

# Программа «КриптоАРМ»

Версия 4

Руководство для начинающих  
пользователей

# Содержание

<b>Введение</b> .....	<b>3</b>
<b>Что такое криптография?</b> .....	<b>4</b>
<b>Для чего нужен «КриптоАРМ»?</b> .....	<b>6</b>
<b>Как начать работу с программой?</b> .....	<b>6</b>
Установка программы «КриптоАРМ» .....	7
Варианты работы с программой .....	7
Режимы работы программы .....	8
<b>Возможности программы</b> .....	<b>9</b>
<b>Цифровые сертификаты</b> .....	<b>10</b>
Для чего нужен цифровой сертификат? .....	10
Жизненный цикл сертификата .....	10
Получить цифровой сертификат .....	10
Создать запрос на сертификат .....	11
Статусы сертификатов .....	13
Что такое самоподписанный сертификат? .....	13
Создать самоподписанный сертификат .....	13
<b>Электронная цифровая подпись</b> .....	<b>16</b>
Когда используют электронную цифровую подпись .....	16
Варианты электронной подписи .....	16
Типы электронной подписи .....	16
Подписать электронный документ .....	17
Добавить дополнительную подпись .....	19
Заверить электронную подпись .....	21
Проверить корректность электронной подписи .....	23
Просмотреть информацию о подписи и сертификате .....	25
Просмотреть подписанный документ .....	25
<b>Шифрование</b> .....	<b>27</b>
Зашифровать файл .....	27
Просмотреть зашифрованный документ .....	31
Расшифровать файл .....	31
<b>Совмещенные операции</b> .....	<b>33</b>
Подписать и зашифровать документ .....	33
Расшифровать и проверить подпись .....	34
<b>Часто задаваемые вопросы</b> .....	<b>35</b>
<b>Перечень сокращений</b> .....	<b>36</b>
<b>Техническая поддержка</b> .....	<b>36</b>
<b>Зарегистрировать программу</b> .....	<b>36</b>
Посмотреть статус лицензии .....	37
<b>О компании «Цифровые технологии»</b> .....	<b>38</b>

## Введение



Перед вами документ для тех, кто впервые столкнулся с такой сложной и даже пугающей областью, как криптография. Шифрование, электронная цифровая подпись, цифровые сертификаты... Вопросов много, а как на них ответить?

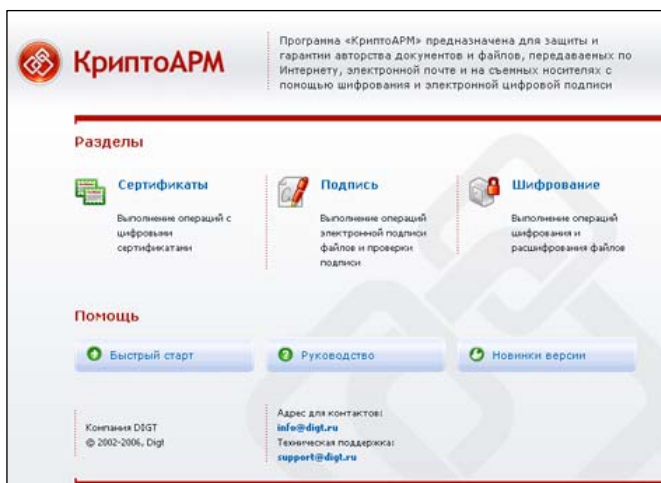
В этом руководстве описывается работа с программой «КриптоАРМ», а также объясняются основные понятия в области криптографической защиты информации. Описание сопровождается многочисленными примерами, которые помогут вам разобраться в возникающих вопросах.

Работа с программой описывается с учетом того, что все необходимые настройки программы будут заранее установлены системным администратором вашей организации (для администраторов разработано подробное техническое руководство).

## Что такое криптография?

Вам нужно отправить важный отчет своему коллеге по электронной почте. Но сделать это нужно так, чтобы никто посторонний не смог его прочитать. Вы просто хотите быть уверены, что ваш коллега будет единственным получателем письма, а он, в свою очередь, желает быть уверен, что именно вы являетесь фактическим отправителем. Риск, конечно, не затрагивает проблему национальной безопасности, но если конкурент получит к отчету доступ, это может влететь вам в копейку. Решение своих задач вы найдете в криптографии.

Криптография - наука о защите данных - необходима для того, чтобы безопасно передавать информацию по открытым каналам связи (например, Интернету) таким образом, что она не будет доступна никому, кроме тех, кому она предназначена.



Перед тем как приступить к работе с «КриптоАРМ», ознакомьтесь со следующими понятиями:



**Цифровой сертификат** - своего рода электронная идентификационная карта, типа паспорта или водительских прав в обычной жизни. В криптографии цифровой сертификат – это документ, позволяющий однозначно определить владельца открытого ключа.

**Удостоверяющий центр** - это служба (сторонняя или внутри вашей организации), которая выдает цифровые сертификаты.

**Ключевая пара** – открытый и закрытый ключи, которые используются для шифрования и электронной подписи данных.

**Закрытый ключ** сохраняется в секрете его владельцем, **открытый ключ** распространяется свободно. Если открытый ключ используется для шифрования сообщения, то только соответствующий ему закрытый ключ может расшифровывать это сообщение. И наоборот. Каждая сторона транзакции имеет как открытый, так и закрытый ключ. Чтобы передавать сообщение с большей надежностью, отправитель при шифровании сообщения использует открытый ключ получателя. Получатель расшифровывает сообщение, используя свой уникальный закрытый ключ. Поскольку никто не знает закрытого ключа, то сообщение не может быть прочитано никем другим, кроме как получателем сообщения. Таким образом, гарантируется секретность сообщения.



**Шифрование** - это способ хранения и отправки закодированной информации. Только тот человек может декодировать сообщение, который обладает верным *ключом*; для всех остальных сообщение будет выглядеть беспорядочным набором букв, цифр и символов. Назначение шифрования — *секретность*.



**Электронная цифровая подпись** - реквизит электронного документа, позволяющий удостовериться в истинности отправителя и в том, что сообщение не было несанкционированно

изменено (подделано). Назначение цифровых подписей — *целостность информации и аутентичность*. Цифровая подпись равнозначна собственноручной подписи.

**Список отзыва сертификатов** – список недействительных сертификатов (они либо отозваны, либо их действие приостановлено).

**Криптографическая операция** – любая из операций: шифрование, расшифрование, создание цифровой подписи и т.д.

**Ключевые носители** – хранилища ваших закрытых ключей, а также сертификатов открытых ключей, к ним относятся

- реестр Windows
- дискета 3,5
- смарт-карты
- USB-брелки



## Для чего нужен «КриптоАРМ»?



Программа "КриптоАРМ" предназначена для надежной защиты информации в вашей организации и гарантии авторства документов и файлов, передаваемых по сети Интернет и на ключевых носителях.

Ваше намерение	Решение
Надежно защитить данные от постороннего доступа	<a href="#">Шифрование</a>
Гарантировать целостность данных при отправке по электронной почте	<a href="#">Шифрование</a>
Обеспечить подлинность авторства документа	<a href="#">Электронная подпись</a>
Согласовать документ с коллегами	Иерархия <a href="#">электронных подписей</a> :  Например, к подписанному вами документу, ваш коллега может добавить свою подпись. А директор своей подписью заверит вашу подпись и подпись вашего коллеги. => Документ согласован!

В программе «КриптоАРМ» вы можете:

- [Шифровать файлы и документы](#)
- [Расшифровывать файлы и документы](#)
- [Подписывать данные электронной цифровой подписью](#)
- [Добавлять подпись](#)
- [Заверять подпись](#)
- [Проверять корректность подписи](#)
- [Шифровать и подписывать файлы и документы](#)
- [Расшифровывать файлы и документы, проверять подпись](#)

## Как начать работу с программой?

- 1 **Шаг:** Ознакомьтесь с данным руководством
- 2 **Шаг:** Установите программу (см. главу [«Установка программы КриптоАРМ»](#))
- 3 **Шаг:** Получите цифровой сертификат (см. главу [«Получить цифровой сертификат»](#)). Для этого:
  - a) Создайте запрос на сертификат и передайте его в Удостоверяющий центр на рассмотрение (см. главу [«Создать запрос на получение сертификата»](#))
  - b) Получите личный сертификат
  - c) Установите его в хранилище
  - d) Скачайте и установите корневой сертификат
  - e) Скачайте и установите актуальный список отзыва сертификатов

Теперь вы можете:

- 4 **Шаг:** Шифровать и подписывать файлы и папки. О том, как это сделать, читайте в Главе [«Электронная цифровая подпись»](#) и [«Шифрование»](#).

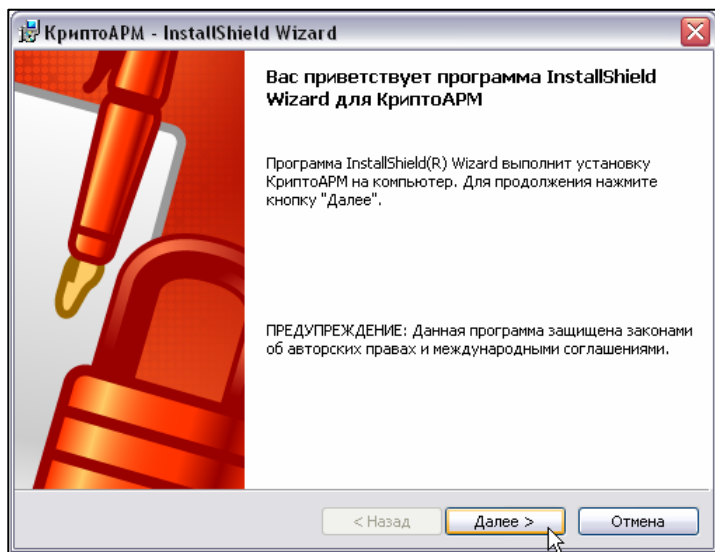
---

**!** Обратитесь к системному администратору для создания настроек работы в программе. Для обмена документами с бухгалтером вы можете создать одну настройку, с партнерами — вторую, с клиентами — третью и использовать каждую из них при взаимодействии с этими группами людей.

---

## Установка программы «КриптоАРМ»

Для установки программы "КриптоАРМ" запустите на исполнение файл **CryptoARM.exe** из дистрибутива программы. Далее следуйте стандартным инструкциям программы InstallShield Wizard.



**Примечание** Установка и удаление **КриптоАРМ** в операционных системах Windows 2000/XP/2003 должна осуществляться пользователем, имеющим права администратора системы.

Перед установкой дистрибутива, удалите все ранее существующие версии устанавливаемого программного обеспечения. Если программа не удалена, новая версия не будет установлена. Для этого используйте пункты основного меню **Windows Пуск - Настройка - Панель управления - Установка и удаление программ**.

Далее следуйте указаниям Мастера установки программы.

Далее следуйте указаниям Мастера

**! Для завершения процедуры установки необходимо выполнить перезагрузку компьютера.**

После установки программы:

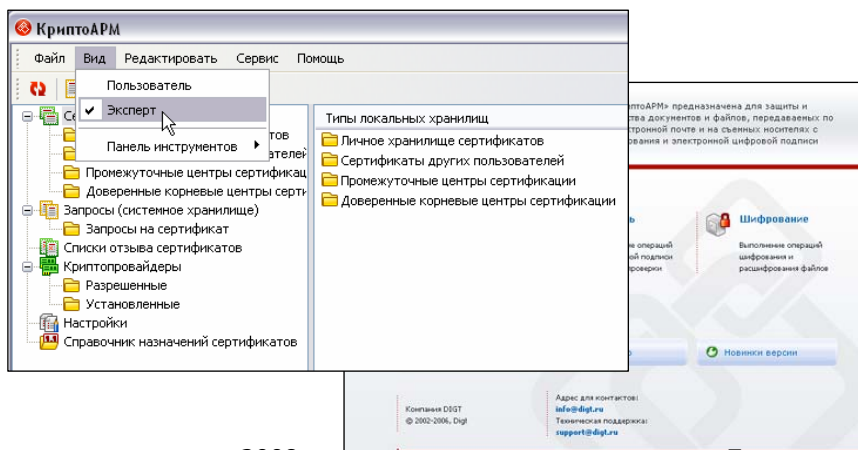
1. В указанном при установке каталоге (по умолчанию в каталоге **Program Files**) будет создан подкаталог **Digt**.
2. В меню панели задач **Пуск -> Программы** появится группа **Digt**, которая содержит меню вызова программы **КриптоАРМ Агент**, главного окна приложения **КриптоАРМ** и документации пользователя и программиста в формате CHM



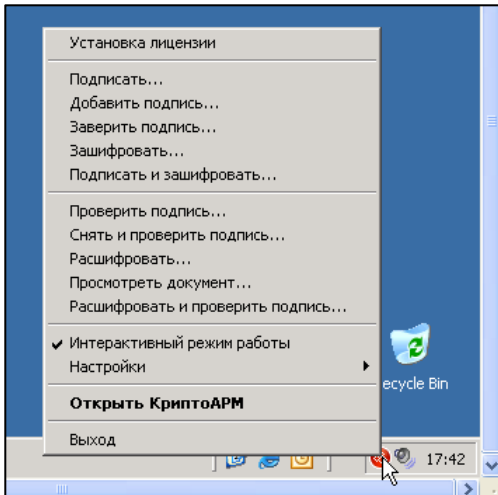
## Варианты работы с программой

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

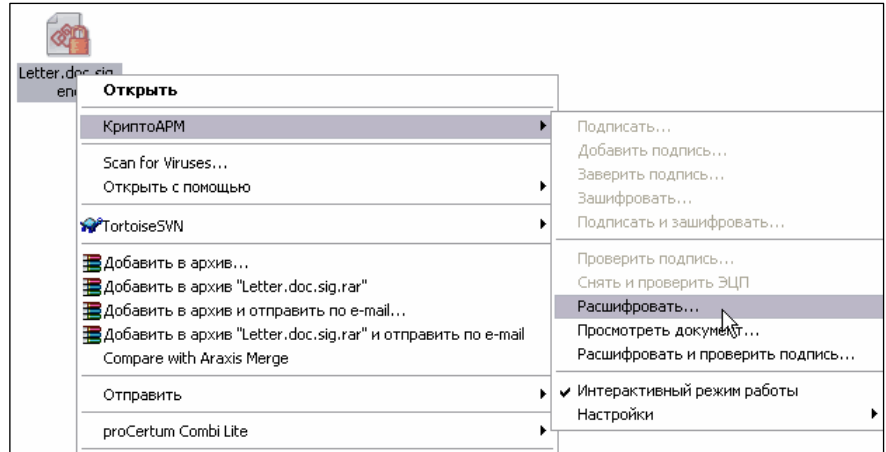
- Главное окно - вид «Пользователь»
- Главное окно – вид «Эксперт»



**Вид «Эксперт»** дает возможность управлять настройками программы. Этот режим предназначен, в большей степени, для администраторов ПК и специалистов по информационной безопасности.



- КристоАРМ Агент, вызываемый правой клавишей мыши (на панели задач)
- Контекстное меню файла, вызываемое правой клавишей мыши (в Проводнике Windows)



## Режимы работы программы

Выполнять криптооперации с помощью программы "КристоАРМ" вы можете в нескольких режимах:

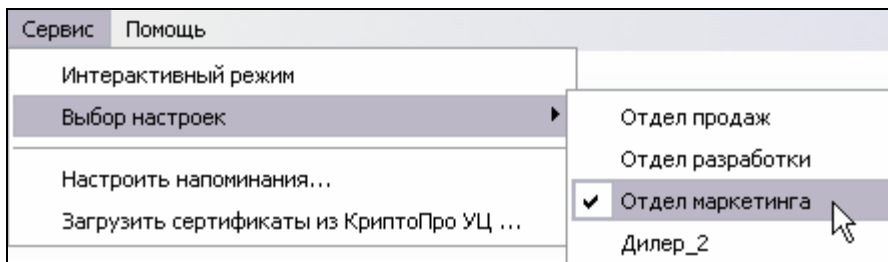
- Интерактивный
- Неинтерактивный

## Интерактивный режим

Интерактивный режим предполагает прохождение всех шагов **Помощника**, то есть вы сами вручную сможете вводить или выбирать все необходимые для выполнения криптооперации параметры.

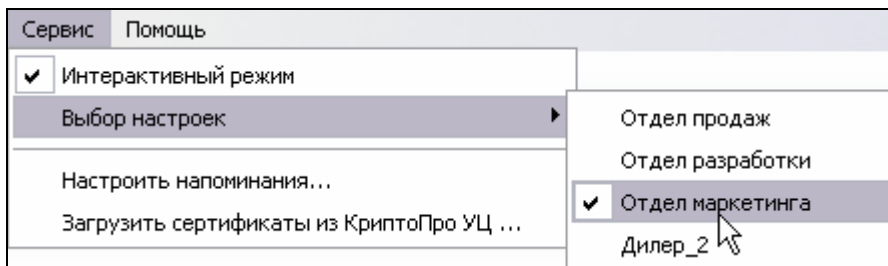
Для установки интерактивного режима:

1. В главном окне программы выберите **Сервис ->Интерактивный режим** (Напротив строки «Интерактивный режим» появится флаг (в виде галочки).



## Неинтерактивный режим

При неинтерактивном режиме программа сама автоматически использует ту настройку, которую вы установили как "По умолчанию". В этом случае во время операции программой запрашивается ввод только тех параметров, которые не указаны в данной настройке:



Для установки неинтерактивного режима:

1. Удалите галочку напротив строки **Интерактивный режим**: меню **Сервис** -> **Интерактивный режим** (Напротив строки «Интерактивный режим» флаг исчезнет)
2. Выберите настройку: Сервис -> Выбор настроек ->....
3. Выбранная настройка будет использоваться по умолчанию.

## Возможности программы

### Гарантия подлинности автора электронных документов

Возможность создания различных вариантов электронной цифровой подписи

- первичная подпись
- дополнительная подпись (возможность подписи документа несколькими пользователями)
- заверяющая подпись (подтверждение подписи подписью другого человека)

Использование дополнительных свойств электронной цифровой подписи (время подписания документа, внесение вашего комментария и др.)

**Длительное хранение электронных цифровых подписей**, обеспечивается в результате

- работы со Службой штампов времени (TSA)
- проверки статуса сертификатов в Службе актуальных статусов (OCSP)
- сохранение штампов времени, списков отзывов сертификатов как неотъемлемых атрибутов подписи (именно они служат "доказательствами подлинности" подписи)

### Обеспечение надежной защиты информации

- шифрование файлов и документов
- расшифрование файлов и документов

**КриптоАРМ - Клиент Удостоверяющего центра**, что позволяет

- создавать запрос на получение сертификата
- обновлять ключи и сертификаты
- приостанавливать действие сертификата
- возобновлять действие сертификата
- отзываться сертификат

### Управление криптографическими объектами

- цифровыми сертификатами
- запросами на сертификаты
- списками отзыва сертификатов
- криптопровайдерами
- ключевыми носителями

- ключевыми контейнерами

## Надежное хранение ключевой информации

Для хранения закрытой ключевой информации «КриптоАРМ» поддерживает работу с отчуждаемыми ключевыми носителями – eToken, ruToken

## Автоматизация работы

Для облегчения работы в программе «КриптоАРМ» можно создавать настройки для выполнения криптографических операций. В настройках могут быть выбраны используемый криптопровайдер, сертификаты подписи и шифрования, определен список получателей и т.д. Программа выполнит операцию точно по заданным вами параметрам настройки.

Более подробную информацию о возможностях программы вы можете найти в руководстве Администратора.

## Цифровые сертификаты

### Для чего нужен цифровой сертификат?

Сертификаты могут выдаваться для различных целей, например, для:

- Шифрования
- Создания цифровой подписи
- Проверки подлинности пользователя Интернет
- Защиты электронной почты

### Жизненный цикл сертификата

Жизненный цикл сертификата включает в себя следующие этапы:

- Создание запроса на сертификат в Удостоверяющий Центр
- Проверка Удостоверяющим центром верности данных
- Выпуск сертификата
- Распространение сертификата среди участников документооборота
- Хранение и выдача сертификата по запросу пользователей и владельцев сертификатов
- Приостановка и возобновление действия сертификата
- Обновление информации, содержащейся в сертификате, и ключевой пары
- Отзыв сертификата по запросу владельца или уполномоченного органа

### Получить цифровой сертификат

Чтобы получить цифровой сертификат, вам необходимо:

- а) [Создать запрос на сертификат](#) и сформировать закрытые ключи

---

**!** При создании запроса сохраняйте закрытый ключ сертификата в памяти ключевого носителя. Носитель с закрытым ключом храните в надежном месте. Никому его не передавайте.

---

- б) Передать созданный файл запроса администратору центра сертификации
- в) Получить личный сертификат
- г) Установить его в хранилище
- д) Скачать и установить корневой сертификат
- е) Скачать и установить актуальный список отзыва сертификатов

## Создать запрос на сертификат

**Запрос на сертификат** - это сообщение, содержащее необходимую информацию для получения сертификата в Удостоверяющем центре

Запрос на сертификат формируется с помощью **Мастера создания запроса**. Процедура создания запроса заключается в заполнении полей диалогов, предлагаемых Мастером. Для перехода к следующему окну, нажимайте кнопку **Далее**.

Для создания запроса на получение сертификата в УЦ:

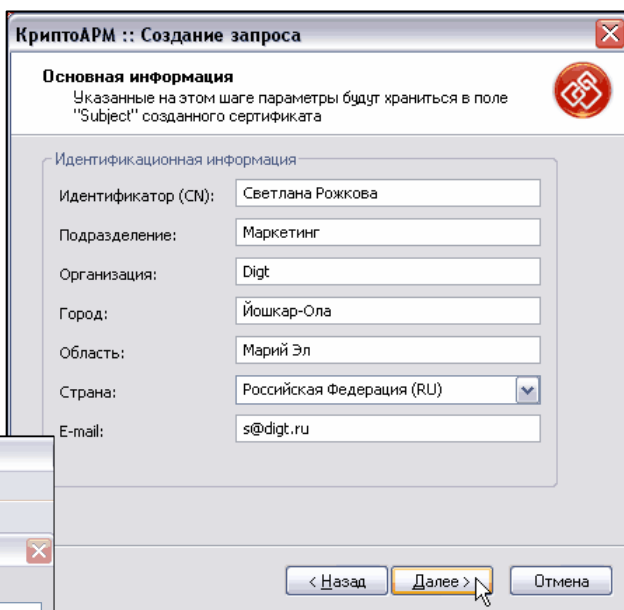
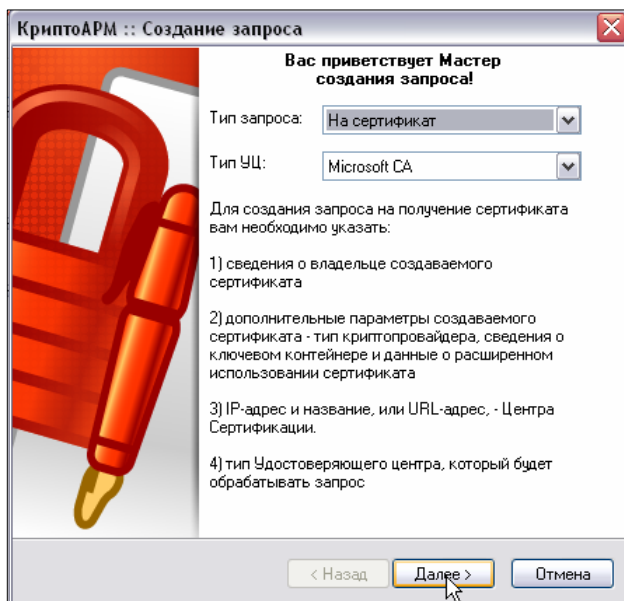
1. В главном окне откройте раздел **Сертификаты**.
2. Выберите **Создать запрос на сертификат**.

Откроется Мастер создания запроса. Ознакомьтесь с порядком и требованиями создания запроса на получение сертификата.

3. В графе **Тип УЦ** укажите тип Удостоверяющего центра, в котором будет обрабатываться запрос (поддерживаются Microsoft Certification Authority и КриптоПро УЦ)
4. В окне **Основная информация** введите ваши данные, которые будут отражены в сертификате:

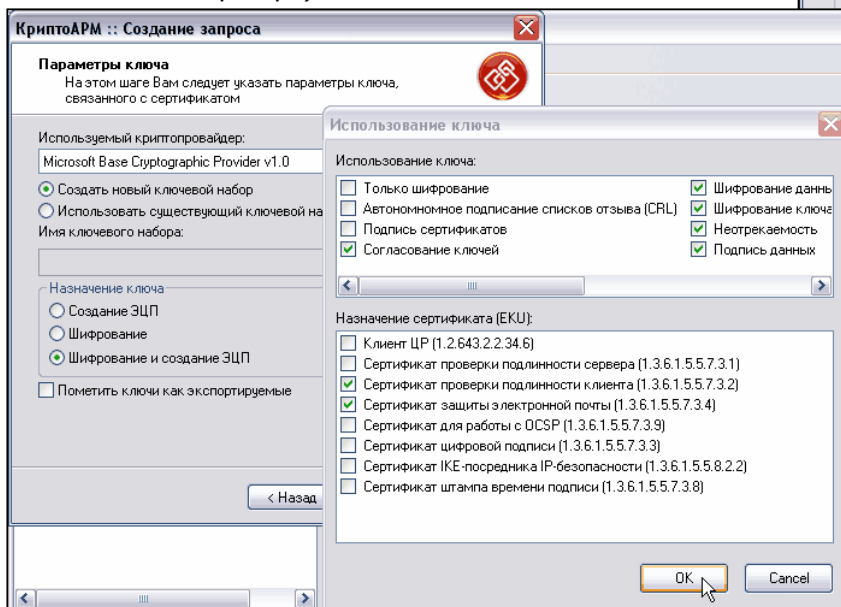
- Имя владельца
- E-mail (адрес электронной почты)
- Подразделение
- Организация
- Город
- Регион
- Страна (выберите из списка)

5. Далее в окне **Параметры ключа** в выпадающем списке выберите криптопровайдер, который будет использован при создании сертификата (уточните у администратора).



6. В этом же окне выберите вариант создания ключевого набора:

- При установке переключателя **Создать ключевой набор** сертификат будет создан на основе нового ключевого набора.
- При установке переключателя **Использовать**



**существующий ключевой набор** – выберите ключевой набор, который будет использован при создании сертификата, из списка существующих (кнопка **Выбрать**)

7. Укажите «Назначение ключа» (конкретные цели использования сертификата), поставив переключатель напротив необходимого пункта

- Создание ЭЦП
- Шифрование
- Шифрование и создание ЭЦП

Нажав на кнопку **Дополнительно**, укажите варианты использования ключа и назначение сертификата (EKU)

---

**!** Уточните у администратора, каково назначение вашего сертификата, и отметьте в списках соответствующие поля.

---

В списке **Назначений ключа** выберите необходимое:

- только шифрование
- автономное подписание списков отзыва
- подпись сертификатов
- согласование ключей
- шифрование данных
- шифрование ключа
- неотракаемость
- подпись данных

В списке **Назначений сертификата (EKU)** выберите необходимое:

- Клиент ЦР (Центра регистрации)
- Сертификат проверки подлинности клиента
- Сертификат защиты электронной почты
- Сертификат цифровой подписи
- и другие

---

**!** Для того чтобы было возможно помещать (экспортировать) сертификат в файл вместе с закрытыми ключами, необходимо поставить флаг **Пометить ключи как экспортируемые**

---

8. Укажите, каким образом вы хотите отправить запрос на обработку

---

**!** Обратитесь к администратору, так как вариант отправки запроса зависит от Удостоверяющего центра, с которым работает ваша организация.

---

**Выбор дополнительных параметров**  
Выберите дополнительные параметры

Сохранить запрос в файл  
Имя:

Отправить запрос по электронной почте

Отправить запрос по сети

- на съемном ключевом носителе (дискете, USB-брелке, смарт-карте), предварительно сохранив запрос в файл
- по электронной почте

Для этого на следующем шаге укажите тему письма, адрес электронной почты 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

9. На основе указанных данных будет сформирован запрос на сертификат открытого ключа. После завершения операции возникнет окно с информацией о ее результатах.

10. На запрос системы установите пароль на данный носитель и подтвердите его.

## Статусы сертификатов

Возможны 3 статуса действительности сертификатов, выданных Удостоверяющим центром:

-  «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 ЭЦП
  - 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

## Что такое самоподписанный сертификат?

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

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

Обменявшись такими сертификатами между собой, вы сможете пересылать друг другу подписанные и зашифрованные электронные данные, не беспокоясь при этом, что информация может быть перехвачена, искажена и использована против ваших интересов.

---

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

---

## Создать самоподписанный сертификат

1. В главном окне откройте раздел **Сертификаты**.

2. Выберите **Создать самоподписанный сертификат**.

Откроется Мастер создания запроса. Ознакомьтесь с порядком и требованиями создания запроса на получение сертификата.

3. В окне **Основная информация** введите ваши данные, которые будут отражены в сертификате:

- Имя владельца
- E-mail (адрес электронной почты)
- Подразделение
- Организация
- Город
- Регион
- Страна (выберите из списка)

КриптоАРМ :: Создание запроса

**Основная информация**  
Указанные на этом шаге параметры будут храниться в поле "Subject" созданного сертификата

Идентификационная информация

Идентификатор (CN): Светлана Рожкова  
Подразделение: Маркетинг  
Организация: Digit  
Город: Йошкар-Ола  
Область: Марий Эл  
Страна: Российская Федерация (RU)  
E-mail: s@digit.ru

< Назад    Далее >    Отмена

4. Далее в окне **Параметры ключа** в выпадающем списке выберите криптопровайдер, который будет использован при создании сертификата (уточните у администратора).

5. В этом же окне выберите вариант создания ключевого набора:

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

КриптоАРМ :: Создание запроса

**Параметры ключа**  
На этом шаге Вам следует указать параметры ключа, связанного с сертификатом

Используемый криптопровайдер:  
Microsoft Base Cryptographic Provider v1.0

Создать новый ключевой набор  
 Использовать существующий ключевой набор  
Имя ключевого набора:

Назначение ключа  
 Создание ЭЦП  
 Шифрование  
 Шифрование и создание ЭЦП  
 Пометить ключи как экспортируемые

Использование ключа

Использование ключа:

Только шифрование  
 Автономное подписание списков отзыва (CRL)  
 Подпись сертификатов  
 Согласование ключей

Назначение сертификата (EKU):

Клиент ЦР (1.2.643.2.2.34.6)  
 Сертификат проверки подлинности сервера (1.3.6.1.5.5.7.3.1)  
 Сертификат проверки подлинности клиента (1.3.6.1.5.5.7.3.2)  
 Сертификат защиты электронной почты (1.3.6.1.5.5.7.3.4)  
 Сертификат для работы с OCSP (1.3.6.1.5.5.7.3.9)  
 Сертификат цифровой подписи (1.3.6.1.5.5.7.3.3)  
 Сертификат IKE-посредника IP-безопасности (1.3.6.1.5.5.8.2.2)  
 Сертификат штампа времени подписи (1.3.6.1.5.5.7.3.8)

OK    Cancel

6. Укажите «Назначение ключа» (конкретные цели использования сертификата), поставив переключатель напротив необходимого пункта

- Создание ЭЦП
- Шифрование
- Шифрование и создание ЭЦП

Нажав на кнопку **Дополнительно**, укажите варианты использования ключа и назначение сертификата (EKU)

**!** Уточните у администратора, каково назначение вашего сертификата, и отметьте в списках соответствующие поля.

В списке **Назначений ключа** выберите необходимое:

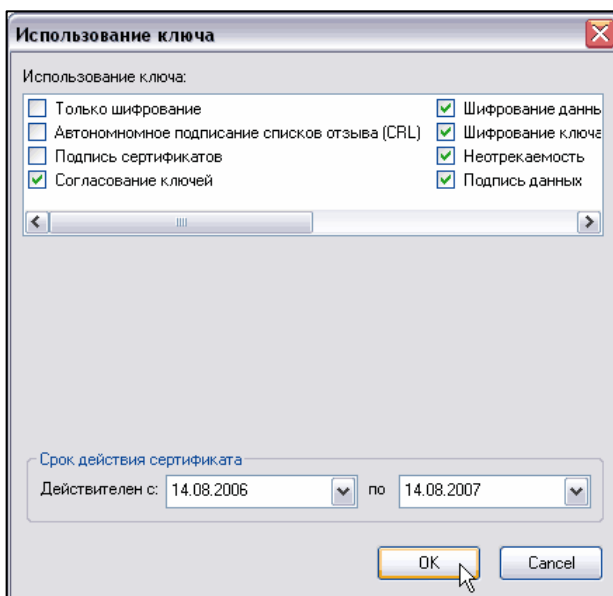
- только шифрование
- автономное подписание списков отзыва
- подпись сертификатов
- согласование ключей
- шифрование данных
- шифрование ключа

- неотрекаемость
- подпись данных

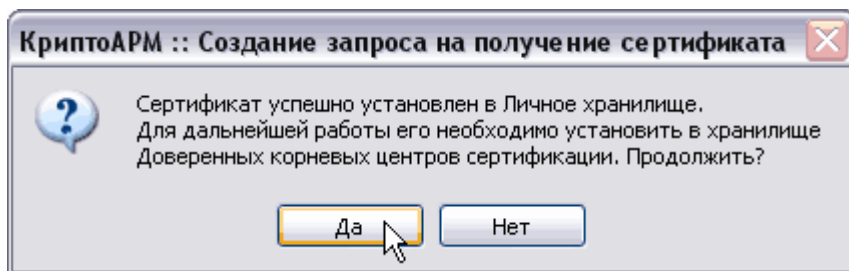
В поле **Срок действия сертификата:**

- **Дата, с которой сертификат действителен** - проставляется текущее системное время (время на вашем компьютере);
- **Дата, до которой сертификат действителен** - проставляется время на 1 год вперед от текущего системного времени.

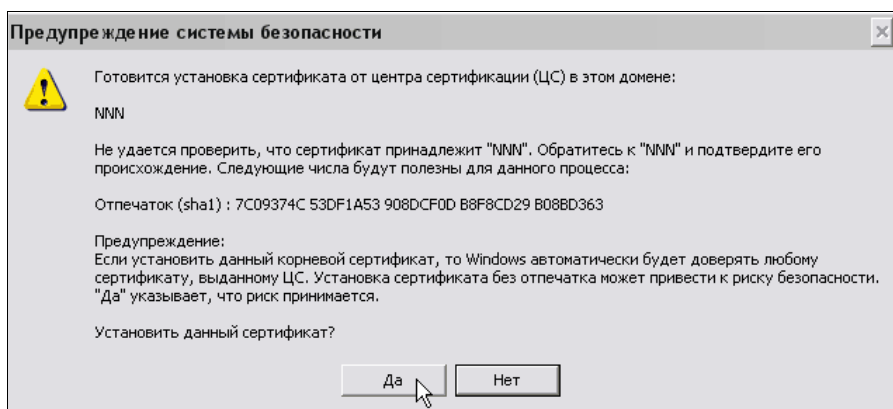
Вы можете отредактировать дату начала и окончания действия сертификата.



7. На основе указанных данных будет сформирован самоподписанный сертификат открытого ключа. После завершения операции возникнет окно с информацией о ее результатах.
8. На запрос системы установите пароль на носитель и подтвердите его.
9. Для дальнейшей работы установите самоподписанный сертификат в хранилище Доверенных корневых центров сертификации.



10. На запрос системы установить ли самоподписанный сертификат в хранилище Доверенных корневых центром сертификации, нажмите на кнопку **Да**.



# Электронная цифровая подпись

## Когда используют электронную цифровую подпись



В конце письма мы привыкли ставить свою подпись, чтобы уведомить получателя о том, кто именно является отправителем этого документа. Кроме того, подпись ответственного лица придает документу юридическую силу, что очень важно.

При соблюдении правовых условий равнозначной собственноручной подписи в документе на бумажном носителе признается электронная цифровая подпись на документе.

Электронная подпись решает следующие практические задачи:

- **Отказ от выполненных действий.** Человек утверждает, что он не посылал некоторый документ, хотя на самом деле этот документ был отправлен от его имени.
- **Изменение документа.** Получатель изменяет полученный документ и утверждает, что именно такую версию документа он и получил от вас.
- **Подделка.** Человек фабрикует сообщение и утверждает, что оно ему прислано.
- **Маскировка.** Отправка сообщения от чужого имени.
- **Повтор.** Злоумышленник С посылает повторно сообщение от А к Б, перехваченное им ранее.

## Варианты электронной подписи

В программе "КриптоАРМ" поддерживаются разные варианты и типы электронной подписи, а также форматы файла электронной подписи.

- **Первичная подпись**
- **Дополнительная подпись**
- **Заверяющая подпись**

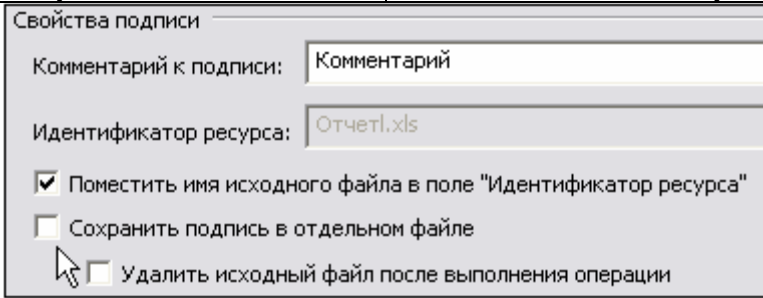
Первичная подпись - это первая электронная подпись, которая поставлена на исходный документ.

К документу, подписанному первичной подписью, могут быть добавлены дополнительные подписи других пользователей (например, при согласовании документа сотрудниками одного отдела). При этом дополнительные и первичная подписи будут иметь равный статус (равнозначны).

Первичная подпись может быть заверена подписью другого пользователя (например, при согласовании документа с начальником отдела). В этом случае будет построена цепочка (иерархия) подписей на файле: заверяющая подпись и первичная подписи будут неравнозначны.

## Типы электронной подписи

<b>Совмещенная подпись</b>	<b>Отделенная подпись</b>
Подпись, соединенная с подписываемыми данными.	Подпись, отделенная от подписываемых данных
Наиболее часто используемый тип подписи, так как он удобен в использовании	С документом, подписанным отделенной электронной подписью могут работать все пользователи, даже если на их компьютере не установлена программа «КриптоАРМ».
<b>Как выбрать тип подписи при подписании документа?</b>	
Для того чтобы документ был подписан совмещенной подписью, во время операции	Для того чтобы документ был подписан отделенной подписью, во время операции

создания ЭЦП в окне <b>Параметры подписи</b> НЕ ставьте флаг напротив строки <b>Сохранить подпись в отдельном файле</b> .	создания ЭЦП в окне <b>Параметры подписи</b> поставьте флаг напротив строки <b>Сохранить подпись в отдельном файле</b> .
	
<b>Что будет результатом подписи файла?</b>	
Результатом операции подписи файла является файл, содержащий как сами данные, так и ЭЦП к этим данным.	Результатом операции подписи файла являются два файла - исходный файл и файл, содержащий электронную подпись к исходным данным.
<b>Как проверить подпись файла?</b>	
Для того чтобы проверить корректность ЭЦП с помощью "КриптоАРМ", необходимо выполнить операцию "Снять и проверить подпись".	Для того чтобы проверить корректность ЭЦП с помощью "КриптоАРМ", необходимо выполнить операцию "Проверить подпись".

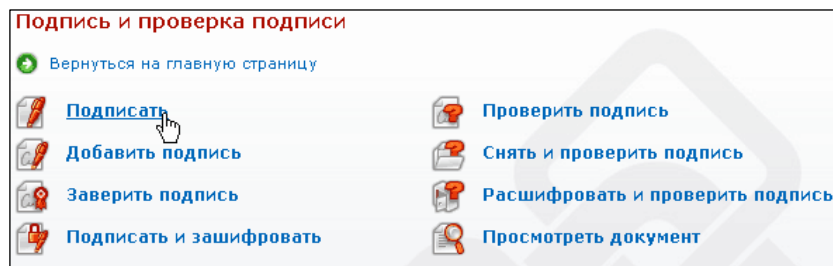
## Подписать электронный документ

**!** В программе «КриптоАРМ» вы можете подписать один файл или целую папку файлов.

Для того чтобы подписать документ:

1. В главном окне откройте раздел **Подпись**.
2. Выберите пункт **Подписать**.

Откроется Мастер создания электронной цифровой подписи.

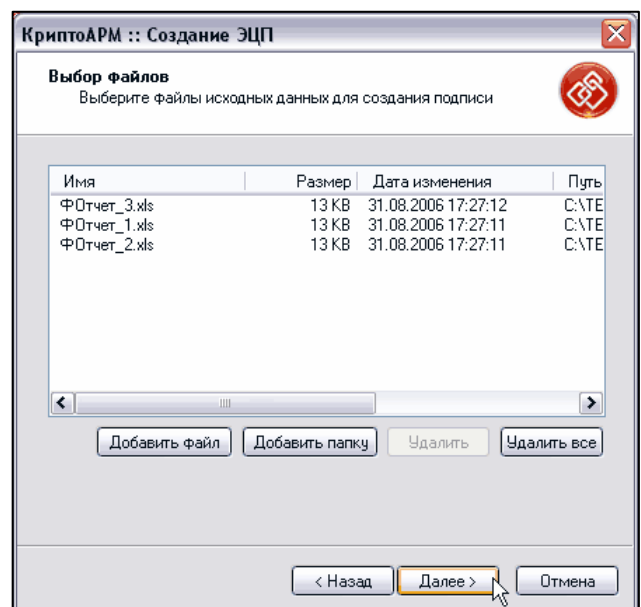


3. На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**. (Для создания настройки обратитесь к администратору.)
4. Выберите папку с файлами или отдельный файл, которые необходимо подписать (кнопки **Добавить папку** и **Добавить файл** соответственно).
5. Введите необходимые свойства подписи:

- **Комментарий к подписи**

\*Комментарием к подписи может служить информация, понятная вам и вашим коллегам, просматривающим подписанный документ (например, "Согласовано!")

- **Идентификатор ресурса**



**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

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)

Флаг	Пояснение
<b>Сохранить подпись в отдельном файле</b>	<p>В этом окне выберите тип электронной подписи:</p> <ul style="list-style-type: none"> <li>При установке флага будет создана <b>отделенная электронная подпись</b> на файле (например, может быть удобна в том случае, если вы отправляете документ человеку, который не использует "КриптоАРМ" и ему важна не столько подпись, сколько сами данные)</li> <li>При отсутствии флага - будет сформирована <b>электронная подпись, включающая в себя файл с исходными данными</b> (в этом случае документ и ЭЦП будут храниться вместе)</li> </ul>
<b>Удалить исходный файл после выполнения операции</b>	<p>Если вы решили создать файл совмещенной подписи, вы можете удалить исходный файл после выполнения операции. Эта возможность важна</p> <ol style="list-style-type: none"> <li>прежде всего, для удобства работы с документами</li> <li>для тех, кому требуется хранить и обмениваться только подписанными ЭЦП документами (в рамках регламента электронного документооборота, принятого в организации)</li> </ol> <p>В случае если вы установите флаг напротив строки <b>Удалить исходный файл после выполнения операции</b>, документ (-ы), выбранный для подписи, будет удален при успешном завершении операции.</p>
<b>Включить время создания подписи</b>	При установке флага - в файл подписи будет включено время подписи

6. Выберите сертификат для создания подписи, т.е. ваш личный сертификат, которым вы собираетесь подписать документ. Хеш алгоритм определится автоматически.

**КриптоАРМ :: Создание ЭЦП**

Статус:  
Данные, необходимые для создания электронной подписи, собраны

Параметры

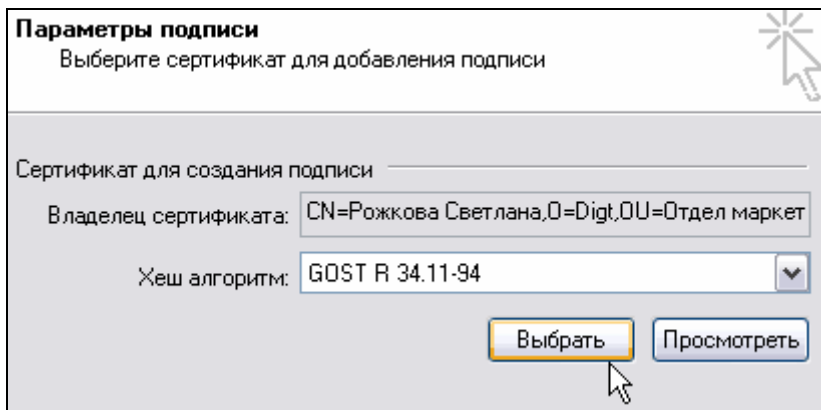
Сертификат подписи	Svetlana Rozhkova
Формат подписи	DER-кодировка (*.sig)
Входной файл 1	C:\TEMP\Ф\Отчет_3.xls
Файл подписи 1	C:\TEMP\Ф\Отчет_3.xls.sig
Входной файл 2	C:\TEMP\Ф\Отчет_1.xls
Файл подписи 2	C:\TEMP\Ф\Отчет_1.xls.sig
Входной файл 3	C:\TEMP\Ф\Отчет_2.xls
Файл подписи 3	C:\TEMP\Ф\Отчет_2.xls.sig

Сохранить данные в настройку для дальнейшего использования

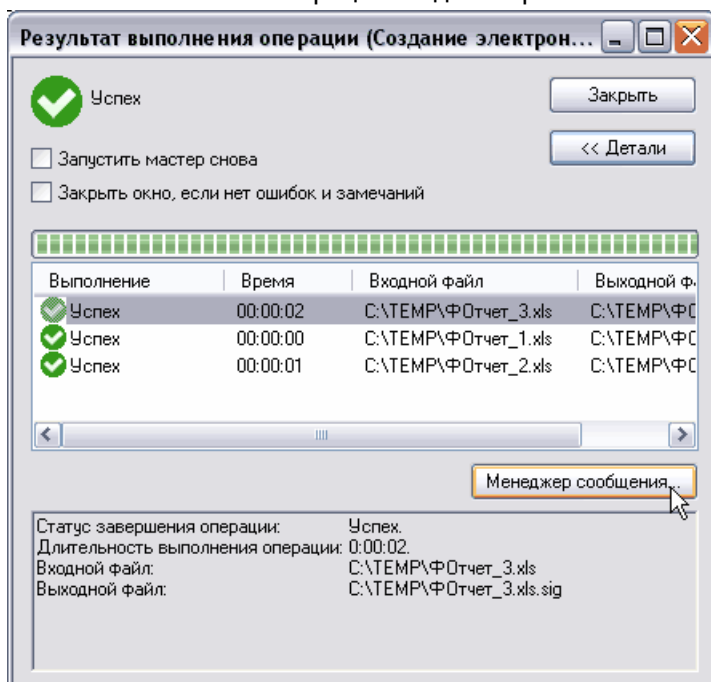
Наименование:

Настроить отображение шагов Мастера Вы можете в меню приложения "Управление настройками".

< Назад **Готово** Отмена



7. Для доступа к выбранному ключевому контейнеру (ГОСТ сертификата) введите пароль.
8. После сбора данных для создания ЭЦП возникнет окно с информацией о статусе операции и об используемых параметрах: сертификат, которым был подписан файл. Нажмите **Готово**.
9. Начнется процесс подписи файла. Остановить процесс можно, нажав на кнопку **Отмена**.



10. Сформированный файл подписи по умолчанию будет сохранен в тот же каталог, в котором находится файл с исходными данными. Имя файла подписи совпадает с именем подписываемого файла, дополненным расширением (\*.sig/\*.p7s/\*.pem). Если файл с таким именем уже существует, сохраните его под другим именем или перезапишите.
11. 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 >>**.

Чтобы просмотреть информацию о подписи и сертификате подписчика, обратитесь к пункту [Просмотр информации о подписи и сертификате](#).

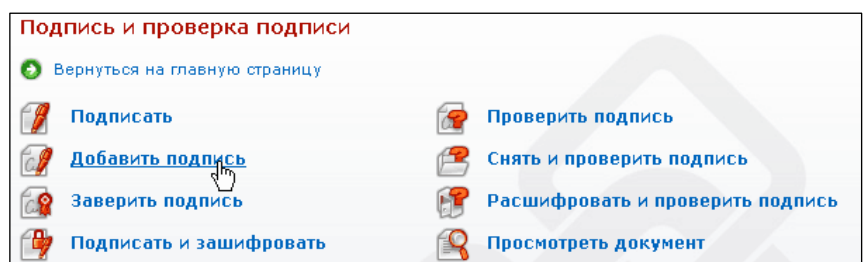
### Добавить дополнительную подпись

! В программе «КриптоАРМ» вы можете подписать один файл или целую папку файлов.

Для того чтобы добавить подпись к уже подписанному файлу:

1. В главном окне откройте раздел **Подпись**.
2. Выберите пункт **Добавить подпись...**

Откроется Мастер создания запроса. Ознакомьтесь с порядком и требованиями создания подписи.



3. 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**. (Для создания настройки обратитесь к администратору.)

- Выберите папку с файлами или отдельный файл, которые необходимо подписать (кнопки **Добавить папку** и **Добавить файл** соответственно).
- Введите необходимые свойства добавляемой подписи:

**Параметры подписи**  
Установите желаемые параметры подписи

Свойства подписи

Комментарий к подписи:

Включить время создания подписи

- Комментарий к подписи**

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

**КриптоАРМ :: Добавление ЭЦП**

**Выбор файлов**  
Выберите файлы исходных данных для добавления подписи

Имя	Размер	Дата изменения	Путь
ФОтчет_1.xls.sig	14 KB	02.09.2006 10:25:54	C:\TE
ФОтчет_2.xls.sig	14 KB	02.09.2006 10:25:54	C:\TE
ФОтчет_3.xls.sig	14 KB	02.09.2006 10:25:54	C:\TE

Добавить файл    Добавить папку    Удалить    Удалить все

< Назад    **Далее >**    Отмена

- Выберите сертификат для добавления подписи, т.е. ваш личный сертификат. Хеш алгоритм определится автоматически.

**Параметры подписи**  
Выберите сертификат для добавления подписи

Сертификат для создания подписи

Владелец сертификата: CN=Рожкова Светлана,O=Digit,OU=Отдел маркетинг

Хеш алгоритм:

Выбрать    Просмотреть

- 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**.

**КриптоАРМ :: Добавление ЭЦП**

Статус  
Данные, необходимые для добавления электронной подписи, собраны

Параметры

Сертификат подписи	Svetlana Rozhkova
Файл подписи 1	C:\TEMP\ФОтчет_1.xls.sig
Файл подписи 2	C:\TEMP\ФОтчет_2.xls.sig
Файл подписи 3	C:\TEMP\ФОтчет_3.xls.sig

Сохранить данные в настройку для дальнейшего использования

Наименование:

Настроить отображение шагов Мастера Вы можете в меню приложения "Управление настройками".

< Назад    **Готово**    Отмена

**Результат выполнения операции (Добавление подпи...)**

Успех

Запустить мастер снова

Закрыть окно, если нет ошибок и замечаний

Выполнение	Время	Входной файл	Выходной файл
<input checked="" type="checkbox"/> Успех	00:00:01	C:\TEMP\ФОтчет_1.xls...	C:\TEMP\Ф...
<input checked="" type="checkbox"/> Успех	00:00:01	C:\TEMP\ФОтчет_2.xls...	C:\TEMP\Ф...
<input checked="" type="checkbox"/> Успех	00:00:02	C:\TEMP\ФОтчет_3.xls...	C:\TEMP\Ф...

Менеджер сообщений

Статус завершения операции: Успех.  
Длительность выполнения операции: 0:00:01.  
Входной файл: C:\TEMP\ФОтчет\_1.xls.sig  
Выходной файл: C:\TEMP\ФОтчет\_1.xls.sig

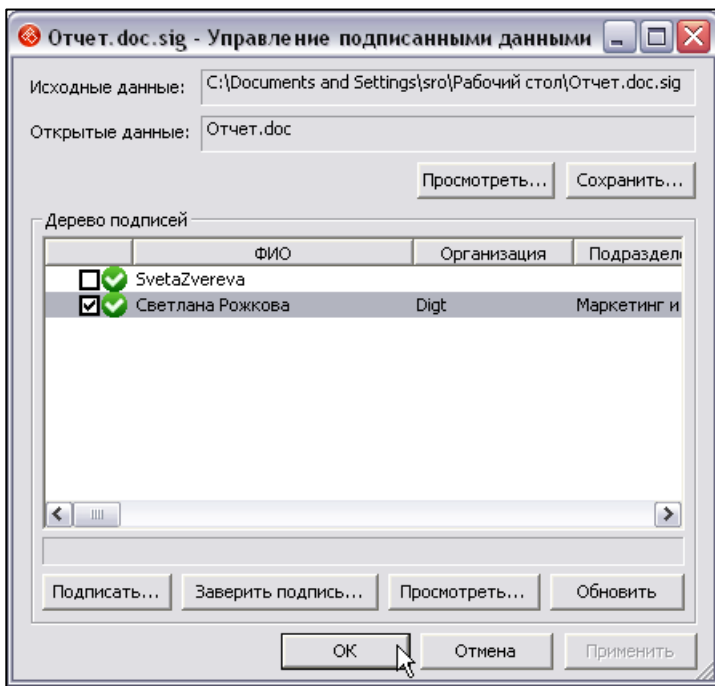
- Данные будут подписаны с использованием вашего личного сертификата. Начнется процесс подписи файла. Вы можете прервать его, нажав на кнопку **Отмена**.
- После завершения операции возникнет окно **Результат выполнения операции**. Чтобы просмотреть детальную информацию о результатах добавления подписи и используемых параметрах: имя исходного файла, имя выходного файла, статус завершения операции,

длительность выполнения операции, нажмите на кнопку **Детали >>**.

10. Если вы хотите посмотреть, кто еще кроме вас поставил подпись под документом, выделите строчку с операцией и нажмите на кнопку **Менеджер сообщения**.

Откроется окно **Управление подписанными данными**, которое содержит дерево подписей.

На данном изображении в дереве подписей верхняя подпись является первичной, а нижняя – добавленной.



Чтобы просмотреть информацию о подписи и сертификате подписчика, обратитесь к пункту [Просмотр информации о подписи и сертификате](#).

### Заверить электронную подпись

С помощью программы "КриптоАРМ" вы можете заверить своей электронной подписью подписи других пользователей (в данном случае подписываются не данные, а подписи).

Вы можете заверить подпись:

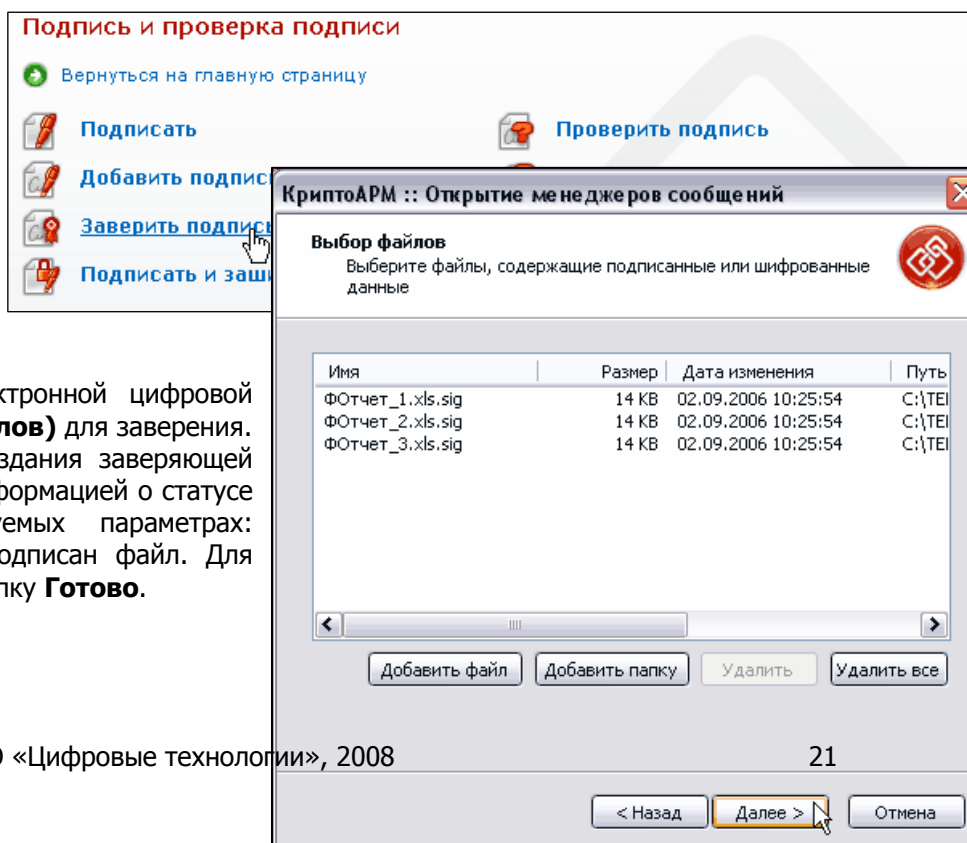
- отдельного файла
- папки файлов (при этом будет создана подпись для каждого файла, входящего в указанную папку. Подписанные файлы автоматически сохраняются в папку с исходными данными)

Для того чтобы заверить подписи:

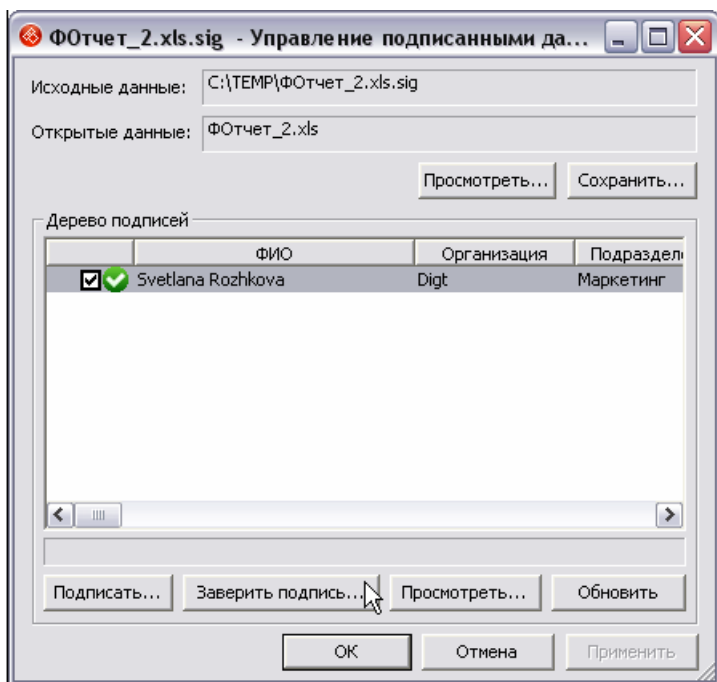
1. В главном окне откройте раздел **Подпись**.
2. Выберите пункт **Заверить подпись...**

Следуйте рекомендациям Помощника по выполнению операции.

3. Выберите подписанный электронной цифровой подписью **файл (папку файлов)** для заверения.
4. 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**.



- 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**.
- Откроется Мастер создания запроса. Ознакомьтесь с порядком и требованиями создания подписи.



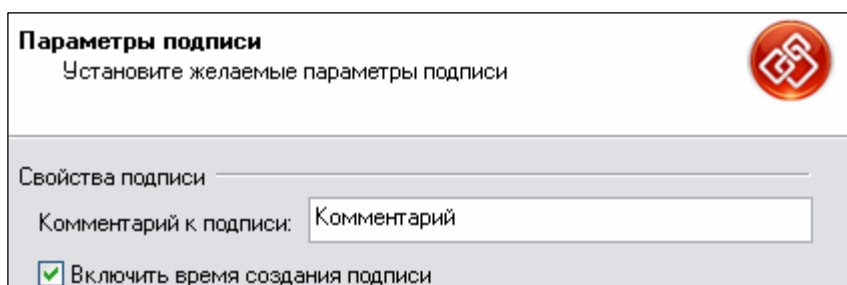
На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для подписи. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**. (Для создания настройки обратитесь к администратору.)

- Введите необходимые свойства добавляемой подписи:

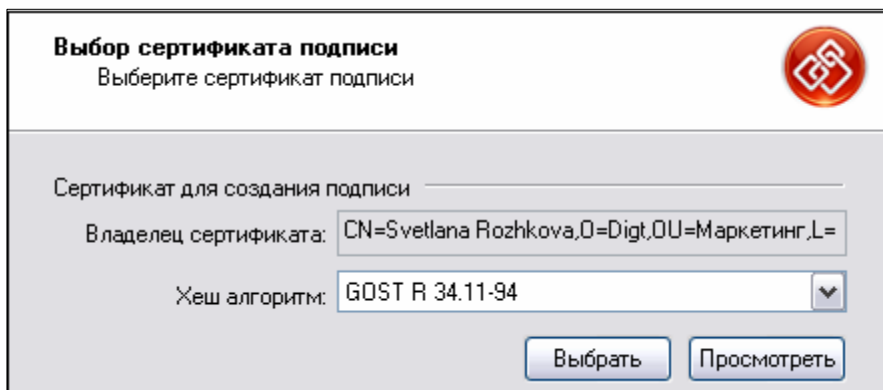
- Комментарий к подписи**

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

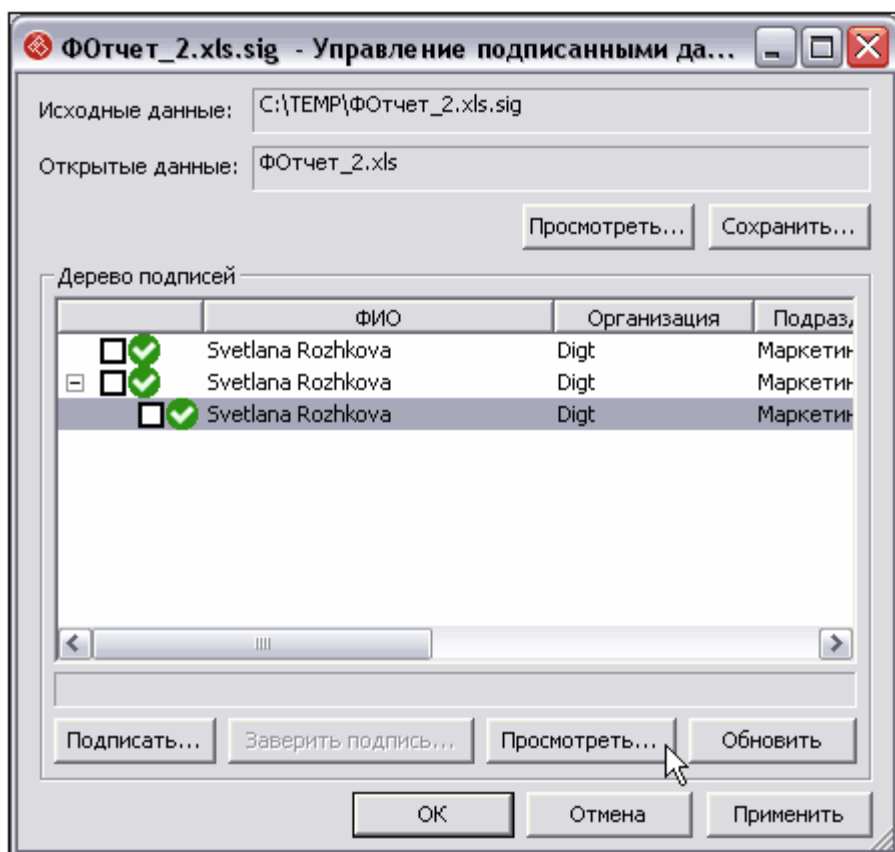
- Выберите сертификат для создания подписи, т.е. ваш личный сертификат, которым вы собираетесь подписать документ. Хеш алгоритм определится автоматически.



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



появится значок заверяющей подписи (в иерархии заверяющая подпись будет подписью второго уровня)



11. Чтобы просмотреть информацию о подписи и сертификате подписчика, обратитесь к пункту [Просмотр информации о подписи и сертификате](#).

### Проверить корректность электронной 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**.

Для того чтобы проверить подпись к файлу:

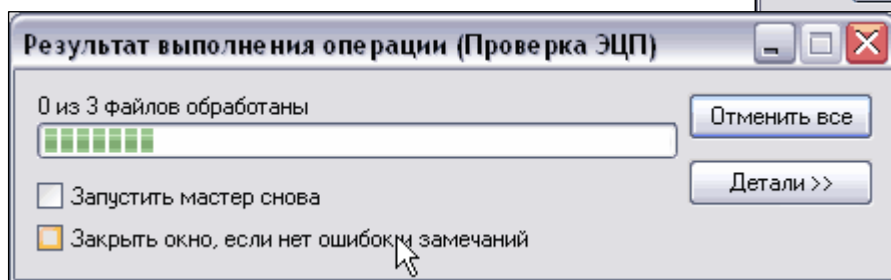
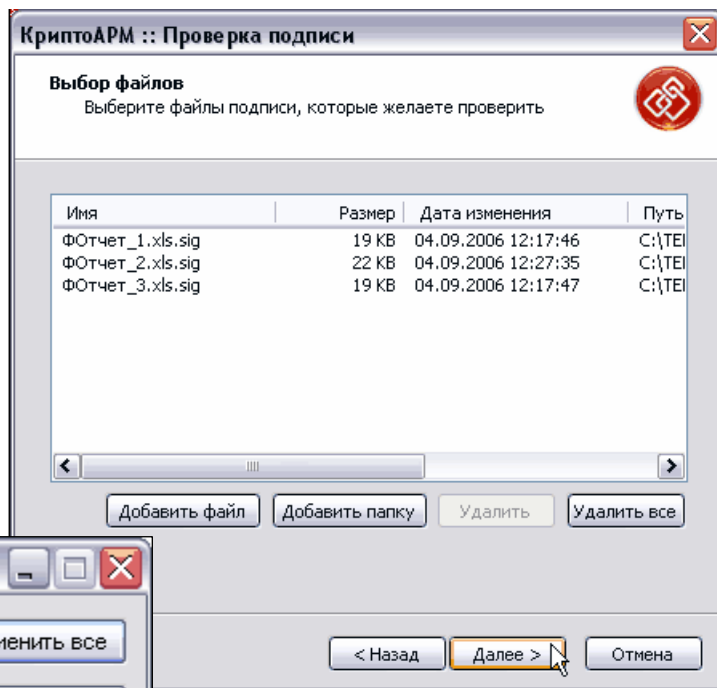
1. В главном окне откройте раздел **Подпись**.
2. Выберите пункт **Проверить подпись...**

Откроется Мастер проверки корректности ЭЦП. Ознакомьтесь с порядком и требованиями проверки подписи.

3. 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,

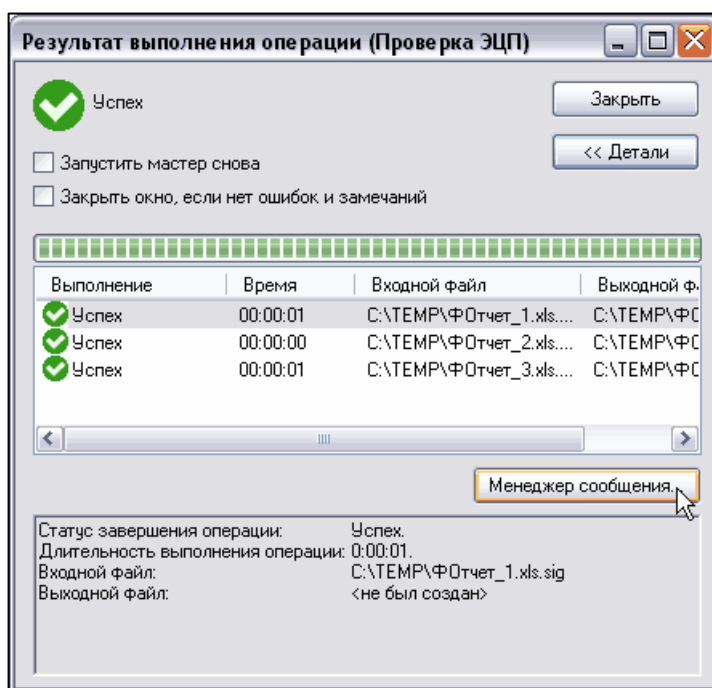
поставьте флаг в пункте **Использовать настройку по умолчанию**. (Для создания настройки обратитесь к администратору.)

4. Выберите файл или папку файлов, подписанных электронной подписью, корректность которых необходимо проверить (кнопки **Добавить папку** и **Добавить файл**).
5. После сбора данных для снятия и проверки подписи возникнет окно с информацией о статусе операции и об используемых параметрах.
6. 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.

7. 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 >>**.



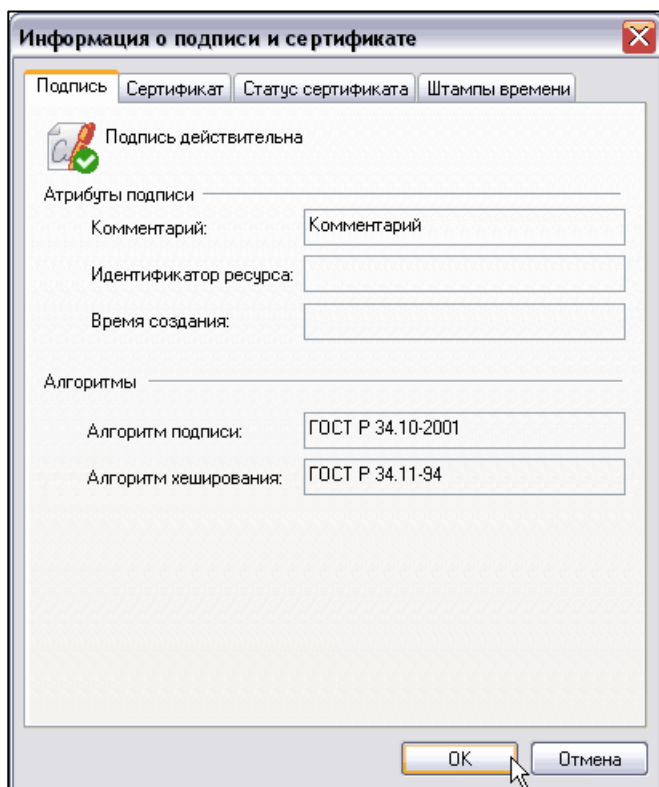
## Просмотреть информацию о подписи и сертификате

Если вы хотите просмотреть информацию о проверяемой ЭЦП 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. Для этого нажмите 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**

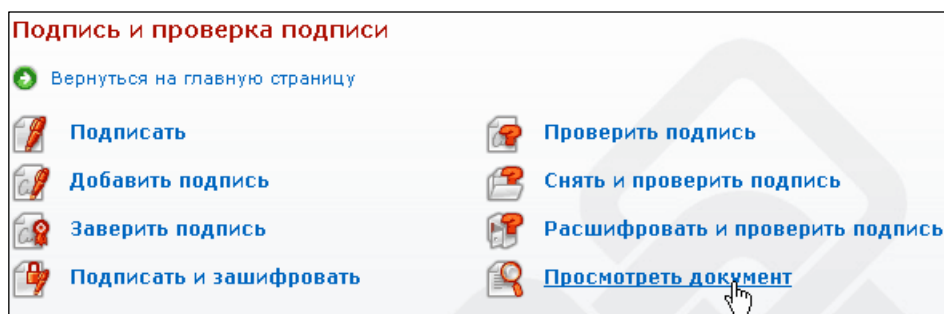
## Просмотреть подписанный документ

Программа "КриптоАРМ" позволяет просматривать исходные данные файла, содержащего совмещенную подпись.

Для того чтобы просмотреть документ:

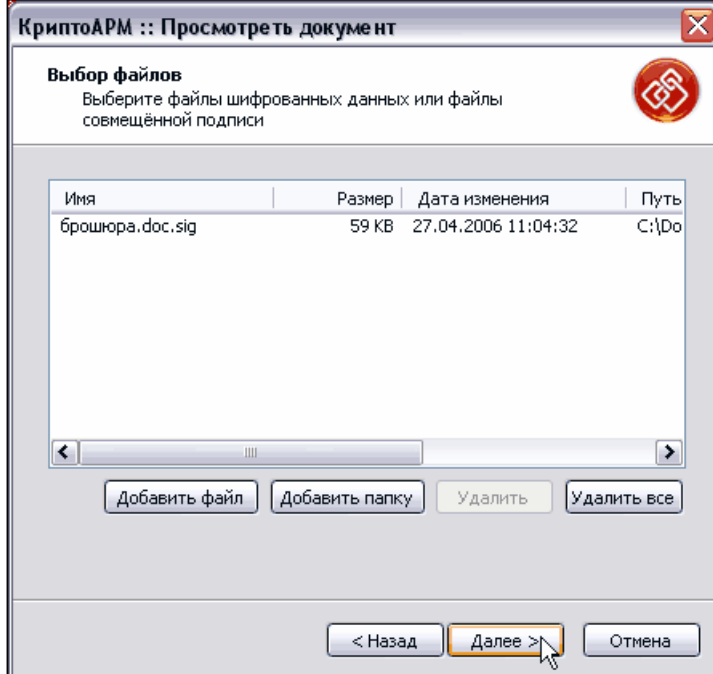
1. В главном окне откройте раздел **Подпись**.
2. Выберите пункт **Просмотреть документ...**

Далее следуйте рекомендациям Мастера выполнения операции:



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

4. После завершения сбора параметров для выполнения операции возникнет окно с информацией о статусе операции. Для продолжения нажмите на кнопку **Готово**.
5. На следующем шаге исходные данные подписанного документа будут открыты для просмотра.



# Шифрование

**Шифрование** — это способ хранения и отправки закодированной информации. Назначение шифрования — *секретность*.

Шифрование информации гарантирует вам:

- Недоступность информации для сторонних лиц
- Подлинность информации (то есть информация поступит к вам в неискаженном виде)
- Целостность информации (данные, которые вы хотите передать останутся целыми в процессе передачи)

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

Например, вы хотите послать коллеге или партнеру важные конфиденциальные данные:

1. Вы зашифровываете данные (открытый текст) с помощью сертификата открытого ключа вашего партнера. Этот сертификат вы получаете у самого партнера или в общедоступной базе данных, в которой хранятся сертификаты всех пользователей.
2. После этого вы отправляете зашифрованные данные партнеру.
3. Ваш партнер получает зашифрованные данные. С помощью своего закрытого ключа он расшифровывает данные. В результате ваш партнер получает тот самый открытый текст (конфиденциальные данные), который вы зашифровали.



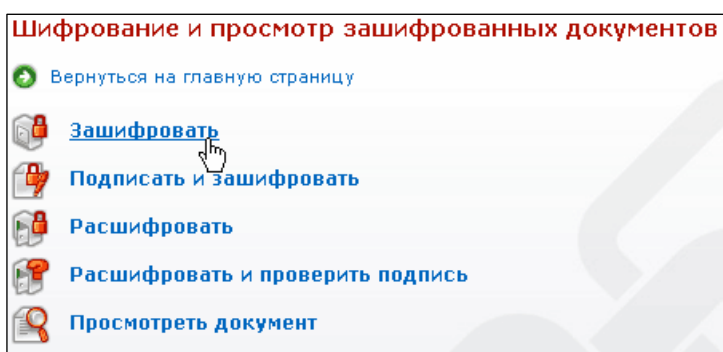
## Зашифровать файл

**!** В программе «КриптоАРМ» вы можете зашифровать один файл или целую папку файлов.

Для того чтобы зашифровать документ:

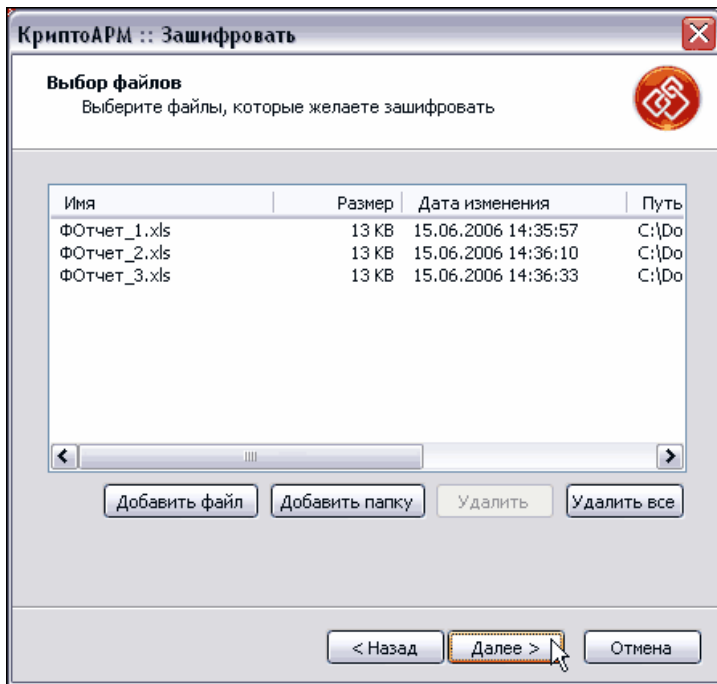
1. В главном окне откройте раздел **Шифрование**.
2. Выберите пункт **Зашифровать...**

Откроется Мастер создания запроса. Ознакомьтесь с порядком и требованиями шифрования файла.



На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек для шифрования. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**. (Для создания настройки обратитесь к администратору.)

Далее следуйте рекомендациям Мастера выполнения операции

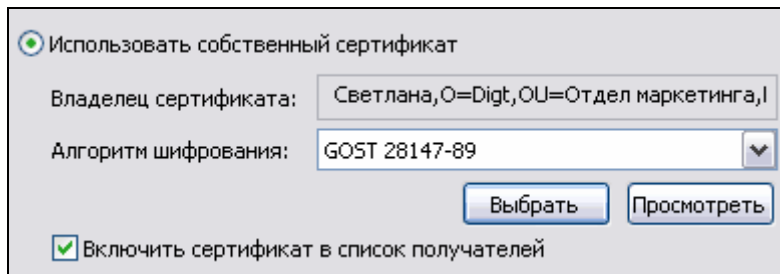


3. Выберите папку с файлами или отдельный файл, которые необходимо зашифровать (кнопки **Добавить папку** и **Добавить файл** соответственно)
4. Выберите **Выходной формат файла** согласно регламенту ЭЦП, принятому в Вашей организации (если параметр задан в настройках, просто нажмите **Далее**)

Для того чтобы после успешного завершения операции исходный файл (с открытыми данными) был удален, установите флаг **Удалить исходный файл после шифрования**.

5. Выберите режим шифрования данных. Для этого поставьте переключатель напротив соответствующей строки:

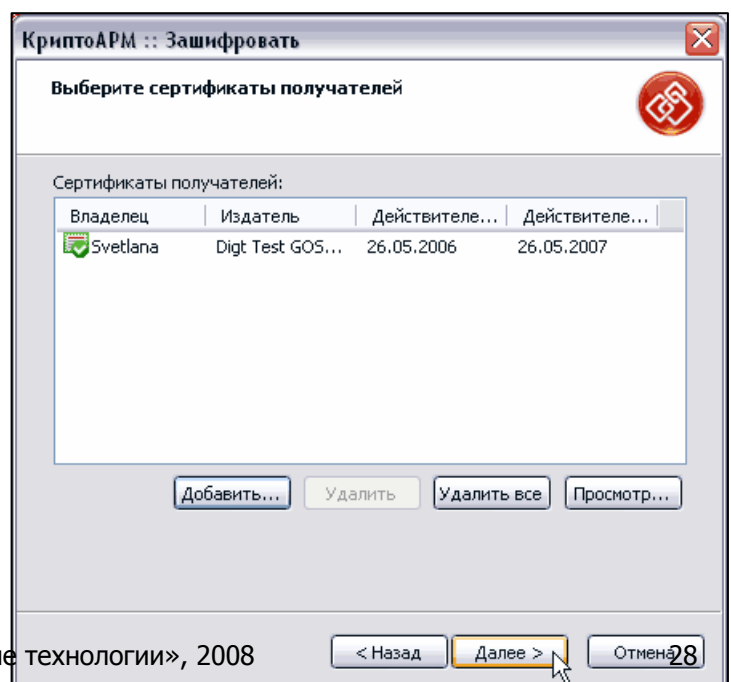
- **Использовать криптопровайдер** (в этом случае в выпадающем списке выберите необходимый тип криптопровайдера и алгоритм шифрования). Данный режим шифрования может быть выбран при отсутствии личного сертификата шифрования в соответствии с регламентом, принятым в вашей организации. (В этом случае личный сертификат не выбирается).
- **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.



6. 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:

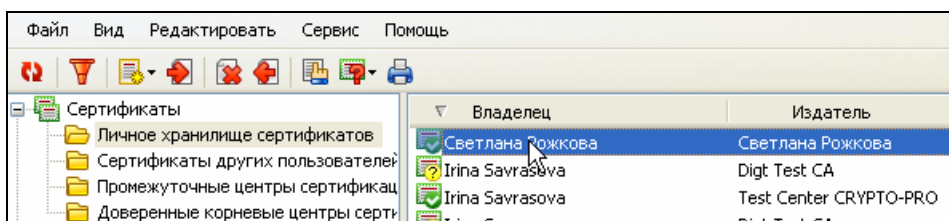


**!** Обратите внимание, для шифрования необходимо, чтобы ключи отправителя и получателя могли быть использованы *для шифрования данных*.

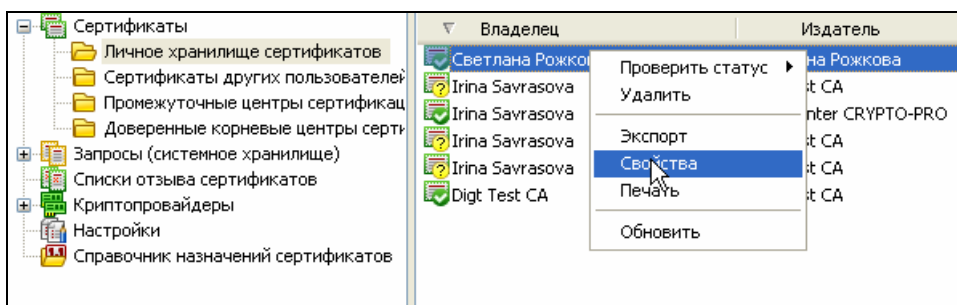
Чтобы это узнать, выполните следующие шаги:

1. Откройте главное окно «Вид эксперт»: **Вид -> Эксперт**
2. В левом окне выберите **Сертификаты**. Откроется список хранилищ.
3. Выберите **Личное хранилище сертификатов**.
4. В открывшемся хранилище выберите ваш сертификат

- двойным нажатием на левую кнопку мыши:



- или в контекстном меню объекта выберите **Свойства**:

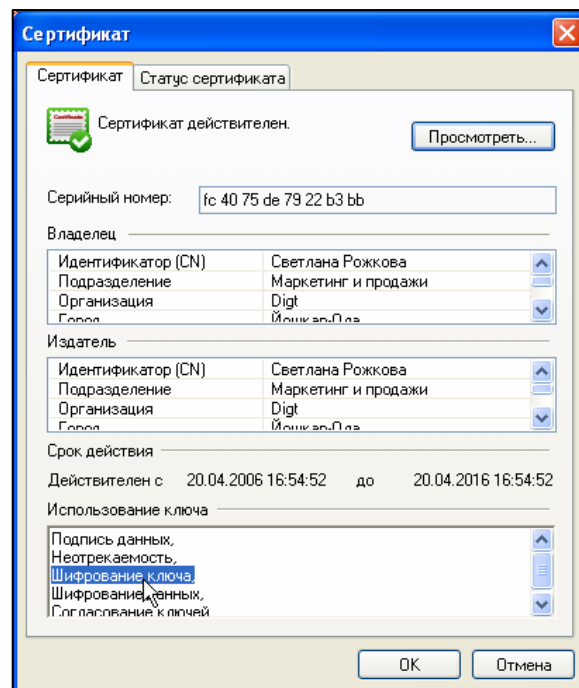


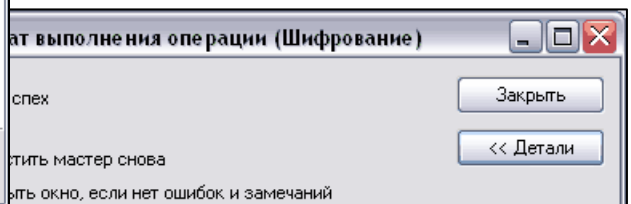
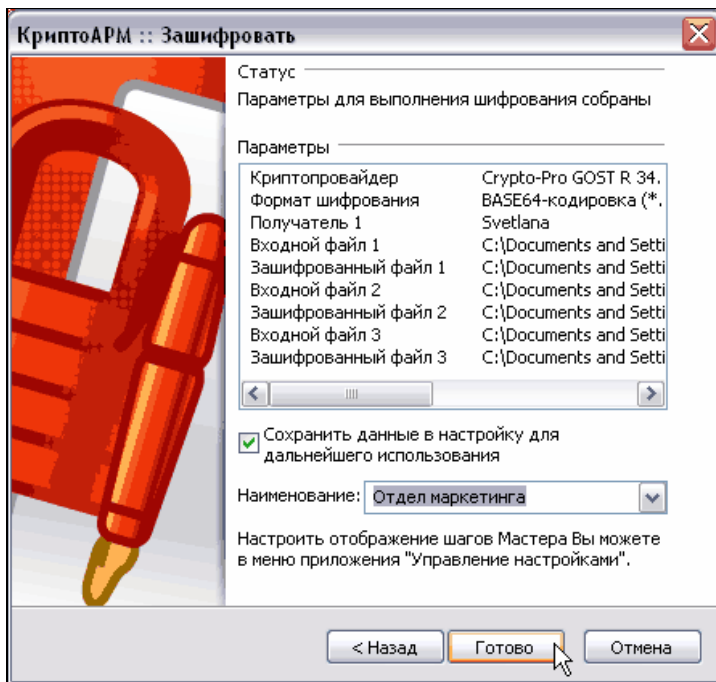
Откроется ваш личный сертификат. В поле «Использование ключа» должно быть указано: **шифрование ключа**:

Чтобы узнать, могут ли ключи получателя быть использованы для шифрования данных, повторите все шаги, начиная с первого пункта, но вместо **Личного хранилища сертификатов** выберите **Сертификаты других пользователей**.

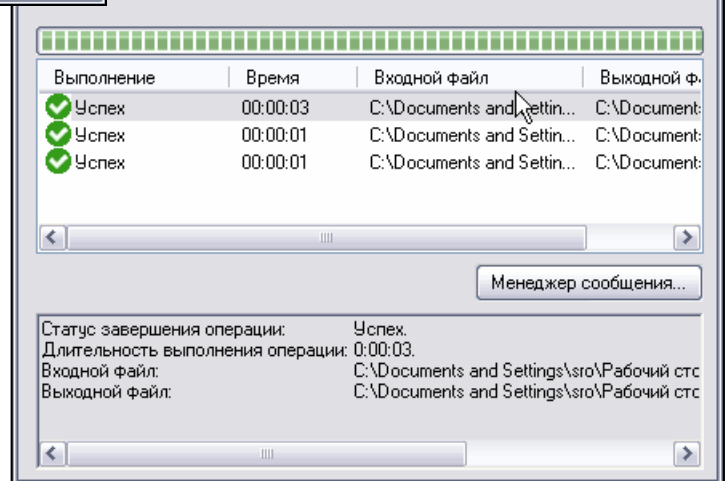
При выборе сертификата получателя автоматически проверяется его статус.

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**.






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

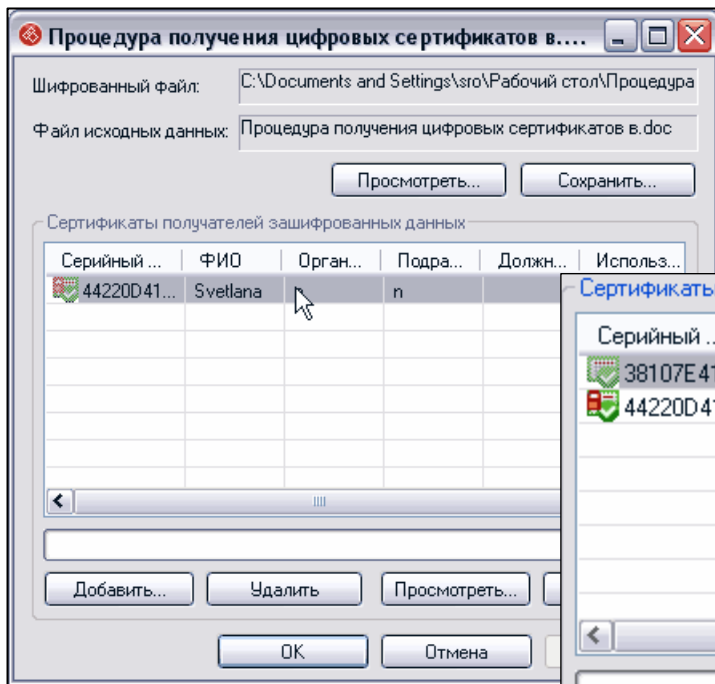


### Редактирование списка получателей

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

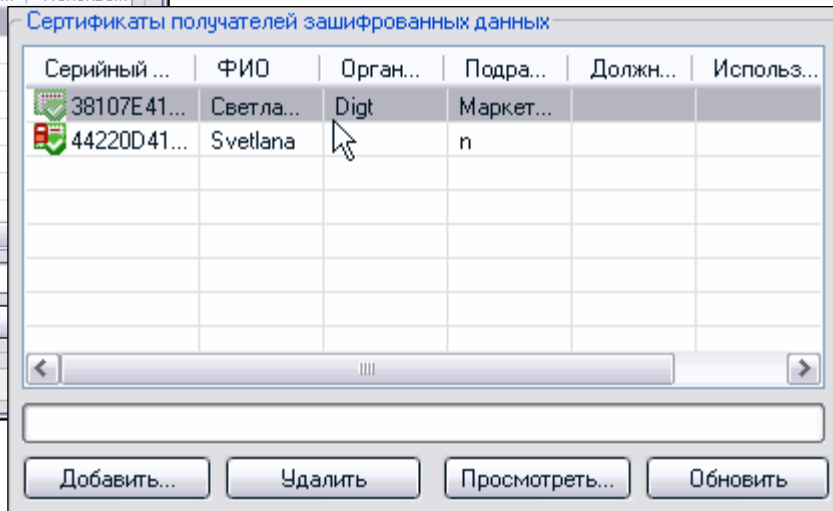
1. Выделите запись в списке окна **Результат выполнения операции** и нажмите на кнопку **Менеджер сообщения**.
2. Откроется окно **Управление шифрованными данными**, в котором вы можете:
  1. просмотреть путь, по которому сохранен зашифрованный файл,
  2. просмотреть зашифрованный файл (кнопка **Просмотреть** рядом со строкой **Файл исходных данных**),
  3. сохранить исходный файл (расшифрованные данные) по указанному пути (кнопка **Сохранить**),
  4. просмотреть информацию о сертификатах получателей зашифрованных данных и их статусы (кнопка **Просмотреть**)

**!** Сертификат расшифрования данных отмечается значком - . Сертификатом расшифрования становится первый из списка сертификатов 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.



### Просмотреть зашифрованный документ

Программа «КриптоАРМ» позволяет просматривать зашифрованный документ. Для того чтобы просмотреть документ:

1. В главном окне откройте раздел **Шифрование**.
2. Выберите пункт **Просмотреть документ...**

Далее следуйте рекомендациям Помощника по выполнению операции:

3. Выберите один или несколько файлов, которые необходимо просмотреть (кнопки **Добавить файл** и **Добавить папку** соответственно)
4. После завершения сбора параметров для выполнения операции возникнет окно с информацией о статусе операции и об используемом параметре. Для продолжения нажмите на кнопку **Готово**.
5. На следующем шаге исходные данные зашифрованного документа будут открыты для просмотра.



### Расшифровать файл

**!** В программе «КриптоАРМ» вы можете расшифровать один файл или целую папку файлов.

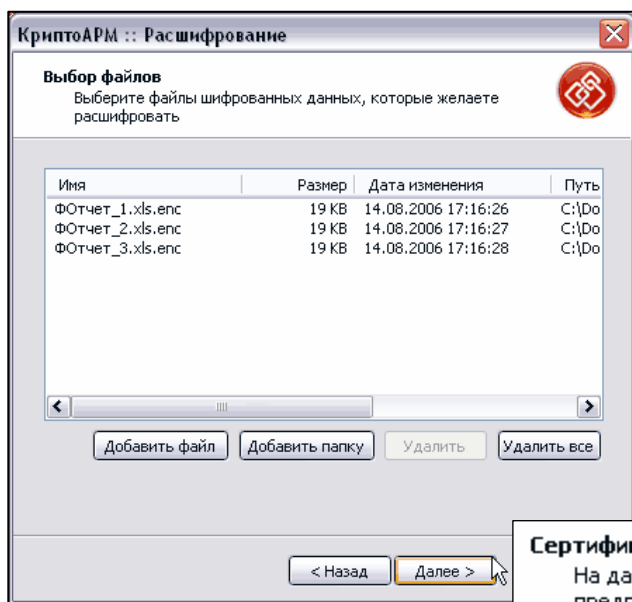
Для того чтобы зашифровать документ:

1. В главном окне откройте раздел **Шифрование**.
2. Выберите пункт **Расшифровать...**

Откроется Мастер расшифрования данных. Ознакомьтесь с порядком и требованиями расшифрования файла.

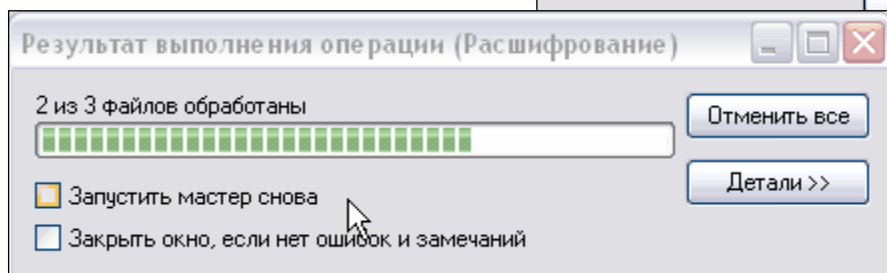
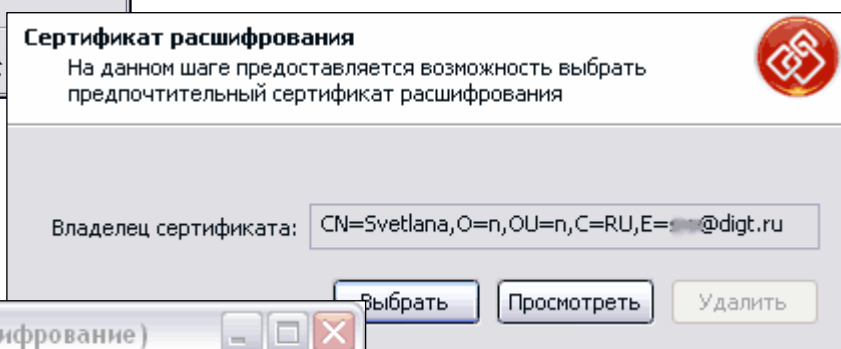
На первом шаге для упрощения работы вы можете выбрать в списке одну из уже установленных настроек. Если вы хотите в дальнейшем использовать выбранную настройку по умолчанию, поставьте флаг в пункте **Использовать настройку по умолчанию**. (Для создания настройки обратитесь к администратору.)

Далее следуйте рекомендациям Мастера выполнения операции



Вы можете прервать его, нажав на кнопку **Отмена**:

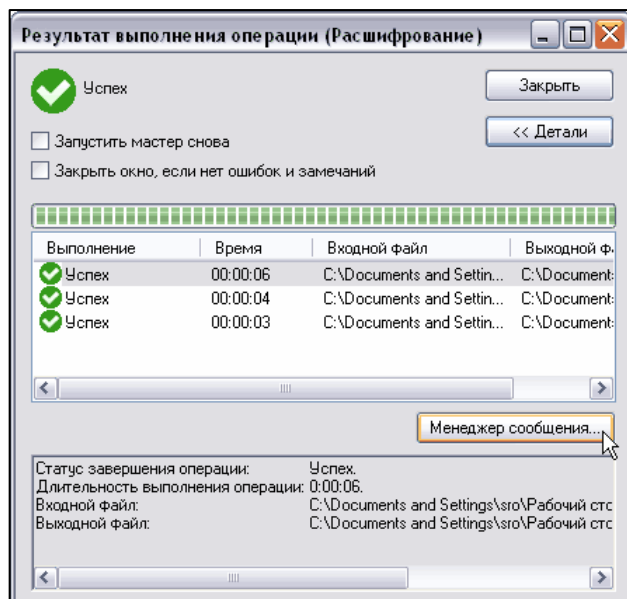
3. Выберите папку с файлами или отдельный файл, которые необходимо расшифровать (кнопки **Добавить папку** и **Добавить файл** соответственно)
4. В следующем окне выберите предпочтительный сертификат расширения (кнопка **Выбрать**). Вы можете просмотреть параметры и свойства выбранного сертификата, нажав на кнопку **Просмотреть**
5. После завершения сбора данных для расшифрования возникнет окно с информацией о статусе операции и об используемых параметрах. Для продолжения нажмите на кнопку **Готово**.
6. Начнется процесс расшифрования файла.



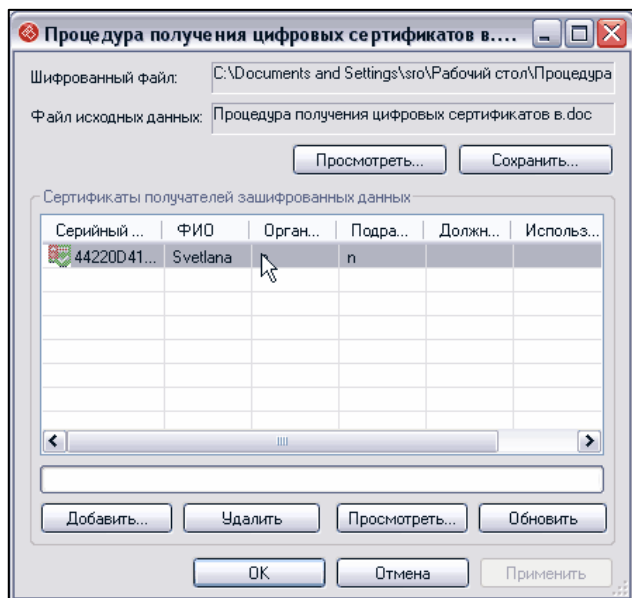
6. Данные будут расшифрованы и по умолчанию сохраняются в тот же каталог, в котором находится исходный (зашифрованный) файл

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 или перезапишите.

7. Если сертификат ГОСТ, введите пароль доступа к нему.
8. 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 >>**
9. 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**.
10. 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

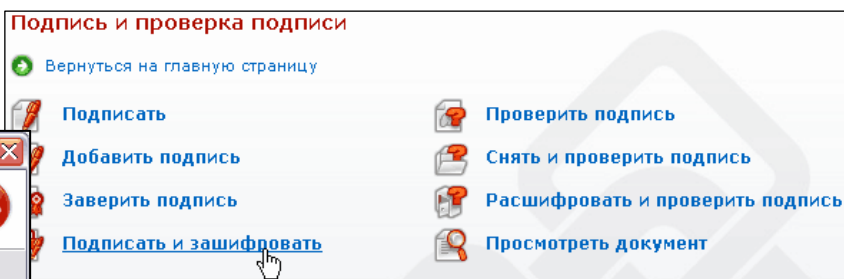
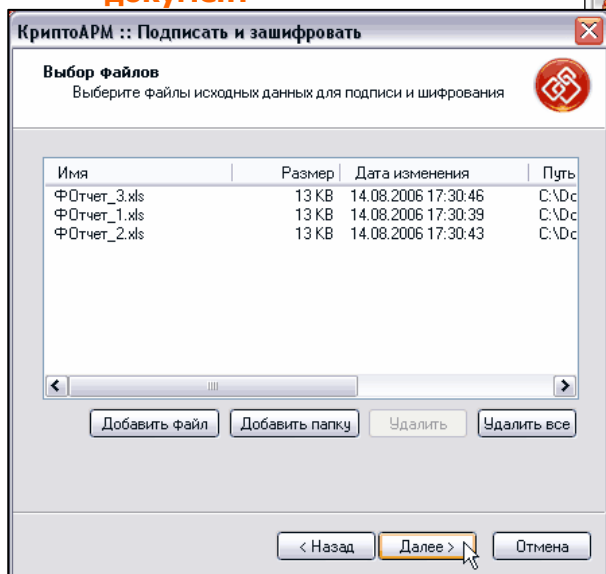
Вы можете расширить/сократить список сертификатов получателей файла (кнопки **Добавить** и **Удалить** соответственно). При нажатии на кнопку **Применить** или **ОК** данные будут повторно зашифрованы в адрес измененного списка получателей.

## Совмещенные операции

Программа «КриптоАРМ» дает возможность сократить время выполнения криптоопераций, то есть вы можете одновременно [шифровать и подписывать](#) документ или [расшифровывать и проверять его подписи](#).

Совмещенные операции не предполагают каких-либо дополнительных трудностей, даже, наоборот, ускоряют и упрощают процесс, экономя ваше время.

### Подписать и зашифровать документ



Для того чтобы подписать и зашифровать документ:

1. В главном окне откройте раздел **Подпись** или **Шифрование**.
2. Выберите пункт **Подписать и зашифровать...**
3. 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**. (Для создания настройки обратитесь к администратору.)

Далее следуйте рекомендациям Мастера выполнения операции

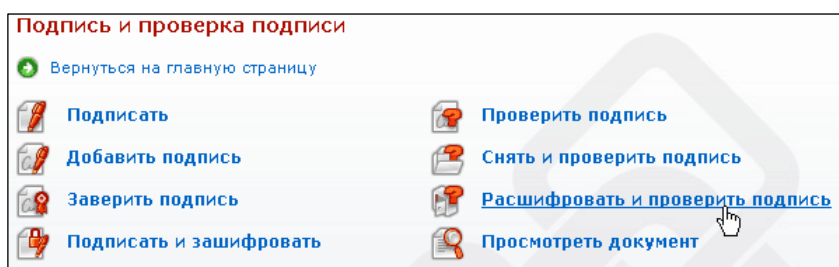
4. Выберите папку с файлами или отдельный файл, которые необходимо подписать и зашифровать (кнопки **Добавить папку** и **Добавить файл** соответственно)
5. Первым этапом следуйте Мастеру создания электронной подписи данных [Подписать электронный документ](#).
6. Вторым этапом следуйте Мастеру шифрования данных [Зашифровать файл](#).

**!** Мастера будут открываться автоматически в ходе операции. Вам не придется выбирать операции в главном окне программы.

## Расшифровать и проверить подпись

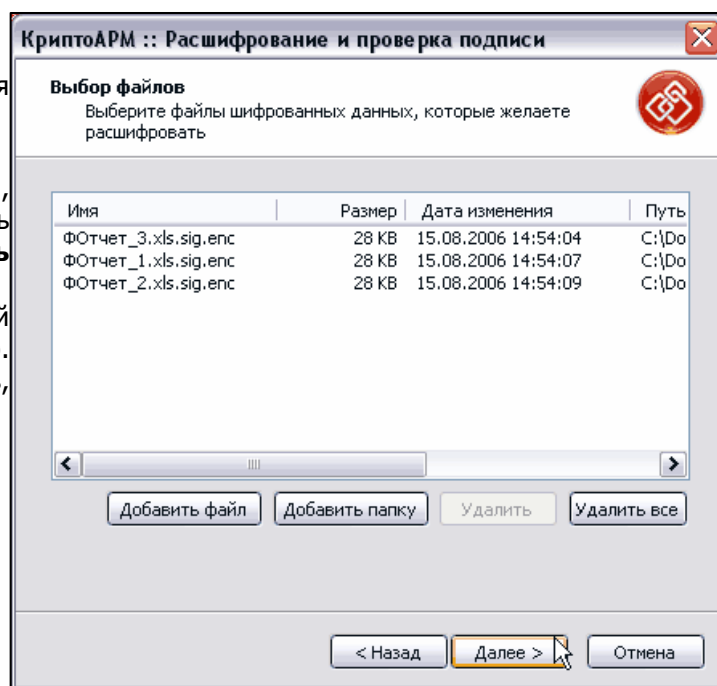
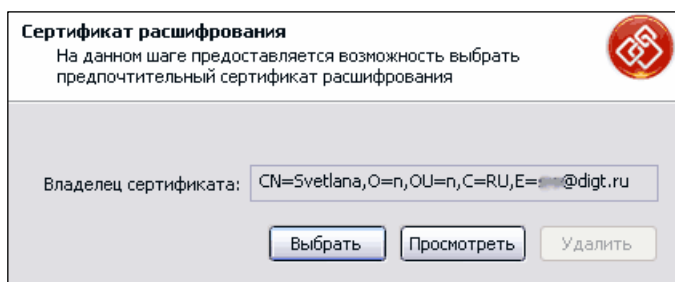
Для того чтобы подписать и зашифровать документ:

1. В главном окне откройте раздел **Подпись** или **Шифрование**.
2. Выберите пункт **Расшифровать и проверить подпись ...**
3. 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**. (Для создания настройки обратитесь к администратору.)



Далее следуйте рекомендациям Мастера выполнения операции

4. Выберите папку с файлами или отдельный файл, которые необходимо расшифровать и подписать которых нужно проверить (кнопки **Добавить папку** и **Добавить файл** соответственно)
5. В следующем окне выберите предпочтительный сертификат расширения (кнопка **Выбрать**). Указанный сертификат вы можете просмотреть, нажав на кнопку **Просмотреть**:



6. 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**. 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 ЭЦП и действительность сертификата отправителя.
7. 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 >>**

Чтобы просмотреть информацию о подписи и сертификате подписчика, обратитесь к пункту [Просмотр информации о подписи и сертификате](#).

## Часто задаваемые вопросы

В главе **Часто задаваемые вопросы** вы найдете информацию по следующим темам:

- Регистрация программы "КриптоАРМ"
- Использование программы "КриптоАРМ"
- Вопросы сотрудничества

### Регистрация программы «КриптоАРМ»

**Потребовалось заменить компьютер, на котором была установлена программа «КриптоАРМ». Поставили ограничение 30 дней. Работает нормально, но напоминает о сроке истечения временной лицензии. Можно ли сделать ее постоянной? Лицензия на 1 рабочее место куплена.**

Если вы удалили программу с компьютера, на котором она стояла, введите имеющуюся лицензию заново на новом рабочем месте.

### Использование программы «КриптоАРМ»

**Каков порядок действий при выходе из строя дискет, содержащих сертификат подписи или шифрования и ключевую пару сотрудников?**

Такие дискеты, как правило, восстановлению не подлежат (нет никакой гарантии, что при попытке восстановления не будет сбит хотя бы один бит информации). Если дубля дискеты (точнее, контейнера с ключами) не имеется, единственное решение - формировать новую ключевую пару и получать новый сертификат.

В последующем необходимо (и всегда рекомендуется!) иметь резервную копию ключевого носителя, что позволяет делать программа "КриптоАРМ", создавая резервную копию контейнера, и хранить копию в каком-либо надежном месте.

**Как я могу распространить свой сертификат среди коллег и партнеров?**

Распространить свой сертификат среди ваших коллег и партнеров вы можете, отправив и сертификат по электронной почте или передав на ключевом носителе. При передаче сертификата, обратите внимание, что вы передаете сертификат с открытым ключом. Закрытый ключ вы должны хранить в тайне (как вашу секретную информацию, которую никто не должен знать), в ином случае конфиденциальность будет утеряна.

**Сможет ли мой партнер прочитать зашифрованное сообщение, если у него не установлена программа «КриптоАРМ» или установлено любое другое ПО по шифрованию и подписи?**

Да, в случае, если шифрование производилось в его адрес (использовался его сертификат открытого ключа) и установлена программа, поддерживающая данный стандарт шифрования.

**Сможет ли мой партнер удостовериться в подлинности моей подписи, если у него не установлена программа «КриптоАРМ»?**

Это зависит от выбранного вами типа подписи. С документом, подписанным [отделенной электронной подписью](#) могут работать все пользователи, даже если на их компьютере не установлена программа «КриптоАРМ».

### Вопросы сотрудничества

## Программа "КриптоАРМ" - для использования учебными заведениями. Что требуется указать в гарантийном письме, для того чтобы использовать программу?

Если вы предполагаете использовать программу "КриптоАРМ Старт", то она действительно бесплатна и вы можете использовать ее без предоставления каких-либо гарантийных писем. Речь о гарантийном письме может идти тогда, когда вы решите использовать версию "КриптоАРМ Стандарт" или «КриптоАРМ СтандартPRO» для работы с сертифицированными криптопровайдерами. (Версия "Старт" поддерживает работу только со стандартными Windows криптопровайдерами).

## Перечень сокращений

Microsoft CA	Microsoft Certification Authority (Удостоверяющий центр от компании Microsoft)
PKC	Сертификат открытого ключа (Public Key Certificate)
PKI	Public Key Infrastructure (Аналог ИОК)
TSA	Time Stamping Authority (Служба штампов времени)
TSP	Доверенная Служба (Trusted Service Provider)
ИОК	Инфраструктура Открытых Ключей (PKI)
ОС	Операционная система
ПО	Программное обеспечение
ПК	Персональный компьютер
СКЗИ	Средство криптографической защиты информации
СООС	Список отзыва сертификатов (Certificate Revocation List)
УЦ	Удостоверяющий центр
ЦС	Центр Сертификации (CA)

## Техническая поддержка

В случае если у Вас возникли вопросы по использованию программы «КриптоАРМ», обратитесь к системному администратору вашей организации.

По вопросам технической поддержки программы "КриптоАРМ", ваш системный администратор может обратиться к нам:

На форум: <http://www.trusted.ru/support> или через программу "КриптоАРМ" (**Помощь** - > **О программе** - > **Поддержка**.)

По электронной почте: [support@trusted.ru](mailto:support@trusted.ru)

По телефонам:

- (8362) 55-62-81,
- (8362) 55-62-27,

По адресу: Россия, Республика Марий Эл, г. Йошкар-Ола, ул. Фестивальная, д.73.

## Зарегистрировать программу

"КриптоАРМ Старт" не требует регистрации и не ограничена временем ее использования.

"КриптоАРМ Стандарт" и "КриптоАРМ СтандартPRO" требуют ввода лицензионного ключа.

*"могут ли с одного компьютера работать несколько пользователей, используя одну лицензию?.."*

Чтобы использовать КриптоАРМ на одном компьютере несколькими пользователями достаточно одной лицензии.

"...я постоянно меняю стационарный компьютер и ноутбук. Можно ли обойтись одной лицензией или необходимо иметь две?"

В случае работы одного пользователя на нескольких компьютерах требуется по одной лицензии на каждое рабочее место.

Период работы с программой зависит от типа используемой лицензии:

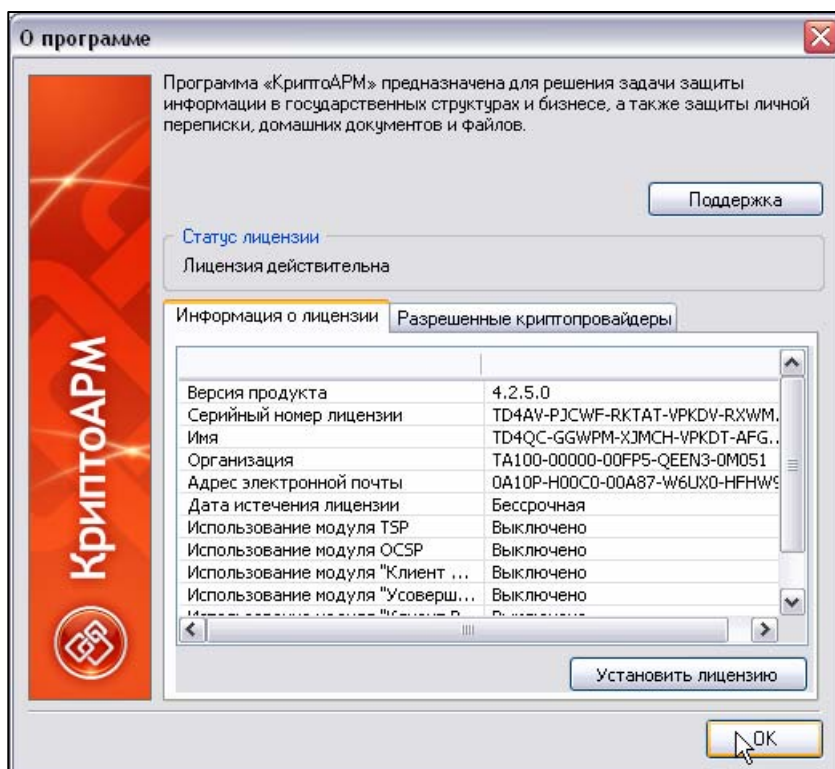
- **временная лицензия**
  - предоставляется для тестирования программы на срок до 1 месяца
  - по истечении тестового периода программа переходит в режим **"КриптоАРМ Старт"**
  - получить временную лицензию можно по адресу [support@trusted.ru](mailto:support@trusted.ru)
- **постоянная лицензия** (для работы с полнофункциональной версией программы без ограничения срока действия ПО).

**!** Регистрация продукта должна осуществляться пользователем, имеющим права администратора системы. Поэтому вам следует обратиться к системному администратору организации.

### Посмотреть статус лицензии

1. В главном окне программы выберите меню **Помощь**
2. В выпадающем списке выберите **О программе - > Статус лицензии**

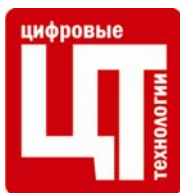
**!** Обратите внимание на графу **Статус лицензии**: лицензия должна быть действительна



В закладке **Информация о лицензии** отображается информация в соответствии с используемой лицензией на программный продукт "КриптоАРМ":

- версия продукта
- серийный номер лицензии
- имя пользователя программы
- организация, в которой работает пользователь
- адрес электронной почты пользователя
- использование дополнительных модулей
- другие

## О компании «Цифровые технологии»



Компания «Цифровые технологии» — российский поставщик программных продуктов, решений и комплексов в области криптографической защиты информации.

Свою цель мы видим в том, чтобы предоставить клиентам возможность выбирать для себя оптимальные программные решения — будь то отдельная программа по шифрованию файлов или комплексное решение по организации конфиденциального документооборота на предприятии.

Чтобы обеспечить эту возможность, мы предлагаем достаточно широкий круг продуктов в области информационной защиты (шифрование, электронная цифровая подпись, аутентификация, защита каналов связи и др.) В списке поставляемых нами решений - как собственные программные продукты, так и продукты наших официальных партнеров - компаний Крипто-Про, Сигнал-КОМ, Aladdin и Актив.

### Лицензии

Компания «Цифровые технологии» имеет [лицензии ФСБ](#) (от 17 апреля 2008 года) на проектирование, производство, распространение и обслуживание сертифицированных шифровальных средств информационных систем, систем и комплексов телекоммуникации, не связанных с обработкой сведений, составляющих государственную тайну.