3.2.1.1 Удаленный доступ к сетям VPN

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

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.

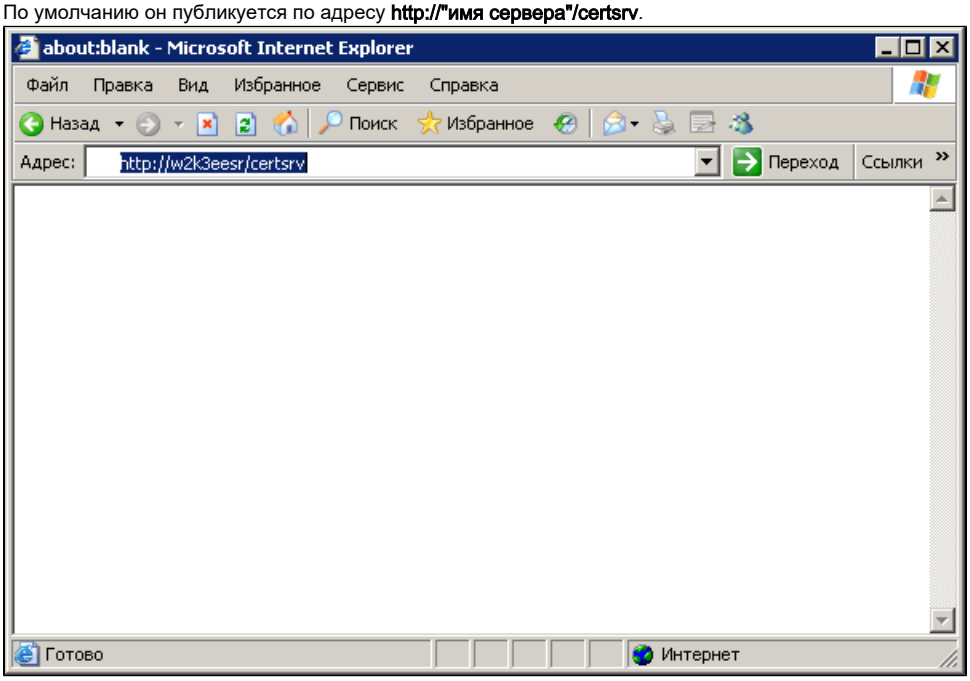
2 этап: Создание и настройка удаленного подключения к сети VPN.

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.

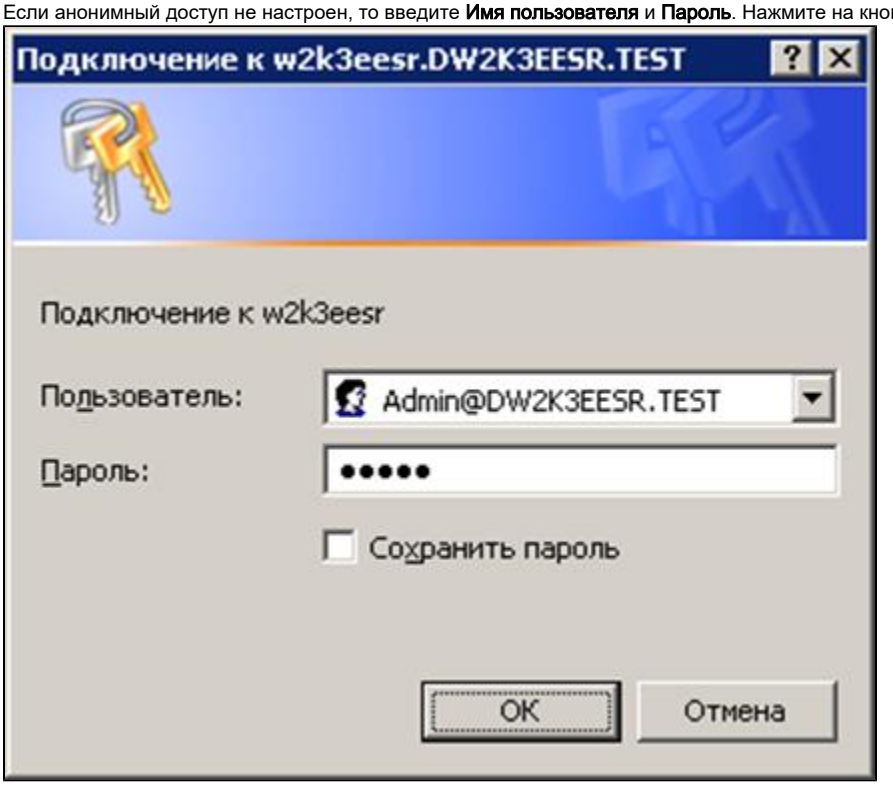
Для установки сертификата Центра сертификации:

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

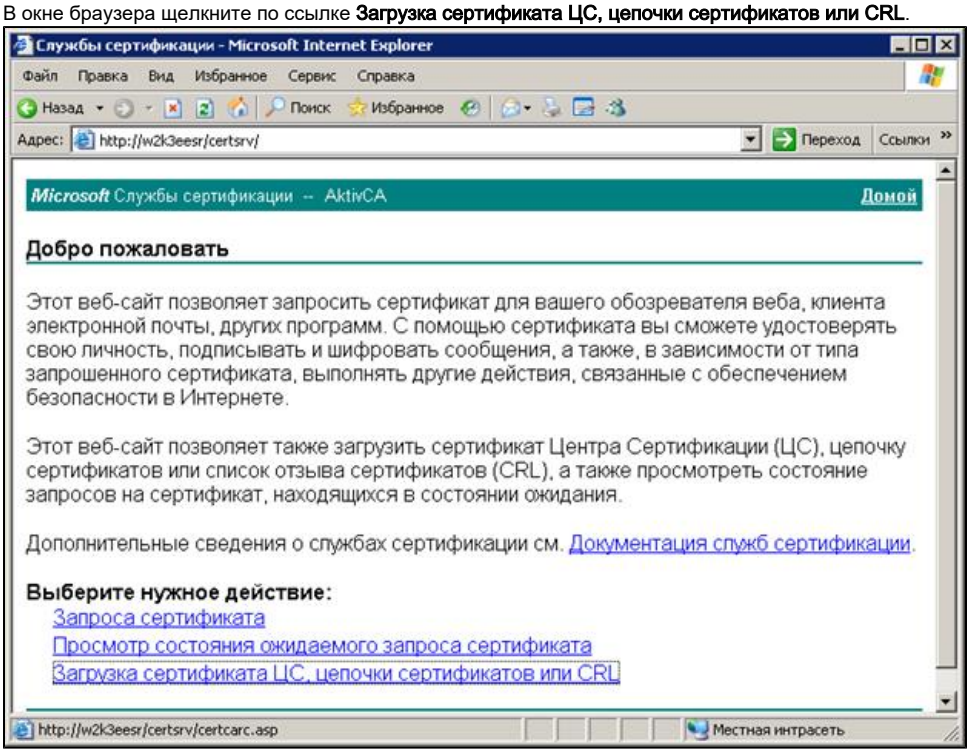


2. Нажмите на клавишу **[Enter]**.

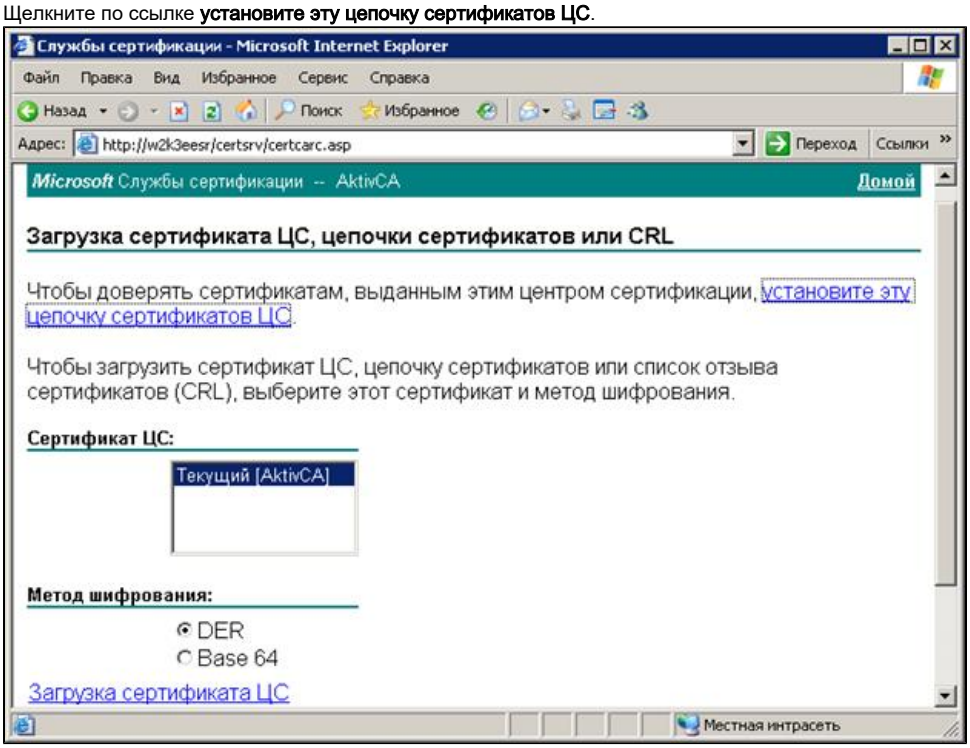
3. Если анонимный доступ не настроен, то введите **Имя пользователя** и **Пароль**. Нажмите на кнопку **[OK]**.



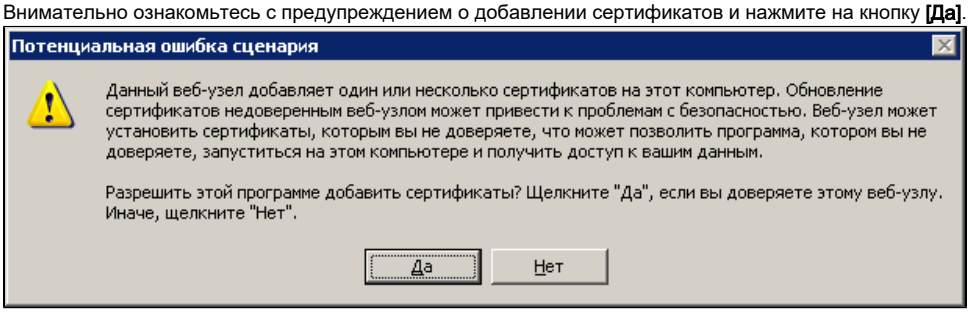
4. В окне браузера щелкните по ссылке **Загрузка сертификата ЦС, цепочки сертификатов или CRL**.



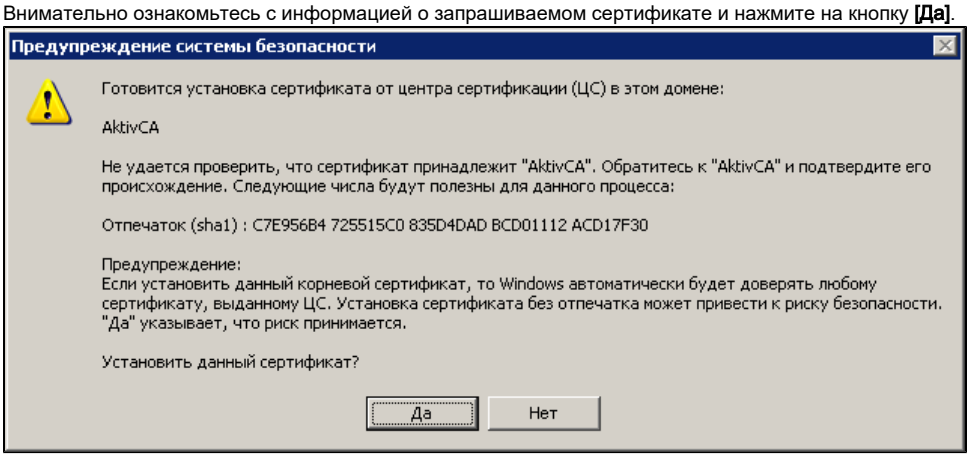
5. Щелкните по ссылке **установите эту цепочку сертификатов ЦС**.



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

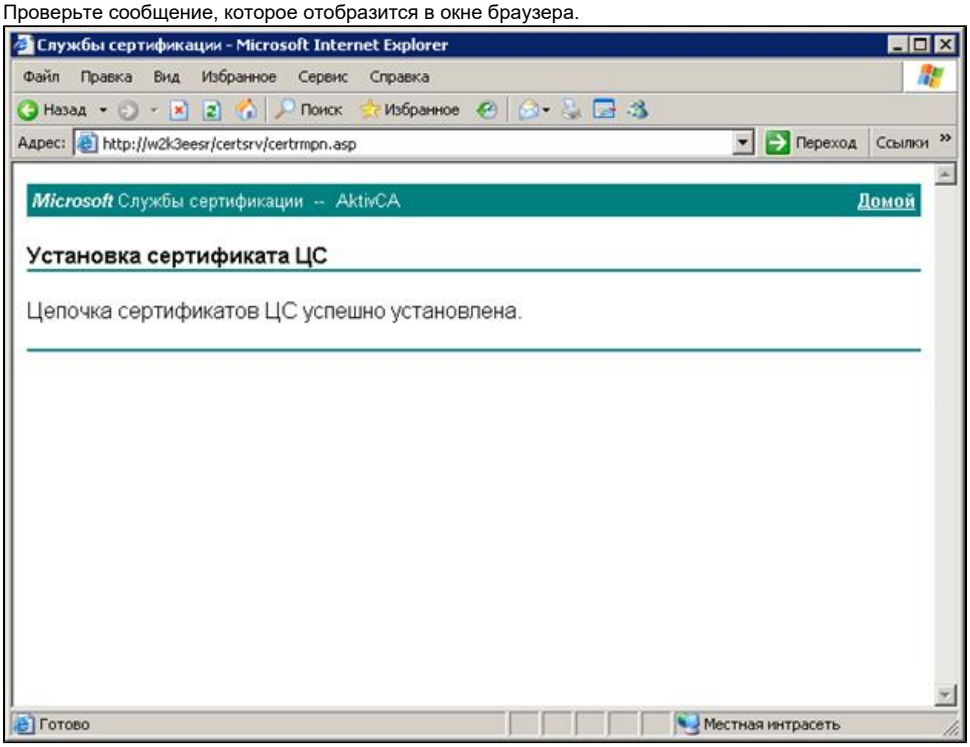


7. Внимательно ознакомьтесь с информацией о запрашиваемом сертификате и нажмите на кнопку **[Да]**.



8. Дождитесь окончания процесса установки сертификата.

9. Проверьте сообщение, которое отобразится в окне браузера.



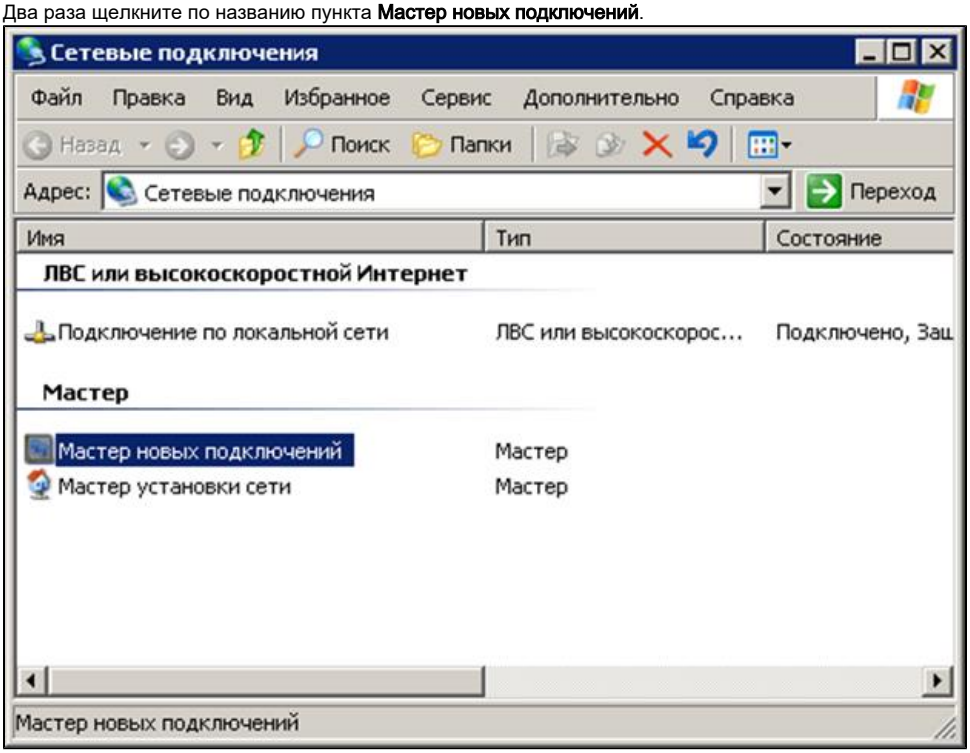
10. Если установка прошла успешно, то закройте окно браузера. В противном случае повторите процедуру, описанную в данном разделе.

Создание и настройка удаленного подключения к сети VPN

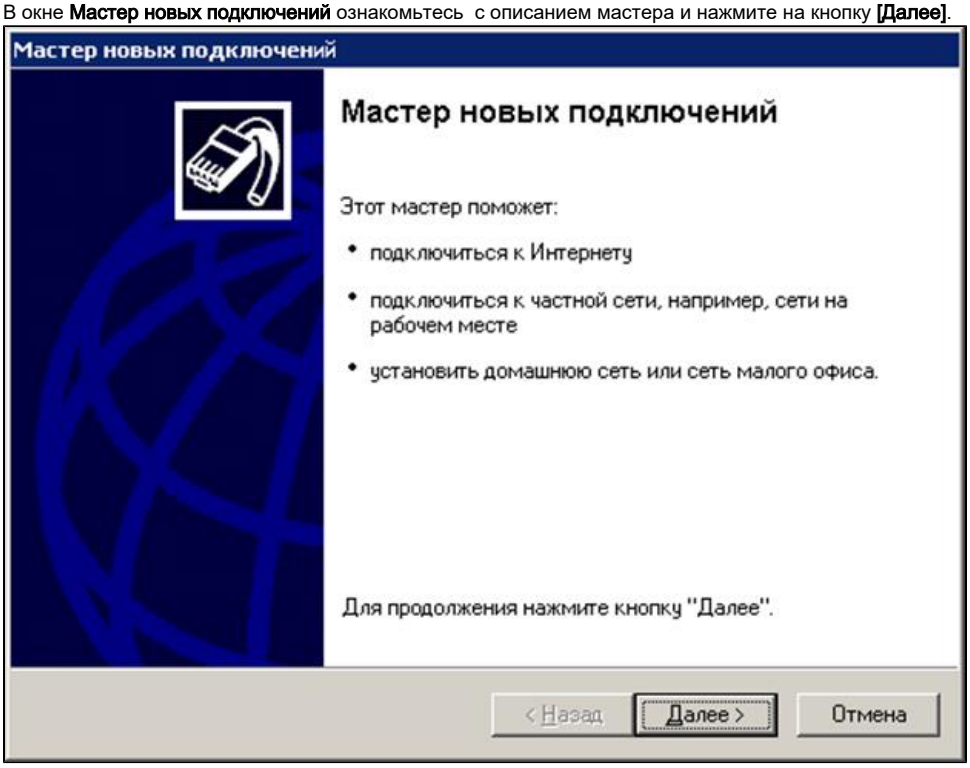
После того как сертификат **Центра сертификации** установлен, можно создавать удаленное подключение к сети VPN.

Для создания и настройки удаленного подключения к сети VPN:

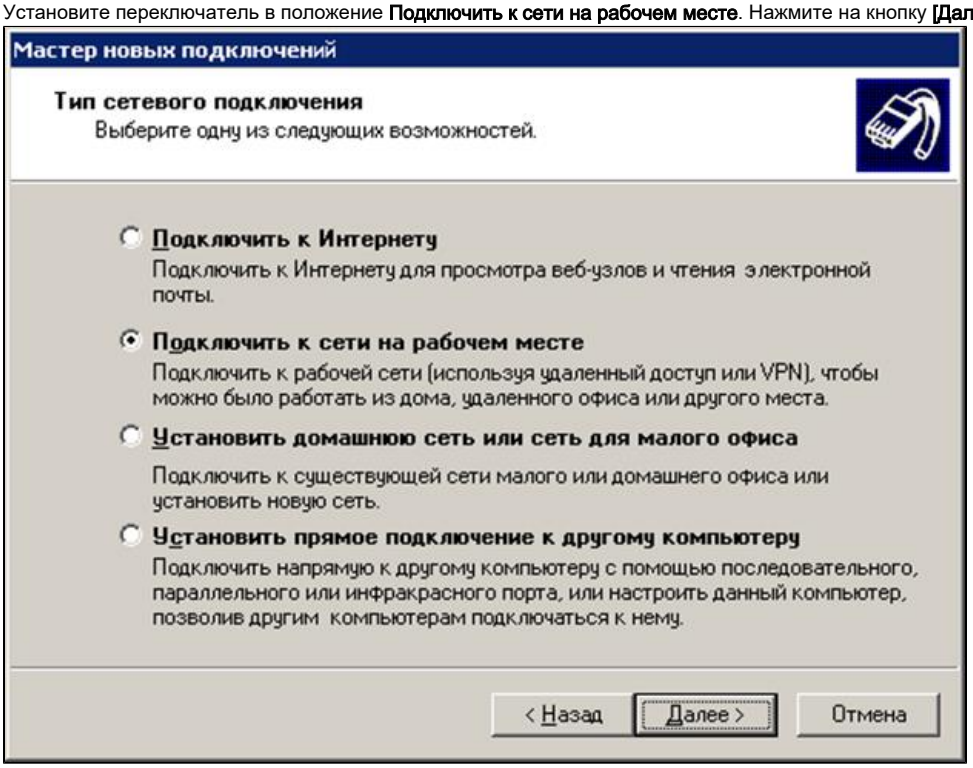
1. Откройте **Панель управления**.
2. Два раза щелкните по названию пункта **Сетевые подключения**.
3. Два раза щелкните по названию пункта **Мастер новых подключений**.



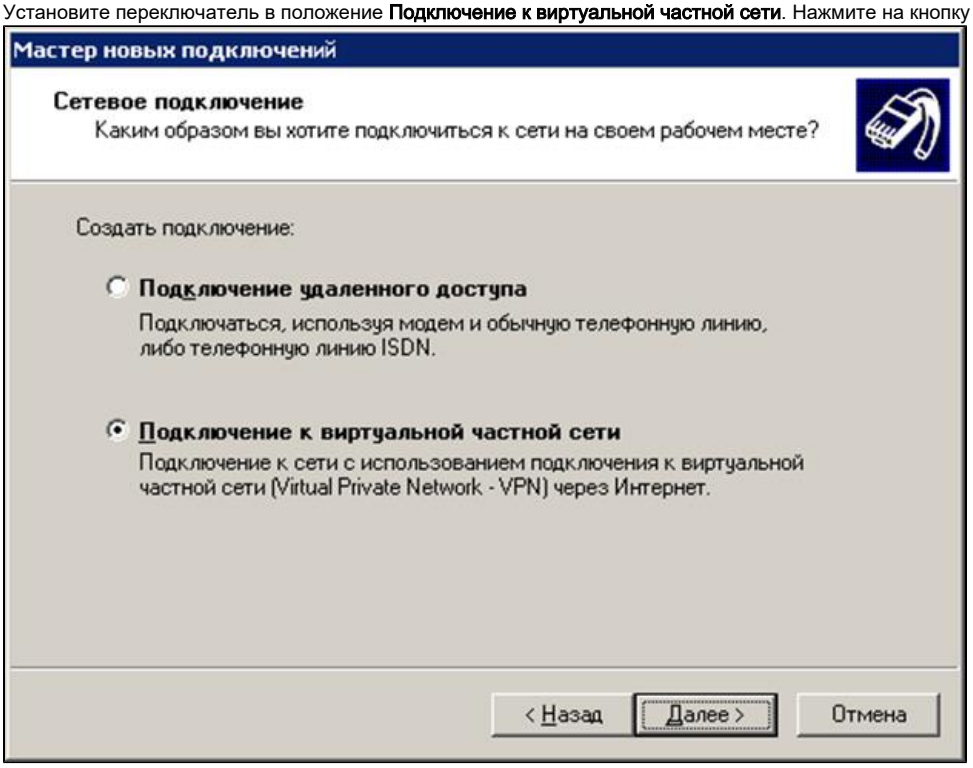
4. В окне **Мастер новых подключений** ознакомьтесь с описанием мастера и нажмите на кнопку **[Далее]**.



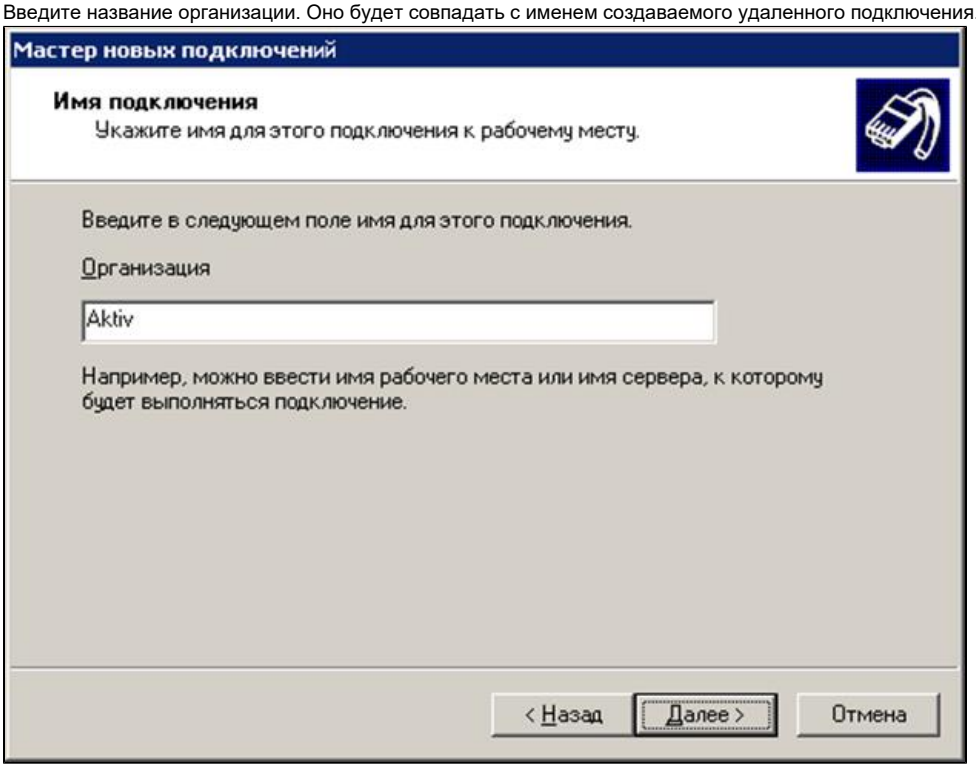
5. Установите переключатель в положение **Подключить к сети на рабочем месте**. Нажмите на кнопку **[Далее]**.



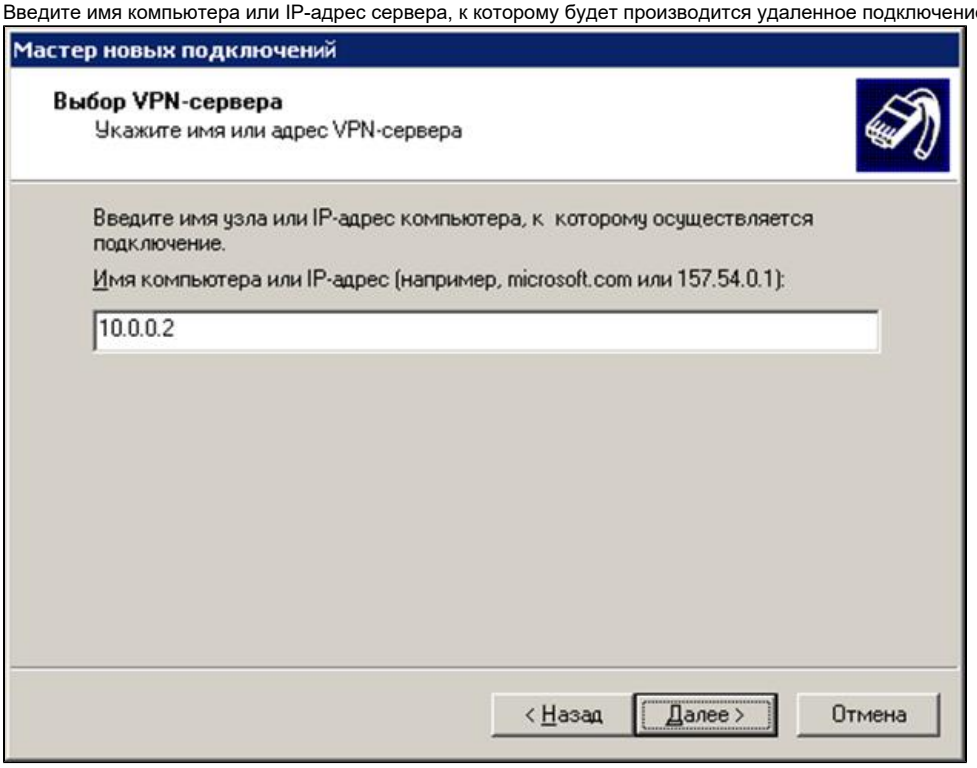
6. Установите переключатель в положение **Подключение к виртуальной частной сети**. Нажмите на кнопку **[Далее]**.



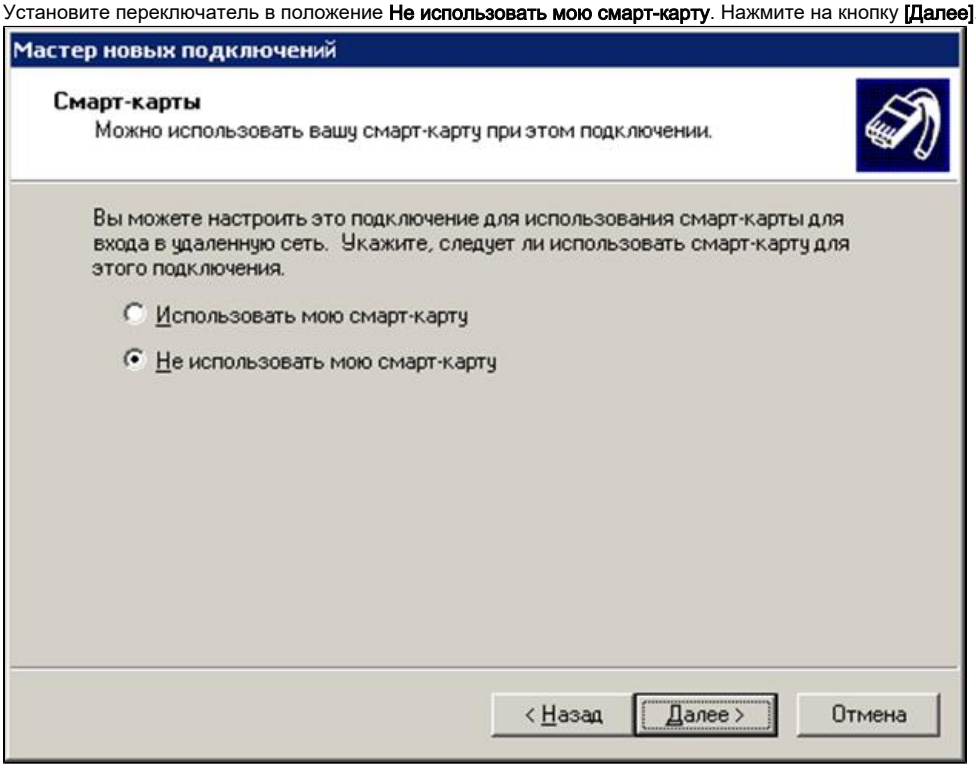
7. Введите название организации. Оно будет совпадать с именем создаваемого удаленного подключения.



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



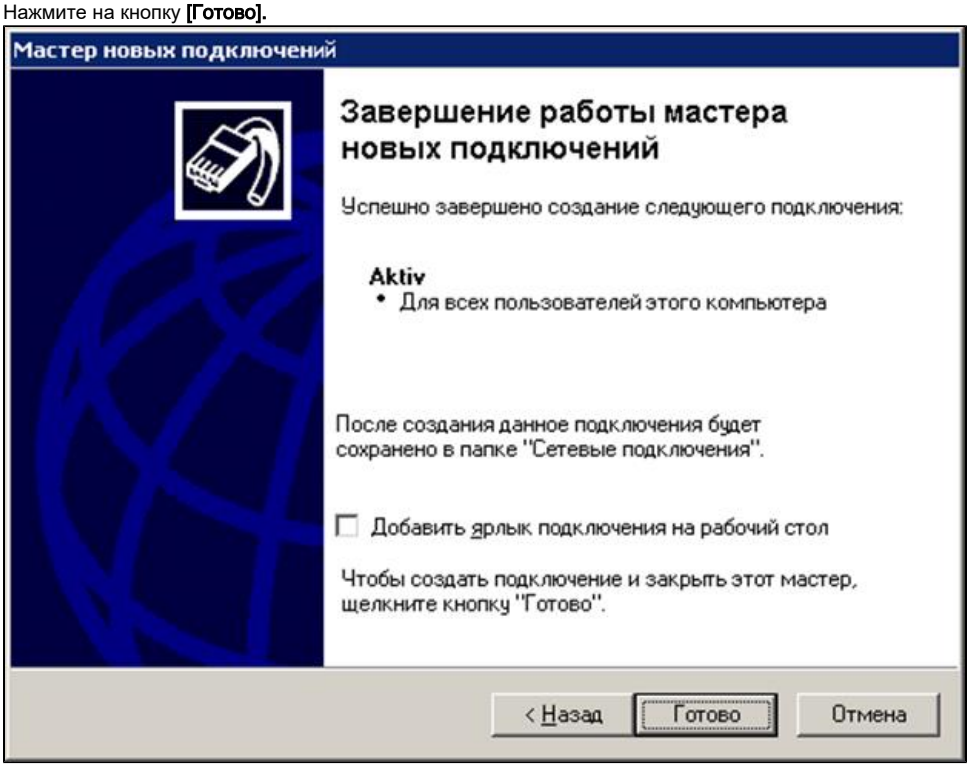
9. Установите переключатель в положение **Не использовать мою смарт-карту**. Нажмите на кнопку **[Далее]**.



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].**

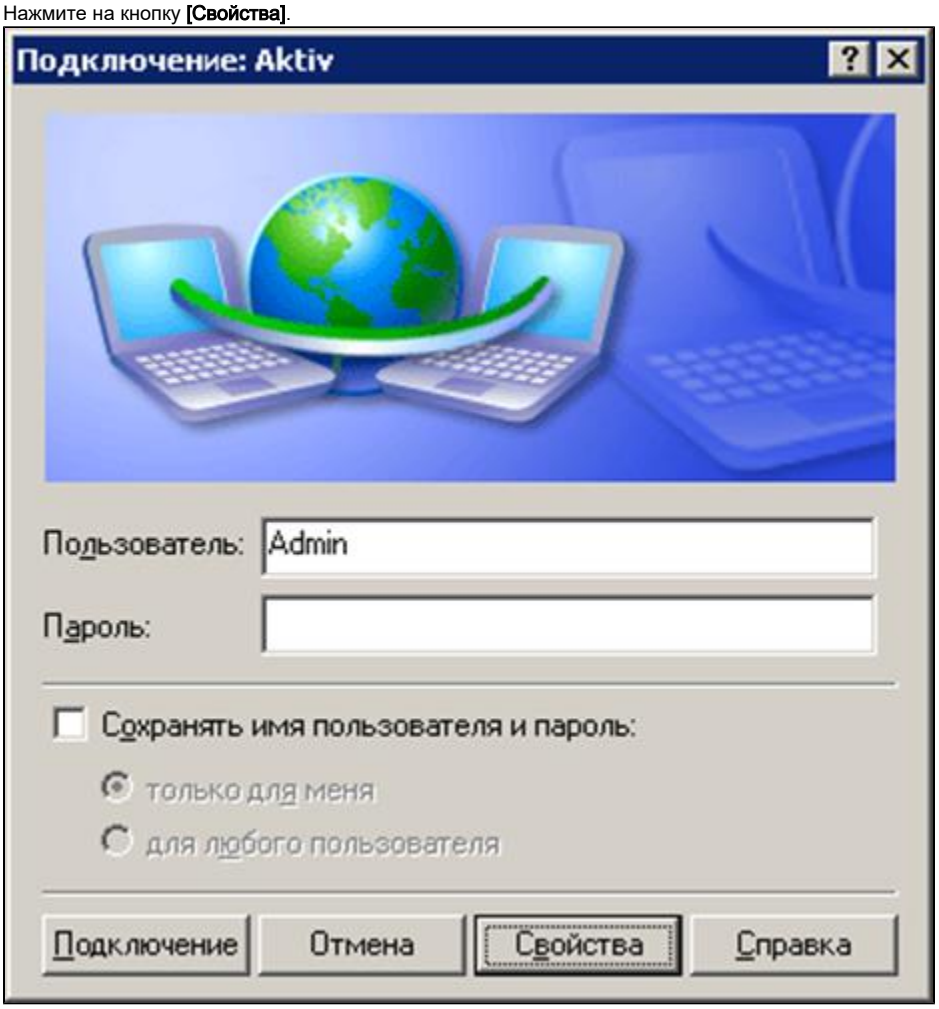


После создания удаленного подключения необходимо настроить его для работы с устройством Рутокен.

Для настройки удаленного подключения к сети VPN:

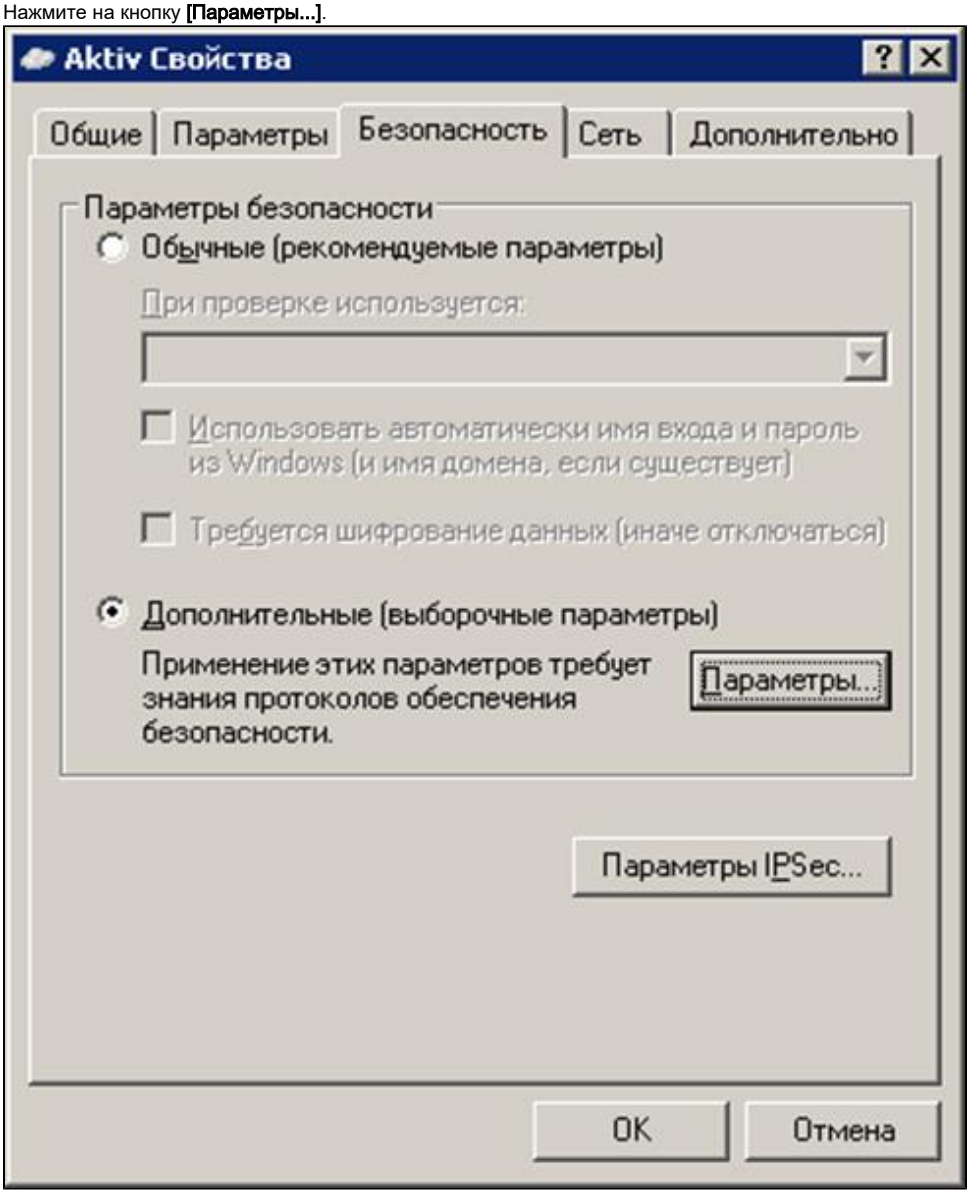
1. Откройте окно подключения.

2. Нажмите на кнопку **[Свойства]**.



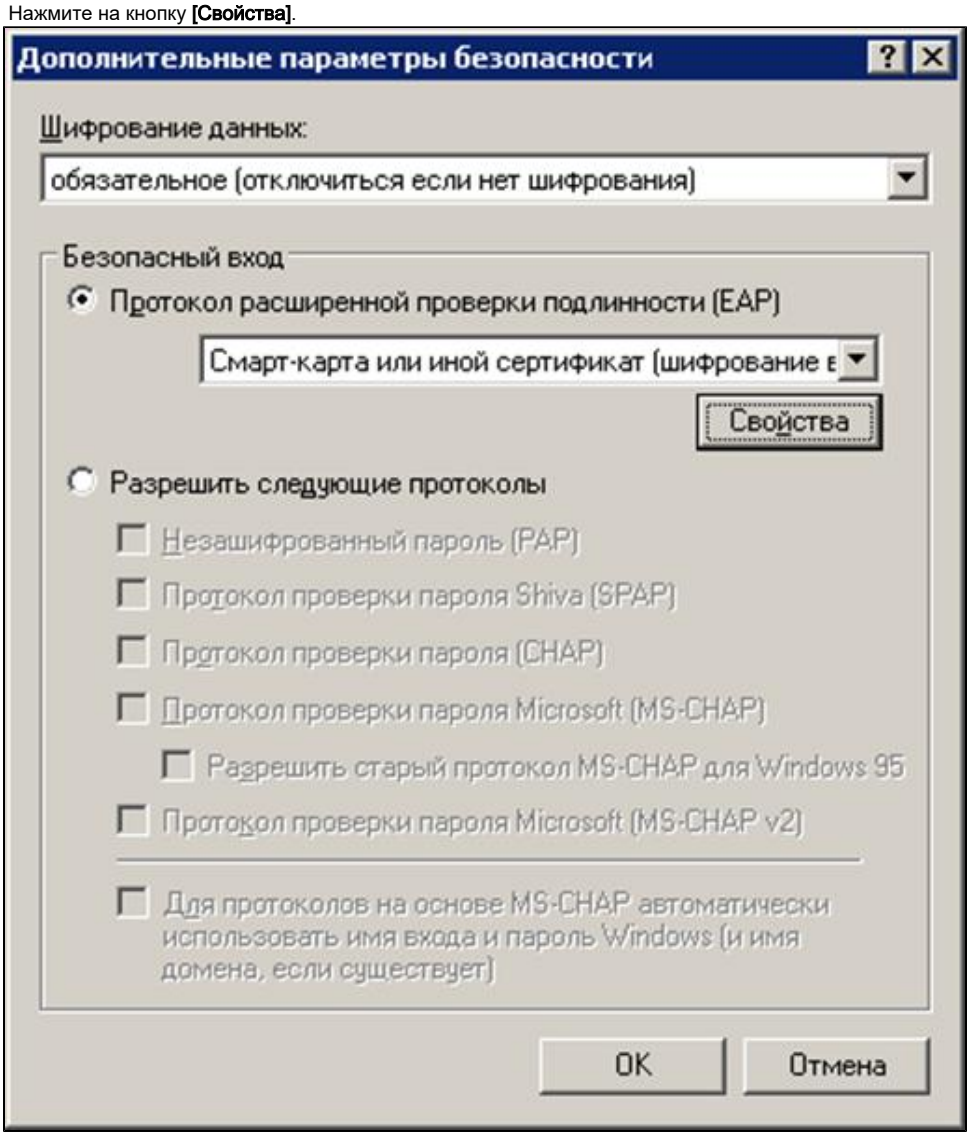
3. Перейдите на вкладку **Безопасность**.
4. Установите переключатель в положение **Дополнительные (выборочные параметры)**.

5. Нажмите на кнопку **[Параметры...]**.

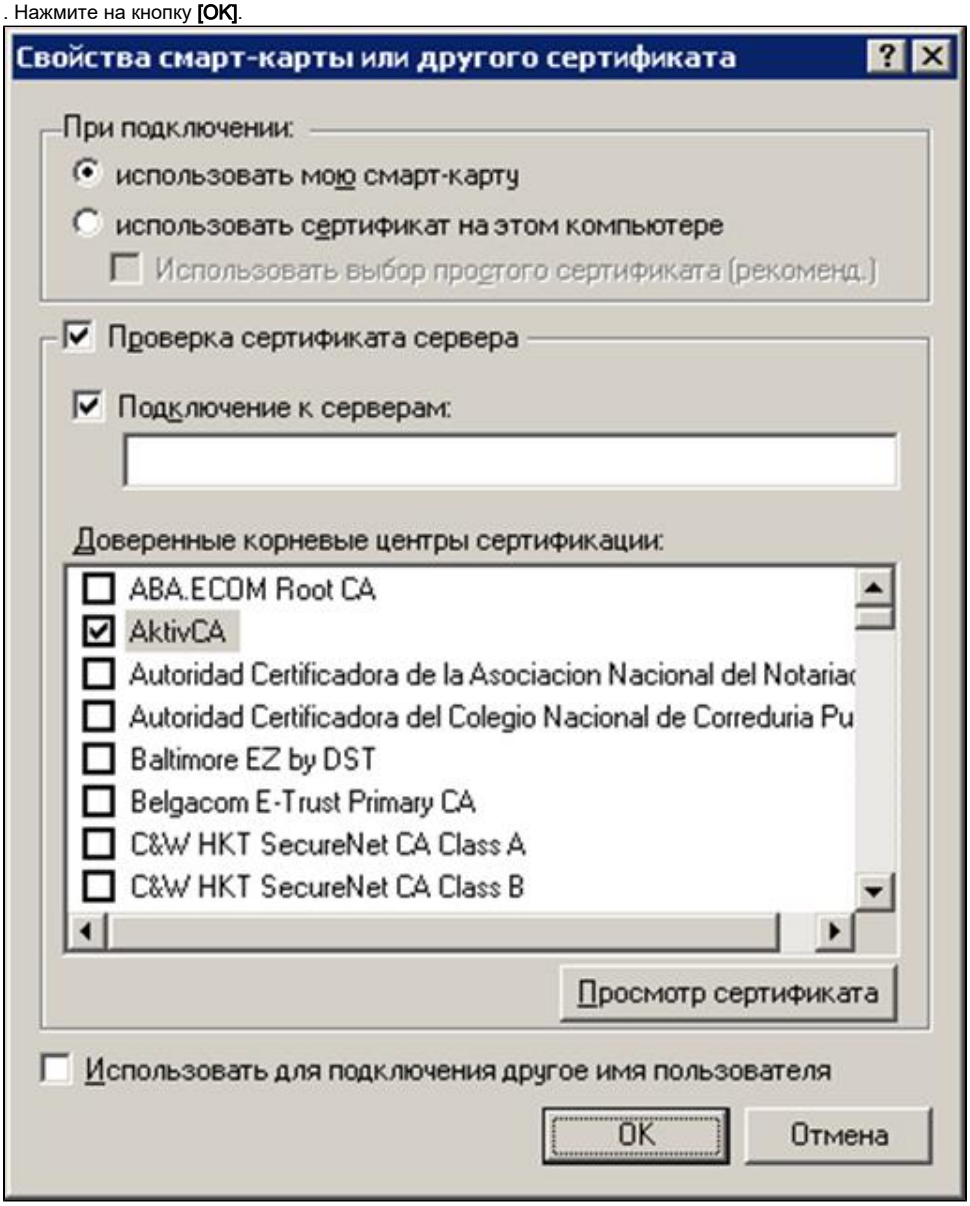


6. В окне **Дополнительные параметры безопасности** установите переключатель в положение **Протокол расширенной проверки подлинности (EAP)**.

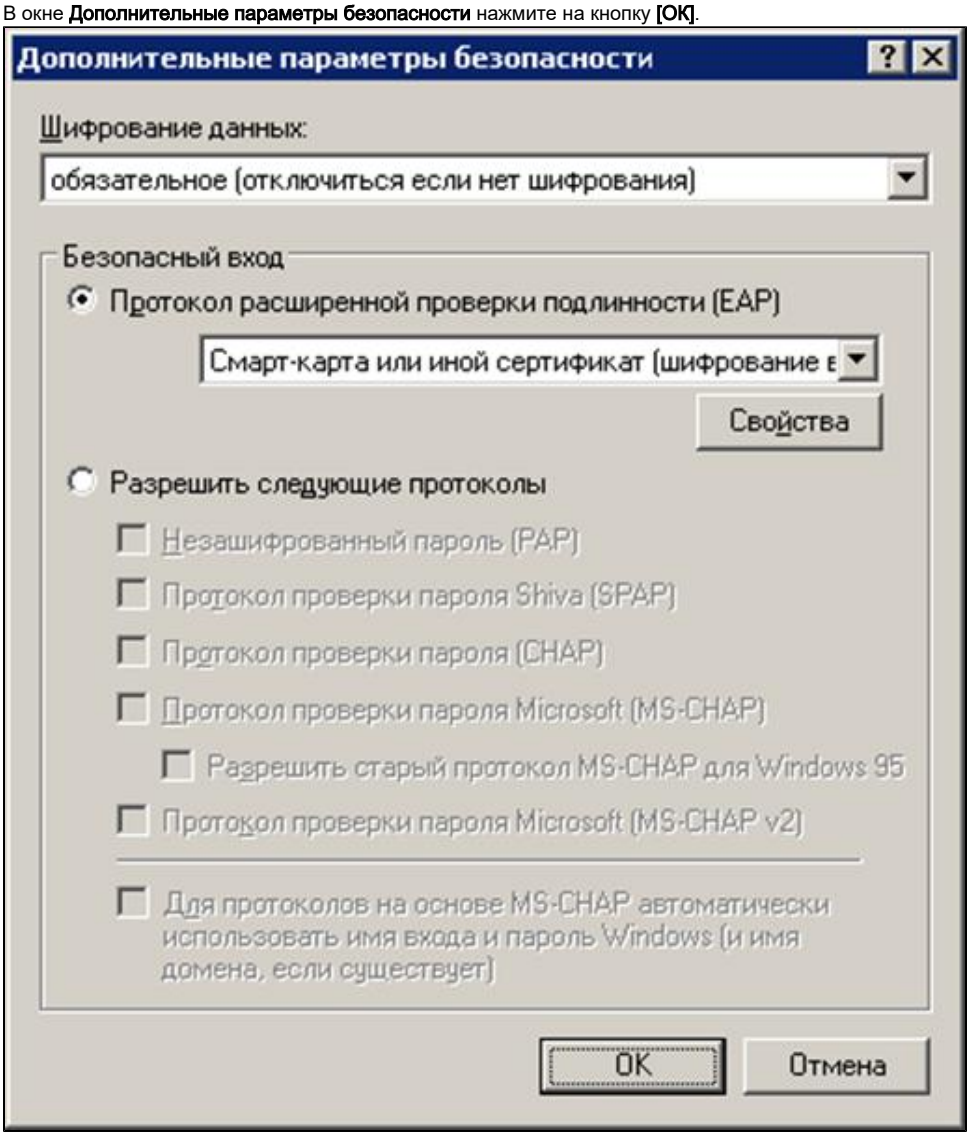
7. Нажмите на кнопку **[Свойства]**.



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

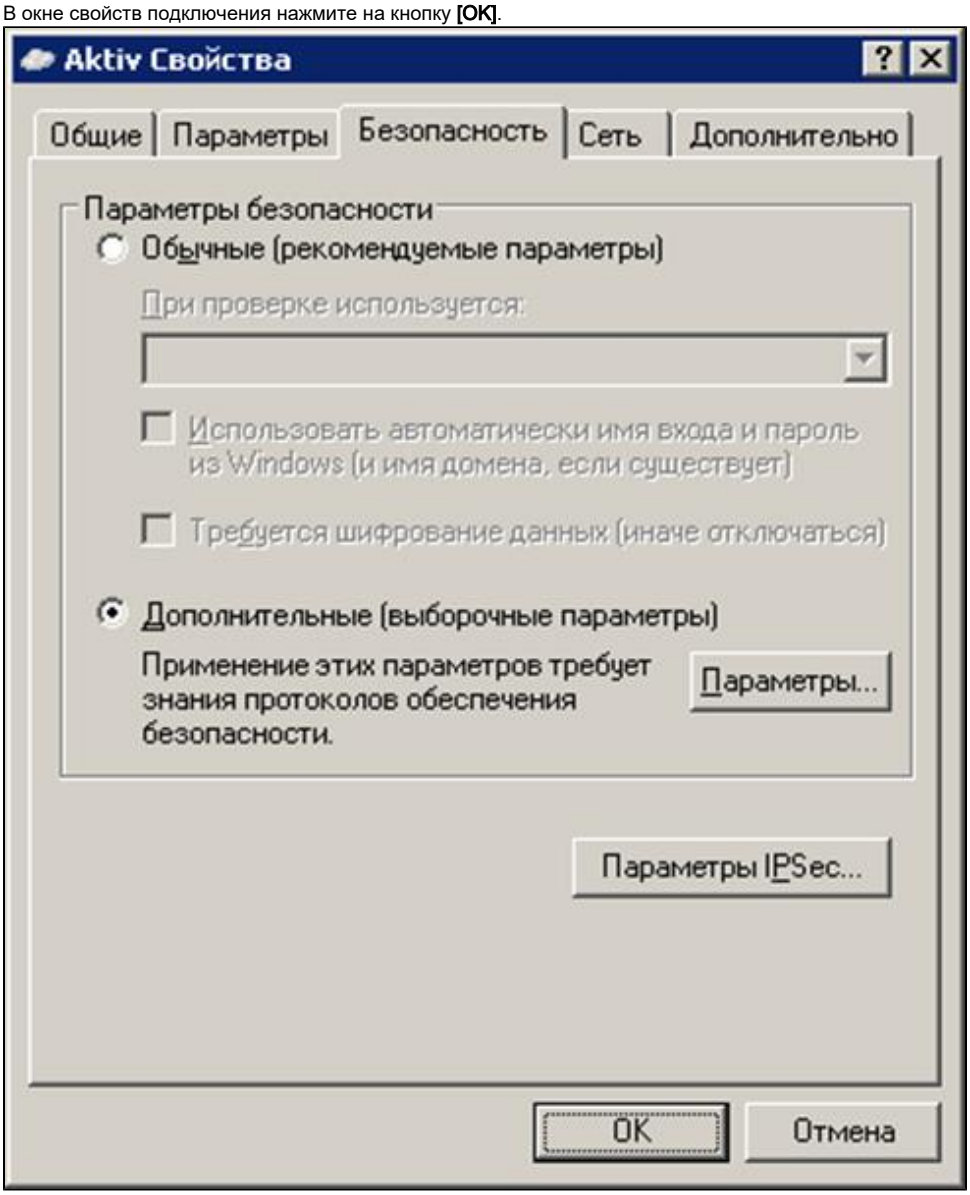


9. В окне **Дополнительные параметры безопасности** нажмите на кнопку **[ОК]**.

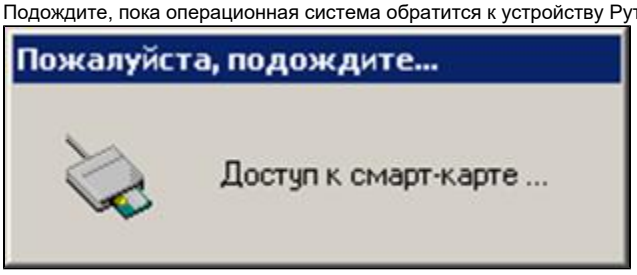


10. Подключите устройство Рутокен к компьютеру (на устройстве должен быть сертификат типа **Пользователь со смарт-картой**).

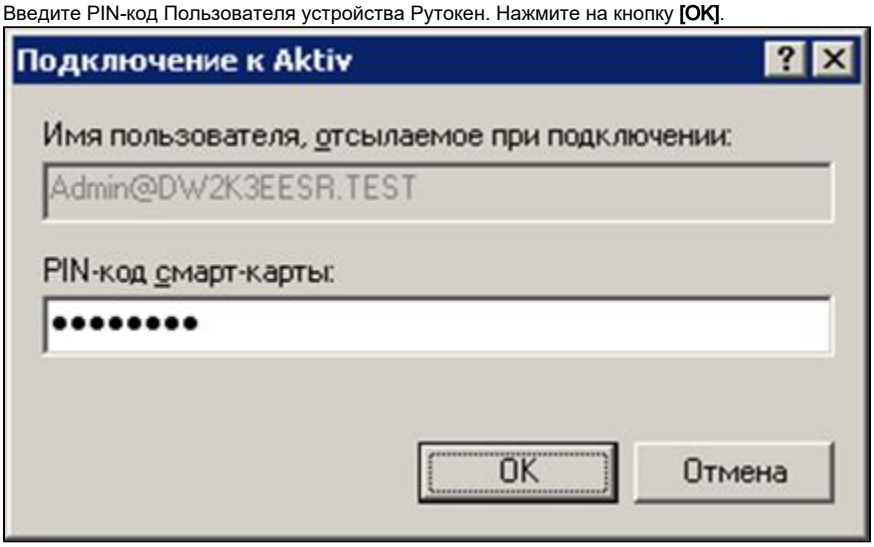
11. В окне свойств подключения нажмите на кнопку **[OK]**.



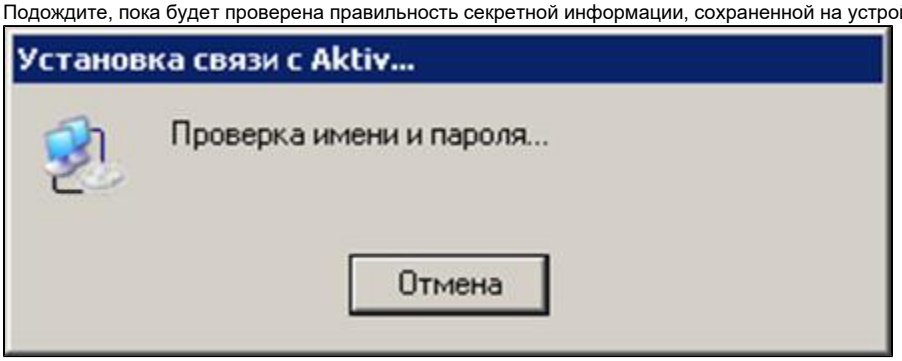
12. Подождите, пока операционная система обратится к устройству Рутокен.



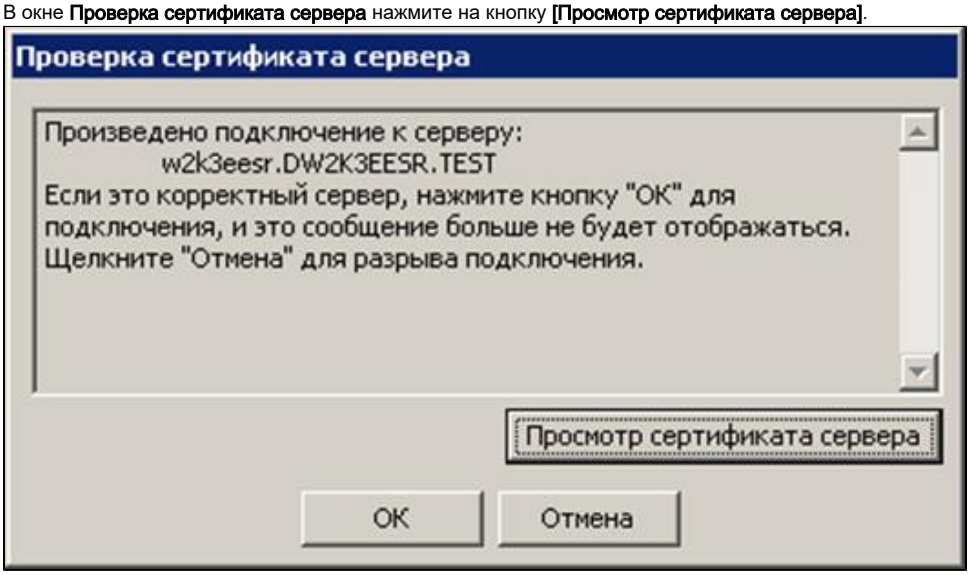
13. Введите PIN-код Пользователя устройства Рутокен. Нажмите на кнопку **[OK]**.



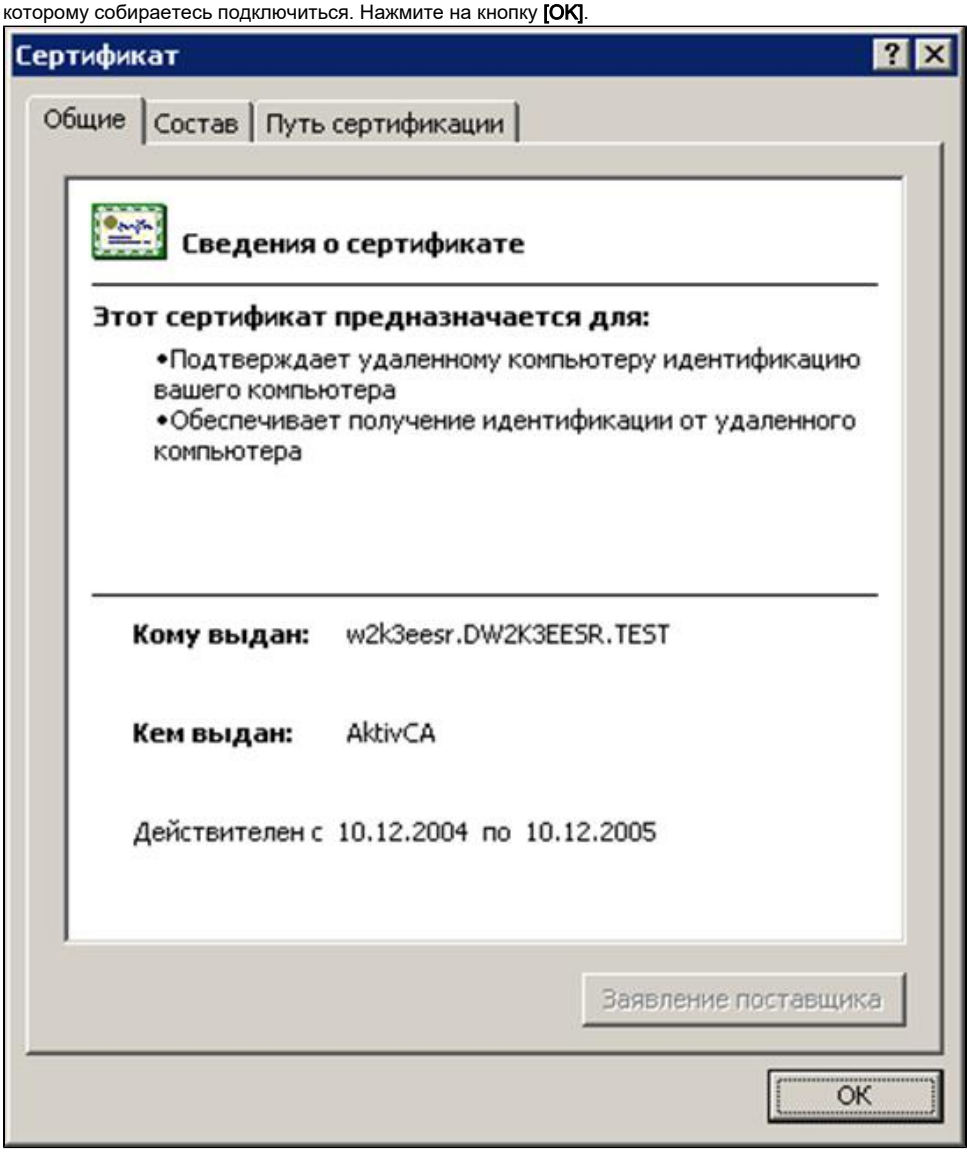
14. Подождите, пока будет проверена правильность секретной информации, сохраненной на устройстве Рутокен.



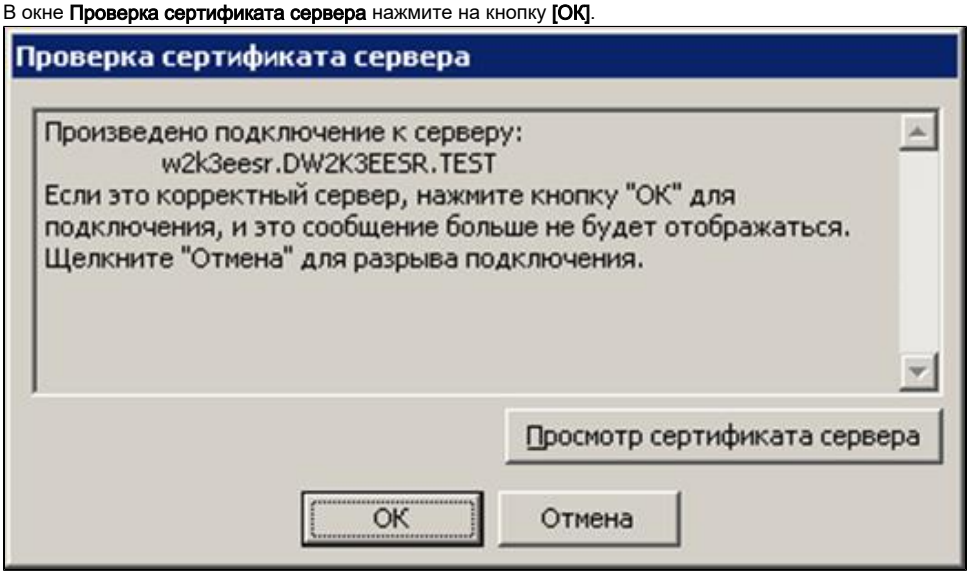
15. В окне **Проверка сертификата сервера** нажмите на кнопку **[Просмотр сертификата сервера]**.



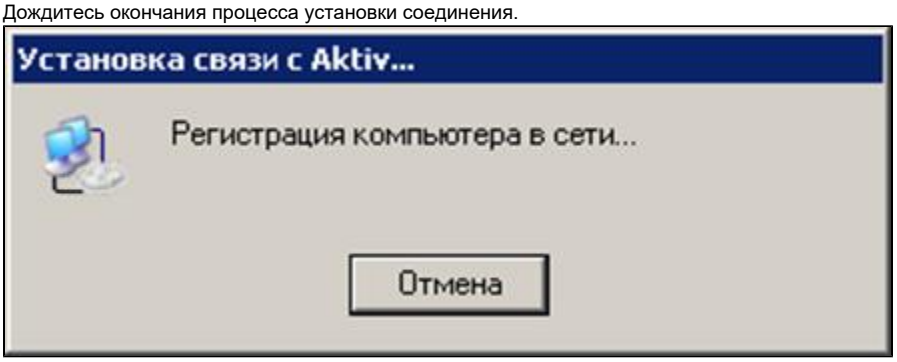
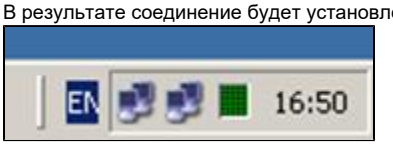
16. Убедитесь, что сертификат выдан ранее настроенным **Центром сертификации** именно тому серверу, на котором его настроили и к которому собираетесь подключиться. Нажмите на кнопку **[OK]**.



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



18. Дождитесь окончания процесса установки соединения.



В результате соединение будет установлено.