



Начинаем работать с программой “КриптоАРМ”

Кратко о самом главном

1

Мы расскажем о самых важных моментах работы с программой и постараемся дать ответы на часто задаваемые вопросы.

2

Подробное руководство пользователя вы найдете

- на сайте www.trusted.ru “Поддержка” - “Центр загрузки”
- в самой программе “КриптоАРМ” - меню “Помощь”.

3

Здесь вы узнаете

- Как установить и настроить программу?
- Как установить цифровой сертификат с токена на компьютер?
- Как подписать файл электронной подписью и проверить ее?
- Как зашифровать файл?

Что такое “КриптоАРМ”?



Программа для
электронной подписи и
шифрования данных



Соответствует всем
требованиям российского
законодательства в части
обеспечения юридически
значимого статуса

- 
- проста в установке и настройке,
 - удобна в работе,
многофункциональна,
 - универсальна: подходит для
многих информационных систем

Устанавливаем «КриптоАРМ»

Скачайте программу «КриптоАРМ»

Вы найдете дистрибутив на установочном диске при покупке ПО либо на официальных сайтах (www.trusted.ru, www.cryptoarm.ru).

Выберите версию программы

В комплекте с сертифицированным криптопровайдером «КриптоПро CSP»

- **«Старт»** вы сможете только проверять корректность электронных подписей под документами, без возможности подписывать и шифровать данных
- **«Стандарт»** - базовая версия, в которой доступен весь основной функционал по работе с электронной подписью, шифрованию и управлению цифровыми сертификатами
- **«Стандарт Плюс»** имеет одно дополнение: работает с USB-токенами с криптографией «на борту» (eToken ГОСТ и Рутокен ЭЦП)

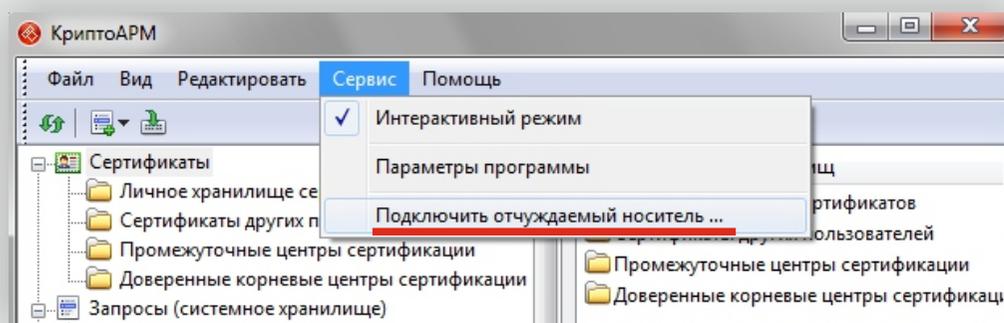
При архивном (длительном) хранении электронных данных используется усовершенствованная электронная подпись. Такой формат подписи предполагает работу с доверенными сервисами - Службой штампов времени и Службой актуальных статусов сертификатов. В этих условиях вам потребуется **комплект «КриптоАРМ Стандарт PRO»**.

Самостоятельно установите программу

Установить «КриптоАРМ» на компьютер совсем несложно. Вы самостоятельно сможете пройти все шаги установки. Единственное, что нужно помнить: вы должны обладать правами администратора на компьютере, где устанавливаете ПО

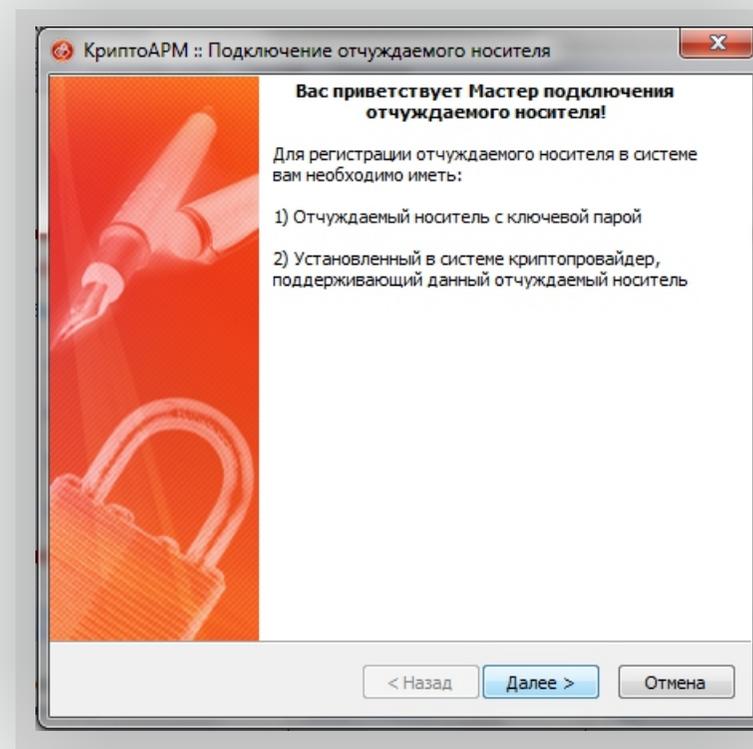
Устанавливаем сертификаты и списки отзыва на компьютер

С помощью программы «КриптоАРМ» вы можете удобно работать с цифровыми сертификатами: устанавливать на компьютер, проверять статус, просматривать и печатать информацию о сертификате и многое другое.



1 В главном окне программы откройте режим «Эксперт»

На верхней панели инструментов выберите пункт «Сервис» -> «Подключить отчуждаемый носитель» и следуйте инструкциям.



2 Выберите из списка криптопровайдер, который планируете использовать.

В качестве ключевого носителя укажите «Смарт-карта/USB-токен».

3 Вставьте USB-токен

Основная информация
Укажите криптопровайдер и тип носителя. Установите носитель перед переходом на следующий шаг мастера.

Выберите криптопровайдер
Crypto-Pro GOST R. 34.10-2001 Cryptographic Service Provider

Выберите тип носителя
Смарт-карта/USB-Токен

Для продолжения необходимо вставить носитель

< Назад Далее > Отмена

Выбор ключевых контейнеров
Выберите подключаемые контейнеры

Список контейнеров

Имя	Идентификатор
<input checked="" type="checkbox"/> Контейнер 01	665e0e1c-97de-40ae-a04d-d655952440a1

Просмотреть сертификат в контейнере

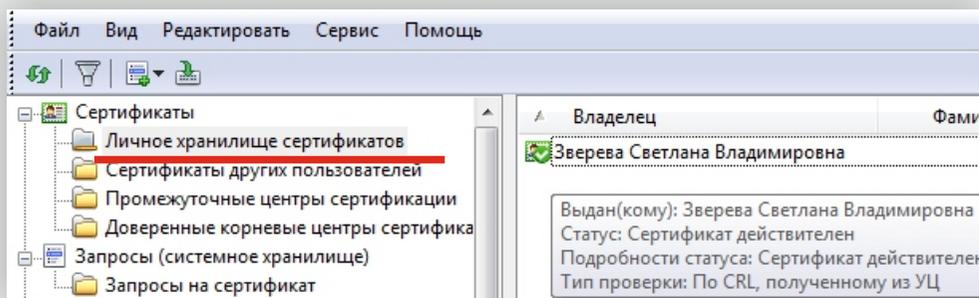
< Назад Готово Отмена

4 Выберите из списка контейнер с нужным сертификатом.

Введите пин-код к USB-токену.

5 Сертификат успешно установлен в личное хранилище сертификатов на ваш компьютер

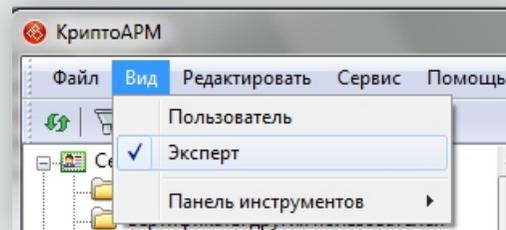
Чтобы «КриптоАРМ» доверял вашему сертификату полностью, добавьте сертификат УЦ в список доверенных центров сертификации



Настраиваем программу

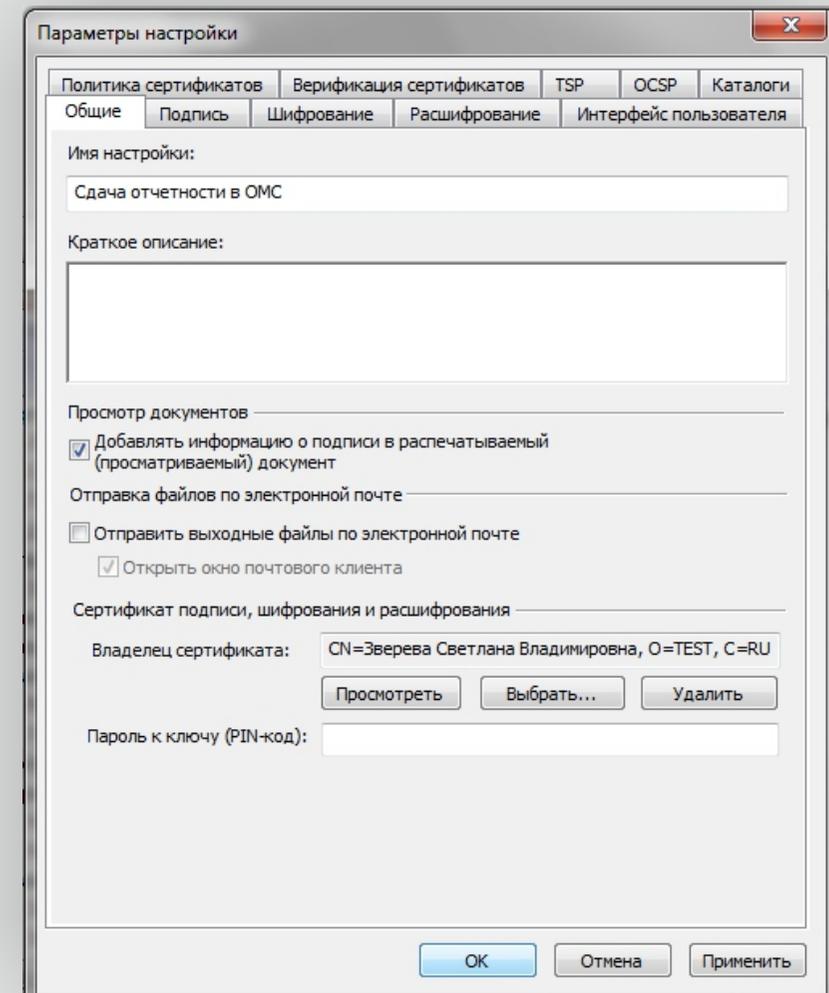
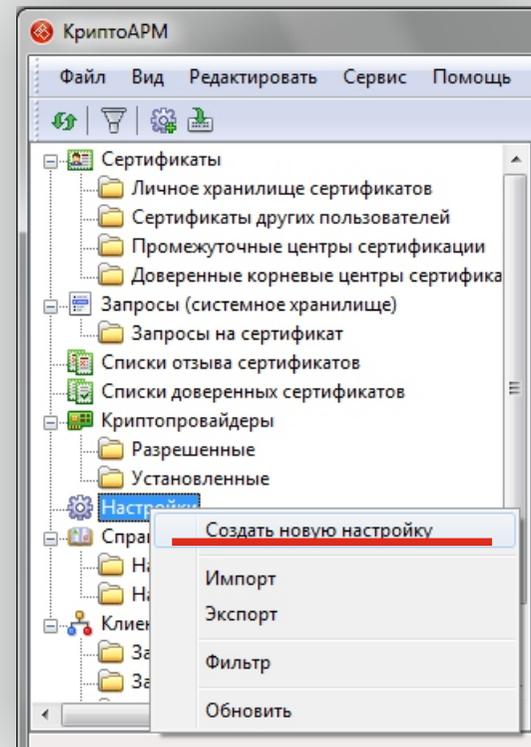
Вы можете намного упростить себе жизнь, создав типовые настройки (шаблоны) для работы с программой. Будьте уверены, «КриптоАРМ» выполнит операции точно по заданным вами параметрам.

1 Откройте «КриптоАРМ» - Вид «Эксперт»



2 Создайте новую настройку

В разделе «Настройки» откройте контекстное меню и выберите «Создать новую настройку»



3 Настройте параметры электронной подписи

В закладке «Подпись» - укажите

- «Сохранять подпись в отдельном файле», если того требует система, с которой вы работаете
- чтобы уменьшить размер отправляемых по почте данных, установите архивирование подписанных данных
- нужный формат и расширение подписанных данных

Политика сертификатов | Верификация сертификатов | TSP | OCSP | Каталоги

Общие | Подпись | Шифрование | Расшифрование | Интерфейс пользователя

Параметры подписи

Тип хэш алгоритма: SHA-1

Формат подписи: Классическая

Использование подписи: [Не задано]

Комментарий к подписи:

Идентификатор ресурса:

Помещать имя исходного файла в поле "Идентификатор ресурса"

Включать время создания подписи

Включать в подпись штамп времени на подпись на подписываемые данные

Включать в подпись: Только сертификат владельца

Сохранять подпись в отдельном файле

Удалять исходный файл после создания подписи

Выходной формат и расширение файла подписи

DER - кодировка *.sig BASE64 - кодировка *.sig

Отключить служебные заголовки

Включать архивирование

Сохранять структуру вложенности каталогов

Установить ассоциацию

4 Настройте параметры проверки статуса сертификатов

В закладке «Верификация сертификатов» - выберите «Получение CRL из УЦ». Нажмите кнопку «Добавить все УЦ»

Политика сертификатов | Верификация сертификатов | TSP | OCSP | Каталоги

Сертификаты, для которых необходимо получение CRL из

Владелец	Издатель	Серийный номер
<input checked="" type="checkbox"/> *	*	*

Добавить... | **Добавить все УЦ** | Удалить | Удалить все

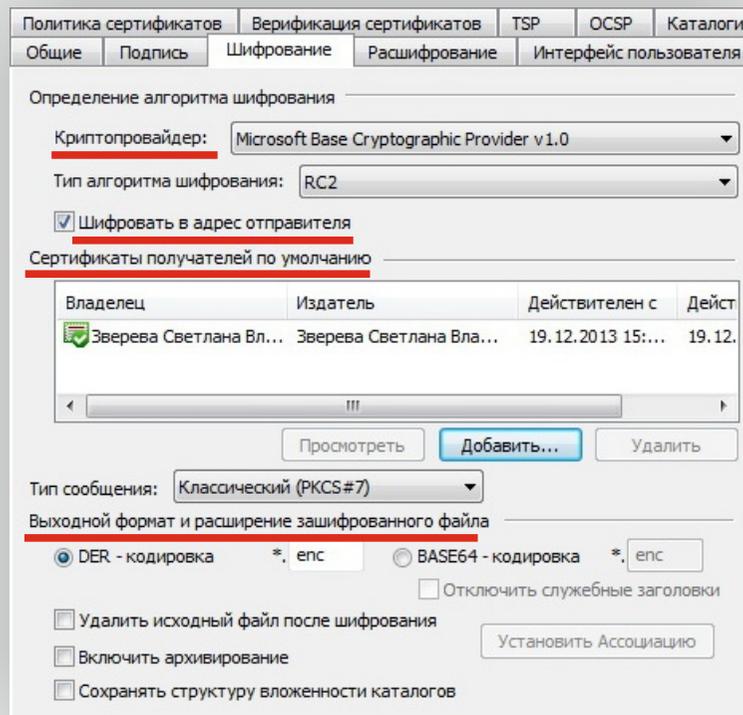
В данном списке для сертификатов, не отмеченных галочкой, CRL не будут загружаться из УЦ, если не выпущено новой версии.

Получение CRL из УЦ | Revocation Provider | Служба актуальных статусов (OCSP)

5 Настройте параметры шифрования

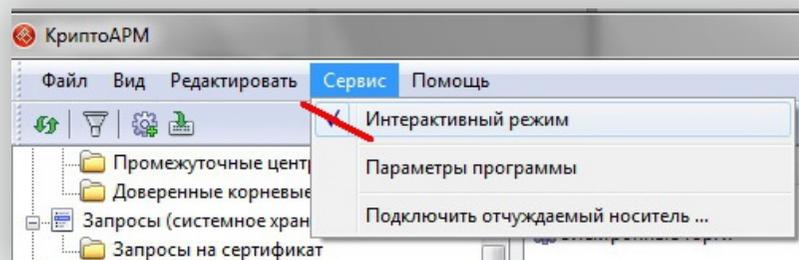
В закладке «Шифрование» - укажите

- криптопровайдер, который будете использовать для шифрования
- «Шифровать в адрес отправителя», чтобы вы смогли расшифровать свои данные
- сертификаты получателей зашифрованных данных
- нужный формат и расширение зашифрованных данных



Настройка /если она одна/ будет использоваться по умолчанию.

Чтобы начать работу с настройками, отключите пошаговый режим выполнения операций. Для этого в верхнем меню в «Сервисе» уберите галочку у строки «Интерактивный режим»



Подписываем электронной подписью

Любые электронные данные

Подписать можно документы, отсканированные образы, презентации, видео, таблицы, базы данных и т.п. (*.doc, *.pdf, *.jpeg, *.png, *.xml и др.)

Один файл или целую папку

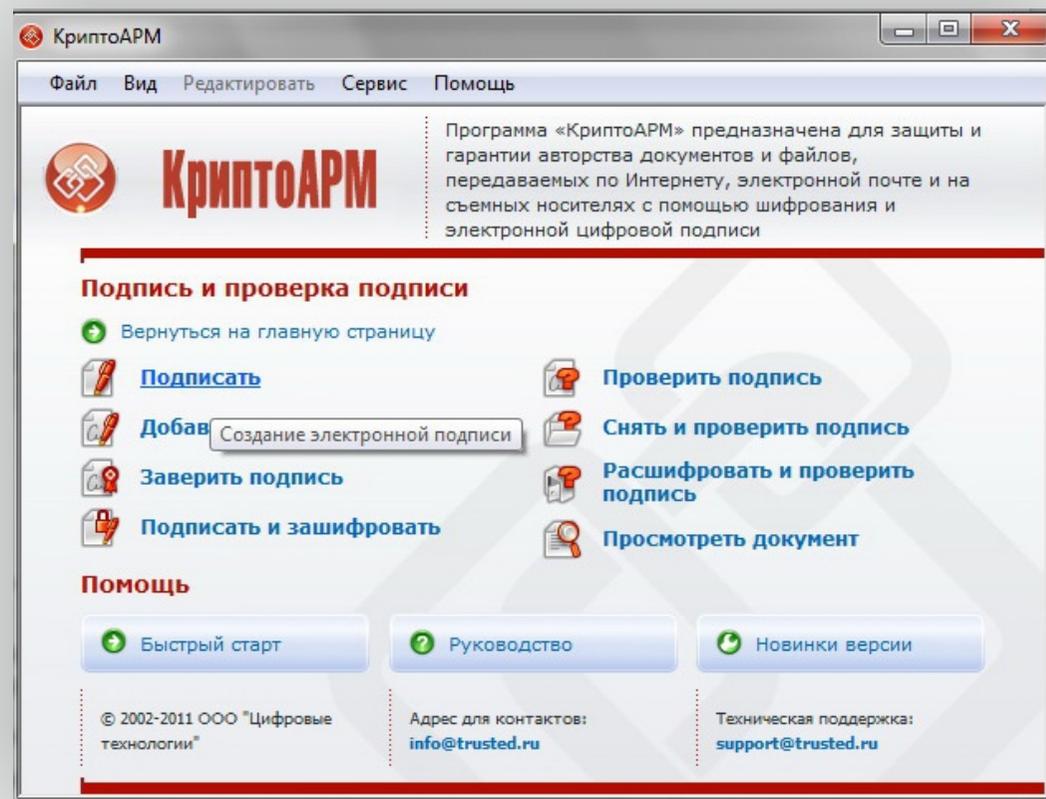
Вы можете подписать как один файл, так сразу и целую папку. При этом каждый файл из указанной папки будет подписан своей электронной подписью.

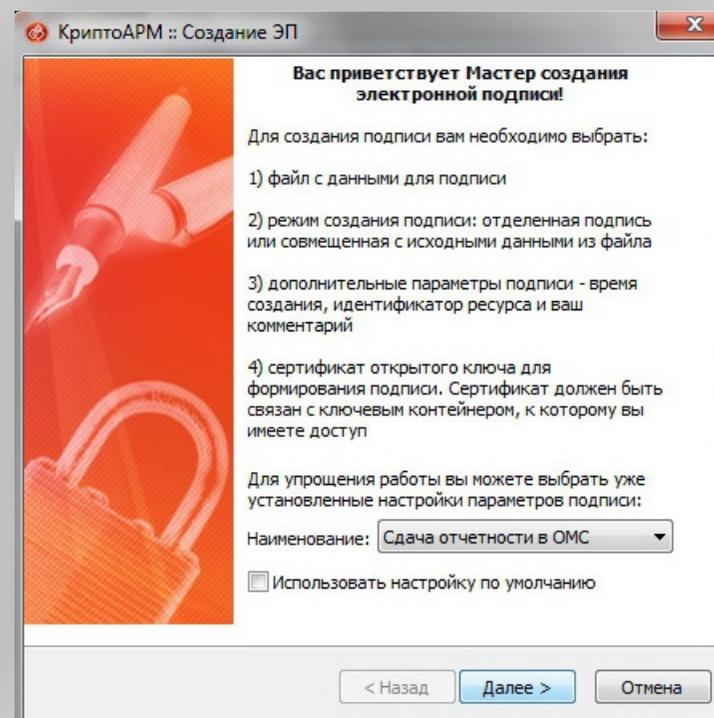
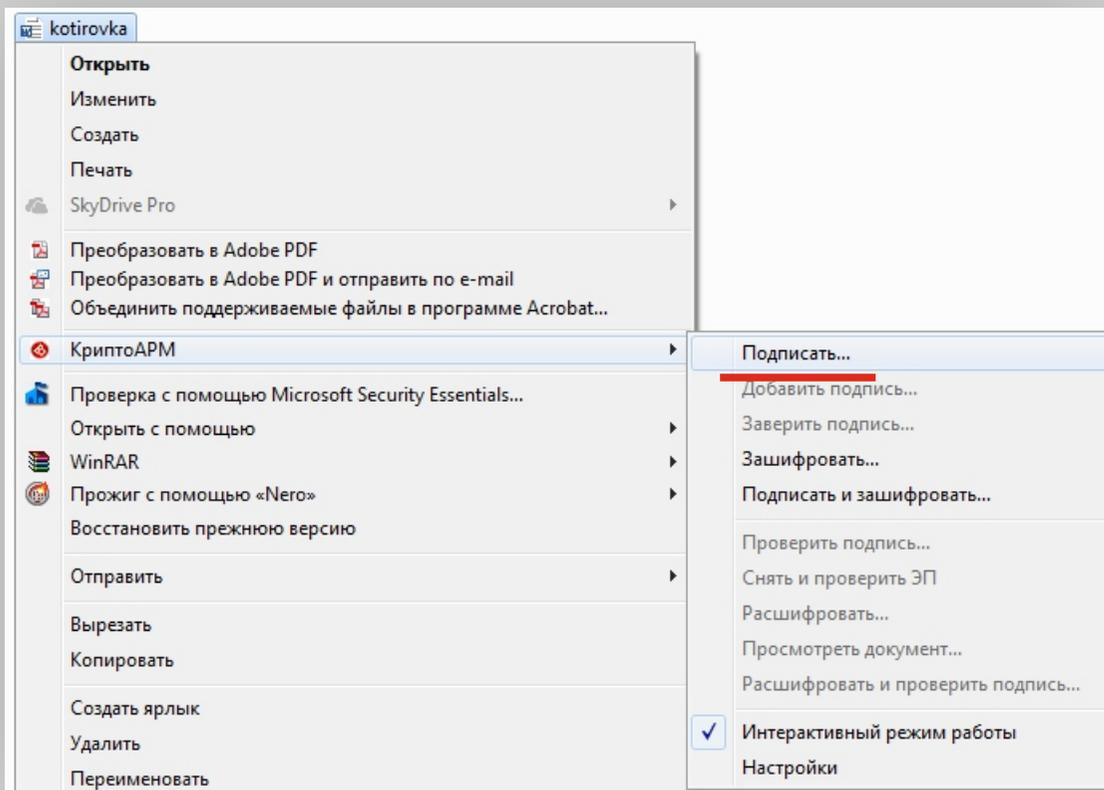
Разными электронными подписями

Электронная подпись может быть создана в двух вариантах: совмещенная с подписываемыми данными и отделенная (т.е. отдельным файлом)

Разными способами

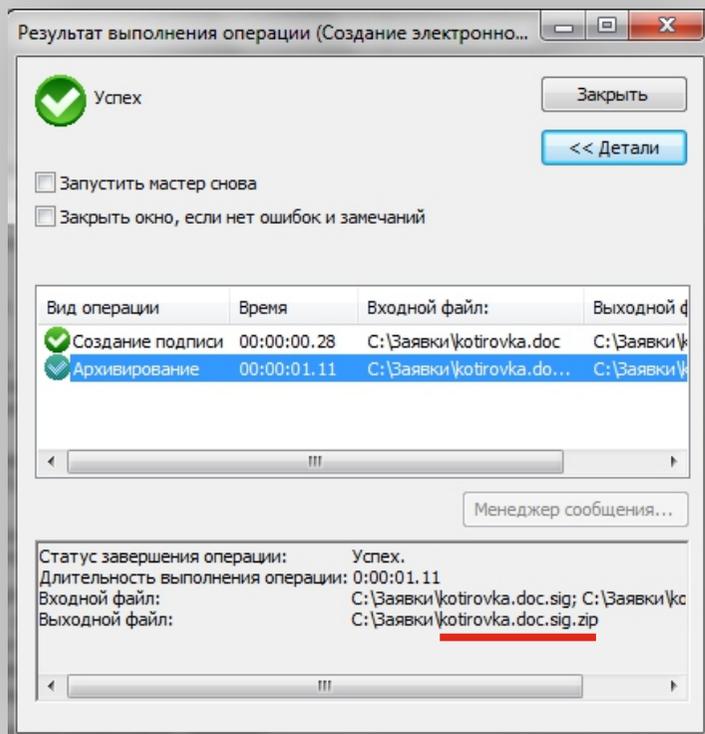
Выберите, как вам удобно подписывать: из главного окна программы, из контекстного меню файла или из панели задач на вашем рабочем столе. В любом случае выбирайте пункт “Подписать” и следуйте инструкциям.



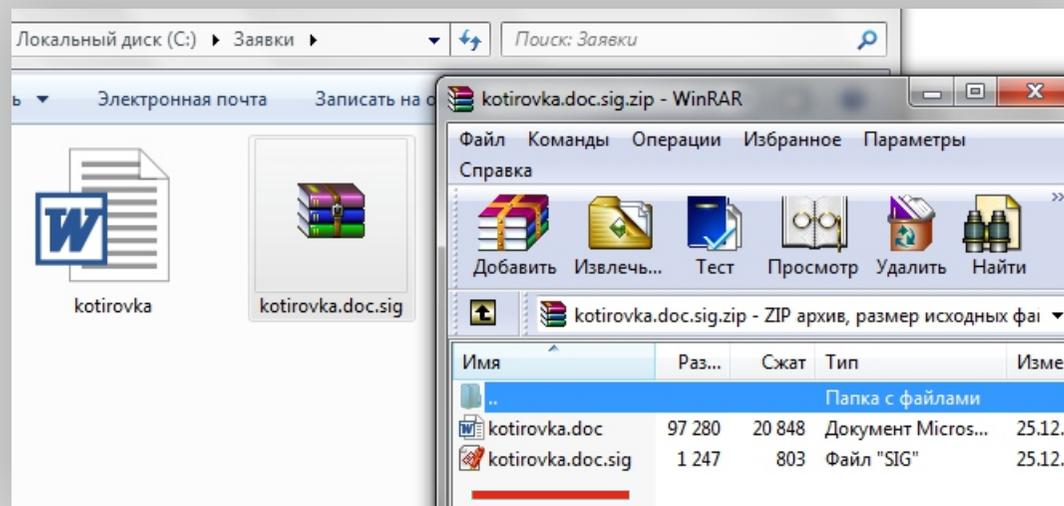


1 На файле, который нужно подписать, правой клавишей мыши откройте контекстное меню и выберите пункт «Подписать»

2 Выберите заранее созданную типовую настройку



3 «КриптоАРМ» подпишет данные строго по заданному шаблону



4 Наш документ, подписанный электронной подписью, обозначается специальным значком. Файл электронной подписи имеет расширение *.sig

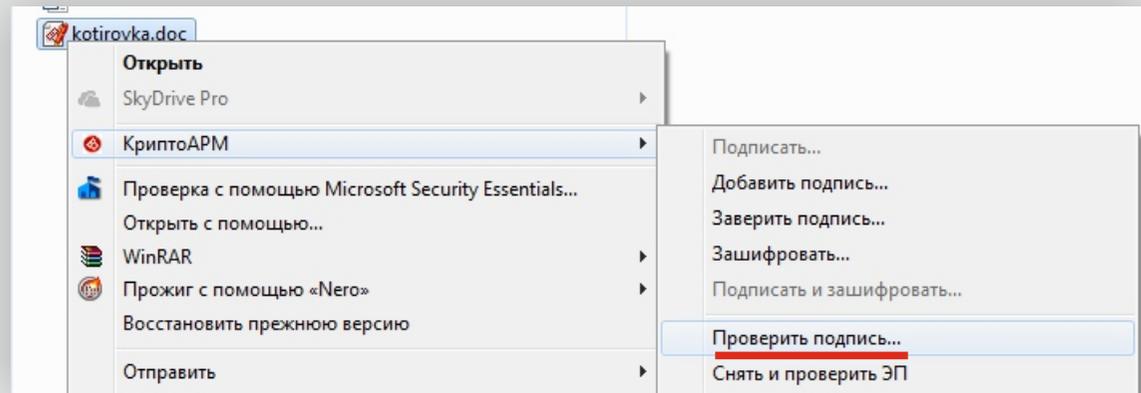


Проверяем, корректна ли электронная подпись

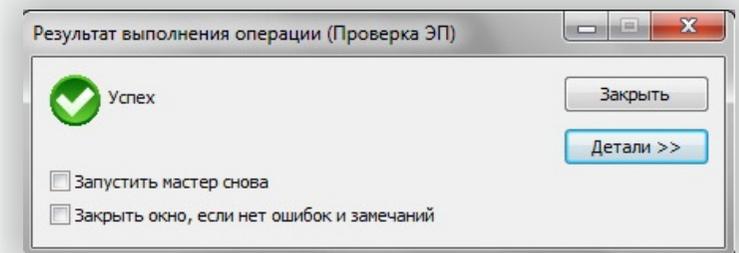
Проверить электронную подпись вы можете также разными способами: и из главного окна, и из контекстного меню файла.

Если вы проверяете отдельную подпись, воспользуйтесь пунктом **«Проверить подпись»**.

Если вам нужно проверить подпись, совмещенную с данными, используйте вариант **«Снять и проверить подпись»**.



1 На файле, который нужно подписать, правой клавишей мыши откройте контекстное меню и выберите пункт **«Подписать»**. Следуйте инструкциям



2 В конце проверки вы увидите результат

Шифруем электронные данные

Любые электронные данные

Зашифровать можно документы, отсканированные образы, презентации, видео, таблицы, базы данных и т.п. (*.doc, *.pdf, *.jpeg, *.png, *.xml и др.)

Один файл или целую папку

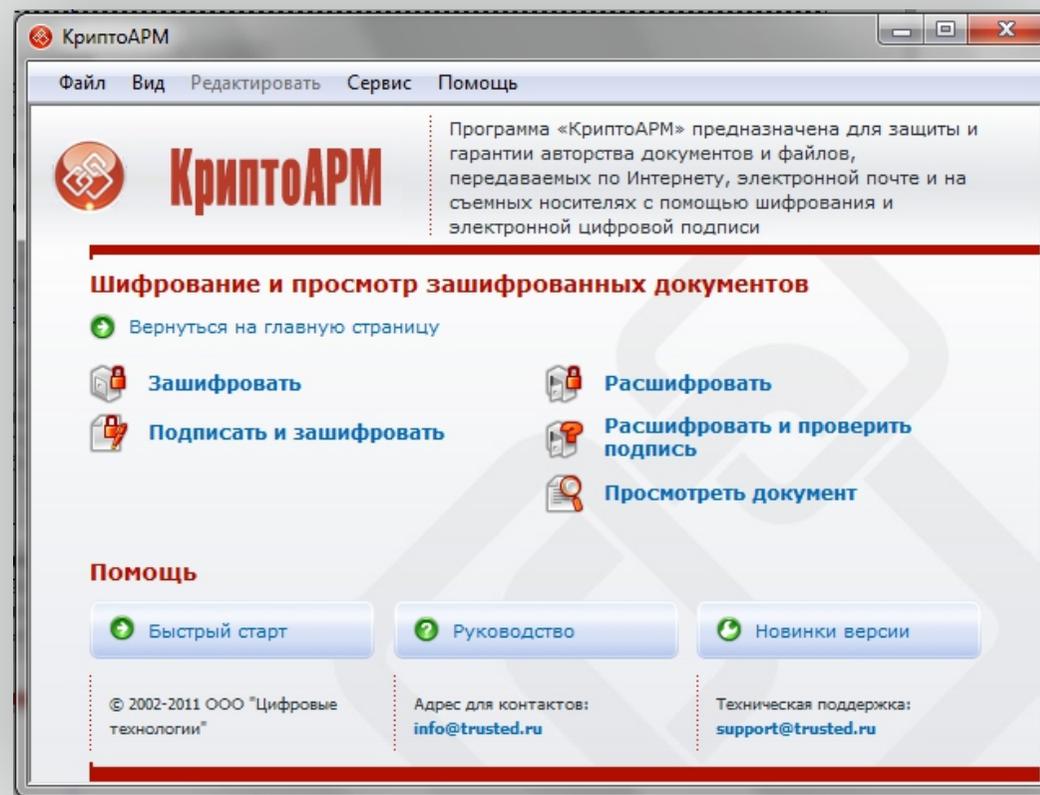
Вы можете зашифровать как один файл, так сразу и целую папку. При этом каждый файл из указанной папки будет зашифрован отдельно.

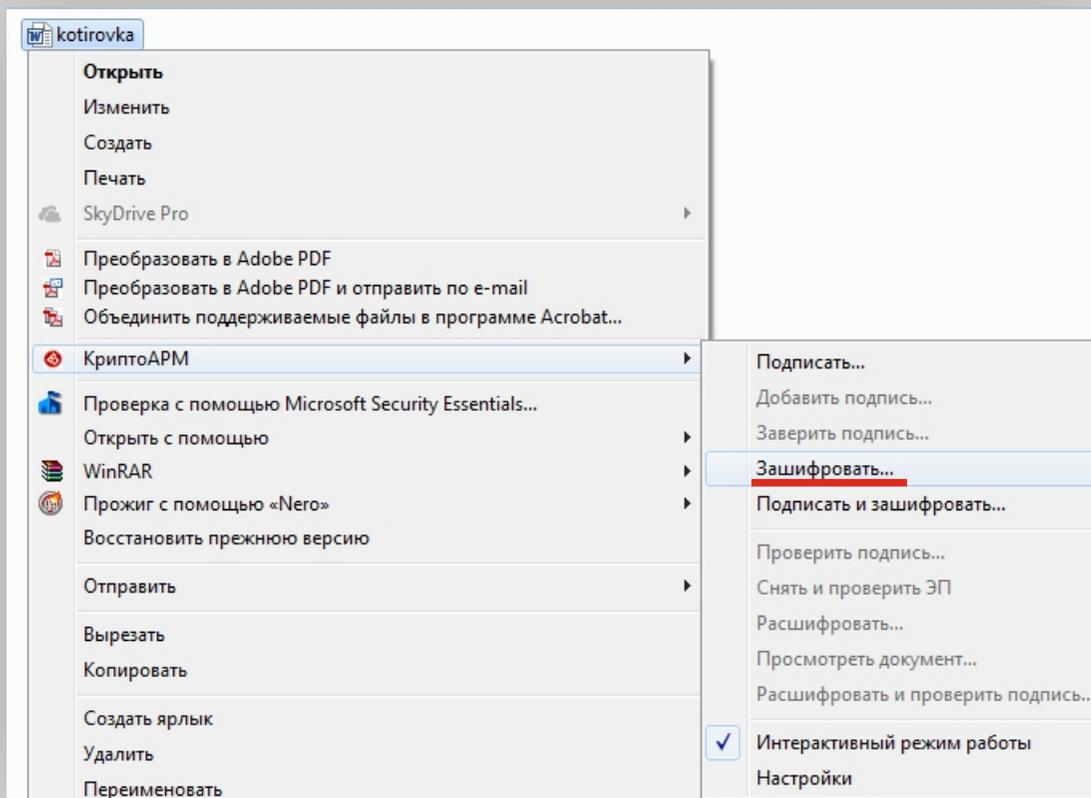
Разными способами

Выберите, как вам удобно шифровать: из главного окна программы, из контекстного меню файла или из панели задач на вашем рабочем столе. В любом случае выбирайте пункт “Зашифровать” и следуйте инструкциям.

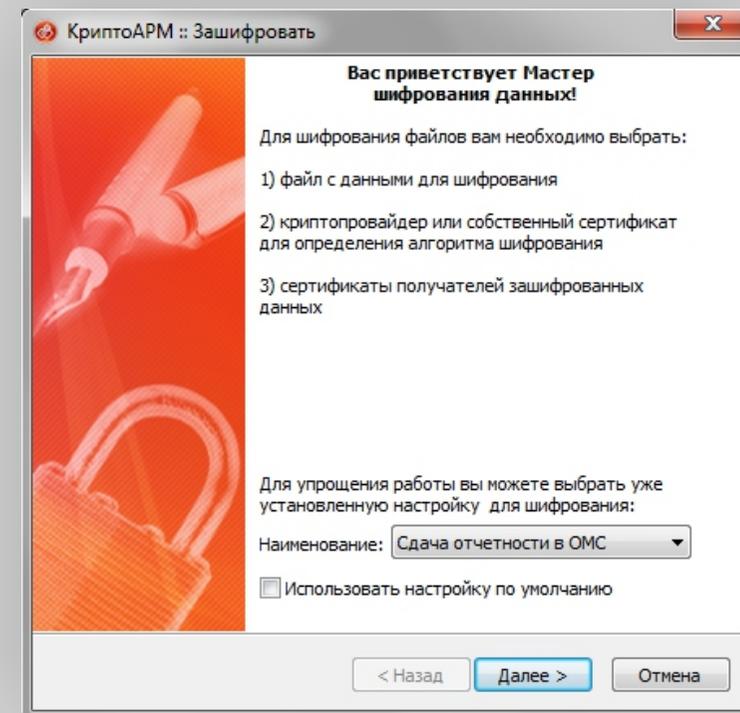
Зашифрованные данные можно подписать

Зашифровав файл, вы сможете одновременно и подписать его своей электронной подписью

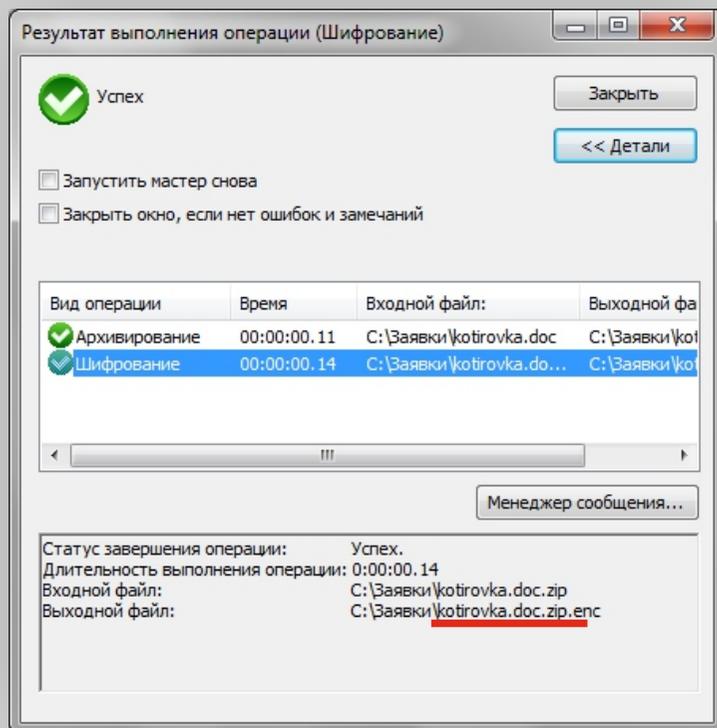




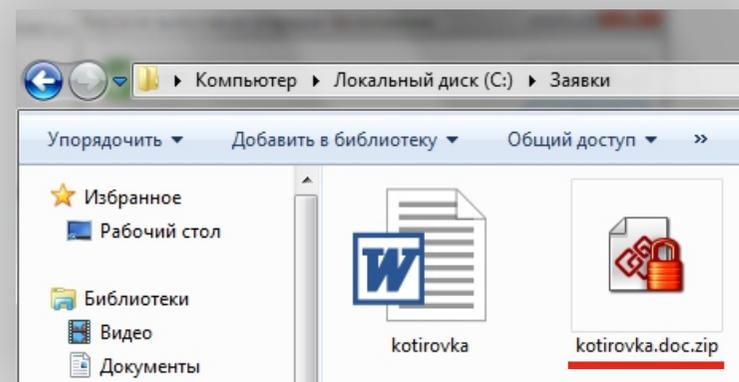
1 На файле, который нужно зашифровать, правой клавишей мыши откройте контекстное меню и выберите пункт «Зашифровать»



2 Выберите заранее созданную типовую настройку



3 «КриптоАРМ» зашифрует данные строго по заданному шаблону



4 Зашифрованные данные обозначаются специальным значком



“КриптоАРМ”

Ваша правая рука в электронном мире

www.trusted.ru
www.cryptoarm.ru