

3.2.1.1 Удаленный доступ к сетям VPN

Для настройки необходим компьютер с установленной операционной системой **Windows XP Rus** и **драйверами РутOKEN**.

При установке удаленного подключения к серверу удаленного доступа происходит аутентификация клиента сервером, и, наоборот, клиент проверяет, что подключается именно к тому серверу, к которому нужно. Однако есть возможность отключить проверку клиентом сервера, что отрицательно скажется на безопасности соединения, поэтому рекомендуется проверять сервер.

Настройка удаленного доступа к сетям VPN состоит из следующих этапов:

1 этап: Установка сертификата Центра сертификации.

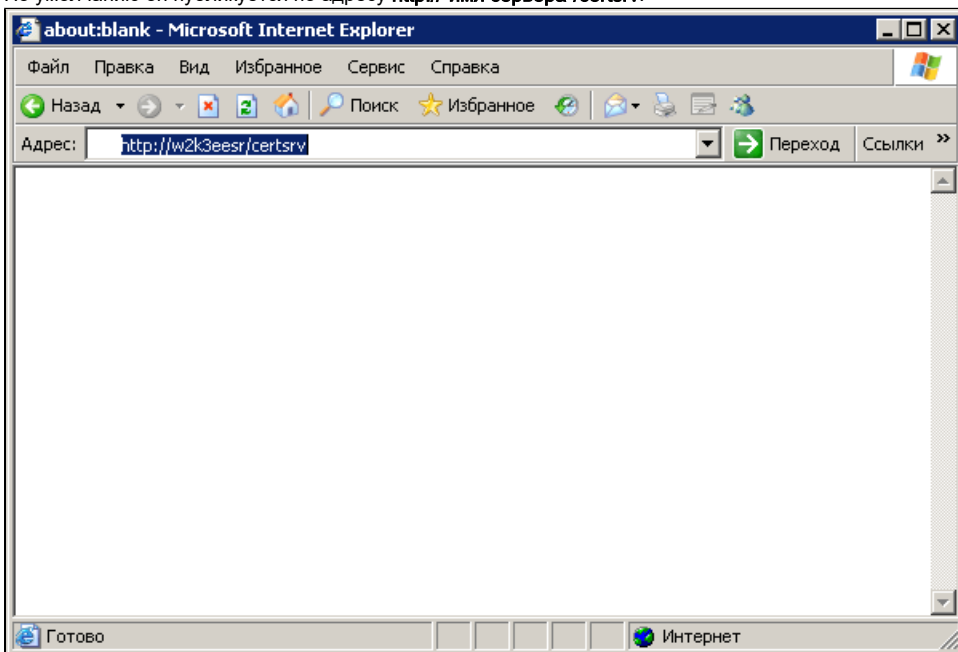
2 этап: Создание и настройка удаленного подключения к сети VPN.

Установка сертификата Центра сертификации

Установка сертификата **Центра сертификации** обеспечит доверие этому **Центру сертификации**. Установить сертификат в ОС **Windows XP Rus** имеет право только локальный администратор в системе.

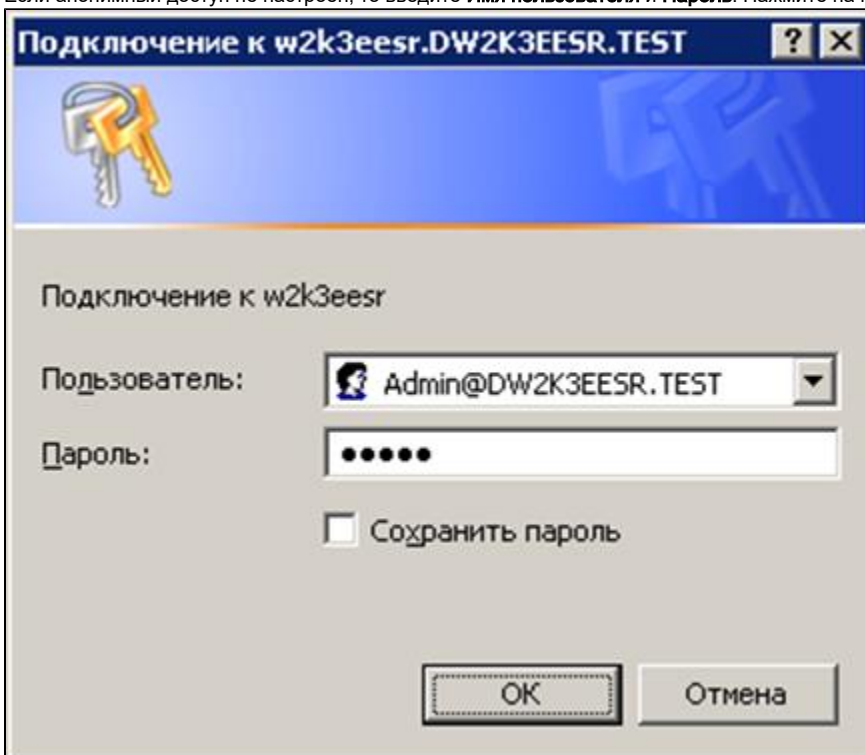
Для установки сертификата Центра сертификации:

1. Введите в адресной строке адрес **Центра сертификации**.
По умолчанию он публикуется по адресу **http://имя сервера/certsrv**.

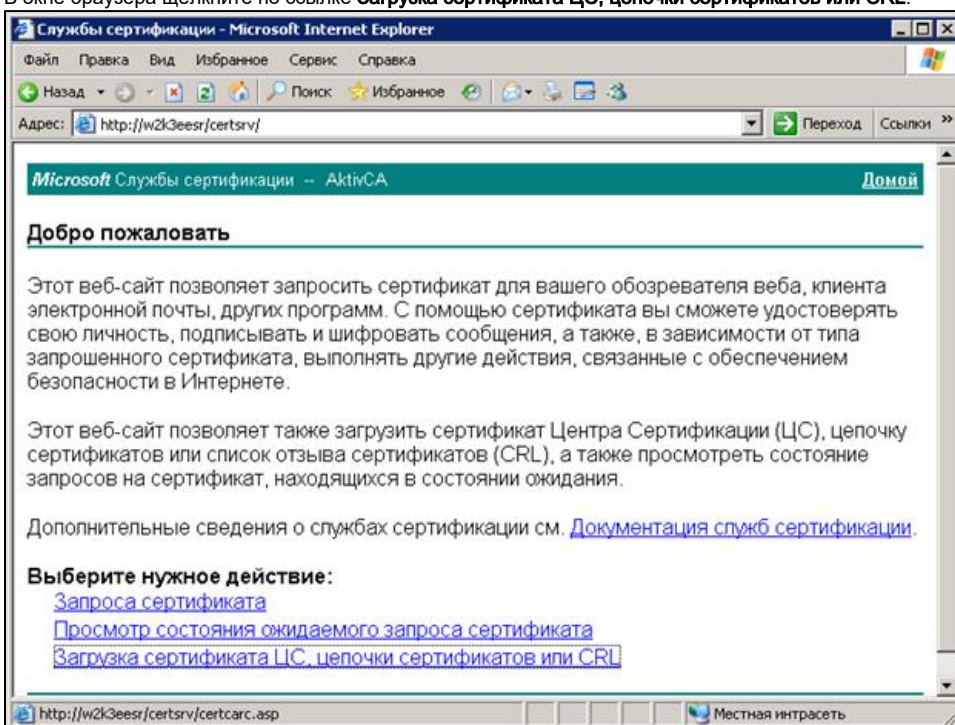


2. Нажмите на клавишу **[Enter]**.

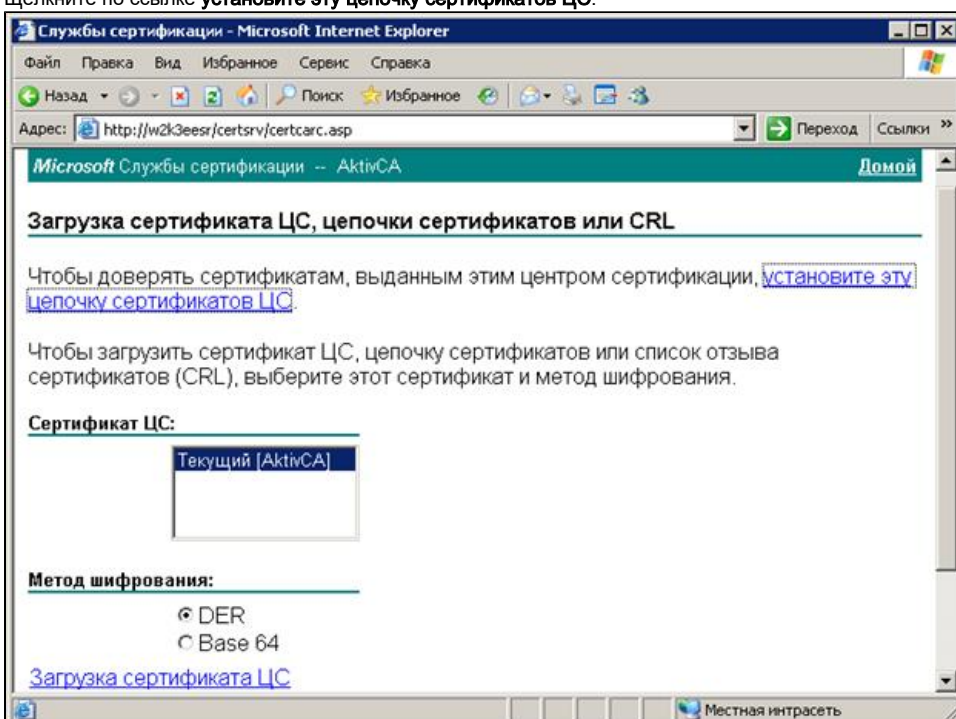
3. Если анонимный доступ не настроен, то введите **Имя пользователя** и **Пароль**. Нажмите на кнопку [OK].



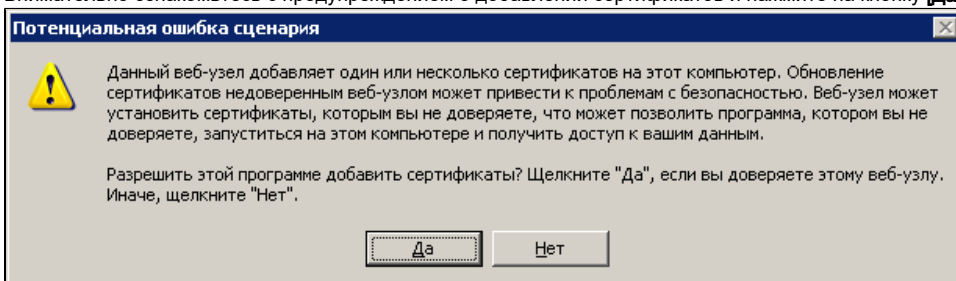
4. В окне браузера щелкните по ссылке **Загрузка сертификата ЦС, цепочки сертификатов или CRL**.



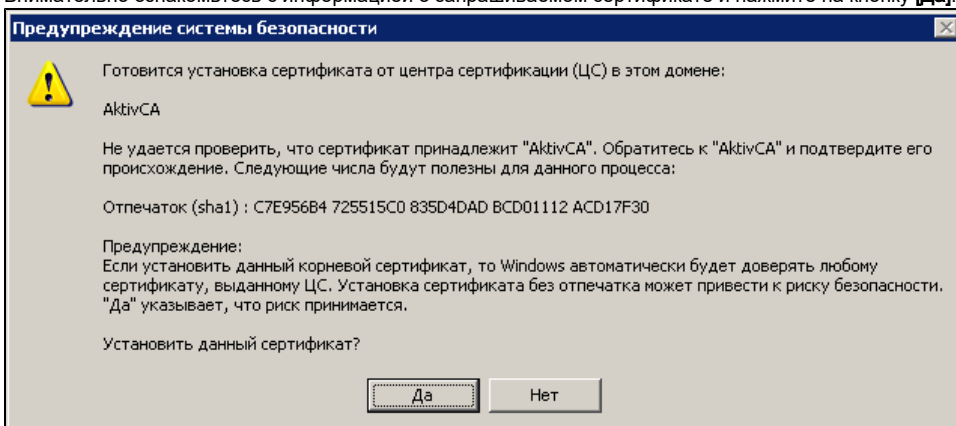
5. Щелкните по ссылке **установите эту цепочку сертификатов ЦС**.



6. Внимательно ознакомьтесь с предупреждением о добавлении сертификатов и нажмите на кнопку **Да**.

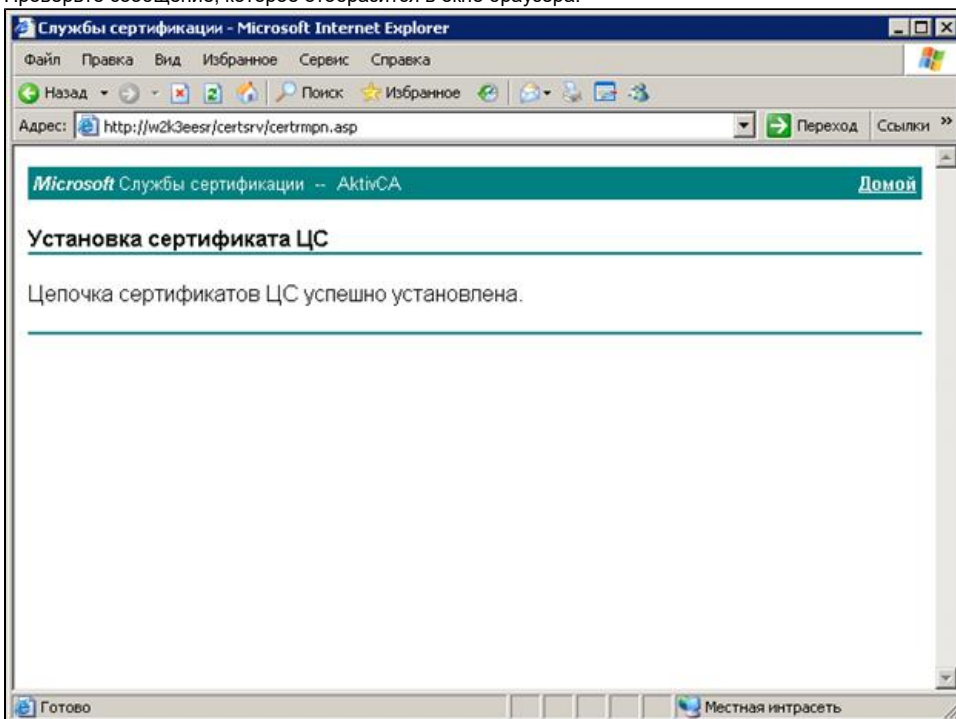


7. Внимательно ознакомьтесь с информацией о запрашиваемом сертификате и нажмите на кнопку **Да**.



8. Дождитесь окончания процесса установки сертификата.

9. Проверьте сообщение, которое отобразится в окне браузера.



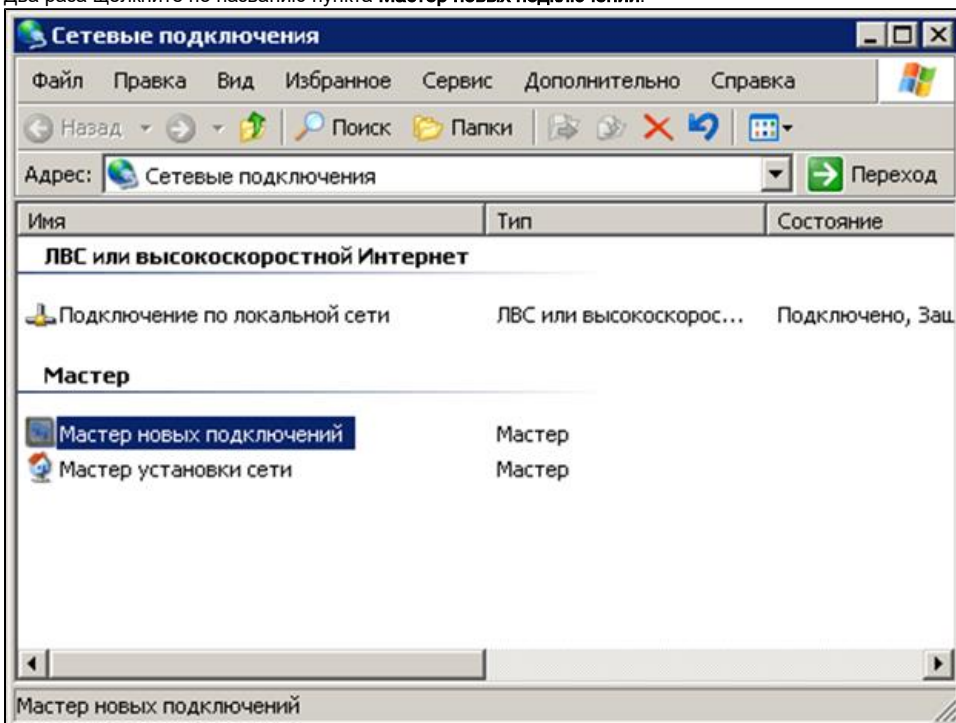
10. Если установка прошла успешно, то закройте окно браузера. В противном случае повторите процедуру, описанную в данном разделе.

Создание и настройка удаленного подключения к сети VPN

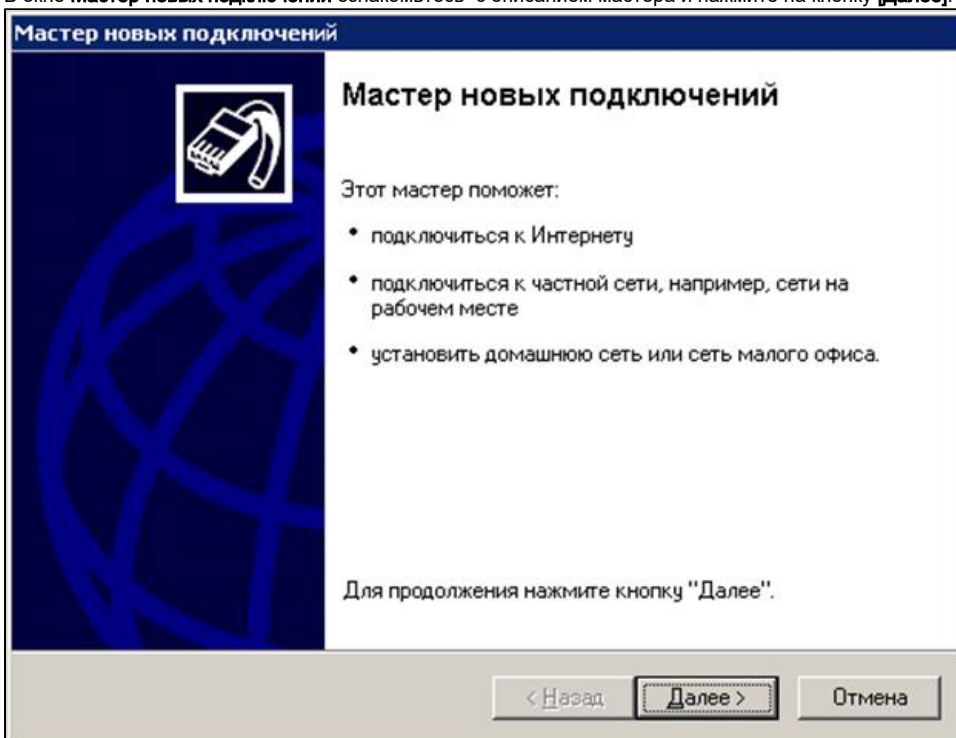
После того как сертификат **Центра сертификации** установлен, можно создавать удаленное подключение к сети VPN.

Для создания и настройки удаленного подключения к сети VPN:

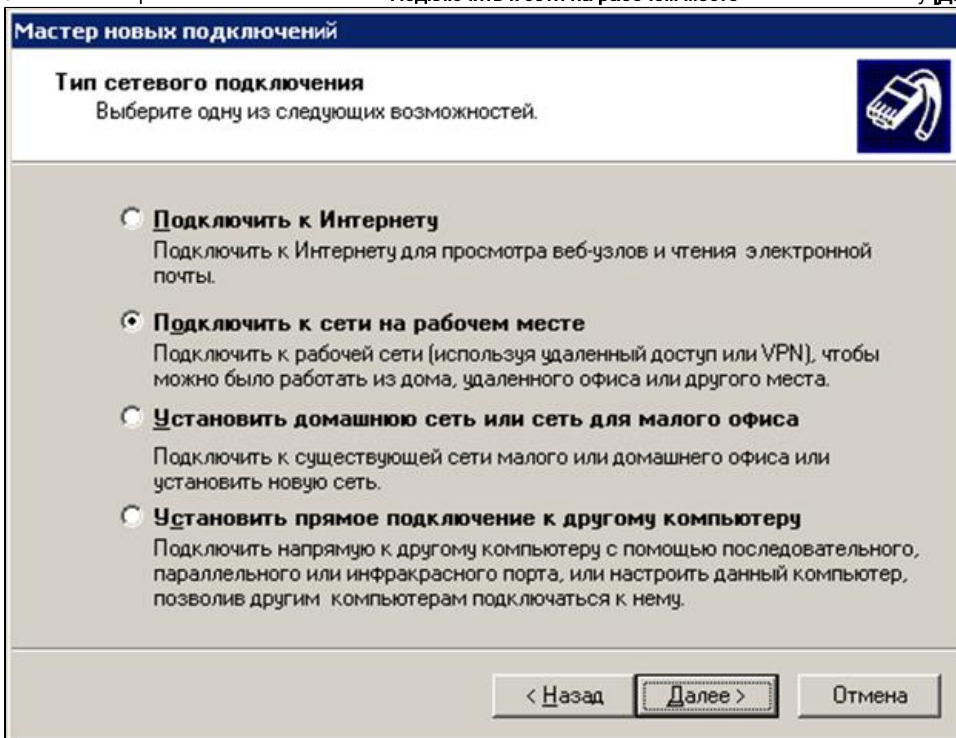
1. Откройте **Панель управления**.
2. Два раза щелкните по названию пункта **Сетевые подключения**.
3. Два раза щелкните по названию пункта **Мастер новых подключений**.



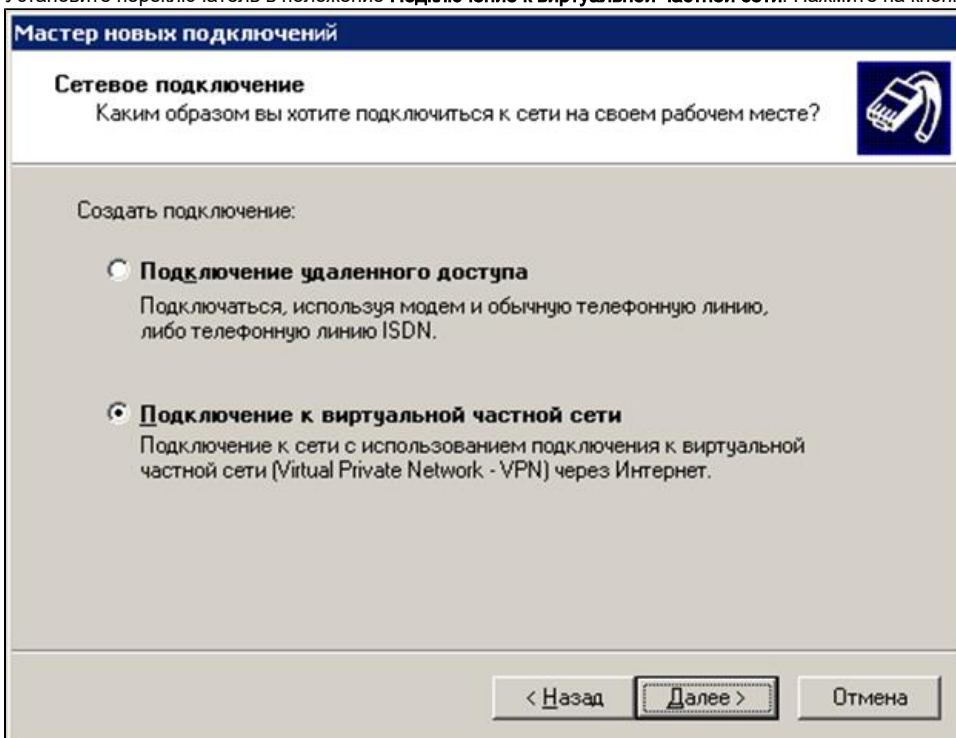
4. В окне **Мастер новых подключений** ознакомьтесь с описанием мастера и нажмите на кнопку **[Далее]**.



5. Установите переключатель в положение **Подключить к сети на рабочем месте**. Нажмите на кнопку **[Далее]**.



6. Установите переключатель в положение **Подключение к виртуальной частной сети**. Нажмите на кнопку **[Далее]**.



Мастер новых подключений

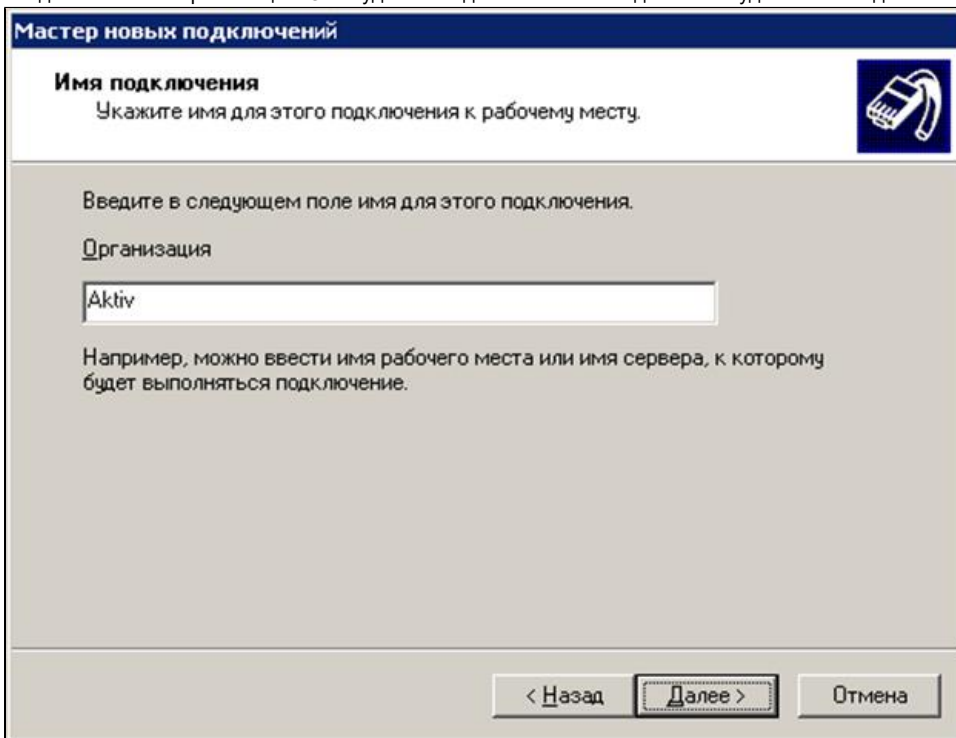
Сетевое подключение
Каким образом вы хотите подключиться к сети на своем рабочем месте?

Создать подключение:

- ☐ **Подключение удаленного доступа**
Подключаться, используя модем и обычную телефонную линию, либо телефонную линию ISDN.
- ☒ **Подключение к виртуальной частной сети**
Подключение к сети с использованием подключения к виртуальной частной сети (Virtual Private Network - VPN) через Интернет.

< Назад **Далее >** Отмена

7. Введите название организации. Оно будет совпадать с именем создаваемого удаленного подключения.



Мастер новых подключений

Имя подключения
Укажите имя для этого подключения к рабочему месту.

Введите в следующем поле имя для этого подключения.

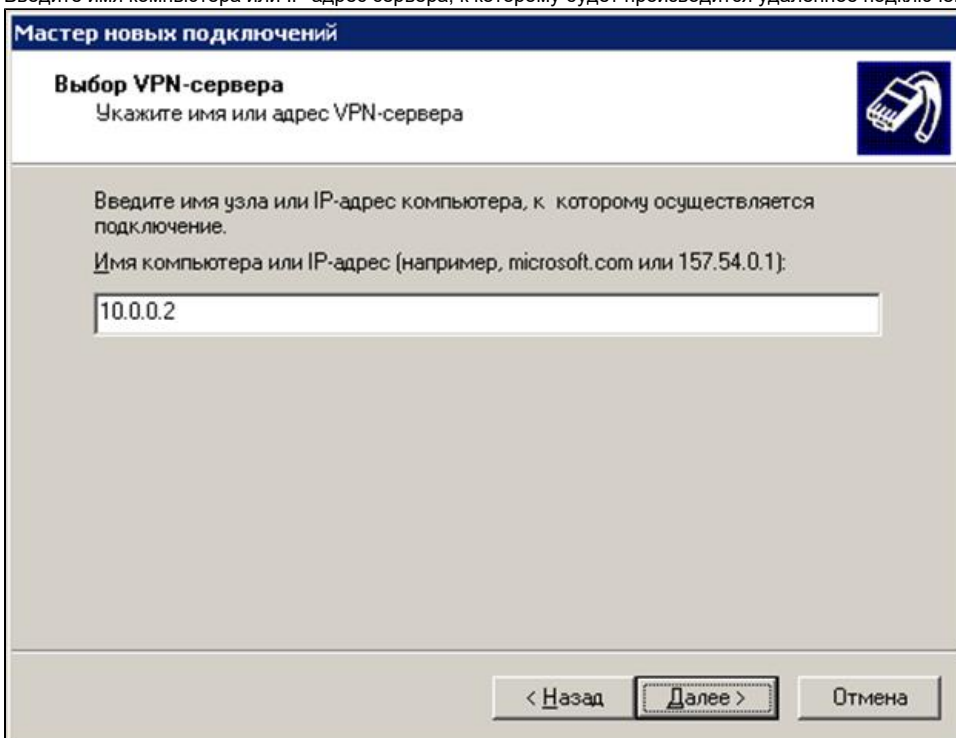
Организация

Aktiv

Например, можно ввести имя рабочего места или имя сервера, к которому будет выполняться подключение.

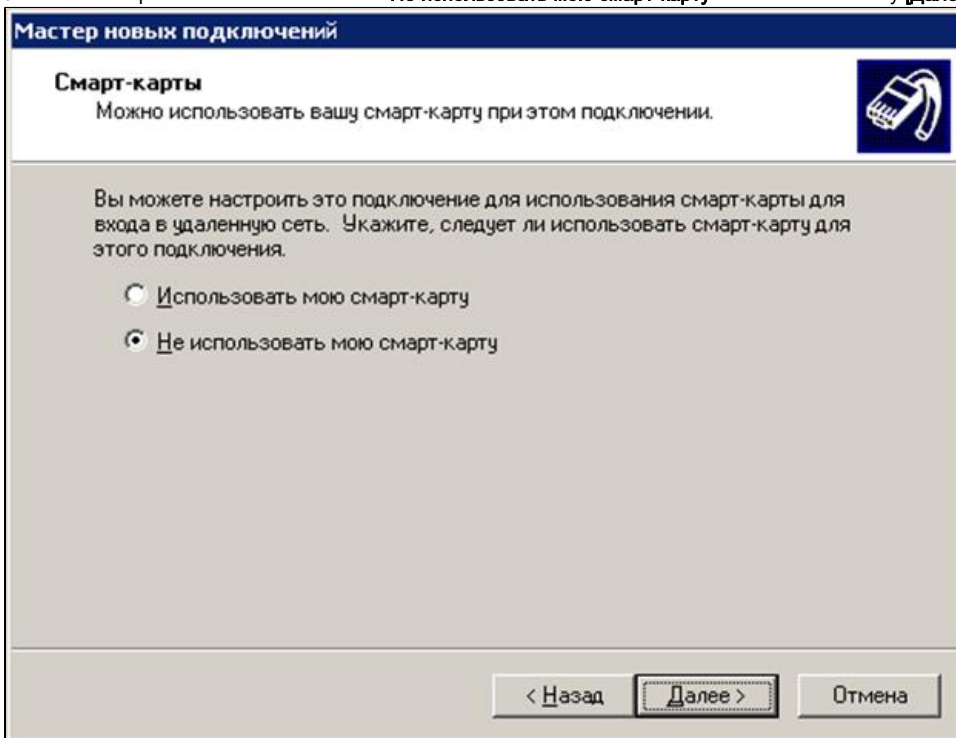
< Назад **Далее >** Отмена

8. Введите имя компьютера или IP-адрес сервера, к которому будет производиться удаленное подключение. Нажмите на кнопку **[Далее]**.



The screenshot shows a Windows XP-style dialog box titled "Мастер новых подключений" (Master of new connections). The main heading is "Выбор VPN-сервера" (VPN server selection). Below it, the text says "Укажите имя или адрес VPN-сервера" (Specify the name or address of the VPN server). A larger instruction reads: "Введите имя узла или IP-адрес компьютера, к которому осуществляется подключение." (Enter the name of the node or IP address of the computer to which the connection is made). Below this, a label says "Имя компьютера или IP-адрес (например, microsoft.com или 157.54.0.1):" (Computer name or IP address (for example, microsoft.com or 157.54.0.1):). A text input field contains "10.0.0.2". At the bottom, there are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel). The "Далее >" button is highlighted with a dashed border.

9. Установите переключатель в положение **Не использовать мою смарт-карту**. Нажмите на кнопку **[Далее]**.

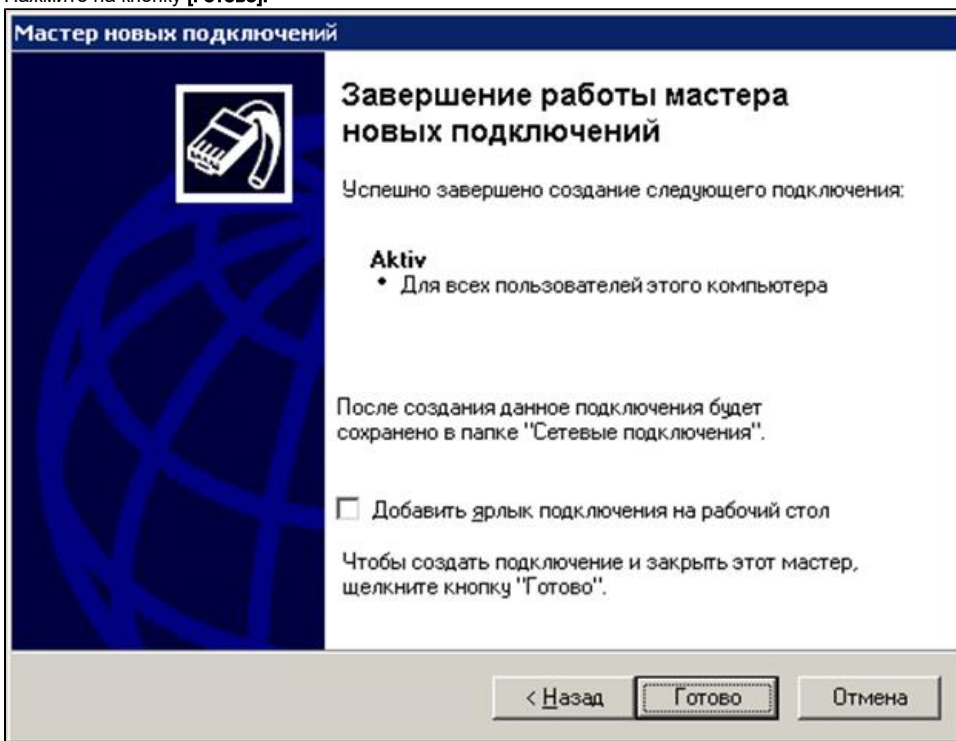


The screenshot shows the same "Мастер новых подключений" dialog box, but at the "Смарт-карты" (Smart cards) step. The heading is "Смарт-карты" and the text says "Можно использовать вашу смарт-карту при этом подключении." (You can use your smart card with this connection). A larger instruction reads: "Вы можете настроить это подключение для использования смарт-карты для входа в удаленную сеть. Укажите, следует ли использовать смарт-карту для этого подключения." (You can configure this connection for using a smart card to log on to the remote network. Specify whether to use a smart card for this connection). There are two radio button options: "Использовать мою смарт-карту" (Use my smart card) and "Не использовать мою смарт-карту" (Do not use my smart card). The second option is selected. At the bottom, there are three buttons: "< Назад" (Back), "Далее >" (Next), and "Отмена" (Cancel). The "Далее >" button is highlighted with a dashed border.

Эту опцию необходимо выбрать, так как параметры по умолчанию для смарт-карт не подходят для работы с устройством Рутокен.

10. В этом примере мы не создаем ярлык данного подключения на рабочем столе. Если вы хотите его создать, то установите галочку **Добавить ярлык подключения на рабочем столе**.

11. Нажмите на кнопку **[Готово]**.



После создания удаленного подключения необходимо настроить его для работы с устройством Рутокен.

Для настройки удаленного подключения к сети VPN:

1. Откройте окно подключения.

2. Нажмите на кнопку **[Свойства]**.

Подключение: Aktiv



Пользователь: Admin

Пароль:

☐ Сохранять имя пользователя и пароль:

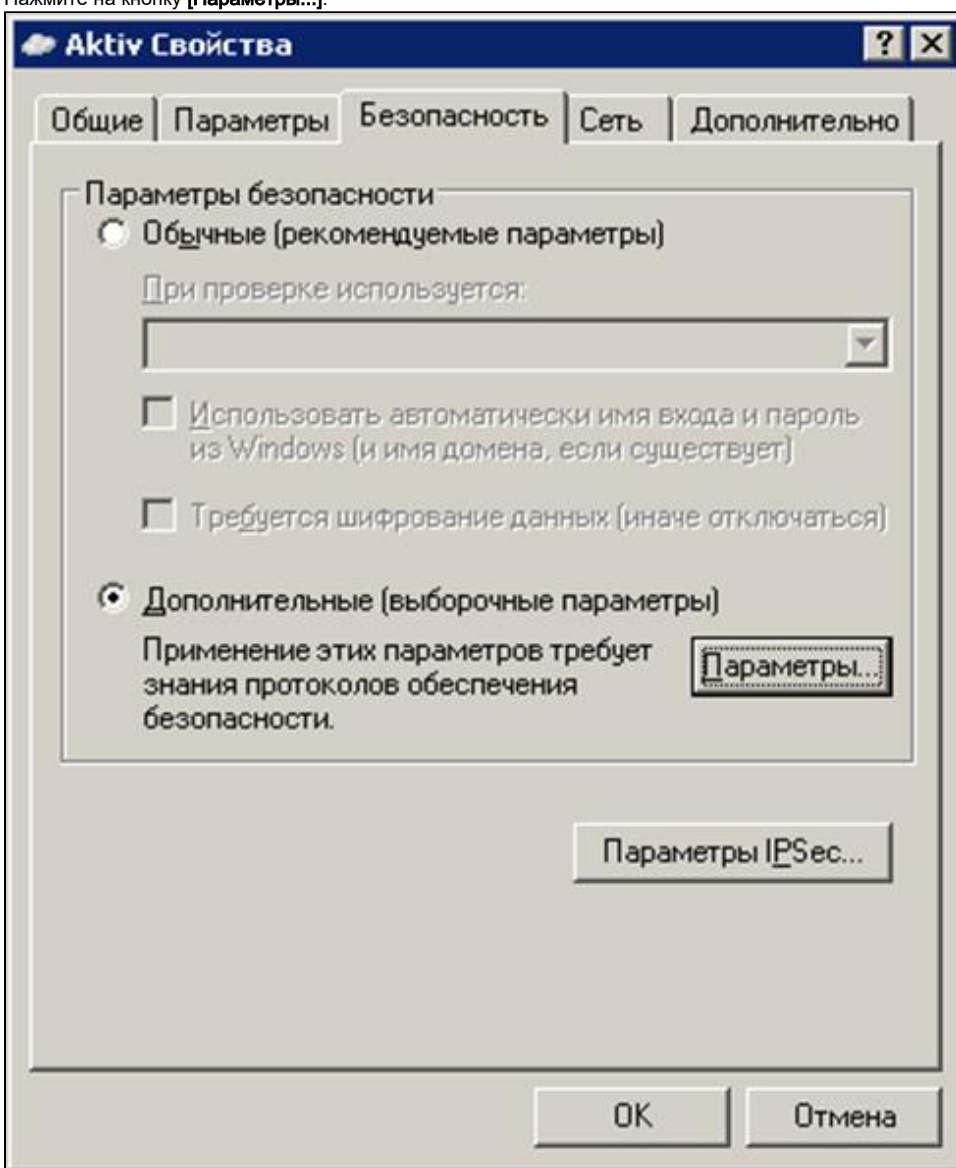
☒ только для меня

☐ для любого пользователя

Подключение Отмена **Свойства** Справка

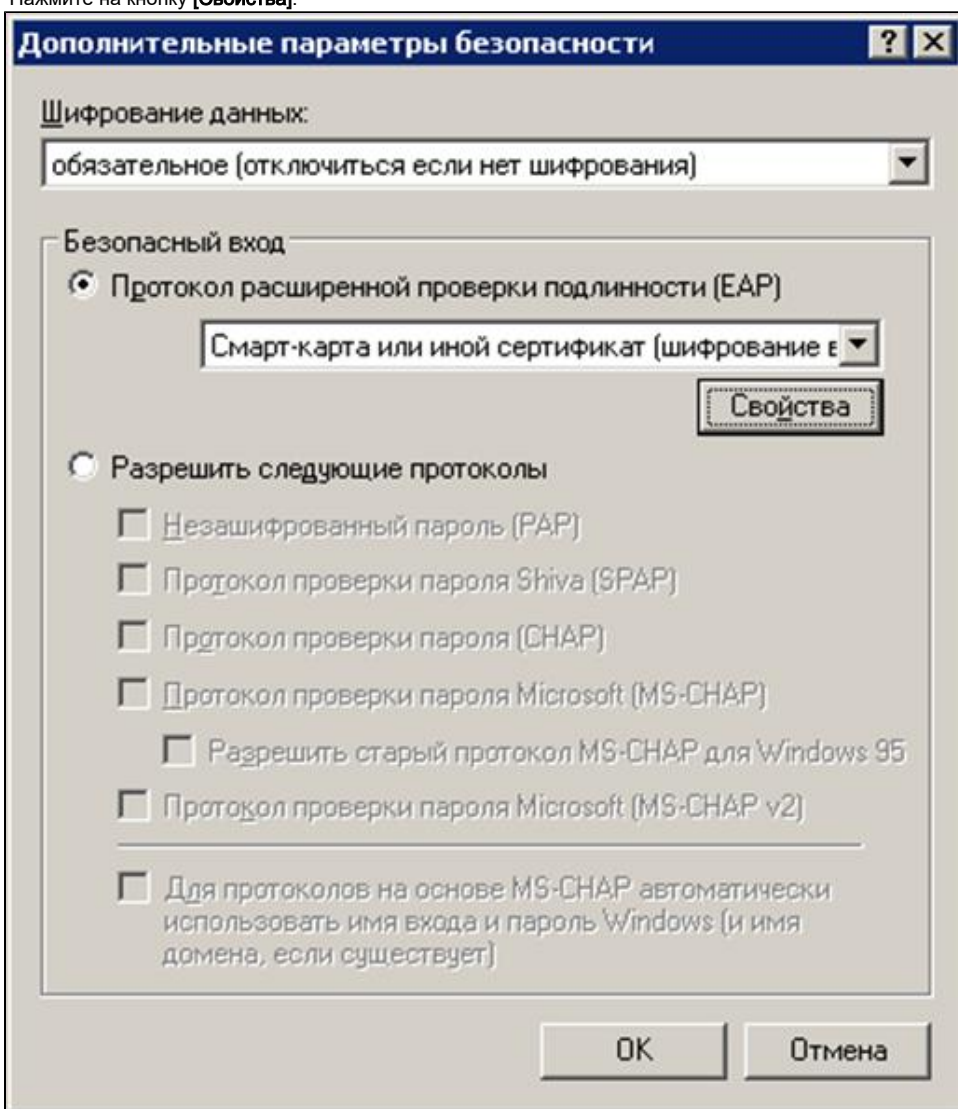
3. Перейдите на вкладку **Безопасность**.
4. Установите переключатель в положение **Дополнительные (выборочные параметры)**.

5. Нажмите на кнопку [Параметры...].



6. В окне **Дополнительные параметры безопасности** установите переключатель в положение **Протокол расширенной проверки подлинности (EAP)**.

7. Нажмите на кнопку [Свойства].

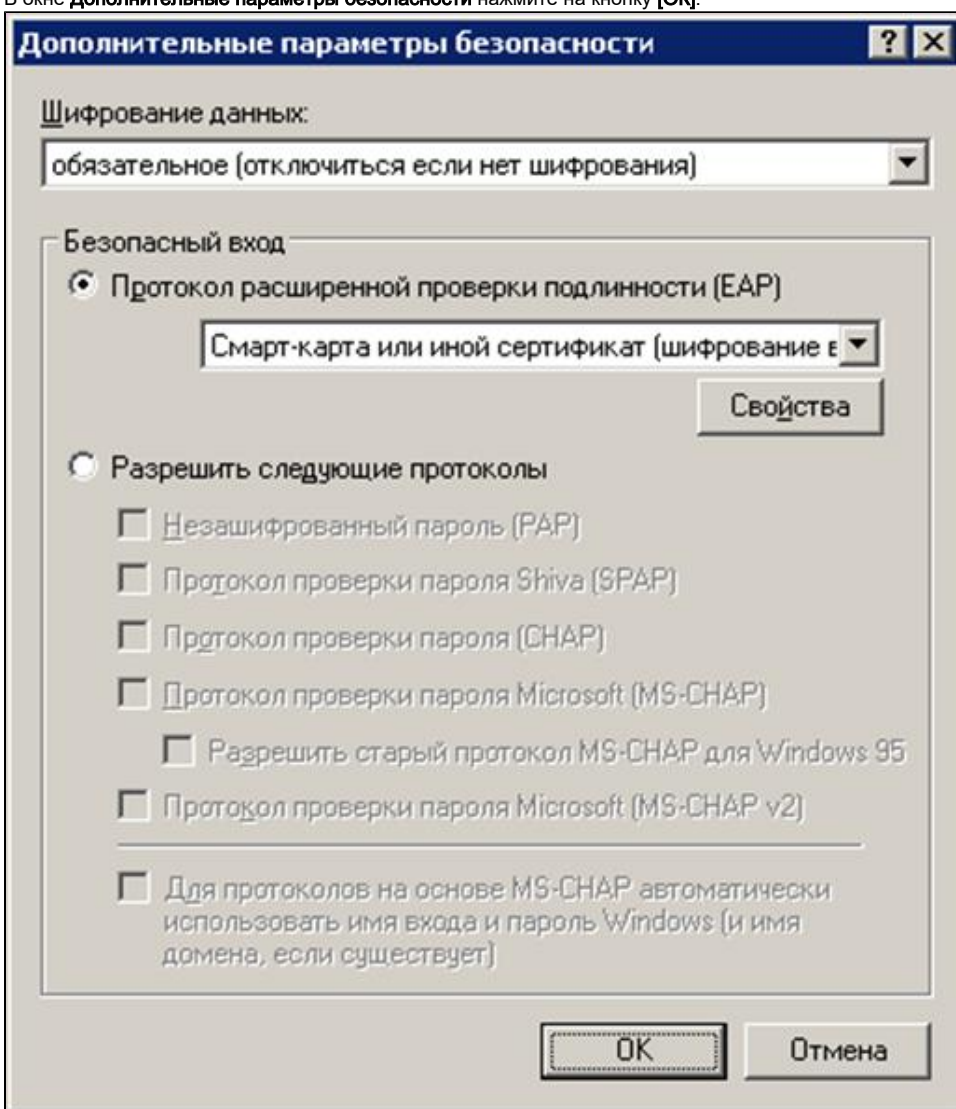


8. В окне **Свойства смарт-карты или другого сертификата** в секции **Доверенные корневые центры сертификации** установите флажок **AktivCA**. Нажмите на кнопку **[OK]**.

The image shows a Windows XP-style dialog box titled "Свойства смарт-карты или другого сертификата". It contains several sections for configuring smart card or certificate properties.

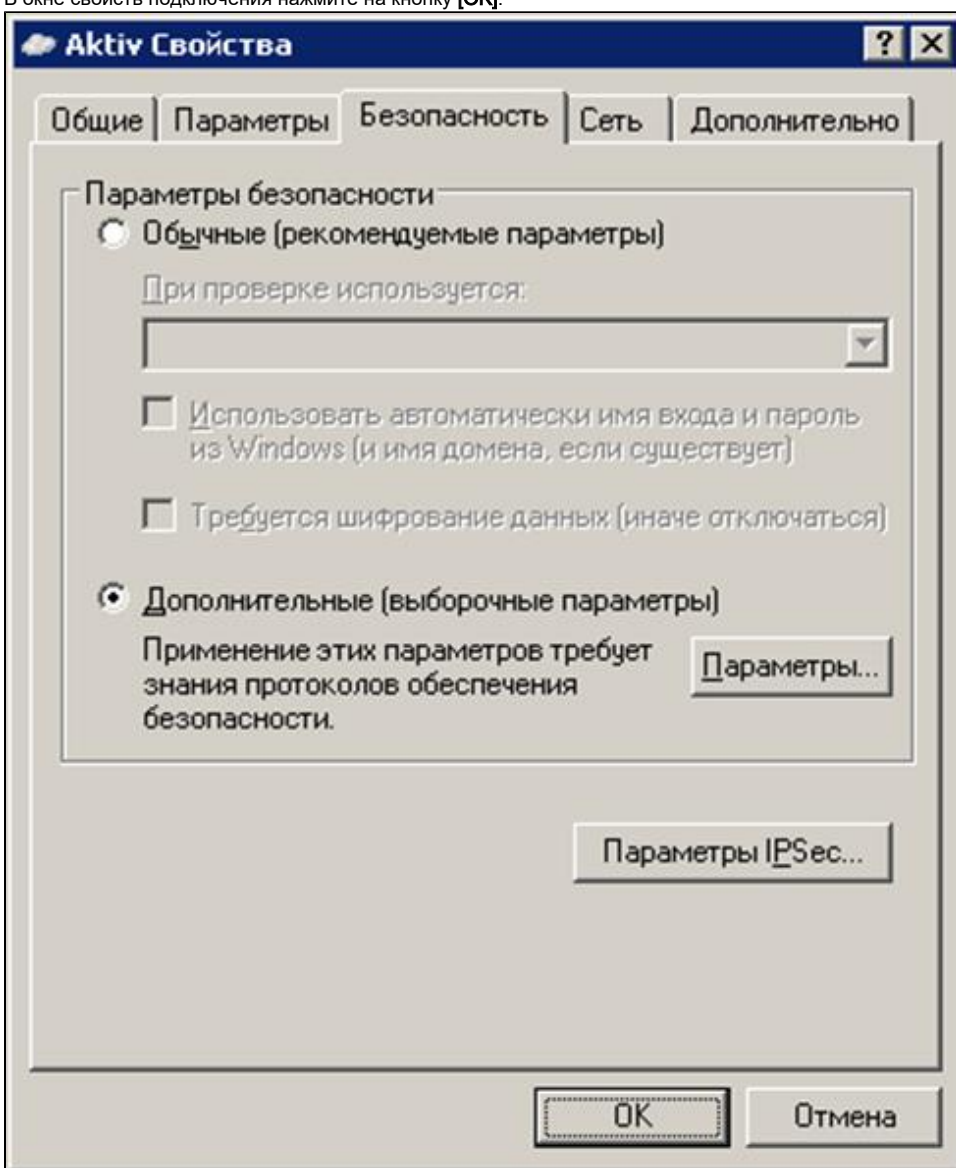
- При подключении:** (When connected) section with two radio buttons:
 - ☒ использовать мою смарт-карту (use my smart card)
 - ☐ использовать сертификат на этом компьютере (use certificate on this computer)A checkbox ☐ "Использовать выбор простого сертификата (рекоменд.)" (Use simple certificate selection (recommended)) is also present.
- Проверка сертификата сервера** (Server certificate verification) section with a checked checkbox ☒ "Подключение к серверам:" (Connection to servers:). Below it is an empty text input field.
- Доверенные корневые центры сертификации:** (Trusted root certification authorities) section containing a list box with the following items:
 - ☐ ABA.ECOM Root CA
 - ☒ AktivCA
 - ☐ Autoridad Certificadora de la Asociacion Nacional del Notariac
 - ☐ Autoridad Certificadora del Colegio Nacional de Correduria Pu
 - ☐ Baltimore EZ by DST
 - ☐ Belgacom E-Trust Primary CA
 - ☐ C&W HKT SecureNet CA Class A
 - ☐ C&W HKT SecureNet CA Class BBelow the list box is a "Просмотр сертификата" (View certificate) button.
- At the bottom, there is a checkbox ☐ "Использовать для подключения другое имя пользователя" (Use different user name for connection).
- At the very bottom are "OK" and "Отмена" (Cancel) buttons.

9. В окне **Дополнительные параметры безопасности** нажмите на кнопку **[ОК]**.

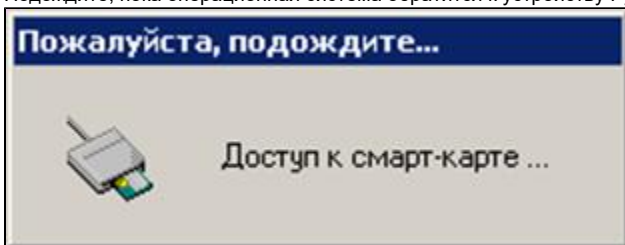


10. Подключите устройство Рутокен к компьютеру (на устройстве должен быть сертификат типа **Пользователь со смарт-картой**).

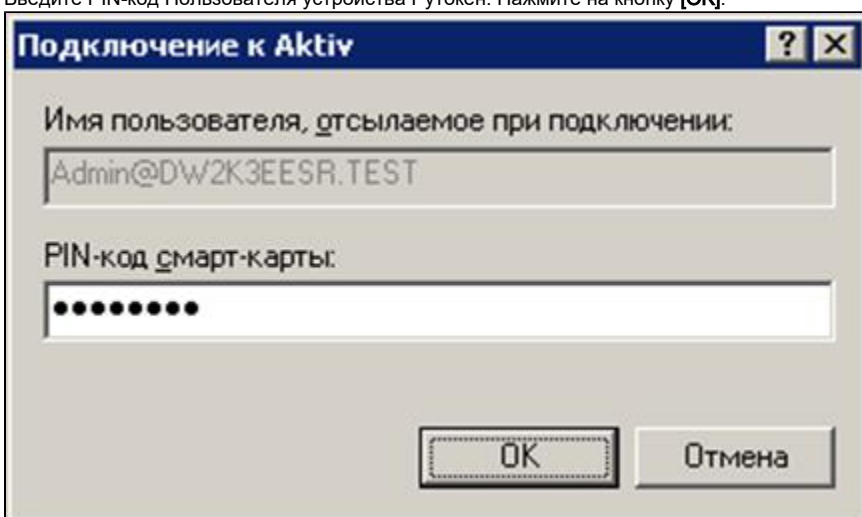
11. В окне свойств подключения нажмите на кнопку [OK].



12. Подождите, пока операционная система обратится к устройству Рутокен.



13. Введите PIN-код Пользователя устройства Рутокен. Нажмите на кнопку [OK].



Подключение к Aktiv

Имя пользователя, отправляемое при подключении:

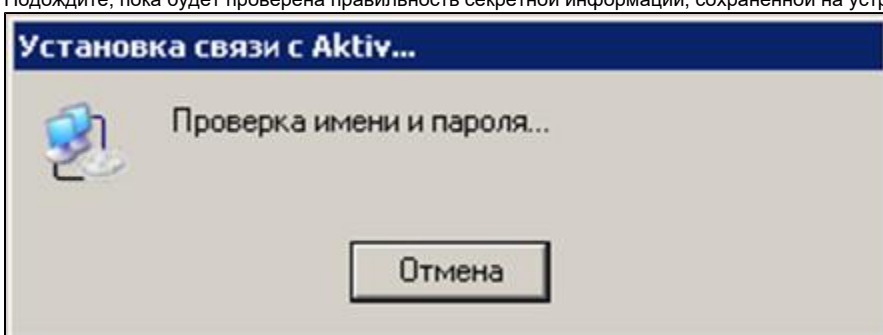
Admin@DW2K3EESR.TEST

PIN-код смарт-карты:

.....

OK Отмена

14. Подождите, пока будет проверена правильность секретной информации, сохраненной на устройстве Рутокен.

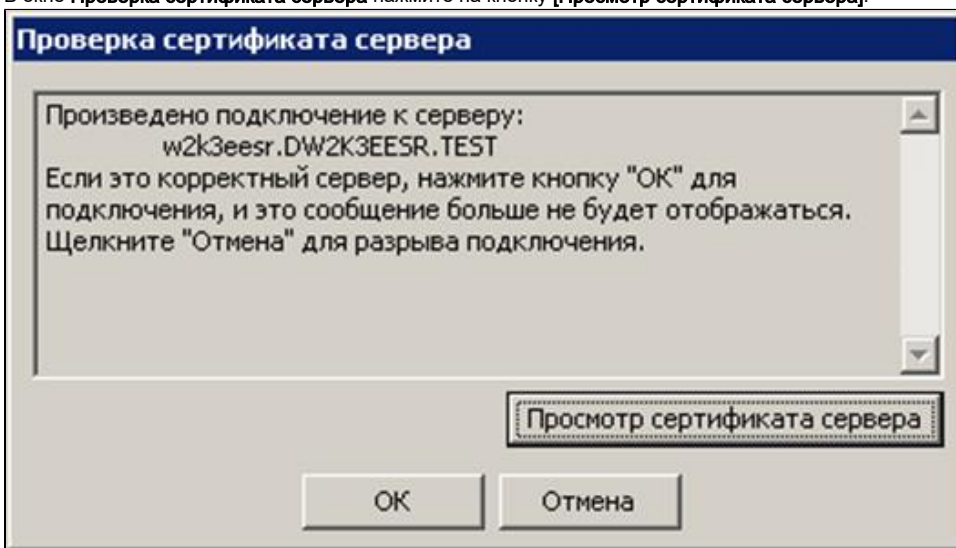


Установка связи с Aktiv...

Проверка имени и пароля...

Отмена

15. В окне Проверка сертификата сервера нажмите на кнопку [Просмотр сертификата сервера].



Проверка сертификата сервера

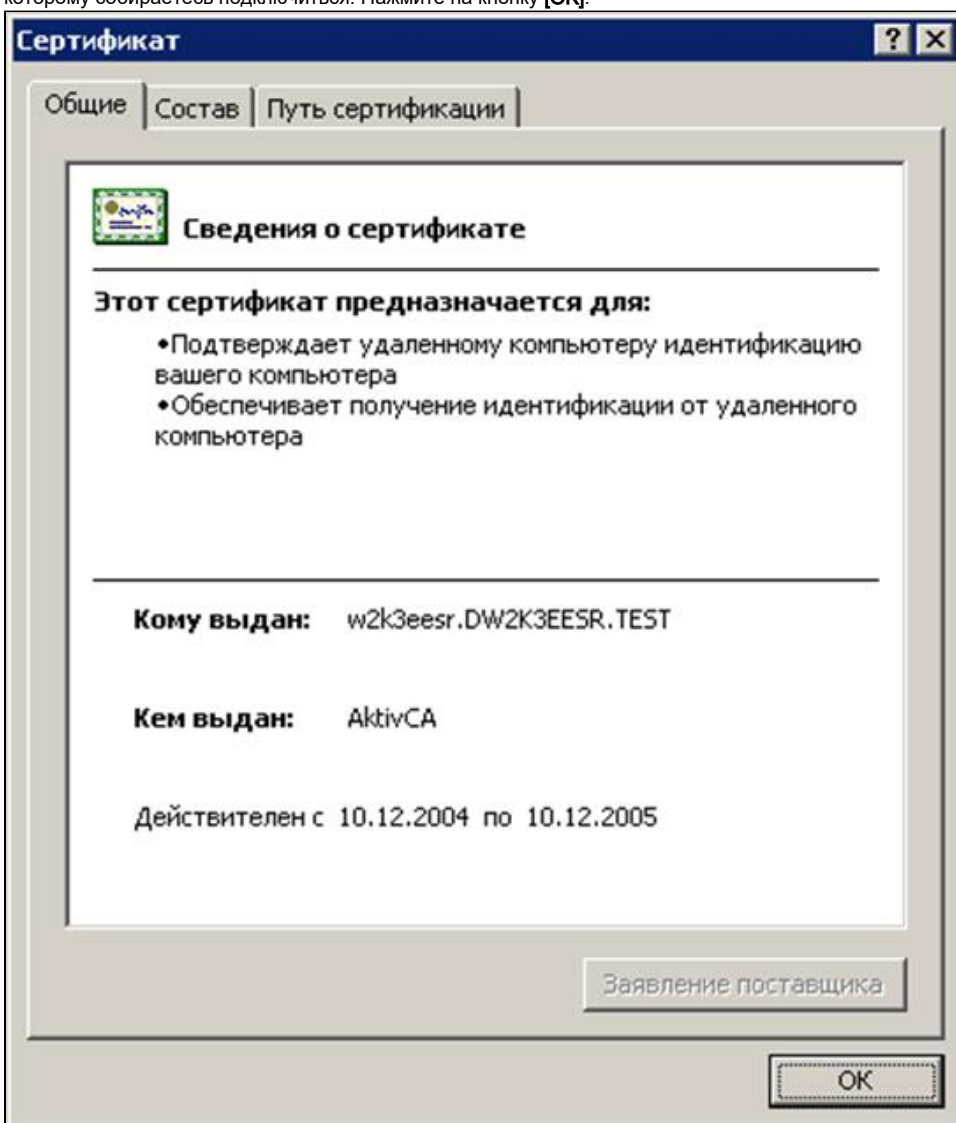
Произведено подключение к серверу:
w2k3eesr.DW2K3EESR.TEST

Если это корректный сервер, нажмите кнопку "OK" для подключения, и это сообщение больше не будет отображаться. Щелкните "Отмена" для разрыва подключения.

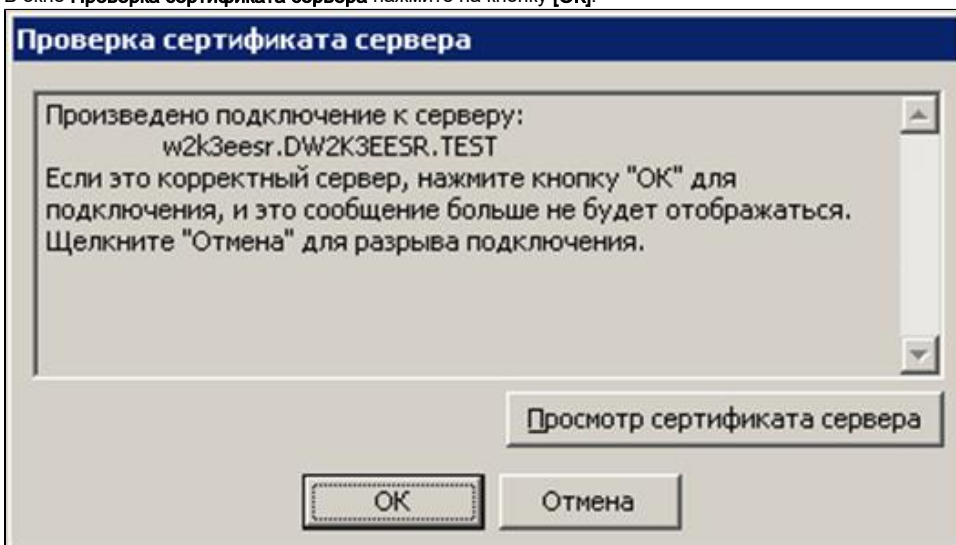
Просмотр сертификата сервера

OK Отмена

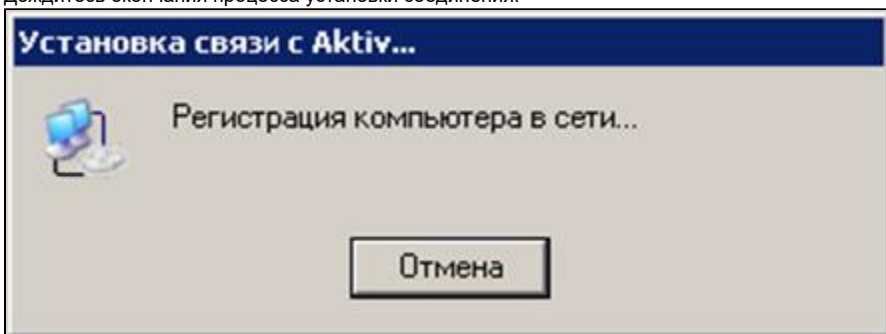
16. Убедитесь, что сертификат выдан ранее настроенным **Центром сертификации** именно тому серверу, на котором его настроили и к которому собираетесь подключиться. Нажмите на кнопку **[ОК]**.



17. В окне **Проверка сертификата сервера** нажмите на кнопку **[ОК]**.



18. Дождитесь окончания процесса установки соединения.



В результате соединение будет установлено.

