Чтобы экспортировать список доверенных сертификатов:

1. В дереве элементов главного окна выберите раздел **Списки доверенных сертификатов**.
2. В правой панели главного окна выделите список (или группу списков), который необходимо экспортировать, в контекстном меню объекта или на панели задач выберите пункт **Экспорт**.
3. Откроется стандартный диалог Мастер экспорта сертификатов, позволяющий выбрать экспортируемый файл СДС.
4. Введите имя файла Списка доверенных сертификатов.
5. В заключение возникнет сообщение об успешном экспорте списка.

Удаление списка

Система позволяет удалять списки доверенных сертификатов (СДС) из хранилища.

Чтобы удалить список:

1. В дереве элементов главного окна выберите раздел Списки доверенных сертификатов.
2. В правой панели главного окна выделите строку со списком доверенных сертификатов (или группу списков), который необходимо удалить, в контекстном меню объекта или на панели инструментов выберите пункт Удалить.
3. Подтвердите решение удалить список.
4. В случае подтверждения список доверенных сертификатов будет удален из хранилища.

Открыть статью на сайте

Операции с криптопровайдерами

Криптопровайдер (CSP, Cryptographic Service Provider) — независимый программный модуль, интегрированный в Windows и содержащий библиотеку криптографических функций со стандартизованным интерфейсом.

Криптопровайдер выполняет следующие криптографические функции:

- формирование/проверка электронной подписи (ЭП),
- шифрование информации,
- хранение ключей всех типов.

Криптопровайдер предназначен для авторизации, обеспечения конфиденциальности и юридической значимости электронных документов при обмене ими между пользователями, контроля целостности информации и др.

Доступны следующие операции с криптопровайдерами:

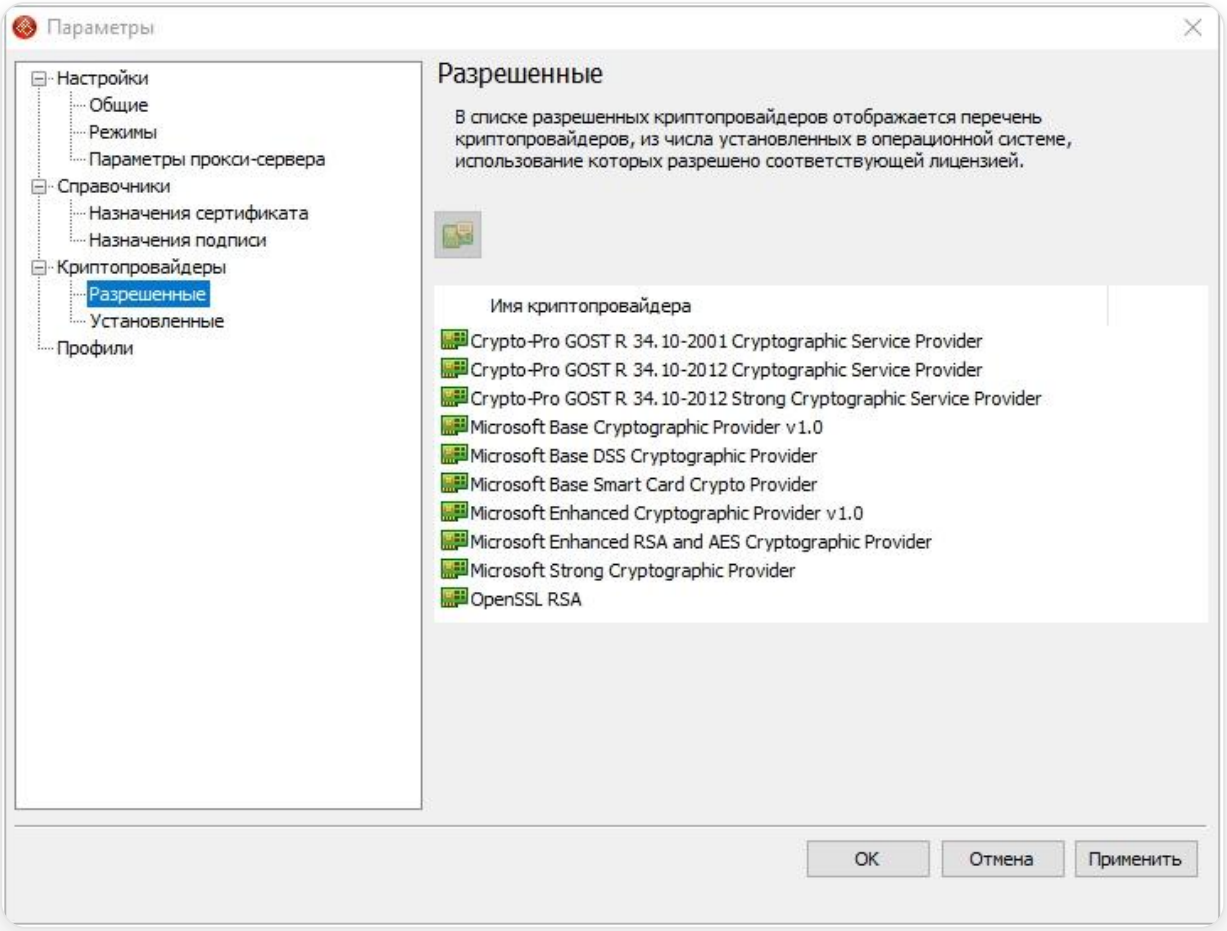
- Просмотр свойств криптопровайдера
- Фильтрация криптопровайдеров

Эти операции можно выполнять через верхнее меню главного окна **Настройки >Управление настройками > Криптопровайдеры**.

Просмотр свойств криптопровайдера

Чтобы просмотреть свойства криптопровайдера:

1. На верхней панели главного окна откройте пункт меню **Настройки > Управление настройками > Криптопровайдеры**. В правой панели главного окна отобразится полный перечень криптопровайдеров, установленных в операционной системе. Для просмотра свойства криптопровайдера выберите необходимый криптопровайдер из списка и в контекстном меню объекта или на панели инструментов выберите пункт **Свойства**.

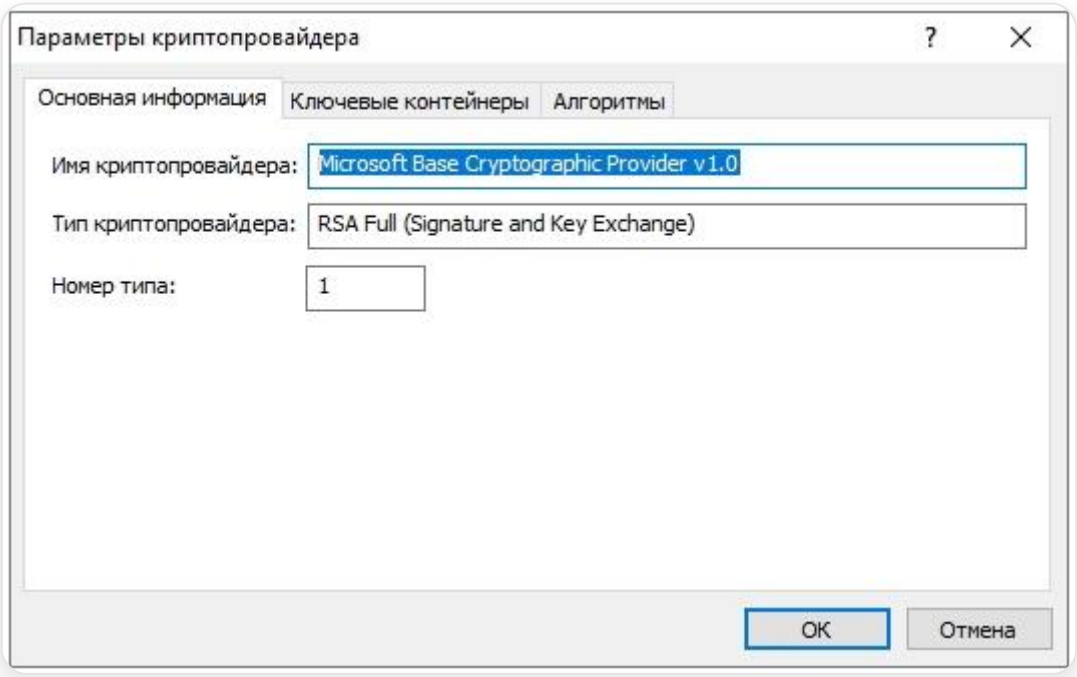


2. Откроется окно **Параметры криптопровайдера**.
   Информация по свойствам криптопровайдера представлена 3 закладками:

   - Основная информация;
   - Ключевые контейнеры;
   - Алгоритмы

Основная информация

Закладка содержит такие данные, как имя провайдера, тип провайдера и номер типа.



Ключевые контейнеры

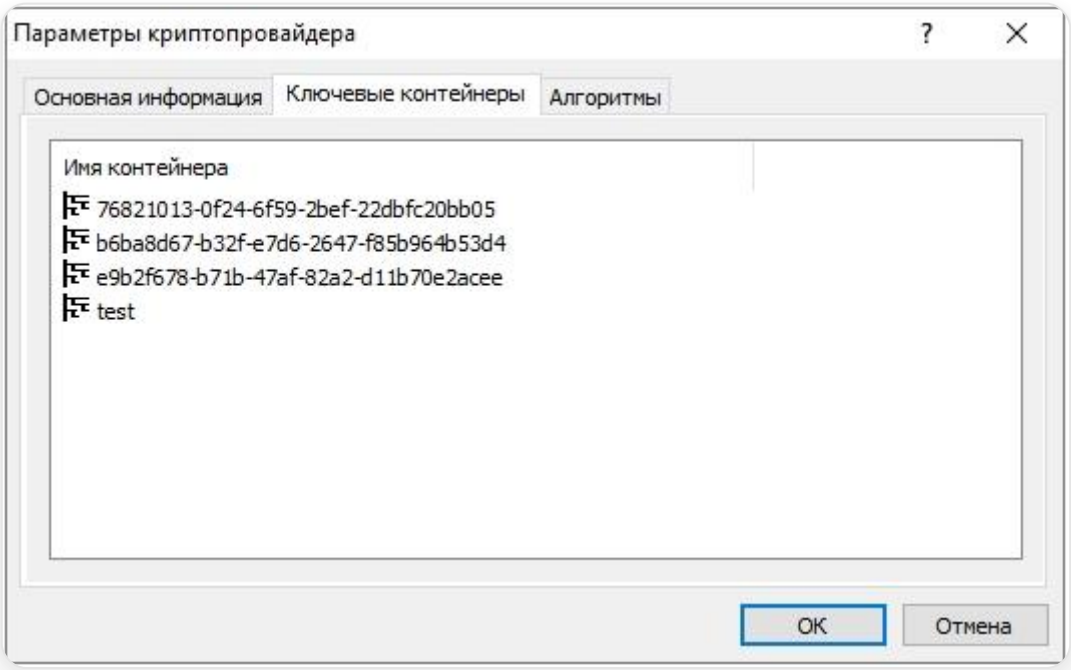
Закладка содержит такие данные, как имя провайдера, тип провайдера и номер типа.

При формировании закрытые ключи записываются на ключевой носитель (ключевой контейнер).
Ключевой контейнер может содержать:

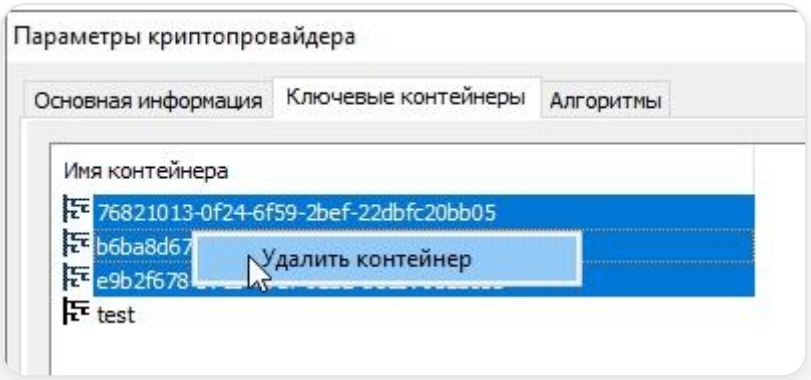
- ключ подписи;
- ключ шифрования;
- ключ подписи и ключ шифрования одновременно.

Дополнительно ключевой контейнер содержит служебную информацию, необходимую для обеспечения криптографической защиты ключей, их целостности и т. п.

Каждый контейнер (независимо от типа носителя) является полностью самостоятельным и содержит всю необходимую информацию для работы как с самим контейнером, так и с закрытыми (и соответствующими им открытыми) ключами.

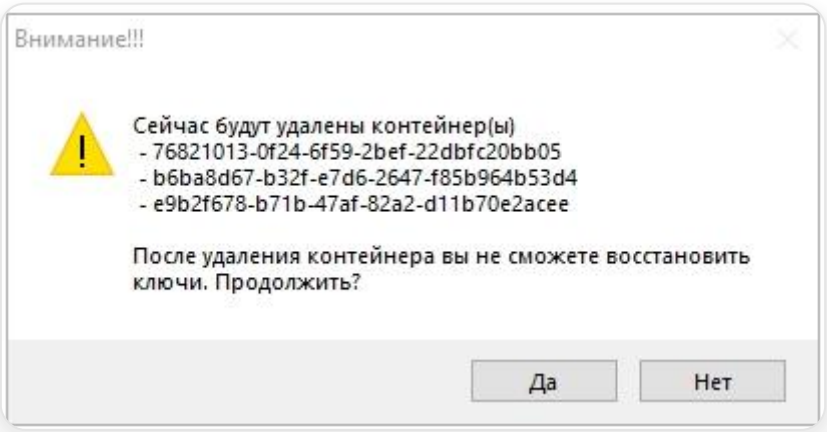


В этой закладке вы также можете удалять ключевые контейнеры. Для этого выберите контейнер, который необходимо удалить, и щелкните на нем правой клавишей мыши: выберите **Удалить.** Откроется окно с предупреждением.



	Обратите внимание, что при удалении контейнера восстановить ключевую пару будет невозможно.

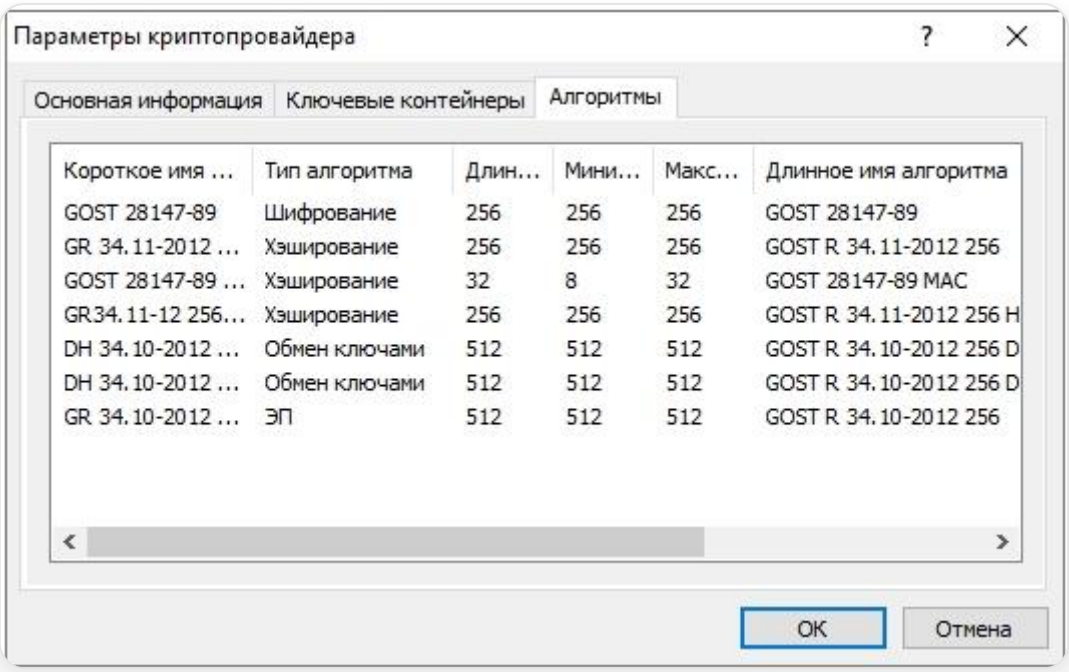
Подтвердите свое решение:



Ключевой контейнер будет удален из общего списка для выбранного криптопровайдера.

Алгоритмы

Закладка содержит информацию об используемых алгоритмах:



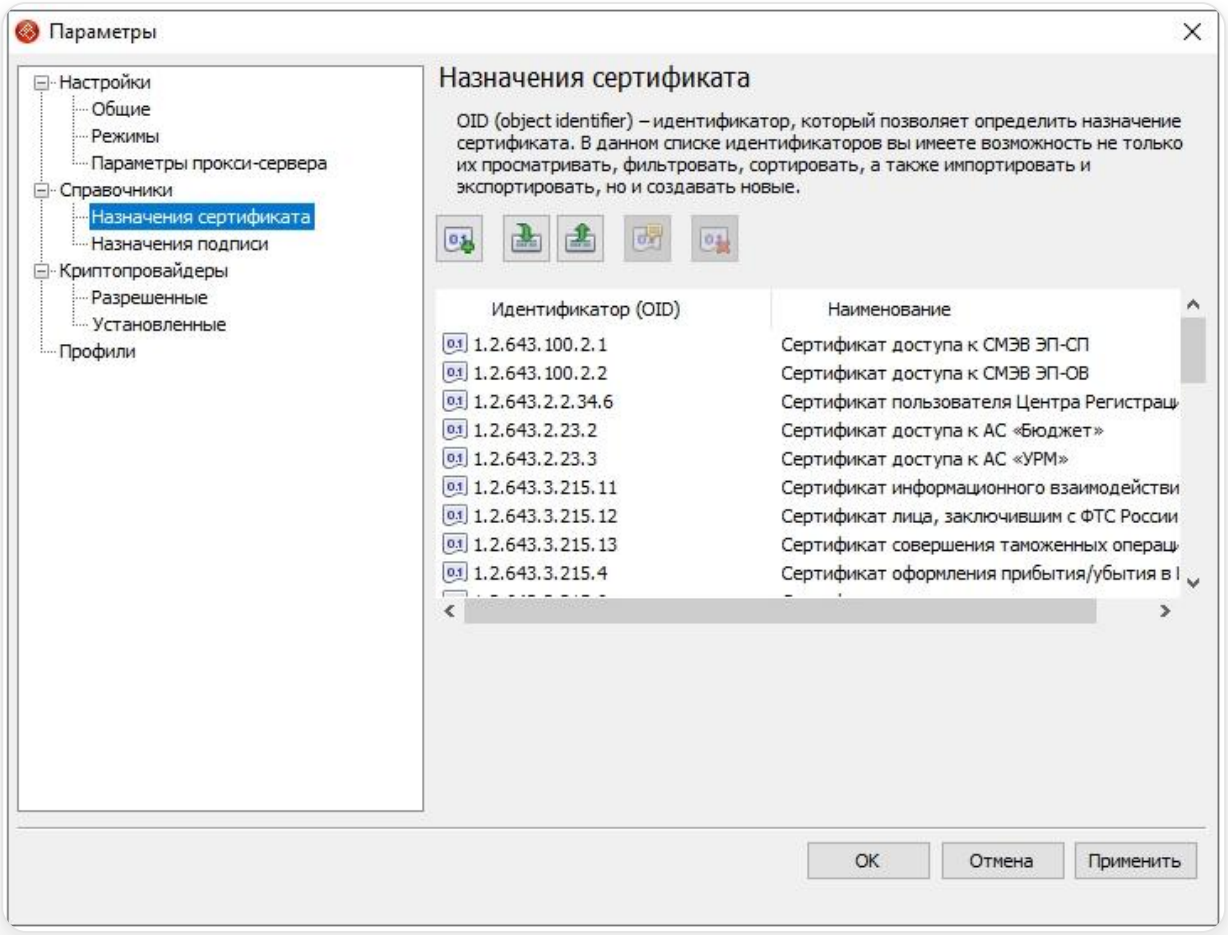
Открыть статью на сайте

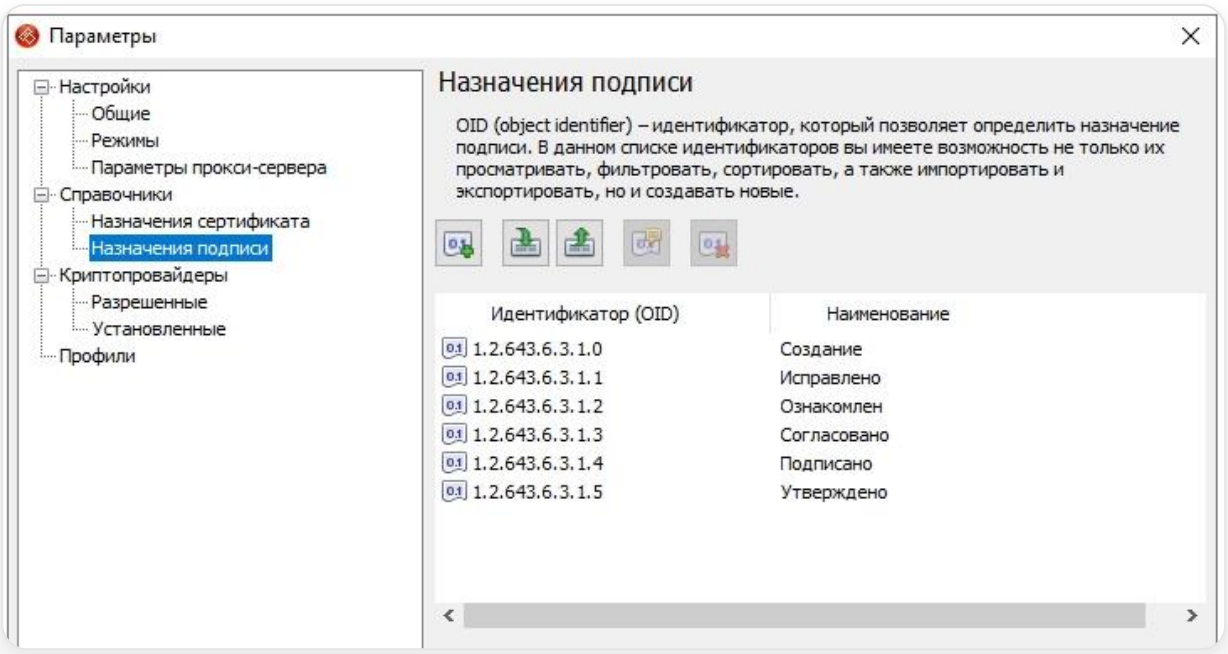
Создание нового назначения

Программа «КриптоАРМ» позволяет добавить к создаваемой подписи или сертификату информацию о его назначении, например, гриф согласования, гриф утверждения и т.п.

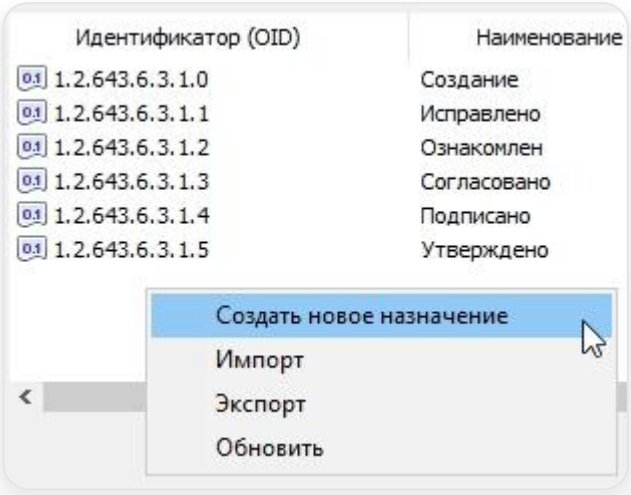
Чтобы создать новое назначение сертификата или подписи:

1. В верхнем меню главного окна выберите **Настройки > Управление настройками > Справочники > Назначения сертификатов** для добавления назначения сертификата или Справочники > Назначения подписи для добавления назначения подписи. В правой части окна отобразится список установленных назначений:

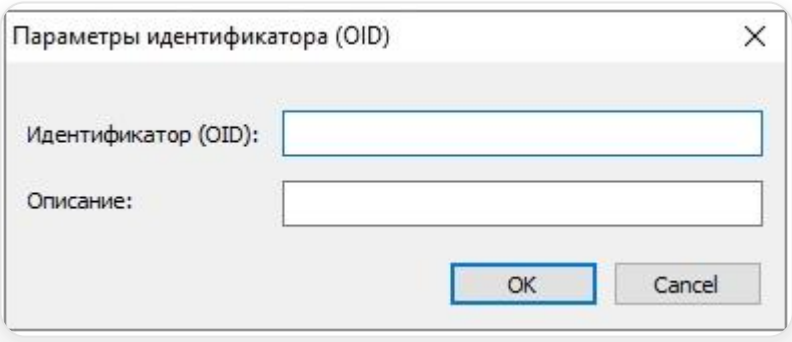




2. Чтобы создать новое назначение, в контекстном меню раздела выберите пункт **Создать новое назначение** или на панели инструментов **Создать**:



3. Появится окно ввода параметров политики. Введите идентификатор (OID) и его описание:



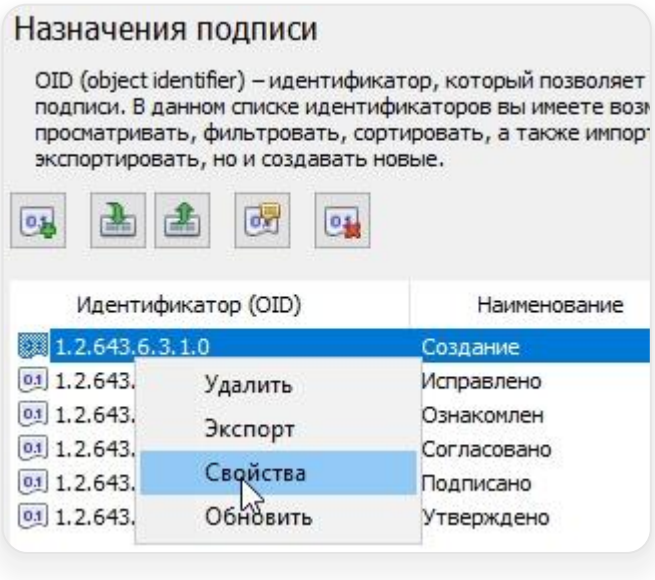
4. В справочник назначений добавится новая запись.

Открыть статью на сайте

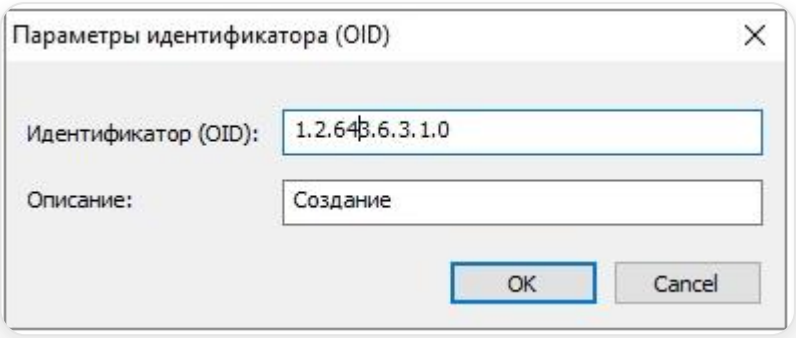
Просмотр свойств назначения

Чтобы просмотреть свойства OID-а:

1. В верхнем меню главного окна выберите **Настройки > Управление настройками > Справочники > Назначения сертификатов** для просмотра свойств назначения сертификата или **Справочники > Назначения подписи** для просмотра свойств назначения подписи. В правой панели главного окна отобразится список установленных назначений сертификатов. Чтобы просмотреть свойства назначения сертификата, выберите его из списка, в контекстном меню объекта или на панели инструментов выберите пункт **Свойства**:



2. Появится окно **Параметры политики**, в котором отобразится информация о идентификаторе (OID) и его описание:



Открыть статью на сайте

Импорт, экспорт и удаление назначения

1. **Импорт назначения**

   Чтобы импортировать назначение сертификата **в формате .xml**

   - В верхнем меню главного окна выберите **Настройки > Управление настройками >Справочники Справочники > Назначения сертификатов** для импорта назначений сертификатов или **Справочники > Назначения подписи** для импорта назначений подписи. В правой панели главного окна отобразится список установленных назначений. Чтобы импортировать назначение, на панели инструментов выберите пункт **Импорт**.
   - В окне проводника выберите файл с OID в формате .xml
   - В справочник назначений будет импортировано новое назначение.

2. **Экспорт назначения**

   Чтобы экспортировать назначение сертификата в формате .xml:

   - В верхнем меню главного окна выберите **Настройки > Управление настройками > Справочники Справочники > Назначения сертификатов** для экспорта назначений сертификатов или **Справочники > Назначения подписи** для экспорта назначений подписи. В правой панели главного окна отобразится список установленных назначений. Чтобы экспортировать назначение (или группу назначений), выберите его из списка. В контекстном меню объекта или на панели инструментов выберите пункт **Экспорт**.
   - В окне проводника введите имя экспортируемого файла с OID
   - Назначение сертификата будет экспортировано в файл с OID в формате .xml. Вы можете экспортировать сразу все назначения, для этого в контекстном меню на разделе **Назначения сертификата/Назначения подписи** или на панели инструментов выберите пункт **Экспорт**.

	При одновременном экспорте всех или нескольких назначений, будет создаваться один .xml файл, содержащий все экспортируемые назначения.

3. **Удаление назначения**

Чтобы удалить назначение сертификата из справочника:

- В верхнем меню главного окна выберите **Настройки > Управление настройками > Справочники > Назначения сертификатов** для удаления назначения сертификатов или **Справочники > Назначения подписи** для удаления назначения подписи. В правой панели главного окна отобразится список установленных назначений. Выберите назначение (или группу назначений) из списка, в контекстном меню объекта или на панели инструментов выберите пункт **Удалить**.
- На запрос системы подтвердите свое решение.
- Выбранное назначение будет удалено из справочника назначений сертификатов.

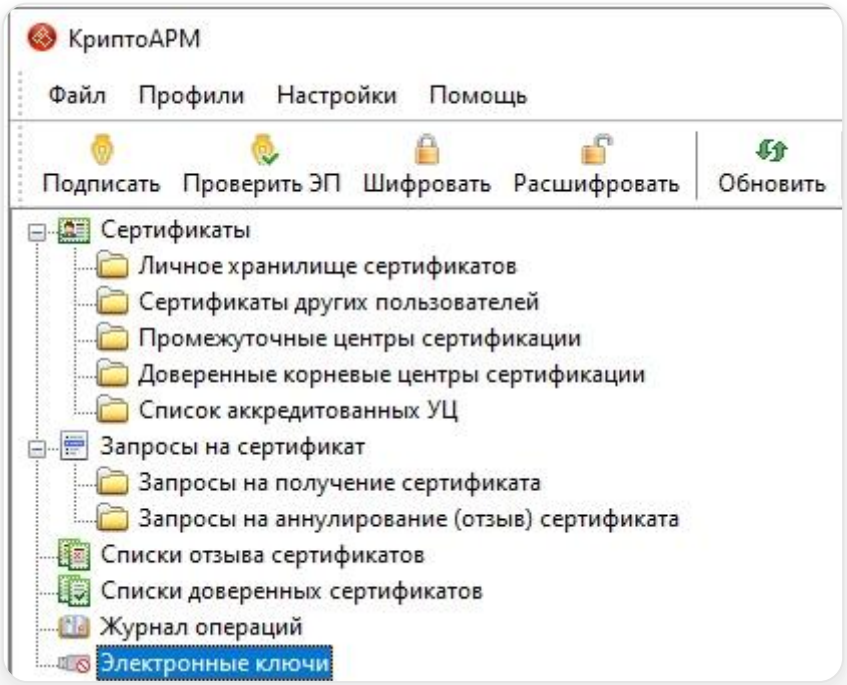
Открыть статью на сайте

Операции с ключевыми носителями

С помощью программы «КриптоАРМ Стандарт» вы можете подключать отчуждаемые ключевые носители и импортировать сертификаты с них в личное хранилище пользователя.

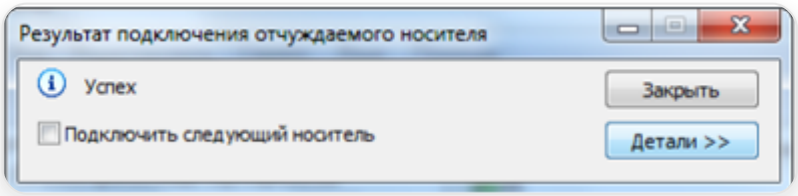
На сегодняшний день работа с отчуждаемыми носителями через «КриптоАРМ» реализована только для «КриптоПро CSP» и «КриптоПРО УЭК CSP». Работать с отчуждаемыми носителями, используя другие криптопровайдеры (например, стандартные Windows), вы можете, но только через средства самого криптопровайдера (а не программы «КриптоАРМ»).

В дереве главного окна откройте раздел **Электронные ключи**.

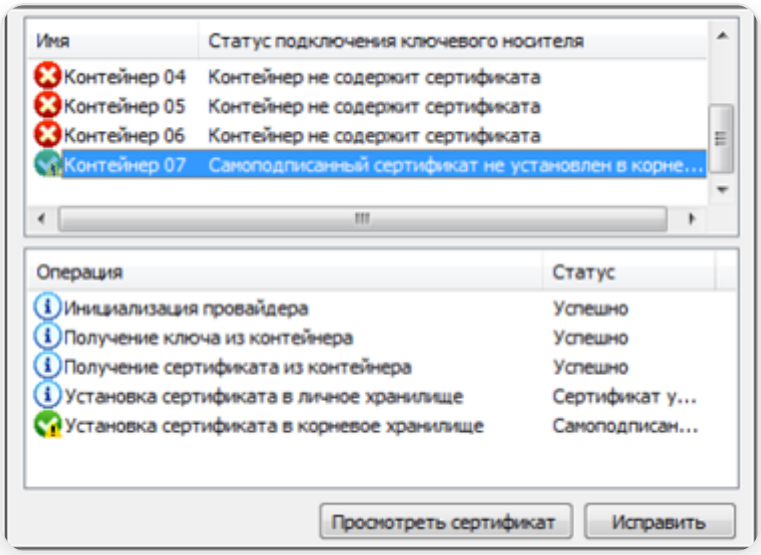


Вставьте ключевой носитель и следуйте указаниям Помощника:

1. На первом шаге ознакомьтесь с порядком и требованиями к подключению отчуждаемого носителя. Нажмите **Далее**.
2. В следующем окне выберите тип криптопровайдера и ключевого носителя. В качестве ключевого носителя может выступать дискета или смарт-карта/USB токен. Для продолжения вставьте носитель и нажать кнопку **Далее**.
3. Выберите в списке контейнеров сертификаты для установки. Вы можете просмотреть информацию о сертификате, выбрав контейнер и нажав на кнопку **Просмотреть сертификат** в контейнере. Для завершения операции нажмите на кнопку **Готово**.
4. При обращении к контейнеру введите pin-код.
5. Далее возникнет окно с результатом выполнения операции. Вы можете просмотреть дополнительную информацию о статусе импорта сертификатов с отчуждаемого носителя, нажав на кнопку **Детали**.



6. В окне результата выполнения операции можно просмотреть журнал операций. В случае возникновения замечаний, их можно исправить, выбрав их в журнале и нажав на кнопку **Исправить**.



7. Чтобы закрыть окно результата выполнения операции, нажмите на кнопку **Закрыть**. Чтобы подключить следующий отчуждаемый носитель, поставьте флаг **Подключить следующий носитель**. При нажатии на кнопку **Закрыть** вновь откроется мастер подключения отчуждаемого носителя.

	Импортированный с ключевого носителя сертификат можно просмотреть в личном хранилище сертификатов пользователя.

Открыть статью на сайте

Как подписать электронный документ?

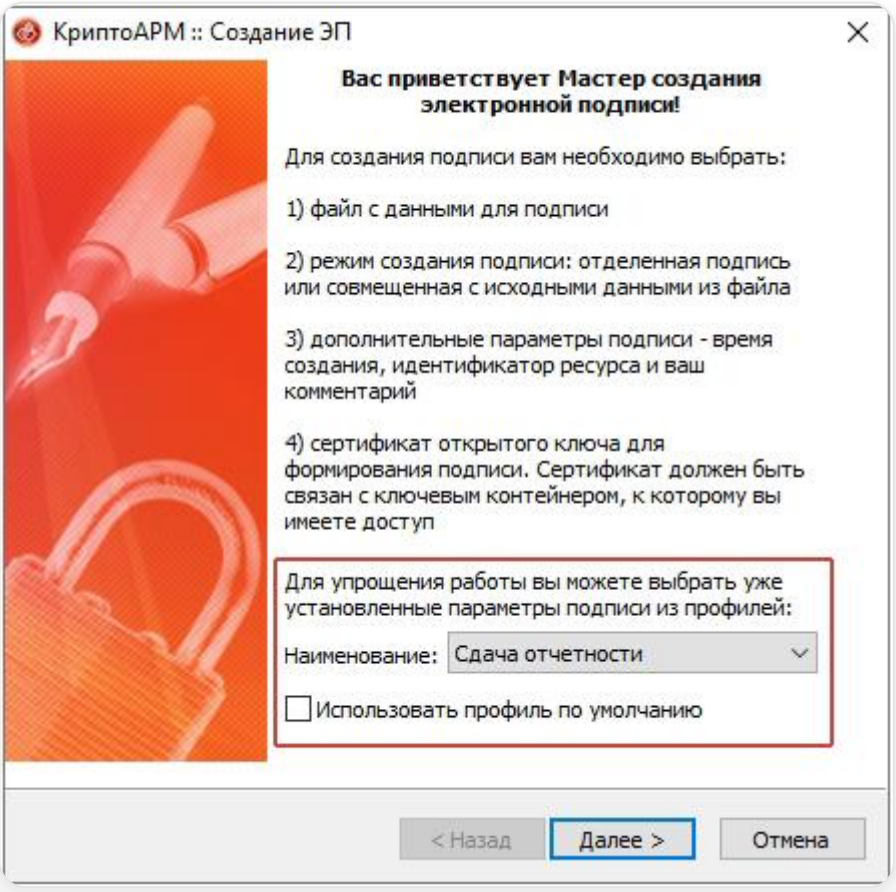
С помощью программы «КриптоАРМ» вы можете подписать отдельный файл или папку файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными).

Подписать данные вы можете через:

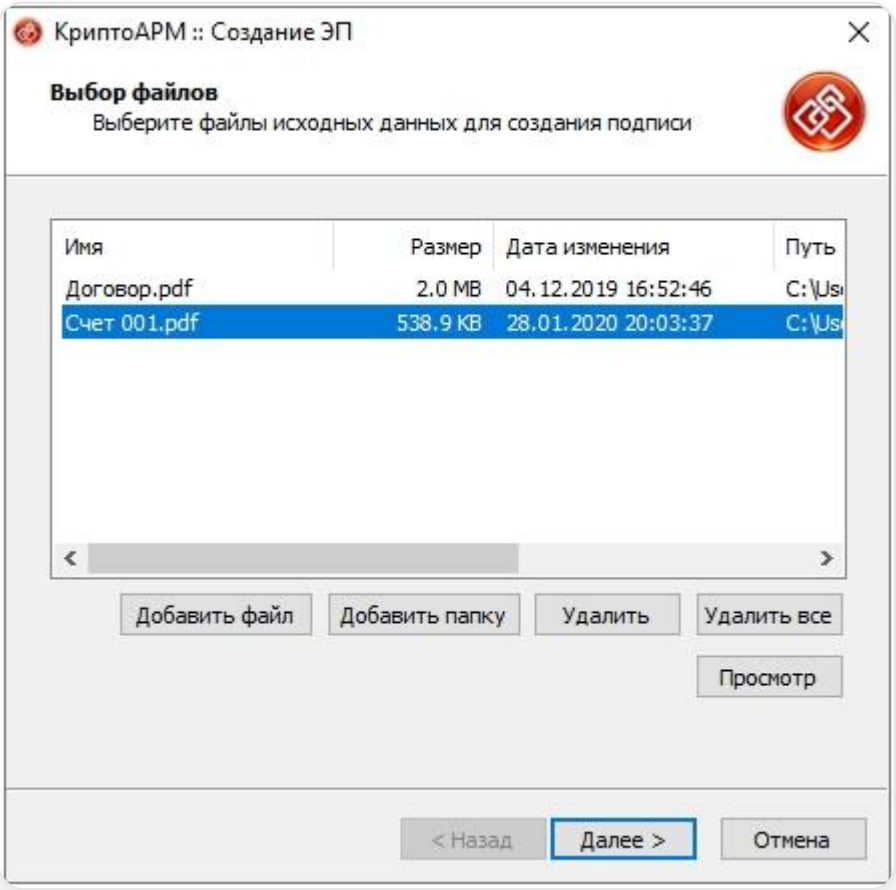
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт **Подписать**. Далее следуйте рекомендациям Помощника по выполнению операции:

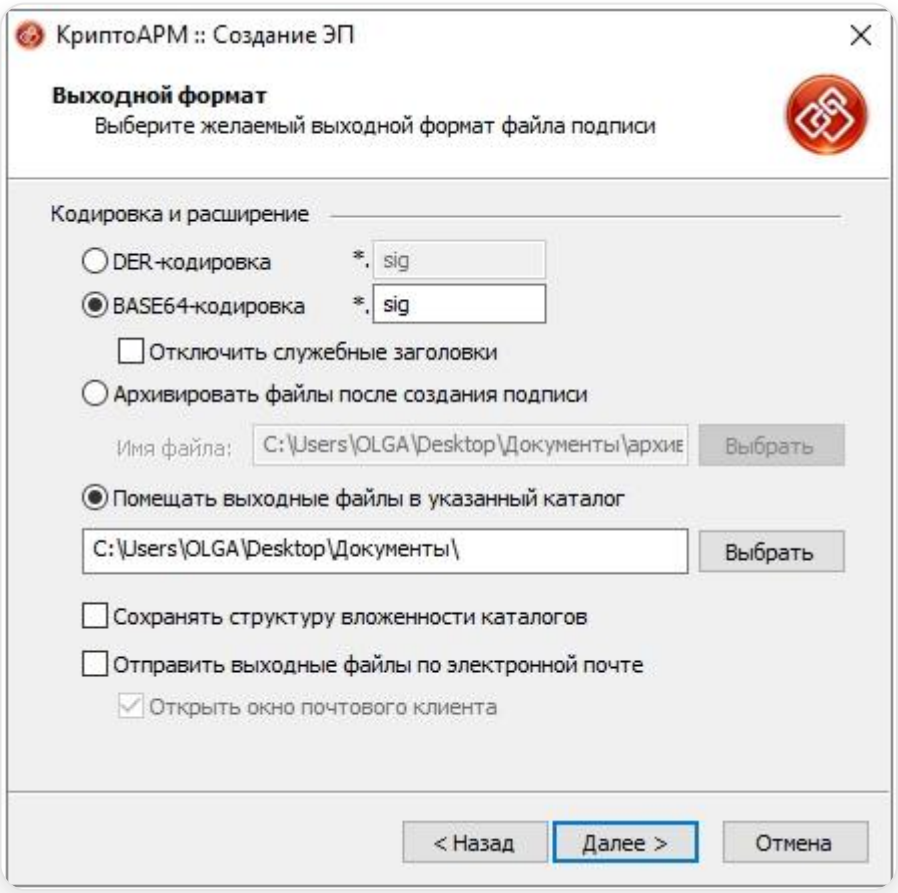
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите папку с файлами или отдельный файл, которые необходимо подписать (кнопки **Добавить папку** и **Добавить файл** соответственно).

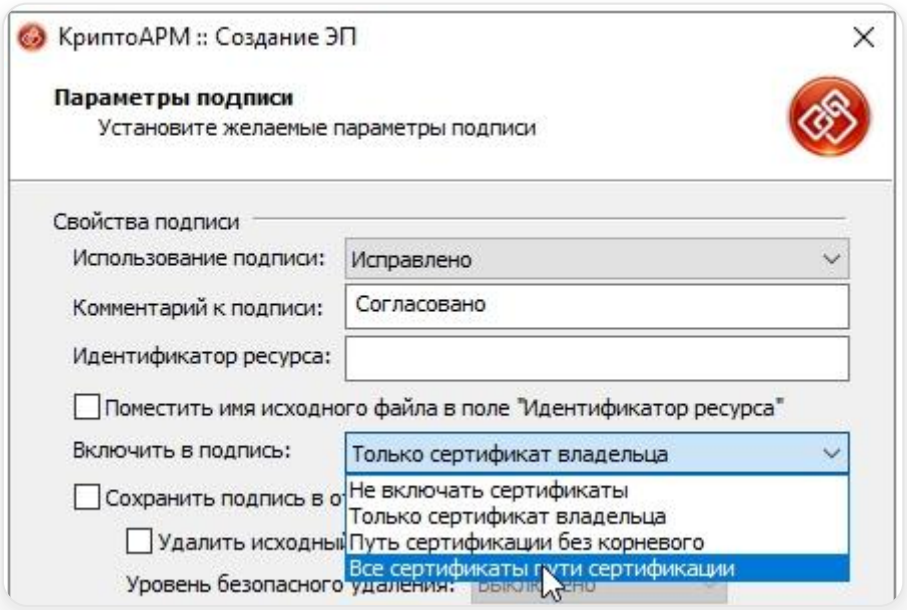


3. В открывшемся окне укажите настройки для выходного формата файла.

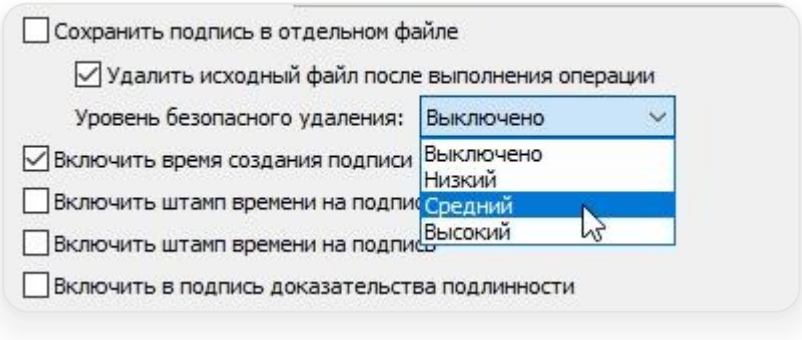


- **Кодировка и расширение;**
  - DER encoded binary X.509. Расширения подписанного файла *.sig, *.p7s.
  - Base64 encoded X.509. Для этого варианта кодирования вы можете указать флаг
- **Отключить служебные заголовки**.
- Расширения подписанного файла *.sig.
- **Архивировать файлы после создания подписи**;
  В строке Имя файла укажите путь до архива и имя создаваемого архива.
- **Помещать выходные файлы в указанный каталог;**
  Если выбрать этот режим и оставить поле ввода пути к каталогу не заполненным, то выходные файлы будут формироваться в каталоге входных файлов.
- **Сохранять структуру вложенности каталогов;**
- **Отправить выходные файлы по электронной почте.**

8. Далее введите необходимые свойства подписи.



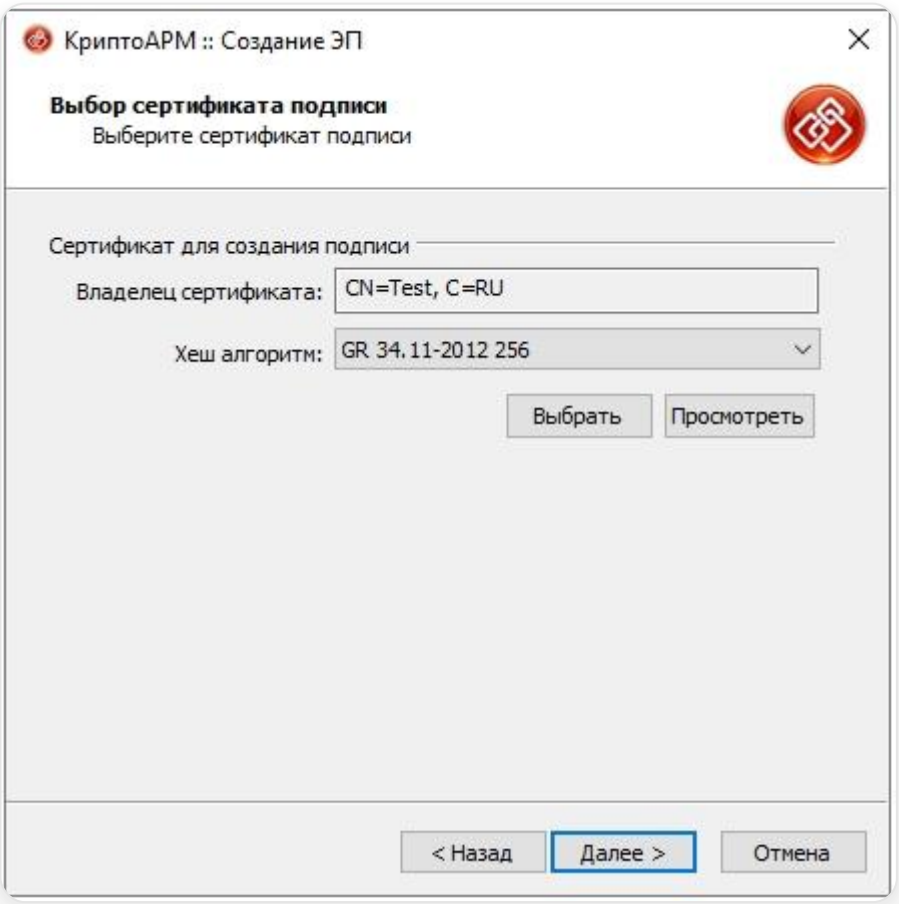
- **Использование подписи;**
  Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений. При выборе из списка какого-либо из назначений, в свойства подписи будет добавлен как идентификатор этого назначения, так и его описание, выбранное в списке. Например, на иллюстрации выбрано назначение "Исправлено". При этом в свойствах подписи будут сохранены идентификатор "1.2.643.6.3.1.1" и его описание "Исправлено".
- **Комментарий к подписи;**
  Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").
- **Идентификатор ресурса;**
- **Включить в подпись:**
  - только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
  - путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
  - все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
  - не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.



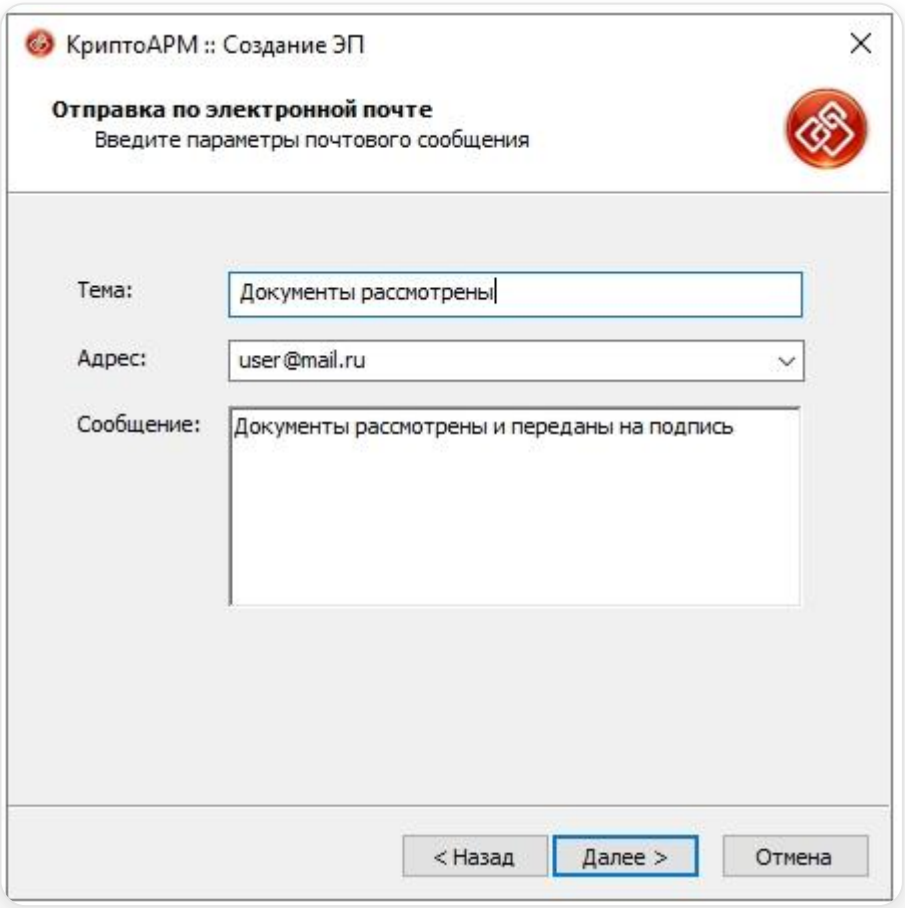
- **Сохранить подпись в отдельном файле;**
  Если установить этот флаг, то будет создана отделенная подпись. Если не устанавливать флаг, будет сформирована совмещенная подпись.
- **Удалить исходный файл после выполнения операции;**
  Если вы решили создать файл совмещенной подписи, вы можете удалить исходный файл после выполнения операции.
- **Уровень безопасного удаления;**
  Подробнее о настройке параметров уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.
- **Включить время создания подписи;**
  При установке флага - в файл подписи будет включено время подписи.
- Флаги **Включить штамп времени на подписываемые данные** и **Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP.
- Флаг **Включить в подпись доказательства подлинности** доступен только при установленной лицензии на «КриптоАРМ СтандартPRO».

	Подробнее о настройке параметров создания подписи вы можете прочитать в разделе Настройки операции подписи.

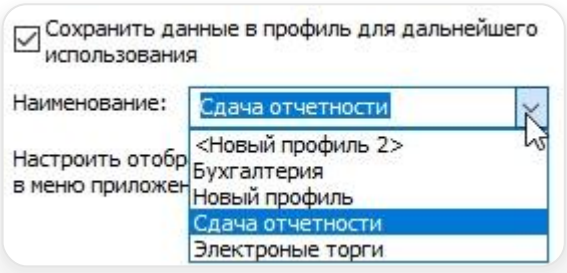
11. Если был установлен флаг **Включить штамп времени на подписываемые данные**, на следующем шаге укажите параметры Службы штампов времени.
12. Укажите личный сертификат для создания ЭП.



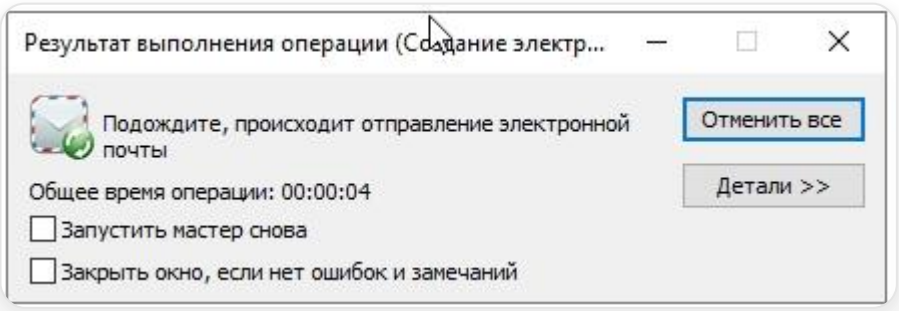
13. Для доступа к выбранному ключевому контейнеру (ГОСТ сертификата) введите пароль.
14. Для отправки подписанных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:



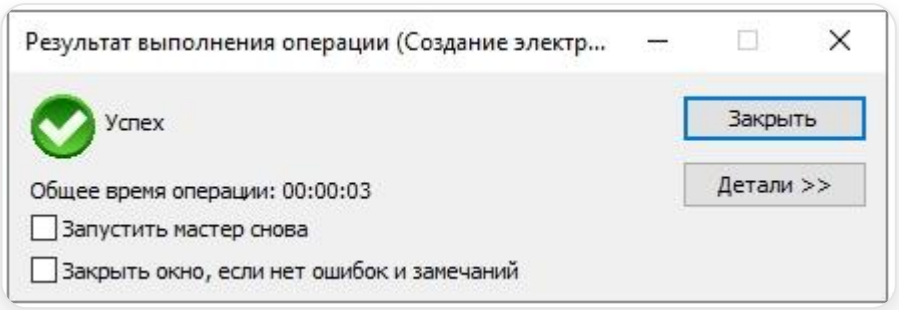
15. После сбора данных для создания ЭП возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл.
    Указанные параметры ЭП можно сохранить в настройку в качестве шаблона для дальнейшего использования. Для этого поставьте флаг в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.



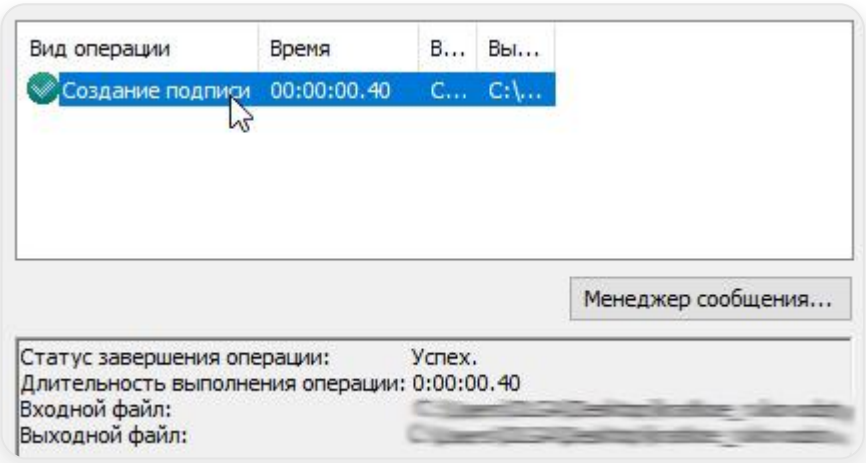
16. Начнется процесс подписи файла. Остановить процесс можно, нажав на кнопку **Отмена**.
17. При отправке подписанных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.



18. Сформированный файл ЭП по умолчанию будет сохранен в тот же каталог, в котором находится файл с исходными данными. Имя файла ЭП совпадает с именем подписываемого файла, дополненным расширением (расширение соответствует выбранному выходному формату). Если файл с таким именем уже существует, сохраните его под другим именем, например.
19. После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах создания подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали**.

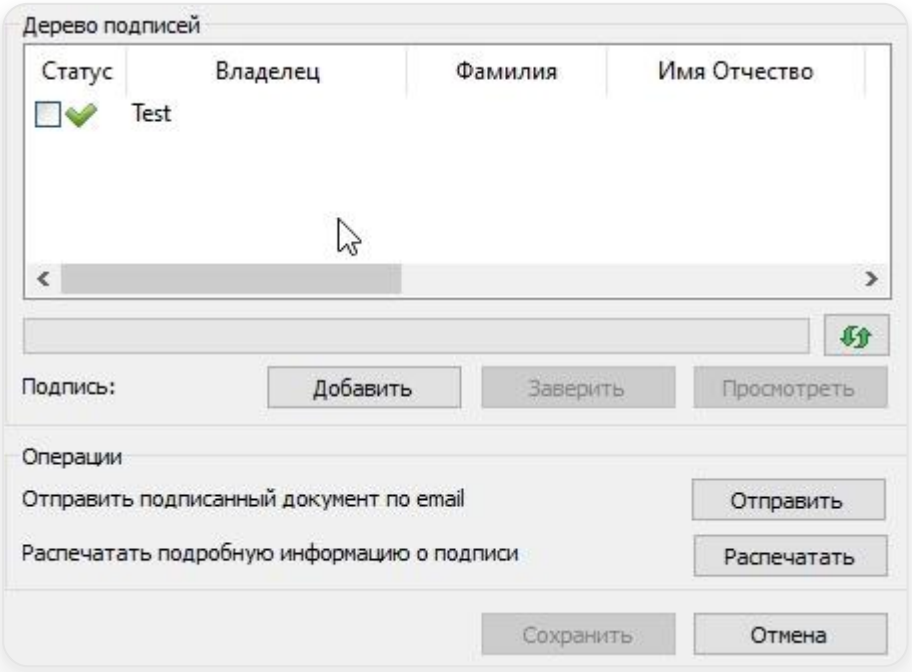


Если вы хотите просмотреть информацию об ЭП и сертификате подписчика, выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.



Откроется окно **Управление подписанными данными**, в котором вы можете:

- Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**).
- Просмотреть следующую информацию (кнопка **Просмотреть**):
  - о добавленной к файлу электронной подписи
  - о сертификате, с помощью которого был подписан файл, и его статусе
  - о штампах времени на подпись и подписываемые данных
- Добавить подпись.
- Заверить подпись(обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя)
- Распечатать информацию (кнопка **На печать**) о ЭП - в новом окне браузера MS IE будет сформирована печатная форма с информацией о подписи.



- Отправить данные по e-mail (кнопка По e-mail) – откроется новое окно ввода информации для получателя сообщения (обратите внимание, что для успешной оправки необходим настроенный почтовый клиент).

Открыть статью на сайте

Добавление заверяющей подписи

Программа «КриптоАРМ» позволяет заверить подпись другой электронной подписью (создать цепочку электронных подписей). В этом случае каждая следующая ЭП подписывает ту ЭП, которой первоначально был подписан файл.
Такой вариант подписи ("заверяющая подпись") используется, когда необходимо заверить исходную подпись файла одной или несколькими электронными подписями других должностных лиц. Цепочка подписей может состоять из 2 уровней: первичная подпись и заверяющие подписи над ней.



Следует помнить, что для проверки подписей, составляющих цепочку, необходимо, чтобы у адресата имелись в наличии корневые сертификаты, подтверждающие подлинность личных сертификатов пользователей, подписавших файл

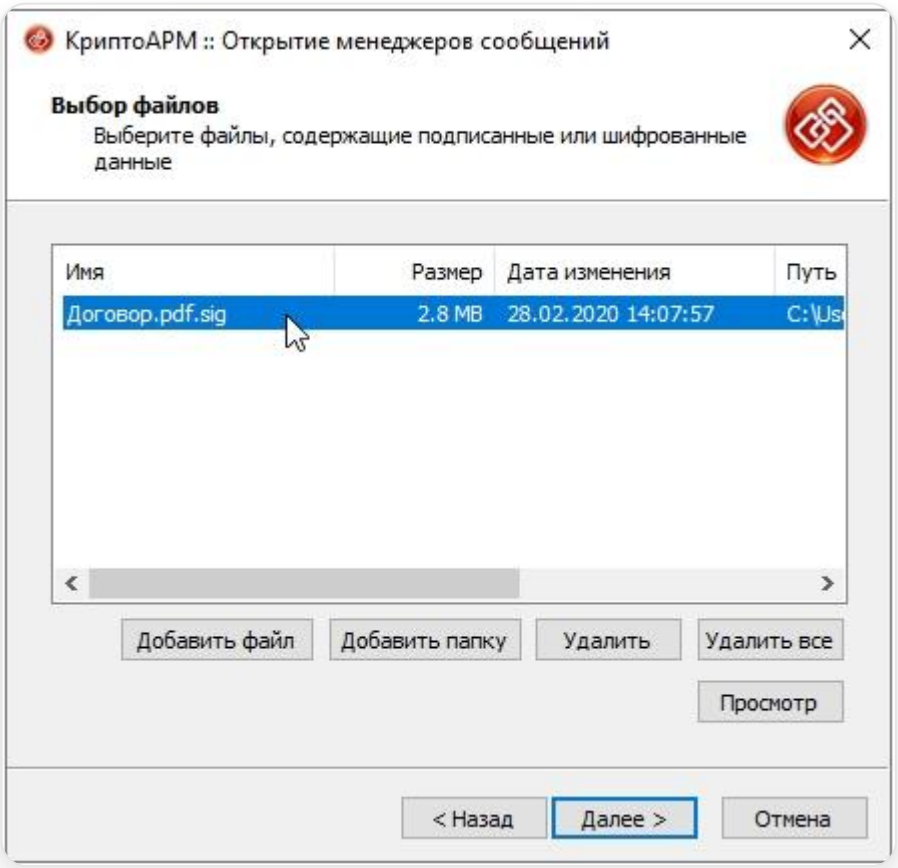
С помощью программы «КриптоАРМ» вы можете заверить своей электронной подписью отдельный подписанный файл или папки подписанных файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными).

Выполнять операции заверения подписи можно для отдельного файла и группы файлов через:

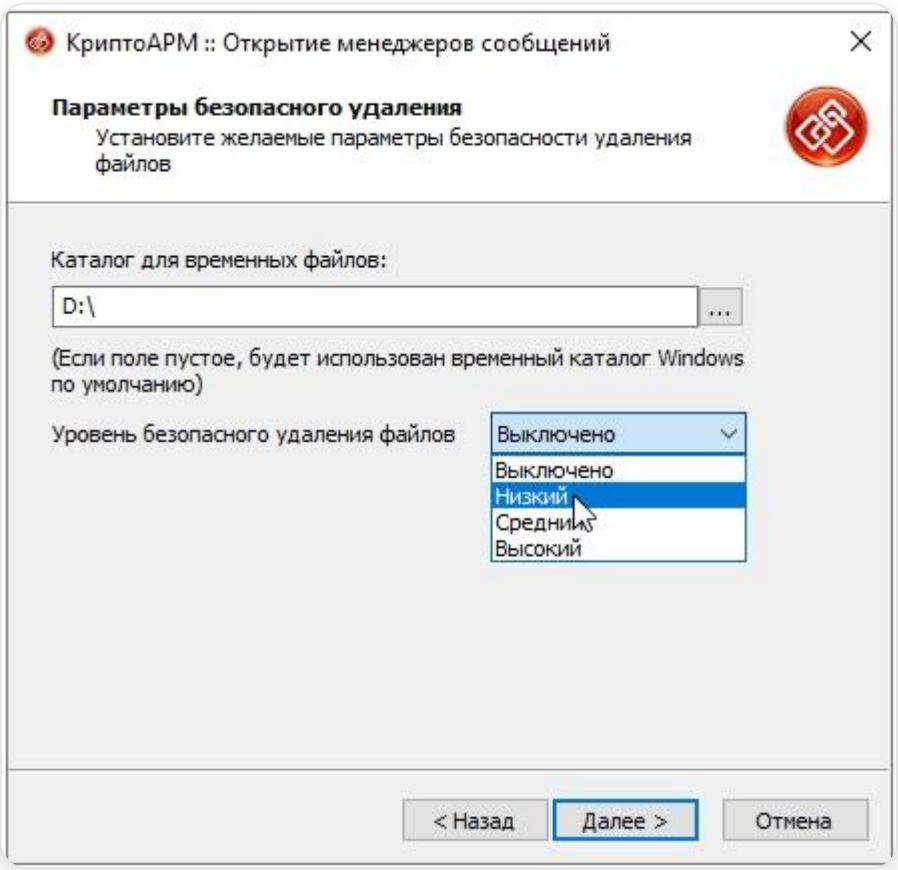
- главное окно
- значок на панели задач
- контекстное меню файла

Для того чтобы заверить подпись файла, выберите пункт меню **Заверить подпись**. Далее следуйте рекомендациям Помощника по выполнению операции:

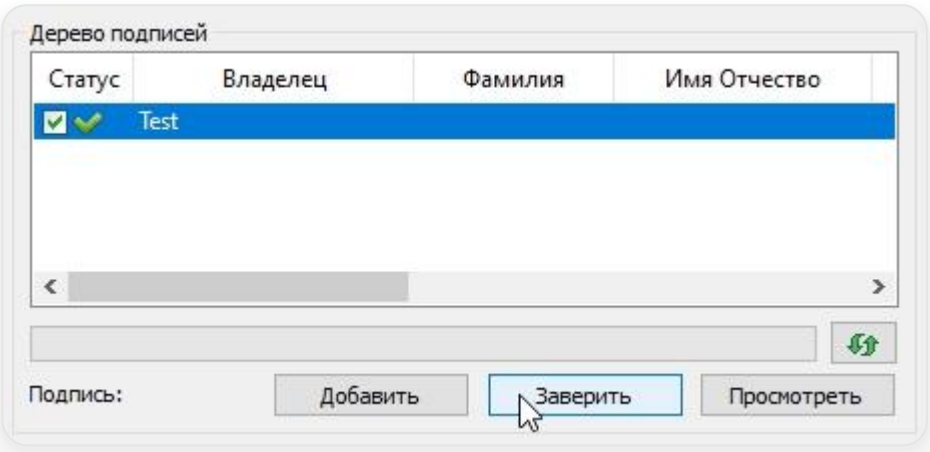
1. Выберите папку с файлами или отдельный файл, которые необходимо заверить электронной подписью (кнопки **Добавить папку** и **Добавить файл** соответственно).



2. Установите параметры безопасности и удаления файлов.



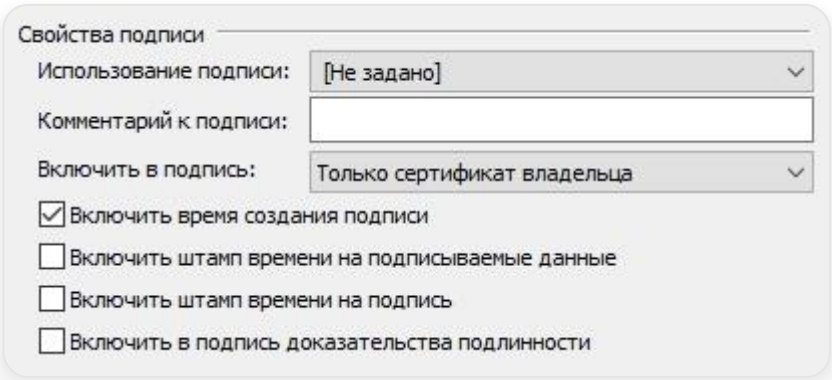
3. После сбора данных для создания заверяющей подписи возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Для продолжения нажмите на кнопку **Готово**.
4. Откроется окно **Управление подписанными данными** (для каждого файла, подпись которого необходимо заверить, откроется свое окно). В поле **Дерево подписей** выберите подпись, которую необходимо заверить, и нажмите на кнопку **Заверить подпись**.



5. Откроется помощник по созданию ЭП. Для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для создания подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**:



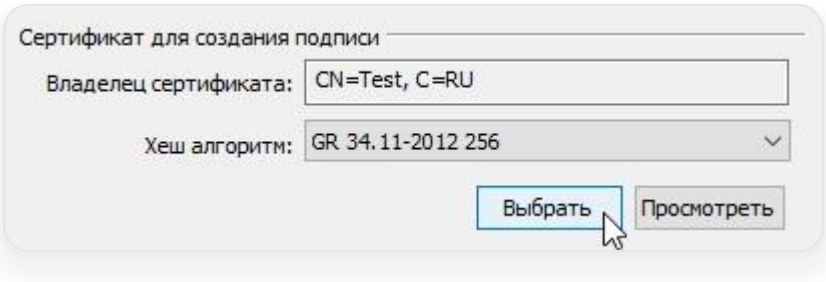
6. В окне параметры подписи введите необходимые свойства добавляемой подписи



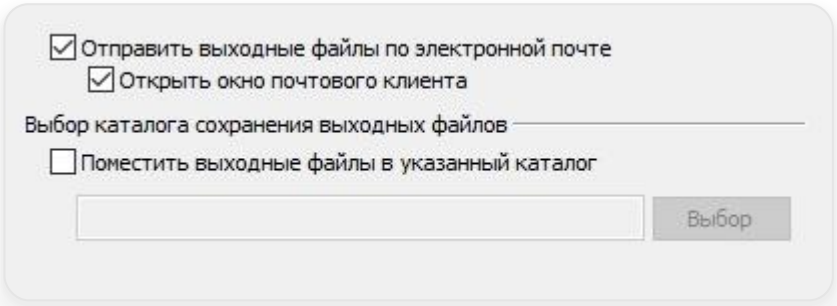
- **Использование подписи**;
  Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.
- **Комментарий к подписи;**
  Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").
- **Включить в подпись**:
  - только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
  - путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
  - все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
  - не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.
  - Флаги **Включить штамп времени на подписываемые данные** и **Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP.
  - Флаг **Включить в подпись доказательства подлинности** доступен только при установленной лицензии на «КриптоАРМ СтандартPRO».

	Подробнее о настройке параметров создания подписи вы можете прочитать в разделе Настройки операции подписи.

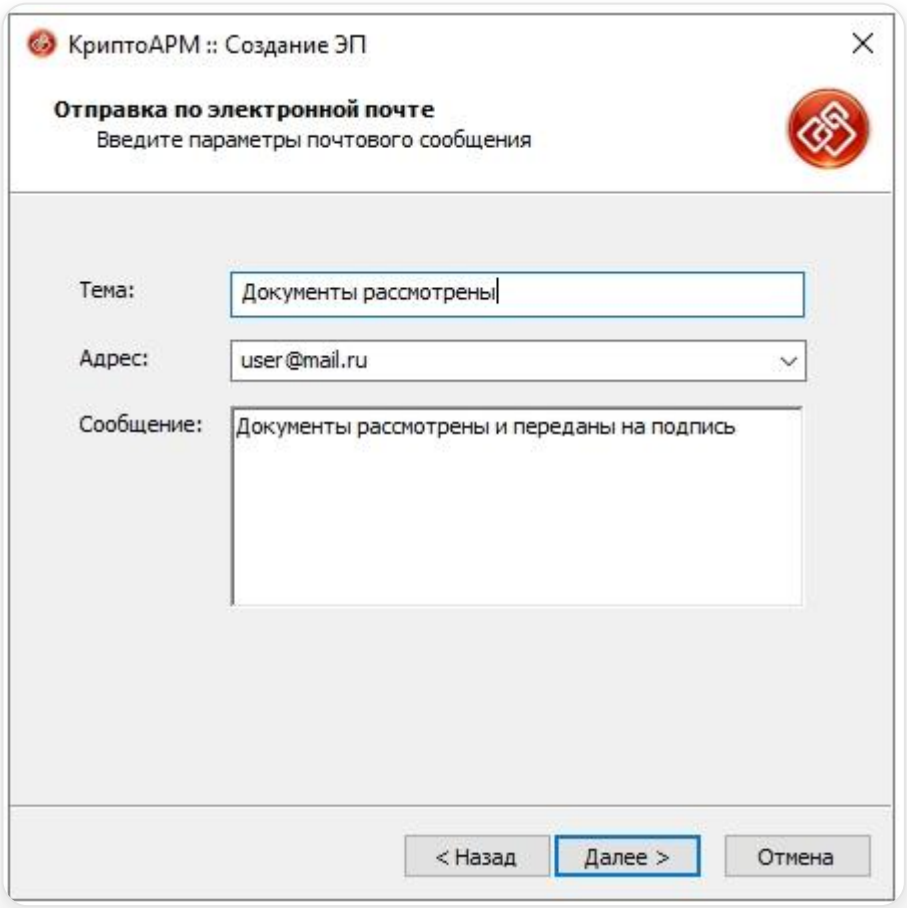
4. Если на ранее вы установили флаг **Включить штамп времени на подписываемые данные**, в следующем окне укажите параметры Службы штампов времени.
5. Далее выберите личный сертификат, который будете использовать для создания ЭП (кнопка **Выбрать**).



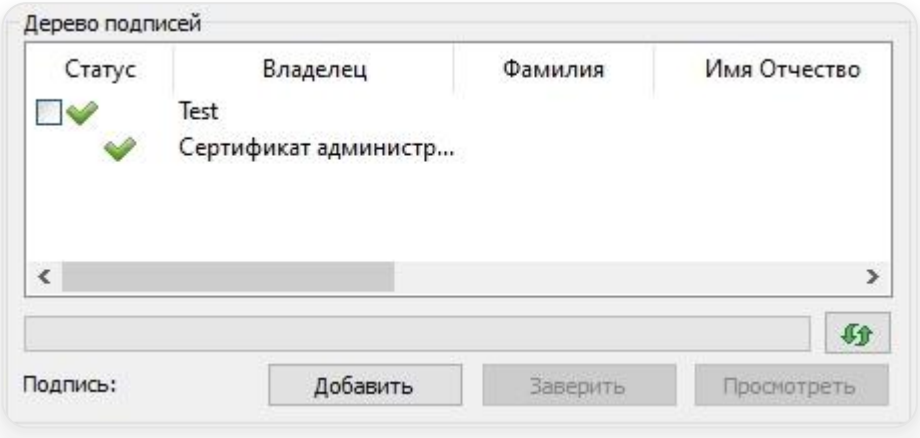
В этом же окне укажите, будете ли вы отправлять выходные файлы по электронной почте:



6. Для отправки подписанных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:

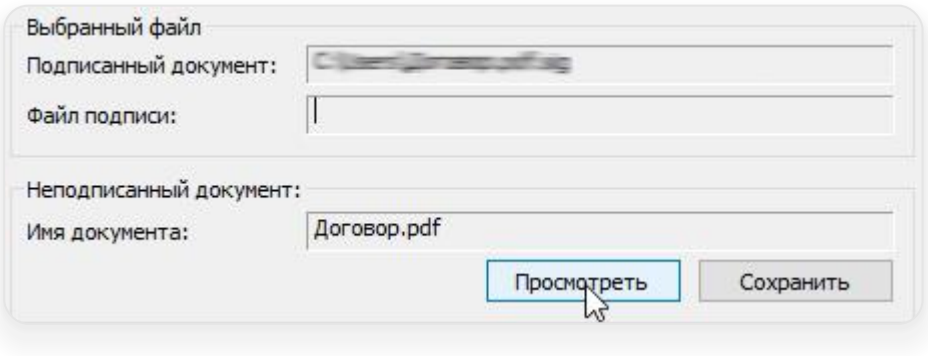


7. Данные для заверения подписи собраны. Нажмите на кнопку **Готово**.
8. Данные будут подписаны. В результате операции в окне **Управление подписанными данными** появится значок заверяющей подписи (в иерархии заверяющая подпись будет подписью второго уровня).

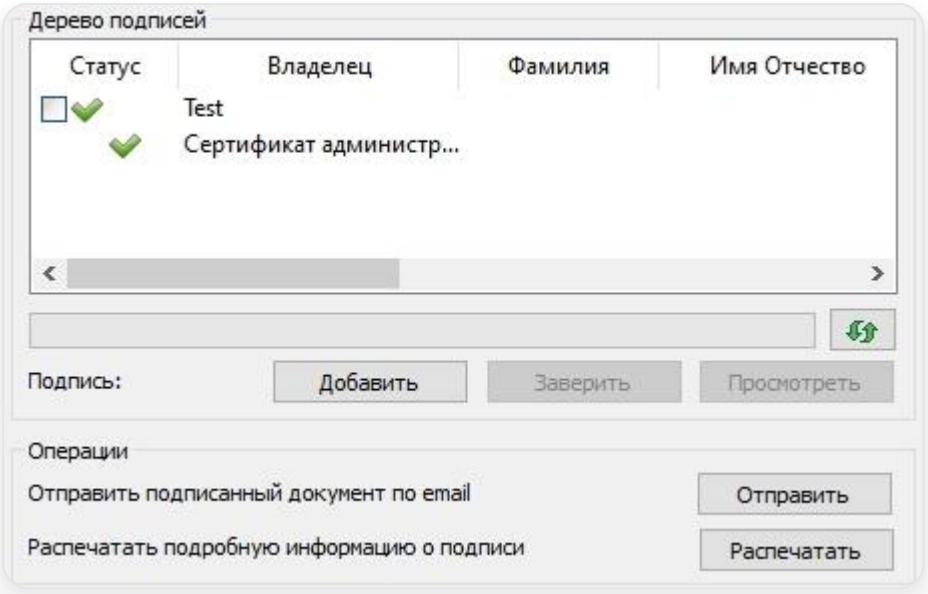


В окне **Управление подписанными данными** вы можете:

- Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**).



- Просмотреть информацию (кнопка Просмотреть)
  - о заверяющей ЭП (атрибуты и алгоритмы подписи);
  - о сертификате, с помощью которого был подписан файл, и его статусе;
  - о штампах времени на подпись и подписываемые данных.
- Добавить соподпись.
- Заверить первичную подпись еще одной заверяющей (обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя).



- Отправить данные по почте (для завершения этой операции необходим настроенный почтовый клиент).
- Распечатать информацию о подписи.

Открыть статью на сайте

Как добавить соподпись (параллельную подпись)?

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

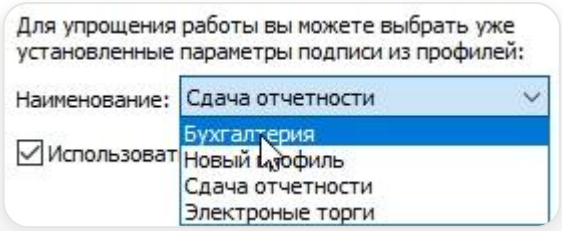
С помощью программы «КриптоАРМ» вы можете добавить электронную подпись к отдельному подписанному файлу или к папке подписанных файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными).

Добавить подпись к подписанному файлу (создать соподпись) вы можете через:

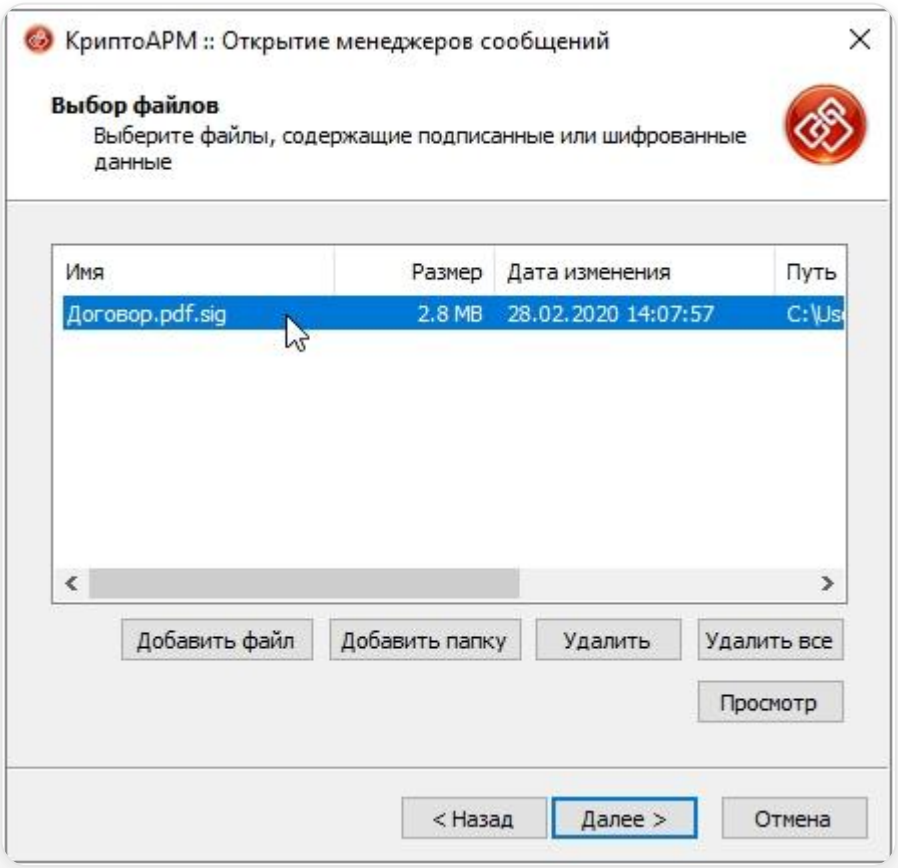
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Добавить подпись**. Далее следуйте рекомендациям Помощника по выполнению операции:

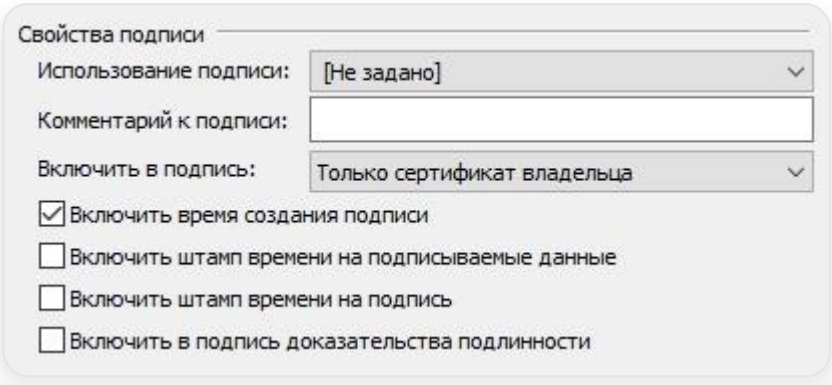
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек создания подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите папку с файлами или отдельный файл, которые необходимо подписать (кнопки **Добавить папку** и **Добавить файл** соответственно):



3. В окне **Параметры подписи** введите необходимые свойства добавляемой подписи.



- **Использование подписи**;
  Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.
- **Комментарий к подписи;**
  Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").
- **Включить в подпись:**
  - только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;

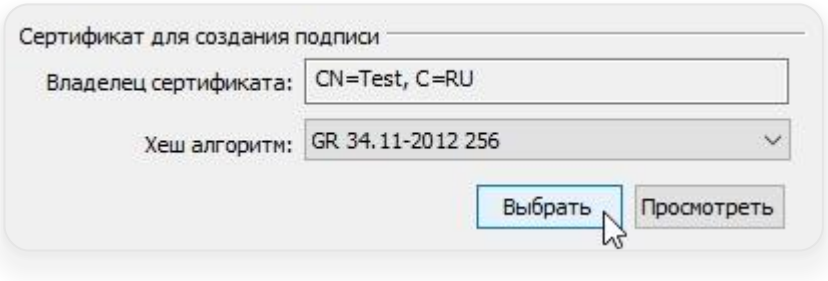
- путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;
- все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
- не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.

◦ Опции **Включить штамп времени на подписываемые данные** и **Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP.

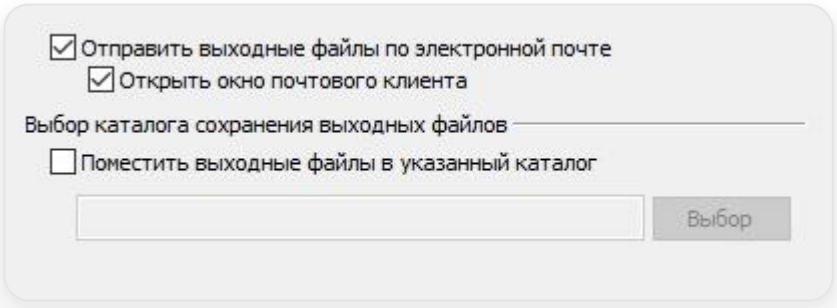
◦ Опция **Включить в подпись доказательства подлинности** доступна только при установленной лицензии на «КриптоАРМ СтандартPRO».

	Подробнее о настройке параметров создания подписи вы можете прочитать в разделе Настройки операции подписи.

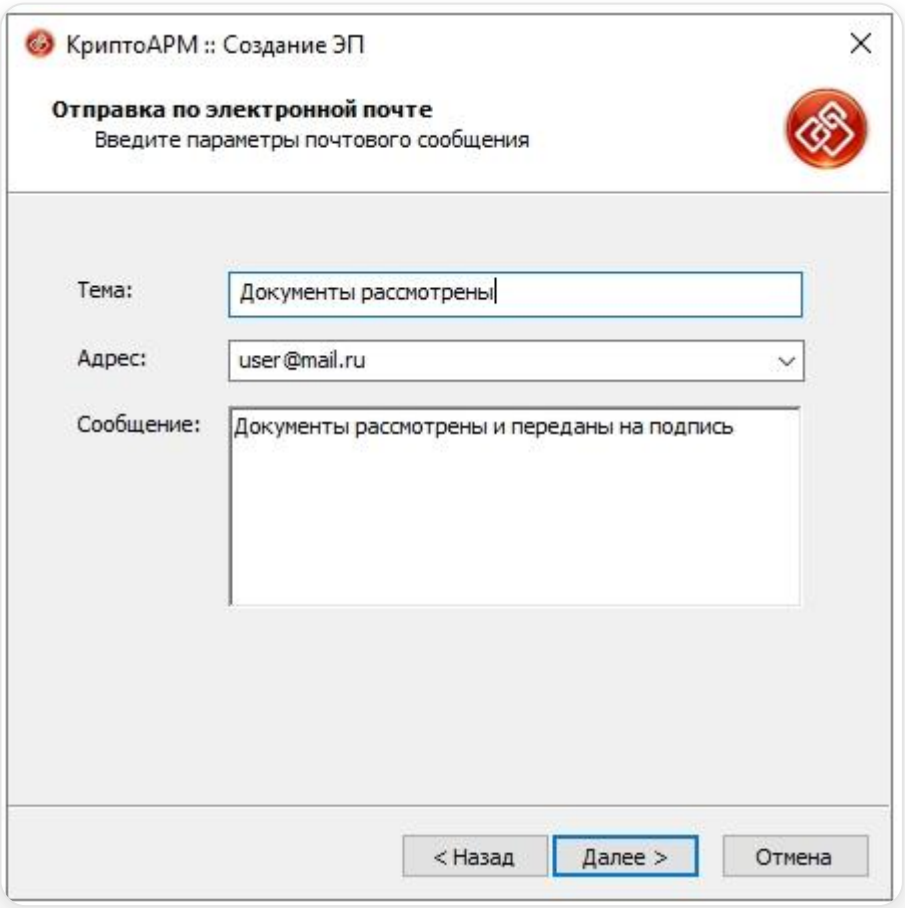
6. Далее выберите личный сертификат, который будете использовать для создания дополнительной ЭП.



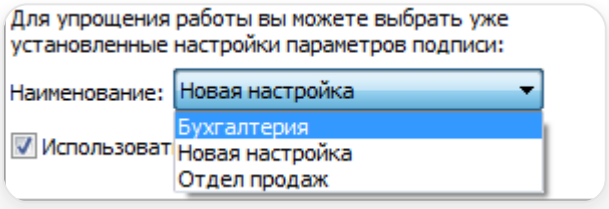
В этом же окне укажите, будете ли вы отправлять выходные файлы по электронной почте:



7. Для отправки подписанных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:

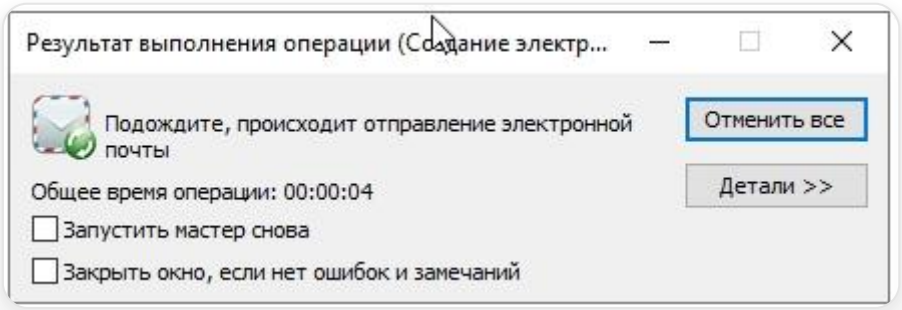


8. Если ранее вы установили флаг **Включить штамп времени** на подписываемые данные, в следующем окне укажите параметры Службы штампов времени .
9. После сбора данных для добавления подписи возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Для продолжения нажмите на кнопку **Готово**.
   Указанные параметры добавления ЭП можно сохранить в настройку в качестве шаблона для дальнейшего использования. Для этого поставьте флаг в пункте **Сохранить данные в настройку** для дальнейшего использования и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.

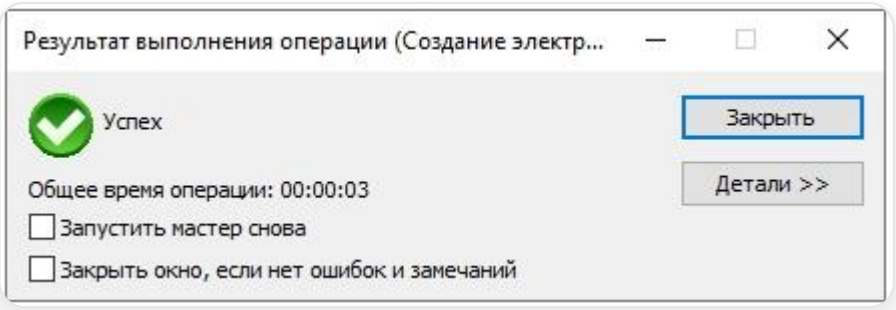


10. Данные будут подписаны с использованием вашего личного сертификата. Начнется процесс подписи файла. Вы можете прервать его, нажав на кнопку **Отмена**.

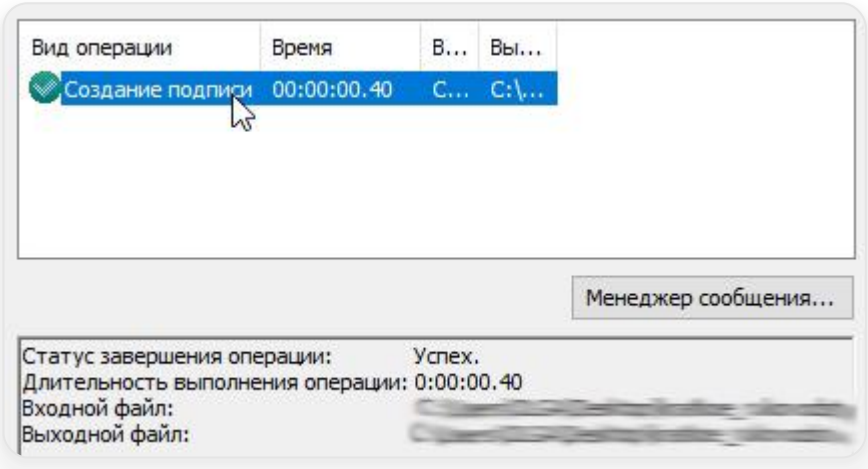
11. При отправке подписанных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.



12. После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах добавления подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите на кнопку **Детали**:

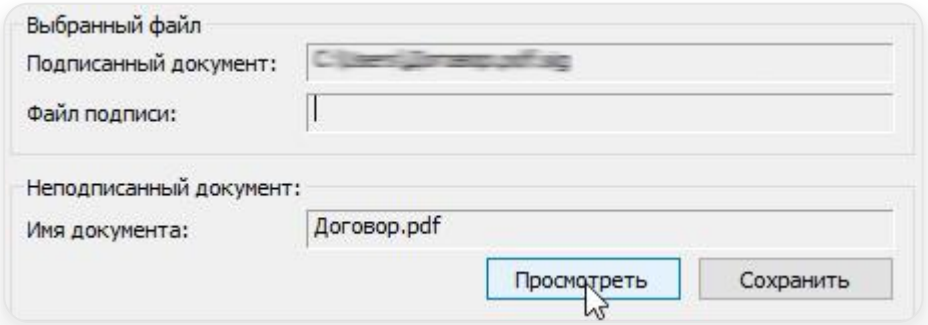


Если вы хотите просмотреть **Дерево подписей**, выделите строчку с операцией и нажмите на кнопку **Менеджер сообщения**. Откроется окно **Управление подписанными данными**, которое содержит дерево подписей:

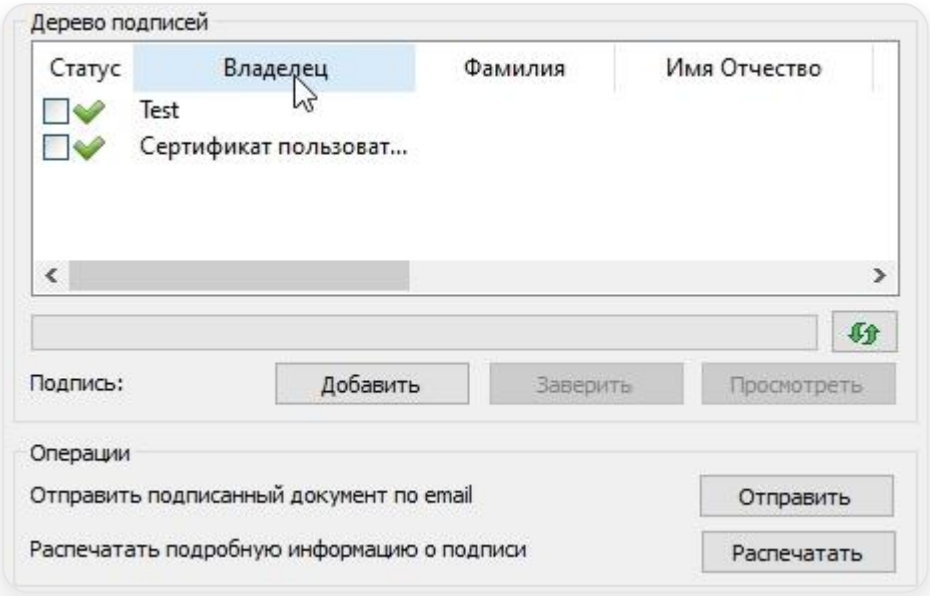


В окне Управление подписанными данными вы можете, выполнить следующие операции:

- Просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**);



- Просмотреть и распечатать информацию (кнопка **Просмотреть**).
  - о добавленной к файлу электронной подписи;
  - о сертификате, с помощью которого был подписан файл, и его статусе;
  - о штампах времени на подпись и подписываемые данных;
- Добавить подпись к уже имеющимся.
- Добавить заверяющую подпись (обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя).



Открыть статью на сайте

Как проверить электронную подпись?

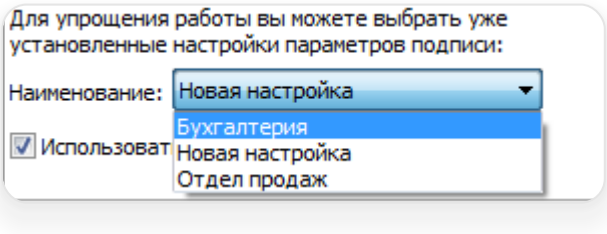
С помощью программы «КриптоАРМ» вы можете проверить корректность электронной подписи отдельного файла или папки файлов (при этом будет проверена подпись каждого файла, входящего в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными).

Проверить корректность электронной подписи вы можете через:

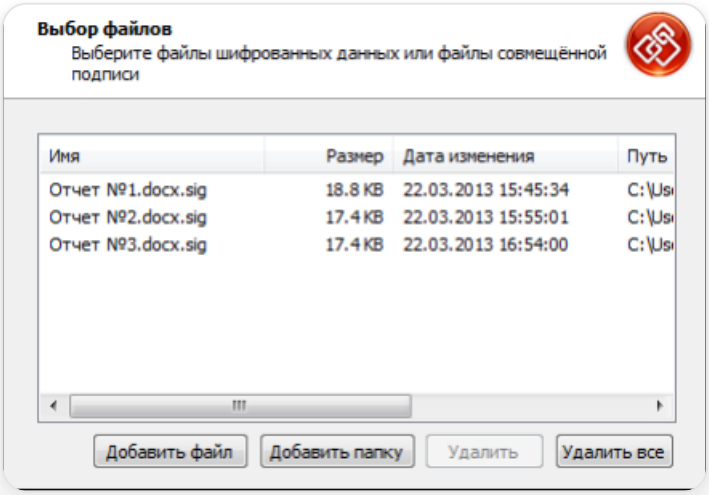
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Проверить подпись**. Далее следуйте указаниям Помощника проверки электронной подписи:

1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию.**

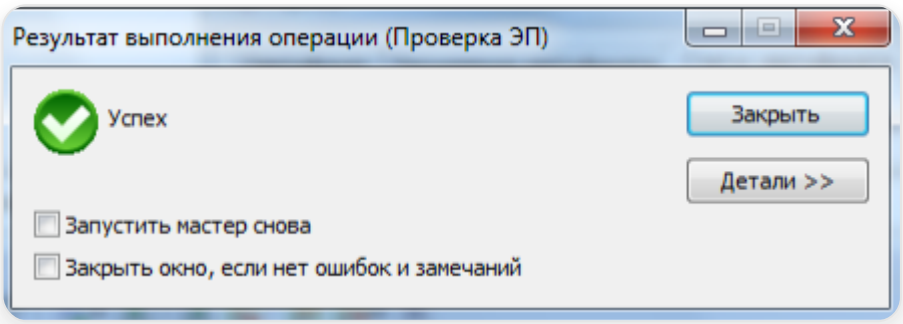


2. Выберите файл или папку файлов, подписанных ЭП, корректность которых необходимо проверить (кнопки **Добавить папку** и **Добавить файл**).

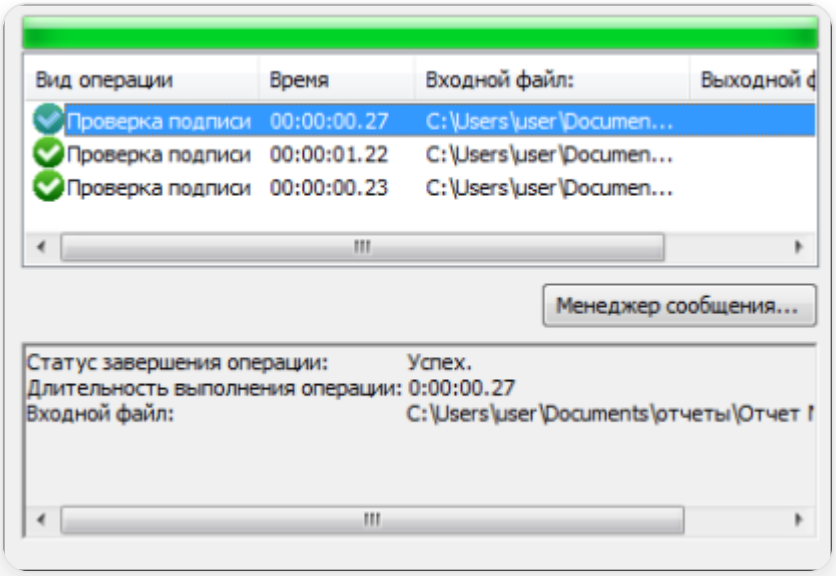


3. После сбора данных для снятия и проверки подписи возникнет окно с информацией о статусе операции и об используемых параметрах. Для продолжения операции нажмите на кнопку **Готово**. Если в файле подписи содержится одна подпись (нет дополнительных и/ или заверяющих), то проверяется корректность ЭП и действительность сертификата отправителя. Если в файле ЭП содержится более одной подписи, то проверяется корректность каждой подписи в коллекции.

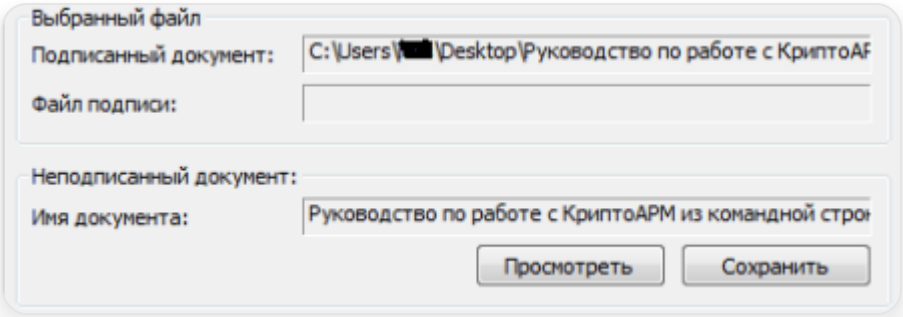
4. Откроется окно **Результат выполнения операции**, в котором отобразится статус операции. Если одна или несколько подписей не действительны, это будет отражено в статусе. Чтобы просмотреть детальную информацию о результатах проверки подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите на кнопку **Детали**.



5. Если вы хотите просмотреть информацию о проверяемой ЭП и сертификате подписчика, выделите необходимую запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**. Откроется окно Управление подписанными данными.

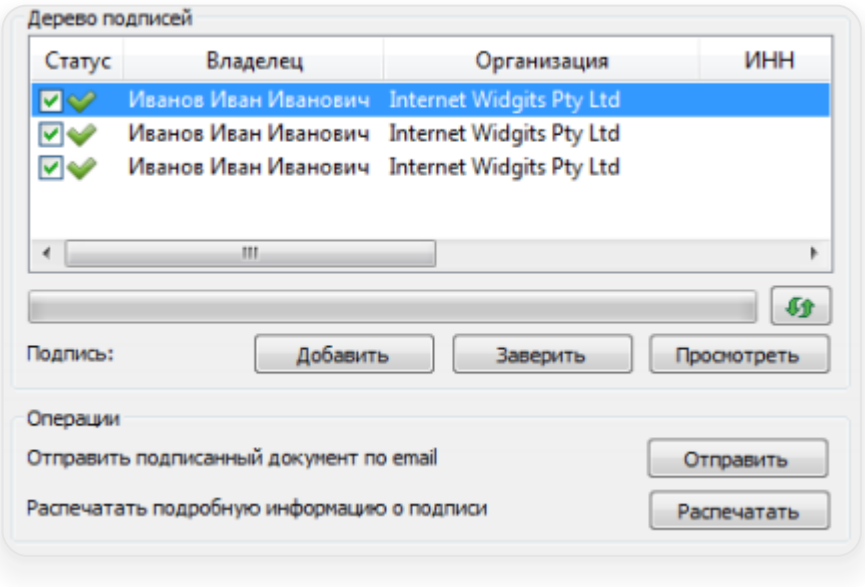


Вы можете просмотреть исходный файл и сохранить его по указанному пути (кнопки **Просмотреть** и **Сохранить** напротив поля **Открытые данные**).



В случае, если просматриваемый документ является документом Microsoft Word или Microsoft Excel, и на компьютере установлен пакет Microsoft Office, можно настроить добавление информации о подписи в конец документа (в случае с Microsoft Excel на отдельный лист). Включить добавление информации о подписи можно в выбранной по умолчанию настройке на странице общих настроек профиля.

Отчет о проверке подписи можно просмотреть, выбрав запись в поле **Дерево подписей** и нажав на кнопку **Просмотреть**. Откроется окно с информацией о подписи, сертификате и его статусе.


Дерево подписей
Статус
Владелец
Организация
ИНН
Иванов Иван Иванович
Internet Widgits Pty Ltd
Иванов Иван Иванович
Internet Widgits Pty Ltd
Иванов Иван Иванович
Internet Widgits Pty Ltd
Подпись:
Добавить
Заверить
Просмотреть
Операции
Отправить подписанный документ по email
Отправить
Распечатать подробную информацию о подписи
Распечатать

Открыть статью на сайте

Снятие и проверка подписи

При проверке совмещенной подписи сначала выполняется снятие подписи с данных и сохранение подписанных данных в отдельный файл, а после этого - собственно проверка корректности подписи.

С помощью программы «КриптоАРМ» вы можете снять и проверить корректность ЭП отдельного файла или папки файлов (при этом будет снята и проверена подпись каждого файла, входящего в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными).

Снять и проверить корректность электронной подписи вы можете через:

- главное окно
- значок на панели задач
- контекстное меню файла

Чтобы снять и проверить корректность электронной подписи, выберите пункт меню **Снять и проверить**. Шаги Помощника данной операции соответствуют шагам Мастера проверки подписи.

Открыть статью на сайте

Как зашифровать данные?

Шифрование — это преобразование данных в вид, недоступный для чтения без соответствующей информации (ключа шифрования). Задача состоит в том, чтобы обеспечить конфиденциальность, скрыв информацию от лиц, которым она не предназначена, даже если они имеют доступ к зашифрованным данным.

Чтобы зашифровать файл, вам потребуется открытый ключ получателя зашифрованных данных. Расшифровать данные получатель сможет, используя свой закрытый ключ.

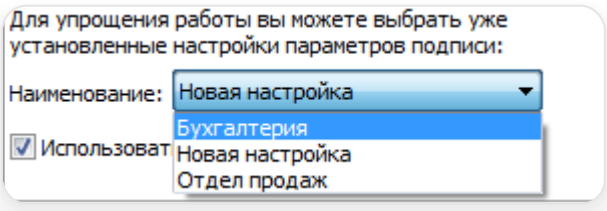
С помощью программы «КриптоАРМ» вы можете зашифровать отдельный файл или папку файлов (при этом будет зашифрован отдельно каждый файл, входящий в указанную папку. Зашифрованные файлы автоматически сохраняются в папку с исходными данными).

Зашифровать файл вы можете через:

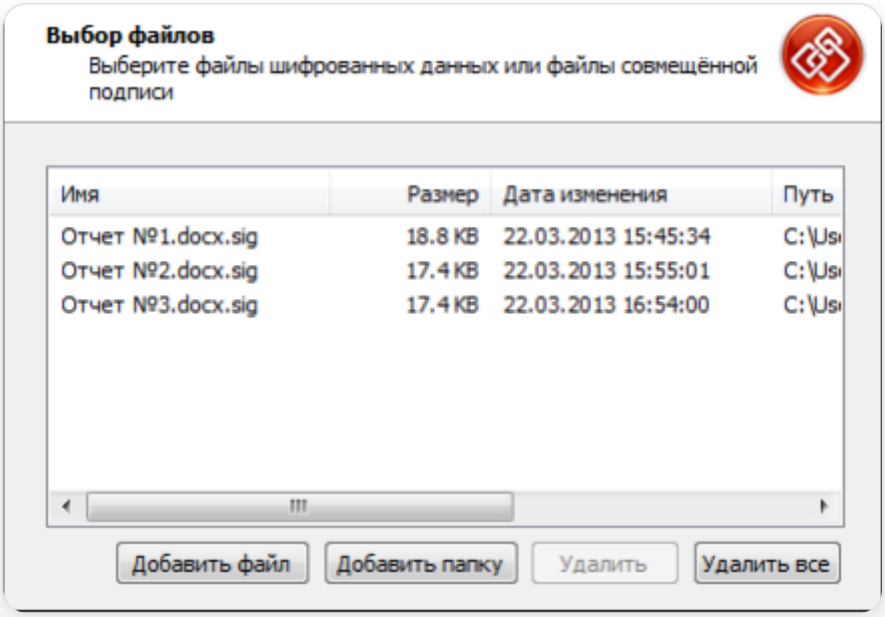
- главное окно
- значок на панели задач
- контекстное меню файла

Чтобы зашифровать файл, следуйте рекомендациям Мастера выполнения операции:

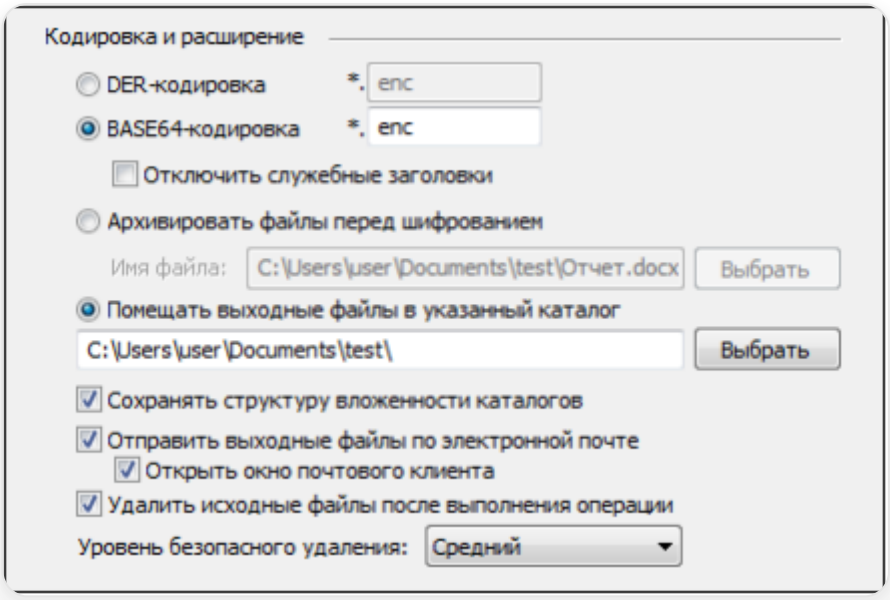
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для шифрования файлов. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите папку с файлами или отдельный файл, которые необходимо зашифровать (кнопки **Добавить папку** и **Добавить файл** соответственно).



3. В открывшемся окне укажите настройки для выходного формата файла.



1) **Кодировка и расширение**;

- DER encoded binary X.509
- Base64 encoded X.509. Для этого варианта кодирования вы можете указать флаг Отключить служебные заголовки. Расширения зашифрованного файла *.enc, *.p7m, *.pem.

2) **Архивировать файлы перед шифрованием**;

В строке Имя файла укажите путь до архива и имя создаваемого архива.

3) **Помещать выходные файлы в указанный каталог**; Если выбрать этот режим и оставить поле ввода пути к каталогу не заполненным, то выходные файлы будут формироваться в каталоге входных файлов.

4) **Сохранять структуру вложенности каталогов**;

5) **Отправить выходные файлы по электронной почте**;

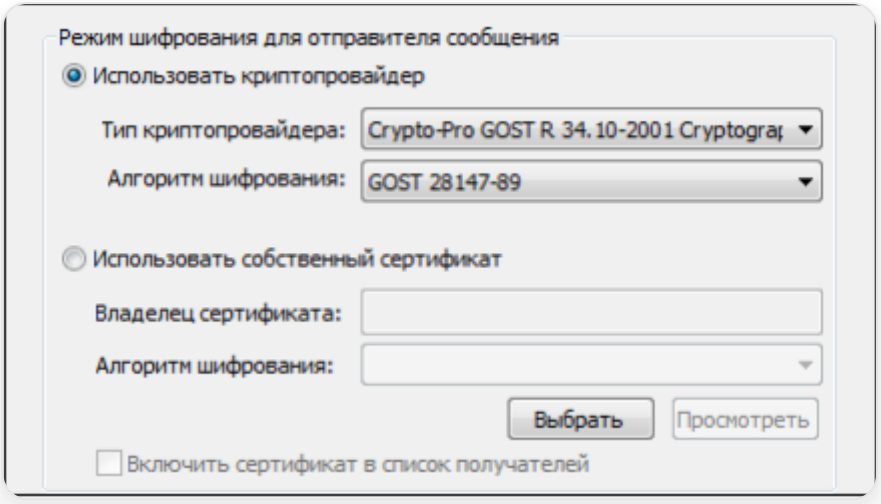
6) **Удалить исходный файл после выполнения операции**; Если вы решили создать файл совмещенной подписи, вы можете удалить исходный файл после выполнения операции.

7) **Уровень безопасного удаления.**
Подробнее о настройке параметров уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.

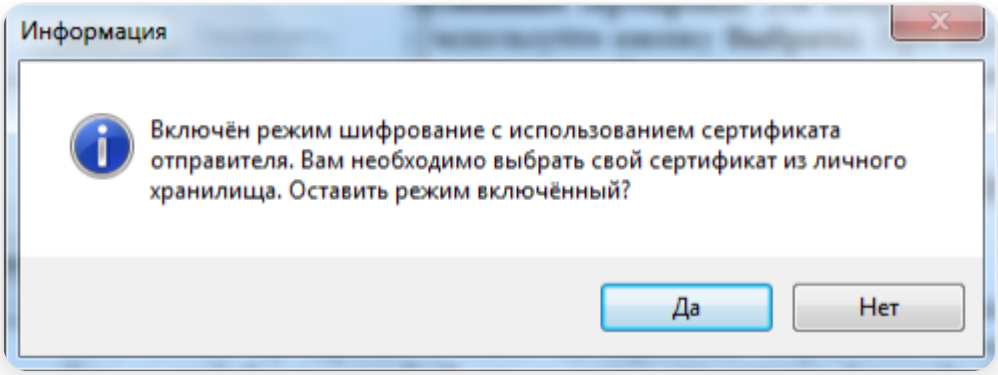
4. В окне **Свойства шифрования** выберите режим шифрования данных.

Для этого поставьте переключатель напротив соответствующей строки:

- **Использовать криптопровайдер** (в этом случае в выпадающем списке выберите необходимый тип криптопровайдера и алгоритм шифрования)

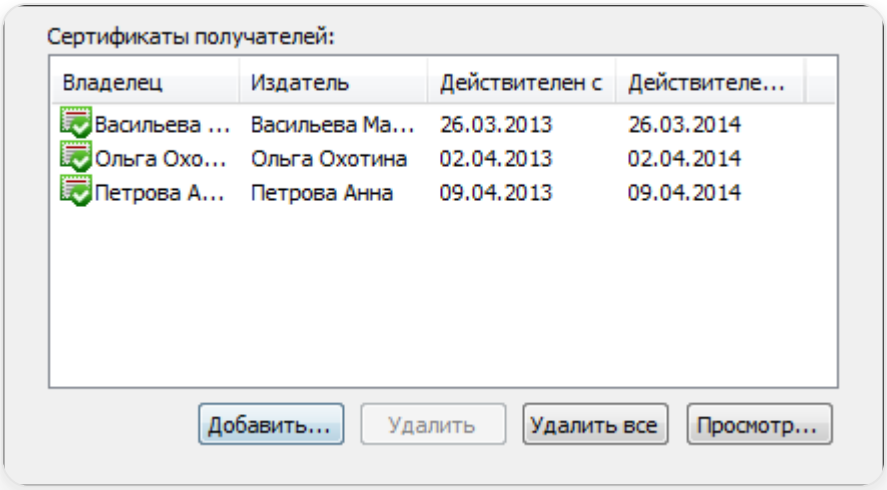


- **Использовать собственный сертификат** для шифрования (Для выбора личного сертификата используйте кнопку **Выбрать**). При выборе личного сертификата проверяется его статус. Личный сертификат автоматически добавляется в список сертификатов получателей шифруемого файла.



Подробнее о настройке параметров шифрования вы можете прочитать в разделе Настройки операции шифрования.

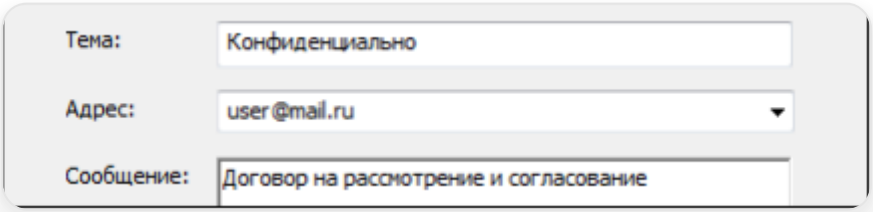
5. На следующем шаге выберите сертификаты получателей шифруемого файла, используя кнопку **Добавить**.



Чтобы иметь возможность расшифровать зашифрованный вами файл, вы должны добавить личный сертификат в список сертификатов получателей зашифрованного файла. Если на предыдущем шаге вы включили режим, при котором для шифрования будет использоваться ваш личный сертификат, на шаге выбора сертификатов получателей он автоматически будет занесен в список.

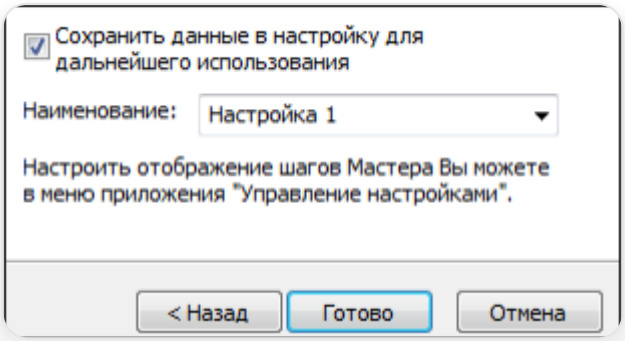
Обратите внимание, для шифрования необходимо, чтобы ключи отправителя и получателя могли быть использованы для шифрования данных.

6. Для отправки зашифрованных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:



7. После завершения сбора параметров для выполнения шифрования возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был зашифрован файл и сертификат получателя (-ей). Для продолжения нажмите на кнопку **Готово**.

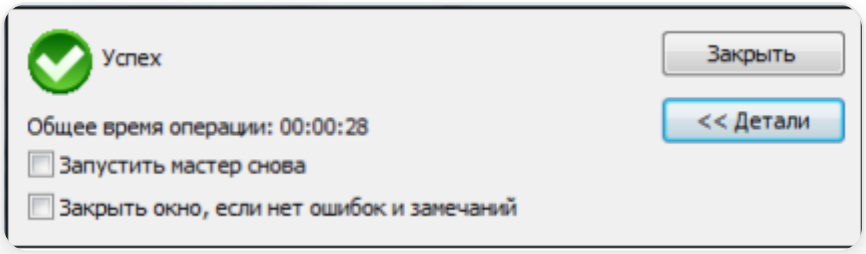
Введенные в Мастер шифрования данные можно сохранить в настройку для дальнейшего использования. Для этого поставьте галочку в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.



8. Начнется процесс шифрования данных. Вы можете прервать его, нажав на кнопку **Отмена**.

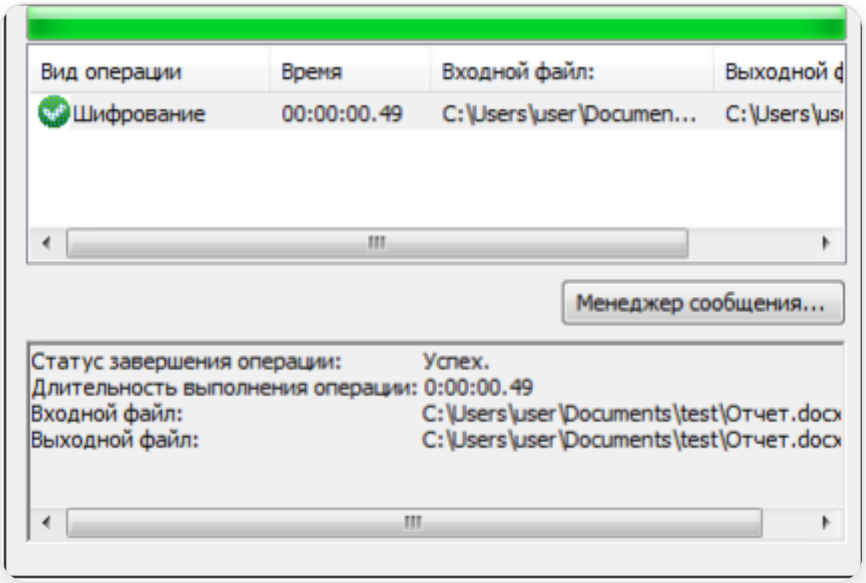
9. При отправке зашифрованных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.

10. Далее возникнет окно **Результат выполнения операции** со статусом завершения операции.



Чтобы просмотреть детальную информацию о результатах шифрования и используемых

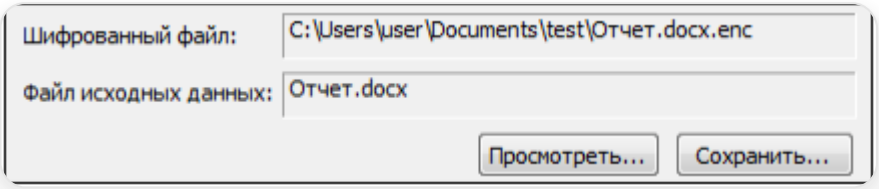
параметрах: имя исходного файла, имя выходного (зашифрованного) файла, статус операции, длительность выполнения операции, нажмите на кнопку **Детали**.



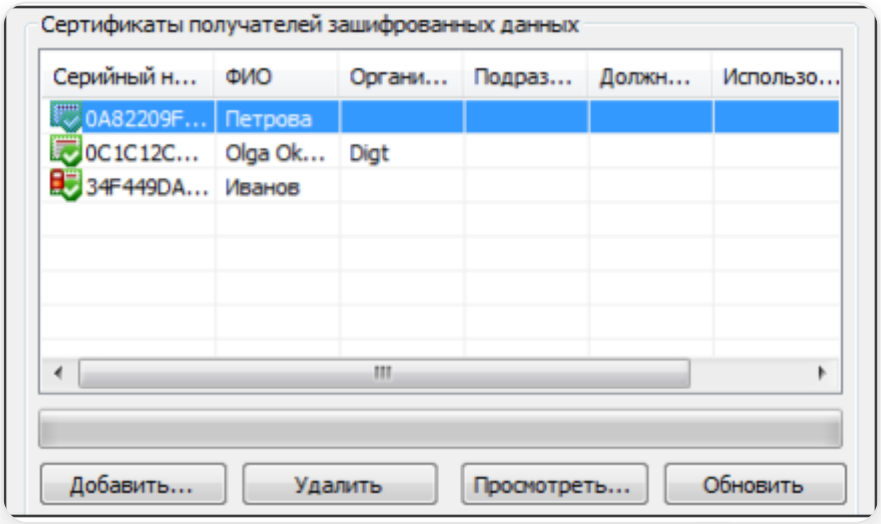
Вы можете отредактировать список получателей зашифрованных данных, просмотреть и сохранить исходные данные.

1. Выделите запись в списке окна Результат выполнения операции и нажмите на кнопку **Менеджер сообщения**.
2. Откроется окно **Управление шифрованными данными**, в котором вы можете:

- просмотреть путь, по которому сохранен зашифрованный файл;
- просмотреть зашифрованный файл (кнопка **Просмотреть** рядом со строкой Файл исходных данных);



- сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**);
- просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**);



Сертификат расшифрования данных отмечается значком - . Сертификатом расшифрования становится первый из списка сертификат получателей, имеющий закрытый ключ. Остальные сертификаты отмечаются стандартными значками.

Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно). При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы в адрес измененного списка получателей.

Открыть статью на сайте

Как расшифровать данные ?

С помощью программы «КриптоАРМ» вы можете расшифровать:

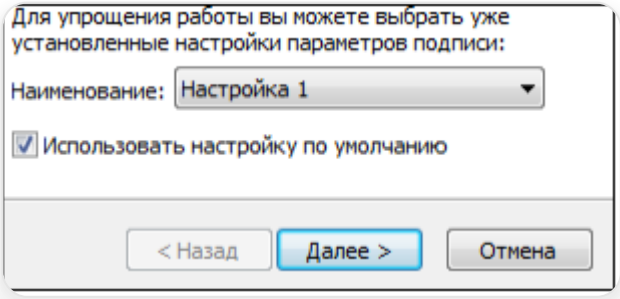
- отдельный файл;
- папку файлов (при этом будет расшифрован каждый файл, входящий в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными).

Расшифровать данные вы можете через:

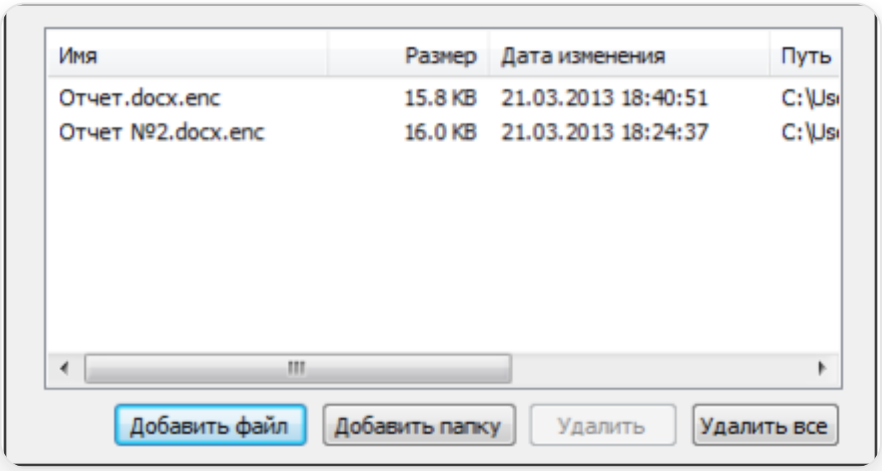
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Расшифровать**. Далее следуйте рекомендациям Помощника по выполнению операции:

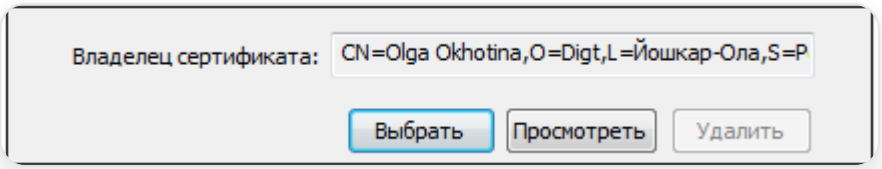
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек расшифрования файлов. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите файл или папку файлов, которые необходимо расшифровать (кнопки **Добавить папку** и **Добавить** файл). Также вы можете выбрать архив с файлами.

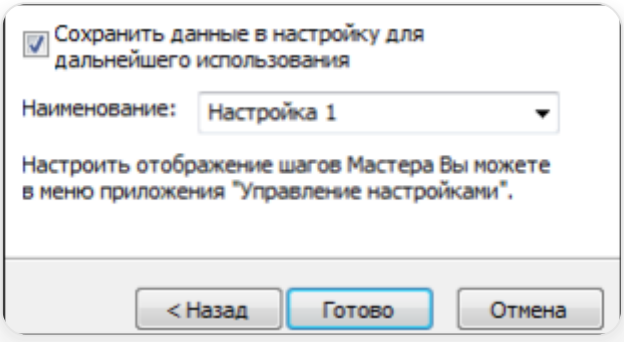


3. В следующем окне выберите предпочтительный сертификат расшифрования (кнопка **Выбрать**). Указанный сертификат вы можете просмотреть, нажав на кнопку **Просмотреть**.



4. После завершения сбора данных для расшифрования возникнет окно с информацией о статусе операции и об используемых параметрах. Для продолжения нажмите на кнопку **Готово**.

Указанные данные можно сохранить в настройку для дальнейшего использования. Для этого поставьте флаг в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.

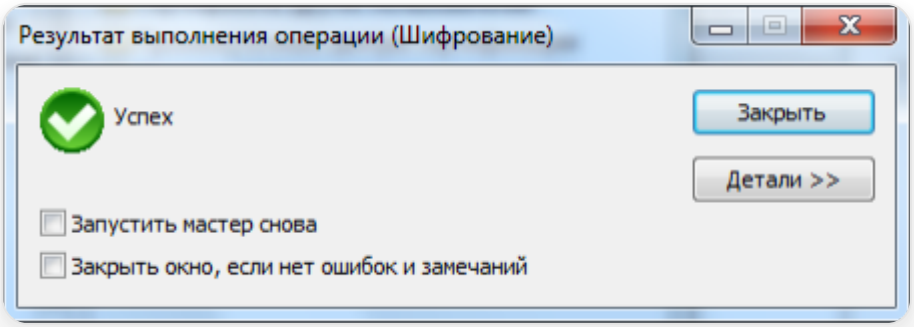


5. Начнется процесс расшифрования файла. Вы можете прервать его, нажав на кнопку **Отменить все**.

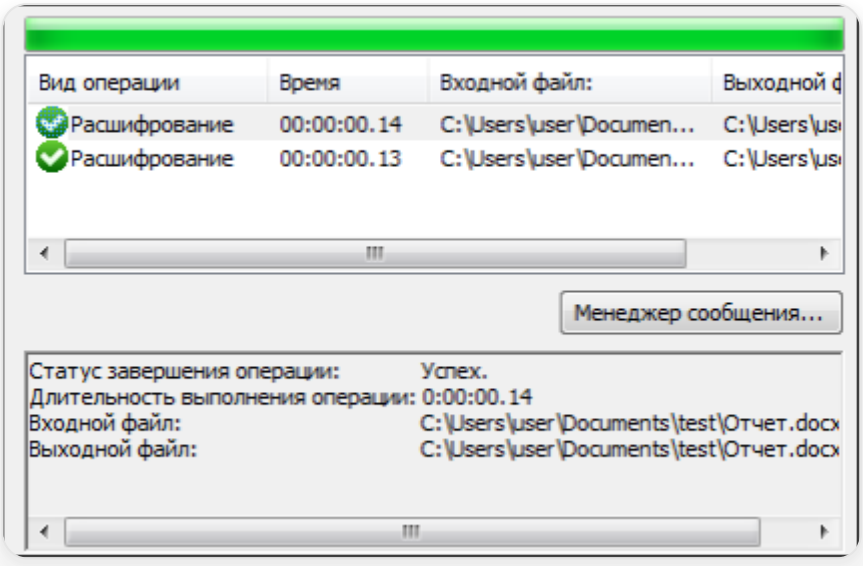
Данные будут расшифрованы и по умолчанию сохранены в тот же каталог, в котором находится исходный (зашифрованный) файл данных. При этом имя расшифрованного файла совпадает с именем зашифрованного файла, но не имеет расширения *.enc. Если файл с таким именем уже существует, сохраните его под другим именем.

Если сертификат ГОСТ, введите пароль доступа к нему.

После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах расшифрования и используемых параметрах: имя исходного файла, имя выходного (расшифрованного) файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали.**

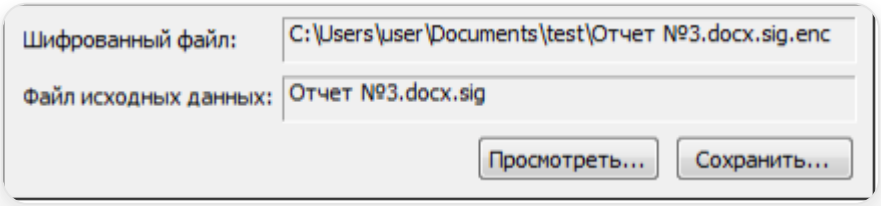


Если вы хотите просмотреть информацию о сертификате расшифрования и сертификатах получателей или изменить список получателей зашифрованных данных, выделите необходимую запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.

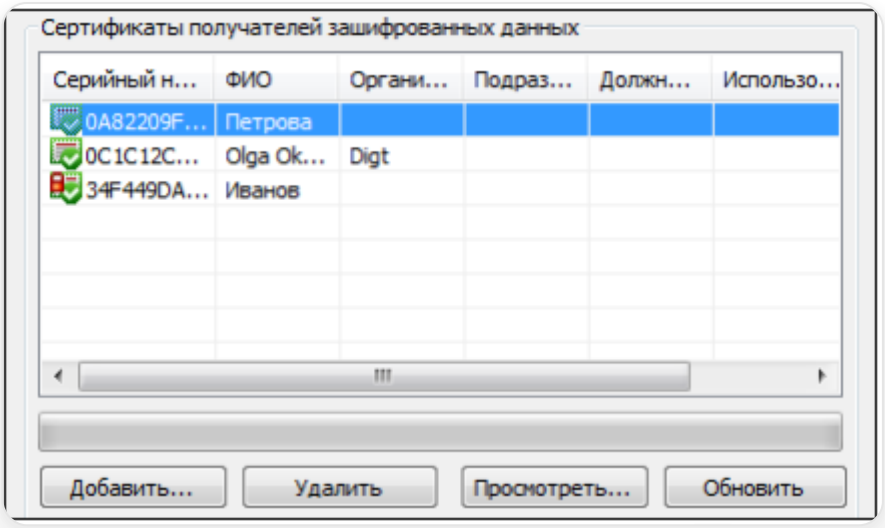


Откроется окно **Управление шифрованными данными**, в котором вы можете:

- просмотреть путь, по которому сохранен зашифрованный файл;
- просмотреть зашифрованный файл (кнопка **Просмотреть** напротив строки **Файл исходных данных**);



- сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**);
- просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**).



Сертификат расшифрования данных отмечается значком - -. Сертификатом расшифрования становится первый из списка сертификат получателя, имеющий закрытый ключ. Остальные сертификаты отмечаются стандартными значками.

Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно). При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы в адрес измененного списка получателей.

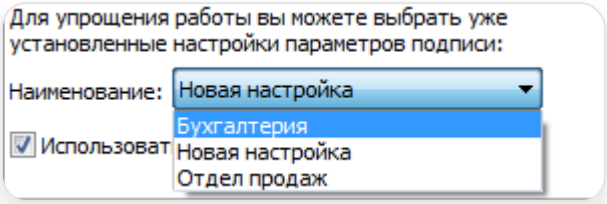
Открыть статью на сайте

Как подписать и зашифровать электронный документ

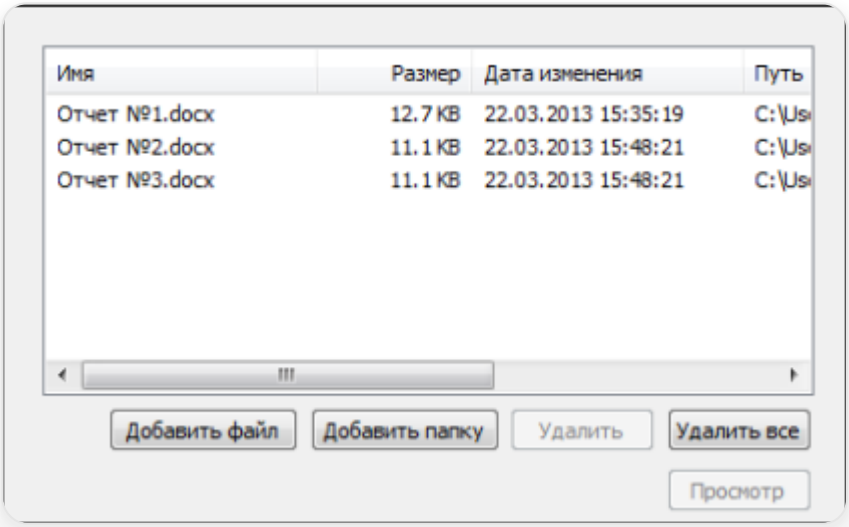
Выберите пункт меню **Подписать и зашифровать** (при этом будет зашифрован и подписан отдельно каждый файл, входящий в указанную папку. Зашифрованные и подписанные файлы автоматически сохраняются в папку с исходными данными).

Далее следуйте рекомендациям Мастера выполнения операции:

1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи и шифрования. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, установите флаг в пункте Использовать настройку по умолчанию.



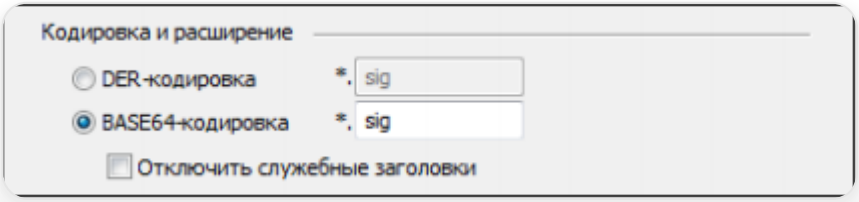
2. Выберите отдельный файл и папку с файлами, которые необходимо зашифровать и подписать (кнопки **Добавить файл** и **Добавить папку** соответственно).



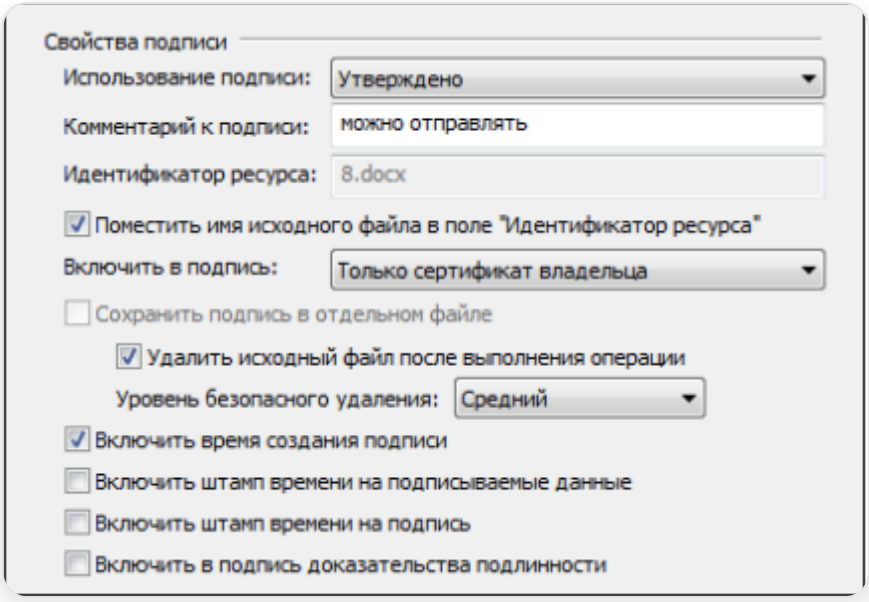
3. Первым этапом укажите параметры для создания электронной подписи данных. Сначала укажите выходной формат файла подписи: кодировку и расширение выходного файла.

- **DER** encoded binary X.509. Расширения подписанного файла *.sig, *.p7s.
- **Base64** encoded X.509.Для этого варианта кодирования вы можете указать флаг Отключить служебные заголовки. Расширения подписанного файла *.sig.

Отключить служебные заголовки. Расширения подписанного файла *.sig.



4. Далее установите параметры подписи.



Использование подписи. Укажите необходимое назначение подписи. О том, как создавать новые назначения вы можете узнать в разделе Операции со справочниками назначений.

Комментарий к подписи. Комментарием к подписи может служить информация, предназначенная людям, просматривающим подписанный документ (например, "Согласовано!").

Включить в подпись:
- только сертификат владельца - режим, установленный по умолчанию. В атрибуты подписи добавляется единственный сертификат;
- путь сертификации без корневого сертификата - в атрибуты подписи добавляется цепочка сертификатов, за исключением корневого сертификата;

- все сертификаты пути сертификации - в атрибуты подписи добавляется вся цепочка сертификатов, в том числе и корневой сертификат;
- не включать сертификаты в подпись - в атрибуты подписи не включаются сертификаты.

Идентификатор ресурса.

Удалить исходный файл после выполнения операции. Если вы решили создать файл совмещенной подписи, вы можете удалить исходный файл после выполнения операции.

Уровень безопасного удаления. Подробнее о настройках уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.

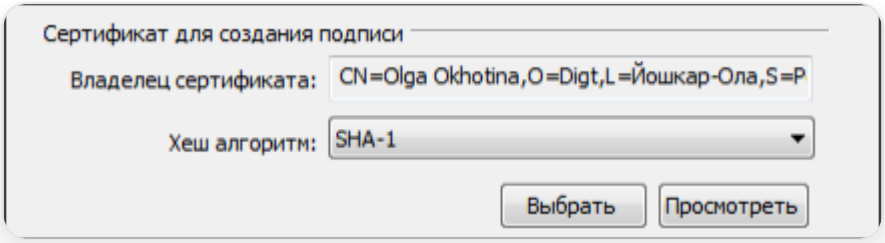
Включить время создания подписи. При установке флага - в файл подписи будет включено время подписи.

Флаги **Включить штамп времени на подписываемые данные** и **Включить штамп времени на подпись**, доступны только при установленной лицензии на модуль TSP (КриптоПро TSP client 2.0.)

Флаг **Включить в подпись доказательства подлинности** доступен только при установленной лицензии на модули TSP и OCSP (КриптоПро TSP client 2.0 и КриптоПро OCSP client 2.0.)

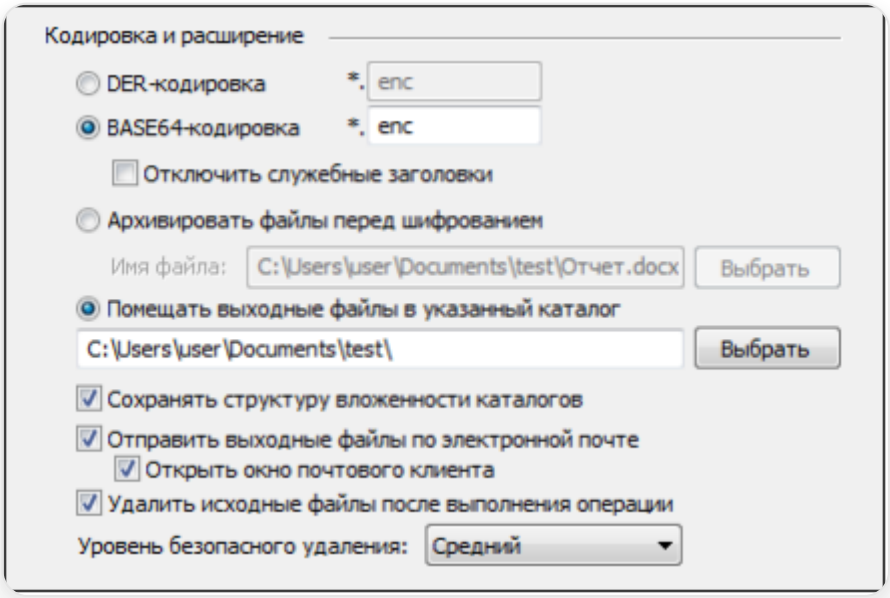
5. Если был установлен флаг **Включить в подпись Штамп Времени**, в следующем окне укажите параметры Службы Штампов Времени.

6. Выберите личный сертификат для создания ЭП (кнопка **Выбрать**).



7. Для доступа к выбранному ключевому контейнеру (ГОСТ сертификата) введите пароль.

8. Вторым этапом укажите параметры для шифрования данных. Укажите настройки для выходного формата файла.



Кодировка и расширение.

- **DER** encoded binary X.509
- **Base64** encoded X.509.Для этого варианта кодирования вы можете указать флаг **Отключить служебные заголовки**. Расширения зашифрованного файла *.enc, *.p7m, *.pem.

Архивировать файлы перед шифрованием.
В строке **Имя файла** укажите путь до архива и имя создаваемого архива.

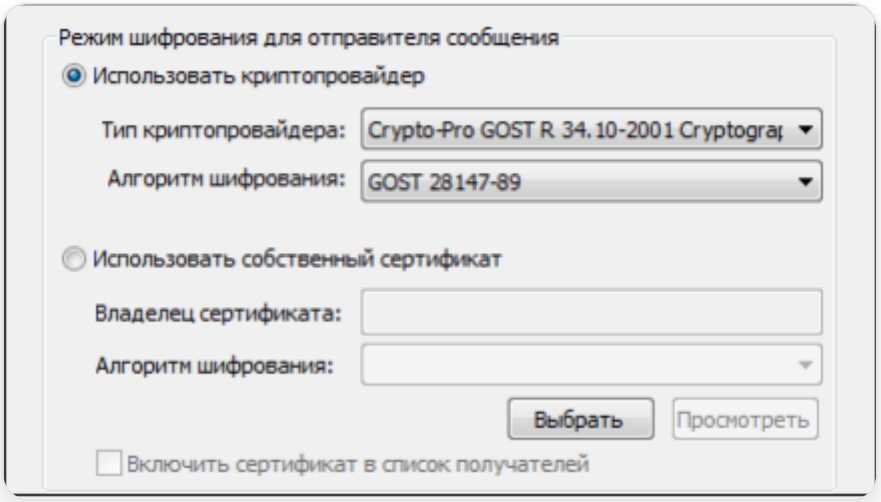
Помещать выходные файлы в указанный каталог.
Если выбрать этот режим и оставить поле ввода пути к каталогу не заполненным, то выходные файлы будут формироваться в каталоге входных файлов.

Сохранять структуру вложенности каталогов.

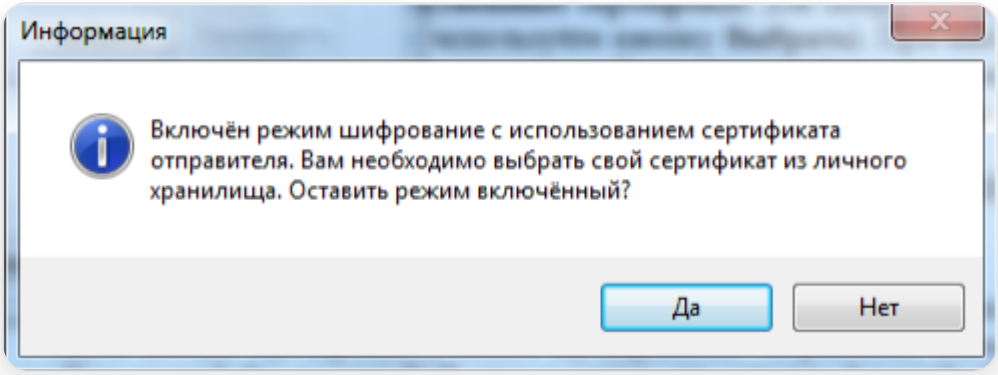
Отправить выходные файлы по электронной почте.

В окне **Свойства шифрования** выберите режим шифрования данных. Для этого поставьте переключатель напротив соответствующей строки:

- **Использовать криптопровайдер** (в этом случае в выпадающем списке выберите необходимый тип криптопровайдера и алгоритм шифрования).



- **Использовать собственный сертификат для шифрования** (Для выбора личного сертификата используйте кнопку **Выбрать**). При выборе личного сертификата проверяется его статус. Личный сертификат автоматически добавляется в список сертификатов получателей шифруемого файла.

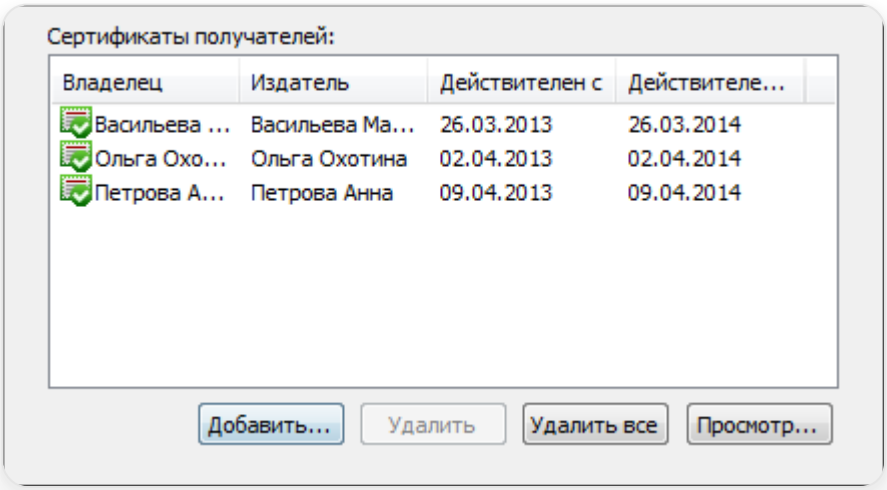


Подробнее о настройке параметров шифрования вы можете прочитать в разделе Настройки операции шифрования.

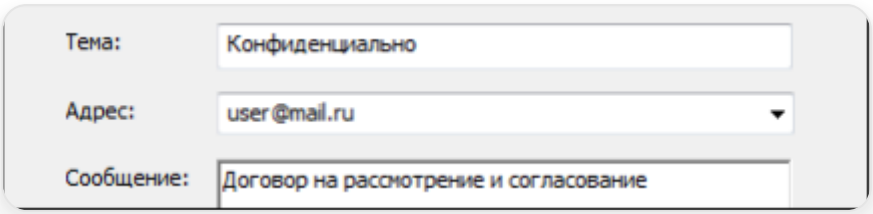
9. На следующем шаге выберите сертификаты получателей шифруемого файла, используя кнопку **Добавить**.

Чтобы иметь возможность расшифровать зашифрованный вами файл, вы должны добавить личный сертификат в список сертификатов получателей зашифрованного файла. Если на предыдущем шаге вы включили режим, при котором для шифрования будет использоваться ваш личный сертификат, на шаге выбора сертификатов получателей он автоматически будет занесен в список.

Обратите внимание, для шифрования необходимо, чтобы ключи отправителя и получателя могли быть использованы для шифрования данных.

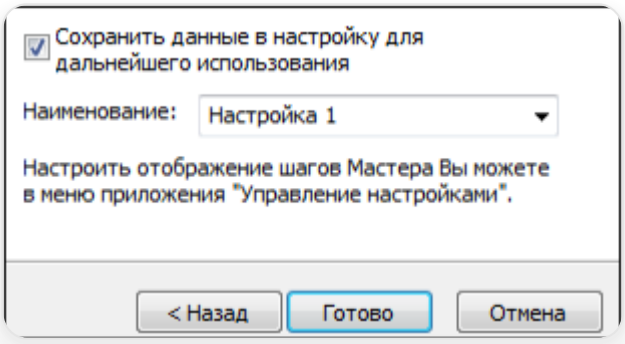


10. Для отправки подписанных и зашифрованных данных по электронной почте укажите тему сообщения, адрес получателя и текст письма:



11. После завершения сбора параметров для выполнения шифрования возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был зашифрован файл и сертификат получателя (-ей). Для продолжения нажмите кнопку **Готово**.

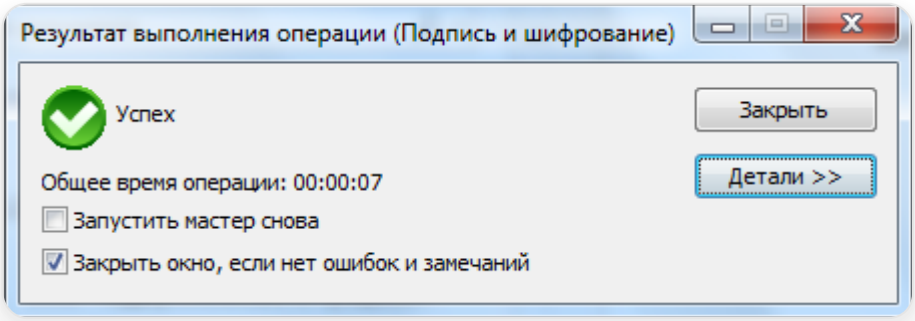
Все указанные параметры можно сохранить в настройку для дальнейшего использования. Для этого установите флаг в пункте **Сохранить данные в настройку для дальнейшего использования** и введите наименование настройки. Также вы можете сохранить все данные в уже существующую настройку, выбрав ее название из списка.



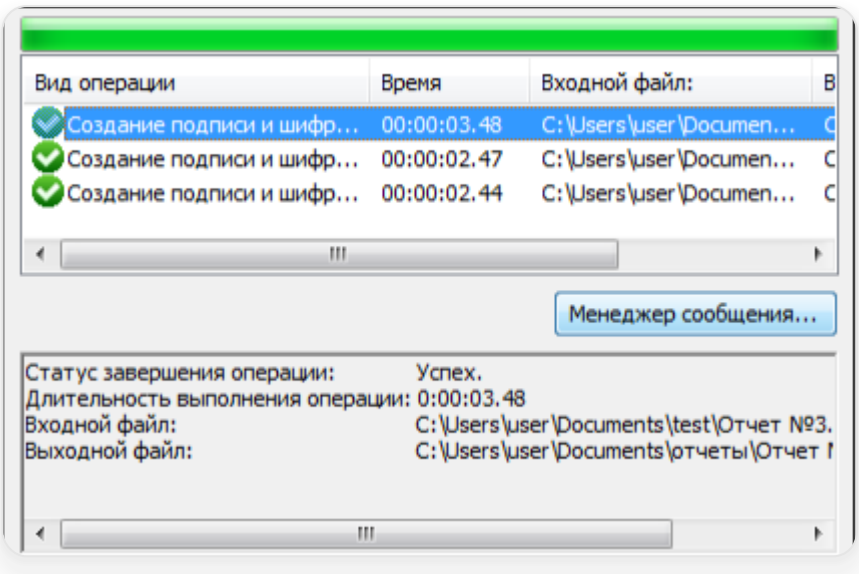
12. Начнется процесс подписи и шифрования файла. Вы можете прервать его, нажав на кнопку **Отмена**.

13. При отправке подписанных и зашифрованных данных по электронной почте (если вы указали "Открыть окно почтового клиента") откроется окно вашего почтового клиента для редактирования сообщения перед отправкой. Внесите необходимые изменения и отправьте письмо стандартным образом.

14. Далее возникнет окно **Результат выполнения операции** со статусом завершения операции.



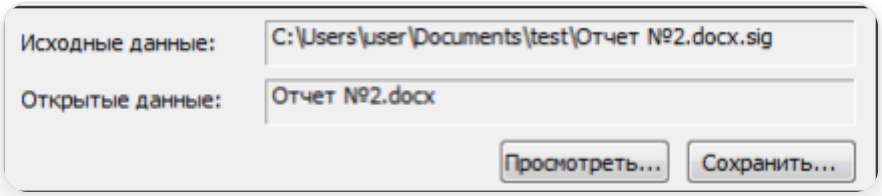
Чтобы просмотреть детальную информацию о результатах шифрования и используемых параметрах: имя исходного файла, имя выходного (зашифрованного) файла, статус операции, длительность выполнения операции, нажмите кнопку **Детали**.



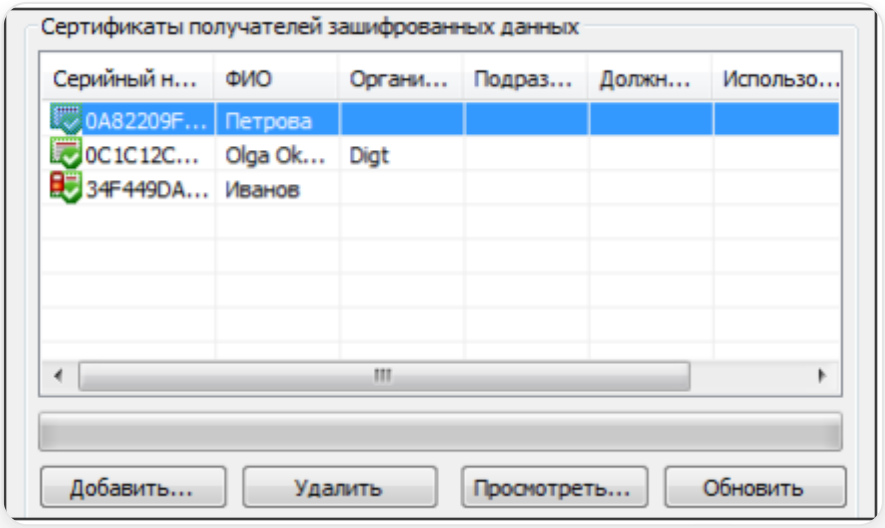
Вы можете отредактировать список получателей зашифрованных и подписанных данных, просмотреть и сохранить исходные данные.

1. Выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.
2. Откроется окно **Управление шифрованными данными**, в котором вы можете:

- Просмотреть путь, по которому сохранен зашифрованный файл;
- Просмотреть зашифрованный файл (кнопка **Просмотреть** напротив строки **Файл исходных данных**);
- Сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**);
-



- Просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**);



Сертификат расшифрования данных отмечается значком - . Сертификатом расшифрования становится первый из списка сертификат получателей, имеющий закрытый ключ. Остальные сертификаты отмечаются стандартными значками.

Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно). При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы и подписаны в адрес измененного списка получателей.

Открыть статью на сайте

Как расшифровать и проверить подпись на электронном документе?

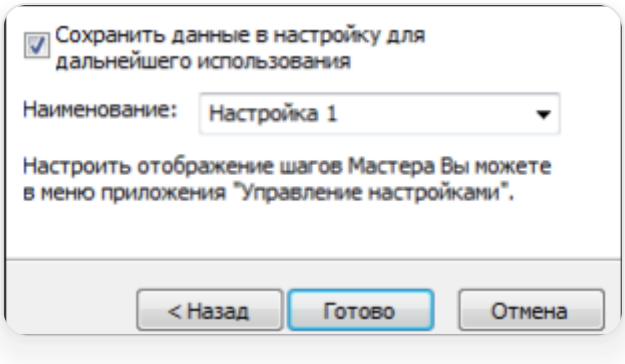
С помощью программы «КриптоАРМ» вы можете расшифровать и проверить ЭП отдельного файла или группы файлов, папку с файлами (при этом каждый файл, входящий в указанную папку, будет расшифрован и проверена подпись) или зашифрованные архивы.

Расшифровать файл и проверить электронную подпись за одну операцию вы можете через:

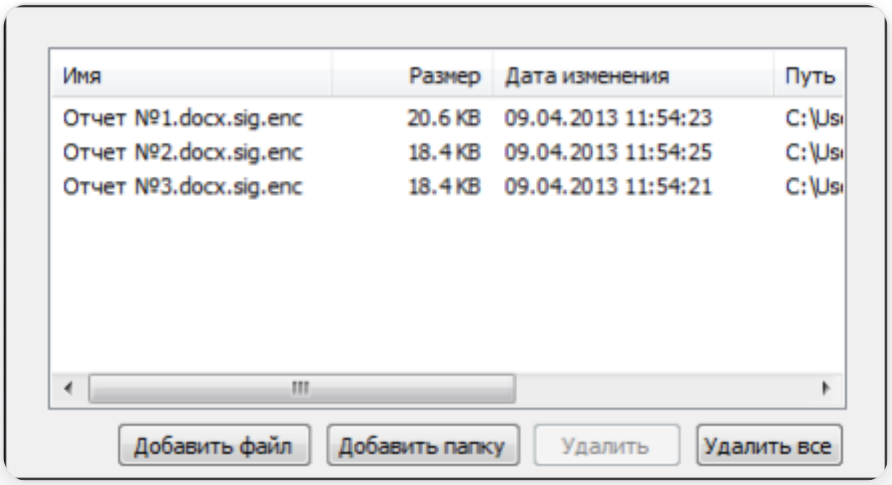
- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Расшифровать и проверить подпись**. Далее следуйте рекомендациям Мастера по выполнению операции:

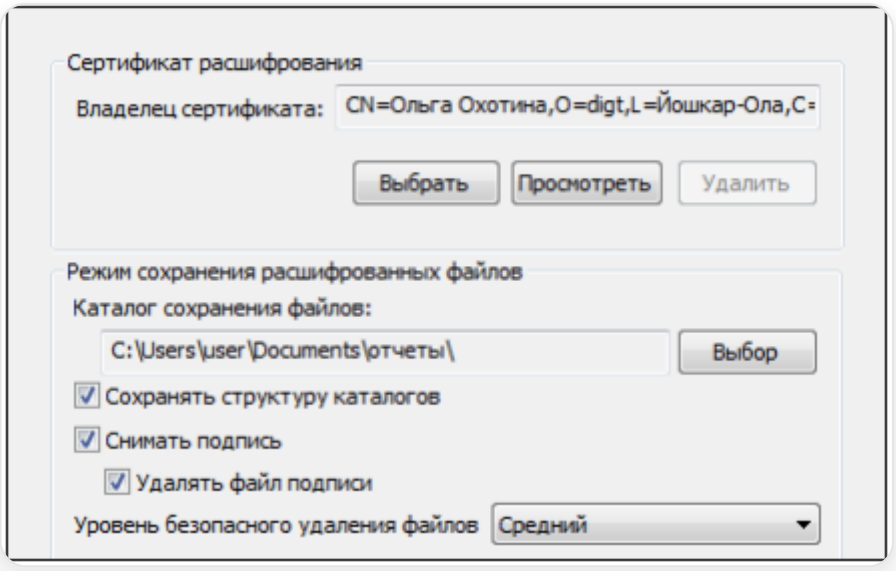
1. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек подписи и расшифрования. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**.



2. Выберите один или несколько файлов с зашифрованными и подписанными данными (кнопки **Добавить файл** / **Добавить папку**).



3. В следующем окне выберите предпочтительный сертификат расширования (кнопка **Выбрать**). Указанный сертификат вы можете просмотреть, нажав на кнопку **Просмотреть**.



В данном окне также можно выбрать:

Каталог сохранения файлов. Если поле каталога оставить пустым, то по результатам операции файлы будут сохранены в текущем каталоге.

Сохранить структуру каталогов - при включении сохраняет структуру каталогов для выбранных файлов.

Снимать подпись - при проверке отделяет файл подписи от исходного файла.

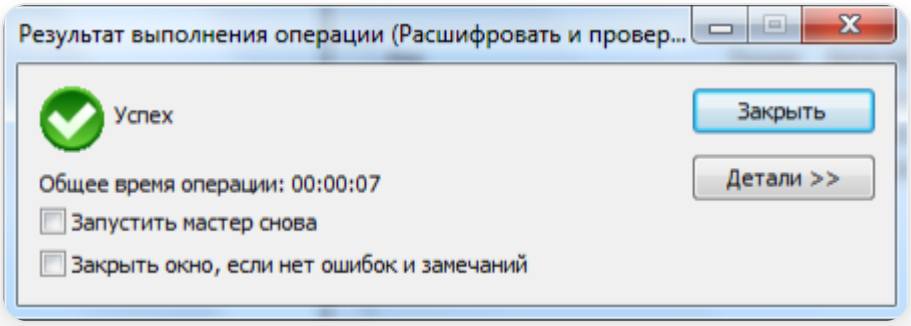
Удалять файл подписи - после снятия подписи удаляет файл подписи, оставляя только исходный файл.

Уровень безопасного удаления файлов. Подробнее о настройках уровня безопасного удаления читайте в разделе Настройки каталогов хранения файлов.

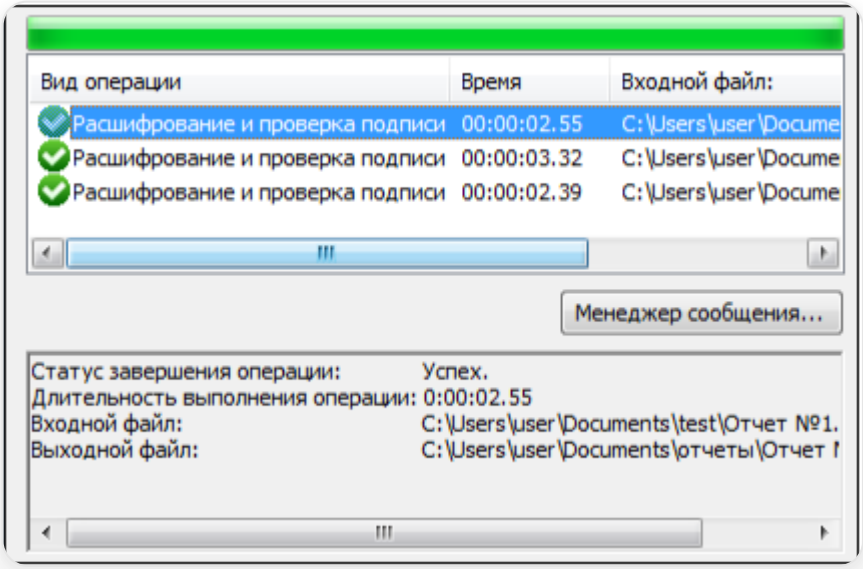
4. После завершения сбора данных для расшифрования и проверки подписи возникнет окно с информацией о статусе операции и об используемых параметрах. Для продолжения нажмите на кнопку **Готово**.

5. Данные будут расшифрованы и по умолчанию сохранены в тот же каталог, в котором находится исходный файл данных. Имя нового файла совпадает с именем подписанного и зашифрованного файла (только без дополнительного расширения). Если файл с таким именем уже существует, сохраните его под другим именем. Далее проверяется корректность ЭП и действительность сертификата отправителя.

6. После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах проверки подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали**.



Если вы хотите просмотреть информацию об ЭП и сертификате подписчика, выделите запись в списке окна Результат выполнения операции и нажмите на кнопку **Менеджер сообщения**.

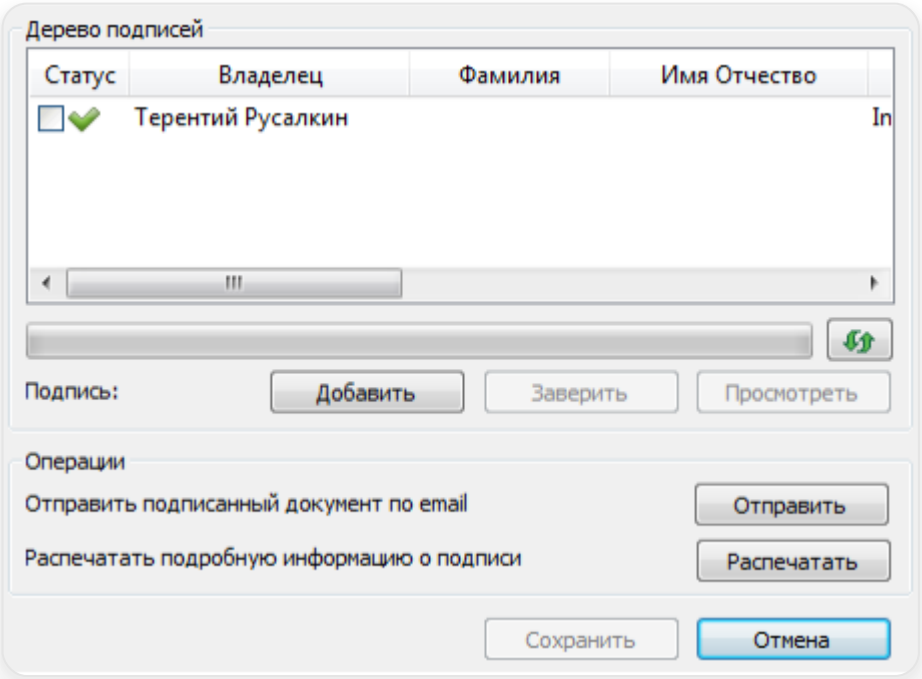


Откроется окно **Управление подписанными данными**, в котором вы можете:

- просмотреть подписанные данные (кнопка **Просмотреть** напротив имени файла) и сохранить их на локальный компьютер или отчуждаемый носитель (кнопка **Сохранить**).
- просмотреть следующую информацию (кнопка **Просмотреть**):

> - о добавленной к файлу электронной подписи;
> - о сертификате, с помощью которого был подписан файл, и его статусе;
> - о штампах времени на подпись и подписываемые данных.

- добавить подпись.
- заверить подпись (обратите внимание, что дерево подписей только двухуровневое, т.е. заверить заверяющую ЭП уже нельзя).
- распечатать информацию (кнопка **На печать**) о ЭП - в новом окне браузера MS IE будет сформирована печатная форма с информацией о подписи.



- отправить по электронной почте.

Открыть статью на сайте

Как просмотреть зашифрованный документ?

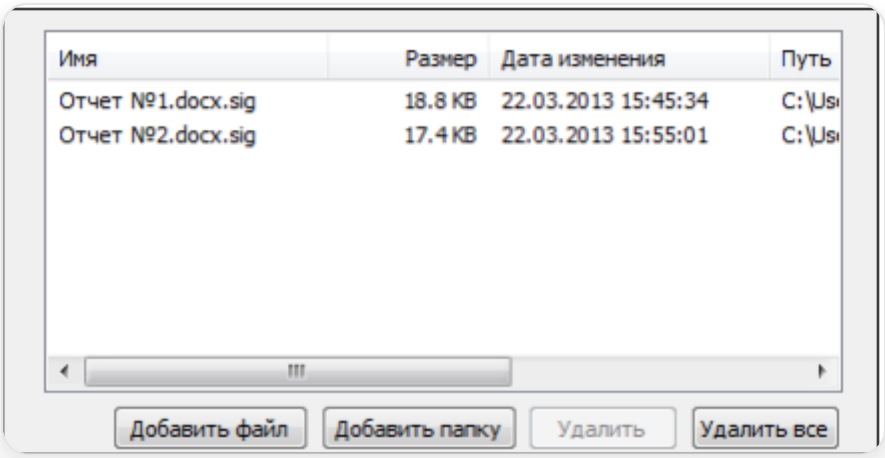
Программа «КриптоАРМ» позволяет просматривать исходные данные зашифрованного файла или файла, содержащего совмещенную подпись.
Для просмотра исходных данных зашифрованного документа, необходимо иметь сертификат расшифрования.

Просмотреть исходные данные зашифрованного файла или файла, содержащего электронную подпись, вы можете через:

- главное окно
- значок на панели задач
- контекстное меню файла

Выберите пункт меню **Просмотреть документ**. Далее следуйте рекомендациям Мастера выполнения операции:

1. Выберите один или несколько файлов, которые необходимо просмотреть (кнопки **Добавить файл** и **Добавить папку** соответственно)



2. После завершения сбора параметров для выполнения операции возникнет окно с информацией о статусе операции. Для продолжения нажмите на кнопку **Готово**.

3. Исходные данные документа будут открыты для просмотра.

Открыть статью на сайте

Как получить штамп в службе штампов времени?

Кроме заверения документов электронной подписью, вы можете удостоверять точное время их создания. Это позволяет предотвращать возможные конфликты при обмене документами между партнерами, коллегами и т.п.

Использование штампов времени в электронном документообороте позволяет создавать официальное доказательство факта существования документа на определённый момент времени.

Модуль поддержки Службы Штампов времени (TSA). «**КриптоАРМ Стандарт Модуль TSP**» поддерживает работу с сервисом Служба штампов времени российского разработчика средств криптографической защиты информации — компании «КриптоПро».

В случае работы со сторонним сервисом штампов времени дополнительно устанавливать ничего не требуется.

Если вы хотите использовать собственный сервис штампов времени, то необходима покупка сервера службы Штампов Времени, например, от компании «КриптоПро» - КриптоПро TSP Server.
Если планируется использовать ГОСТ алгоритмы, то необходима покупка ГОСТового криптопровайдера «КриптоПро CSP»(КриптоПро CSP 4 или КриптоПро CSP 5.)

Схема получения штампа времени:

1. Настройте параметры для работы со Службой штампа времени.

2. Получить штамп времени на документ вы можете во время операции электронной подписи документа.

3. В финальном окне операции электронной подписи документа или операции проверки электронной подписи документа вы можете просмотреть информацию штампа времени, сформированную на подписанном документе.

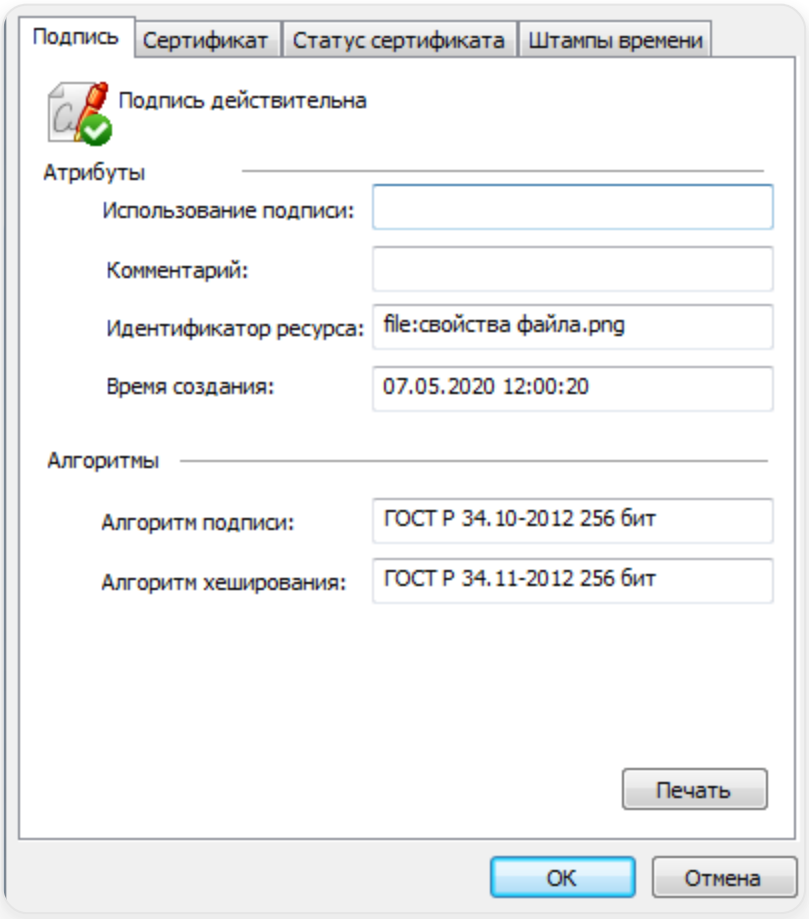
Открыть статью на сайте

Как просмотреть штамп времени?

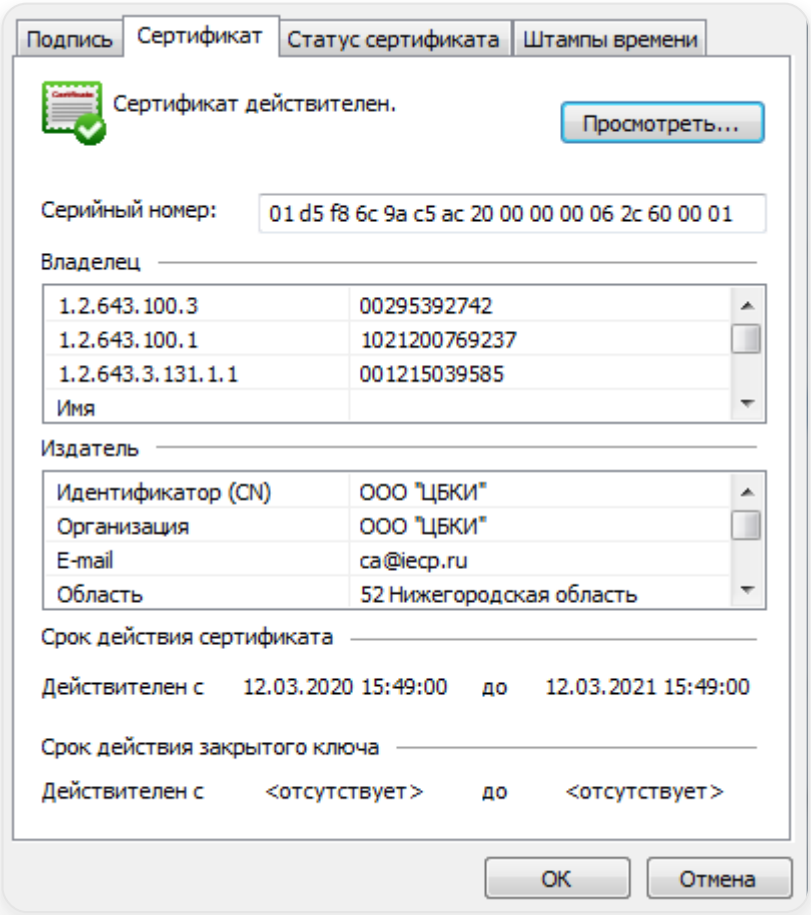
В окне **Управление подписанными данными** откройте информацию о подписи (двойным кликом на ней или нажав на кнопку **Просмотреть**).

Вы увидите следующие закладки:

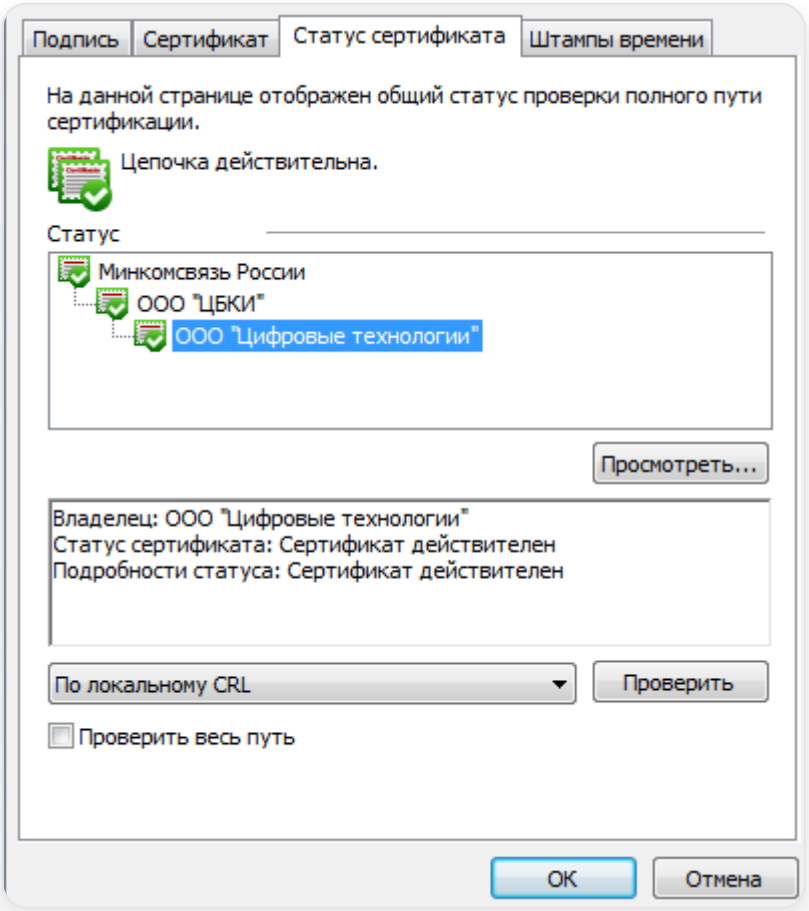
Подпись - в ней содержится информация об атрибутах подписи, времени ее создания, используемых алгоритмах подписи и хеширования.



Сертификат - содержит информацию о сертификате: статус сертификата /действителен и др./, номер, данные о владельце и издателе, сроках действия сертификата и его использовании.

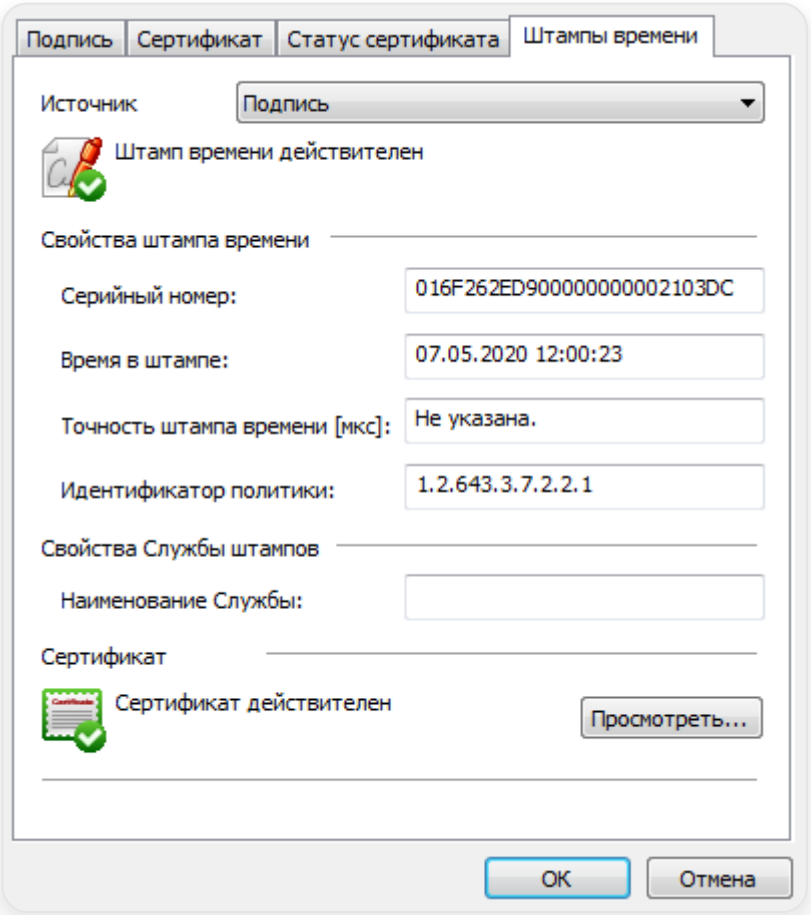


Статусы сертификата - включает общий статус проверки полного пути сертификации (о статусах сертификата читайте подробнее в главе Проверка статуса сертификата.). Кроме этого, в закладке вы можете установить способ, каким проверять статус сертификатов (по локальному СОС, по СОС, полученного из УЦ, с использованием Revocation Provider, проверить в OCSP службе).



Штампы времени - содержит:

- свойства штампа времени (время в штампе, точность штампа времени (мкс), идентификатор политики);
- свойства Службы штампов времени (наименование службы);
- сертификат Службы (содержится в том случае, если во время подписи документа в качестве одного из параметров штампа времени вы указали Запросить сертификат Службы штампов времени).

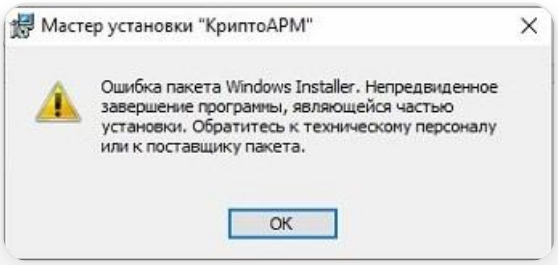

Подпись
Сертификат
Статус сертификата
Штампы времени
Источник
Подпись
Штамп времени действителен
Свойства штампа времени
Серийный номер:
016F262ED900000000002103DC
Время в штампе:
07.05.2020 12:00:23
Точность штампа времени [мкс]:
Не указана.
Идентификатор политики:
1.2.643.3.7.2.2.1
Свойства Службы штампов
Наименование Службы:
Сертификат
Сертификат действителен
Просмотреть...
OK
Отмена

Открыть статью на сайте

Ошибка пакета Windows installer

Текст ошибки:
Ошибка пакета Windows installer. Непредвиденное завершение программы, являющейся частью установки. Обратитесь к техническому персоналу или к поставщику пакета.

Как выглядит ошибка:



Решение

Скачайте утилиту для удаления программы.

После того как запустите утилиту cryptoarm.remover, перезагрузите компьютер и начните установку программы КриптоАРМ без дополнительных модулей TSP и OCSP.

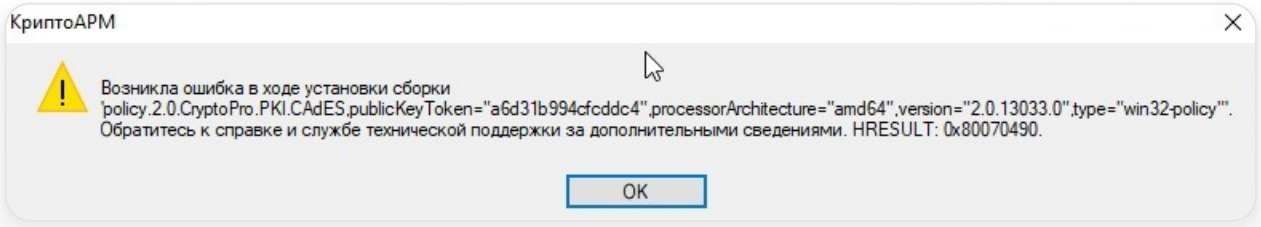
Для этого запустите установку КриптоАРМ-а, выберите не быструю установку, а настраиваемую и отключите эти модули.

Открыть статью на сайте

Ошибка в ходе установки сборки

Текст ошибки:
Возникла ошибка в ходе установки сборки 'CryptoProASN1,publicKeyToken=@a6d31b994cfcddc4",processorArchitecture="amd64", version="2.0.11452.0",type="win32"'Обратитесь к службе технической поддержки за дополнительными сведениями. HRESULT: 0x800708C9.

Как выглядит ошибка:



Решение

КриптоАРМ не устанавливается из-за ошибок установщика Windows, возникающих при установке распространяемых пакетов Microsoft, включенных в состав дистрибутива КриптоАРМ. Если попробовать установить эти пакеты отдельно, возникнет такая же ошибка. Скачать их можно с сайта производителя по следующей ссылке:

Распространяемый пакет Microsoft Visual Studio 2015, 2017, 2019 и 2022.

Исправить эти ошибки иногда помогают системные инструменты DISM и SFC. Приводим небольшую инструкцию по их использованию.

Запустите от имени администратора консоль (в меню **Пуск** в поиске введите **cmd**, вызовите на найденном приложении правой кнопкой мыши контекстное меню и выберите пункт **Выполнить от имени администратора**) и выполните в ней следующие команды:

DISM.exe /Online /Cleanup-image /Scanhealth

DISM.exe /Online /Cleanup-image /Restorehealth

Если они не помогут, попробуйте выполнить так же в консоли администратора команду

SFC /scannow

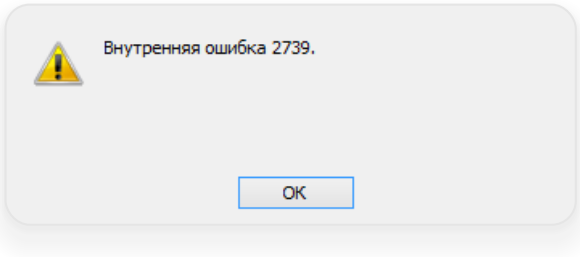
Подробную инструкцию по использованию этой команды можно увидеть на сайте Microsoft.

Открыть статью на сайте

Внутренняя ошибка 2739

Текст ошибки:
Внутренняя ошибка 2739.

Как выглядит ошибка:



Решение

Необходимо запустить утилиту "**Выполнить**" сочетанием клавиш **Win + R** (клавиша Win находится между кнопками Ctrl и Alt слева от Пробела) и выполнить следующие команды с правами администратора:

Если операционная система 64-битная, то в появившейся строке вписать:

c:\windows\SysWOW64\regsvr32 c:\windows\SysWOW64\vbscript.dll

И нажать кнопку **Ок** или клавишу **Enter**

Так же выполнить команду:

c:\windows\SysWOW64\regsvr32 c:\windows\SysWOW64\jscript.dll

Для 32 разрядных систем то же самое, только без команд с syswow64:

c:\windows\System32\regsvr32.exe c:\windows\System32\vbscript.dll

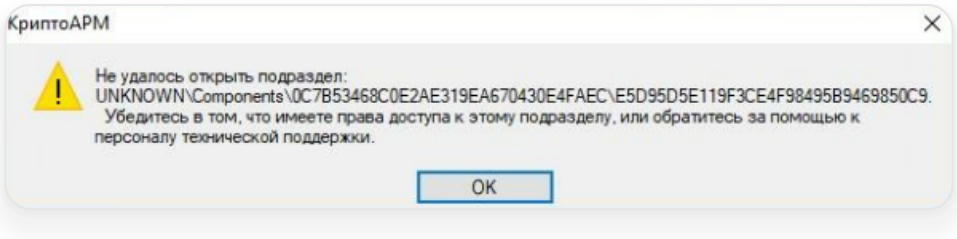
c:\windows\System32\regsvr32.exe c:\windows\System32\jscript.dll

Открыть статью на сайте

Не удалось открыть подраздел: UNKNOWN/Components

Текст ошибки:
Не удалось открыть подраздел `UNKNOWN\Components\0C7B54368C0E2AE319EA670430E4FAEC\E5D95D5E119F3CE4F98495B9469850C9`.
Убедитесь в том, что имеете права доступа к этому подразделу, или обратитесь за помощью к персоналу технической поддержки.

Как выглядит ошибка:



Решение

Чаще всего ошибка возникает в том случае, если на пк установлен антивирус 360. Отключите его на время установки или следуйте далее.

Нужно дать полные права на ветку

HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Installer\UserData\S-1-5-18\Components\B605419A1EFE72D5AD47173A/E5D95D5E119F3CE4F98495B9469850C9.

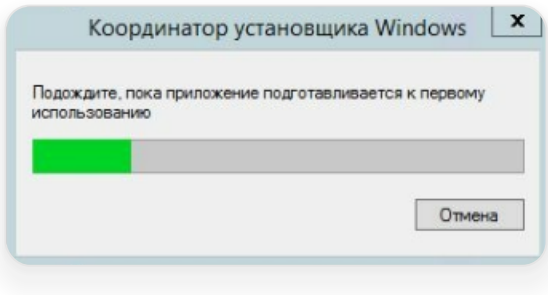
Или временно отключите установленный антивирус.

Открыть статью на сайте

Координатор установщика Windows

Текст ошибки:
Координатор установщика Windows. Выполняется подготовка к первому использованию приложения, подождите.

Как выглядит ошибка:



Решение

Подобное сообщение может говорить о проблемах со службой установки Windows.

Попробуйте её перезапустить (в окне Администрирование компьютера в разделе "Службы и приложения"→"Службы"). Также можно попробовать применить средство исправления ошибок обновления.
Оно предназначено для настольных систем, а не для серверных.

Для серверных систем есть рекомендации по исправлению ошибки в статье.

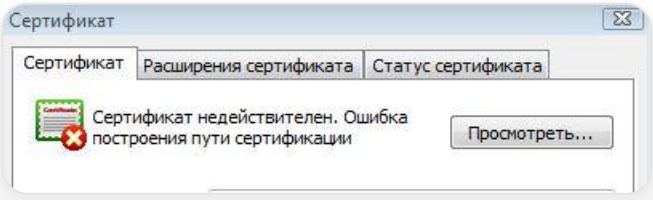
Открыть статью на сайте

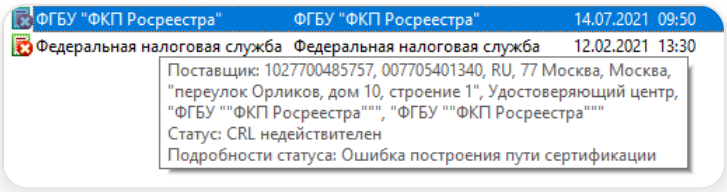
Ошибка построения пути сертификации

Текст ошибки:

Сертификат не действителен. Ошибка построения пути сертификации.

Как выглядит ошибка:





Решение

Описанные ниже действия в видео файле разместили на Яндекс диске.

Сообщение **Статус сертификата: недействителен, ошибка построения пути сертификации** говорит о том, что нужно на рабочем месте установить корневой сертификат удостоверяющего центра, чтобы цепочка доверия могла быть построена и проверена программой.

Корневой сертификат УЦ, как правило, можно загрузить с сайта удостоверяющего центра. Также его можно скачать по ссылке, указанной в сертификате.

Для сертификатов, полученных в УЦ ФНС России скачать корневые сертификаты УЦ ФНС России можно здесь. Корневой сертификат Головного УЦ Минцифры (от 02 февраля 2026 г.) скачайте здесь.

Установить оба сертификата нужно в хранилище текущего пользователя. Сертификат УЦ ФНС России — в папку **Промежуточные центры сертификации**, сертификат УЦ Минцифры — в **Доверенные корневые центры сертификации**.

Для остальных сертификатов нужно:

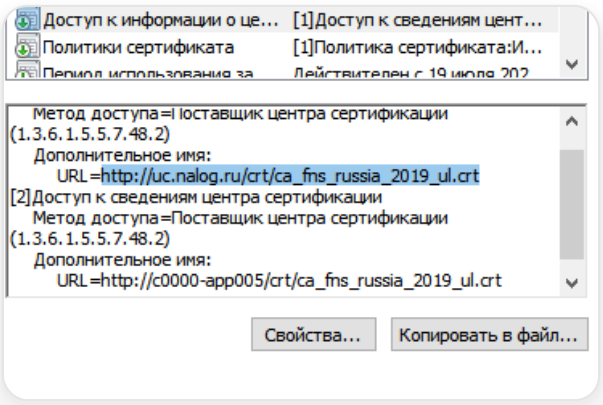
1. В личном хранилище сертификатов в КриптоАРМ выбрать сертификат и двойным кликом левой клавиши мыши открыть его.

2. Нажать на кнопку **Просмотреть**.

3. Выбрать вкладку **Состав**.

4. Выбрать в составе строку **Доступ к информации о центрах сертификации**.

5. Скопировать ссылку для скачивания корневого сертификата, расположенную в нижней части окна (это ссылка с окончанием **crt** или **cer**). Копирование правой клавишей мышки здесь не работает. После того как выделили ссылку, нажмите **Ctrl C.**



6. Вставить ссылку в адресную строку браузера нажав сочетание клавиш **Ctrl V** и нажать **Enter**.

7. Выбрать в КриптоАРМ папку **Промежуточные центры сертификации**, нажать **Импорт** на панели инструментов и установить загруженный сертификат. В мастере импорта НЕ СТАВИТЬ галочки "установить личный сертификат", "поместить сертификат в контейнер".

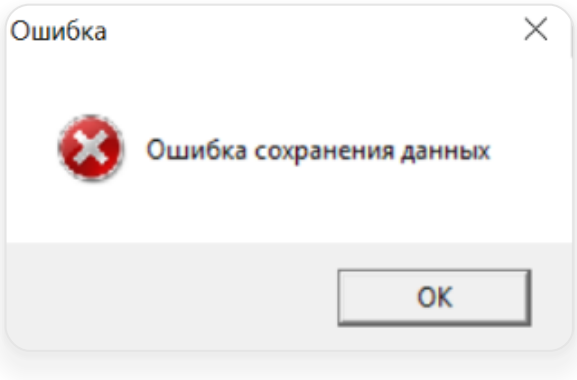
Открыть статью на сайте

Ошибка сохранения данных

Текст ошибки:

Ошибка сохранения данных.

Как выглядит ошибка:



Решение

Запустите программу КриптоАРМ от имени администратора, для этого нужно нажать на ярлык программы и выбрать **Запуск от имени администратора,** точно так же после этого перейдите в меню **Помощь \ Установить лицензию** и внесите лицензионный ключ в соответствующее поле.

Если ошибка возникнет снова, то откройте редактор реестра и найдите в нем ветки

HKEY_LOCAL_MACHINE\SOFTWARE\Digt\Trusted Desktop\License

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Digt\Trusted Desktop\License и в значение текстового параметра **SerialNumber** сохраните лицензионный ключ.

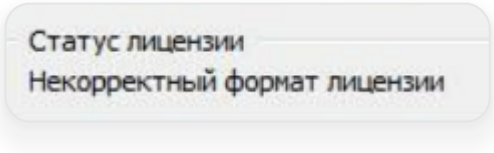
Открыть статью на сайте

Некорректный формат лицензии

Текст ошибки:

Некорректный формат лицензии

Как выглядит ошибка:



Решение:

Внимательно посмотрите на то, какой лицензионный ключ вы вносите в программу.

Ключ лицензии КриптоАРМ версии 5 всегда начинается с **TD5**. И представляет собой набор символов, состоящий из 7 блоков, сгруппированных по 5 и разделенных дефисом.

Если вы прописываете ключ вручную, то будьте внимательны и не вставляйте лишних пробелов. Лучше скопировать символы из письма комбинацией клавиш **Ctrl+C** и внести с помощью комбинации **Ctrl+V**. Если при этом возникнет **Ошибка сохранения данных**, посмотрите как ее обойти в соответствующей инструкции.

Открыть статью на сайте

Ошибка исполнения функции (0x0000065b)

Текст ошибки:

Ошибка сохранения сообщения (0x80004005)

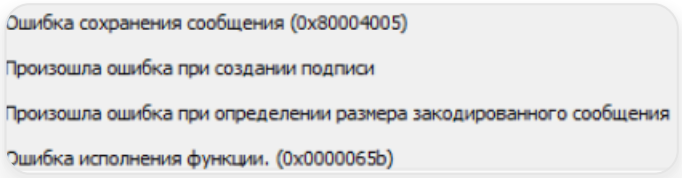
Ошибка сохранения сообщения (0x80004005)

Произошла ошибка при создании подписи

Произошла ошибка при определении размера закодированного сообщения

Ошибка исполнения функции. (0x0000065b)

Как выглядит ошибка:



Решение

Скорее всего отсутствует лицензионный ключ или истек срок его действия для программ КриптоАРМ или КриптоПро CSP. Лицензионные ключи должны быть установлены в обеих программах, они должны быть активны.

Проверить наличие и статус лицензии на КриптоАРМ можно в верхнем меню программы в разделе **Помощь** - **О программе**.

Если статус лицензии Лицензия не действительна, то внесите лицензионный ключ по инструкции.

В КриптоПро CSP эта информация есть на вкладке **Общие**.

Если срок действия лицензии истек, то внесите лицензионный ключ нажав на кнопку **Ввод лицензии**.

Открыть статью на сайте

Указан неправильный алгоритм (0x80090008)

Текст ошибки:

Ошибка сохранения сообщения (0x80004005)

Ошибка сохранения сообщения (0x80004005)

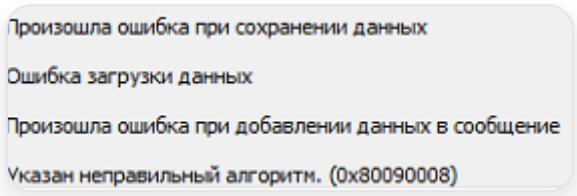
Произошла ошибка при сохранении данных

Ошибка загрузки данных

Произошла ошибка при добавлении данных в сообщение

Указан неправильный алгоритм. (0x80090008)

Как выглядит ошибка:



Решение

В большинстве случаев ошибка Указан неправильный алгоритм (0x80090008) решается переустановкой сертификата подписи. Переустановить сертификат можно несколькими способами:

1. В программе КриптоАРМ так, как показано в видео инструкции.

2. В личном хранилище сертификатов КриптоАРМа найдите ваш сертификат, выделите нажав на него курсором мыши. Нажмите на кнопку **Экспорт**, в открывшемся окне мастера нажмите **Далее**, в следующем окне обязательно укажите **НЕТ НЕ ЭКСПОРТИРОВАТЬ ЗАКРЫТЫЙ КЛЮЧ**, в мастере экспорта выберите кодировку **DER**, нажав кнопку **Обзор** поместите его на рабочий стол под любым именем. Удалять сертификат из личного хранилища при этом не нужно. Затем снова импортируйте его в личное хранилище, используя кнопку **Импорт** на панели инструментов, в мастере импорта сертификатов установите чекбоксы **Установить личный сертификат** и **Поместить сертификат в контейнер**. Далее понадобится выбрать криптопровайдер и контейнер вручную. После успешного импорта сертификата повторите подписание.

3.Также переустановку сертификата можно выполнить через КриптоПро CSP. Для этого откройте программу КриптоПро CSP и перейдите во вкладку **Сервис**. Затем нажмите на кнопки **Просмотреть сертификаты в контейнере** и **Обзор**. Выберите нужный контейнер и нажмите кнопку **Ok**, а после **Установить**. Снова повторите подписание.

После выполненных переустановок сертификата, если ошибка возникнет снова, войдите в КриптоАРМ в меню **Профили**, далее **Управление профилями**, откройте профиль по умолчанию (он помечен зеленой галочкой в списке), перейдите на вкладку **Общие**. Здесь в поле **Владелец сертификата** добавьте этот сертификат, нажмите **Применить** и **ОК**. После этого повторите подписание.

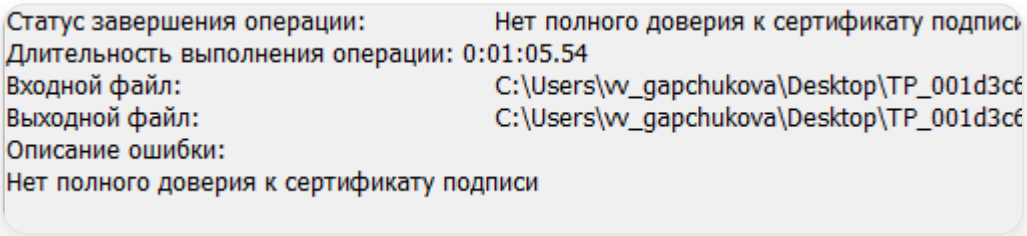
Открыть статью на сайте

Предупреждение «Нет полного доверия к сертификату подписи» или «Подпись математически корректна, но нет полного доверия к сертификату подписи»

Текст ошибки:

Нет полного доверия к сертификату подписи.

Как выглядит ошибка:



Решение

1. Если в вашей организации используется прокси-сервер, то запишите настройки прокси в соответствующем меню КриптоАРМа. Если прокси не используется, то в меню **Настройки** - **Управление настройками** - **Параметры прокси-сервера** отключите использование прокси.

2. В верхнем меню КриптоАРМ выберите пункт **Настройки**, затем **Управление настройками**, далее вкладка **Общие** - снимите чекбокс с опции **Отключить проверку личных сертификатов по спискам отзыва**.

3. Зайдите в меню **Профили** - **Управление профилями**, откройте профиль, который используется по умолчанию (он отмечен галочкой в списке профилей). Достаточно нажать по нему 2 раза левой клавишей мышки. Далее в разделе **Верификация сертификатов** в таблице нажмите кнопку **Добавить все** УЦ и установите чекбокс в ячейке рядом с появившимися звездочками в таблице, нажмите **Применить** и **ОК**. Выполните подписание, если предупреждение еще возникает, то переходите к следующему пункту.

4. Выберите в окне программы КриптоАРМ ветку **Личное хранилище сертификатов**. Затем справа выберите нужный сертификат и нажмите правой кнопкой мыши, чтобы вызвать контекстное меню. В появившемся меню выберите Проверить статус - **По CRL, полученному из УЦ**.

5. Если статус сертификата стал с зеленой галочкой, повторите ваше изначальное действие, подпишите файл.

- Если статус вашего сертификата не изменился, то перейдите в папку **Списки отзыва сертификатов** в КриптоАРМ и посмотрите, появился ли там актуальный список отзыва от вашего удостоверяющего центра (УЦ). Если список отзыва не появился, откройте сертификат, нажмите **Просмотреть**, перейдите на вкладку **Состав**, найдите строку **Точки распространения списков отзыва**, скопируйте ссылку и скачайте по ней список отзыва. Файл списка установите в папку **Списки отзыва сертификатов** нажатием кнопки **Импорт**. Если подгруженный список отзыва имеет недействительный статус, то это значит, что в системе отсутствует промежуточный сертификат УЦ.
- Для загрузки сертификата УЦ откройте в личном хранилище КриптоАРМ свой сертификат, нажмите **Просмотреть**, далее **Состав**. Найдите строку **Доступ к информации о центре сертификации**, в окне внизу найдите ссылку с окончанием **crt**, скопируйте ее комбинацией клавиш **ctrl+C**, вставьте в адресную строку браузера с помощью комбинации клавиш **ctrl+V** и нажмите **Enter**. Далее в КриптоАРМ выберите папку **Промежуточные центры сертификации**, на панели инструментов выберите **Импорт**. В открывшемся мастере импорта сертификата галки “установить личный сертификат” и “поместить в контейнер” ставить не нужно, перейдите **Далее** и выберите из папки загрузок сертификат УЦ. После успешного импорта статус вашего сертификата изменится. Повторите попытку подписания.

6. Если к промежуточному сертификату удостоверяющего центра тоже нет полного доверия, то выполните эти же действия по загрузке списка отозванных сертификатов.

Открыть статью на сайте

Ошибка установки свойства в контекст сертификата (0x80092004)

Текст ошибки:

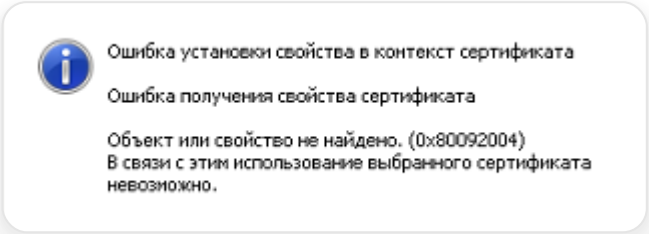
Ошибка установки свойства в контекст сертификата

Ошибка получения свойств сертификата

Объект или свойство не найдено. (0x80092004)

В связи с этим использование выбранного сертификата невозможно.

Как выглядит ошибка:



Решение

Ошибка 0x80092004 говорит о том, что сертификат был установлен без привязки к закрытому ключу. Попробуйте переустановить сертификат через КриптоПро CSP.

Для этого откройте программу КриптоПро CSP и перейдите во вкладку **Сервис**. Затем нажмите на кнопки **Просмотреть сертификаты в контейнере** и **Обзор**. Выберите нужный контейнер и нажмите кнопку **Ok**, а после **Установить**.

Либо выполните переустановку другими способами, указанными в инструкции к ошибке Указа н неправильный алгоритм.

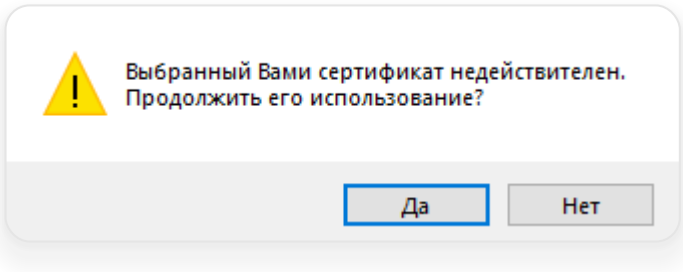
Открыть статью на сайте

Выбранный вами сертификат не действителен, продолжить его использование?

Текст ошибки:

Выбранный вами сертификат не действителен, продолжить его использование?

Как выглядит ошибка:



Решение

Это оповещение означает, что в настройках профиля КриптоАРМ по умолчанию выбран сертификат с истекшим сроком действия.

Откройте КриптоАРМ, перейдите в меню **Профили**, далее **Управление профилями**, затем откройте профиль который помечен галочкой, войдите на вкладку **Общие**. В открывшемся окне в поле **Владелец сертификата** нажмите **Выбрать**, выберите действующий сертификат и нажмите **ОК**. Затем **Применить** - **Ок**.

Таким образом вы добавите актуальный сертификат в настройки профиля, и при подписании он будет автоматически попадать в окно выбора сертификата.

Открыть статью на сайте

Отказано в доступе. (0x80090010)

Текст ошибки:

Ошибка сохранения сообщения (0x80004005)

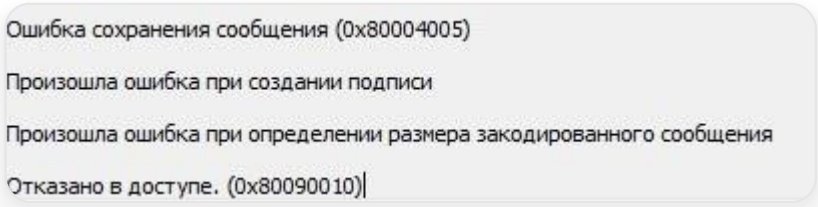
Ошибка сохранения сообщения (0x80004005)

Произошла ошибка при создании подписи

Произошла ошибка при определении размера закодированного сообщения

Отказано в доступе. (0x80090010)

Как выглядит ошибка:



Решение

Переустановите ваш сертификат через КриптоПро CSP так: Перейдите на вкладку **Сервис**, далее **Просмотреть сертификаты в контейнере**, затем **Обзор**, выберите контейнер и нажмите **Установить**.

Если переустановка не поможет, то проверьте контейнер ключа при помощи кнопки **Протестировать** на той же вкладке. Если в результате тестирования возникнет ошибка “Использование ключа обмена запрещено. Срок действия закрытого ключа истек. Срок действия закрытого ключа не может превышать 3 года для неизвлекаемых ключей, хранящихся на ФКН и на HSM, и 1 год 3 месяца для прочих ключей”, то подписать этим сертификатом вам не удастся, нужно получить новый сертификат.

Также вероятная причина ошибки это ограничение прав доступа к ресурсу, на котором находится ключевой контейнер. Например в следующей статье описана похожая ошибка на серверной Windows, где причиной было ограничение прав пользователя к флешке на которой находился ключевой контейнер.

Также возможно ограничение прав на ветку реестра с контейнером, так как понадобятся не только права чтения, но и права записи.

Ключи носителя "реестр" КриптоПро CSP хранит в следующей ветке реестра:

HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\Crypto Pro\Settings\Users\<SID пользователя>\Keys

Пользователю в разрешениях (доступно из контекстного меню для ветки реестра) должен быть предоставлен полный доступ (начиная с раздела <SID пользователя>).

Если не получается исправить эту ошибку добавлением прав пользователя для носителя контейнера, то с этим вопросом стоит обратиться в техподдержку компании КриптоПРО.

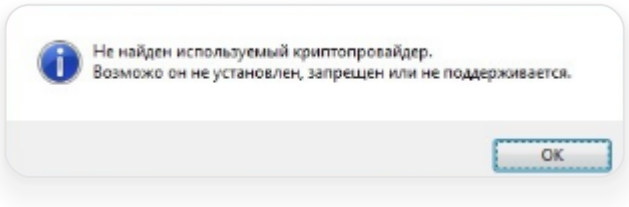
Открыть статью на сайте

Не найден используемый криптопровайдер. Возможно он не установлен, запрещен или не поддерживается.

Текст ошибки:

Не найден используемый криптопровайдер. Возможно он не установлен, запрещен или не поддерживается.

Как выглядит ошибка:



Решение

Чаще всего это оповещение возникает в том случае, если у вас установлена устаревшая сборка ПО КриптоАРМ.

Проверьте номер сборки в главном окне КриптоАРМ нажав на кнопку **Помощь**, далее **О программе**. Устаревшими считаются сборки 4, 5.0, 5.1, 5.2, 5.3. Актуальна сборка 5.4.

Обновить КриптоАРМ можно скачав сборку 5.4.4.52. После загрузки запустите установку файла **trusteddesktop.exe,** выберите из предложенных вариантов **Изменить** и дождитесь окончания установки. После обновления выполните перезагрузку компьютера.

	СКЗИ КриптоАРМ 5 (сборки 5.4.1.93) работает только с КриптоПро CSP 4 версии.

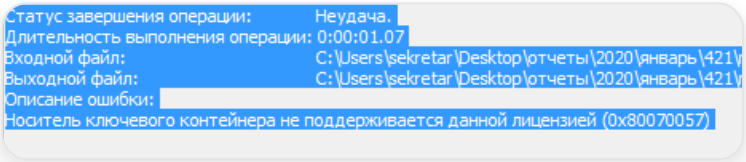
Открыть статью на сайте

Носитель ключевого контейнера не поддерживается данной лицензией (0x80070057)

Текст ошибки:

Носитель ключевого контейнера не поддерживается данной лицензией (0x80070057)

Как выглядит ошибка:



Решение

В сборках, выпущенных ранее, для того чтобы КриптоАРМ мог извлечь сертификат из облачного хранилища, ему нужна была дополнительная лицензия на модуль поддержки КриптоПро DSS. Ошибка “Носитель ключевого контейнера не поддерживается данной лицензией (0x80070057)” возникает в том случае, если лицензии нет.

В КриптоАРМе сборки 5.4.4.4 отдельная лицензия на модуль КриптоПро DSS не нужна, в связи с этим она была снята с продаж. Поддержка модуля КриптоПро DSS включена в состав лицензии на версию КриптоАРМ Стандарт Плюс 5.

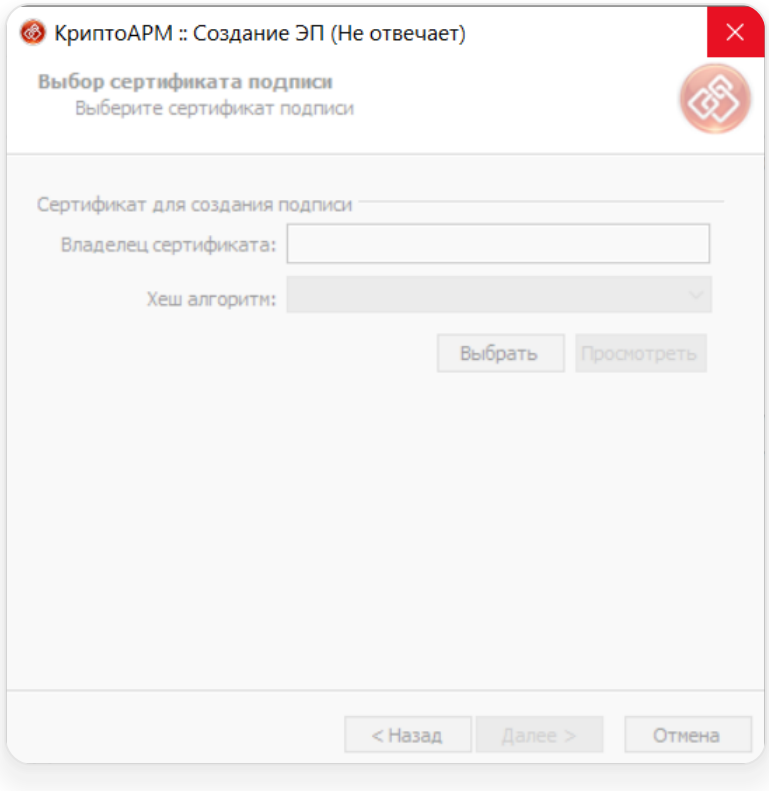
Открыть статью на сайте

КриптоАРМ зависает (не отвечает) в момент выбора сертификата подписи

Текст ошибки:

КриптоАРМ зависает (не отвечает) в момент выбора сертификата подписи.

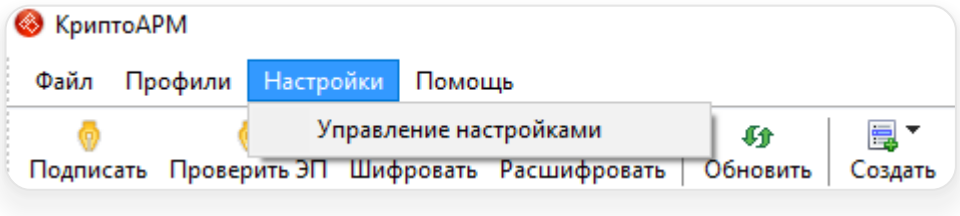
Как выглядит ошибка:



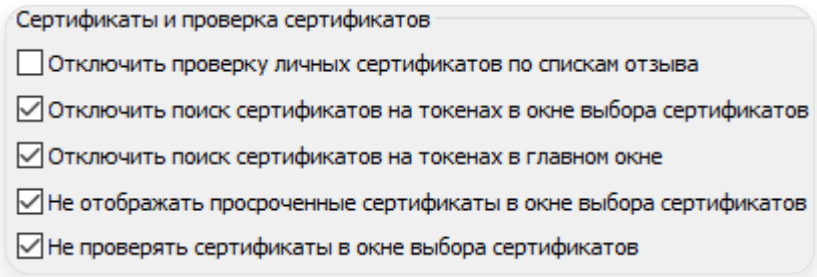
Решение:

Зависание в момент выбора сертификата подписи может происходить по причине проверок и поиска сертификата.

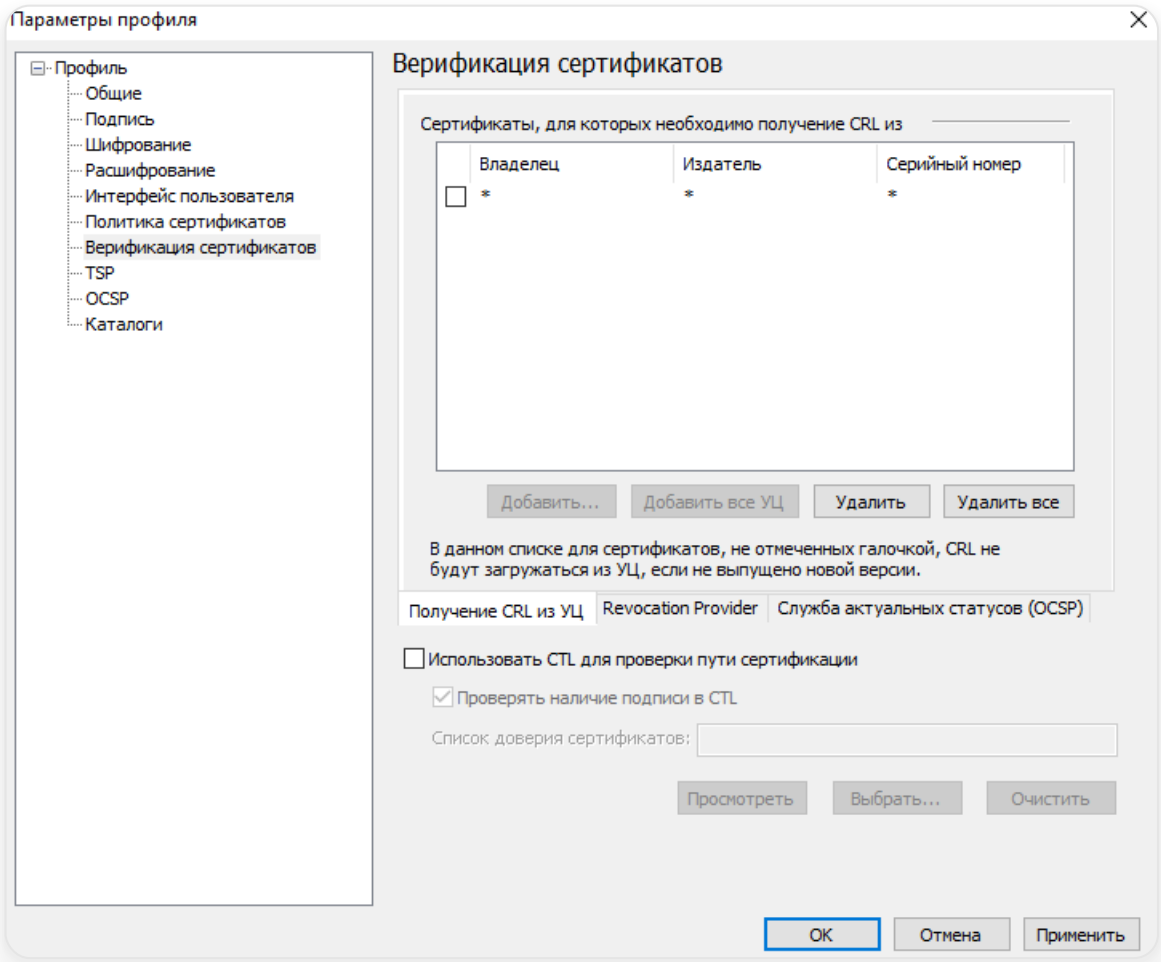
Для отключения проверок зайдите в верхнее меню КриптоАРМа **Настройки - Управление настройками - Общие** и установите 4 нижних галочки, касающихся проверки и поиска сертификатов, а именно:



- Отключить поиск сертификатов на токенах в окне выбора сертификатов
- Отключить поиск сертификатов на токенах в главном окне
- Не отображать просроченные сертификаты в окне выбора сертификатов
- Не проверять сертификаты в окне выбора сертификатов



Также зайдите в меню **Профили - Управление профилями**, откройте профиль, установленный как профиль по умолчанию, и во вкладке **Верификация сертификатов** уберите галочку в ячейке в таблице. Повторите подписание. Если это не помогло, то там же в профиле в верификации сертификатов нажмите **Удалить все**.


Параметры профиля
Профиль
Общие
Подпись
Шифрование
Расшифрование
Интерфейс пользователя
Политика сертификатов
Верификация сертификатов
TSP
OCSP
Каталоги
Верификация сертификатов
Сертификаты, для которых необходимо получение CRL из
Владелец
Издатель
Серийный номер
*
*
*
Добавить...
Добавить все УЦ
Удалить
Удалить все
В данном списке для сертификатов, не отмеченных галочкой, CRL не будут загружаться из УЦ, если не выпущено новой версии.
Получение CRL из УЦ
Revocation Provider
Служба актуальных статусов (OCSP)
Использовать CTL для проверки пути сертификации
Проверять наличие подписи в CTL
Список доверия сертификатов:
Просмотреть
Выбрать...
Очистить
OK
Отмена
Применить

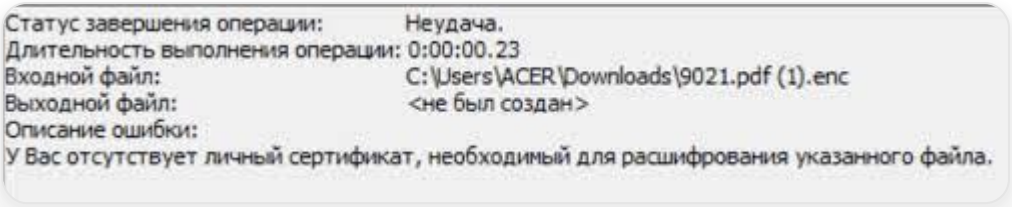
Открыть статью на сайте

Отсутствует личный сертификат для расшифрования

Текст ошибки:

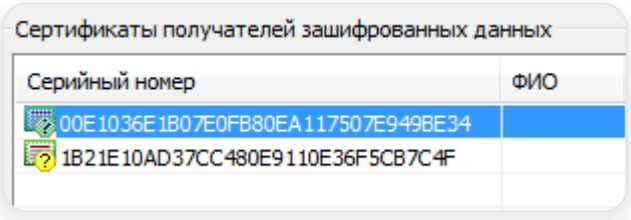
У Вас отсутствует личный сертификат, необходимый для расшифрования указанного файла.

Как выглядит ошибка:

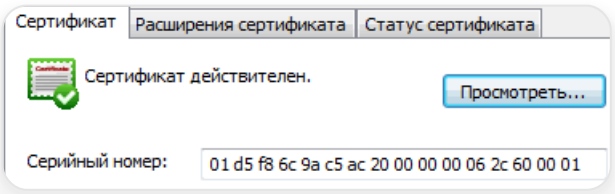


Решение

1. В первую очередь проверьте наличие лицензии на КриптоАрм. **Помощь \ О программе** - если истек срок действия лицензии, то расшифровать не получится. Если лицензия действительна, то проверьте, зашифрован ли файл в адрес вашего сертификата. Для этого в окне с ошибкой нажмите кнопку **Детали,** затем **Менеджер сообщения** - там будут указаны серийные номера сертификатов получателей.



2. Среди них надо поискать серийный номер вашего сертификата. Сам номер в сертификате увидеть так: открыть сертификат в личном хранилище - в поле **Серийный номер** будут прописаны нужные символы.



3. Если в списке получателей зашифрованных данных нет серийного номера вашего сертификата, то расшифровать файл вам не удастся. Если серийный номер среди получателей все же есть, но расшифровать не получается, проверьте, тот ли сертификат указан в используемом профиле.

4. **Профили** \ **Управление профилями** - откройте профиль, отмеченный зеленой галочкой, двойным нажатием левой клавиши мыши и перейдите на вкладку **Общие,** там в поле **Владелец сертификата** проверьте, какой сертификат прописан. Кнопкой **Выбрать** добавьте нужный сертификат, нажмите **Применить** и **ОК**. Повторите попытку расшифрования.

5. Если вышеперечисленные действия вам не помогли, то выполните переустановку сертификата одним из способов, описанных нами ранее.

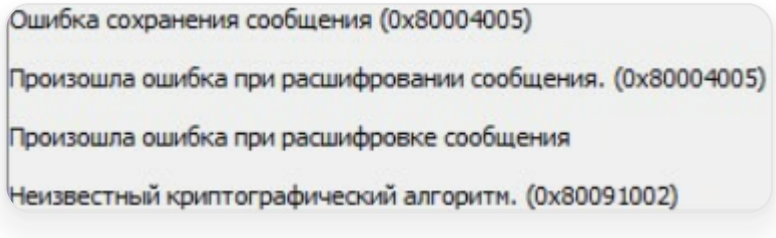
Открыть статью на сайте

Неизвестный криптографический алгоритм. (0x80091002)

Текст ошибки:

Ошибка сохранения сообщения (0x80004005)
Ошибка сохранения сообщения (0x80004005)
Произошла ошибка при расшифровке сообщения
Неизвестный криптографический алгоритм. (0x80091002)

Как выглядит ошибка:



Решение:

Данная ошибка сейчас стала возникать у пользователей, клиентов Центробанка.

Дело в том, что Центробанк оповещал о переходе с 01 июня 2024 года на национальный стандарт шифрования, а именно:

- ГОСТ Р 34.12-2015 «Информационная технология. Криптографическая защита информации. Блочные шифры» (далее — ГОСТ Р 34.12-2015);
- ГОСТ Р 34.13-2015 «Информационная технология. Криптографическая защита информации. Режимы работы блочных шифров» (далее — ГОСТ Р 34.13-2015).

До этого времени следовало удостовериться, что ваше программное обеспечение соответствует требованиям системы и поддерживает данные стандарты шифрования. КриптоАРМ сборки 5.4.4.52 поддерживает ГОСТ Р 34.12-2015 и ГОСТ Р 34.13-2015. Если ваша сборка ниже, то обновитесь.

*В других версиях КриптоАРМ - КриптоАРМ ГОСТ 2.5 и КриптоАРМ ГОСТ 3 поддержка алгоритмов "Магма" и "Кузнечик" также имеется.

Из таблицы сравнения версий КриптоПро CSP следует, что поддержка алгоритмов "Магма" и "Кузнечик", появилась только в КриптоПро CSP 5.0 R2 (5.0.12000):

Поддерживаемые алгоритмы

	CSP 4.0 R4	CSP 5.0	CSP 5.0 R2	CSP 5.0 R3
ГОСТ Р 34.10-2012 Создание подписи	512 / 1024 бит	512 / 1024 бит	512 / 1024 бит	512 / 1024 бит
ГОСТ Р 34.10-2012 Проверка подписи	512 / 1024 бит	512 / 1024 бит	512 / 1024 бит	512 / 1024 бит
ГОСТ Р 34.10-2001 Создание подписи*	512 бит	512 бит	512 бит	512 бит
ГОСТ Р 34.10-2001 Проверка подписи**	512 бит	512 бит	512 бит	512 бит
ГОСТ Р 34.11-2012	256 / 512 бит	256 / 512 бит	256 / 512 бит	256 / 512 бит
ГОСТ Р 34.11-94	256 бит	256 бит	256 бит	256 бит
ГОСТ Р 34.12-2015			256 бит	256 бит
ГОСТ Р 34.13-2015			256 бит	256 бит
ГОСТ 28147-89	256 бит	256 бит	256 бит	256 бит

* До 31 декабря 2019 года включительно.

** До окончания действия сертификатов, содержащих указанный алгоритм ключа проверки электронной подписи.

Это значит, что пользователи версии КриптоПро CSP 4.0 должны были обновить программу до КриптоПро CSP 5.0. Проверьте криптопровайдер КриптоПро CSP на вашем компьютере.

Если это КриптоПро CSP 4, то его следует обновить, установив с сайта разработчика сертифицированную сборку КриптоПро CSP.

Лицензионный ключ КриптоПро CSP 4 подлежит обновлению, заказать его можно у нас или у любых других партнеров КриптоПро. Перед обновлением лицензию следует прислать на проверку на почту sales@cryptoarm.ru .

Открыть статью на сайте

Неправильное значение индекса. (0x80091008)

Текст ошибки:

Произошла ошибка при расшифровании сообщения.

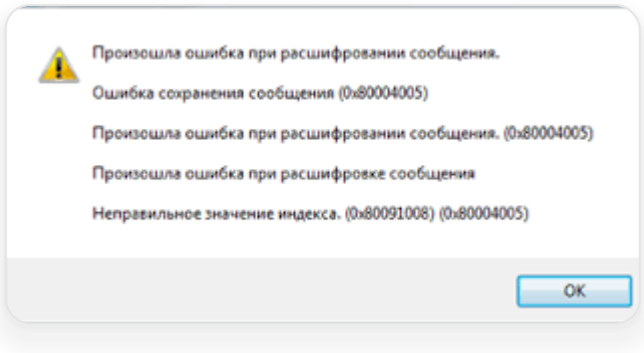
Ошибка сохранения сообщения (0x80004005)

Произошла ошибка при расшифровании сообщения.(0x80004005)

Произошла ошибка при расшифровке сообщения

Неправильное значение индекса.(0x80091008)

Как выглядит ошибка:



Решение

В старых версиях КриптоАРМ-а похожая ошибка происходила из-за того, что КриптоАРМ неправильно проверял доступность ключа расшифрования. Для этого создавалась подпись случайных данных, а в случае, если срок действия закрытого ключа истёк, КриптоПро CSP запрещает выполнять подпись, но разрешает выполнять расшифрование. В результате для сертификатов с истёкшим сроком действия закрытого ключа расшифрование завершалось с ошибкой. Если у вас сборка более ранняя чем 5.4.2.315, то рекомендуем обновить КриптоАРМ, скачав актуальную по ссылке. Проверить номер сборки можно через меню **Помощь \ О программе**.

Ошибка может происходить также из-за прав доступа к данным самого ключа - в случае, если контейнер ключа находится на флешке и текущему пользователю не заданы полные права на папки и файлы контейнера, происходит ошибка с подобным кодом. Задайте полные права на файлы вашему пользователю.

Открыть статью на сайте

Error initialize resource dll, неизвестная ошибка

Текст ошибки:

Ошибка сохранения сообщения (0x80004005)

Ошибка сохранения сообщения (0x80004005)

Error initialize resource dll

Неизвестная ошибка

Как выглядит ошибка:

Решение

Проверьте пожалуйста наличие библиотек: **DigtTSPClient.dll** по этому пути

C:\Program Files\Digt\Trusted\Desktop\DigtTSPClient.dll

Или в настройках КриптоАРМа в меню **Профили** -**Управление профилями** - профиль с зеленой галочкой открыть двойным кликом мыши - присутствует ли в меню слева пункты **TSP** и **OCSP**?

Если библиотека или ветка TSP в настройках отсутствуют, то запустите снова установочный файл **trusteddesktop.exe**, выберите настраиваемую установку и включите модули **TSP** и **OCSP**. Когда установка завершится, повторите подписание.

Как настроить службу штампов времени смотрите в соответствующей статье.

Открыть статью на сайте

Данные настройки для этого продукта повреждены. Обратитесь в службу поддержки. (0x0000064a)

Текст ошибки:

Ошибка сохранения сообщения (0x80004005)

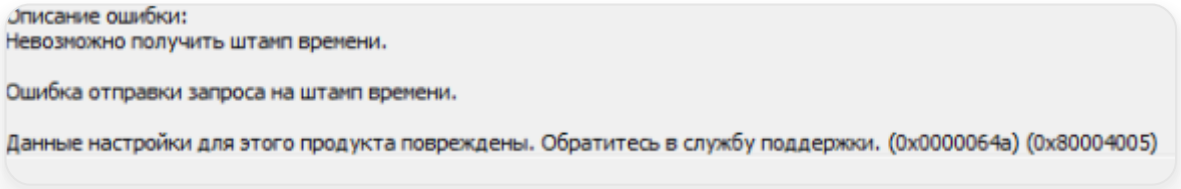
Ошибка сохранения сообщения (0x80004005)

Произошла ошибка при создании подписи

Ошибка создания атрибутов усовершенствованной подписи

Данные настройки для этого продукта повреждены. Обратитесь в службу поддержки. (0x0000064a)

Как выглядит ошибка:



Решение

Эта ошибка означает, что у вас отсутствуют лицензии на модули, предоставляющие возможность использовать атрибуты штампа времени на подпись и проверки валидности сертификата - КриптоПро TSP client и КриптоПро OCSP client.

Посмотреть информацию о лицензиях на модули можно через меню **Пуск** - **Все программы** - **КриптоПро** - **КриптоПро PKI** - **Управление лицензиями**.

Приобрести лицензии можно на этом сайте в магазине.

Если лицензии действительны, то проверьте наличие самих модулей через меню КриптоАРМа **Профили** -**Управление профилями** - профиль с зеленой галочкой открыть двойным кликом мыши - присутствуют ли в меню слева пункты **TSP** и **OCSP**?

Если ветки TSP и OCSP в настройках отсутствуют, то запустите снова установочный файл trusteddesktop.exe, выберите **настраиваемую** установку и включите модули **TSP** и **OCSP**. Когда установка завершится, повторите подписание.

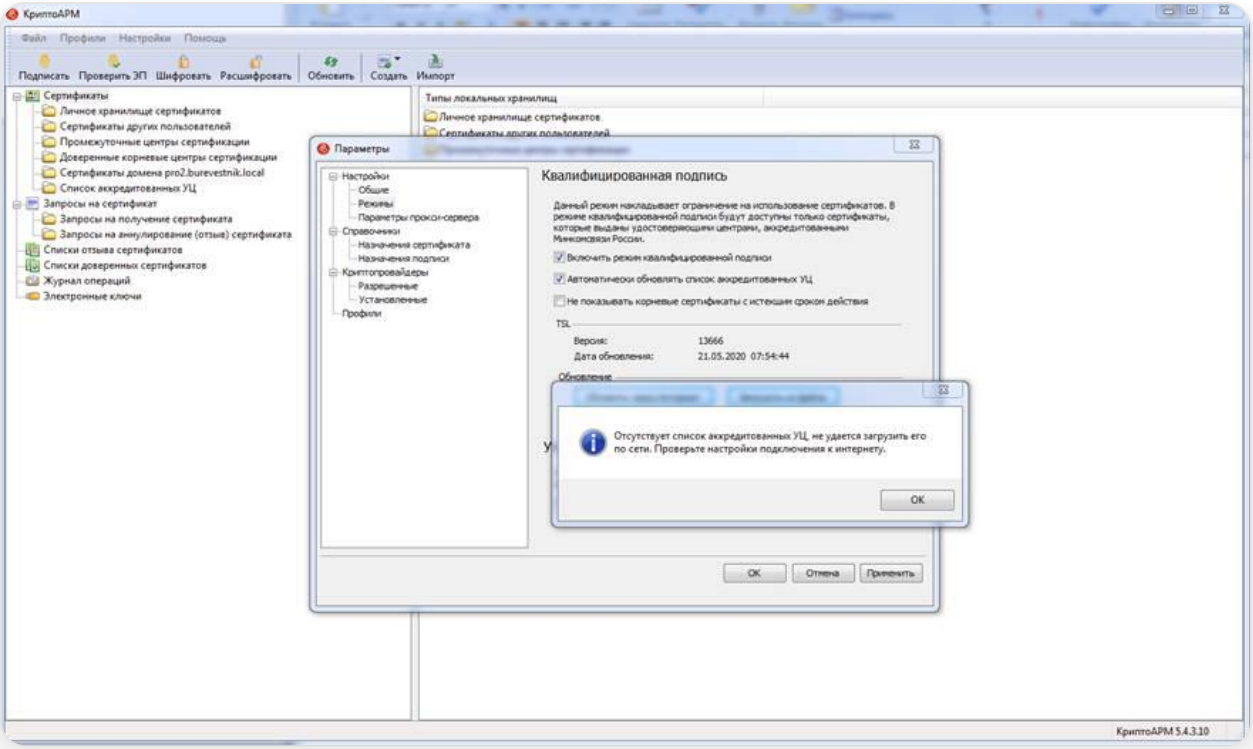
Открыть статью на сайте

Отсутствует список аккредитованных УЦ

Текст ошибки:

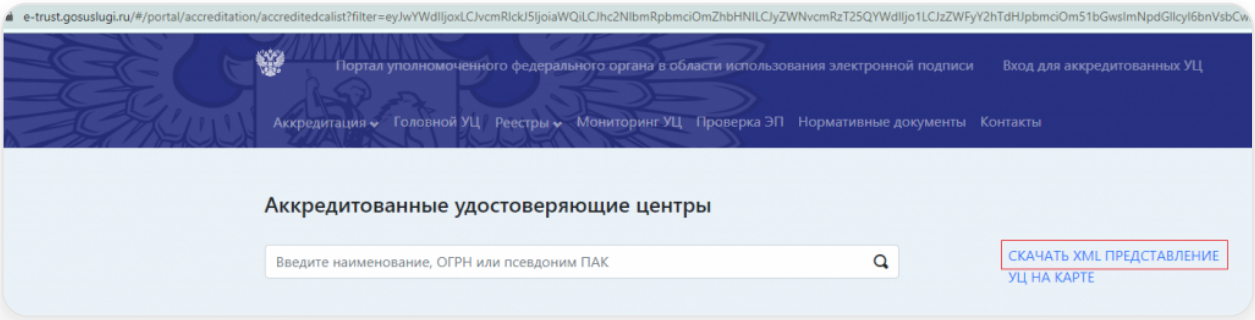
Отсутствует список аккредитованных УЦ, не удается загрузить его по сети. Проверьте настройки подключения к интернету.

Как выглядит ошибка:

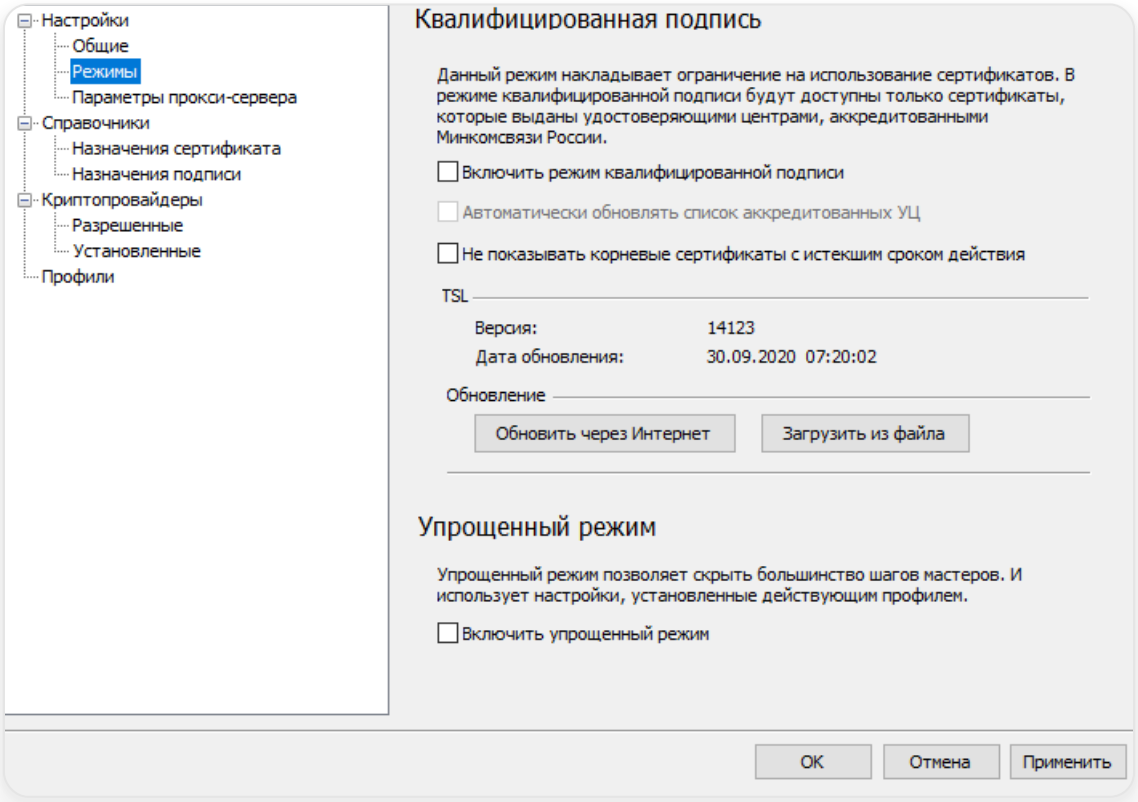


Решение

Загрузите XML представление списка с сайта Госуслуг.



Загруженный документ XML устанавливается в меню КриптоАРМ **Настройки** - **Управление настройками** - **Режимы** - кнопкой **Загрузить из файла**.



Также загруженный файл XML можно поместить в папку: **C:\Users\<Имя пользователя>\AppData\Local\КриптоАРМ\tsl**.

Папка AppData является скрытой. Чтобы в неё перейти нужно зайти в папку "Пользователи" (в корневом каталоге диска C:), затем перейти в папку вашего пользователя (по имени учётной записи). В ней нужно поставить курсор в адресную строку добавить к пути \AppData и нажать ввод. При этом произойдёт переход в папку C:\Users<Имя пользователя>\AppData\. В ней уже можно найти подпапку Local и остальные.

Открыть статью на сайте

Внутренняя ошибка (CSP). (0x80090020)

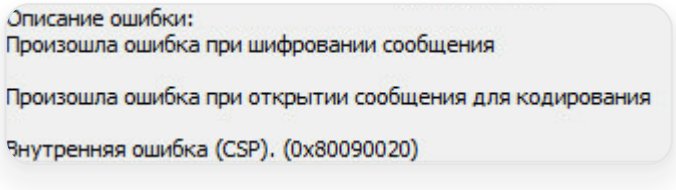
Текст ошибки:

Произошла ошибка при шифровании сообщения

Произошла ошибка при открытии сообщения для кодирования

Внутренняя ошибка (CSP). (0x80090020)

Как выглядит ошибка:



Решение

Чаще всего проблема возникает из-за конфликта криптопровайдеров КриптоПро CSP и VipNet CSP. При наличии двух этих криптопровайдеров на одном рабочем месте необходимо в настройках VipNet CSP во вкладке "Дополнительно" отключить настройку "Поддержка работы ViPNet CSP через Microsoft CryptoAPI". После изменения компьютер перезагрузится. Ошибка будет исправлена.

Если конфликтующего криптопровайдера не установлено и используется только КриптоПро CSP, то выполните восстановление настроек реестра утилитой.

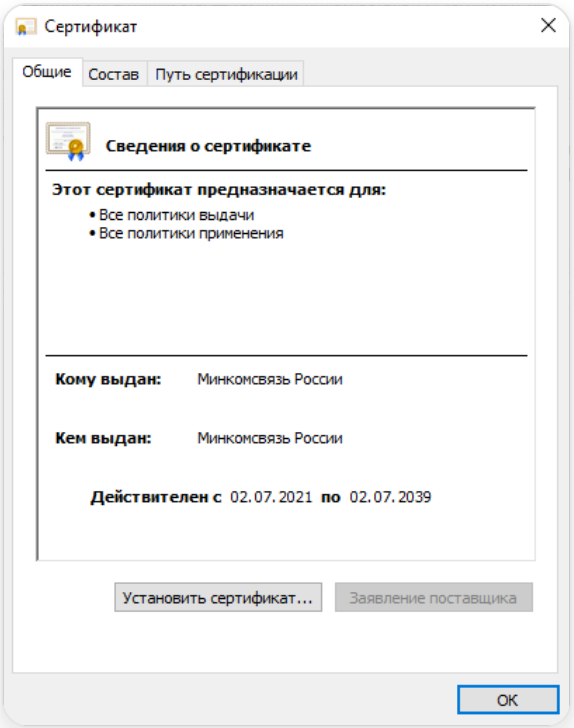
Если предложенные действия не помогли, напишите нам на support@trusted.ru.

Открыть статью на сайте

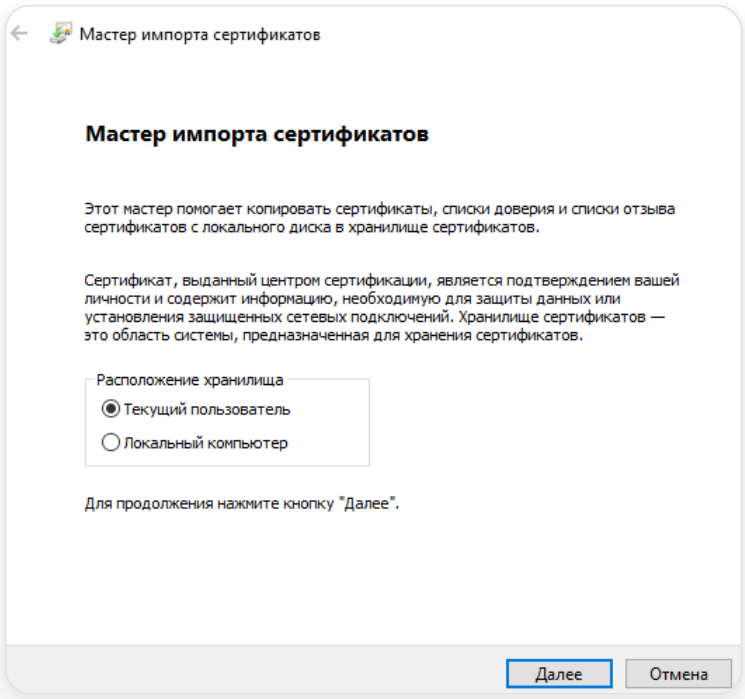
Установка сертификатов из файла p7b и cer

1. **Установка сертификата из файла cer.**

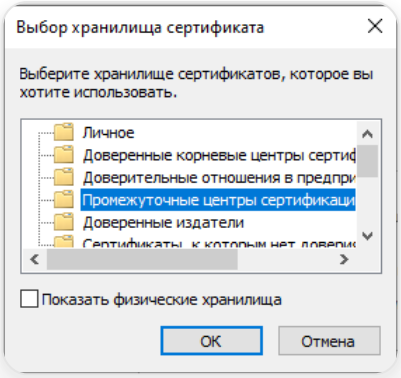
При наличии сертификата пользователя в формате cer файла установка выполняется таким образом - открывается файл (дважды кликните по файлу левой кнопкой мышки), установка запускается кнопкой Установить сертификат.



Хранилище текущего пользователя.



Далее выбирается папка в системе, куда его нужно поместить:



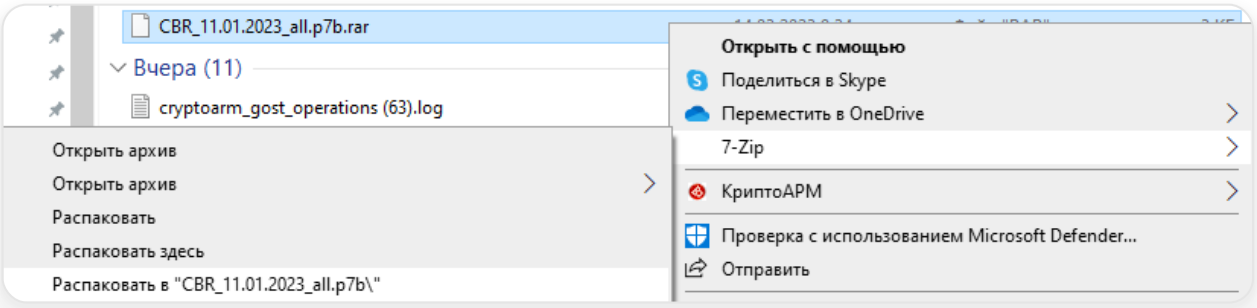
Остается нажать кнопку Готово. Так сертификат будет установлен.

2. Установка сертификата из архива p7b.

Часто возникает необходимость установить сертификаты других пользователей к себе в программу. На примере сертификата Центрального Банка рассмотрим установку из архива.

Из личного кабинета ЦБ скачивается архив с сертификатами, файл называется CBR_11.01.2023_all.p7b.rar. Для начала его нужно распаковать стандартным архиватором.

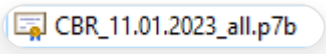
По файлу нажать правой кнопкой мышки, выбрать в контекстном меню архиватор, и далее выбрать Распаковать в CBR_11.01.2023_all.p7b.



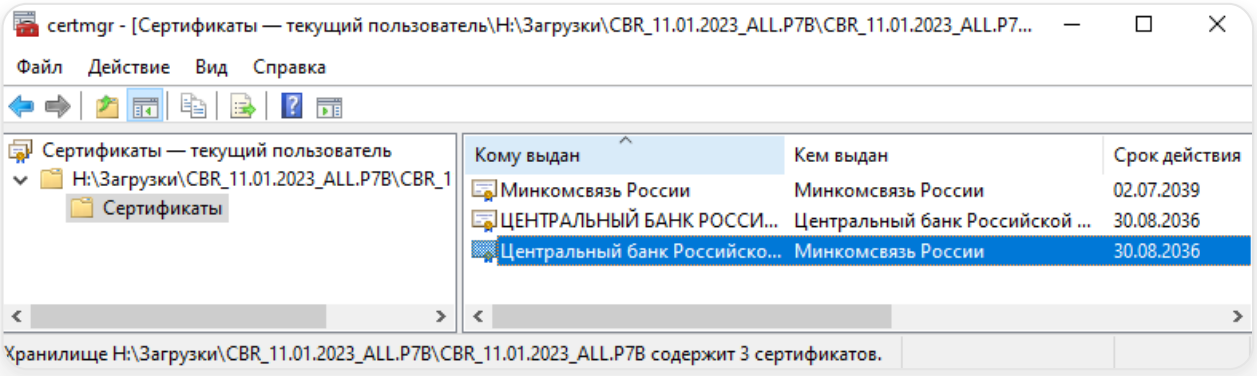
Извлеченный архив будет выглядеть как папка с расширением p7b.



Двойным кликом левой клавиши мышки можно открыть папку, в ней находятся все сертификаты пути сертификации для Центрального Банка.



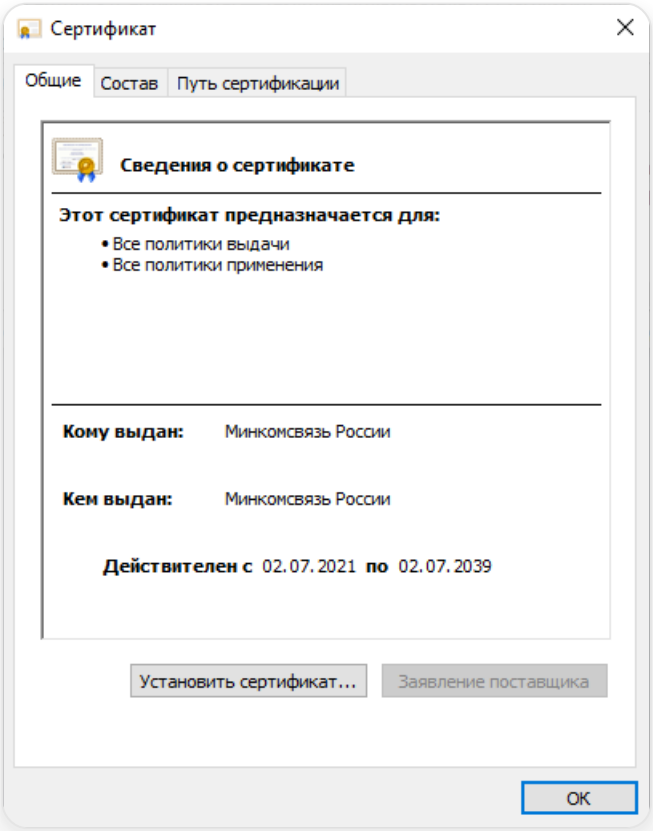
По нажатию левой клавиши мышки по данному файлу откроется хранилище, которое содержит в себе 3 сертификата - корневой сертификат Минкомсвязи, промежуточный сертификат Центрального банка и сертификат конечный, который предназначен для шифрования.



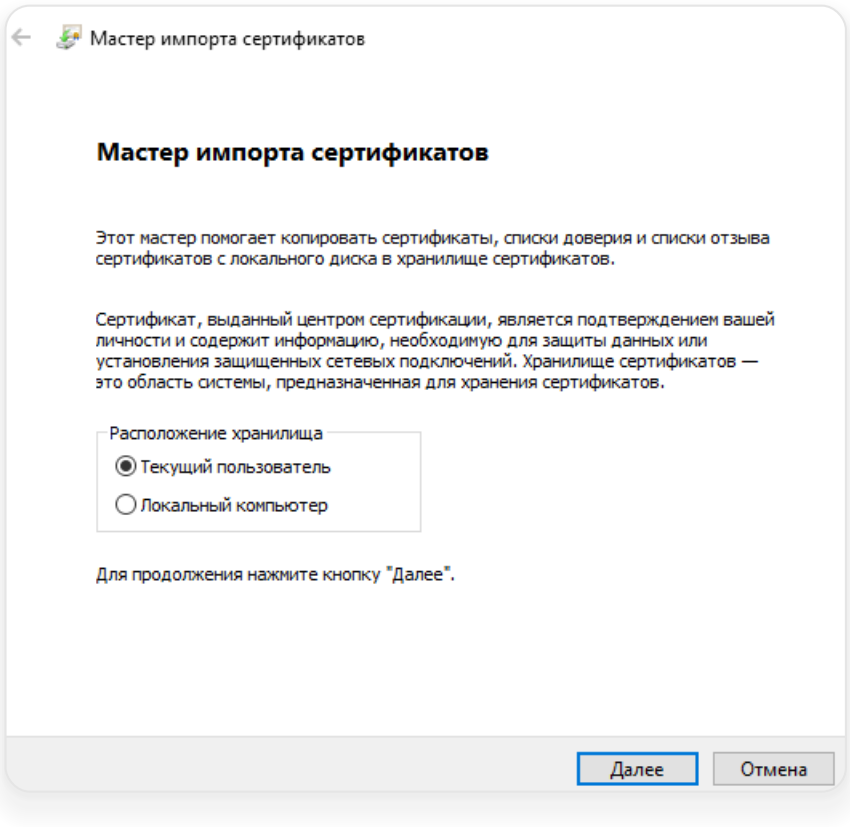
Теперь для установки нужно поочередно выбирать каждый из сертификатов. Начать можно с любого. Установить необходимо все. Это нужно для построения правильной цепочки сертификации.

Открыть сертификат Минкомсвязи двойным кликом левой клавиши мышки. Нажать в меню

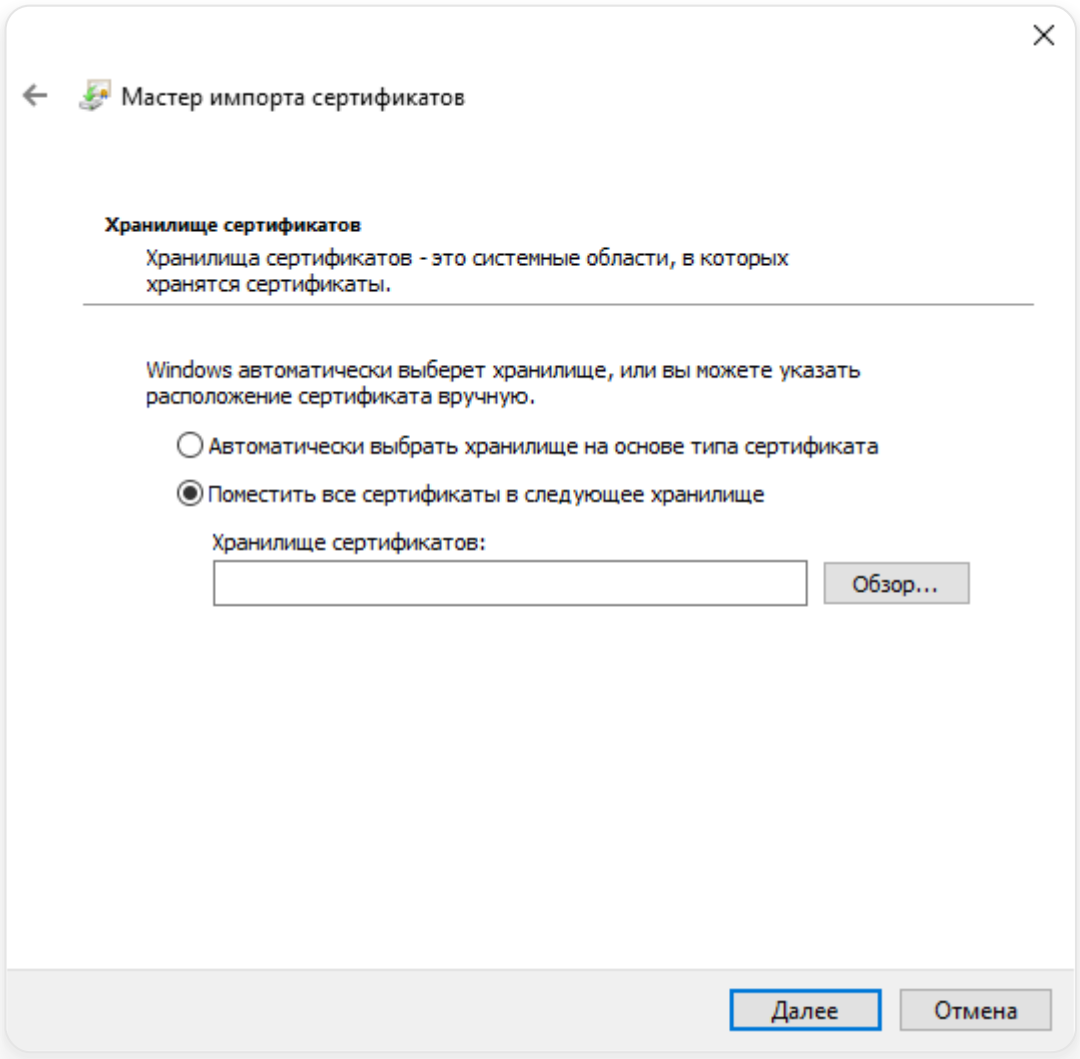
сертификата Установить сертификат. Откроется стандартный мастер установки сертификатов.



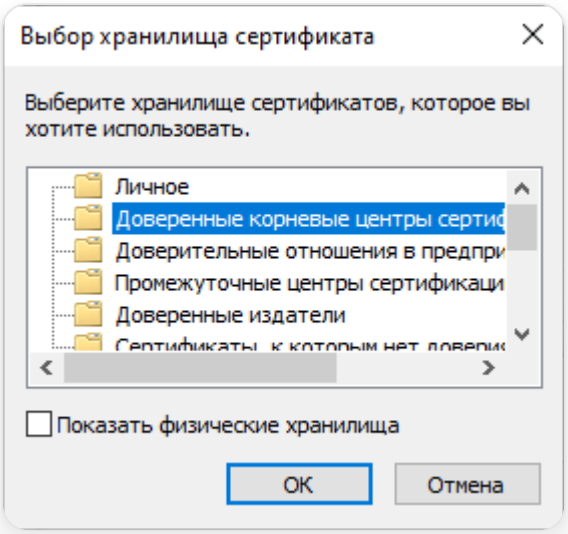
Выбрать хранилище Текущего пользователя и нажать Далее.



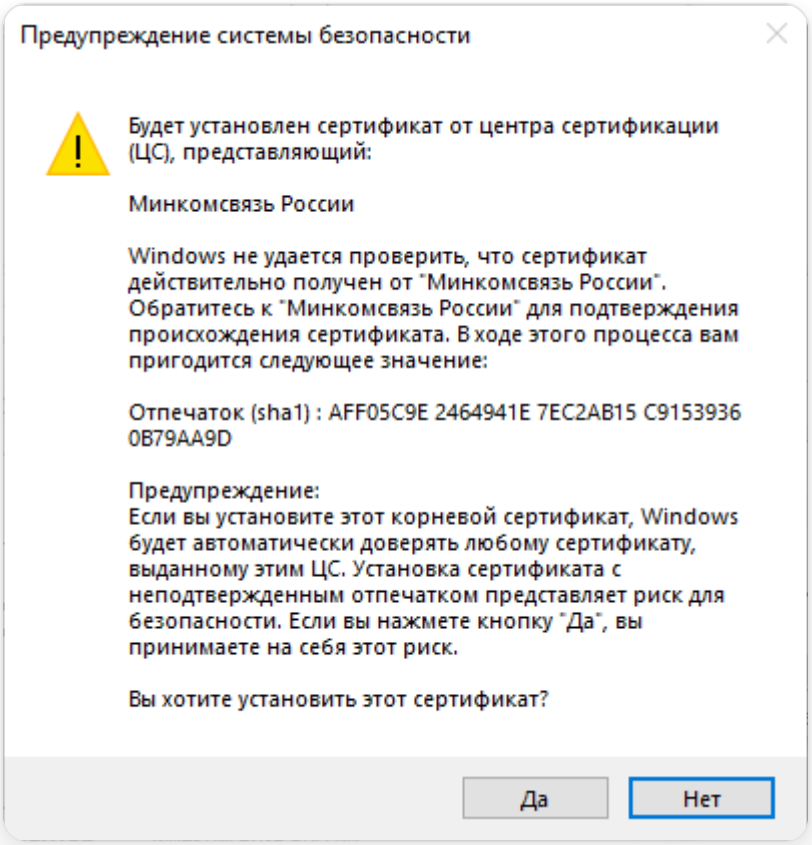
Выбрать вариант установки Поместить все сертификаты в следующее хранилище.



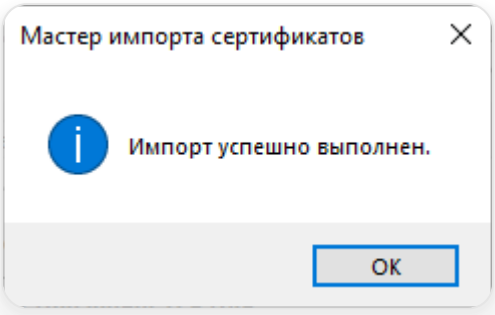
Нажать кнопку Обзор и для сертификата Минкомсвязи выбрать папку Доверенные корневые центры сертификации, нажать кнопку ОК.



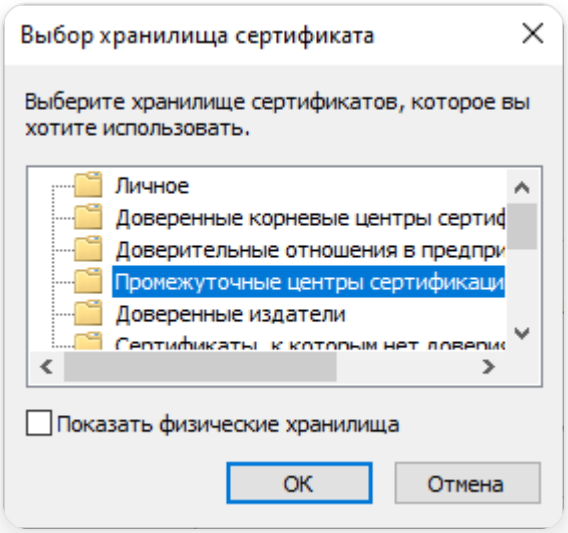
Вероятно появление уведомления, здесь необходимо согласиться и нажать Да:



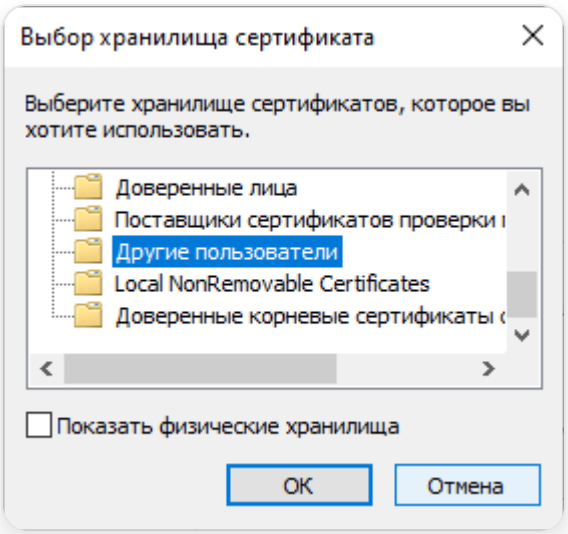
Далее завершить установку кнопкой Готово.



Теперь в папке выберем сертификат с именем Центральный банк, выданный Минкомсвязью. Точно также открыть его можно дважды щелкнув левой клавишей мышки, Установить сертификат, выбрать хранилище Текущего пользователя, выбрать Поместить все сертификаты в следующее хранилище, кнопкой Обзор выбрать хранилище Промежуточные центры сертификации.



Сертификат с именем ЦЕНТРАЛЬНЫЙ БАНК РОССИЙСКОЙ ФЕДЕРАЦИИ, выпущенный Центральным банком, таким же способом устанавливается в папку Другие пользователи.



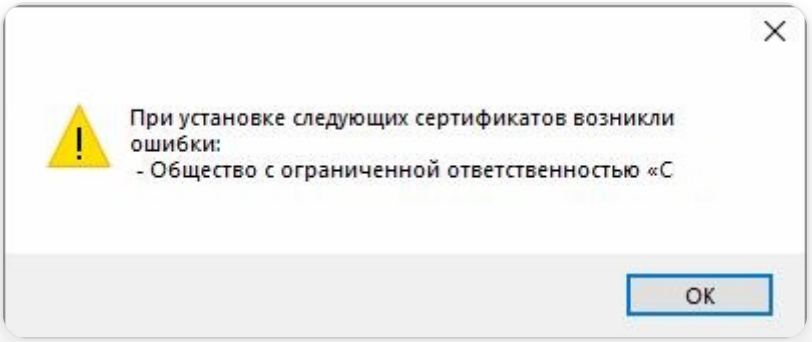
Открыть статью на сайте

При установке следующих сертификатов возникли ошибки

Текст ошибки:

При установке следующих сертификатов возникли ошибки.

Как выглядит ошибка:



Решение

В верхнем меню КриптоАРМ зайдите в **Настройки**, далее **Управление настройками**, выберите вкладку **Режимы** и снимите галочку **Включить режим квалифицированной подписи**. Сертификат после этого появится в личном хранилище сертификатов.

Открыть статью на сайте

Не поддерживается безопасное удаление файлов с атрибутом "сжатый"

Текст ошибки:

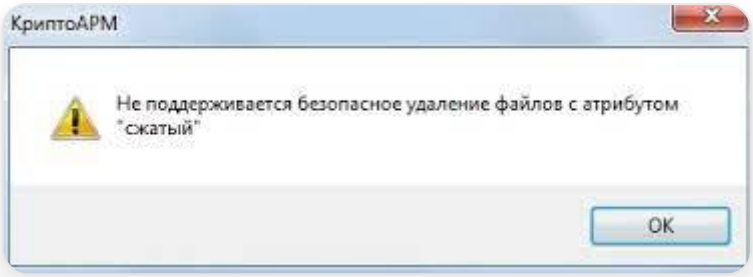
Ошибка сохранения сообщения (0x80004005)

Ошибка сохранения сообщения (0x80004005)

Произошла ошибка при создании подписи

Не поддерживается безопасное удаление файлов с атрибутом "сжатый"

Как выглядит ошибка:



Решение

При открытии документа для просмотра он сохраняется во временный файл. Информация о подписи так же при этом сохраняется во временный файл. Эти временные файлы впоследствии удаляются, и если в профиле включено безопасное удаление, то они перед этим перезаписываются случайными данными. Но со сжатыми файлами безопасное удаление не работает, поэтому и возникает предупреждение.

Безопасное удаление можно отключить в меню **Профили** - **Управление профилями** - профиль с галочкой открыть двойным кликом мыши.

Там на вкладке **Каталоги.** Нужно в выпадающем списке **Уровень безопасного удаления** выбр ать **Выключено**. Проверьте все профили. Если безопасное удаление отключено, а ошибка возникает, то стоит снять атрибут "сжатый" с папки временных файлов:

C:\Users<Имя пользователя>\AppData\Local\Temp

Открыть статью на сайте

В URL (сетевом адресе) указан неподдерживаемый протокол (0x00002ee6)

Текст ошибки:

Ошибка сохранения сообщения (0x80004005)

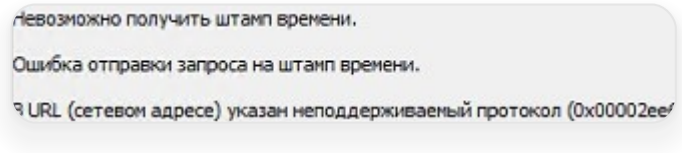
Ошибка сохранения сообщения (0x80004005)

Произошла ошибка при создании подписи

Ошибка создания атрибутов усовершенствованной подписи

В URL (сетевом адресе) указан неподдерживаемый протокол (0x00002ee6)

Как выглядит ошибка:



Решение

Пожалуйста проверьте, каким образом прописан адрес службы штампов времени в настройка х службы TSP.

Ссылка должна быть прописана с протоколом, без лишних пробелов.

Если выход в сеть ограничен прокси-сервером, то вы можете настроить параметры доступа в настройках Параметров прокси-сервера, задайте адрес также с использованием протокола.

Открыть статью на сайте

Содержание раздела

Операции с сетификатами

- Проверка на квалифицированность
- Как получить новый сертификат?
- Как создать самоподписанный сертификат?
- Импорт (установка) сертификата
- Хранение сертификатов
- Как проверить статус сертификата?
- Работа с квалифицированными сертификатами
- Просмотр информации о сертификате
- Фильтрация и сортировка сертификатов
- Печать сертификата
- Экспорт сертификата
- Удаление сертификата

Открыть статью на сайте

Содержание раздела

- Создание нового назначения
- Просмотр свойств назначения
- Импорт, экспорт и удаление назначения
- Операции с ключевыми носителями

Открыть статью на сайте

Содержание раздела

Управление профилями

- Операции с профилями
- Общие параметры профиля
- Настройки операции подписи
- Настройки операции шифрования
- Настройки операции расшифрования
- Настройки управления интерфейсом
- Настройки использования политик сертификатов
- Настройки верификации сертификатов
- Настройки службы штампов времени TSP
- Настройки службы актуальных статусов OCSP

Открыть статью на сайте

Содержание раздела

Параметры программы

- Интерфейс программы
- Общие настройки
- Режим "Квалифицированная подпись"
- Упрощенный режим работы
- Параметры прокси-сервера
- Настройки каталогов хранения файлов

Открыть статью на сайте

Содержание раздела

- Как создать запрос на получение сертификата
- Просмотр информации о запросах, фильтрация и сортировка запросов в списке
- Как создать запрос на аннулирование сертификата

Открыть статью на сайте

Содержание раздела

- Установка списка отзывов в хранилище
- Просмотр информации о списках
- Фильтрация и сортировка списков отзыва
- Экспорт и удаление списков отзыва

Открыть статью на сайте

Содержание раздела

- Как создать список доверенных сертификатов?
- Установка списка в хранилище
- Просмотр информации о списке
- Фильтрация и сортировка списка
- Экспорт и удаление списка
- Операции с криптопровайдерами

Открыть статью на сайте

Содержание раздела

Ошибки, возникающие при установке КриптоАРМ

- Ошибка пакета Windows installer
- Ошибка в ходе установки сборки
- Внутренняя ошибка 2739
- Не удалось открыть подраздел: UNKNOWN/Components
- Координатор установщика Windows

Ошибки, возникающие при установке сертификата

- При установке следующих сертификатов возникли ошибки
- Ошибка построения пути сертификации

Ошибки, возникающие при установке лицензии

- Ошибка сохранения данных
- Некорректный формат лицензии

Ошибки, возникающие при подписании файлов

- Ошибка исполнения функции (0x0000065b)
- Указан неправильный алгоритм (0x80090008)
- Предупреждение «Нет полного доверия к сертификату подписи»
- Ошибка установки свойства в контекст сертификата (0x80092004)
- Выбранный вами сертификат не действителен, продолжить его использование?
- Отказано в доступе. (0x80090010)
- Не найден используемый криптопровайдер. Возможно он не установлен, запрещен или не поддерживается.
- Носитель ключевого контейнера не поддерживается данной лицензией (0x80070057)
- КриптоАРМ зависает (не отвечает) в момент выбора сертификата подписи

Ошибки, возникающие при расшифровании файлов

- Отсутствует личный сертификат для расшифрования
- Неизвестный криптографический алгоритм. (0x80091002)
- Неправильное значение индекса. (0x80091008)

Ошибки, возникающие при подписании с использованием штампа времени и доказательств подлинности

- Error initialize resource dll, неизвестная ошибка
- Данные настройки для этого продукта повреждены. Обратитесь в службу поддержки. (0x0000064a)

Другие ошибки

- Отсутствует список аккредитованных УЦ
- Внутренняя ошибка (CSP). (0x80090020)
- Установка сертификатов из файла p7b и cer

Открыть статью на сайте

Содержание раздела

- Как подписать электронный документ?
- Как добавить соподпись (параллельную подпись)?
- Добавление заверяющей подписи
- Как проверить электронную подпись?
- Снятие и проверка подписи
- Как зашифровать данные?
- Как расшифровать данные?
- Как подписать и зашифровать электронный документ?
- Как расшифровать и проверить подпись на электронном документе?
- Как просмотреть зашифрованный документ?
- Как получить штамп в службе штампов времени?
- Как просмотреть штамп времени?

Открыть статью на сайте

Содержание раздела

- Где скачать дистрибутив КриптоАРМ и как его правильно выбрать?
- Как установить КриптоАРМ?
- Где купить лицензию на КриптоАРМ?
- Временная лицензия и срок ее действия
- Проверка наличия ГОСТ - криптопровайдера
- Установка лицензии
- Удаление программы