Инструкция по установке, настройке и использованию КриптоАРМ

Листов 16

ИнфоТеКС Интернет Траст
2021 г.

Оглавление

I. Введение

✓ Документ предназначен для пользователей, осуществляющих установку и настройку **ПО *КриптоАРМ 5*** для выполнения над отдельными файлами криптографических операций - шифрования/расшифрования и создания/проверки электронной подписи.

✓ ***КриптоАРМ*** не является самостоятельным средством шифрования и электронной подписи, для обеспечения выполнения криптографических операций на компьютере должно быть предварительно установлено средство криптографической защиты информации (СКЗИ) ViPNet CSP или КриптоПро CSP.

✓ В удостоверяющем центре группы компаний ИнфоТеКС (далее - УЦ ГК ИнфоТеКС) срок действия ключей и сертификата ЭП установлен равным 1 году.

✓ При необходимости произвести плановую (скорое истечение срока действия ЭП) или внеплановую (изменение учетных данных владельца ЭП, потеря доступа к ключевому носителю, потеря ключевого носителя и т.д.) смену ЭП необходимо повторно прибыть в УЦ ГК ИнфоТеКС по согласованию с менеджером АО «ИнфоТеКС Интернет Траст».

✓ Для правильной работы необходимо выполнить все пункты данного руководства в указанной последовательности.

✓ **Необходимо обращать особое внимание на примечания помеченные знаком .**

Внимание! Вид окон может отличаться в зависимости от используемой операционной системы.
В примерах использовалась операционная система Windows 7.

Всю необходимую документацию по услугам нашей компании вы можете загрузить на нашем сайте www.iitrust.ru раздел «Поддержка», кнопка «Пользовательская документация»

II. Получение и установка КриптоАРМ

Для получения КриптоАРМ загрузите архив с дистрибутивом КриптоАРМ с web-ресурса http://www.trusted.ru/support/downloads/?product=133:

trusteddesktop.exe - для установки на 32-х/64-х разрядной ОС Windows, и сохраните у себя на компьютере предлагаемый файл.

Запустите установку КриптоАРМ из файла ***trusteddesktop.exe.*** При выборе варианта установки программы следует выбрать ***«Быстрая установка (рекомендуется)»***. Далее следуйте инструкциям мастера установки. (Рисунок 1).

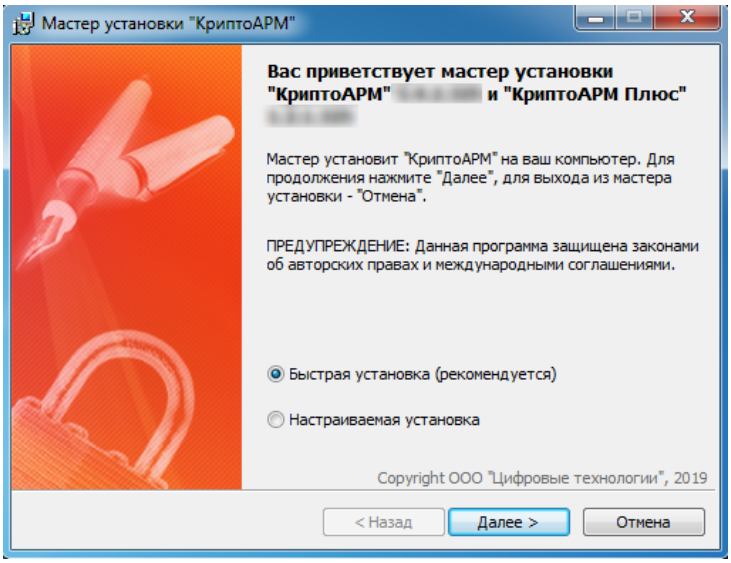

Рисунок 1

После завершения установки КриптоАРМ, мастер установки предложит перезагрузить компьютер. Необходимо нажать ***«Да»*** и перезагрузить компьютер. (Рисунок 2).

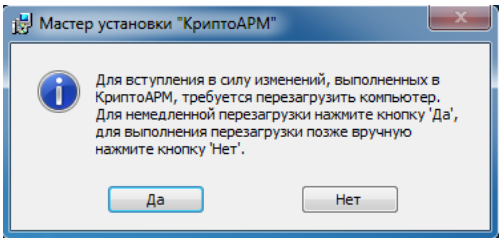

Рисунок 2

При первичной установке программы на компьютер автоматически будет активирован 14-дневный ознакомительный период ***«КриптоАРМ Стандарт Плюс»*** или ***«КриптоАРМ Терминал»*** (в зависимости от типа операционной системы). По истечению ознакомительного периода программа автоматически переключится в режим ***«КриптоАРМ Старт»*** и предложит приобрести лицензию в официальном интернет-магазине: http://cryptoarm.ru/

Работу с КриптоАРМ можно условно разделить на следующие основные сценарии:

А. Подписание файлов.

Б. Проверка электронной подписи в полученных файлах.

В. Подписание и шифрование файлов.

Г. Расшифрование и проверка подписи в полученных зашифрованных файлах.

А. Электронная подпись файлов.

Запустите КриптоАРМ.

Для того чтобы подписать и зашифровать файл декларации, нажмите кнопку ***«Подписать»*** (Рисунок 3).

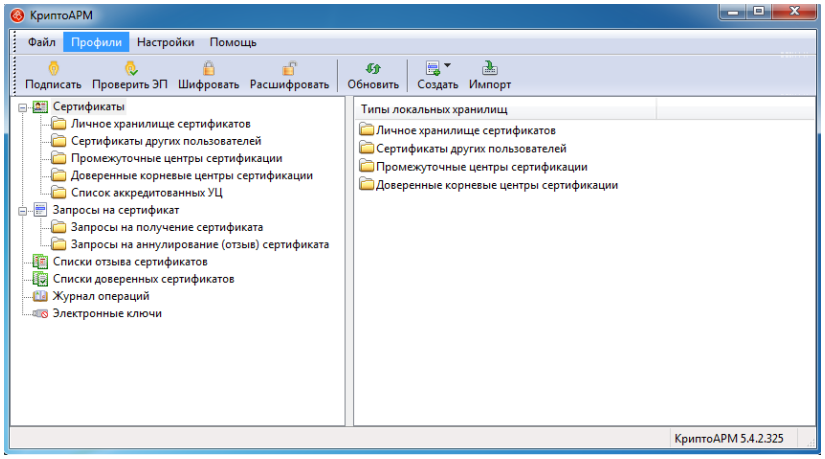

Рисунок 3

Далее следуйте указаниям Мастера создания электронной цифровой подписи. В окне выбора файла необходимо нажать ***«Добавить файл»*** и указать на файл. Затем нажмите на кнопку ***«Далее»*** (Рисунок 4).

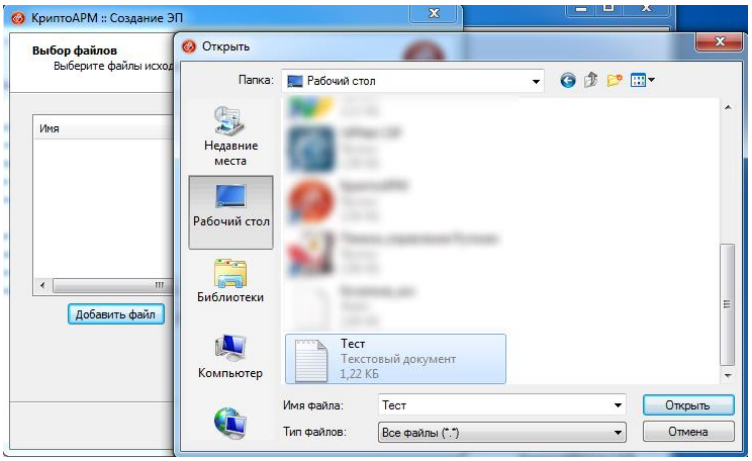

Рисунок 4

В окне выбора желаемого выходного формата файла подписи выбрать ***«BASE64-кодировка *.sig».*** Нажмите на кнопку ***«Далее»*** (Рисунок 5).

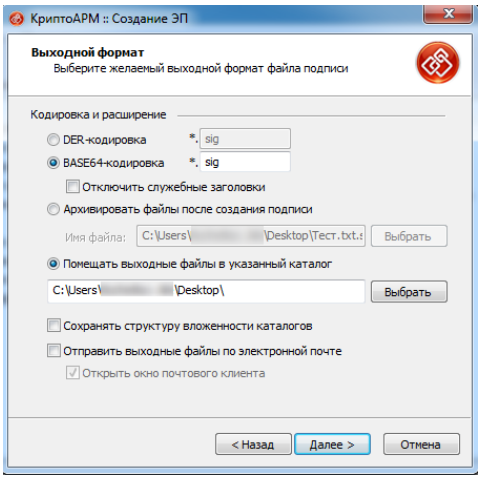

Рисунок 5

В окне параметров подписи выбрать ***«Подписано»*** и нажать ***«Далее»***. При необходимости введите остальные свойства подписи (Рисунок 6).

- **Комментарий к подписи** – информация, понятная просматривающим подписанный документ;
- **Идентификатор ресурса** – имя файла, указывается для того, чтобы в случае изменения имени файла получатель подписанного документа смог определить первоначальное его название;
- **Сохранить подпись в отдельном файле**. При установке флага будет создана отделенная электронная подпись на файле (например, может быть удобна в том случае, если вы отправляете документ человеку, который не использует программное обеспечение для извлечения и проверки электронной подписи (Cryptofile или 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);
- **Включить время создания подписи** - при установке флага - в файл подписи будет включено время подписи;
- **Включить штамп времени на подписываемые данные** - При установке этого флага в файл ЭП 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 ЭП. Такой штамп удостоверяет, например, что подпись была создана до того, как сертификат ключа подписи был аннулирован (отозван). Таким образом, сохраняется возможность использования отозванного сертификата для проверки ЭП, созданных до момента отзыва. Эта проблема актуальна для всех систем электронного документооборота.
- **Включить штамп времени на подпись** - при установке этого флага в файл ЭП будет включен штамп времени на создаваемую электронную подпись.

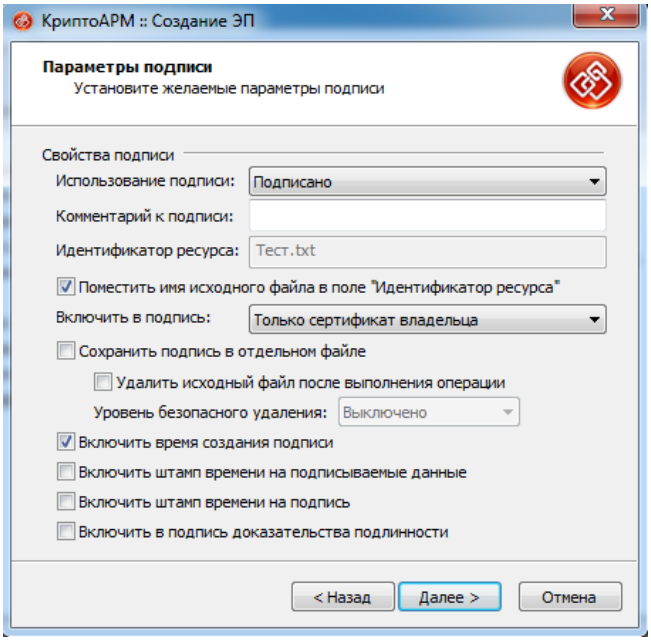

Рисунок 6

В окне выбора сертификата для создания подписи необходимо нажать кнопку ***«Выбрать»***, указать на личный сертификат из Личного хранилища сертификатов, затем нажать на кнопку ***«ОК»*** и ***«Далее»***. При необходимости для доступа к ключевому контейнеру введите пароль (Рисунок 7).

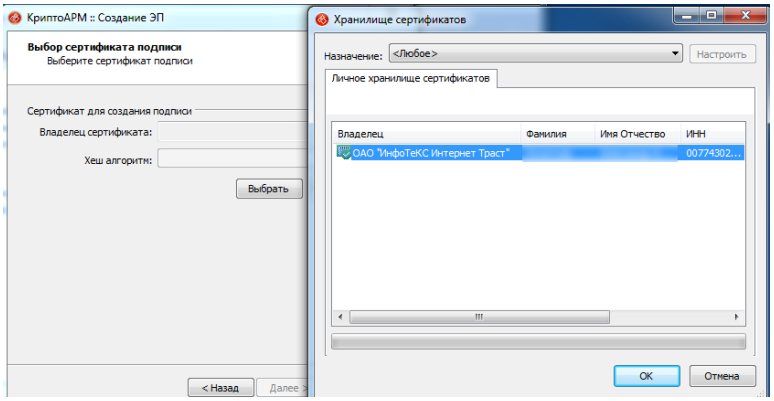

Рисунок 7

В последнем окне мастера Вы можете сохранить указанные данные в профиль для дальнейшего использования. Для этого необходимо поставить галку, задать имя настройки и нажать на кнопку ***«Готово»*** (Рисунок 8).

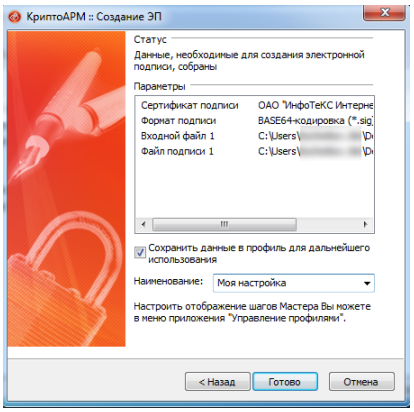

Рисунок 8

✓ Далее выйдет окно «**Результат выполнения операции**», после чего будет создан файл вида ***.sig**. (Рисунок 9).

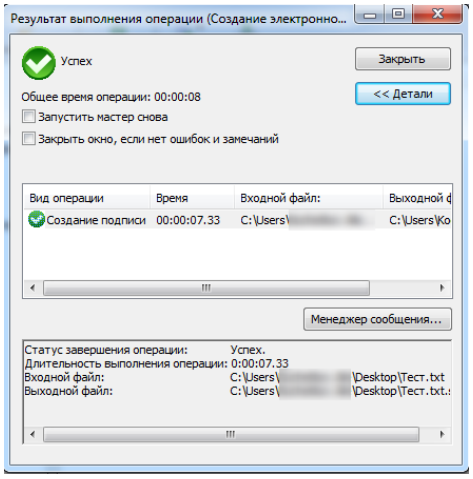

Рисунок 9

На этом процедура подписи файла завершена. Подписанный файл с прикрепленной подписью (или файл откреплённой подписи) находится в той же папке, что и подписываемый файл и имеет формат ***"Имя подписываемого файла"."Расширение подписываемого файла".sig***.

Б. Проверка электронной подписи, в полученных файлах

Запустите КриптоАРМ. Для того чтобы проверить подпись к файлу, нажмите на кнопку ***«Проверить ЭП»***[1] (Рисунок 10).

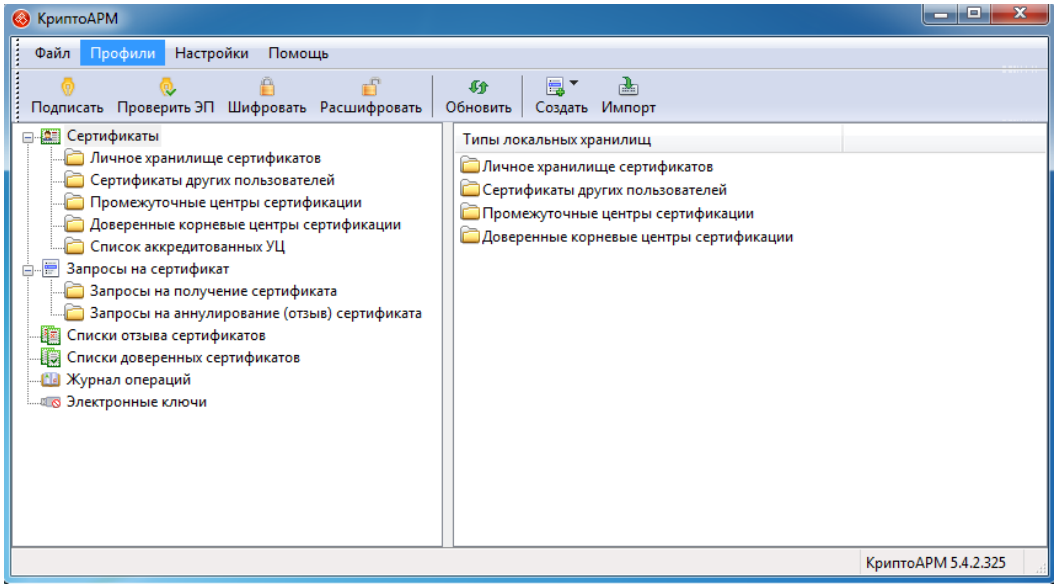

Рисунок 10

Далее следуйте указаниям мастера проверки корректности ЭЦП. В окне выбора файла необходимо нажать ***«Добавить файл»*** и указать на файл (Рисунок 11).

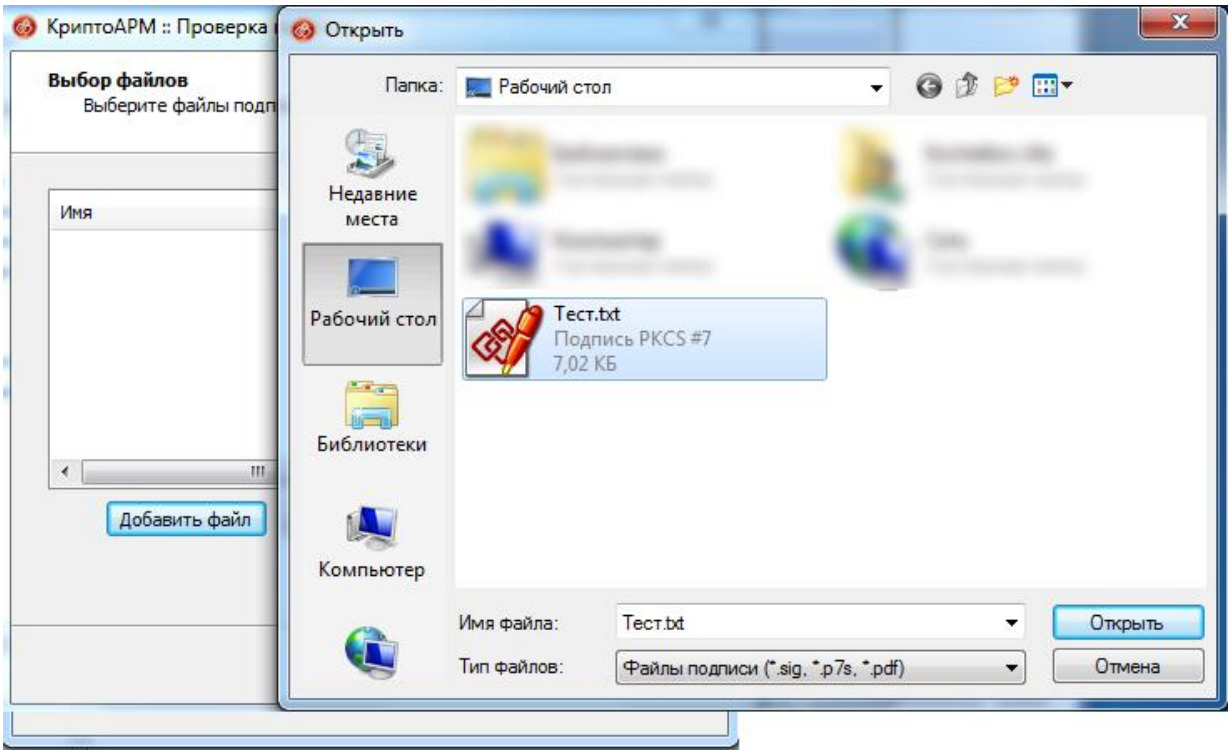

Рисунок 11

[1] 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**».

✓ После сбора данных для снятия и проверки подписи выйдет окно с информацией о статусе операции и об используемых параметрах[2] (Рисунок 12).

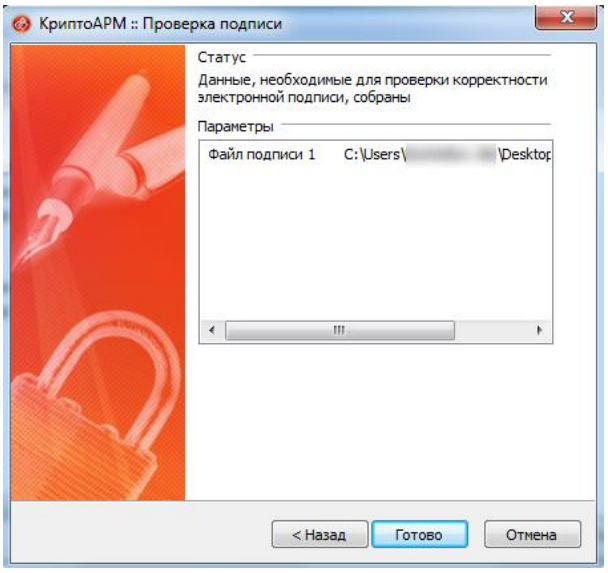

Рисунок 12

✓ Далее выйдет окно ***«Результат выполнения операции»***. При необходимости Вы можете просмотреть более подробную информацию, нажав на кнопку ***«Менеджер сообщения»***, а также распечатать подробную информацию о подписи (Рисунок 13).

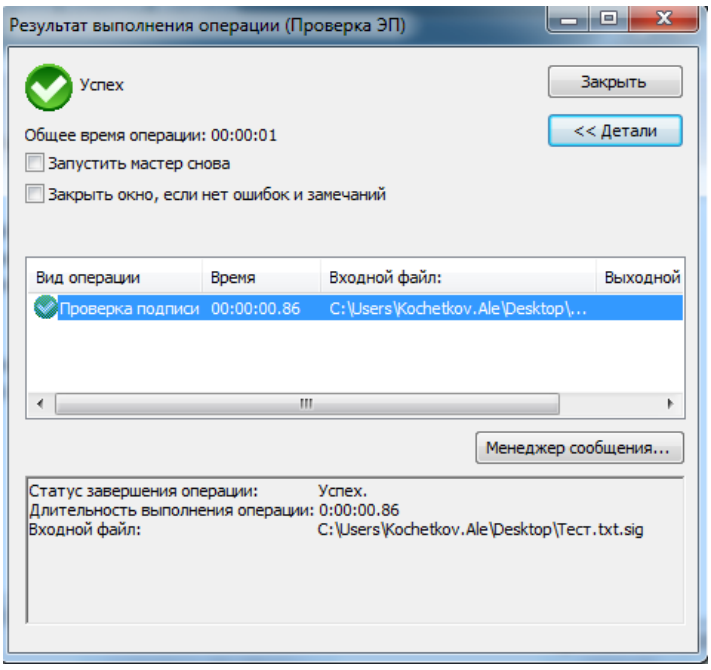

Рисунок 13

На этом процедура проверки подписи файла завершена.

[2] Если в файле подписи содержится одна подпись (нет дополнительных и/ или заверяющих), то проверяется корректность подписи и действительность сертификата отправителя. Если в файле содержится более одной подписи, то проверяется корректность каждой подписи в коллекции.

В. Электронная подпись и шифрование файлов

Запустите КриптоАРМ. Для того чтобы подписать и зашифровать файл, нажать пункт меня ***Файл – Подписать и зашифровать…*** (Рисунок 14).

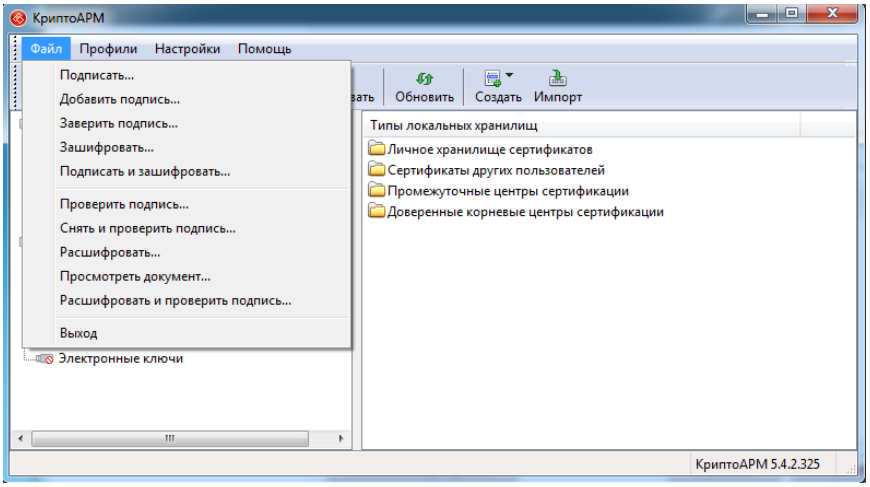

Рисунок 14

Далее следуйте указаниям мастера подписи и шифрования. В окне выбора файла необходимо нажать на кнопку ***«Добавить файл»*** и выбрать файл (Рисунок 15).

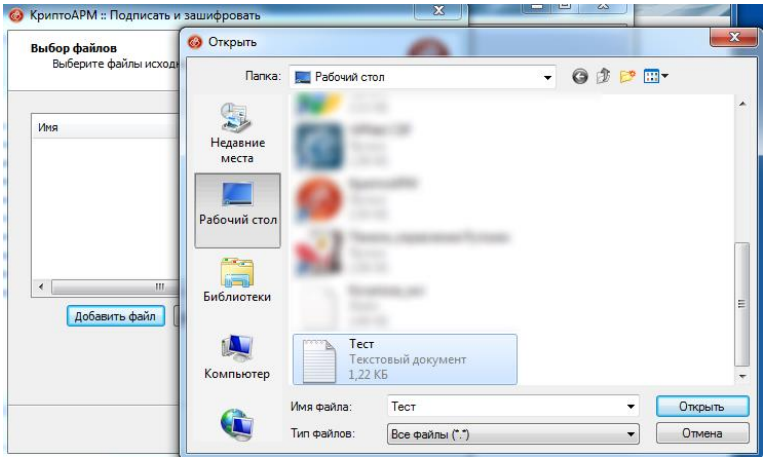

Рисунок 15

В окне выбора желаемого выходного формата файла подписи выберите ***«BASE-64-кодировка *.sig»*** и нажмите на кнопку ***«Далее»*** (Рисунок 16)

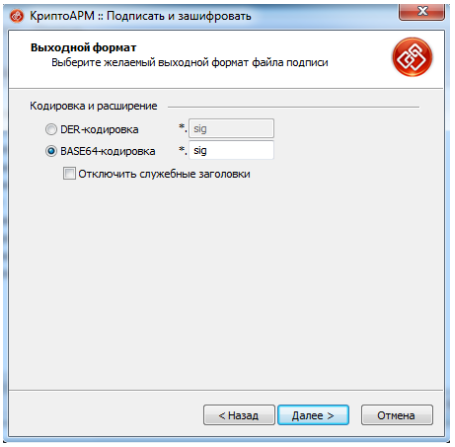

Рисунок 16

В окне выбора сертификата для создания подписи нажмите кнопку ***«Выбрать»***, укажите на личный сертификат из Личного хранилища сертификатов, затем нажмите ***«ОК»*** и ***«Далее»*** (Рисунок 17).

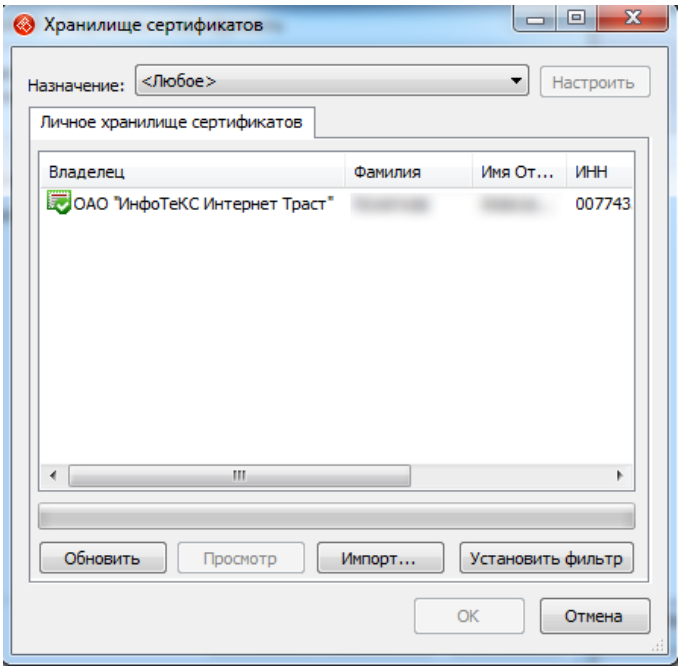

Рисунок 17

В окне выбора желаемого выходного формата зашифрованного файла следует выбрать ***«BASE-64-кодировка *.enc»***[3] и нажать ***«Далее»*** (Рисунок 18).

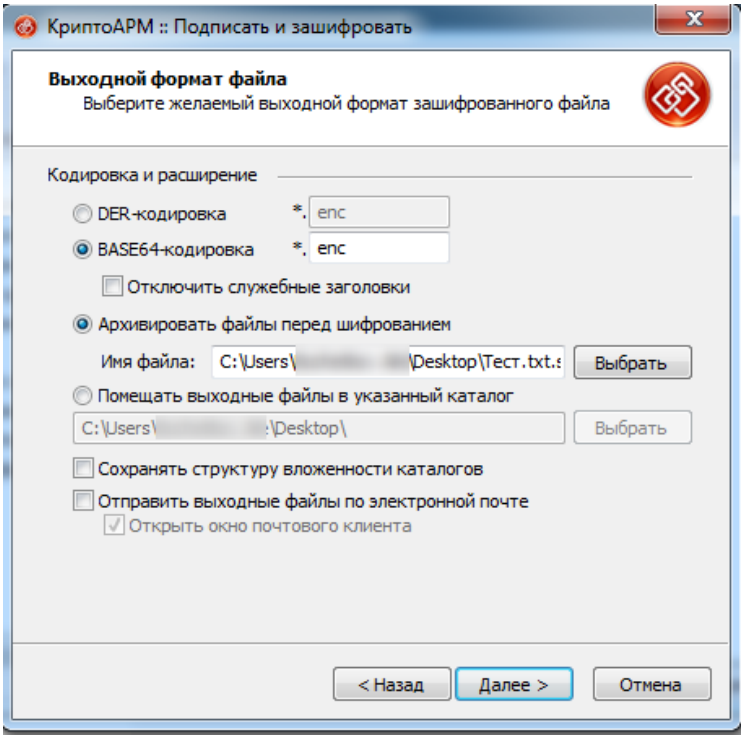

Рисунок 18

В окне выбора дополнительных файлов для шифрования нажать ***«Далее»***, ничего не выбирая.

[3] Если необходимо архивировать, выберите пункт «**Архивировать файлы перед шифрованием**».

В окне ***«Режим шифрования для отправителя сообщения»*** выбираете «**Использовать криптопровайдер**»; Тип криптопровайдера выбирается в зависимости от СКЗИ, например, **Infotecs GOST 2012/512 Cryptographic Service Provider,** если используется ViPNet CSP (Рисунок 19).

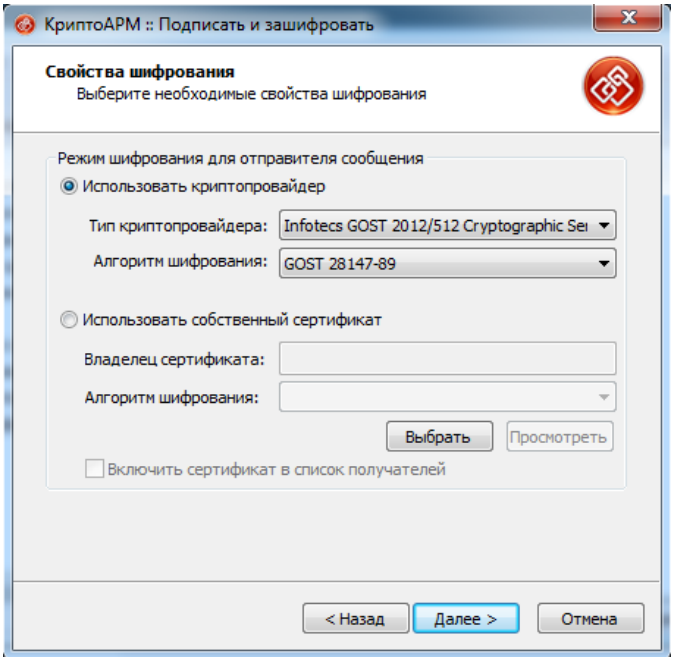

Рисунок 19

В окне выбора сертификатов получателей необходимо нажать ***«Добавить…»***, указать на импортированный ранее открытый ключ сертификата получателя[4] (хранилище ***«Другие пользователи»***), нажать ***«ОК»*** и ***«Далее»*** (Рисунок 20).

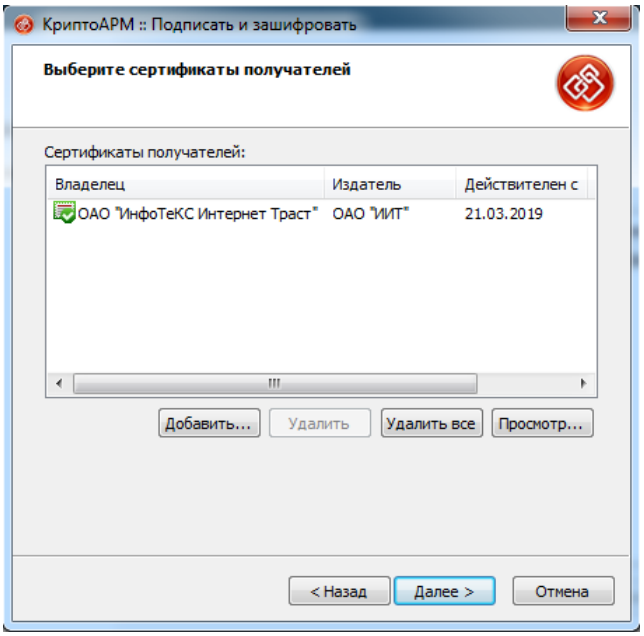

Рисунок 20

В последнем окне мастера Вы можете сохранить указанные данные в настройку для дальнейшего использования. Для этого необходимо поставить галку, задать имя настройки и нажать ***«Готово»***. (Рисунок 21).

[4] Срок действия сертификата получателя должен быть актуальным

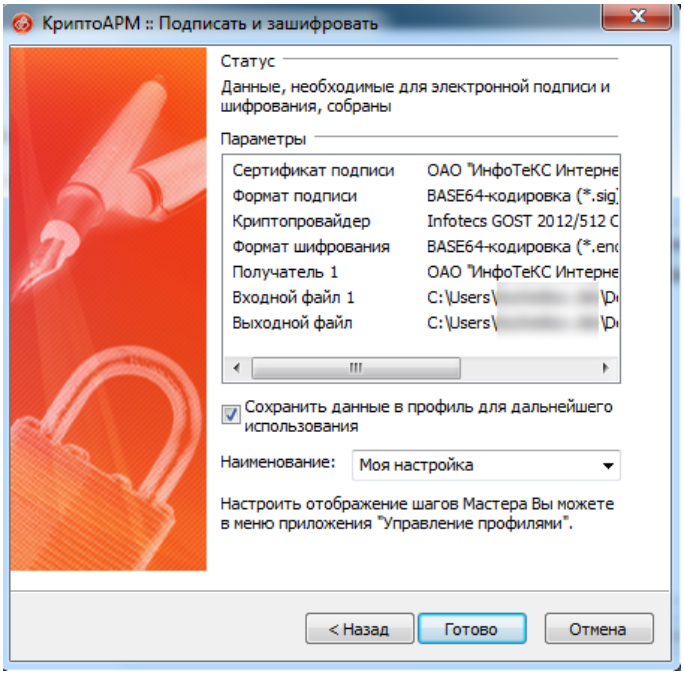

Рисунок 21

Далее появится окно ***«Результат выполнения операции»***, после чего будет создан файл вида ***.txt.sig.[zip].enc**. (Рисунок 21).

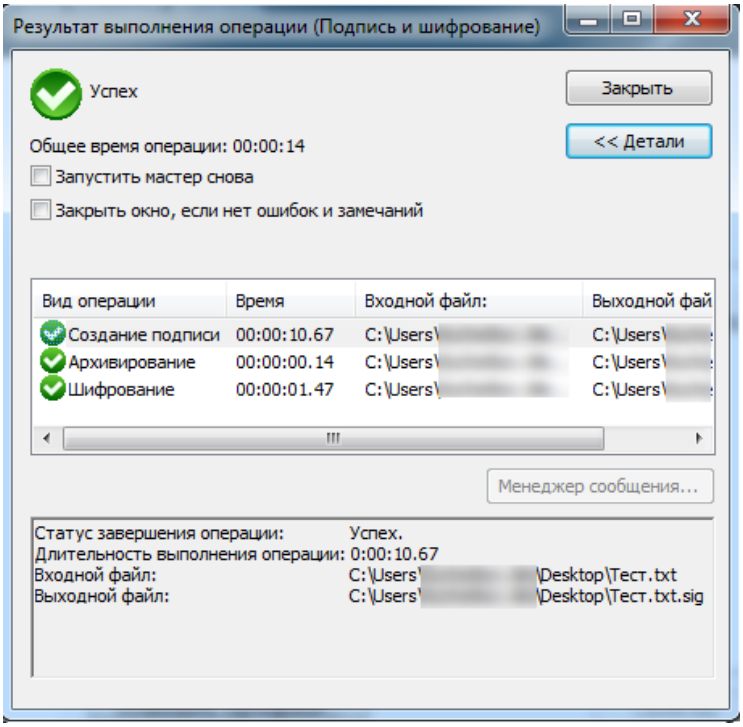

Рисунок 21

На этом процедура подписи и шифрования файла завершена. Подписанный и зашифрованный файл находится в той же папке, что и исходный файл и имеет формат ***"Имя подписываемого файла"."Расширение подписываемого файла".sig.[zip].enc***.

Г. Расшифрование и проверка электронной подписи в полученных файлах.

Запустите КриптоАРМ. Для того чтобы расшифровать и проверить подпись файла, нажмите на пункт меню **Файл – Расшифровать и проверить подпись…** (Рисунок 22).

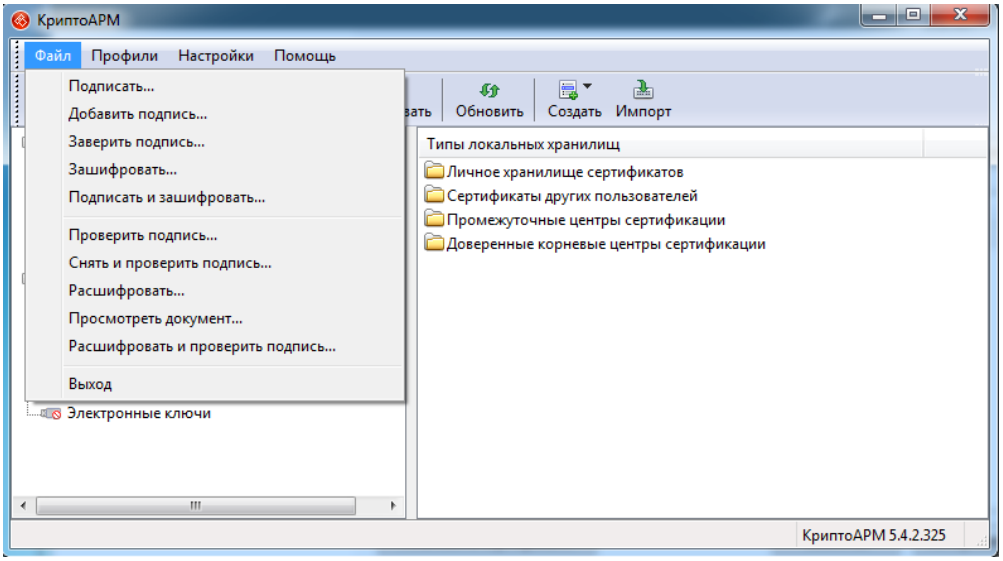

Рисунок 22

Далее следуйте указаниям мастера подписи и шифрования.

В окне выбора файла необходимо нажать ***«Добавить файл»*** и указать на файл (Рисунок 23).

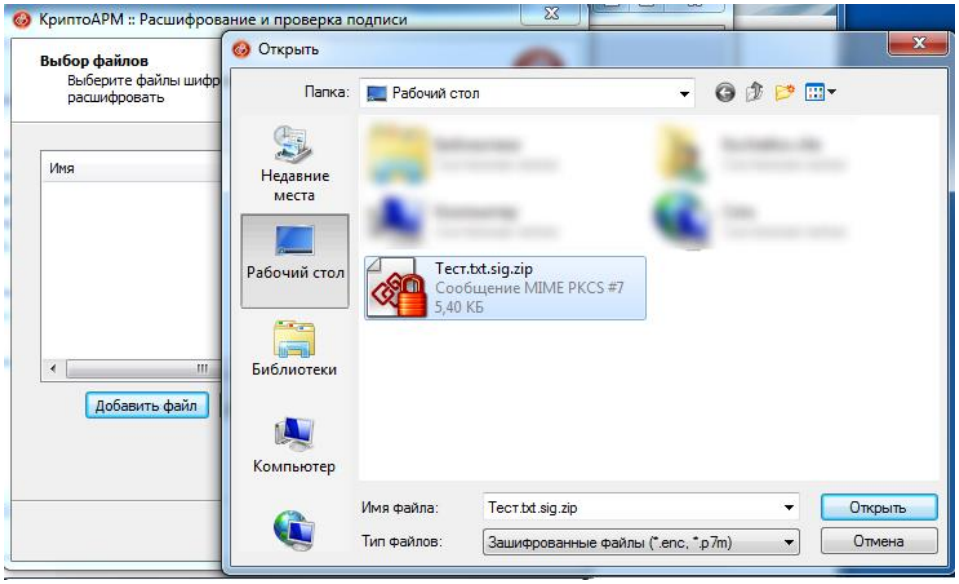

Рисунок 23

В следующем окне выберите предпочтительный сертификат расшифрования (кнопка ***«Выбрать»***). Указанный сертификат вы можете просмотреть, нажав на кнопку ***«Просмотреть»*** (Рисунок 24).

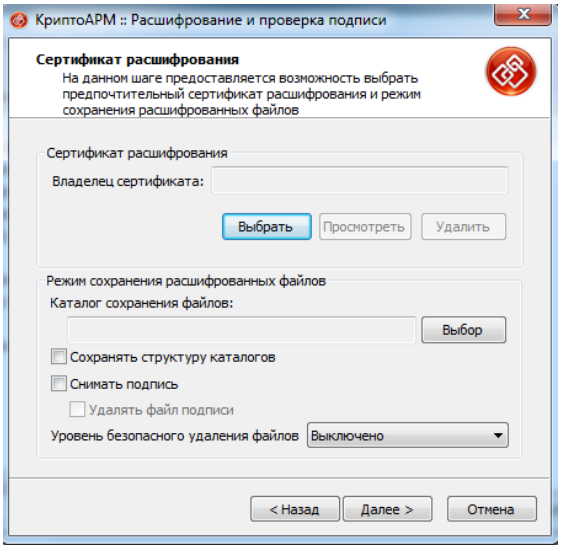

Рисунок 24

После завершения сбора данных для расшифрования и проверки подписи выйдет окно с информацией о статусе операции и об используемых параметрах. Для продолжения нажмите на кнопку ***«Готово»***. Данные будут расшифрованы и по умолчанию сохранены в тот же каталог, в котором находится исходный файл данных. Имя нового файла совпадает с именем зашифрованного файла без расширения. Если файл с таким именем уже существует, сохраните его под другим именем или перезапишите. Далее проверяется корректность ЭП и действительность сертификата отправителя. (Рисунок 25)

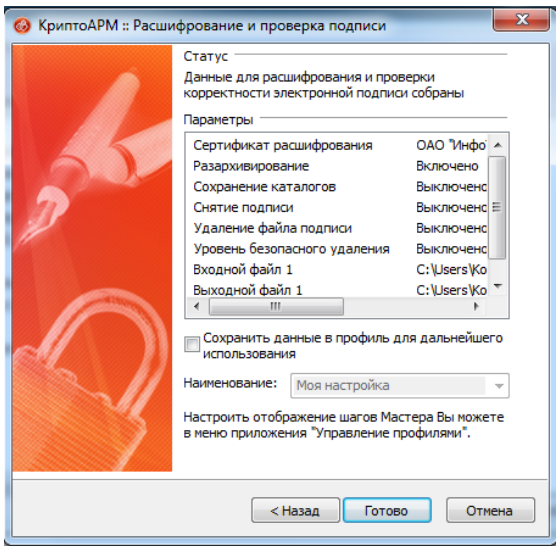

Рисунок 25

После завершения операции возникнет окно «**Результат выполнения операции**» со статусом завершения операции. Чтобы просмотреть детальную информацию о результатах расшифрования и используемых параметрах: имя исходного файла, имя выходного (расшифрованного) файла, статус операции, длительность выполнения операции, нажмите на кнопку «**Детали**» (Рисунок 26).

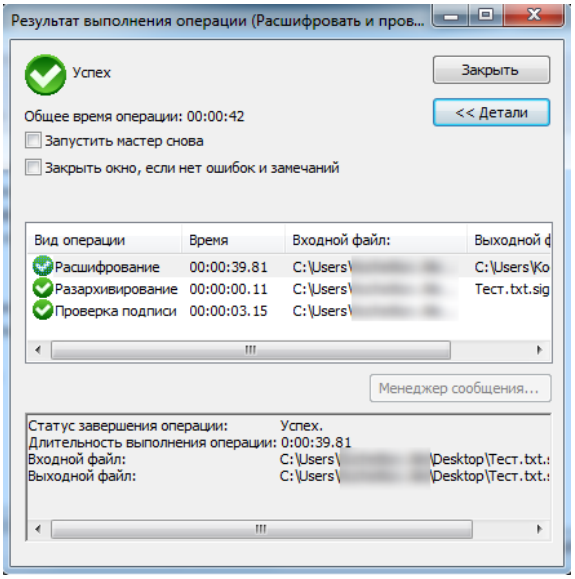

Рисунок 26

На этом процедура расшифрования и проверки подписи файла завершена. Расшифрованный (извлеченный) файл будет сохранен в той же папке, что и зашифрованный файл.