УТВЕРЖДЕНО
Проректор по цифровизации

_____А.В. Антонов
«24» апреля 2024 года

Программа по обучению пользователей СКЗИ

Краткое руководство пользователя
ViPNet Client Monitor

Назначение ПО ViPNet Client

Программное обеспечение ViPNet Client входит в состав пакетов ViPNet CUSTOM и ViPNet OFFICE. ViPNet Client выполняет функции VPN-клиента в сети ViPNet и обеспечивает защиту компьютера от несанкционированного доступа при работе в локальных или глобальных сетях. Программное обеспечение ViPNet Client может быть установлено для защиты трафика на любом компьютере с ОС Windows, будь то стационарный, удаленный, мобильный компьютер или сервер.

Состав ПО ViPNet Client

Программное обеспечение ViPNet Client состоит из следующих компонентов:

- Низкоуровневый драйвер сетевой защиты ViPNet-драйвер.
- Программа ViPNet Монитор.
- Транспортный модуль ViPNet MFTP.
- Программа ViPNet Контроль приложений.
- Программа ViPNet Деловая почта.

ViPNet Монитор

Программа ViPNet Монитор предназначена для настройки различных параметров ViPNet-драйвера (см. «Принцип работы ViPNet-драйвера» на стр. 15) и записи событий, возникающих в процессе работы драйвера, в журнал регистрации IP-пакетов (см. «Работа с журналом IP-пакетов» на стр. 213). Если выгрузить программу ViPNet Монитор из памяти компьютера, ViPNet-драйвер продолжит работу и будет обеспечивать безопасность компьютера, но в журнале регистрации IP-пакетов может отсутствовать информация о трафике, обработанном драйвером при закрытой программе ViPNet Монитор (ViPNet-драйвер может хранить в памяти не более 10000 записей журнала).

На компьютере программа ViPNet Монитор:

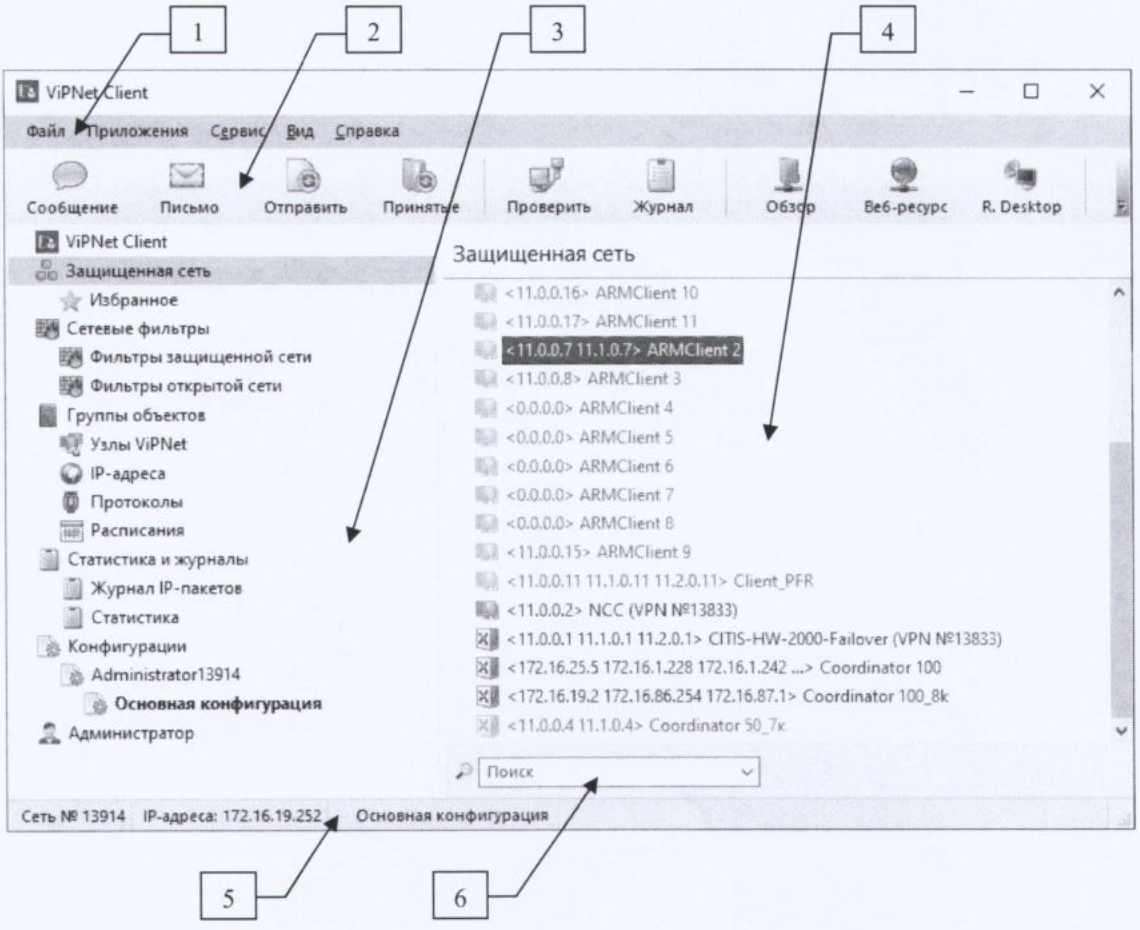
•Выполняет функции персонального сетевого экрана. В связи с этим возможны проблемы с доступом к ресурсам ПЭВМ с установленным ViPNet Монитор, которые решаются настройкой соответствующих правил в фильтрах открытой сети. Также могут быть проблемы с доступом к туннелируемым ресурсам, расположенными за координаторами других сетей, т.к. понадобится добавлять новые связи в ЦУС ViPNet и прописывать дополнительные правила в фильтрах туннелируемых ресурсов на соответствующем координаторе.

•Шифрует IP-трафик компьютера.

•Позволяет управлять параметрами обработки прикладных протоколов.

•Предоставляет встроенные функции для защищенного обмена сообщениями, проведения конференций, файлового обмена и так далее.

Интерфейс программы ViPNet Монитор



Цифрами на рисунке обозначены:

1. Главное меню программы.
2. Панель инструментов. Чтобы удалить или добавить кнопки на панель инструментов,в меню **Вид** выберите пункт **Настроить панель**.
3. Панель навигации. Содержит перечень разделов, предназначенных для настройки различных параметров ViPNet Монитор:
    - **Защищенная сеть** (этот раздел выбран по умолчанию) — содержит список сетевых узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью

- **Сетевые фильтры**. Содержит подразделы с правилами фильтрации IP-трафика:
    - **Фильтры защищенной сети** — предназначен для настройки правил фильтрации защищенного трафика.
    - **Фильтры открытой сети** — предназначен для настройки правил фильтрации открытого трафика.
- **Группы объектов** — содержит различные объекты использующиеся в работе ViPNet.
- **Блокированные IP-пакеты** — предназначен для просмотра информации о заблокированных IP-пакетах.
- **Статистика** — предназначен для просмотра статистики фильтрации IP-пакетов
- **Журнал IP-пакетов** — предназначен для поиска записей в Журнале IP-пакетов
- **Конфигурации** — предназначен для управления конфигурациями программы ViPNet Монитор
- **Администратор** — отображается только после ввода пароля администратора сетевого узла и служит для настройки дополнительных параметров программы

> **Примечание.** Количество и порядок расположения разделов на панели навигации зависит от уровня полномочий пользователя, который определяется в ViPNet Центр управления сетью или ViPNet Manager.

4. Панель просмотра. Предназначена для отображения раздела, выбранного на панели навигации
5. Строка поиска. Отображается в разделах **Защищенная сеть**, **Фильтры защищенной сети**, **Фильтры открытой сети** и **Блокированные IP-пакеты**. Для поиска по разделу введите в этой строке часть адреса, имени или другие параметры сетевого узла. В разделе **Защищенная сеть** поиск ведется по следующим параметрам:
    - Имя узла (отображается в разделе **Защищенная сеть** и в окне **Свойства узла** на вкладке **Общие**). о Имя компьютера (окно **Свойства узла**, вкладка **Общие**).
    - Псевдоним (окно **Свойства узла**, вкладка **Общие**).
    - Реальные и виртуальные IP-адреса (окно **Свойства узла**, вкладка **IP-адреса**, список **IP-адреса**).
    - DNS-имя (окно **Свойства узла**, вкладка **IP-адреса**, список **DNS-имя**).
    - Идентификатор узла (окно **Свойства узла**, вкладка **Общие**).

    Чтобы очистить строку поиска, нажмите кнопку **Всё**.
6. Строка состояния.

Работа в разделе «Защищенная сеть»

Раздел **Защищенная сеть** содержит список защищенных узлов ViPNet, которые связаны с данным сетевым узлом в программе ViPNet Центр управления сетью. Значок

рядом с именем сетевого узла, а также цвет имени обозначают текущий статус сетевого узла:

Таблица5. Обозначение статуса сетевых узлов

Значок	Цвет имени	Статус сетевого узла
	Синий	Свой сетевой узел
	Серый	Клиент в данный момент отключен от сети либо нет данных о его статусе
	Фиолетовый	Клиент в данный момент подключен к сети
	Серый или фиолетовый, полужирный	Новый сетевой узел, с которым была создана связь
	Красный	Координатор в данный момент отключен от сети либо нет данных о его статусе
	Красный	Координатор в данный момент подключен к сети

Примечание. Внешний вид значков зависит от используемой операционной системы (в таблице приведены значки для Windows Vista и Windows 7).

Чтобы настроить параметры внешнего вида раздела **Защищенная сеть**, выберите в окне программы ViPNet Монитор в меню **Сервис** пункт **Настройки** и далее перейдите к разделу **Общие**.

Для удобства просмотра списка и поиска сетевые узлы в разделе **Защищенная сеть** можно сгруппировать по папкам.

Для поиска сетевого узла в списке введите часть имени, IP-адреса или другие параметры узла в строку поиска Для просмотра свойств сетевого узла дважды щелкните имя узла. Откроется окно **Свойства узла**, в котором приведены общие сведения о сетевом узле и содержатся настройки доступа к узлу. Чтобы проверить соединение с другим узлом, начать сеанс обмена защищенными сообщениями, отправить файл или использовать другие встроенные функции программы ViPNet Монитор, выполните одно из действий:

- Выберите сетевой узел в списке и нажмите соответствующую кнопку на панели инструментов.
- Выберите соответствующий пункт в контекстном меню сетевого узла.

Общие сведения о сетевых фильтрах

Сетевые фильтры создаются отдельно для защищенного и открытого трафика. С помощью фильтров для открытой сети на защищенном узле можно разрешить либо запретить обмен IP-пакетами определенного типа с открытыми узлами, то есть с узлами, на которых не установлено программное обеспечение ViPNet с функцией шифрования трафика.

Примечание. К открытым узлам относятся также компьютеры с программным обеспечением ViPNet CryptoService и ViPNet Registration Point.

С помощью фильтров защищенной сети можно ограничить обмен IP-трафиком с защищенными узлами ViPNet, с которыми данный узел имеет связь. По умолчанию любые соединения с защищенными узлами разрешены фильтром **<Все защищенные узлы>** (см. «Фильтры защищенной сети, настроенные по умолчанию» на стр. 135).

Списки сетевых фильтров представлены на правой панели в окне **ViPNet Client [Монитор]** в разделах **Фильтры защищенной сети** и **Фильтры открытой сети**. Сетевые фильтры в программе ViPNet Client имеют следующие особенности:

- Фильтры защищенной сети и фильтры открытой сети разделены на группы:
  - **Локальные фильтры** определяют правила фильтрации для нешироковещательных IP-пакетов, которыми сетевой узел обменивается с внешними сетевыми устройствами.
  - **Широковещательные фильтры** определяют правила фильтрации пакетов,
  - адреса назначения которых являются широковещательными. Такие адреса используются для рассылки пакетов на все компьютеры в локальной сети.
- Сетевые фильтры имеют двухуровневую структуру.

  На первом уровне находятся правила, в которых задается список IP-адресов или защищенных узлов ViPNet, на которые распространяется действие фильтров, создаваемых на втором уровне.

  Фильтры привязаны к конкретным правилам и определяют действие, применяемое к IP-пакетам, в соответствии с заданными параметрами: протокол, порты, типы, коды, направление соединения, расписание действия данного фильтра.
- Действие правила определяется фильтрами. Фильтры могут пропускать или блокировать IP-пакеты, соответствующие заданным параметрам.

  Чтобы изменить действие правила, двойным щелчком откройте фильтр и из списка **Действие фильтра** выберите требуемое значение (см. «Создание фильтров» на стр.142).

  Правило включено, если установлен флажок рядом с именем правила. Если флажок снят, то правило отключено. То же самое относится к фильтрам. Чтобы включить или отключить правило или фильтр, установите или снимите соответствующий флажок.
- Внутри каждой группы IP-пакеты проверяются на соответствие правилам по порядку сверху вниз, в соответствии с расположением правил в списке. Когда пакет блокируется или пропускается первым подходящим правилом, последующие правила уже не оказывают никакого влияния на данный пакет. Порядок правил можно изменять с помощью кнопок **Вверх** и **Вниз**, с помощью перетаскивания правила можно перемещать и копировать (при нажатой клавише **Ctrl**).
- Внутри правила IP-пакеты также проверяются на соответствие фильтрам по порядку сверху вниз, в соответствии с положением фильтров в списке. Когда срабатывает первый подходящий фильтр, последующие фильтры не оказывают на данный пакет никакого влияния. Порядок фильтров можно изменять с помощью кнопок **Вверх** и **Вниз**, с помощью перетаскивания фильтры можно перемещать и копировать (при нажатой клавише **Ctrl**).
- При фильтрации открытого трафика всех протоколов установленные соединения имеют приоритет над другими правилами фильтрации. Если был разрешен некоторый трафик в определенном направлении, для пропускания такого трафика создается временное соединение. Автоматически будет пропущен и ответный трафик, удовлетворяющий параметрам данного соединения. При фильтрации защищенного трафика такое правило действует только для протокола TCP.

Более подробная информация по настройке сетевых фильтров и других параметров программы находится в полном руководстве.

Краткое руководство пользователя КриптоПро CSP

Назначение ПО КриптоПро CSP

Криптопровайдер КриптоПро CSP предназначен для:

- авторизации и обеспечения юридической значимости электронных документов при обмене ими между пользователями, посредством использования процедур формирования и проверки электронной подписи (ЭП) в соответствии с отечественными стандартами ГОСТ Р 34.11-94 / ГОСТ Р 34.11-2012 и ГОСТ Р 34.10-2001 / ГОСТ Р 34.10-2012;
- обеспечения конфиденциальности и контроля целостности информации посредством ее шифрования и имитозащиты, в соответствии с ГОСТ 28147-89;
- обеспечения аутентичности, конфиденциальности и имитозащиты соединений по протоколу TLS;
- контроля целостности системного и прикладного программного обеспечения для его защиты от несанкционированных изменений и нарушений правильности функционирования;
- управления ключевыми элементами системы в соответствии с регламентом средств защиты.

Возможности ПО КриптоПро CSP

Программное обеспечение СКЗИ позволяет использовать российские криптографические алгоритмы и сертификаты открытых ключей стандарта X.509 с различным программным обеспечением Microsoft:

- Центр Сертификации - Microsoft Certification Authority, входящий в состав Windows 2000 Server, Advanced Server, Windows 2003 Server, Windows 2008 Server, Windows 2008R2.
- Электронная почта - MS Outlook (Office 2010, Office 2007, Office 2003, Office XP, Office 2000).
- Электронная почта - Microsoft Outlook Express в составе Internet Explorer, Почта Windows Mail, Live Mail. Microsoft Word, Excel, InfoPath из состава Microsoft Office 2003, 2007, 2010 (с помощью плагина КриптоПро Office Signature).
- Средства контроля целостности ПО, распространяемого по сети - Microsoft Authenticode.
- Службы терминалов для Windows 2003 Server, Windows 2008 Server, Windows 2008R2 Server (включая шлюз служб терминалов).
- Защита TCP/IP соединений в сети Интернет - протокол TLS/SSL при взаимодействии Internet Explorer – web-сервер IIS, TLS-сервер, TLS-клиент (IE).
- SQL-сервер.

- ISA сервер.
- Сервер TMG Сервер UAG.
- Сервер терминалов и клиент (RDP).

Состав ПО КриптоПро CSP

В дистрибутив СКЗИ "КриптоПро CSP" помимо самого криптопровайдера входят следующие продукты:

- **КриптоПро TLS** - Модуль поддержки сетевой аутентификации КриптоПро TLS, входящий в состав СКЗИ КриптоПро CSP, реализует протокол Transport Layer Security (TLS v. 1.0, RFC 2246), с использованием российских криптографических стандартов. Протокол TLS предназначен для обеспечения криптографическими средствами аутентификации отправителя (клиента) - адресата (сервера), контроля целостности и шифрования данных информационного обмена.
- **КриптоПро Winlogon** - КриптоПро Winlogon предназначен для ОС семейства Microsoft Windows и реализует первоначальную аутентификацию пользователя протокола Kerberos V5 (RFC 4120) по сертификату и ключевому носителю (смарт-карта, USB-токен) с использованием сертифицированного СКЗИ "КриптоПро CSP" версии 3.0 и выше.
- **КриптоПро Revocation Provider** - архитектура CryptoAPI предоставляет возможность подключения и внешних модулей проверки статуса сертификата. Продукт "КриптоПро Revocation Provider", предназначен для встраивания проверки статусов сертификатов открытых ключей в режиме реального времени по протоколу OCSP в операционные системы семейства Microsoft Windows. При этом менять что-либо в самих приложениях не требуется. "КриптоПро Revocation Provider" вызывается автоматически каждый раз, когда приложение осуществляет действия с сертификатом.
- **Пользовательский интерфейс**. Представляет собой интерфейс, позволяющий настраивать параметры работы в инфраструктуре открытых ключей (PKI).

Тестирование контейнера закрытого ключа

Для того чтобы провести тест работоспособности контейнера закрытого ключа, выполните **Пуск - Программы - КриптоПро - КриптоПро CSP** и перейдите на вкладку **Сервис** (см. Рис. 1). Нажмите кнопку **Протестировать.**

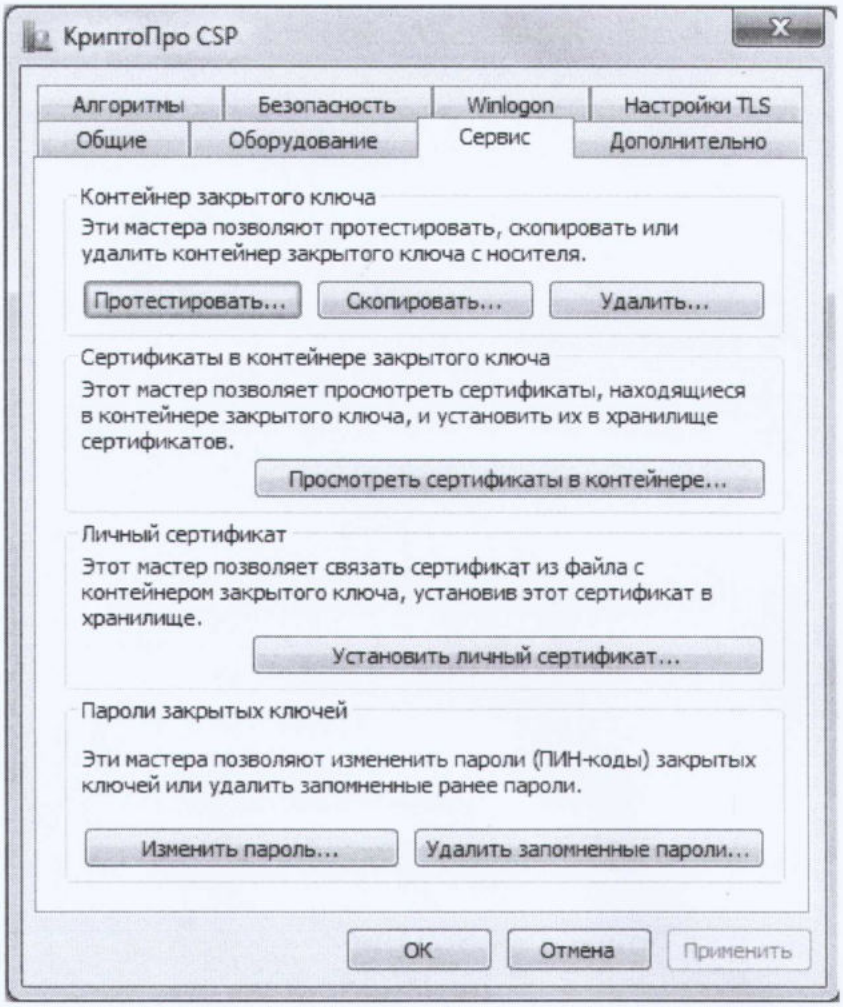


Рис. 1. Контрольная панель. Вкладка «Сервис»

Система отобразит окно «Тестирование контейнера закрытого ключа» (см. Рис. 2).

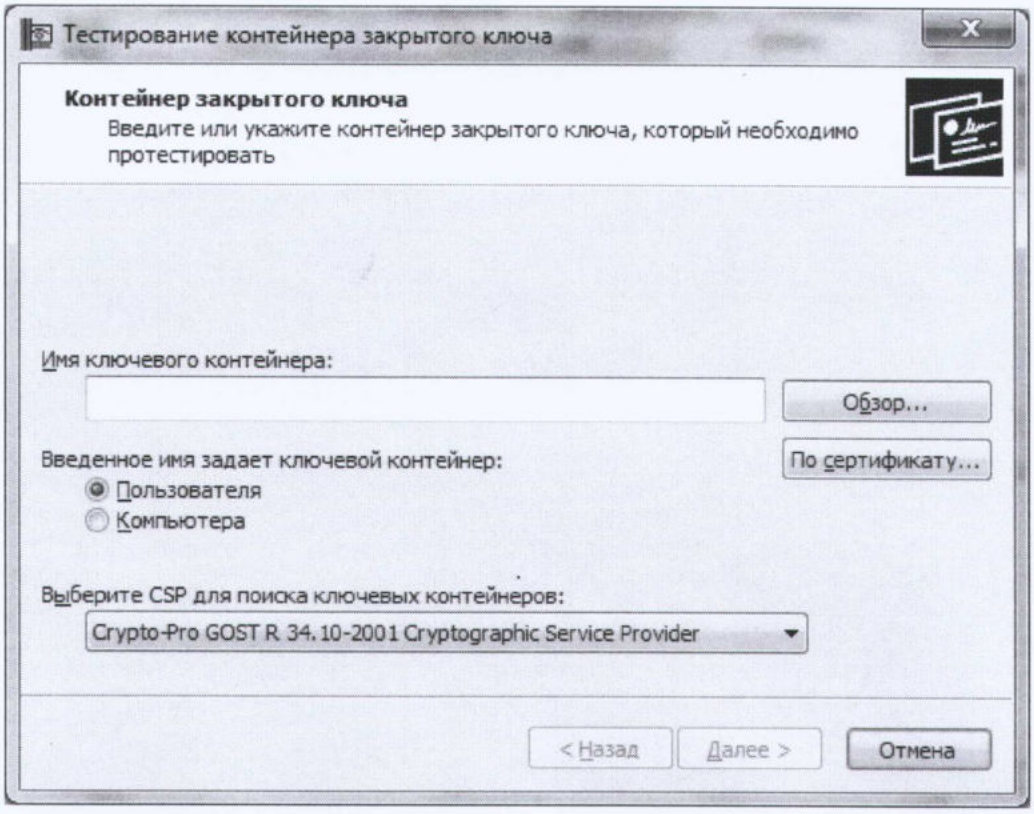


Рис. 2. Окно «Тестирование контейнера закрытого ключа»

В этом окне необходимо заполнить следующее поле ввода:

Имя ключевого контейнера – вводится вручную или выбирается из списка посредством нажатия кнопки **Обзор.**

Опции поиска:

Введенное имя задает ключевой контейнер – переключатель устанавливается в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер.

Выберите CSP для поиска ключевых контейнеров - необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

Можно также выбрать контейнер, соответствующий установленному в системе сертификату. Для этого вместо кнопки **Обзор** нужно нажать **По сертификату** и выбрать из списка сертификатов, установленных в личные хранилища пользователя или, если есть права администратора, локального компьютера, тот, контейнер которого необходимо протестировать;

После того, как все поля заполнены, нажмите кнопку **Далее**.

Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Система отобразит итоговое окно мастера «Тестирование контейнера закрытого ключа» (см. Рис. 3), в котором будет выведена информация о данном контейнере и результат теста.

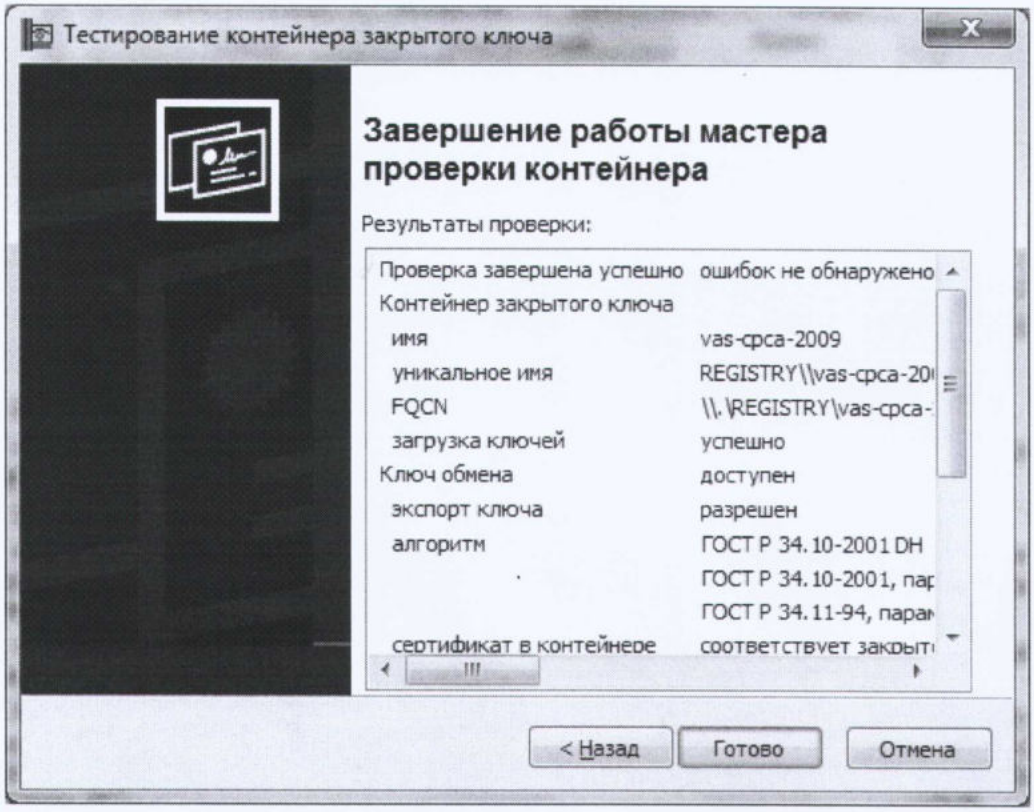


Рис. 3. Итоговое окно «Тестирование контейнера закрытого ключа»

Установка личного сертификата, хранящегося в контейнере закрытого ключа

Примечание. В данном разделе руководства под установкой личного сертификата понимается установка сертификата в хранилище **Личные** с формированием ссылки на закрытый ключ, соответствующий данному сертификату

Реализация КриптоПро CSP позволяет хранить личные сертификаты пользователя не только в локальном справочнике сертификатов компьютера, а так же вместе с личными ключами пользователя на ключевом носителе (при условии, что ключевой носитель имеет достаточный объем памяти для записи сертификата). Хранение сертификата на ключевом носителе позволяет пользователю переносить всю необходимую ключевую информацию с компьютера, где был сформирован ключ пользователя на другие рабочие места.

Для того чтобы воспользоваться личными ключами и сертификатами пользователя в различных приложениях на другом компьютере, необходимо на этом компьютере установить пользовательский сертификат в локальных справочник и создать ссылку, которая будет однозначно связывать сертификат с личным ключом пользователя.

Для того чтобы установить личный сертификат, выполните последовательность действий:

Для того чтобы просмотреть сертификат, хранящийся в контейнере закрытого ключа, в меню выполните Пуск ⇒ Программы ⇒ КриптоПро PKI ⇒ КриптоПро CSP. В контекстном меню раздела выберите Свойства, вкладку Сервис, нажмите кнопку Просмотреть сертификаты в контейнере.

В окне просмотра свойств сертификата нажмите кнопку **Установить сертификат**.

Осуществится запуск **Мастера импорта сертификатов** (см. Рис. 4).

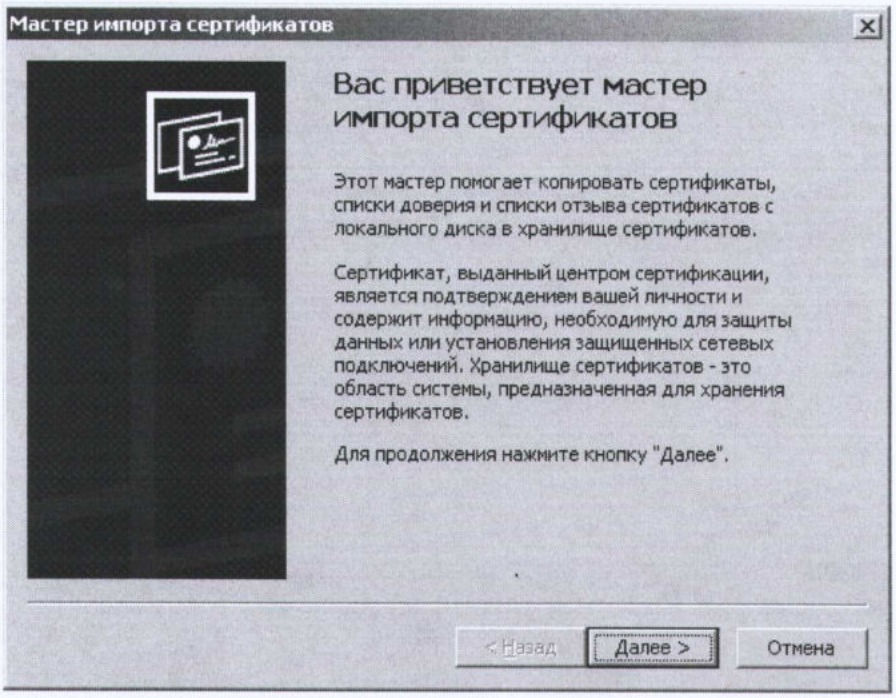


Рис. 4. Запуск мастера импорта сертификатов

Нажмите кнопку **Далее**. Система отобразит окно «Хранилище сертификатов», в котором необходимо указать, в какое хранилище требуется поместить сертификат (см. Рис. 5).

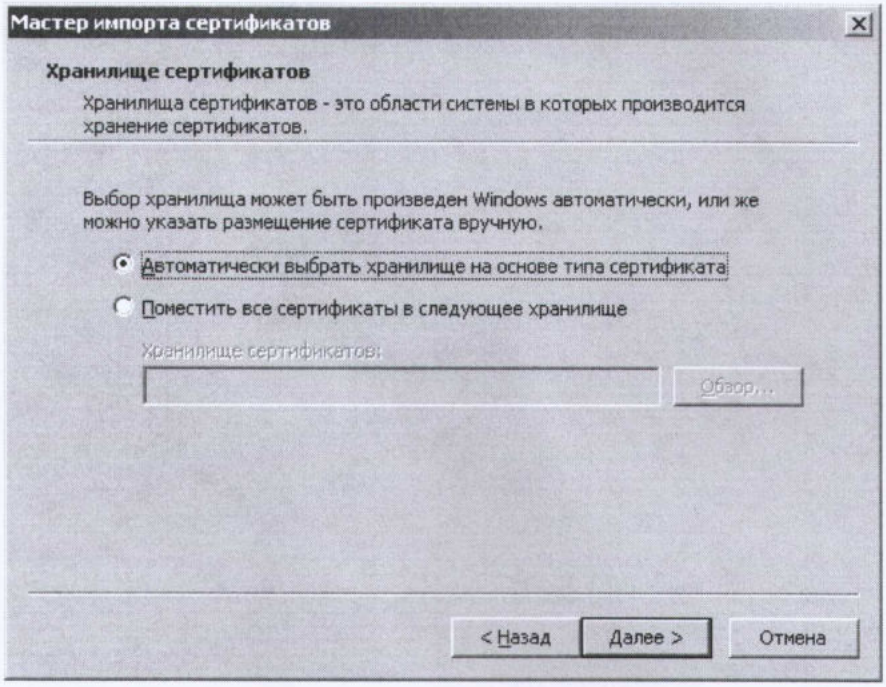


Рис. 5. Окно «Хранилище сертификатов»

Установите переключатель **Автоматически выбрать хранилище на основе типа сертификата**.

Внимание! Сертификат будет установлен в хранилище **Текущий пользователь/Личные** независимо от того, где расположен контейнер закрытого ключа. При необходимости установки сертификата в хранилище **Локальный компьютер/Личные** следует использовать кнопку **Установить личный сертификат**.

После выполненных действий нажмите кнопку **Далее.**

Система отобразит окно «Завершение работы мастера импорта сертификатов» (см. Рис. 6).

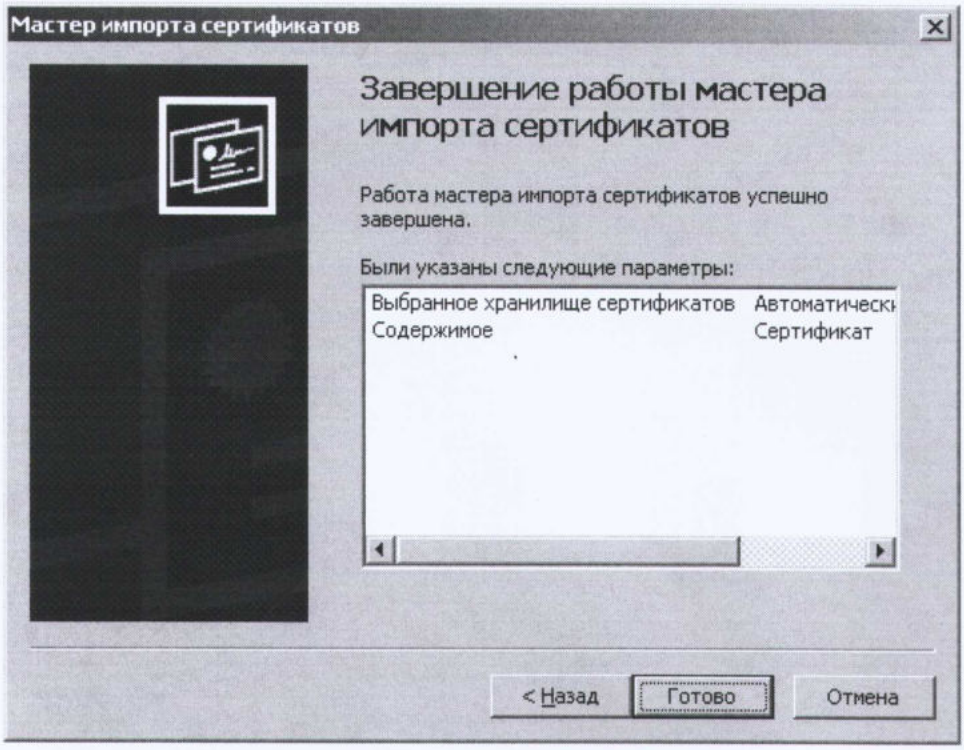


Рис. 6. Завершение мастера импорта сертификатов

Проверьте правильность выбранных параметров и нажмите кнопку **Готово.** Система отобразит окно, информирующее пользователя об успешной установке сертификата (см. Рис. 7)

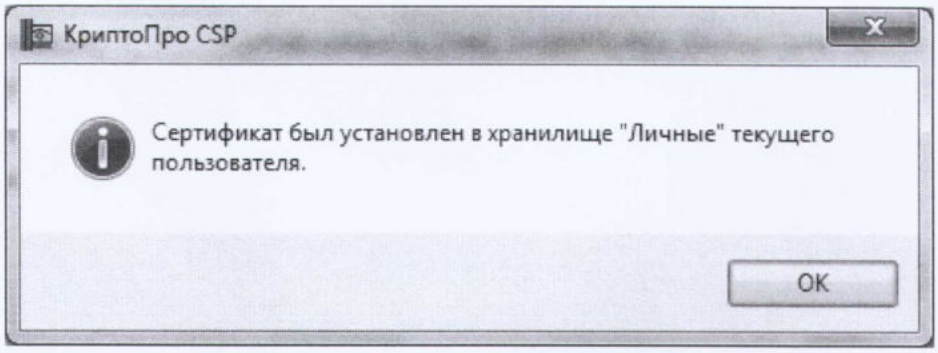


Рис. 7. Успешное выполнение импорта

Установка личного сертификата, хранящегося в файле

Примечание. В данном разделе инструкции под установкой личного сертификата понимается установка сертификата в хранилище **Личные** с формированием ссылки на закрытый ключ, соответствующий данному сертификату.

Для того чтобы установить личный сертификат в меню, выполните **Пуск ⇒ Программы ⇒ КриптоПро PKI ⇒ КриптоПро CSP.** В контекстном меню раздела выберите **Свойства,** вкладку **Сервис** (, нажмите кнопку **Установить личный сертификат**.

Система отобразит окно «Мастер установки личного сертификата» (см. Рис. 8). Ознакомьтесь с текстом и нажмите кнопку **Далее.**

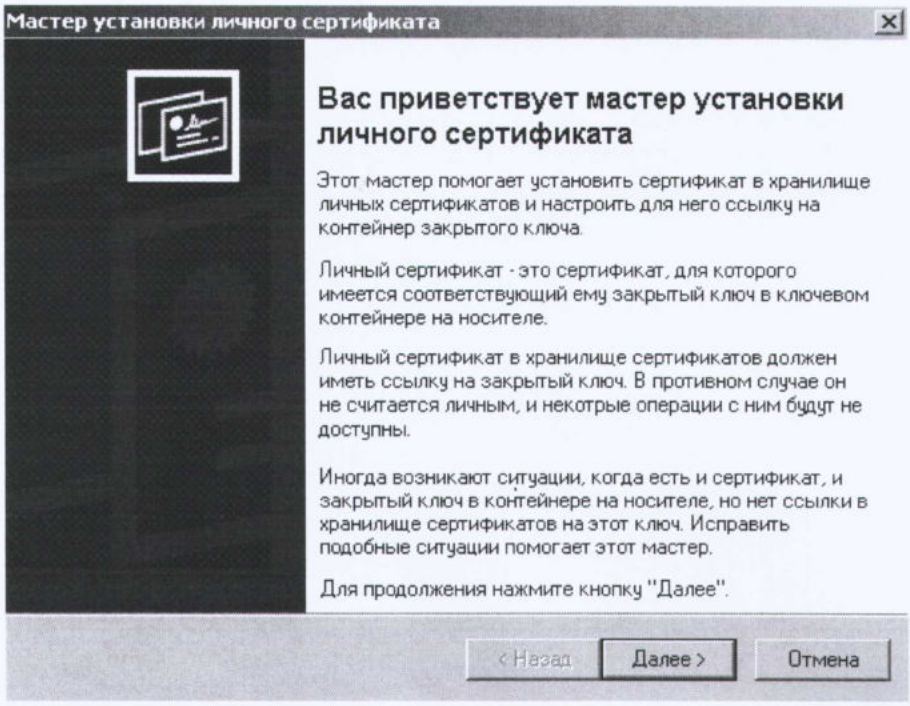


Рис. 8. Окно «Мастер установки личного сертификата»

Система отобразит окно «Расположение файла сертификата» (см. Рис. 9). В поле **Имя файла сертификата** укажите полный путь к этому файлу (удобно воспользоваться кнопкой **Обзор**) и нажмите кнопку **Далее.**

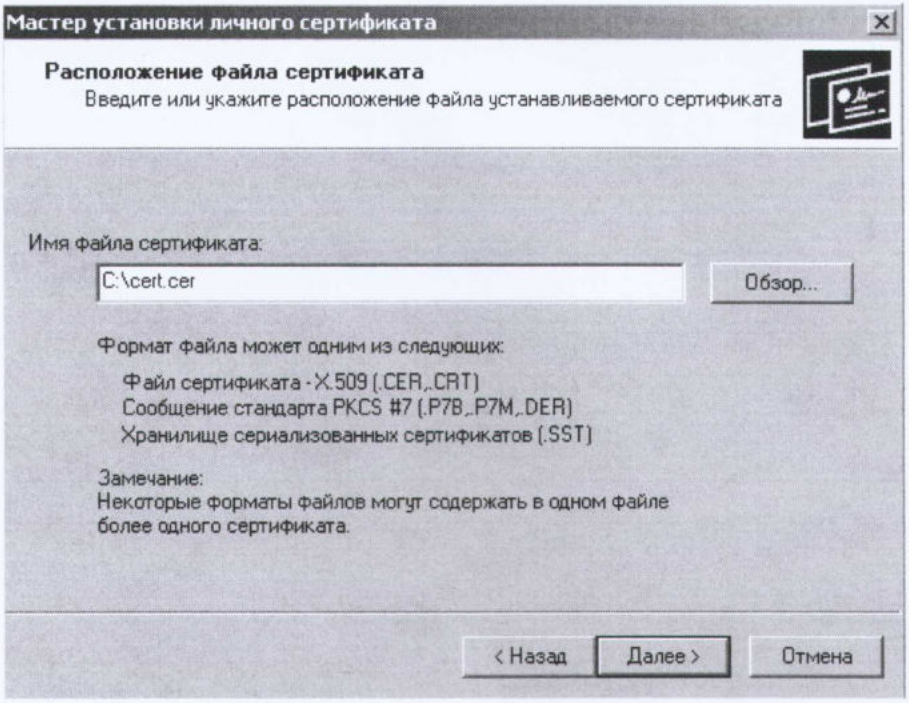


Рис. 9. Окно «Расположение файлов сертификата»

Система перейдет к окну «Сертификат для установки» (см. Рис. 10). В нем выводится основная информация о сертификате. Нажав на кнопку **Свойства** можно просмотреть подробную информацию о сертификате в стандартном окне просмотра свойств сертификата.

Рис. 10. Окно «Сертификат для установки»

Нажмите кнопку Далее. Система отобразит окно «Контейнер закрытого ключа» (см. Рис. 11).

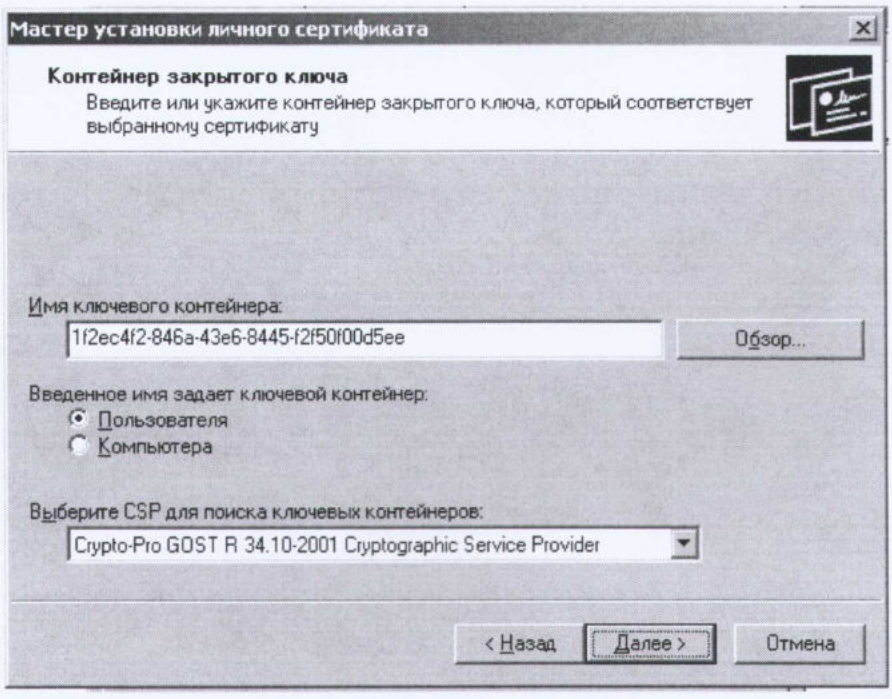


Рис. 11. Окно «Контейнер закрытого ключа»

В нем необходимо заполнить следующие поля ввода:

Имя ключевого контейнера – вводится вручную или выбирается из списка посредством нажатия кнопки **Обзор**;

Введенное имя задает ключевой контейнер – переключатель устанавливается в положение **Пользователь** или **Компьютер,** в зависимости от того, в каком хранилище расположен контейнер;

Выберите CSP для поиска ключевых контейнеров - необходимый криптопровайдер (CSP) выбирается из предлагаемого списка.

После того, как все поля заполнены, нажмите кнопку **Далее**.

Если на доступ к закрытому ключу установлен пароль, то система попросит ввести его. Введите пароль и нажмите кнопку **ОК**.

Система отобразит окно «Хранилище сертификатов» (см. Рис. 12).

С помощью кнопки **Обзор** выберите хранилище **Личные**. Сертификат будет установлен в хранилище **Текущий пользователь/Личные** или **Локальный компьютер/Личные** в зависимости от значения переключателя **Пользователь/Компьютер**. Изменить значение переключателя **Пользователь/Компьютер** нельзя; оно определяется расположением контейнера закрытого ключа (см. предыдущий пункт)

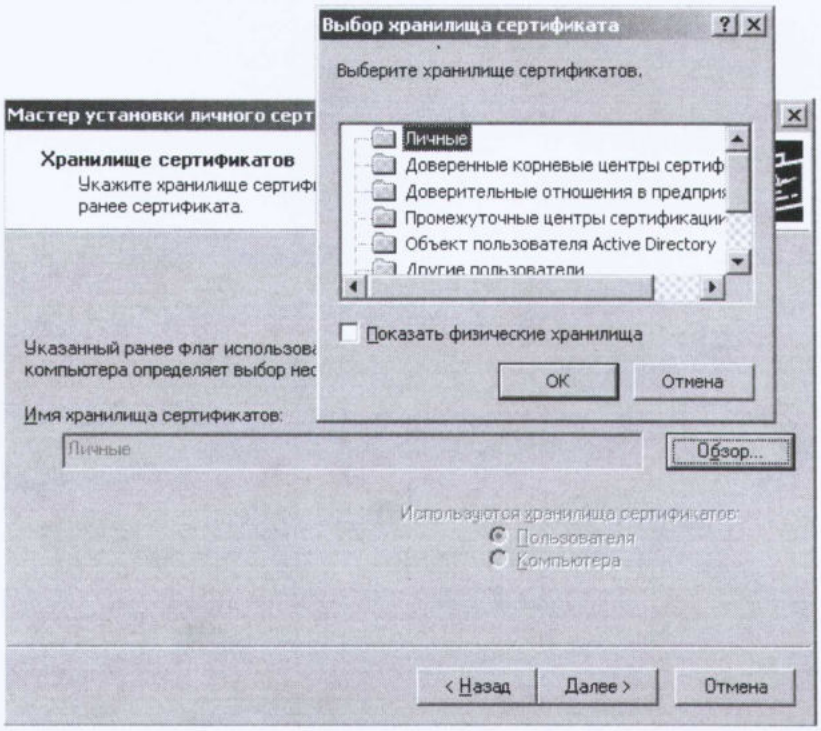


Рис. 12. Окно «Хранилище сертификатов»

После выбора хранилища система отобразит окно «Завершение работы мастера установки личного сертификата» (см. Рис. 13).

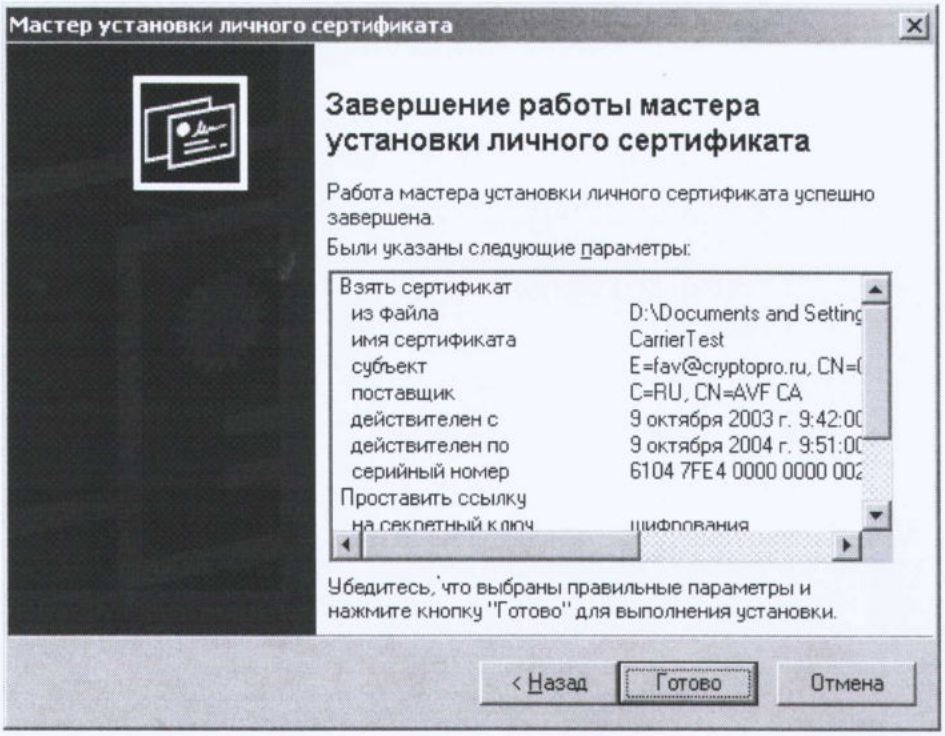


Рис. 13. Завершение работы мастера установки личного сертификата

Проверьте правильность указанных данных и нажмите кнопку **Готово.** СКЗИ «КриптоПро CSP» произведет установку сертификата.

Начальник ОИБ М.Е. Коршунов