ЮЗЭДО для пользователей

1. ОБЩИЕ ПОЛОЖЕНИЯ

Организация, имеющая сложную интегрированную, территориально-распределенную структуру, сталкивается с такими информационными проблемами, как разрозненность финансовой и управленческой информации; запаздывание поступающих из отдаленных филиалов данных с вытекающими затруднениями в принятии оперативных решений; несбалансированность информационных потоков.

В условиях территориально-распределенной структуры возникают сложные схемы организации документооборота между юридическими лицами одной организации, удаленными подразделениями одного юридического лица, центральной компании и ее филиалами и дочерними компаниями.

Основными узкими местами в документообороте между удаленными структурными единицами являются: многократная регистрация одного документа; утрата документов; невозможность осуществления контроля за исполнением документов и сроков их согласования и подписания; отсутствие единого полного реестра изданных и полученных документов с целью осуществления их оперативного поиска и сбора статистических данных; многократное копирование одного документа с целью его рассылки удаленным адресатам организации; длительные сроки согласования проектов документов и принятия управленческих решений.

Предлагаемое решение по организации юридически значимого защищенного документооборота (ЮЗЭДО) направлено на решение перечисленных проблем. В системе обмена юридически значимыми документами по телекоммуникационным каналам связи для передачи сообщений между абонентами используется открытая телекоммуникационная сеть – Интернет. Доступ к данным, проходящим через Интернет, не может быть физически ограничен. С другой стороны, информация, которой обмениваются абоненты, является конфиденциальной, составляет налоговую или коммерческую тайну. Таким образом, остро встает вопрос защиты этой информации от несанкционированного доступа третьих лиц.

Для комплексного решения задачи организации защищенного обмена юридически значимыми электронными документами между абонентами предлагаемого решения разработано решение организации юридически значимого документооборота в электронном виде по телекоммуникационным каналам связи, который обеспечивает требуемый уровень защиты информации, работая в правовом поле России.

ЮЗЭДО регулирует взаимоотношения коммерческих организаций при условии, что эти организации заранее не имеют предпосылок к тому, чтобы доверять друг другу «на слово», и любой результат их взаимодействия документируется с целью иметь в будущем доказательную базу для того, чтобы иметь возможность отстоять как свои права, так и обязанности противоположной стороны. Подобные взаимоотношения организаций предоставляют широкую сферу для применения ЭЦП в качестве аналога собственноручной подписи.

Все электронные документы, циркулирующие между организациями, требуют юридической значимости для того, чтобы каждая из сторон была уверена в исполнении другой стороной своих обязательств. Юридически значимый электронный документ – это электронный документ, обладающий такими свойствами, что права и обязательства каждой из сторон, вытекающие из этого электронного документа, защищены действующим законодательством, в нашем случае, законодательством РФ. Юридическую значимость электронного документа обеспечивается с помощью ЭЦП.

2. ИСПОЛЬЗУЕМЫЕ ТЕХНОЛОГИИ И ПРОГРАММНЫЕ СРЕДСТВА

Решение ЮЗЭДО строится на основе применения систем цифровой подписи - защиты участников информационного обмена от навязывания ложной информации, установления факта модификации информации, которая передается или сохраняется, и получения гарантии ее подлинности, а также решение вопроса об авторстве сообщений. Технология цифровой подписи предполагает, что каждый пользователь сети имеет свой секретный ключ, который используется для формирования подписи, а также соответствующий этому секретному ключу открытый ключ, известный некоторому кругу пользователей сети и предназначенный для проверки подписи. Цифровая подпись вычисляется на основе секретного ключа отправителя информации и собственно информационных бит документа (файла).

Один из пользователей может быть избран в качестве «нотариуса» и заверять с помощью своего секретного ключа любые документы. Остальные пользователи могут провести верификацию его подписи, то есть убедиться в подлинности полученного документа. Способ вычисления цифровой подписи таков, что знание открытого ключа не может привести к подделке подписи. Проверить подпись может любой пользователь, имеющий открытый ключ, в том числе независимый арбитр, который уполномочен решать возможные споры об авторстве сообщения (документа).

В качестве средства электронной цифровой подписи, обеспечивающего реализацию функций создания электронной цифровой подписи в электронном документе с использованием закрытого ключа электронной цифровой подписи, подтверждения с использованием открытого ключа электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе, создания закрытых и открытых ключей электронных цифровых подписей, используются продукты: «КриптоАРМ стандарт», СКЗИ КриптоПро CSP, отчуждаемый носитель либо комплекты «КриптоТри» или «eToken КриптоАРМ».

Пользователи ЮЗЭДО должны обеспечить сохранность в тайне закрытых ключей электронных цифровых подписей.

3. НЕОБХОДИМОСТЬ ПРИМЕНЕНИЯ СЕРТИФИЦИРОВАННЫХ СРЕДСТВ ОБЕСПЕЧЕНИЯ ЭЦП

Простой анализ информационных рисков, которые возникают при использовании не сертифицированных средств криптографической защиты информации (к которым, безусловно, относятся средства электронной цифровой подписи) без каких-либо оговорок, уже дает достаточно оснований сделать выбор в пользу применения сертифицированных систем защиты информации и средств для работы с ЭЦП.

Собственно риск фальсификации электронной подписи едва ли можно считать значительным. Во-первых, большинство не сертифицированных средств ЭЦП используются уже довольно давно и на практике доказали свою надежность; во-вторых, даже для того, чтобы фальсифицировать подпись, которая накладывается с помощью любого несовершенного алгоритма, могут понадобиться довольно значительные затраты. Между тем есть менее затратные способы компрометации системы, чем попытки прямого взлома.

Первый риск состоит в том, что участник системы документооборота может, ссылаясь на то, что средства ЭЦП не сертифицированы (а значит, не имеют гарантий криптографической стойкости), заявить, что его подпись была подделана, и отозвать, таким образом, электронный документ со своей подписью. Отметим, что для этого совсем не нужно, чтобы подделка действительно имела место. Виртуальный, по большому счету, риск фальсификации ЭЦП порождает абсолютно реальный риск отказа от ЭЦП.

С этой проблемой в системах документооборота, которые используют не сертифицированные средства, справляются единственным образом: подписывая дополнительные соглашения между участниками документооборота, в которых стороны

признают данное средство ЭЦП достаточным для обеспечения юридической силы подписанных ЭЦП документов. Подписывая такое соглашение, участники документооборота фактически признают, что данное средство ЭЦП обеспечивает высокий уровень криптостойкости, подпись не может быть подделана, а потому они добровольно отказываются от возможности предоставить рекламацию в связи с фальсификацией подписи. Проблема в том, что подписание такого соглашения требует достаточной смелости - ведь рядовой участник документооборота едва ли способен самостоятельно провести экспертизу и убедиться в истинности того утверждения, под которым он подписывается.

Другой риск, который связан с возможностью отказаться от авторства подписанного документа, еще более серьезный. Дело в том, что не сертифицированное средство ЭЦП никто не проверял, во-первых, с точки зрения качества выполнения основной функции (и на этом основан описанный выше риск), а во-вторых, с точки зрения отсутствия побочных действий. Автор заверенного ЭЦП электронного документа может в принципе попробовать отказаться от содержания этого документа, утверждая, что средство ЭЦП неадекватно преобразовало предложенный ему файл: не только поставило ЭЦП, но и «случайно» что-то еще изменило в файле в силу ошибки в программе. Скорее всего, это утверждение ошибочно. Маловероятно, чтобы испытанное на практике средство ЭЦП действительно дало такой сбой. Риск неадекватного преобразования входного файла - чисто виртуальный. В то же время, основанный на нем риск отказа от содержания файла целиком реальный. Автор утверждает, что программа дала сбой и на выходе получен правильно заверенный ЭЦП файл, отличный от того, которое было передано программе на вход.

Использование сертифицированных средств криптографической защиты информации гарантом качества выполнения основной функции и отсутствия побочного действия заложено в основу предлагаемого решения ЮЗЭДО разработчиками. А при использовании не сертифицированных средств криптографической защиты информации таких гарантий не может дать никто.

4. СООТВЕТСТВИЕ ПРИМЕНЯЕМЫХ РЕШЕНИЙ РОССИЙСКОМУ ЗАКОНОДАТЕЛЬСТВУ

Предлагаемая схема юридически значимого электронного документооборота на базе продуктов «КриптоТри» и «e-tokenКриптоАРМ» для организации внутрикорпоративного документооборота и обмена документами между юридическими лицами по открытым каналам связи соответствует базовым нормам российского законодательства, и основывается на следующих законодательных актах:

1. Федеральном законе «Об информации, информатизации и защите информации» от 20 февраля 1995 г. №24-ФЗ (устанавливающего возможность использования электронного документа и электронной цифровой подписи);
2. Гражданском кодексе РФ, предусматривающем возможность заключения договора путем обмена документами посредством «…телеграфной, телетайпной, электронной и иной связи» (п.2 ст.234), а также «использования электронной подписи либо иного аналога собственноручной подписи в случаях и порядке, предусмотренных законодательными актами или соглашением сторон» (ч.2 ст.160);
3. Федеральном законе «Об электронной цифровой подписи» от 10 января 2002 г.№1-ФЗ, определяющем условия признания равнозначности электронной цифровой подписи и собственноручной подписи (п.1 ст.4), а также регламентирующем применение при совершении сделок электронной цифровой подписи (ЭЦП) и сертификатов ключей ЭЦП, выпускаемых удостоверяющими центрами.
4. Арбитражном процессуальном кодексе РФ, устанавливающем, что документы, полученные посредством электронной связи, а также документы, подписанные электронной цифровой подписью, допускаются в качестве письменных доказательств в случаях и в порядке, которые установлены федеральным законом, иным нормативным

правовым актом или договором (ч.3 ст.75), а также что письменные доказательства предоставляются в арбитражный суд в подлиннике или в форме надлежащим образом заверенной копии (ч.8 ст.75).

5. Гражданском процессуальном кодексе РФ, который признает письменными доказательствами содержащие сведения об обстоятельствах, имеющих значение для рассмотрения и разрешения дела, акты, договоры, справки, деловую корреспонденцию, иные документы и материалы, выполненные в форме цифровой, графической записи, в том числе полученные посредством факсимильной, электронной или другой связи, либо позволяющим установить достоверность документа (п.1 ст.71).

6. РОЛЬ УДОСТОВЕРЯЮЩИХ ЦЕНТРОВ В РЕШЕНИИ ЮЗЭДО

Для обеспечения целостности и конфиденциальности, а также защиты от подделки электронных документов участники документооборота должны использовать средства криптографической защиты информации, в том числе – электронную цифровую подпись. Для создания правовых взаимоотношений между участниками, они должны присоединиться к регламенту ЮЗЭДО, путем заключения Договора присоединения (публичная оферта) на предлагаемых организатором ЮЗЭДО условиях. Организатором ЮЗЭДО в рассматриваемой схеме является Удостоверяющий центр.

В Удостоверяющем центре должен быть зарегистрирован список объектных идентификаторов (OID) системы документооборота. Объектные идентификаторы определяют отношения, при осуществлении которых документ с электронной цифровой подписью будет иметь юридическое значение.

Остальные объектные идентификаторы включаются в издаваемый сертификат на основании Заявления на изготовление сертификата ключа подписи.

Идентификаторы вносятся в сертификаты публичного ключа клиентов документооборота и позволяют контролировать полномочия пользователей на совершение операций с документами в конкретной системе документооборота.

При заключении договора присоединения к настоящим правилам организатор ЮЗЭДО предоставляет Участнику право на приобретение и использование программного обеспечения ЮЗЭДО следующими способами: осуществление с использованием данного программного обеспечения приема, обработки и передачи электронных документов между участниками ЮЗЭДО. Участник имеет право самостоятельно устанавливать программное обеспечение ЮЗЭДО на соответствующем оборудовании в требуемой программной среде.

Удостоверяющим центром, выдающим сертификаты ключей подписей для использования в ЮЗЭДО, являются все Удостоверяющие центры, осуществляющие свою деятельность в рамках российского законодательства и на основании федеральных законов об ЭЦП.

При организации и функционировании ЮЗЭДО принимаются и признаются сертификаты ключей подписей, изданные Удостоверяющими центрами, в составе и формате, определяемом Удостоверяющими центрами.

Сертификат ключа подписи признается изданным Удостоверяющим центром, если подтверждена подлинность электронной цифровой подписи уполномоченного лица Удостоверяющего центра с использованием средства электронной цифровой подписи и сертификата ключа подписи уполномоченного лица Удостоверяющего центра.

Должность сотрудника организации, которому выдается сертификат ключа подписи, должна соответствовать уровню принимаемых решений.

Идентификационные данные, занесенные в поле «Субъект» (Subject Name) сертификата ключа подписи однозначно идентифицируют владельца сертификата ключа подписи и соответствуют идентификационным данным владельца сертификата ключа подписи.

Для определения статуса сертификата ключа подписи, получения актуального списка отозванных сертификатов, актуальных сертификатов уполномоченных лиц УЦ участниками ЮЗЭДО используется специализированное ПО «КриптоАРМ».

7. ОРГАНИЗАЦИОННО-СТРУКТУРНЫЕ СХЕМЫ ЮЗЭДО

Для защиты от рассмотренных угроз компания «Цифровые технологии» совместно с партнером – компанией «Актив» и компанией «Aladdin» предлагает комплексное организационно-техническое решение по созданию защищённого юридически значимого электронного документооборота.

1.1. ДЕЙСТВИЯ ОРГАНИЗАТОРА ДОКУМЕНТООБОРОТА

На основе аппаратно-программного комплекса «КриптоТри» или «eToken КриптоАРМ» возможна организация ЮЗЭДО без необходимости развертывания сложной системы электронного документооборота.

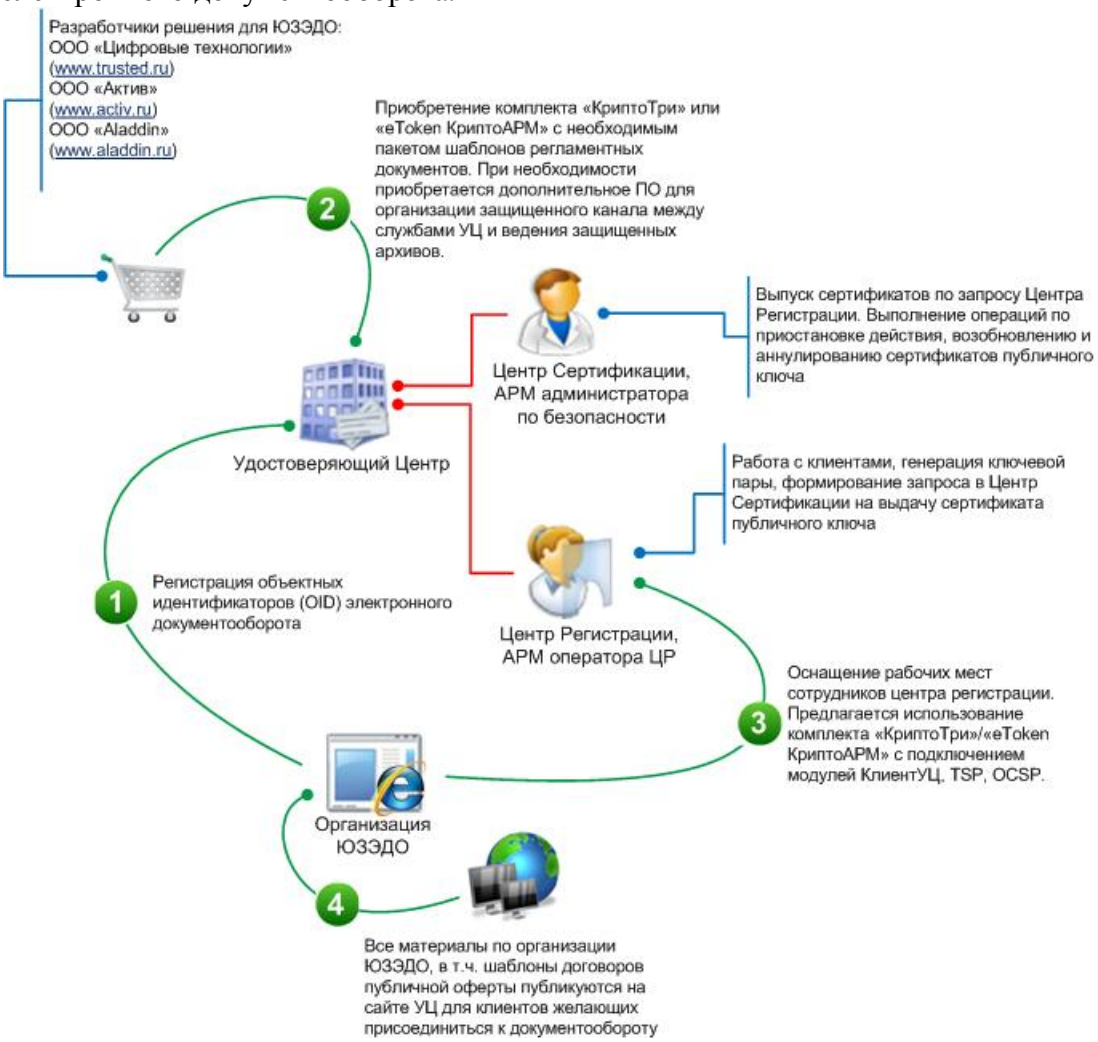

Рис.1. Действия УЦ при организации ЮЗЭДО
(владельцем документооборота является сам удостоверяющий центр)

1 Организаторам (владельцам) схемы документооборота необходимо зарегистрировать список объектных идентификаторов (OID) системы документооборота. Объектные идентификаторы определяют отношения, при осуществлении которых документ с электронной цифровой подписью будет иметь юридическое значение, если он был создан внутри конкретной системы документооборота.

Идентификаторы вносятся в сертификаты публичного ключа клиентов документооборота и позволяют контролировать полномочия пользователей на

совершение операций с документами в конкретной системе документооборота. OID зарегистрированные в Удостоверяющем центре включаются состав следующих расширений сертификата ключа подписи: Key Usage (использование ключа), Extended Key Usage (расширенное использование ключа), Application Policy (политики применения сертификата).

Остальные идентификаторы используются по усмотрению организаторов документооборота как расширения объектного идентификатора самой системы.

2 Организаторам документооборота можно использовать уже готовые решения, предлагаемые компаниями «Цифровые технологии», «Актив», «Aladdin» в части приобретения необходимого специализированного программного обеспечения и шаблонов организационно-нормативных документов. Заинтересованному в организации ЮЗЭДО лицу необходимо адекватно оценить требуемую сложность системы документооборота с точки зрения технической реализации. Для этого требуется «проработать» следующие направления:

- Размер организации. Общее число сотрудников. Число пользователей системы.
- Организационная структура предприятия. Модель компетенций в системе документооборота. Модель принятия решений.
- Процессная модель организации. Какие системы управления развиты, то есть, какие области документооборота будут представлены в решении.
- Проработанность правил документооборота, классификация документов, форм документов, процедур работы с документами.
- Информационная инфраструктура. Вся совокупность программного обеспечения, используемого в организации.
- Техническое обеспечение системы.
- Каналы связи.
- Число бизнес - процессов – насколько они сложны, детально проработаны, регламентированы.
- Функции, которые документ выполняет в организации.
- Требования безопасности.

3 Центр Регистрации при УЦ должен обеспечивать принятие, предварительную обработку внешних запросов на создание сертификатов или на изменение статуса уже действующих сертификатов. Центр Регистрации может быть территориально удаленным образованием, который должен использовать специализированное ПО чтобы обеспечить:

1. Разграничение доступа к элементам управления ЦР на основе состава представленного Администратором взаимодействия с пользователем собственного электронного сертификата, определяющего ролевую принадлежность администратора и уровня полномочий.
2. Получение и обработку запроса от Администраторов взаимодействия с пользователями на выпуск сертификата или изменение статуса уже выпущенного сертификата с последующей передачей запроса в ЦС.
3. Хранение заверенных запросов и журналов событий в течение установленного срока, предусмотренного регламентом работы системы, в составе которой функционирует УЦ.
4. Резервное копирование на внешние носители локального архива.

Под реализацию данных функциональных возможностей разрабатывался модуль КлиентУЦ в составе ПО «КриптоТри» или «eToken КриптоАРМ». Данный модуль позволяет задавать шаблон атрибутов и расширений с предустановленными значениями, используемый в Мастере создания запроса на сертификат. Для использования защищенного канала между удаленным центром регистрации и центром сертификации можно установить ПО Trusted TLS.

4. Все материалы, которые необходимы клиентам организуемого документооборота, должны быть опубликованы на web-портале удостоверяющего центра для оказания информационной поддержки пользователей документооборота. Среди материалов описывающих принятую схему документооборота, определение основных типов операций, порядка решения конфликтных ситуаций и т.п., требуется предоставить для ознакомления потенциальным пользователям системы шаблон договора для присоединения к существующей системе документооборота.

1.2. ДЕЙСТВИЯ ПОЛЬЗОВАТЕЛЕЙ СИСТЕМЫ ДОКУМЕНТООБОРОТА

1. Пользователям, желающим присоединиться к существующему документообороту, требуется скачать с web-портала организатора всю необходимую документацию. В составе документации должен быть шаблон договора, форма, необходимая для получения сертификата в ЦР (первичная сертификация) и инструкции по оснащению рабочего места пользователя.
2. С сайта производителей пользователям необходимо скачать и установить дистрибутив продукта «КриптоТри». Основными преимуществами данного продукта для пользователей являются:
   - Стоимость комплекта продуктов под единой маркой «Крипто 3» («eToken КриптоАРМ») существенно ниже суммы, затрачиваемой при покупке этих же продуктов по отдельности;
   - Сокращение времени на саму процедуру покупки: купить комплексный продукт «Крипто 3» у одного поставщика быстрее и проще, чем обращаться к разным компаниям за каждым продуктом по отдельности;
   - Все программное обеспечение собрано в единый дистрибутивный файл. Установка производится «одним кликом мыши». При установке выполняются необходимые операции по настройке программных модулей.
   - Работа с сертифицированными криптографическими алгоритмами;
   - Соответствие требованиям Федерального Закона РФ № 1-ФЗ от 10.01.2002 «Об электронной цифровой подписи»;
   - Поддержка международных стандартов и рекомендаций в области защиты информации (X.509, PKCS, CMS);
   - Ключевая информация в защищённой памяти Rutoken остается в безопасности даже в случае утери USB-токена;
   - В стандартную поставку «Крипто 3» входят шаблоны документов (регламентов), позволяющие заказчику самостоятельно сформировать полный пакет документации, необходимой для установления юридически значимого электронного документооборота;
   - Имеется положительное заключение ЦБС ФСБ России о корректности встраивания КриптоПро CSP в КриптоАРМ.
3. Следует отметить, что в зависимости от принятой схемы хождения документа, многим участникам в организуемой системе документооборота изначально не требуется совершать операции по созданию ЭЦП над документами и их шифрования. Большинство заинтересованы в выполнении операции проверки ЭЦП присланных документов и в случае успешного ее завершения – сохранения документов в файловой системе. По этой причине, программные компоненты в составе дистрибутива «КриптоТри», которые обеспечивают выполнение операций с ЭЦП можно установить без ввода лицензии, т.е. совершенно бесплатно. В этом случае пользователь получает на своем рабочем месте набор ПО с ограниченным функционалом, но позволяющим выполнять функцию получателя пакетов подписанных электронных документов.
4. Для обеспечения возможности формирования ЭЦП пользователю требуется иметь закрытый ключ и соответствующий ему сертификат открытого ключа подписи. Для

прохождения процедуры первоначальной сертификации ему следует обратиться в удостоверяющий центр, в котором будут пройдены следующие этапы:

1. Формирование закрытого ключа. Сгенерированный закрытый ключ должен помещаться на отчуждаемый носитель (токен). Ключевой контейнер на токене защищается путем задания пин-кода, что позволяет усилить безопасность его хранения и транспортировки, а также обеспечить юридическую значимость использования закрытого ключа.
2. Создание запроса на сертификат. Дополнительно к стандартным атрибутам имени владельца (таким как, CN, E, C, O, OU и др.) будет добавлен атрибут «UnstructuredName», содержащий ИНН и КПП организации. Объектный идентификатор данного атрибута равен «1.2.840.113549.1.9.2», значение атрибута имеет следующий формат: «ИНН:nnnnnnnnnnnn, КПП:nnnnn», где n – цифра. В расширении «Улучшенный ключ» (OID 2.5.29.37) запроса на сертификат будут помещены следующие объектные идентификаторы:
   - проверка подлинности TLS-клиента (OID 1.3.6.1.5.5.7.3.2);
   - защищенная электронная почта (OID 1.3.6.1.5.5.7.3.4);
   - объектные идентификаторы ветки Ассоциации Электронных Торговых Площадок (1.2.643.6.3.*).

5 Выпуск сертификата. Он производится посредством обработки запроса на сертификат, полученного в предыдущем пункте. После генерации сертификата сотрудник УЦ записывает пользователю на токен следующие данные:

- клиентский сертификат, изданный для пользователя данным УЦ;
- корневой сертификат данного УЦ;
- сертификат Уполномоченного лица УЦ или владельца документооборота, которым подписываются Доверительные списки сертификатов (CTL).

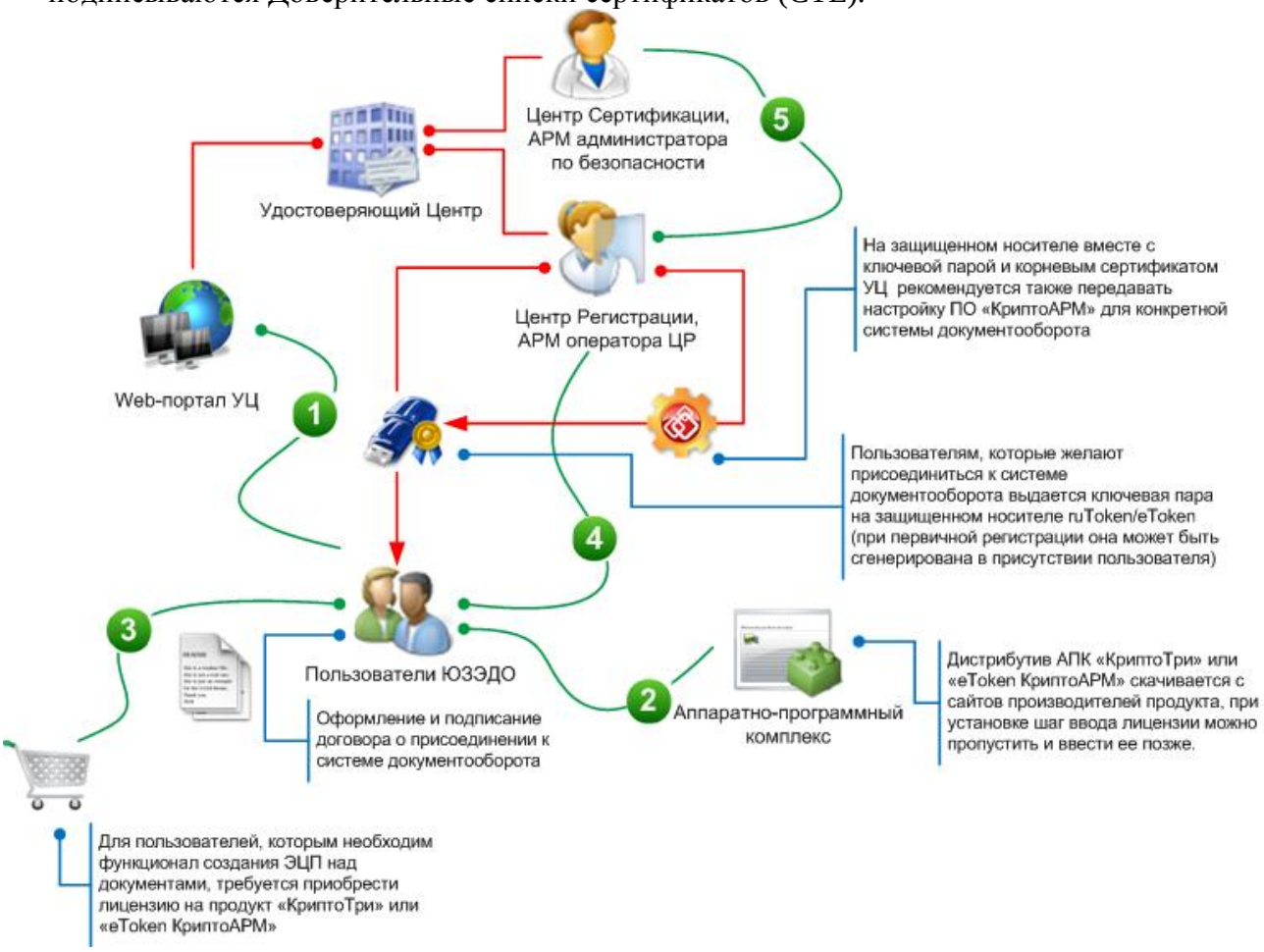

Рис. 2. Действия клиента УЦ для присоединения к ЮЗЭДО и организации рабочего места

Также на защищенный носитель может помещаться настройка для ПО «КриптоАРМ», которую не рекомендуется распространять по незащищенным каналам - это позволят значительно упростить первоначальную инициализацию программного комплекса на рабочем месте пользователя. Для этого пользователь импортирует настройку в приложение «КриптоАРМ», которая имеет все необходимые параметры для осуществления документооборота.

8. ТИПОВЫЕ ДОКУМЕНТЫ, ЦИРКУЛИРУЮЩИЕ В ЮЗЭДО

Перечень электронных документов, которые могут быть подписаны электронной цифровой подписью и в которых электронная цифровая подпись признается равнозначной собственноручной в случае выполнения всех условий равнозначности электронной цифровой подписи собственноручной, определяется и утверждается организатором (владельцем) ЮЗЭДО.

Электронная цифровая подпись документа хранится отдельно от электронного документа. Формат электронной цифровой подписи определяется рекомендациями RFC 3852 «Cryptographic Message Syntax (CMS)», с учетом использования криптографических алгоритмов ГОСТ 28147-89, ГОСТ Р 34.10-94, ГОСТ Р 34.10-2001, ГОСТ Р 34.11-94 в соответствии с RFC 4490 «Using the GOST 28147-89, GOST R 34.11-94, GOST R 34.10-94, and GOST R 34.10-2001 Algorithms with Cryptographic Message Syntax (CMS)».

В рамках данного решения предлагается работа со следующими видами документов:

1. **Договоры** - в соответствии с Гражданским кодексом счет, содержащий все условия договора, является офертой, поскольку удовлетворяет всем признакам, установленным ст.435 ГК РФ: счет является адресованным одному или нескольким конкретным лицам предложением, которое достаточно определенно и выражает намерение лица, сделавшего предложение, считать себя заключившим договор с адресатом, которым будет принято предложение. Если лицо, получившее оферту, совершает действия по выполнению условий договора, указанных в этой оферте (отгружает товар, предоставляет услугу, выполняет работу, уплачивает денежную сумму и т.п.), то такие действия считаются акцептом (ст.438 ГК РФ).
   Принятие оферты (ее акцепт) создает договор и порождает обязанность его исполнения. А в силу упомянутой ст.434 ГК, обмен документами, порождающими договор, может быть совершен в различных формах, в том числе и в электронной форме.
2. **Накладные (ТН, ТТН) и унифицированные акты** - накладная является первичным бухгалтерским документом, оформляющим передвижение товарно-материальных ценностей. Применяемые формы накладных должны соответствовать альбомам унифицированных форм Госкомстата. Так, для внутреннего перемещения ценностей применяется форма М-11, при отпуске сторонним организациям форма М-15, для учета в организациях торговли форма ТОРГ-12 и т.д. При этом накладные, чьи унифицированные формы не предусматривают наложение печати (это прежде всего касается накладных на перемещение ценностей в пределах одной организации) могут быть созданы в электронном виде при условии их подписания с помощью ЭЦП.
3. **Неунифицированные акты** - гражданское законодательство относит работы и услуги к объектам гражданских прав, но, в отличие от имущества и имущественных прав, после выполнения работ или оказания услуг потребляется их результат. Услуга отличается от работы прежде всего тем, что результат выполнения работ имеет материальное выражение, поэтому исполнителю работ есть что передавать.
   Результат оказания услуг, как правило, не имеет материального выражения, поскольку услуга потребляется в процессе ее оказания. Поэтому оказание услуг невозможно

оформить накладной или актом сдачи-приемки работ. Стороны могут составить акт оказания услуг, который лишь подтвердит, что услуга фактически оказана. На сегодняшний день унифицированная форма акта об оказании услуг не утверждена.

Исполнитель в одностороннем порядке подтверждает факт оказания услуг. При этом способ подтверждения может быть различным. Например, исполнитель после оказания услуг может направить отчет или справку оговоренной сторонами формы. В ряде случаев могут существовать иные материальные доказательства оказания услуг (например, по договору о размещении рекламы - экземпляр печатного издания или эфирная справка). Организация - заказчик в рамках учетной политики утверждает форму первичного документа, и, на основании подтверждения исполнителя, в одностороннем порядке составляет такой документ. Составление возможно в электронной форме с применением ЭЦП.

В свою очередь, исполнитель не должен требовать обязательного подписания заказчиком акта, по форме исполнителя. Вместо этого заказчик может сделать отметку в произвольной форме (например, на возвратном экземпляре отчета исполнителя), либо дать иное подтверждение факта оказания услуг в любой форме (например, электронной), позволяющей достоверно установить, что документ исходит от него. В случае, если это предусмотрено договором, подтверждением может считаться отсутствие письменных мотивированных возражений заказчика в какой-либо конкретно оговоренный срок (например, в месячный срок с момента отправки заказного письма с отчетом исполнителя). Получив от заказчика подтверждение (или удостоверившись в отсутствии претензий), исполнитель самостоятельно составляет первичный документ по форме, утвержденной в своей учетной политике. Такой документ может быть составлен в электронной форме и быть подписан с помощью ЭЦП.

При обмене указанными видами документов между участниками сервиса не вводится ограничений на их форматы. Сервис и клиентское программное обеспечивает работу на уровне файлов или архивов для передачи по каналам связи.

9. ПОРЯДОК ФОРМИРОВАНИЯ И ПРОВЕРКИ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

Формирование электронной цифровой подписи электронного документа осуществляется с использованием применяемого средства электронной цифровой подписи и программного обеспечения ЮЗЭДО.

Формирование электронной цифровой подписи может быть осуществлено только владельцем сертификата ключа подписи, соответствующий закрытый ключ которого действует на момент формирования электронной цифровой подписи.

Подтверждение подлинности электронной цифровой подписи электронного документа осуществляется с использованием применяемого средства электронной цифровой подписи и программного обеспечения ЮЗЭДО.

Подтверждение подлинности электронной цифровой подписи может быть осуществлено пользователями сертификатов ключей подписей. Пользователь сертификата ключа подписи с использованием применяемых средств подтверждения подлинности электронной цифровой подписи должен удостовериться, что электронная цифровая подпись в электронном документе равнозначна собственноручной, и только после признания электронной цифровой подписи равнозначной собственноручной обеспечить исполнение данного электронного документа.

Юридически значимый электронный документооборот включает в себя следующие этапы формирования и проверки документов:

1. Формирование электронных документов;
   - Электронный документ формируется в установленном Организатором ЮЗЭДО для данного электронного документа формате.

- Подлинником электронного документа считается документ с воспроизведенным содержанием и электронно-цифровой подписью.

2. Подписание ЭЦП и шифрование электронных документов с помощью комплекта («КриптоТри» или «e-token КриптоАРМ»);
   - • Электронный документ передаваемый в рамках ЮЗЭДО, должен быть подписан электронно-цифровой подписью, указанном в действующем сертификате ключа и использование которой допускается в системе Организатора ЮЗЭДО.
   - • Каждый уполномоченный представитель участника ЭДО должен иметь свой индивидуальный закрытый ключ электронно-цифровой подписи для подписания исходящих от него электронных документов.
3. Отправка электронного документа Участнику ЮЗЭДО, например, по электронной почте;
   - Электронный документ передается как вложение по открытому каналу связи от Отправителя Получателю.
   - Если в системе требуется обеспечить конфиденциальность передаваемой информации Отправитель предварительно производит шифрование электронного документа в адрес Получателя.

4. Проверка подлинности и целостности электронных документов с помощью комплекта («КриптоТри» или «e-token КриптоАРМ»);
   - Полученный электронный документ проверяется на целостность, т.е. его доставку в неискаженном (по отношению к первоначальному) виде, путем расшифрования и обязательной проверки электронно-цифровой подписи.
   - Полученный электронный документ проверяется на соответствие установленному для него формату (форматы электронных документов определяются в правилах Организатора ЮЗЭДО. При работе вне системы документооборота ограничение на форматы файлов не вводится).
   - Получатель производит расшифровку полученных электронных документов и проверку их электронно-цифровой подписи. После завершения расшифровки и проверки электронно-цифровой подписи принятые электронные документы разбираются и сохраняются на рабочем месте Получателя.
   - Электронный документ подлежит дальнейшей обработке и исполнению только в случае положительного результата проверки целостности электронного документа и его соответствия установленному формату и подлинности электронно-цифровой подписи.
   - В случае невозможности расшифрования электронного документа, а также при отрицательном результате проверки целостности электронного документа и подлинности электронно-цифровой подписи электронный документ считается не полученным и не подлежит дальнейшей обработке и исполнению.

10. ПОРЯДОК РАЗРЕШЕНИЯ КОНФЛИКТНЫХ СИТУАЦИЙ, СВЯЗАННЫХ С ПРИМЕНЕНИЕМ ЭЛЕКТРОННОЙ ЦИФРОВОЙ ПОДПИСИ

1.3. ОБЩИЕ ПОЛОЖЕНИЯ

Разрешение конфликтных ситуаций, связанных с применением электронной цифровой подписи, осуществляется Согласительной комиссией.

Согласительная комиссия создается с целью разрешения конфликтных ситуаций, возникающих в связи с подтверждением подлинности электронной цифровой подписи и установления равнозначности электронной цифровой подписи собственноручной.

При возникновении разногласий Участник ЮЗЭДО, заявляющий о разногласии (инициатор), обязан направить организатору (владельцу) ЮЗЭДО заявление о разногласиях, подписанное уполномоченным должностным лицом, с подробным изложением причин разногласий и предложением создать комиссию по ее разрешению.

Заявление должно содержать фамилии представителей стороны - инициатора, которые будут участвовать в работе комиссии.

До подачи заявления стороне - инициатору рекомендуется убедиться в целостности установленных на его технических средствах программного обеспечения, в том числе средства электронной цифровой подписи, а также отсутствии несанкционированных действий со стороны своего персонала и третьих лиц.

По заявлению о разногласиях организатор (владелец) ЮЗЭДО формирует согласительную комиссию, в которую входят:

- представитель организатора (владельца) ЮЗЭДО – председатель комиссии;
- представитель инициатора;
- представитель ответчика;
- представитель Удостоверяющего центра;

Члены комиссии от каждой стороны назначаются приказами соответствующей стороны.

Издержки по проживанию и прибытию на место разбора конфликтной ситуации, а так же командировочные расходы специалиста УЦ несет инициатор разбора.

Комиссия осуществляет свою деятельность по месторасположению организатора (владельца) ЮЗЭДО.

1.4. ДОКУМЕНТЫ, ПРЕДОСТАВЛЯЕМЫЕ ИНИЦИАТОРОМ

Сторона-инициатор представляет заявление о разногласии с указанием:

- даты и номера заявления;
- реквизитов инициатора и ответчика;
- обстоятельств, на которых основаны заявленные требования, и сведений о подтверждающих их доказательствах;
- обоснованного расчета заявленных требований;
- нормы законодательных и иных нормативных правовых актов, на основании которых предъявляется требование;
- перечня прилагаемых к заявлению о разногласии документов, составляющих доказательную базу. В состав указанных документов должны быть включены:
  - файл, содержащий электронный документ с электронной цифровой подписью, либо файл, содержащий электронный документ и файл, содержащий электронную цифровую подпись этого документа;
  - файл, содержащий сертификат ключа подписи, соответствующий электронной цифровой подписи.

1.5. ПОРЯДОК РАБОТЫ СОГЛАСИТЕЛЬНОЙ КОМИССИИ

Ответчик обязан в период работы комиссии представить инициатору и комиссии возражения по каждому требованию, изложенному в заявлении о разногласиях.

В возражениях ответчика на каждое требование должны содержаться документально обоснованные ответы или сделана ссылка на доказательства, которые могут быть представлены в ходе работы комиссии.

Любая сторона в ходе работы комиссии может внести ходатайства об изменении или дополнении своих требований или возражений.

Комиссия в ходе разбирательства в любой момент может затребовать от сторон предоставления документов, вещественных или иных доказательств в устанавливаемый комиссией срок.

Рассмотрение спора производится на основании всех представленных документов, доказательств.

В том случае, если обстоятельства, имеющие значение для принятия решения по делу, могут быть исследованы только на основе применения специальных научных знаний,

комиссия вправе назначить экспертизу по подтверждению подлинности электронной цифровой подписи в электронном документе.

Проведение экспертизы возлагается на экспертов Удостоверяющего центра. Запрос на проведение экспертизы оформляется Заявлением на подтверждение подлинности электронной цифровой подписи в произвольной форме в электронном документе, подающемся в Удостоверяющий центр.

Экспертиза может быть назначена комиссией по обоснованному ходатайству любой из сторон или по ее собственной инициативе.

Экспертиза осуществляется с использованием применяемого средства электронной цифровой подписи и специализированного программного обеспечения (СПО) «КриптоПро УЦ. Программный комплекс разбора конфликтных ситуаций».

Технический порядок проведения экспертизы определяется эксплуатационной документацией на данное СПО.

Экспертиза осуществляется на компьютере, конфигурация и технические характеристики которого полностью соответствуют требованиям, изложенным в эксплуатационной документации данного СПО.

1.6. ОФОРМЛЕНИЕ РЕЗУЛЬТАТОВ РАБОТЫ СОГЛАСИТЕЛЬНОЙ КОМИССИИ

По итогам работы согласительной комиссии составляется акт, в котором содержится краткое изложение выводов комиссии и решение комиссии по рассматриваемому разногласию.

Помимо изложения выводов согласительной комиссии и решения комиссии акт должен содержать следующие данные:

- состав комиссии;
- дату и место составления акта;
- дату и время начала и окончания работы комиссии;
- краткий перечень мероприятий, проведенных комиссией;
- собственноручные подписи членов комиссии;
- указание на особое мнение члена (или членов комиссии), в случае наличия такового.

Акт составляется в 3-х экземплярах и предоставляется организатору (владельцу) ЮЗЭДО и Участникам ЮЗЭДО, полномочные представители которых являлись членами согласительной комиссии.

11. КОМПЛЕКТАЦИЯ РАБОЧЕГО МЕСТА ПОЛЬЗОВАТЕЛЯ ЮЗЭДО

Типовое рабочее место пользователя системы защищенного электронного документооборота комплектуется на базе компьютера с ОС Windows XP/2000/2003 и включает:

- программный комплекс «КриптоТри» для защиты файлов (электронных документов) и присоединений в почтовых сообщениях;
- дополнительный модуль «КриптоАРМ: клиент УЦ» для генерации ключей и запросов на сертификацию в обслуживаемом УЦ;
- секретный ключевой носитель (рекомендуется отчуждаемый носитель ruToken или eToken), содержащий индивидуальный секретный ключ пользователя;
- корневой сертификат УЦ, установленный в локальное хранилище сертификатов на компьютере (может использоваться в т.ч. для установления защищенного взаимодействия с Web-сервером);
- драйвера ключевых носителей (при использовании ruToken или eToken);
- почтовый клиент (рекомендуется Microsoft Outlook);
- Интернет-браузер «Microsoft Internet Explorer», «Netscape Communicator», «FireFox», «Opera», «Lotus Notes» и др.

11.1. ИНСТАЛЛЯЦИЯ ПРОГРАММ (АПК «КРИПТО ТРИ»)

Для начала работы с системой необходимо установить на рабочем месте клиента программное обеспечение, приобретенное в компании «Актив». Для этого необходимо:

1. Вставить компакт диск с программным обеспечением в дисковод.
2. Затем нужно запустить установочный файл Crypto3.36.Rus.v.1.00.00.0005.msi, находящийся в корневом каталоге компакт диска.

Появится следующее окно:

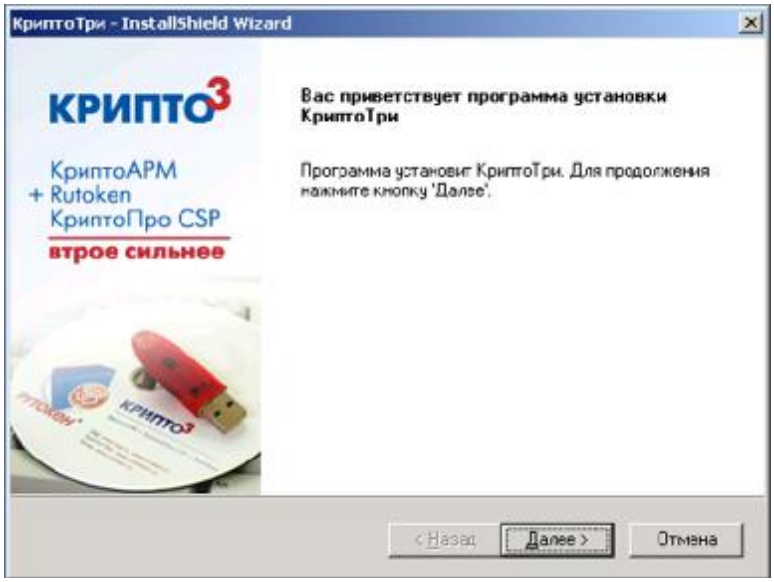

Рис. 1.1. Начальное окно мастера установки АПК «КриптоТри»

После проверки конфигурации оборудования и наличия, установленных ранее программных компонент, мастер предложит начать установку ПО (рис.1.2). От пользователя требуется нажать кнопку «Установить».

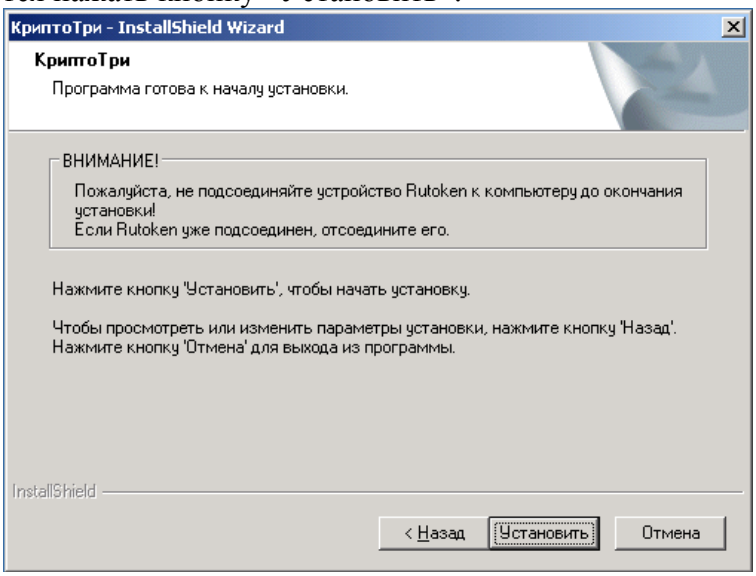

Рис. 1.2. Подтверждение процесса установки

При нажатии кнопки «Установить» происходит запуск мастера установки СКЗИ «КриптоПро CSP» (рис. 1.3). Пользователю необходимо нажать на кнопку «Далее», чтобы подтвердить установку и регистрацию криптобиблиотеки на своем рабочем месте.

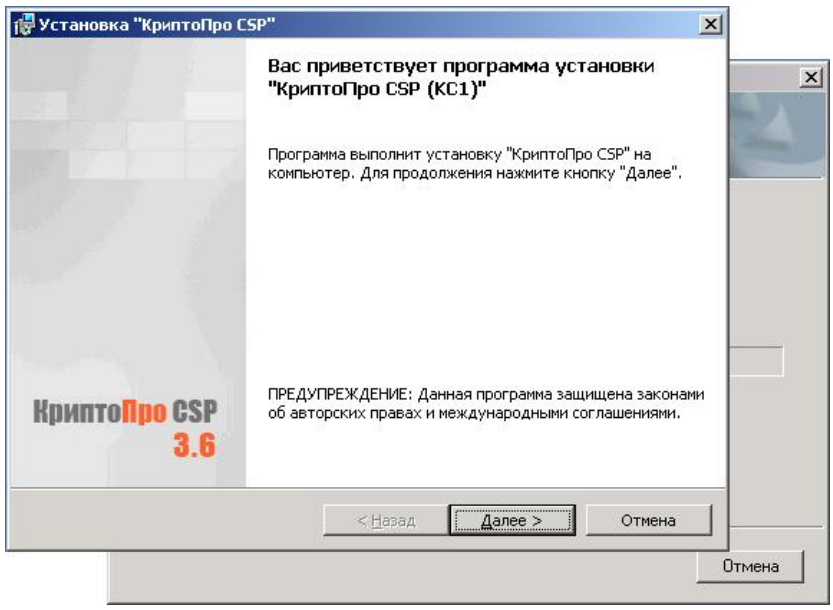

Рис. 1.3. Начальное окно мастера установки СКЗИ «КриптоПро CSP»

На следующем шаге мастера установки СКЗИ «КриптоПро CSP» пользователю предлагается ознакомиться с текстом лицензионного соглашения об использовании программного продукта (рис. 1.4). От пользователя требуется принять данное лицензионное соглашение и нажать на кнопку «Далее», чтобы продолжить установку.

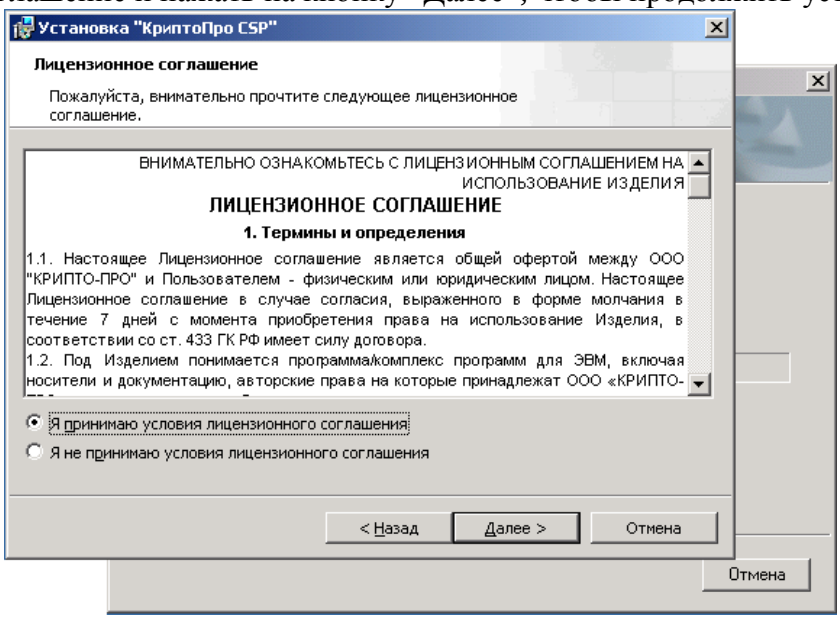

Рис. 1.4. Знакомство с лицензионным соглашением об использовании СКЗИ

Далее от пользователя потребуется указание серийного номера лицензии на СКЗИ «КриптоПро CSP» (рис. 1.5). Если пропустить данный шаг и не ввести серийный номер лицензии, продукт будет функционировать в полноценном режиме в течение трех месяцев, а после их истечения – в ограниченном режиме (только для проверки ЭЦП). Серийный номер можно также ввести непосредственно через диалоговое окно приложения «КриптоПро CSP» после его установки.

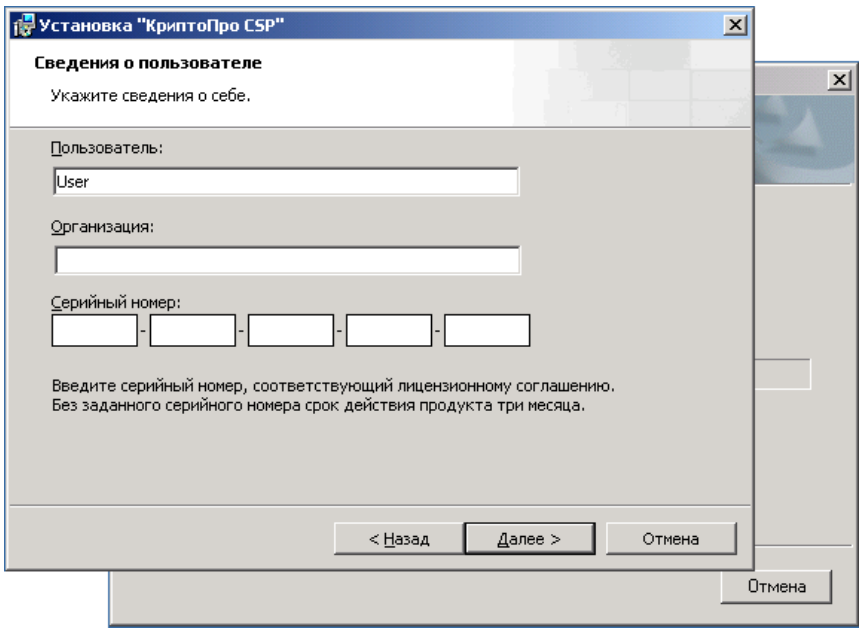

Рис. 1.5. Ввод лицензии на СКЗИ «КриптоПро CSP»

На следующем шаге установки предлагается выбрать один из двух режимов установки компонент программного продукта (рис. 1.6). В обычном режиме установки производится инсталляция всех необходимых компонент для работы с приложением «КриптоАРМ» в системе документооборота. Производить установку дополнительных компонент (рис. 1.7), при организации рабочего места пользователя, не требуется.

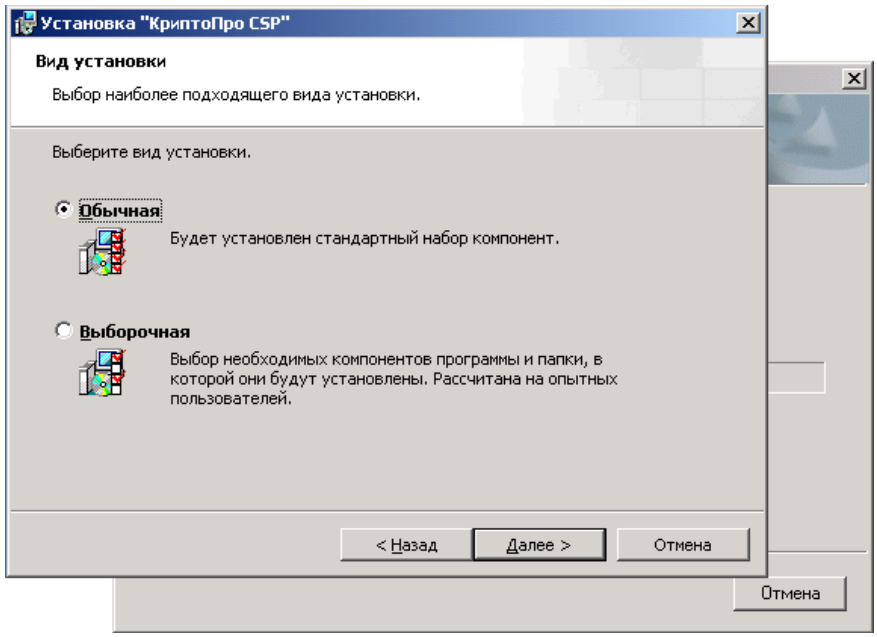

Рис. 1.6. Выбор режима установки приложения

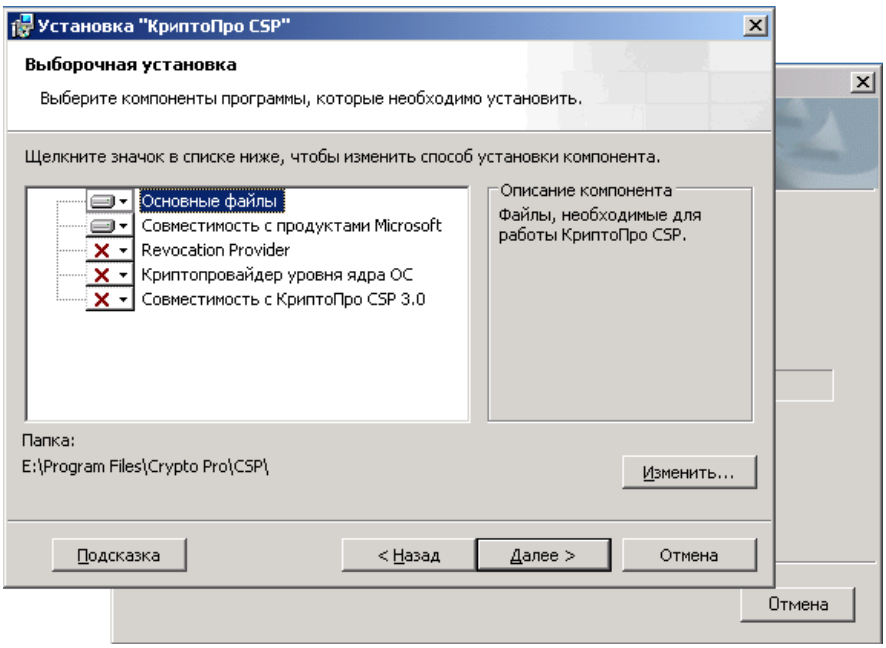

Рис. 1.7. Режим выборочной установки компонент ПО

На следующем шаге мастера установки «КриптоПро CSP» от пользователя потребуется отметить те носители контейнера закрытого ключа, которые будут использоваться при совершении операции с подписью и шифрованием на рабочем месте пользователя (рис. 1.8). Для продолжения установки от пользователя требуется – нажать на кнопку «Установить».

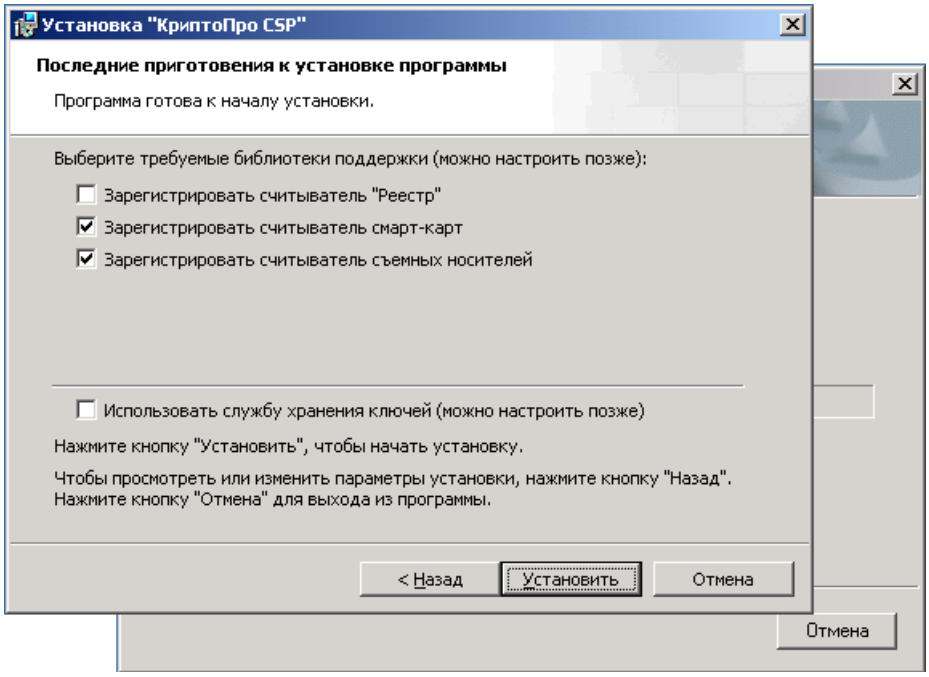

Рис. 1.8. Выбор списка регистрируемых считывателей

По завершении установки СКЗИ «КриптоПро CSP» необходимо нажать кнопку «Готово» (рис. 1.9) и без участия пользователя сразу начнется установка драйверов отчуждаемого носителя ruToken (рис. 1.10).

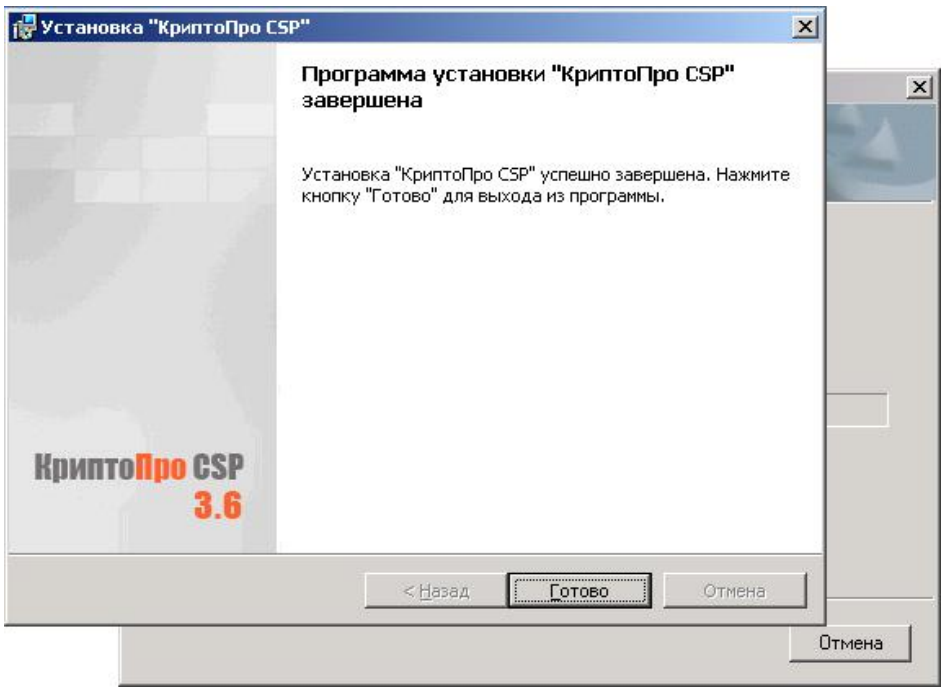

Рис. 1.9. Финальное окно мастера установки СКЗИ «КриптоПро CSP»

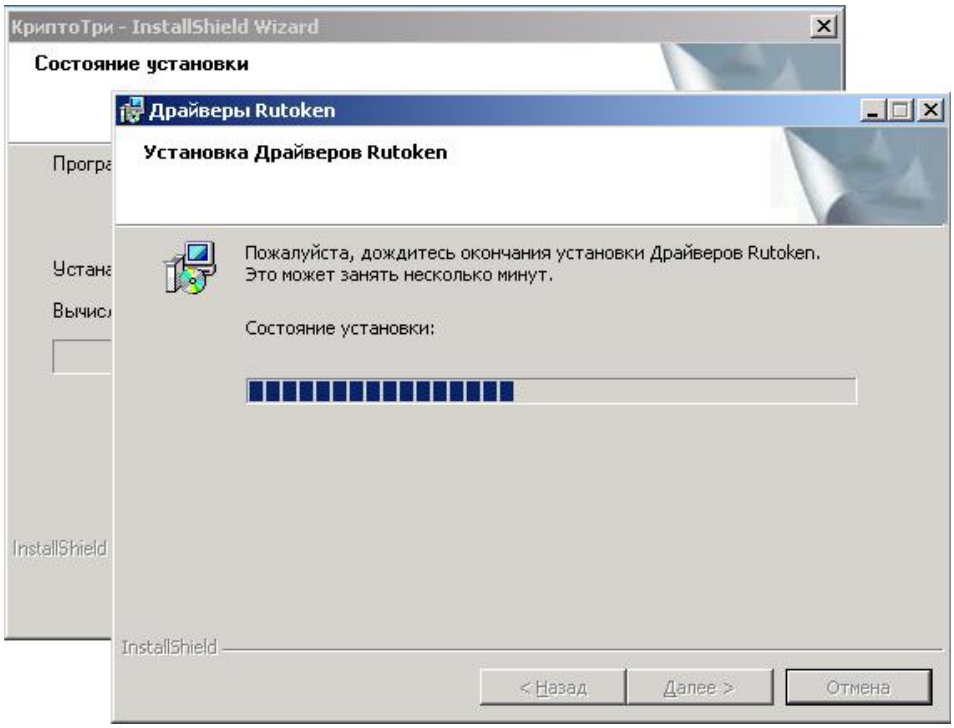

Рис. 1.10. Установка драйверов отчуждаемого носителя ruToken

После окончания процесса установки драйверов ruToken, запустится мастер установки приложения «КриптоАРМ» (рис. 1.11). Пользователю необходимо нажать кнопку «Далее».

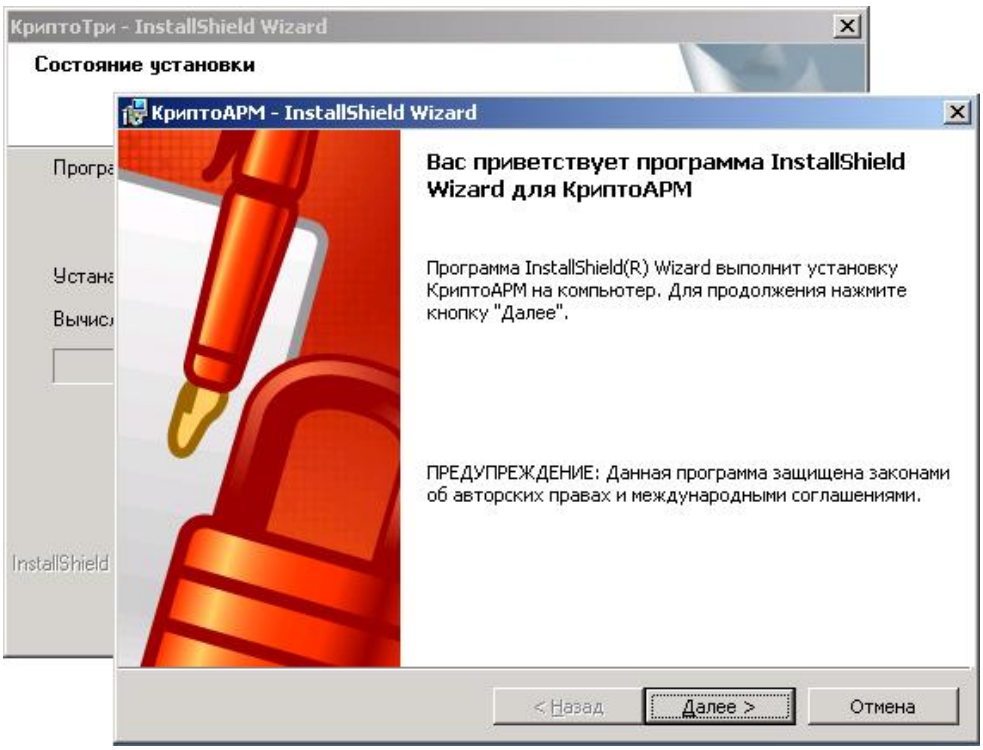

Рис. 1.11. Начальное окно мастера установки «КриптоАРМ»

На следующем шаге мастера от пользователя потребуется выбрать вариант установки приложения (рис. 1.12).

Установка приложения КриптоАРМ Старт предполагает использование СКЗИ «КриптоПро CSP» только для проверки подписи. Приложение обладает полным функционалом при выполнении операций с ЭЦП и шифрованием с использованием предустановленных в системе криптопровайдеров (Microsoft). Ввод лицензии на эту версию установки не требуется. Работа с ГОСТ СКЗИ «КриптоПро CSP» поддерживается только в режиме проверки подписи.

Установка приложений «КриптоАРМ Стандарт» и «КриптоАРМ СтандартPRO» требует ввода лицензии для активации полнофункциональной версии. При вводе лицензии будет обеспечена работа с установленным в системе СКЗИ «КриптоПро CSP».

Если у пользователя отсутствует лицензия на ПО «КриптоАРМ» ему не следует прерывать инсталляцию продукта, и продолжить установку без ввода лицензии. После получения лицензии на продукт, ее можно будет ввести через диалоговое окно приложения.

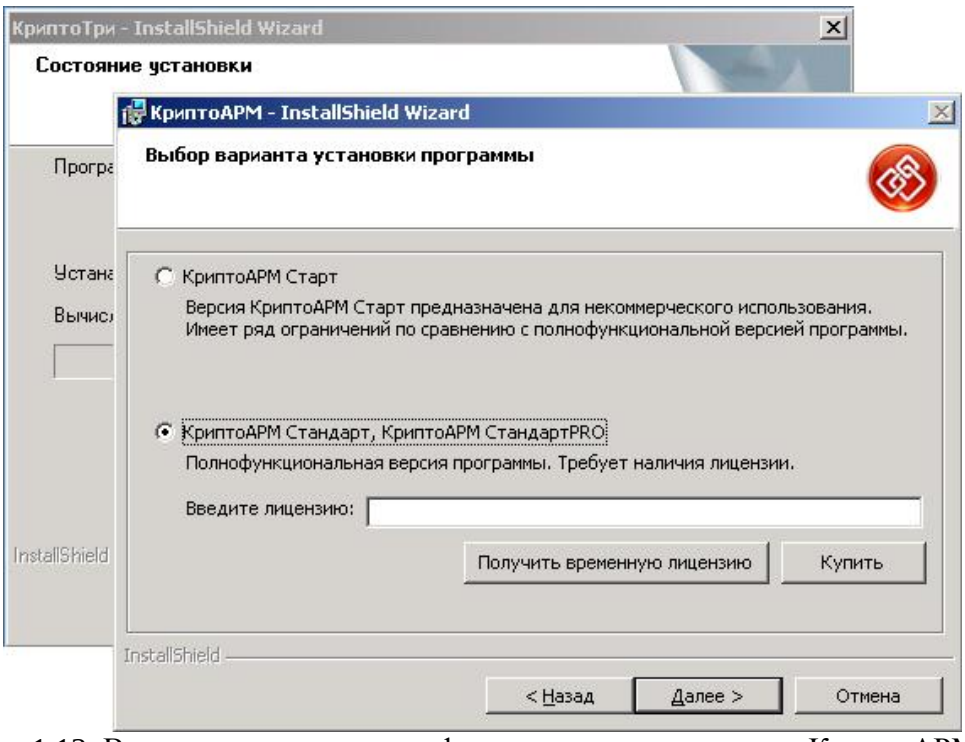

Рис. 1.12. Ввод лицензии на полнофункциональную версию «КриптоАРМ»

Для продолжения установки приложения от пользователя требуется ознакомиться с текстом лицензионного соглашения и принять его. Чтобы перейти к следующему шагу мастера – потребуется нажать на кнопку «Далее».

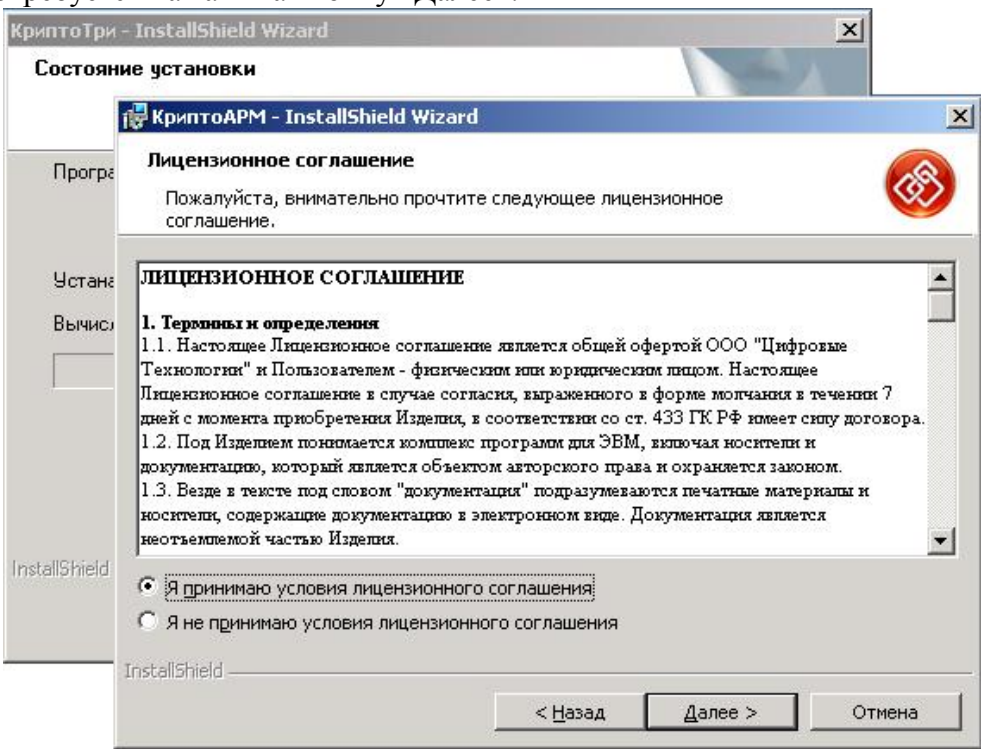

Рис. 1.13. Просмотр лицензионного соглашения об использовании ПО «КриптоАРМ»

Чтобы выполнить установку приложения только для конкретного пользователя (текущей учетной записи) нужно выбрать режим - «только для меня (User)». В противном случае установка приложения производится для всех пользователей этого компьютера (всех учетных записей) (рис. 1.14). После выбора режима нужно нажать кнопку «Далее».

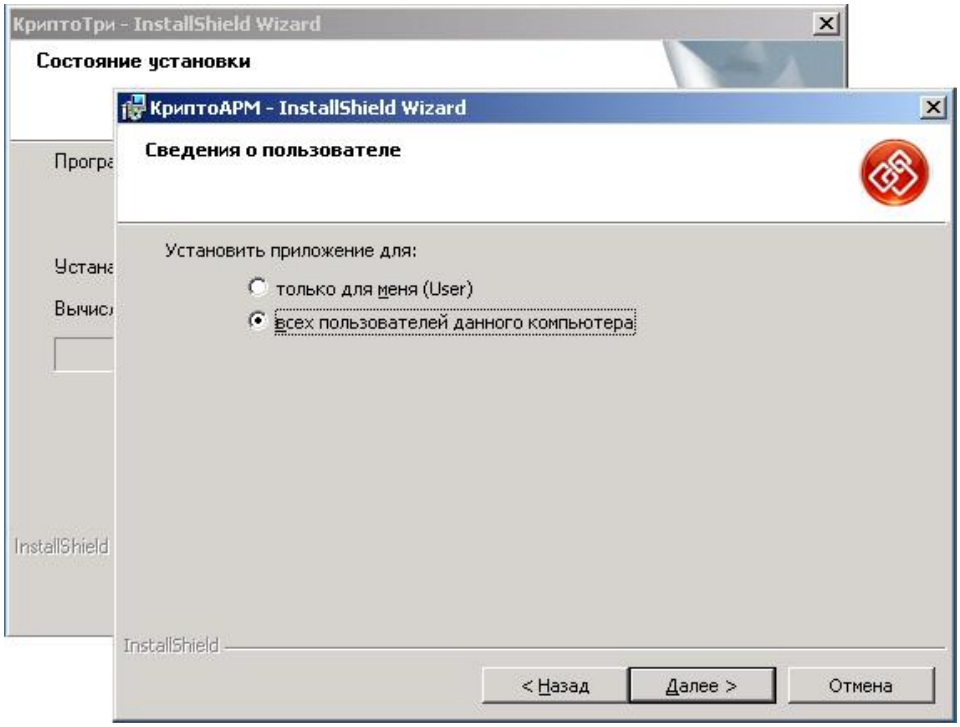

Рис. 1.14. Выбор варианта установки в системе

При нажатии кнопки «Установить» (рис. 1.15) происходит инсталляция компонент приложения на жесткий диск, создания ярлыка «КриптоАРМ» на рабочем столе. Весь процесс происходит без вмешательства пользователя.

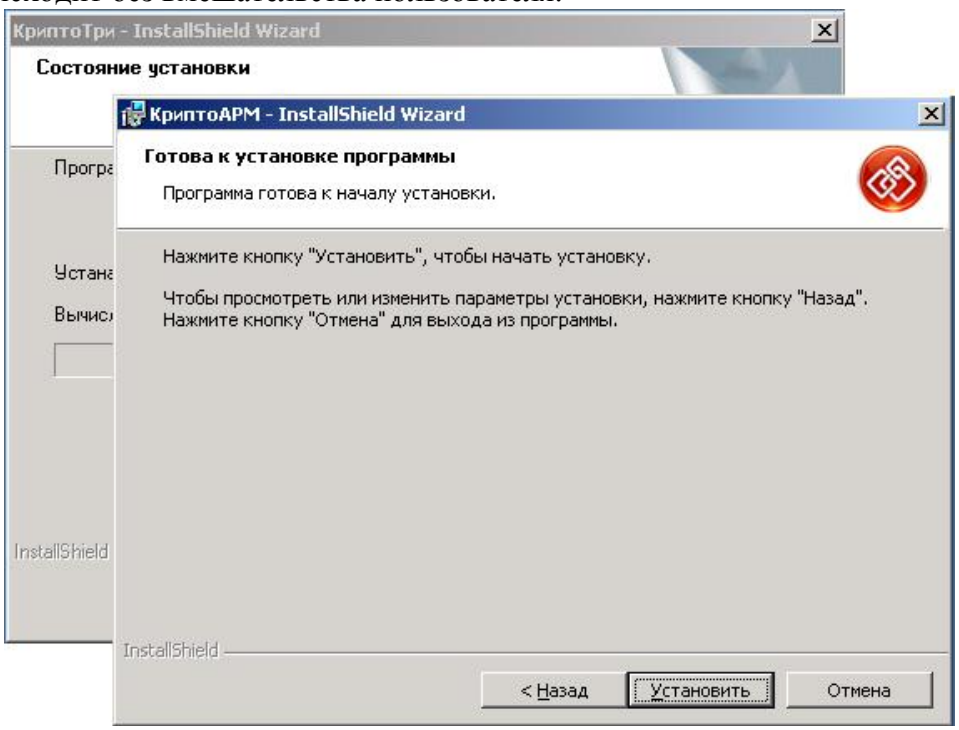

Рис. 1.15. Подтверждение процесса установки ПО «КриптоАРМ»

После завершения процесса установки ПО «КриптоАРМ», на экране должно появиться следующее диалоговое окно (рис. 1.16); от пользователя потребуется нажать на кнопку «Готово».

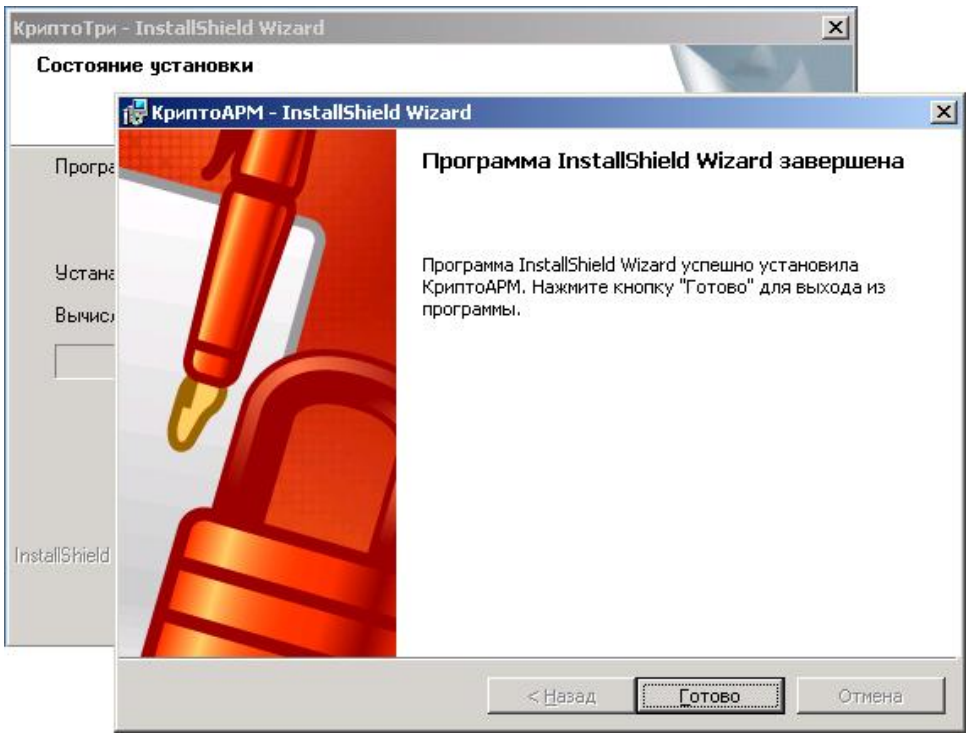

Рис. 1.16. Завершение установки приложения «КриптоАРМ»

При завершении установки последнего компонента – ПО «КриптоАРМ», входящего в состав АРМ «КриптоТри» появляется финальное окно мастера установки дистрибутива с предложением произвести перезагрузку. Чтобы закончить установку пользователю требуется перезагрузить компьютер, чтобы регистрации криптобиблиотеки и программных модулей КриптоАРМ вступили в силу.

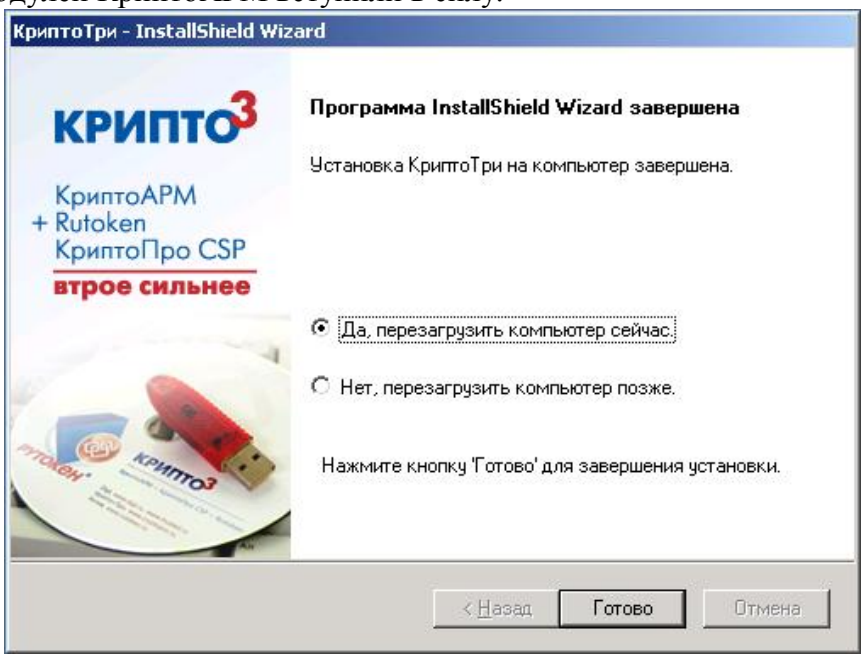

Рис. 1.17. Финальное окно мастера установки «КриптоТри»

11.2. ИНСТАЛЛЯЦИЯ ПРОГРАММ (АПК «eTOKEN КРИПТОАРМ»)

Для начала работы с системой необходимо установить на рабочем месте клиента программное обеспечение, приобретенное в компании «Aladdin» или у официальных дилеров. Для этого необходимо:

1. Вставить компакт диск с программным обеспечением в дисковод.
2. Затем нужно запустить установочный файл singlepackinstaller_1.0.0.10.msi, находящийся в корневом каталоге компакт диска. Появится следующее окно (рис. 2.1).

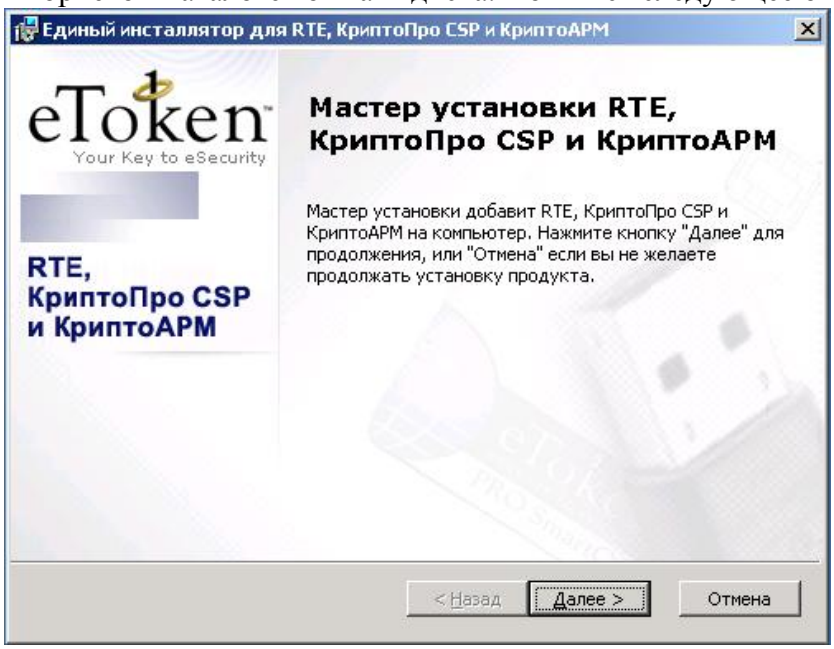

Рис. 2.1. Начальное окно мастера установки АПК «eToken КриптоАРМ»

После проверки конфигурации оборудования и наличия, установленных ранее программных компонент, мастер предложит начать установку ПО (рис.2.2). От пользователя требуется нажать кнопку «Установить».

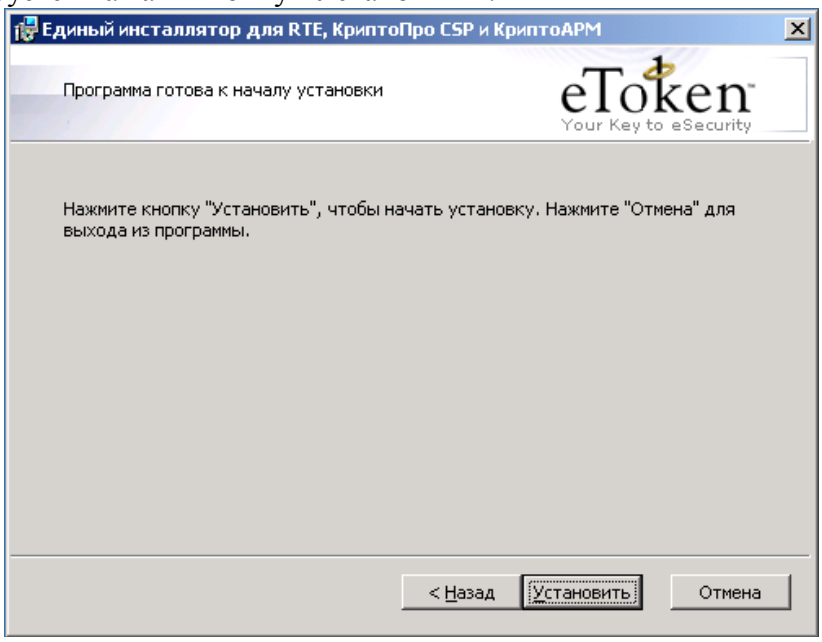

Рис. 2.2. Подтверждение процесса установки

При нажатии кнопки «Установить» происходит собственно инсталляция программ на жесткий диск, создания ярлыка «КриптоАРМ» на рабочем столе и регистрация криптобиблиотеки в операционной системе пользователя. Весь процесс происходит без вмешательства пользователя (рис. 2.3, 2.4).

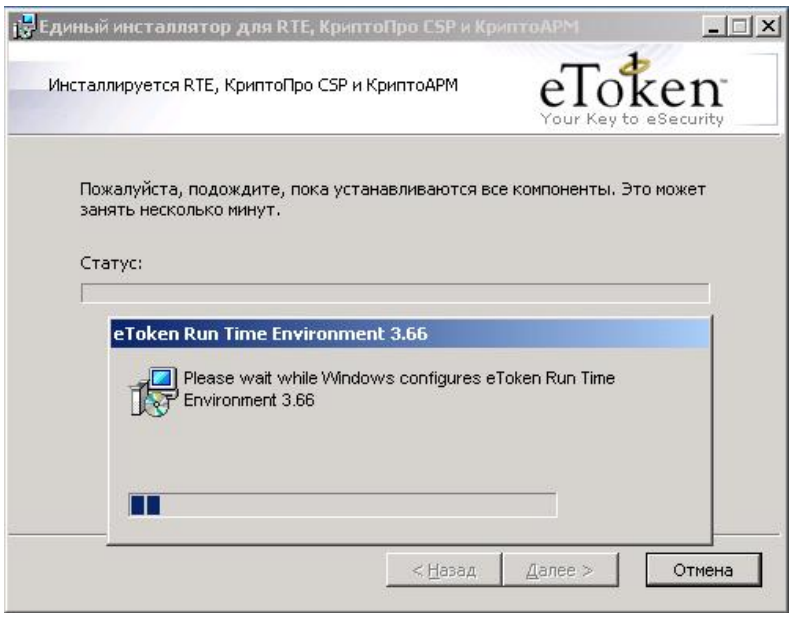

Рис. 2.3. Установка драйверов eToken в автоматическом режиме

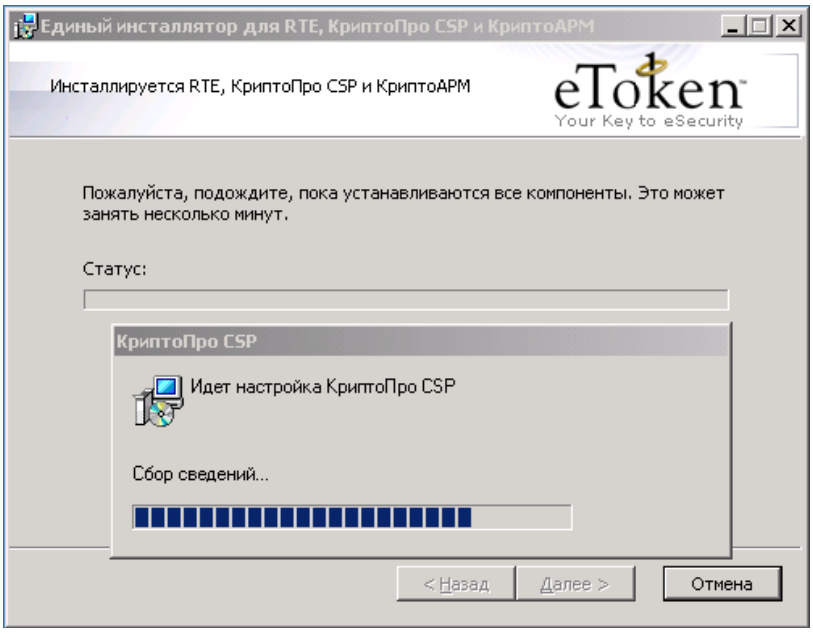

Рис. 2.4. Установка программных компонент «КриптоАРМ» и «КриптоПро CSP»

По завершении установки необходимо нажать кнопку «Готово» (рис. 2.5) и следует произвести перезагрузку операционной системы для вступления регистрации криптобиблиотеки и программных модулей КриптоАРМ в силу.

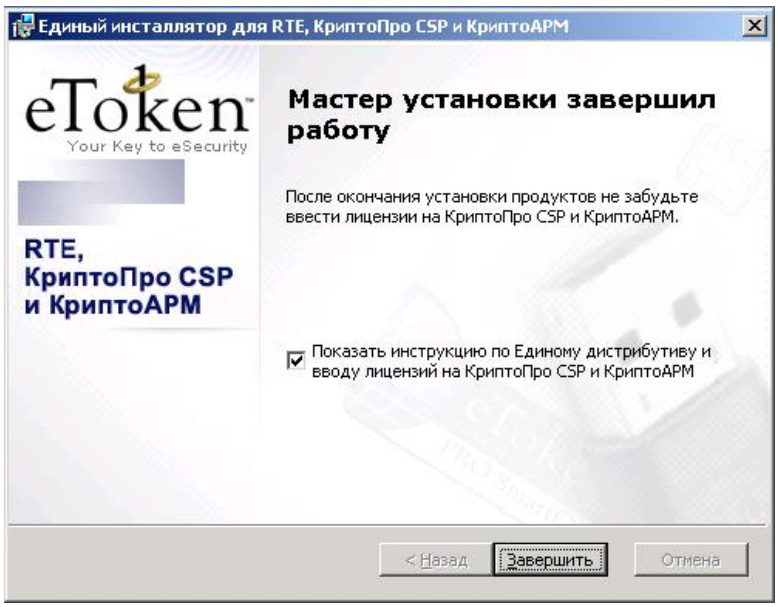

Рис. 2.5. Финальное окно мастера при успешном завершении процесса установки

Для управления отчуждаемым носителем eToken в систему устанавливается утилита, которая позволяет выполнить настройку свойств подключаемых носителей и несколько упростить процесс первоначальной инициализации криптосистемы на рабочем месте (рис. 2.6).

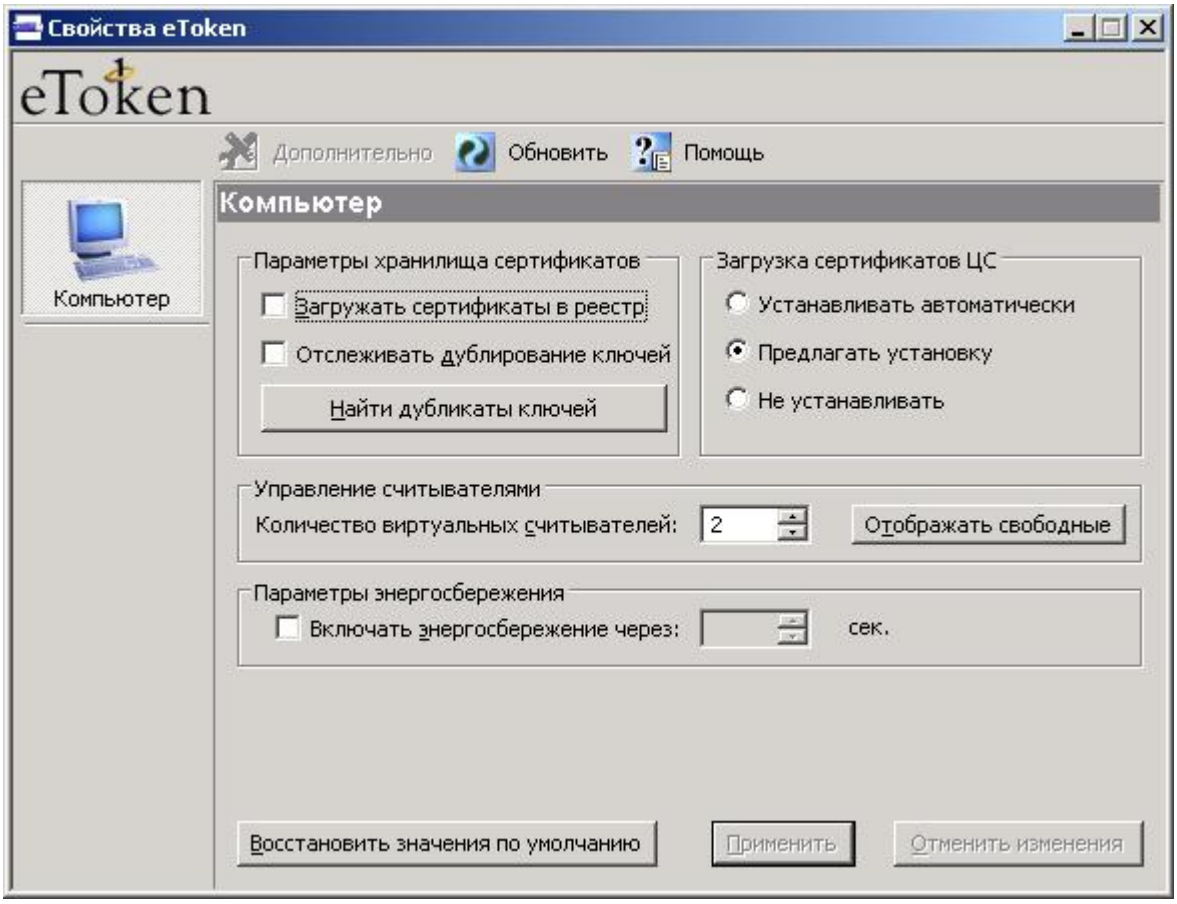

Рис. 2.6. Дополнительная утилита управления отчуждаемым носителем

11.3. РЕКОМЕНДАЦИИ ПО БЕЗОПАСНОСТИ

Для обеспечения защиты данных от несанкционированного доступа, согласно регламенту электронного документооборота на предприятии, подключенном к системе юридически значимого документооборота в электронном виде по телекоммуникационным каналам связи, должны соблюдаться следующие меры безопасности:

1. Хранение контейнера закрытого ключа пользователя производится на USB-токене или другом надежном хранилище. При хранении контейнера закрытого ключа в реестре необходимо задание пароля или исключение возможности доступа к рабочему месту посторонних лиц.
2. PIN-код отчуждаемого носителя или пароль контейнера закрытого ключа должен быть известен только самому владельцу; хранение пароля на физических носителях не рекомендуется.
3. Не допускается экспорт и хранение незащищенного контейнера закрытого ключа и сертификата в одном месте.
4. USB-токен с контейнером закрытого ключа используется только на время работы в системе документооборота при совершении криптографических операций.
5. При утере или хищении пароля, PIN-кода или самого отчуждаемого носителя, утечке информации о них немедленно ставится в известность администратор системы или владелец документооборота. Инициируется предусмотренный регламентом процесс блокирования и внештатной смены сертификата и контейнера закрытого ключа.
6. Штатная смена сертификата и контейнера закрытого ключа (без личного визита, по защищенному каналу связи) производится не реже одного раза в год.