



Настройка аутентификации VPN с использованием сервера SoftPI RADIUS

Настройка SoftPI RADIUS сервера

Сервер SoftPI RADIUS (далее RADIUS сервер) выполняет проверку пользователей, подключающихся к точке доступа (аутентификация), проверяет, имеет ли право данный пользователь подключаться к точке доступа в текущий момент (авторизация), и ведет учет всех сессий пользователей (аккаунтинг).

Первым делом нужно в программе "Консоль управления RADIUS" сервера настроить параметры сервера доступа, в качестве которого будет выступать VPN сервер.

Необходимо ввести его IP адрес и общий секрет. Общий секрет – это пароль, используемый при обмене данными между сервером RADIUS и VPN сервером. Использование этого пароля исключает возможность появления неавторизованного VPN сервера. RADIUS-сервер будет игнорировать все запросы от сервера доступа, если ему неизвестен IP-адрес или общий секрет сервера. Пример добавления сервера доступа приведен на рисунке 1.

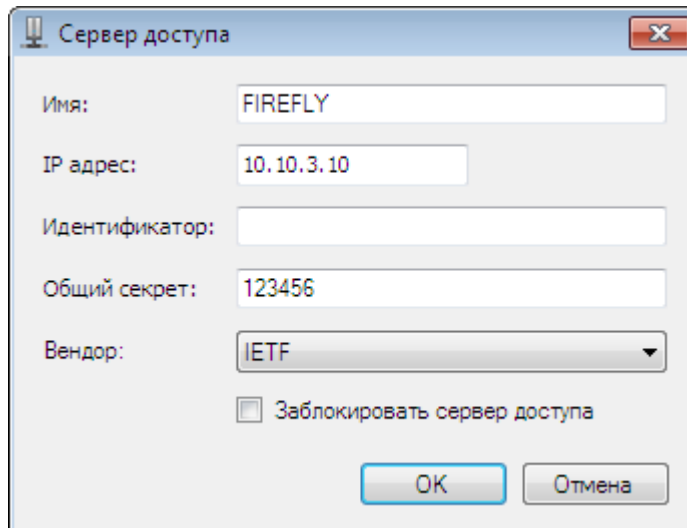


Рисунок 1

Далее необходимо ввести параметры пользователей, которые будут иметь право подключаться к VPN серверу. Для добавления пользователя следует использовать режим "Консоли настройки RADIUS-сервера": "Пользователи/Группы" → "Пользователи". Для пользователя обязательно следует указать имя пользователя и пароль. Также можно указать группу атрибутов, разрешенное время входа, и ряд других параметров. Окно добавления пользователя приведено на рисунке 2.

После создания пользователя при необходимости следует задать ему атрибуты. Для отправки атрибутов авторизованному пользователю, необходимо в параметре "Тип" выбрать значение: "Отправлять в Access-Accept".

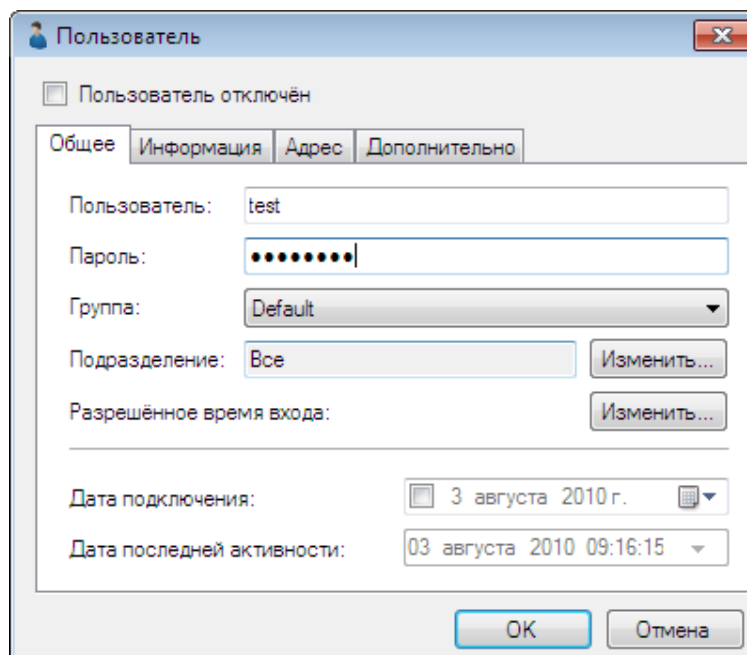


Рисунок 2

Для задания выдаваемого пользователю IP адреса можно добавить пользователю атрибут Framed-IP-Address и в качестве значения указать требуемый IP адрес (рисунок 3).

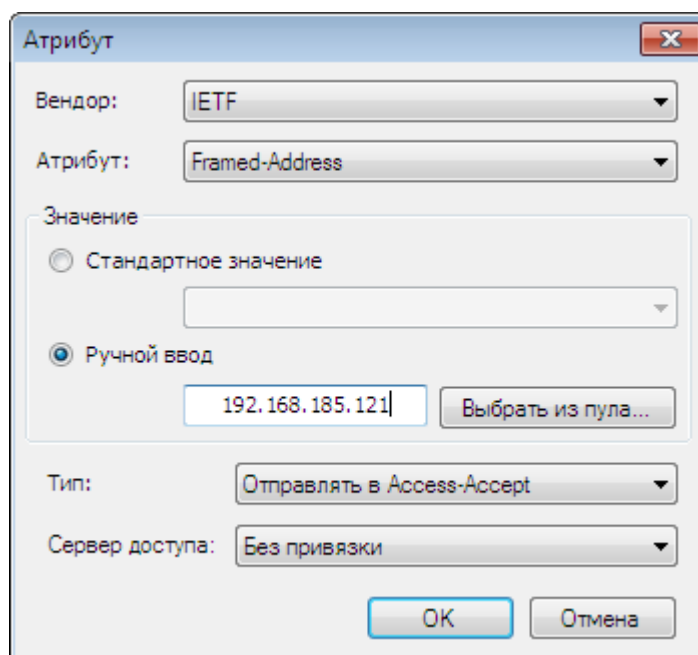


Рисунок 3

Для ограничения времени сессии пользователя средствами сервера доступа (если такая возможность есть), можно воспользоваться атрибутом Session-Timeout (или другим, который поддерживается конкретным сервером доступа), который задаёт максимальную длительность сессии в секундах.

Аналогичным образом можно создать нужное количество логинов пользователей.

Кроме ручного создания пользователей, SoftPI Radius поддерживает также импорт данных из Active Directory или другого каталога, поддерживающего протокол LDAP.

Сервер доступа (VPN сервер) может поддерживать и другие атрибуты, которые можно задать для пользователя и/или группы пользователей.

Настройка сетевого сервера доступа (Network Access Server - NAS)

В зависимости от типа VPN сервера настройка может иметь отличия. Для настройки аутентификации и авторизации по протоколу RADIUS необходимо указать:

1. IP адрес сервера аутентификации RADIUS.
2. Номер порта аутентификации (по умолчанию – 1812).
3. Общий секрет, введенный ранее в настройках RADIUS сервера.
4. При необходимости ведения учета предоставленных услуг следует указать IP адрес биллингового сервера.

Настройка компьютера клиента VPN (Пример настройки для WindowsXP)

1. Создание нового подключения.
 - 1.1 Откройте окно «Сетевые подключения» и выберите пункт «Создание нового подключения».
 - 1.2 Создайте новое подключение для подключения с использованием VPN (рисунки 4 - 7).

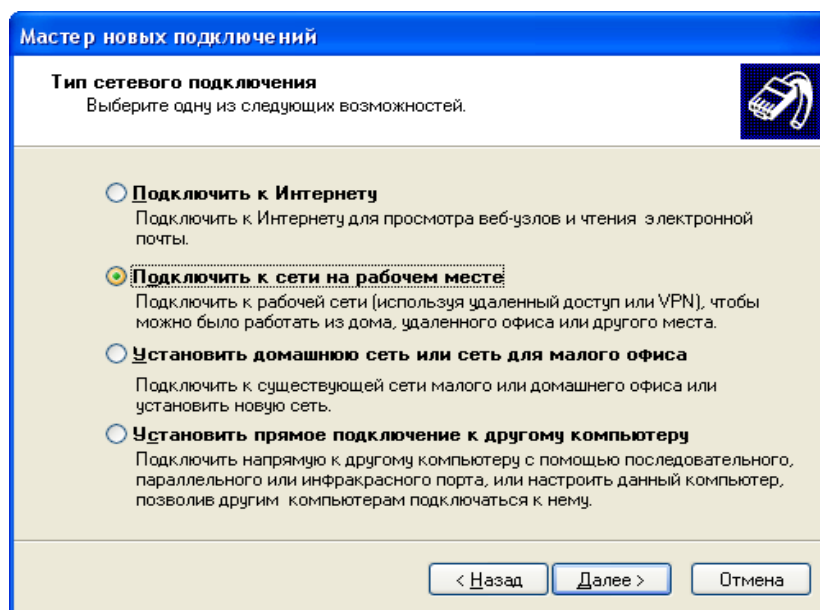


Рисунок 4

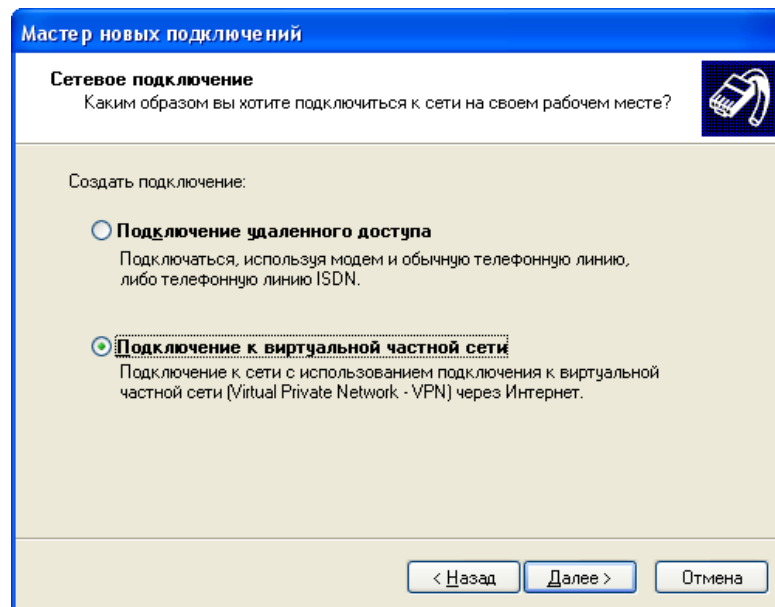


Рисунок 5

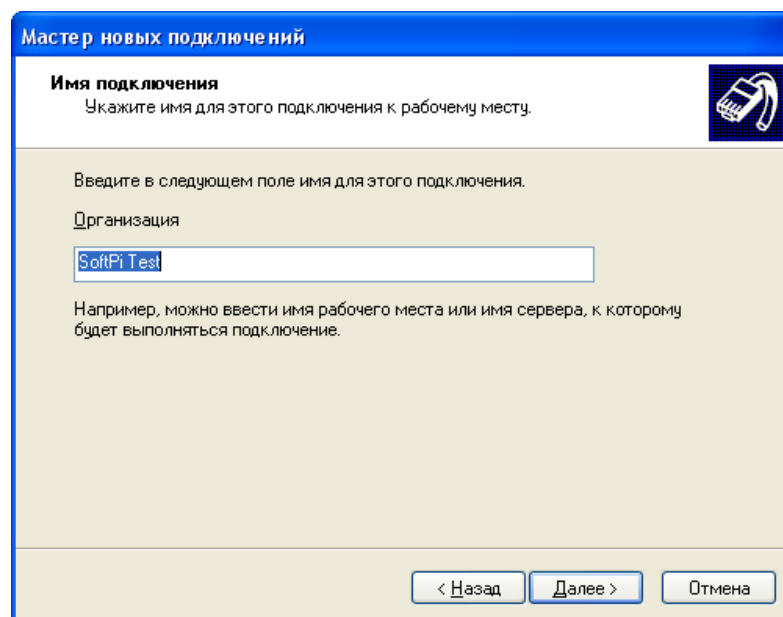


Рисунок 6

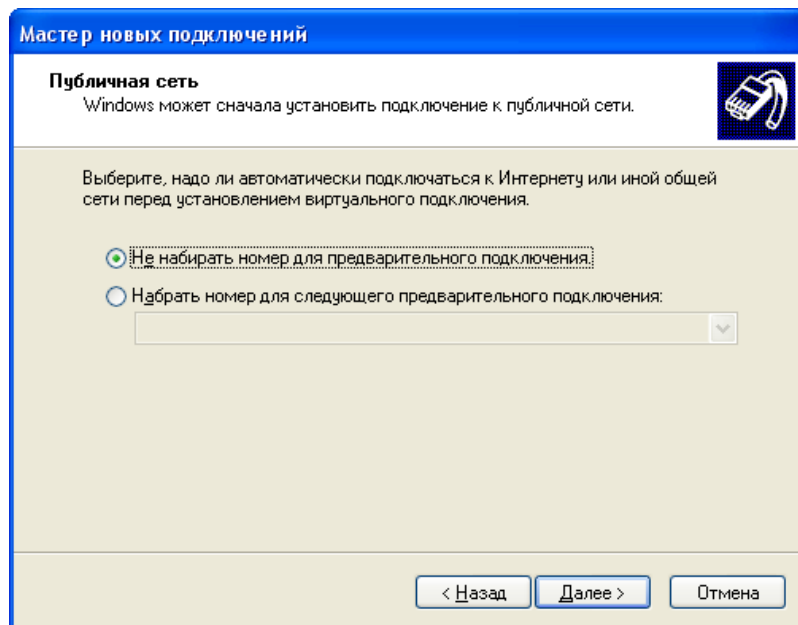


Рисунок 7

1.3 Укажите IP адрес VPN сервера (рисунок 8).

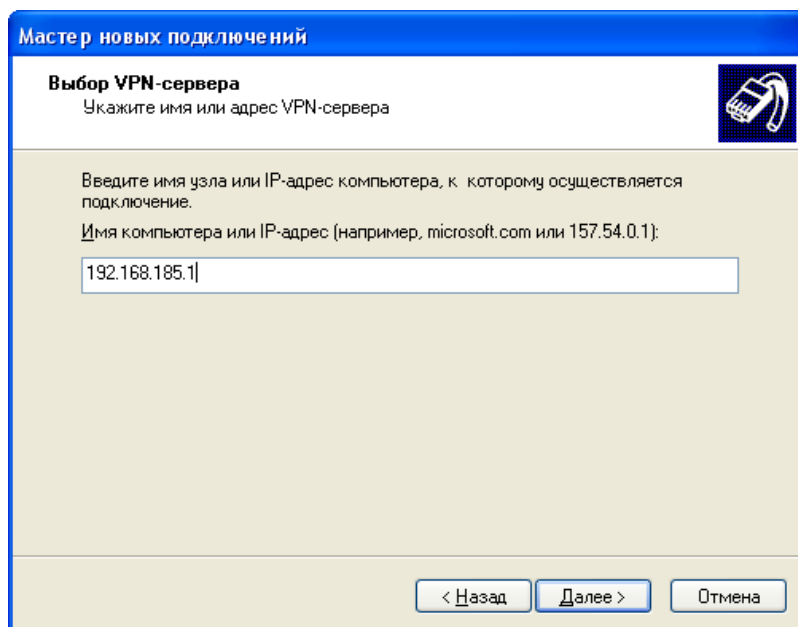


Рисунок 8

2. Настройка VPN подключения.

2.1 Откройте созданное подключение, введите имя пользователя и пароль, а затем выберите «Свойства» (рисунок 9).

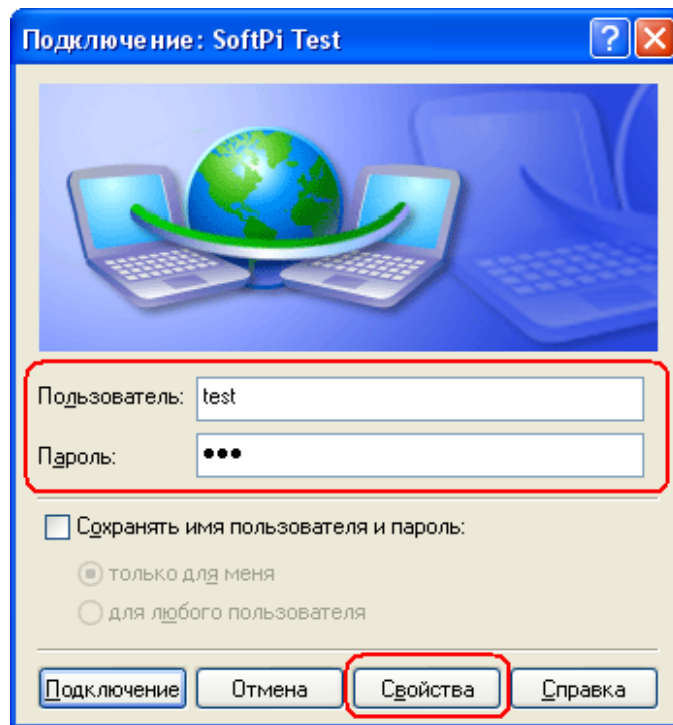


Рисунок 9

- 2.2 Во вкладке "Безопасность" выберите опцию "Дополнительные" и щелкните по кнопке "Параметры" (рисунок 10).

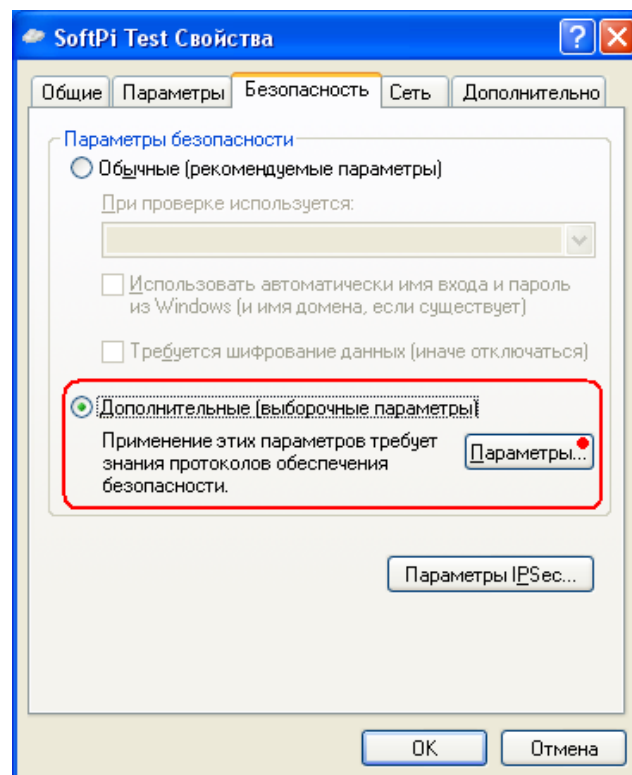


Рисунок 10

- 2.3 В окне "Дополнительные параметры безопасности" выберите протокол(ы) для проверки подлинности (рисунок 11).

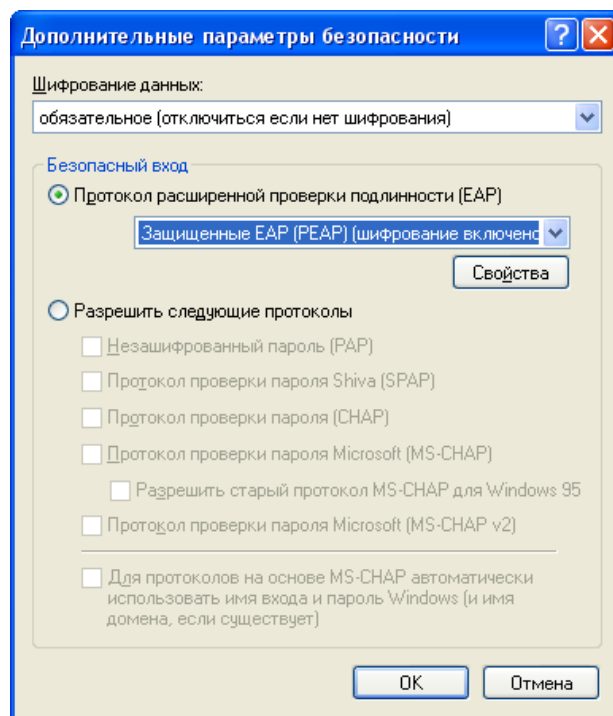


Рисунок 11

Наиболее защищённый протокол из представленных – EAP. Дополнительные настройки для протокола PEAP описаны далее в соответствующем разделе. Для использования в локальной сети может быть достаточно протокола MS-CHAPv2. Не рекомендуется использовать протоколы PAP/CHAP в виду их слабой защищённости.

Настройки для протокола PEAP.

При выборе опции «Протокол расширенной проверки подлинности (EAP)» становится доступным список протоколов, из которого необходимо выбрать протокол PEAP. По нажатию кнопки «Свойства» отобразится диалог «Дополнительные параметры безопасности» для задания настроек PEAP. В диалоге следует выбрать опции проверки сертификата RADIUS сервера или отключить проверку сертификатов. При включённой опции «Проверять сертификат сервера» на компьютере клиента, в хранилище сертификатов, должен быть установлен корневой сертификат SoftPI RADIUS сервера. Этот сертификат должен быть выбран в списке «Доверенные корневые центры сертификации». Другие опции следует задать, как показано на рисунке 12.

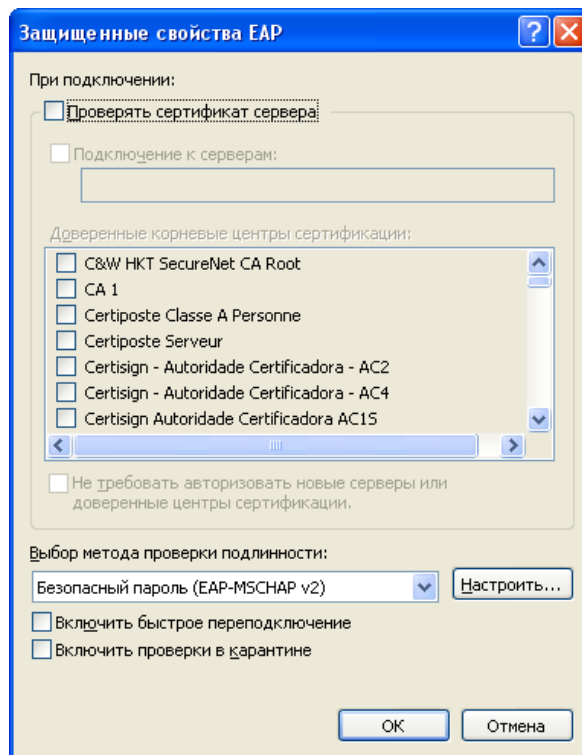


Рисунок 12

На рисунке 13 показан вид окна свойств метода проверки подлинности EAP-MSCHAP v2.

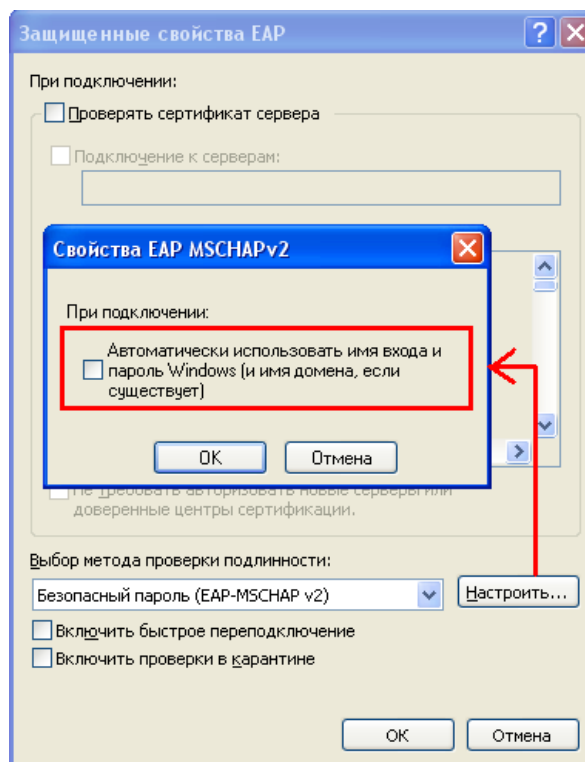


Рисунок 13

Пример настройки для Windows Vista/Windows 7

Порядок действий по созданию и настройке подключения через VPN канал для операционных систем Windows Vista и Windows 7 аналогичный инструкциям для Windows XP. На рисунках, приведенных ниже, показаны основные шаги настройки для Windows 7.

Откройте режим "Панели управления" Windows, позволяющий создать VPN подключение (рисунки 14, 15).

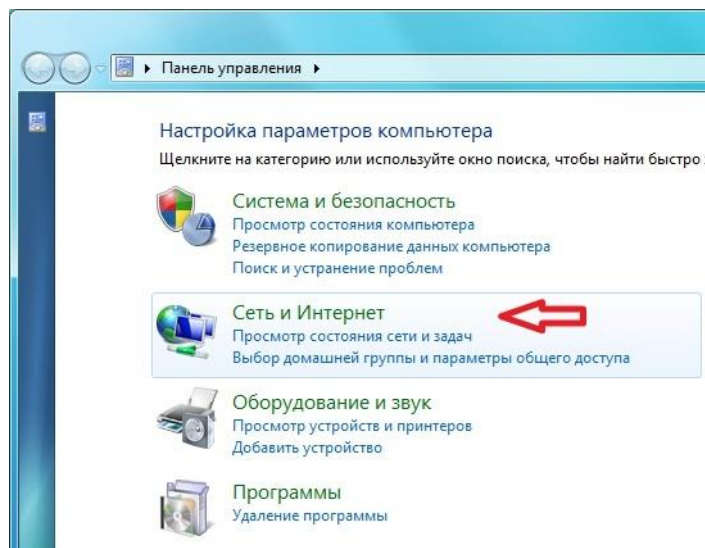


Рисунок 14

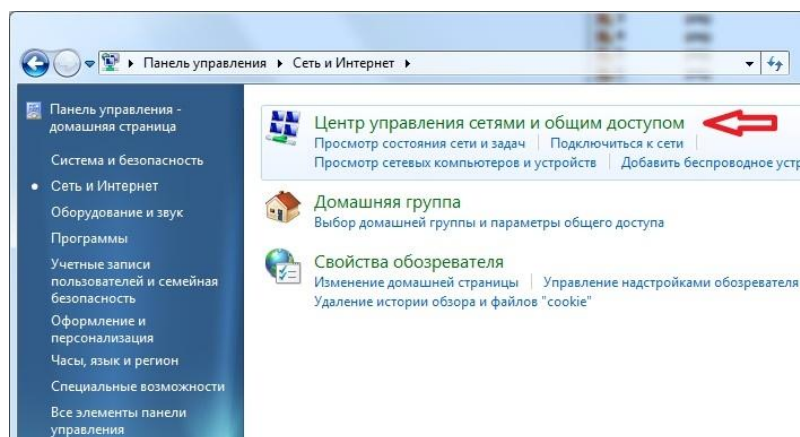


Рисунок 15

Далее необходимо открыть мастер создания подключения, как показано на рисунке 16.

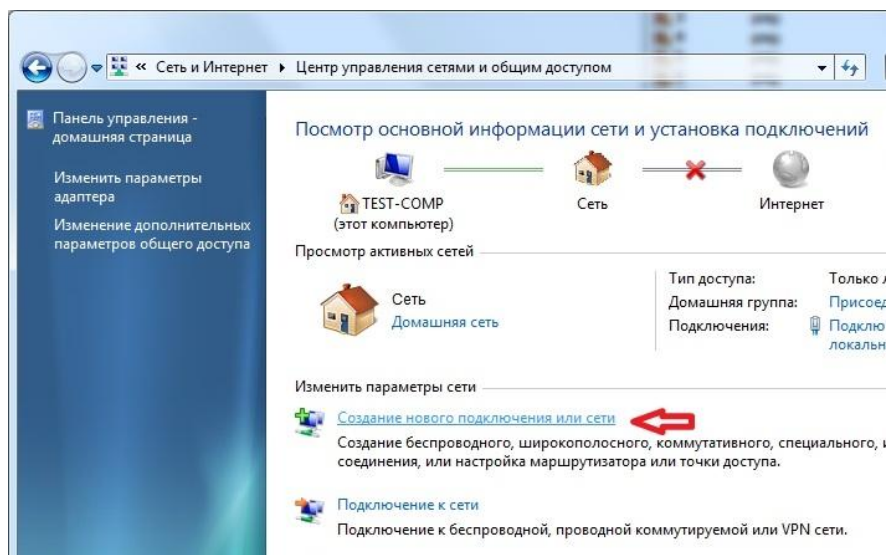


Рисунок 16

Выберете тип подключения «Подключение к рабочему месту» (VPN) (рисунок 17).

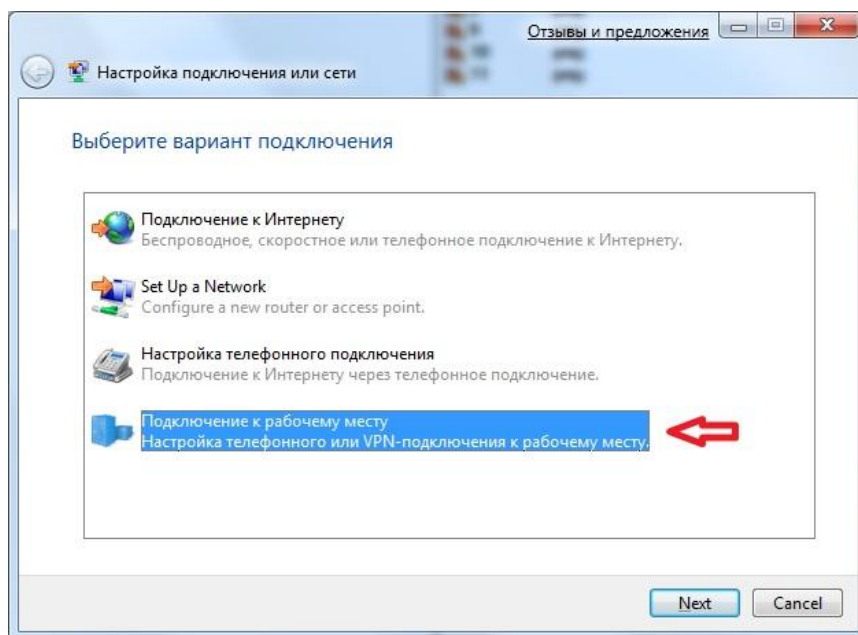


Рисунок 17

Для создания нового подключения выбираем тип подключения «Подключение к сети с помощью виртуальной частной сети (VPN)» (рисунки 18 - 19).

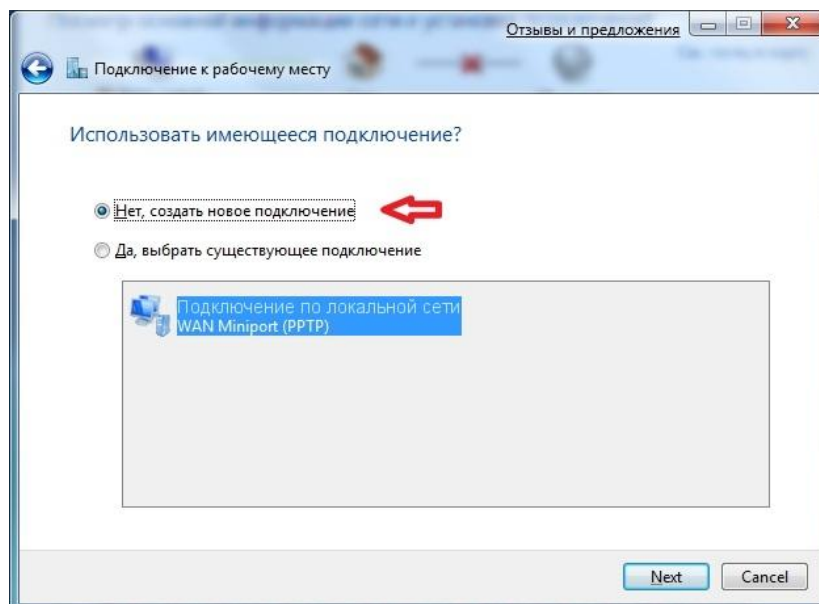


Рисунок 18

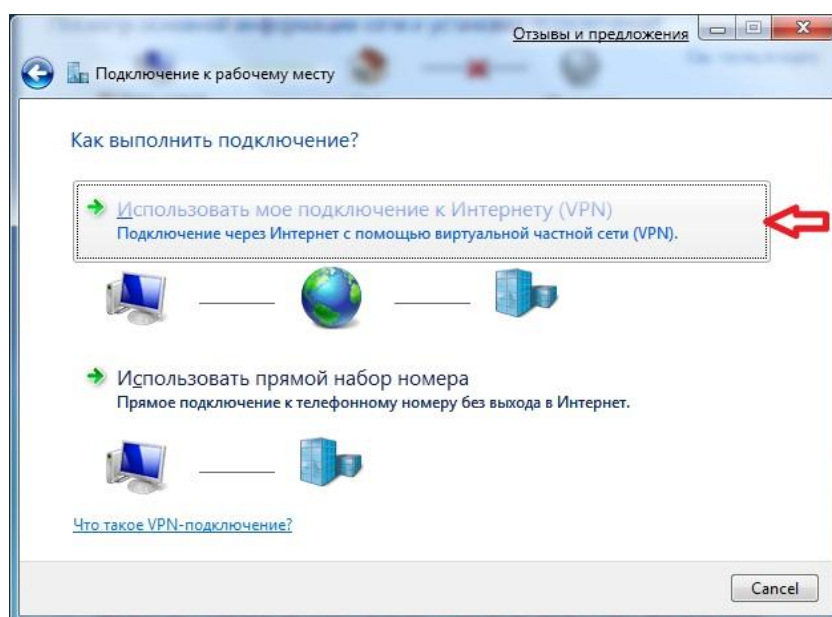


Рисунок 19

Далее следует выбрать параметр «Отложить настройку подключения к Интернету», т.к. не все параметры еще установлены (рисунок 20).

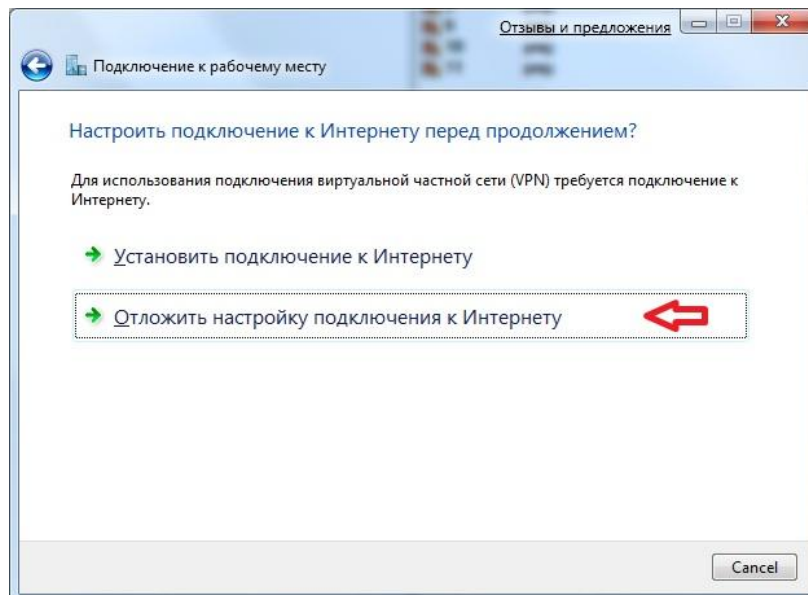


Рисунок 20

Введите адрес или доменное имя сервера VPN, и произвольное имя создаваемого подключения (рисунок 21).

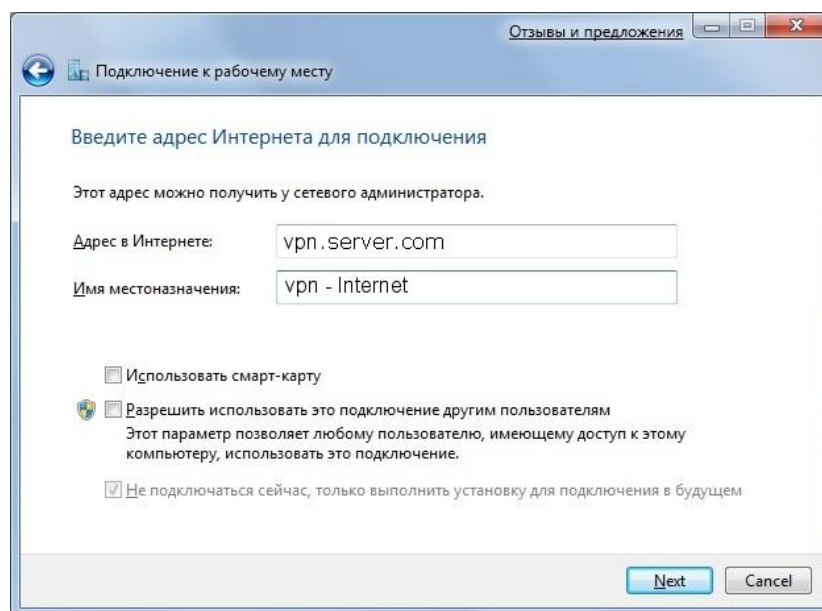


Рисунок 21

Введите логин и пароль (рисунок 22).

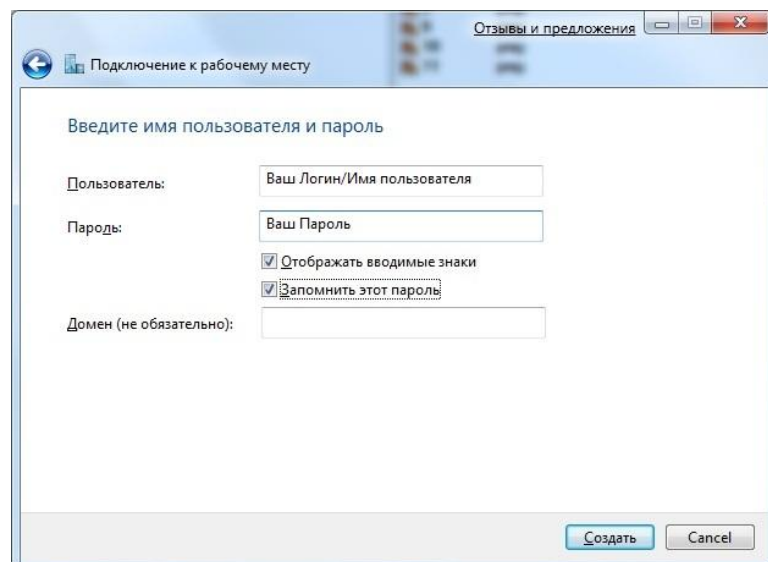


Рисунок 22

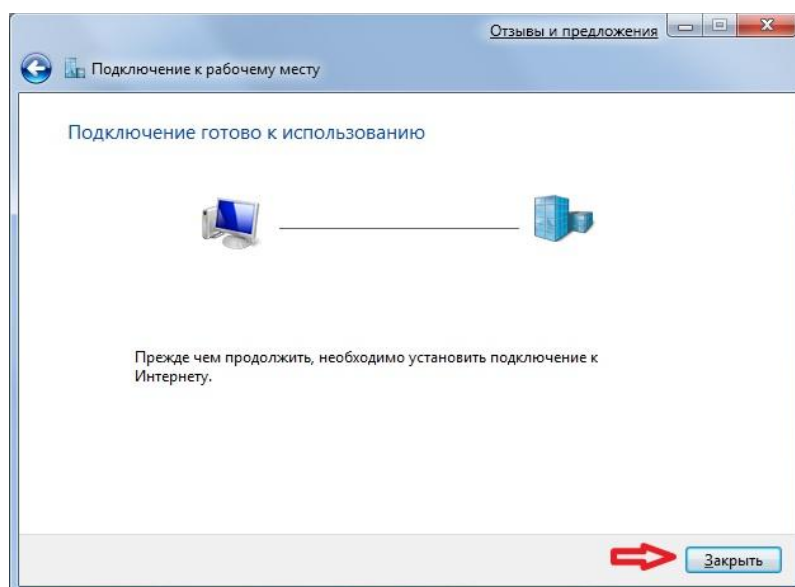


Рисунок 23

После создания подключения следует перейти к его свойствам и настроить параметры безопасности. Настройка аналогична настройке для Windows XP.