

## Формирование ЭП с помощью программы «КриптоАРМ»

С помощью программы "КриптоАРМ" вы можете подписать

- отдельный файл
- 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 (создать первичную электронную подпись) вы можете через:

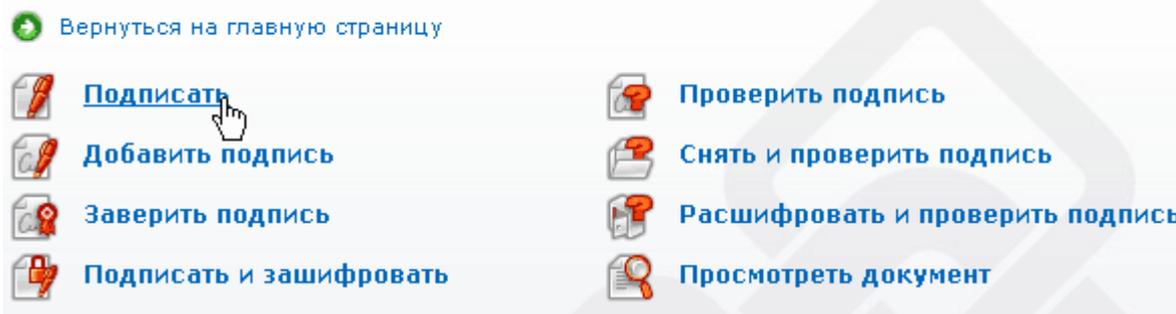
- Главное окно программы
- КриптоАРМ Агент
- контекстное меню

Чтобы открыть главное окно программы "КриптоАРМ" активизируйте приложение "КриптоАРМ" (Пуск - > Программы - > **Digit** - > **КриптоАРМ** - > **КриптоАРМ**)

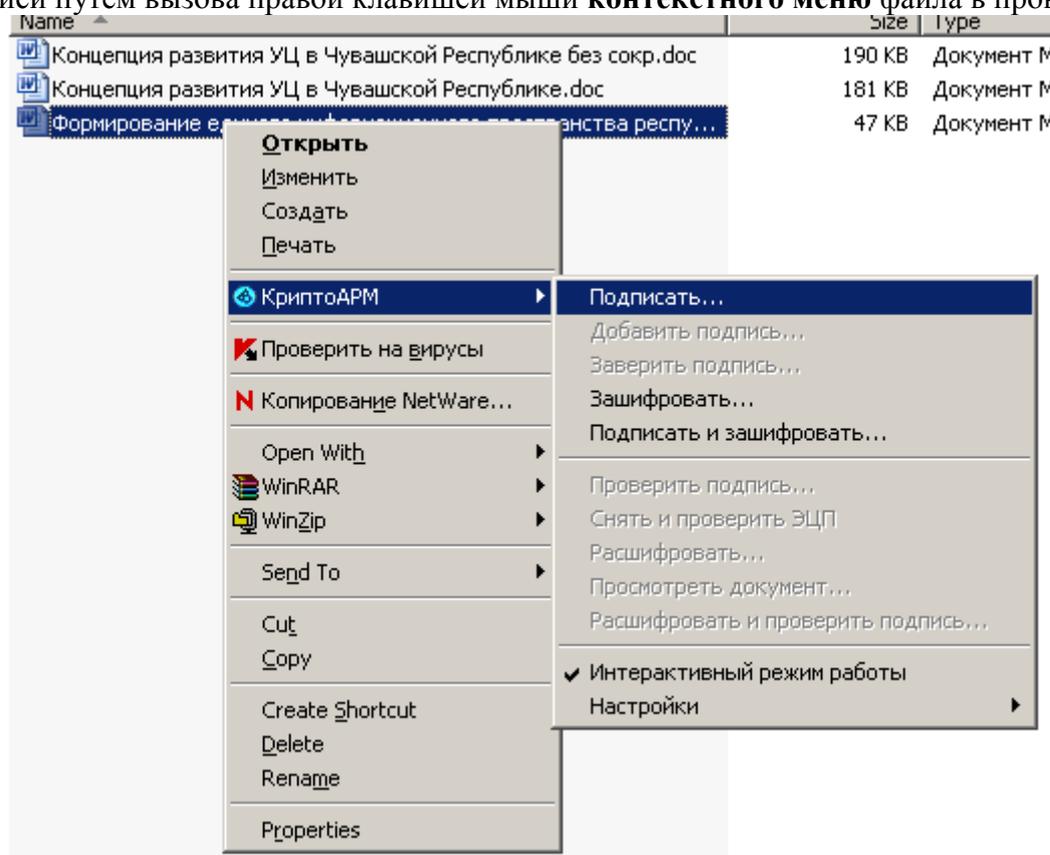
Для того чтобы подписать данные, выберите пункт меню **Подписать...**:

- Главное окно, вид "Пользователь":

### Подпись и проверка подписи

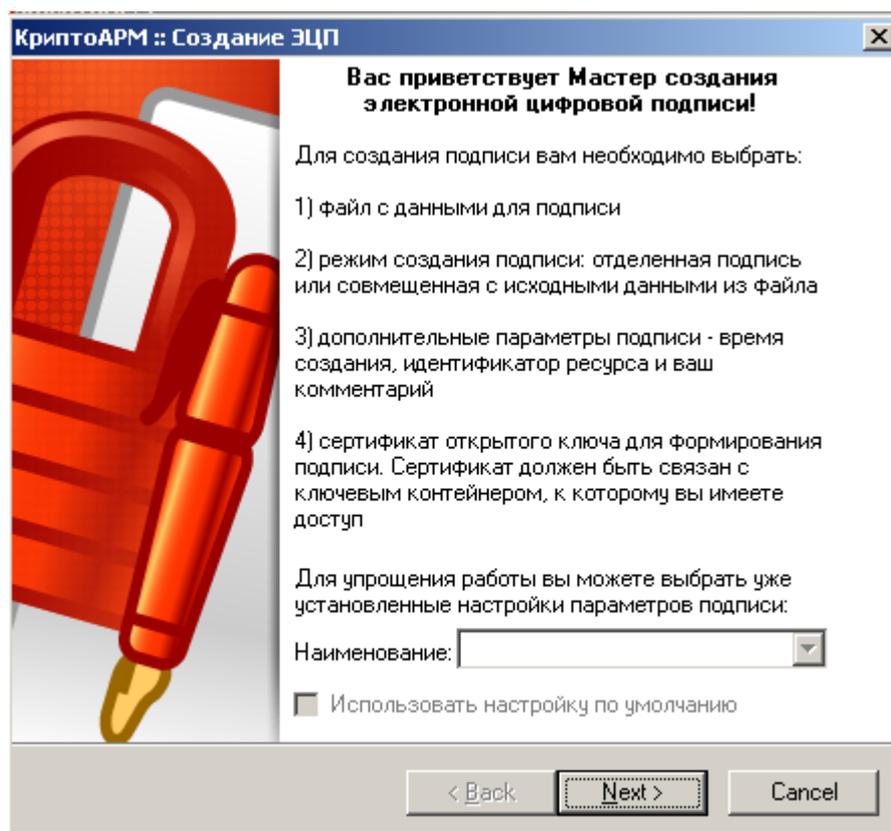


Рекомендуется использовать наиболее удобный способ, позволяющий производить операцию подписи путем вызова правой клавишей мыши **контекстного меню** файла в проводнике Windows.

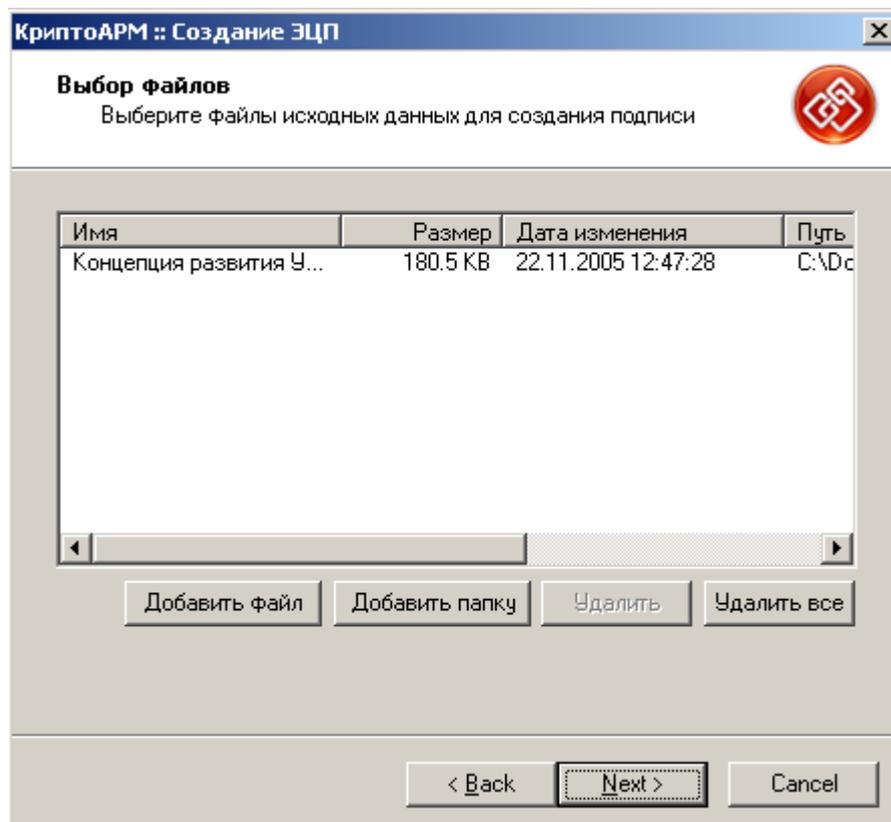


Далее следуйте рекомендациям Помощника по выполнению операции:

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**.



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



В открывшемся окне укажите кодировку и расширение выходного файла и требуется ли заархивировать подписанные файлы.

Выходной файл может быть сформирован в формате \*.sig, \*.p7s

Для формата PKCS#7 Message 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").

КриптоАРМ :: Создание ЭЦП

**Выходной формат**  
Выберите желаемый выходной формат файла подписи

Кодировка и расширение

DER-кодировка \* .sig

BASE64-кодировка \* .sig

Отключить служебные заголовки

Архивировать файлы после создания подписи

Имя архива: C:\Documents and Settings\info4\My Docu 

< Back   Next >   Cancel

КриптоАРМ :: Создание ЭЦП

**Параметры подписи**  
Установите желаемые параметры подписи

Свойства подписи

Комментарий к подписи:

Идентификатор ресурса:

Поместить имя исходного файла в поле "Идентификатор ресурса"

Сохранить подпись в отдельном файле

Удалить исходный файл после выполнения операции

Включить время создания подписи

Включить штамп времени на подписываемые данные

Включить штамп времени на подпись

Включить в подпись доказательства подлинности

< Back   Next >   Cancel

Далее введите необходимые свойства подписи (комментарий к подписи\*, идентификатор ресурса\*\*, включение времени создания подписи).

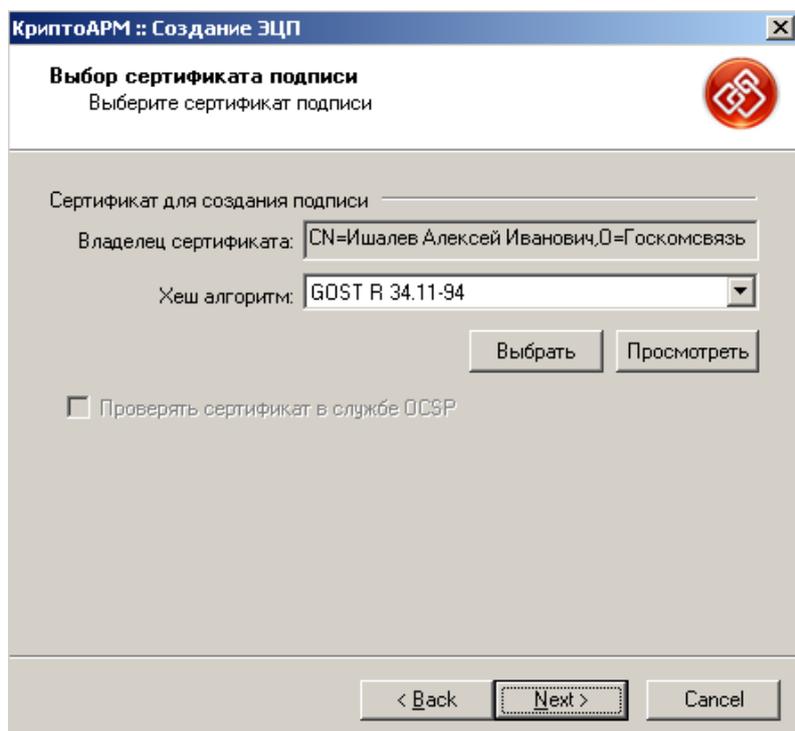
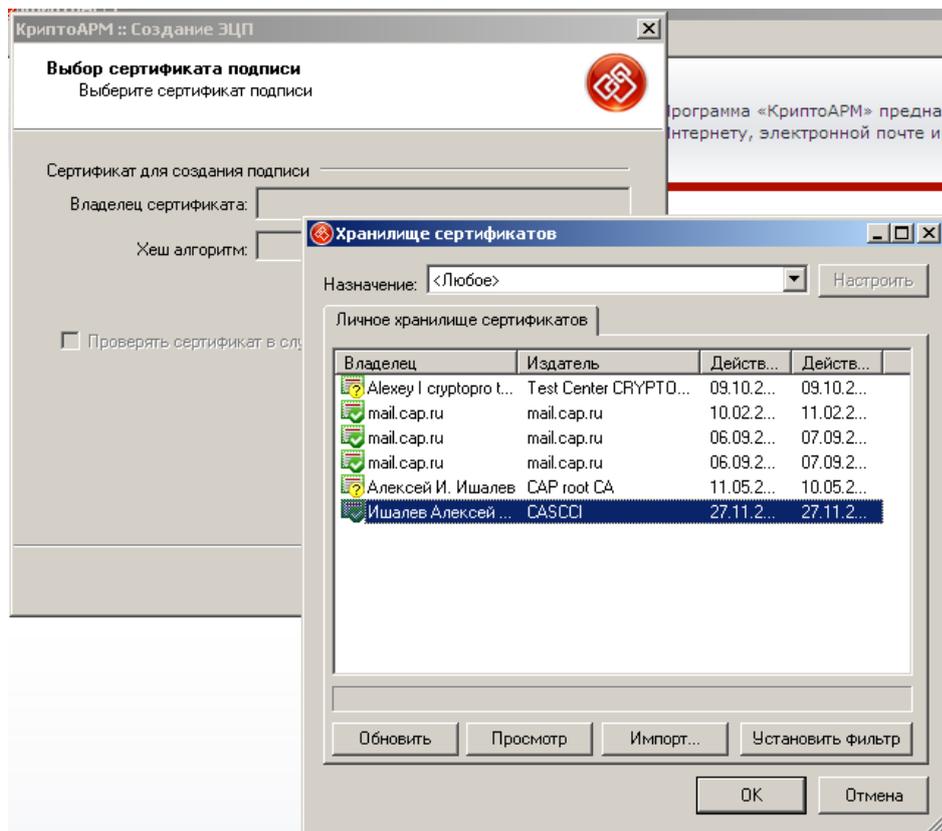
\* Комментарием к подписи может служить информация, предназначенная для прочтения людям, просматривающим подписанный документ (например, "Согласовано!")

\*\* Под идентификатором ресурса понимается:

- путь до исходного, подписываемого файла (на компьютере или в Интернете, где находится данный файл)

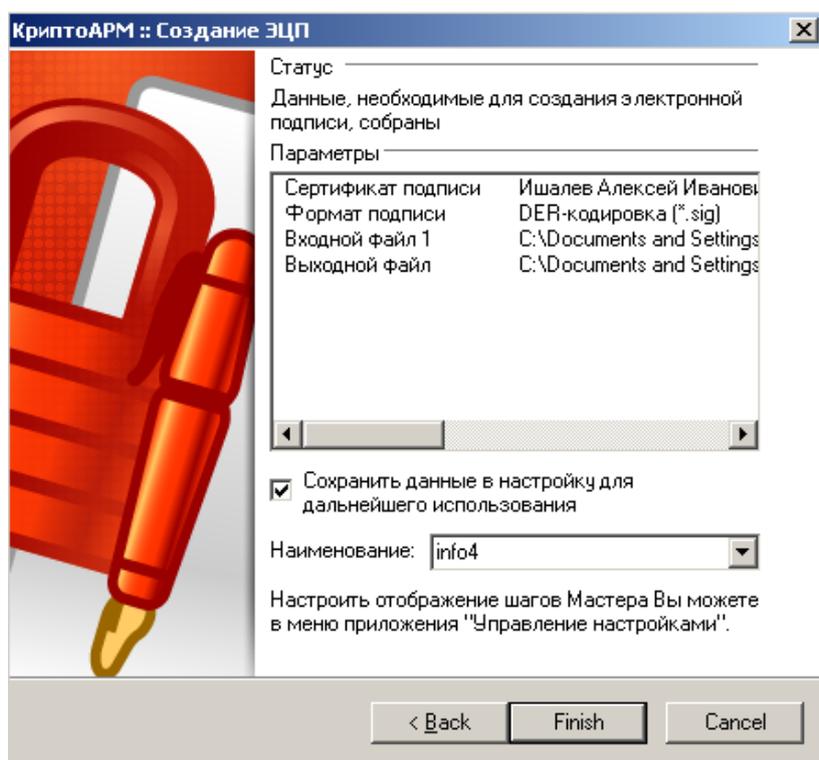
- имя файла (указывается для того, чтобы в случае изменения имени файла получатель подписанного документа смог определить первоначальное его название)

Укажите необходимые параметры ЭП - личный сертификат для создания ЭП.



Для доступа к выбранному ключевому контейнеру введите пароль.

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 флажок 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.

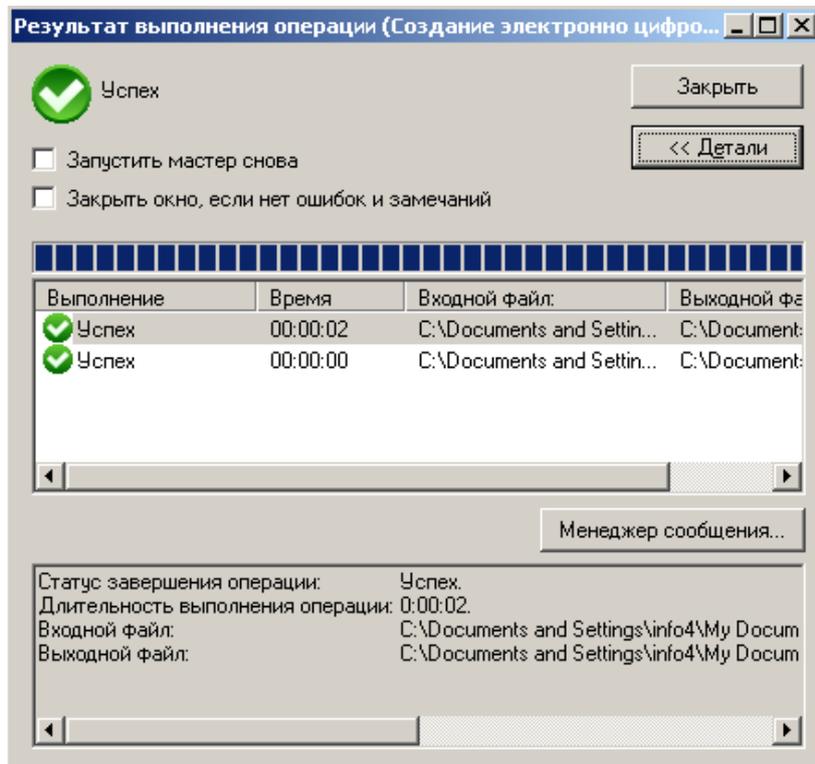
Начнется процесс подписи файла. Остановить процесс можно, нажав на кнопку **Отмена**.

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:



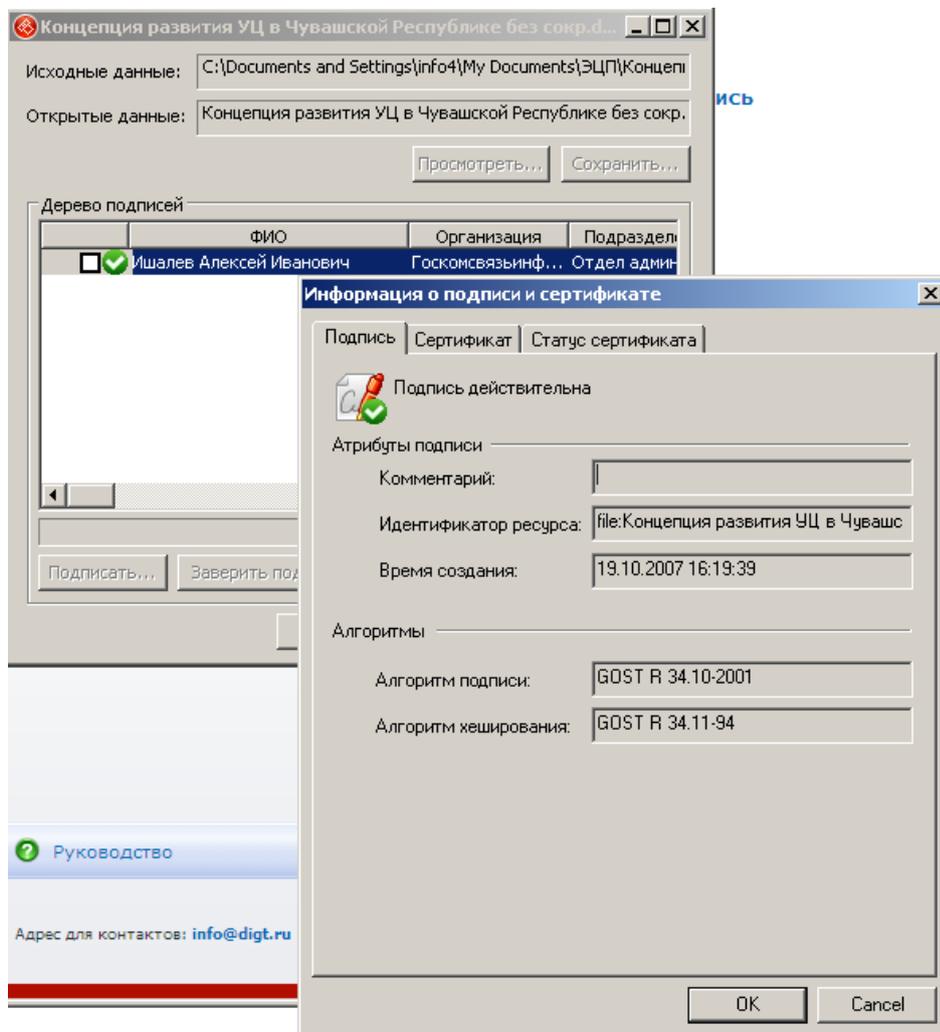
После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах создания подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции, длительность выполнения операции, нажмите кнопку **Детали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

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 информацию о подписи и сертификате:

- просмотреть подписанный файл, нажав на кнопку **Просмотреть** напротив имени файла,
- сохранить по указанному пути, нажав на кнопку **Сохранить**,
- просмотреть информацию о подписи, сертификате и его статусе (кнопка **Просмотреть**)



Проверка электронной цифровой подписи

С помощью программы "КриптоАРМ" вы можете проверить корректность электронной цифровой подписи

- отдельного файла
- папки файлов (при этом будет проверена подпись каждого файла, входящего в указанную папку. Выходные файлы автоматически сохраняются в папку с исходными данными)

! Проверка корректности всех вариантов и типов подписи выполняется по единой схеме, за исключением следующего момента:

- При проверке совмещенной подписи сначала выполняется снятие подписи с данных и сохранение подписанных данных в отдельный файл, а после этого - собственно проверка корректности подписи. Поэтому для того чтобы проверить корректность совмещенной подписи, в контекстном меню программы выберите пункт **Снять и проверить подпись**.

- При проверке отделенной подписи выберите пункт **Проверить подпись**.

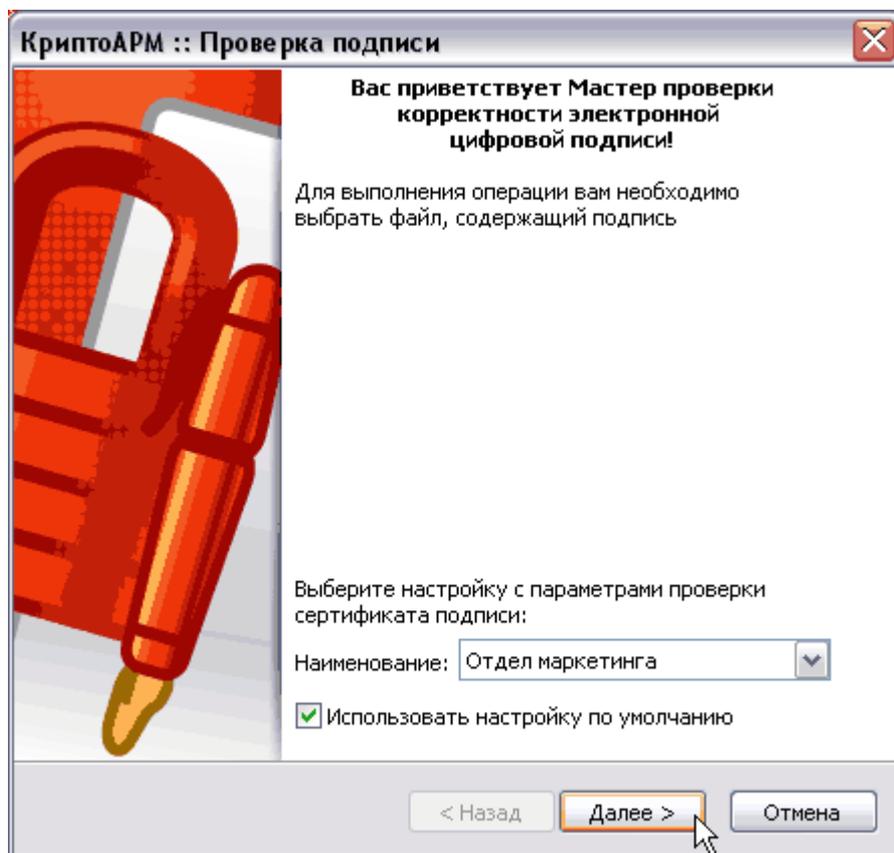
Проверить корректность электронной подписи вы можете через:

- Главное окно программы
- КриптоАРМ Агент
- контекстное меню

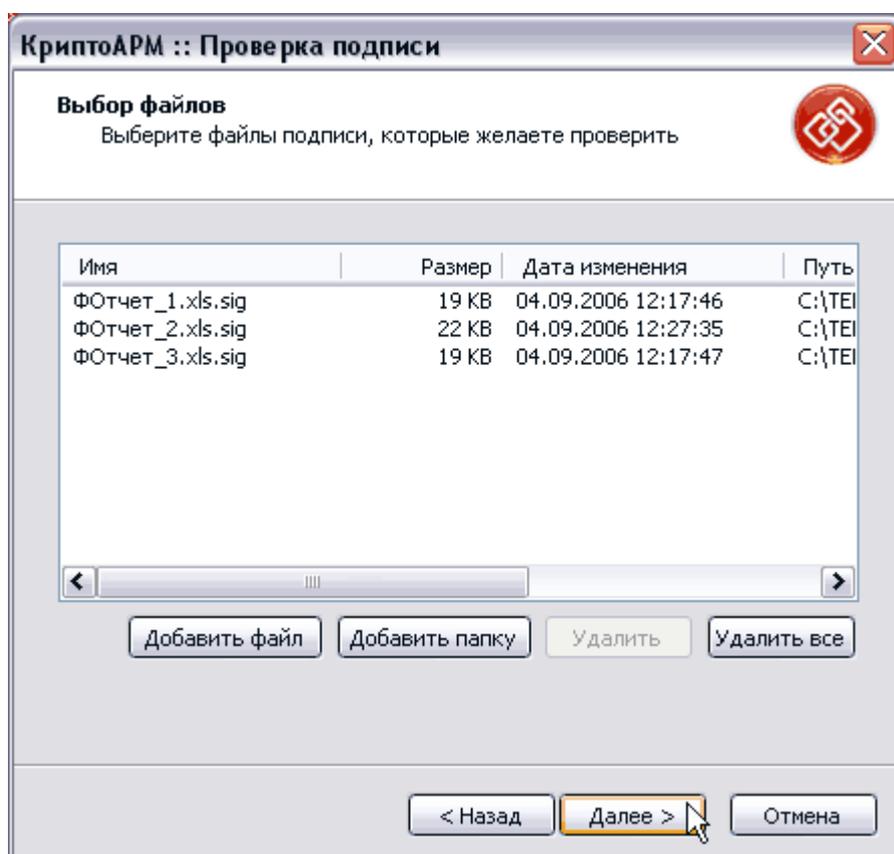
Для того чтобы проверить подпись к файлу:

1. На первом шаге 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**.

2.

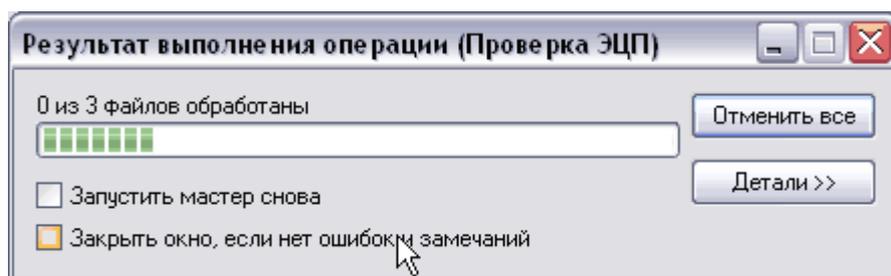


Выберите файл или папку файлов, подписанных ЭП, корректность которых необходимо проверить (кнопки **Добавить папку** и **Добавить файл**).



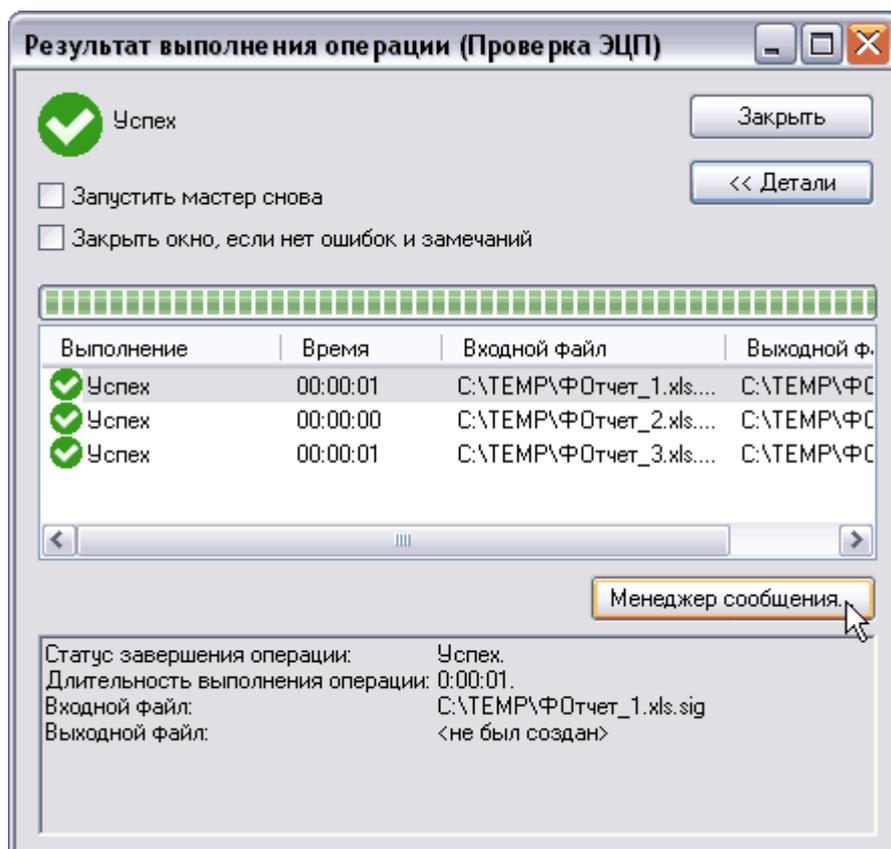
3. После сбора данных для снятия и проверки подписи возникнет окно с информацией о статусе операции и об используемых параметрах.

4. 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.

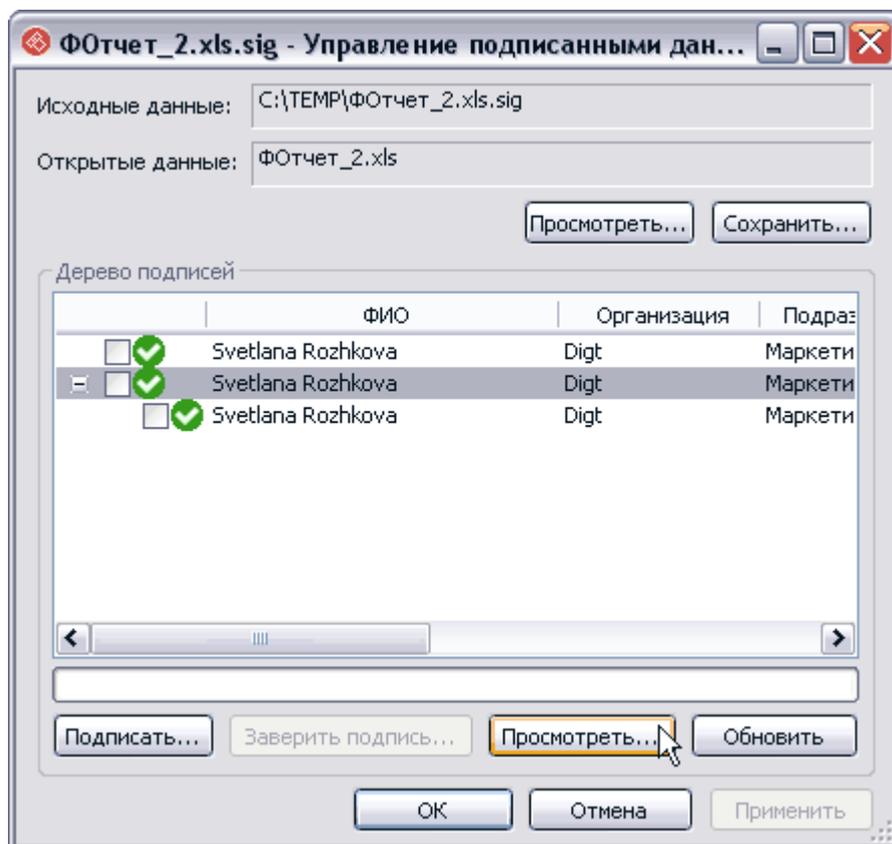


Откроется окно **Результат выполнения операции**, в котором отобразится статус операции. Если одна или несколько подписей не действительны, это будет отражено в статусе. Чтобы просмотреть детальную информацию о результатах проверки подписи и используемых параметрах: имя исходного файла, имя выходного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

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.

Закладка **Подпись** содержит информацию об атрибутах подписи, времени ее создания, используемых алгоритмах подписи и хеширования.

В закладке **Сертификат** вы можете просмотреть сведения о сертификате и проверить его статус. Также в этом окне доступна информация о владельце и издателе сертификата, сроках действия сертификата и возможных вариантах использования.

В закладке **Статус сертификата** отображен общий статус проверки полного пути сертификации. Вы можете проверить путь сертификации, выбрав способ проверки из выпадающего списка и нажав на кнопку **Проверить**

В закладке **Штамп времени** дается информация о штампе времени на подпись (для классической ЭП) и информация о штампах времени на подпись и доказательства подписи (для усовершенствованной ЭП)

## Информация о подписи и сертификате



Подпись Сертификат Статус сертификата Штампы времени



Подпись действительна

### Атрибуты подписи

Комментарий:

Комментарий

Идентификатор ресурса:

file:ФОтчет\_2.xls

Время создания:

04.09.2006 12:06:55

### Алгоритмы

Алгоритм подписи:

ГОСТ Р 34.10-2001

Алгоритм хеширования:

ГОСТ Р 34.11-94

OK

Отмена