VPNR-i10 Base
VPNR-i05 Base

Техническое руководство

модель i10

модель i05

Содержание

1. Общие сведения

Сервер удалённого доступа VPNR, далее VPN (Virtual Private Network — виртуальная частная сеть) сервер либо просто сервер, предназначен для организации удалённого доступа к внутренним ресурсам локальной сети, по средствам создания виртуального, защищённого, канала связи через Интернет.
Доступ к ресурсам локальной сети может быть получен из любой точки мира где есть доступ к Интернет, при этом, для удалённого клиента создаётся полная эмуляция работы в локальной сети, так как если бы он был подключен к ней физически.
В качестве ресурсов подразумевается любое устройство с поддержкой протокола IP, это может быть файловое хранилище, система видеонаблюдения, одиночная IP камера, отдельный компьютер, система контроля доступа или хранилище баз данных, внутренняя система сообщения или документооборота, мультимедийные и развлекательные системы и т. д. Ко всем этим ресурсам можно получить доступ в любой момент времени из любой точки мира.

Принцип организации удалённого доступа можно описать следующим образом.
Удалённые клиент соединяется с VPN сервером используя для этого глобальную сеть Интернет. При этом в случае успешной авторизации, между VPN сервером и удалённым клиентом организуется виртуальный, зашифрованный канал передачи данных, сквозь который пользователь получает доступ к внутренним ресурсам локальной сети так, как если бы он был подключен локально (рис 1.1).

Рисунок 1.1.

Важной отличительной особенностью, в сравнении с технологией удалённого рабочего стола, является возможность одновременного подключения множества удалённых клиентов и полная эмуляция локального сетевого подключения, с доступом к любым ресурсам локальной сети.

VPN сервер представляет собой полностью законченное программно-аппаратное решение. Для большего удобства размещения, допускается как вертикальная так и горизонтальная установка сервера (рис. 1.2).

Рисунок 1.2.*

* - На рисунке показан внешний вид модели VPNR-i10 Base

Управление сервером осуществляется при помощи максимально упрощённого Web интерфейса, рассчитанного в первую очередь на не подготовленного пользователя. Все настройки организованны таким образом чтобы избежать возможных ошибок со стороны того кто будут осуществлять настройку и управление VPN сервером. Все изменяемые параметры снабжены всплывающими подсказками, в которых содержится вся необходимая информация для настройки.
Одной из отличительных особенностей является, отсутствие необходимости установки дополнительного программного обеспечения на операционную систему удалённых клиентов. Весь процесс настройки клиентов осуществляется штатными средствами операционной системы, предельно прост и детально задокументирован.

2. Выбор соединения

Прежде чем приступать непосредственно к настройке сервера необходимо ознакомиться с информацией по выбору соединения с сетью Интернет. Данный пункт является одним из ключевых. От правильности выбора соединения, будет зависеть дальнейшая работа всей системы удалённого доступа в целом.

Соединение с VPN сервером целиком зависит от качества соединения с Интернет, причём как со стороны клиента так и со стороны сервера. Именно по этому следует крайне внимательно отнестись к процессу выбора соединения, и его характеристикам.
Следует различать соединение сервера с Интернет и соединение удалённого клиента с Интернет.
В не зависимости от выбранного подключения, оно должно удовлетворять следующим требованиям:

1. Наличие реального IP адреса (только на стороне VPN сервера)
2. Отсутствия фильтрации трафика: PPTP (GRE), 1723TCP, 1723UDP, 1701UDP, 1522TCP
3. Для соединения по протоколу PPTP требуется корректная поддержка протокола GRE
4. Стабильное соединение, обеспечивающие необходимую пропускную способность.

Под реальным адресом подразумевается то, что этот адрес должен действительно существовать в адресном пространстве сети Интернет, или проще говоря должен быть уникальным.
Ниже приведены ориентировочные (примерные) значения по выбору скорости соединения, в зависимости от того какие внутренние ресурсы сети будут использоваться удалённо (табл. 2.1).

Таблица 2.1.

Используемые ресурсы	Минимальная рекомендуемая скорость
Работа с документами Word, Excel	0.5 Мбит/с
Работа с системами контроля доступа	0.5 Мбит/с
Видеонаблюдение (1 IP камера)	1 Мбит/с

Значения приведены расчёте на одного удалённого пользователя. Соответственно при нескольких удалённых (одновременно активных) подключениях эти значения должны быть умножены на число этих подключений. Также следует учитывать ещё и тот факт, что Интернет канал может также использоваться непосредственно для приложений локальной сети, например просмотр Web страниц, почты, общения и др.
В общем случае выбор способа соединения и поставщика доступа к Интернет (провайдера) зависит от множества факторов, и в каждом конкретном случае носит индивидуальный характер. В приложении, пункт «Поддерживаемые провайдеры», вы можете ознакомиться со списком провайдеров которые были проверены на работу с VPN сервером.

2.1 Соединение сервера с Интернет

Наиболее предпочтительным является проводное соединение сервера с Интернет.
Мобильное или иначе говоря беспроводное подключение не желательно и его следует использовать только в том случае если проводное соединение не возможно.
Мобильные подключения по средствам GPRS и EDGE, поддерживаются но при этом качество такого соединения как правило оставляет желать лучшего. Так например теоретическая скорость для GPRS составляет 171,2 кбит/с, а для EDGE 474 кбит/с, однако на практике реальная скорость в 5-15 раз меньше, что делает их практически не применимыми. Именно по этому, если всё же используется мобильное подключение,то рекомендуется использовать 3G либо 4G сети, в которых скорость и качество соединения находятся на достаточно высоком уровне.
От выбора типа соединения сервера с сетью Интернет напрямую зависит режим его работы.
VPN сервер может осуществлять работу в двух режимах «Маршрутизатор и VPN» либо «Только VPN».

В первом случае сервер также является маршрутизатором сети обеспечивая при этом наибольшее быстродействие и наилучшую стабильность соединения, но для этого режима необходимо наличие выделенной линии по технологии Ethernet (без авторизации), либо соответствующая поддержка беспроводного USB адаптера (в комплект поставки не входит). Список поддерживаемых USB адаптеров вы можете найти в пункте «Технические характеристики».

Во втором случае в качестве маршрутизатора выступает внешнее устройство с поддержкой маршрутизации (далее модем либо сторонний маршрутизатор) которое обеспечивает связь с Интернет. При этом стабильность соединения и пропускная способность будут также зависеть от модема.
В данном режиме работы необходимо перенаправить все поступающие VPN запросы с стороннего маршрутизатора (модема) на VPN сервер.
Далее будут рассмотрены оба режима работы.

2.1.1 Режим «Маршрутизатор и VPN»

В данном режиме сервер выступает в роли VPN сервера и маршрутизатора сети. Этот режим является предпочтительным.
Для работы в режиме «Маршрутизатор и VPN» необходима выделенная линия по технологии Ethernet, и отсутствие дополнительной авторизации у провайдера (PPTP, L2TP, PPPoE и др.), либо поддержка соответствующего беспроводного USB адаптера (например 4G Yota: Samsung SWC-U200).
Схема работы сети в таком режиме показана на рисунке 2.1.

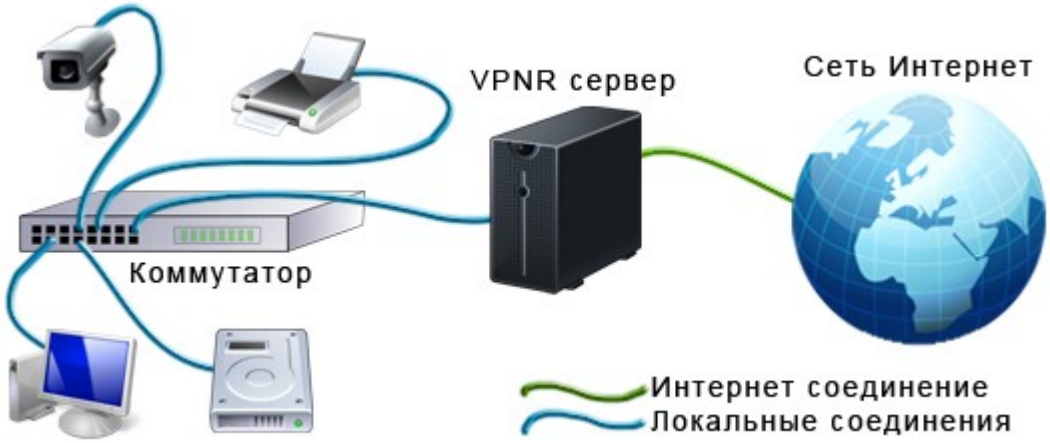


Рисунок 2.1.

В зависимости от выбранного способа подключения, на сервере будут задействованы либо 2 Ethernet порта - «Internet» и «LAN», либо 1 Ethernet порт - «LAN» и беспроводной USB адаптер.

Для проводного соединения сервера с Интернет используется Ethernet порт «Internet» в который подключается выделенная линия от провайдера.

Для беспроводного соединения сервера с Интернет используется беспроводной USB адаптер подключенный в любой свободный USB порт.

Исходящие Интернет запросы от внутренний сети поступают на VPN сервер который перенаправляет их в Интернет.
Поступающие VPN запросы из Интернет попадают непосредственно на VPN сервер, и в случае успешной авторизации удалённым клиентам предоставляется доступ к внутренним ресурсам локальной сети.

2.1.2 Режим «Только VPN»

В случае невозможности использования режима «Маршрутизатор и VPN», следует использовать режим «Только VPN». В данном случае в качестве маршрутизатора будет выступать модем обеспечивающий связь с Интернет. При этом стабильность соединения и пропускная способность будут также зависеть от модема.
Важно понимать что при такой схеме работы модем должен уметь перенаправлять все поступающие VPN запросы на VPN сервер. О том, как это сделать, читайте пункт «Настройка стороннего маршрутизатора».

Схема работы сети в таком режиме показана на рисунке 2.2.

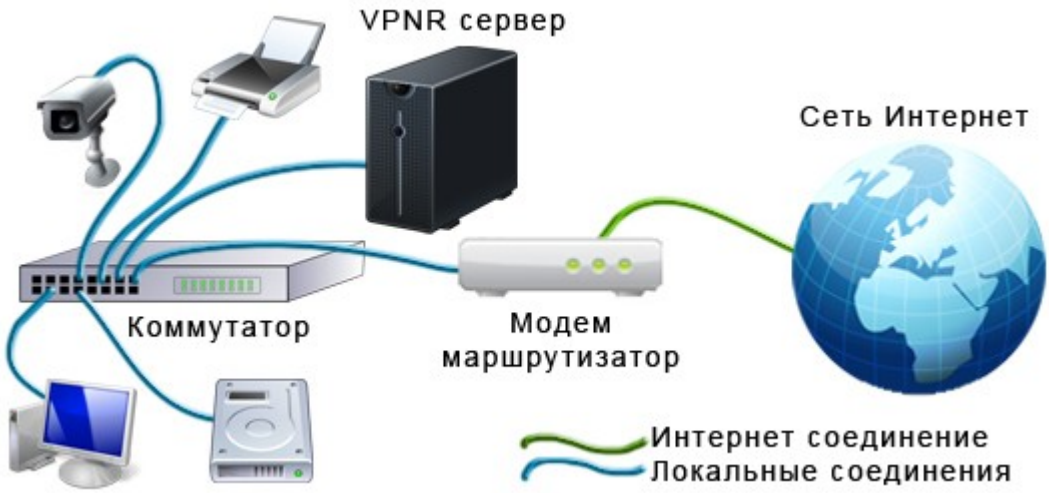


Рисунок 2.2.

В таком режиме на сервере задействован только 1 Ethernet порт. Порт - «LAN» подключается к коммутатору внутренний сети.
При такой схеме работы, доступ клиентам локальной сети к Интернет предоставляет сторонний маршрутизатор (модем).
Поступающие из Интернет VPN запросы попадают на сторонний маршрутизатор, который перенаправляет их на VPN сервер, который уже в свою очередь, в случае успешной авторизации, предоставляет удалённым клиентам доступ к внутренним ресурсам локальной сети.

2.2 Соединение клиентов с Интернет

В целом для выбора способа подключения клиентов к сети Интернет следует руководствоваться теми же принципами что и для сервера, хотя требования здесь более мягкие.
Наиболее оптимальным вариантом является проводное подключение по выделенной линии, вне зависимости от технологии, как например Ethernet или ADSL. Разумеется, такое подключение должно обеспечивать необходимую скорость подключения и соответствующее качество. Такой вид соединения не всегда удобен в силу отсутствия мобильности, и в случае её необходимости следует прибегнуть к беспроводному (мобильному) Интернет.
Как и в случае с сервером не рекомендуется использовать GPRS и EDGE соединения, скорость которых в реальных условиях далека даже от теоретических значений, а качество, мягко говоря, оставляет желать лучшего.
Оптимальным вариантом здесь является использование 3G и 4G сетей. Обе эти технологии, при должных условиях, обеспечивают достаточно высокую скорость и качество соединения.
Следует отметить, что в случае выбора 3G подключения, модемы обеспечивающие связь с Интернет, могут, в случае отсутствия 3G сети, начать работать в обычном GPRS или EDGE (2.5G) режиме, и не обеспечить требуемую скорость и качество соединения.
О возможности доступа по технологии 3G и 4G в конкретном месте проконсультируйтесь с сотрудниками компании предоставляющий доступ к Интернет.
Также существуют условно мобильные соединения — Wi-Fi. При такой схеме подключения, клиент сначала, по беспроводному каналу, подключается к W-iFi точке доступа, а та уже в свою очередь предоставляет доступ к сети Интернет. Радиус действия одной такой точки доступа как правило ограничен несколькими десятками метров, и данный вариант соединения является наилучшем если клиент находиться в рамках ограниченного пространства, например дома, в офисе или кафе с Wi-Fi.
В данном случае скорость и качество зависит как от соединения клиента с Wi-Fi точкой доступа, так и от соединения точки доступа с сетью Интернет.

3. Подключение и первоначальная настройка сервера

На данном этапе должно быть чёткое понимание того в каком режиме будет работать сервер, от этого будет зависеть его подключение и настройка. Также рекомендуется произвести планирование внутренний сети, если её ещё нет, либо произвести её ревизию в случае если она уже существует. Под планированием и ревизией здесь понимается чёткое представление о том какие внутренние адреса будут применяться, какое оборудование в сети, какова топология сети и т. д. Структурированный, системный подход к внутренний организации сети позволит избежать многих возможных ошибок. В приложении, пункт «Примеры планирования сети», вы можете ознакомиться с примерами планирования сети.

3.1 Установка и подключение

В зависимости от условий эксплуатации, выберете горизонтальную либо вертикальную установку сервера. После этого, прикрепите входящие в комплект ножки, на одну из боковых сторон, в специально предназначенные для этого выемки в корпусе.
По скольку VPN сервер (особенно в случае если он выполняет также и роль маршрутизатора) является одним из ключевых элементов сети, то для обеспечения его стабильной работы рекомендуется использовать системы бесперебойного питания.
На задней панели корпуса расположены все необходимые разъёмы для его подключения (рис. 3.1).

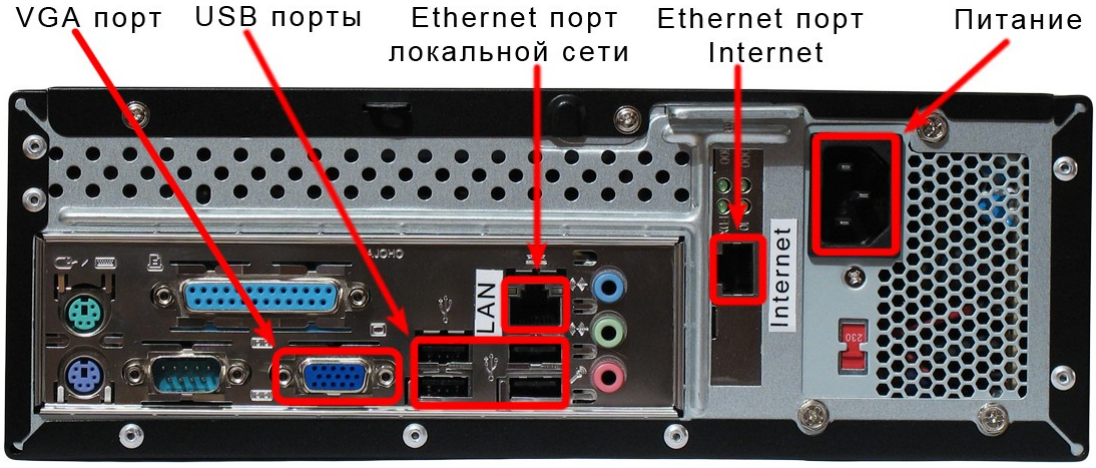


Рисунок 3.1.

В зависимости от необходимого режима работы сервера и способа его соединения с Интернет, подключение будет несколько отличаться.

3.1.1 Режим «Маршрутизатор и VPN», проводное соединение с Интернет

Перед тем как использовать проводное соединение с Интернет, удостоверьтесь в том что выбранный провайдер поддерживает доступ в сеть по выделенной Ethernet линии без дополнительной авторизации (PPTP, L2TP, PPPoE и др.), а также предоставляет услугу «Реального IP адреса».
Стандартными методами удостоверьтесь в том что соединение стабильно, а пропускная способность канала достаточна. Если вы ещё не оплатили услуги, сделайте это для того чтобы иметь полноценный доступ в Интернет. Также в случае необходимости подключите услугу «Реального IP адреса», о том как это сделать проконсультируйтесь с вашим Интернет провайдером.
Только после того как все вышеперечисленный действия произведены, подключите в порт с надписью «Internet» кабель приходящий от Интернет провайдера.

3.1.2 Режим «Маршрутизатор и VPN», беспроводное соединение с Интернет

Перед тем как использовать беспроводное соединение по средствам специального USB адаптера, обязательно удостоверьтесь в том, что он поддерживается сервером. Список поддерживаемых USB адаптеров вы можете найти в пункте «Технические характеристики».
Далее необходимо проверить соединение с Интернет стандартным способом, подключив беспроводной USB адаптер к компьютеру.
Удостоверьтесь в том что соединение стабильно, а пропускная способность канала достаточна. Если вы ещё не оплатили услуги, сделайте это для того чтобы иметь полноценный доступ в Интернет. Также вам

необходимо подключить услугу «Реального IP адреса», о том как это сделать проконсультируйтесь с вашим Интернет провайдером, как правило эта услуга подключается бесплатно в течении 1-2 дней, по требованию клиента.
Только после того как все вышеперечисленный действия произведены, подключите беспроводной USB адаптер к серверу удалённого доступа в любой USB порт.
Помните что если вы не оплатили услуги доступа в Интернет, или не подключили услугу «Реального IP адреса», вы не сможете пользоваться удалённым доступом.

3.1.3 Режим «Только VPN»

В данном режиме работы, на сервере будет задействован только один Ethernet порт - «LAN», который после первоначальной настройки необходимо будет подключить к внутренней локальной сети. Удостоверьтесь в том что ваш модем обеспечивает стабильное соединение и необходимую пропускную способность. Также вам необходимо подключить услугу «Реального IP адреса», о том как это сделать проконсультируйтесь с вашим Интернет провайдером. После этого, вам необходимо соответствующим образом настроить ваш модем, для перенаправления поступающих VPN запросов на сервер удалённого доступа. О том, как это сделать, читайте пункт «Настройка стороннего маршрутизатора».

3.1.4 Настройка стороннего маршрутизатора

Как было написано ранее, для того чтобы предоставить удалённый доступ клиентам, когда сервер работает в режиме «Только VPN», необходимо перенаправить все поступающие VPN запросы с стороннего маршрутизатора на сервер. Это делается за счёт перенаправления входящего трафика (port forwarding или virtual server) на VPN сервер.

Необходимо перенаправить следующие типы запросов:

xxx.xxx.xxx.xxx - GRE → yyy.yyy.yyy.yyy - GRE
xxx.xxx.xxx.xxx - 1723TCP → yyy.yyy.yyy.yyy – 1723TCP
xxx.xxx.xxx.xxx - 1723UDP → yyy.yyy.yyy.yyy - 1723UDP
xxx.xxx.xxx.xxx - 1701UDP → yyy.yyy.yyy.yyy – 1701UDP
xxx.xxx.xxx.xxx - 1522TCP → yyy.yyy.yyy.yyy – 1522TCP
где:
xxx.xxx.xxx.xxx – Интернет (внешний) IP адрес стороннего маршрутизатора
yyy.yyy.yyy.yyy – Локальный (внутренний) IP адрес VPN сервера

Следует отметить, что для работы по протоколу PPTP сторонний маршрутизатор должен корректно поддерживать перенаправление протокола GRE.
Также в случае если ваш провайдер предоставляет вам динамический IP адрес вам потребуется включить и настроить сервис DDNS (Dynamic Domain Name System – система динамичных доменных имён) на вашем модеме.
Настройка стороннего маршрутизатора зависит от конкретной модели, о такой возможности и как это сделать читайте в инструкции по вашему маршрутизатору.

3.2 Вход на сервер

Для первоначального входа на сервер убедитесь что у компьютера с которого будет производиться настройка включён режим назначения IP адреса по DHCP. О том как это сделать вы можете узнать в справке по вашей операционной системе. В приложении, пункт «Настройка сети», вы можете узнать как это сделать для операционной системы Windows.
Подключите сервер к источнику питания, и нажмите на кнопку включения расположенной на передней панели. После того как сервер загрузиться (~35 сек), вставьте в Ethernet «LAN» порт идущий в комплекте патч-корд, другой конец которого подсоедините к любому компьютеру.
Прямое соединение необходимо только на этапе первоначальной настройки, чтобы избежать влияния других участников сети.

Откройте браузер и наберите в строке адреса, IP VPN сервера.
Значение **IP по умолчанию: 192.168.55.1**.
В ответ на это вы увидите окно с предложением ввести имя пользователя и пароль (рис. 3.2) .
Имя пользователя: vpn_admin, **пароль по умолчанию: 123456**.

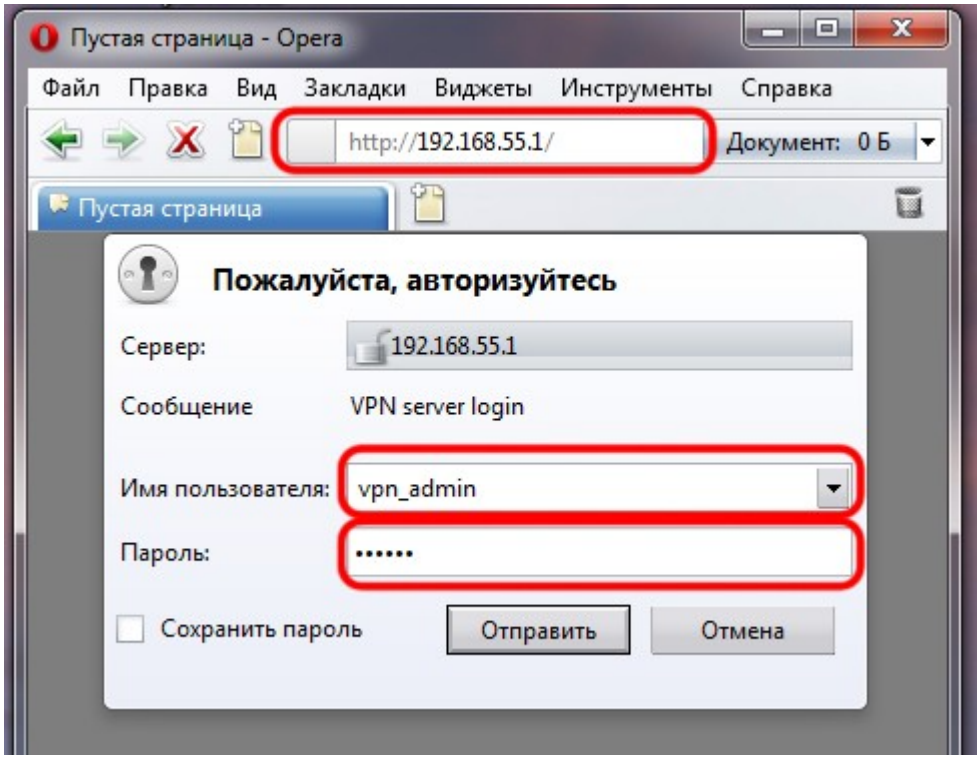


Рисунок 3.2.

После того как вход на сервер выполнен вы увидите окно с приветствием (рис. 3.3).

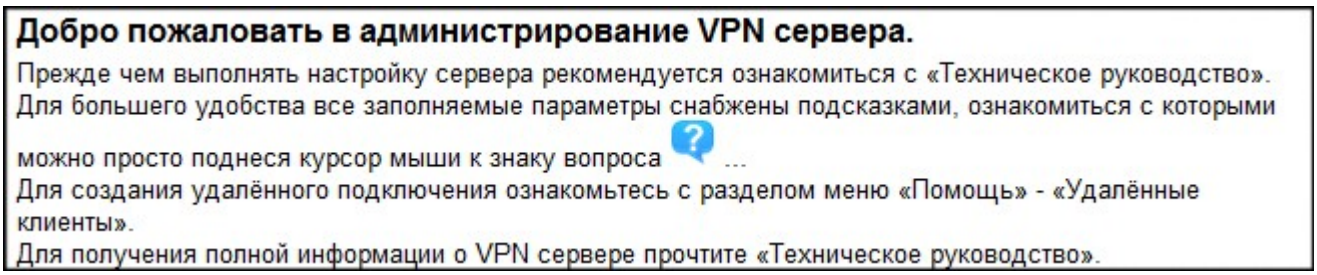


Рисунок 3.3.

Если сервер должен работать в режиме «Только VPN», срезу переходите к следующему пункту - «Локальные настройки».

3.3 Интернет настройки

На открывшейся странице, в меню, выберите - "Настройка: Интернет", после чего вам будут показаны текущие настройки Интернет (рис. 3.4).

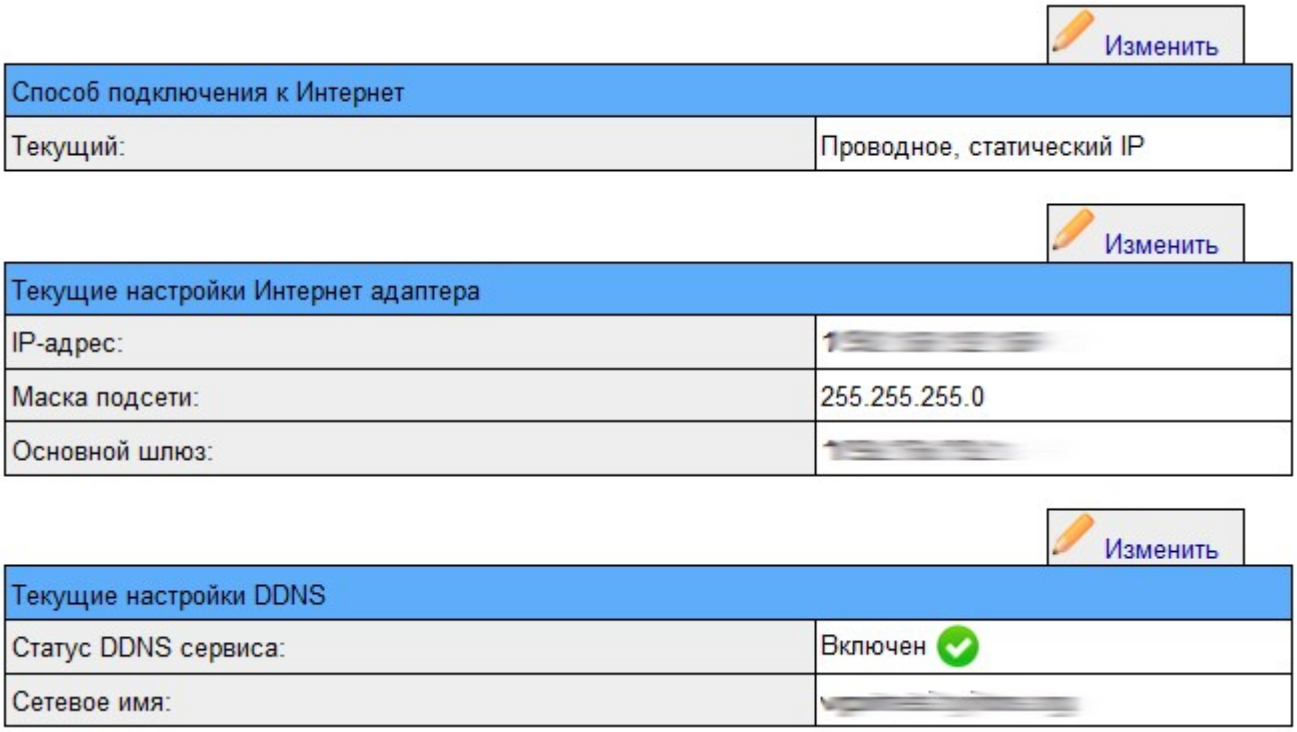


Рисунок 3.4.

В начале необходимо выбрать способ подключения к Интерет, для чего нажмите на закладку "Изменить", находящуюся в верхнем углу таблицы способа подключения к Интернет.
В открывшемся окне выберете желаемый способ подключения к Интернет, после чего подтвердите свой выбор нажав Сохранить (рис. 3.5).

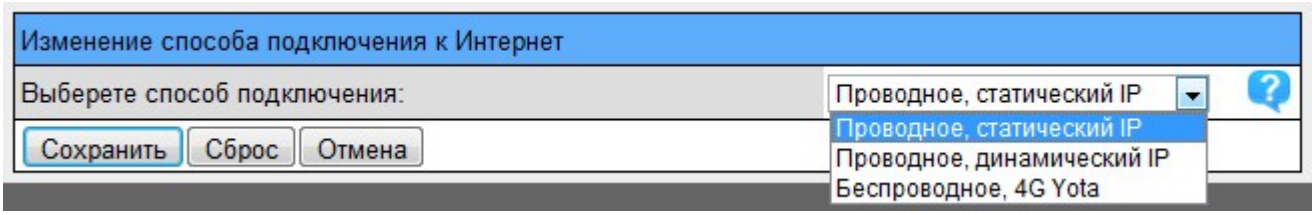


Рисунок 3.5.

Обратите внимание на то, что пункт "Беспроводное, 4G Yota" доступен только в случае если беспроводной USB адаптер подключен к серверу.

В случае если выбран способ подключения "Проводное, статический IP", также необходимо изменить настройки Интернет адаптера, для чего нажмите на закладку "Изменить" находящуюся в верхнем углу таблицы текущих настроек Интернет адаптера.
В открывшемся окне заполните соответствующее поля, значениями которые вам предоставил Интернет провайдер, после чего подтвердите свой выбор нажав Сохранить (рис. 3.6).

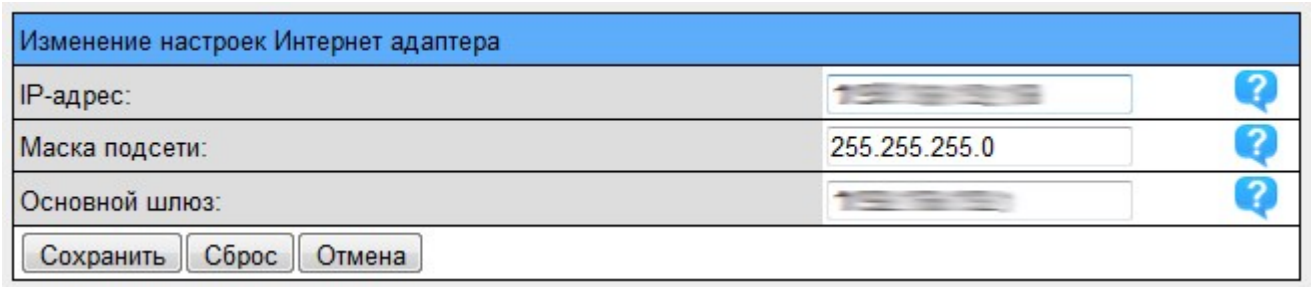


Рисунок 3.6.

Если вы выбрали способ подключения "Проводное, динамический IP" или "Беспроводное, 4G Yota", дополнительных IP настроек не требуется (рис. 3.7).

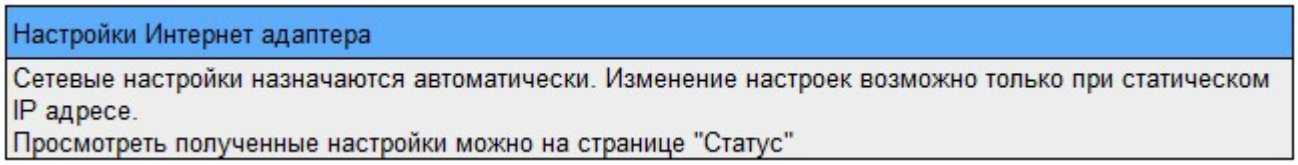


Рисунок 3.7.

В случае когда настройки назначаются автоматически, Интернет IP адрес будет постоянно меняться, что делает невозможным удалённые подключения по IP адресу.
Для этого случая необходимо использовать специальный сервис DDNS (Dynamic Domain Name System – система динамичных доменных имён), который позволяет использовать постоянное сетевое (доменное) имя для удалённого подключения, при меняющемся Интернет IP адресе.
Каждый раз, когда сервер удалённого доступа подключается к Интернет, он сообщает свой текущий IP адрес Интернет адаптера, при помощи DDNS сервиса. Этот IP адрес автоматически сопоставляется доменному (сетевому) имени. Это позволяет осуществлять удалённые подключения используя доменное имя, вне зависимости от того какой IP адрес назначен в данный момент серверу удалённому доступа.
Сервис DDNS можно также использовать и при статическом IP адресе, например для случая если ваш провайдер изменит сетевые настройки вам не придётся изменять настройки на удалённых клиентах.
Для использования DDNS необходимо пройти регистрацию на сайте одного из DDNS провайдеров, а также внести соответствующие изменения в своём аккаунте. О том как это сделать читайте в приложении, пункт «DDNS».
После того как вы зарегистрировались на сайте провайдера DDNS и выполнили соответствующие настройки в своём аккаунте, нажмите на закладку "Изменить" находящуюся в верхнем углу таблицы текущих настроек DDNS.
В открывшемся окне включите сервис и заполните соответствующее поля, значениями вашего аккаунта, после чего подтвердите свой выбор нажав Сохранить. (рис. 3.8). Обратите внимание на то, что если в качестве провайдера используется dyndns.com, то в поле Логин — вводится ваш логин, а в случае no-ip.com в поле Логин — вводится ваш e-mail.

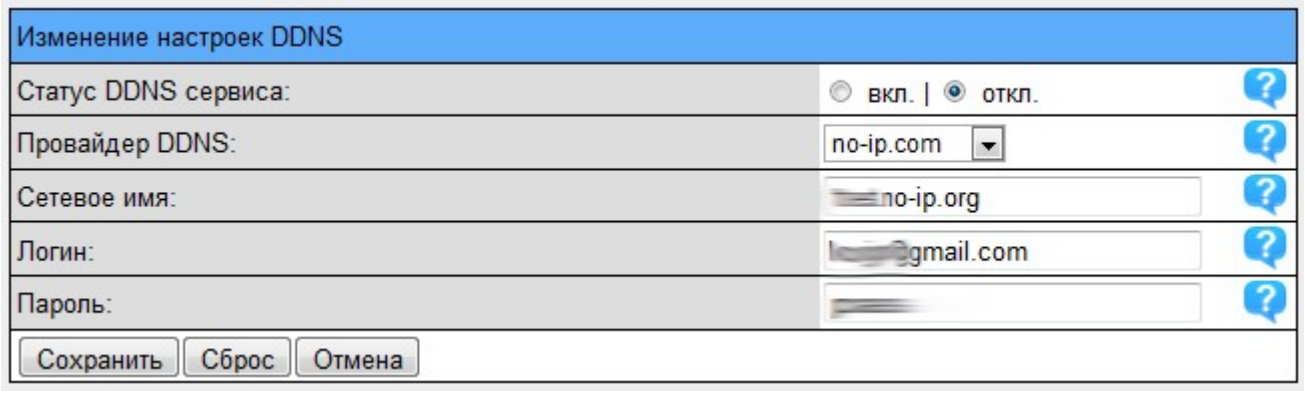


Рисунок 3.8.

В случае если всё было сделано верно, то на компьютере с которого вы настраиваете сервер должен появиться доступ к сети Интернет.
На этом настройка Интернет завершена.

3.4 Локальные настройки

Выберите в меню "Настройка: Локальные", после чего вам будут показаны настройки относящиеся к локальной сети (рис. 3.9).

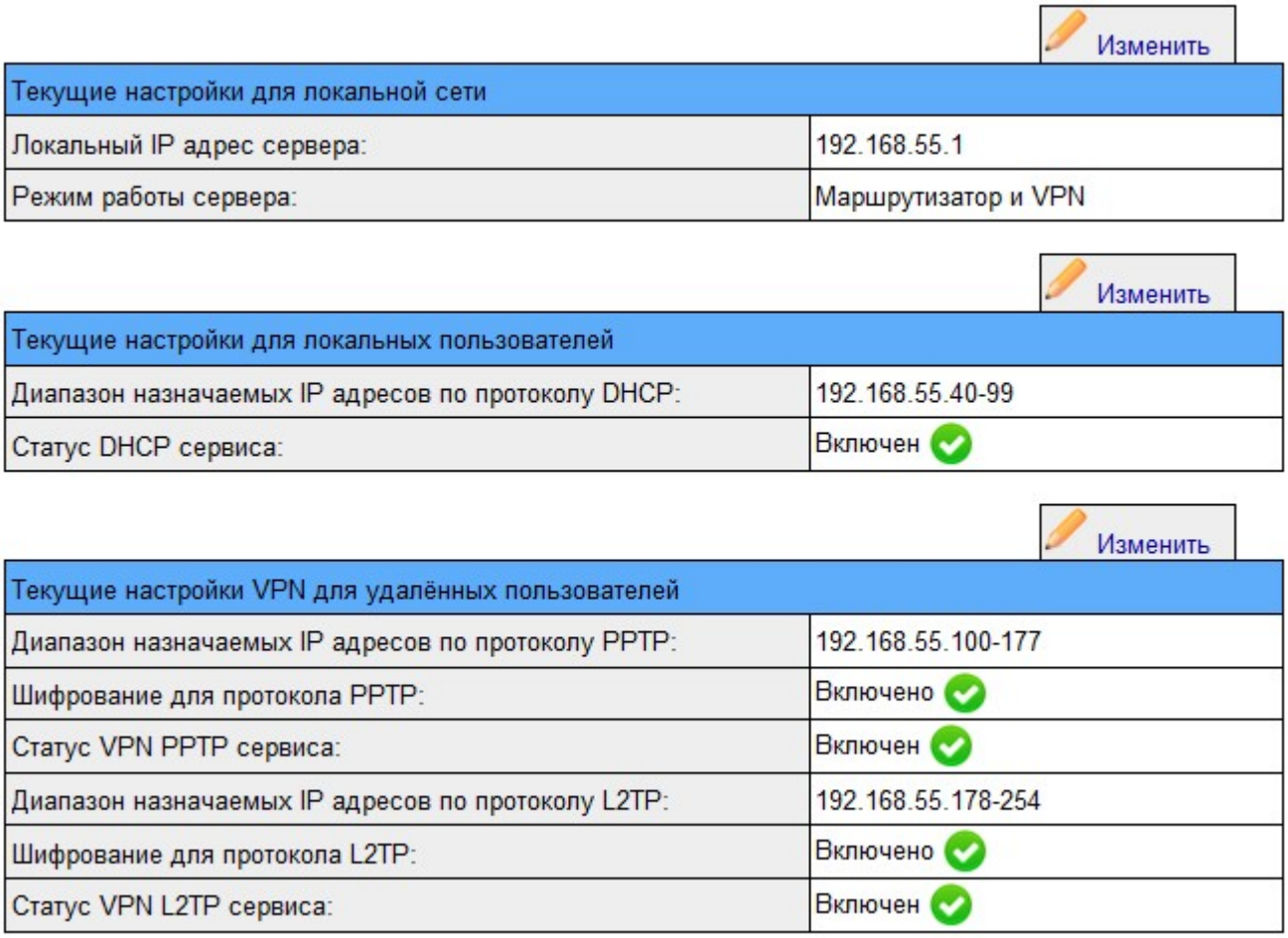


Рисунок 3.9.

Прежде всего необходимо изменить настройки для локальной сети, для чего нажмите на закладку "Изменить", находящуюся в верхнем углу соответствующей таблицы.
В открывшемся окне установите локальный IP адрес сервера с учётом подсети. При этом рекомендуется изменить номер подсети установленный по умолчанию (55) на любой другой, если вы только планируете сеть либо на номер подсети которая у вас уже используется.
В итоге должно получиться что-то на подобии 77.1 или например 158.1 и т. д. При этом первое число будет соответствовать номеру подсети и должно быть одинаковым на всех других устройствах входящих в локальную сеть, а второе число будет относиться к адресу сервера в этой сети и должно быть уникальным (рис 3.10).

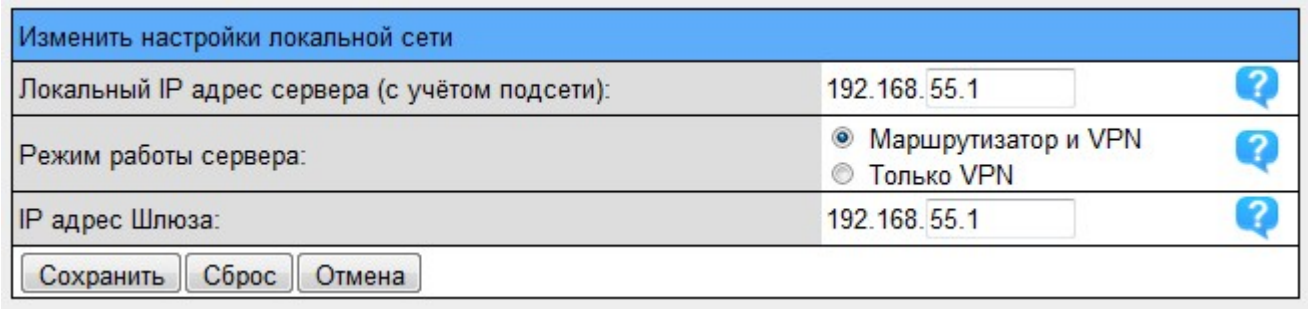


Рисунок 3.10.

Настоятельно не рекомендуется использовать подсети с номерами: 0, 1, 100!
Подсети с номерами: 0, 1, 100 как правило используют производители сетевого оборудования для домашних локальных сетей. Из-за этого велика вероятность того, что подсети с одинаковыми номерами будут использоваться как на стороне сервера так и на стороне удалённого клиента.
Это приведёт к тому что будет невозможно отделить адресное пространство локальной сети сервера от

адресного пространства внутренней сети удалённого клиента. Очевидно, что гораздо проще один раз изменить настройки на стороне сети сервера, чем менять сетевые настройки на стороне каждого удалённого клиента, которому необходимо предоставить доступ.
Настройки всех остальных служб будут изменены автоматически с учётом новой подсети.
В этом же окне необходимо выбрать режим работы сервера, а также если выбран режим «Только VPN» указать адрес шлюза (стороннего маршрутизатора, модема) который используется для соединения с Интернет.
После того как все изменения внесены, подтвердите свой выбор нажав Сохранить, при этом произойдёт перезагрузка сервера (рис 3.11).

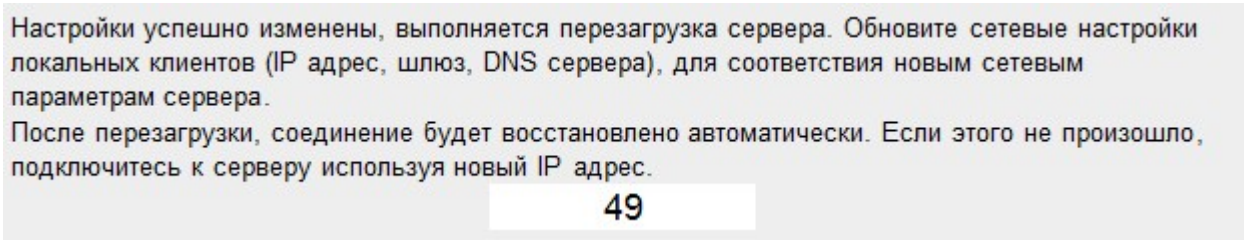


Рисунок 3.11.

Если вы последовали рекомендации и подсоединены к серверу, с помощью патч-корда, напрямую, DHCP сервис включён на VPN сервере а на компьютере выставлено автоматическое назначение IP адреса по DHCP, то в тот момент пока сервер перезагружается, отключите патч-корд от компьютера, подождите **15** секунд, после чего вновь подключите провод. Соединение должно восстановиться автоматически.

Если DHCP сервис выключен, на компьютере с которого производиться настройка, сетевые параметры указаны в ручную, или по каким-то иным причинам сетевые настройки не были изменены автоматически, то необходимо обновить их с учётом новых настроек сервера. Требуется (по необходимости) изменить IP адрес и шлюз. После этого введите новый IP адрес сервера, который вы установили ранее, в адресную строку браузера и повторите процесс подключения.

Когда вы возобновили связь с сервером, заново перейдите - "Настройка: Локальные", для продолжения процесса настройки параметров относящихся к локальной сети.

В VPN сервере присутствует DHCP сервер который отвечает за автоматическую выдачу IP адресов и др. сетевых настроек локальным клиентам. Другими словами если вы хотите, чтобы адреса в локальной сети назначались автоматически, или правильнее сказать динамически, DHCP сервис должен быть включён. Также при настройке, необходимо указать диапазон IP адресов из которого будут назначаться адреса локальным пользователям. Помните что в сети может быть только один DHCP сервер, по этому если в сети присутствует ещё один DHCP сервер (например в Wi-Fi точке доступа, модеме и т.д.), то его необходимо отключить, либо сделать это на VPN сервере. При этом рекомендуется чтобы сервис DHCP предоставлялся VPN сервером, а не другими устройствами сети.
При задании диапазона адресов выдаваемых DHCP сервером необходимо учесть, что этот диапазон не должен пересекаться с диапазоном адресов выдаваемых удалённым VPN пользователям, а также в него не должны попадать адреса других устройств сети. В случае необходимости измените настройки DHCP сервиса для локальных пользователей. Для изменения настроек нажмите на закладку "Изменить" соответствующей таблицы. После того как необходимые настройки измерены подтвердите свой выбор нажав Сохранить (рис. 3.12).

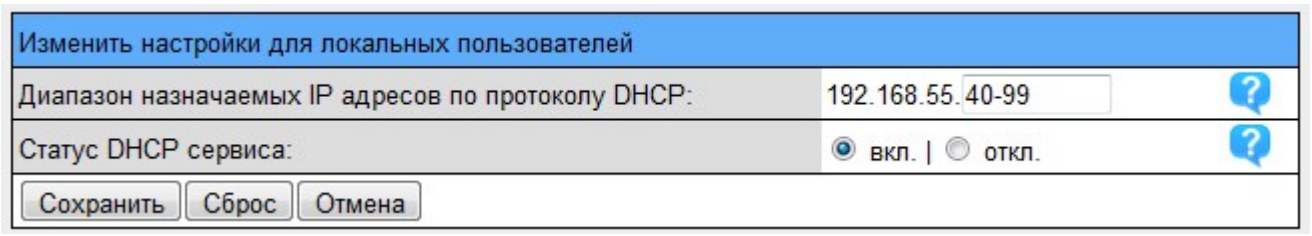


Рисунок 3.12.

Довольно часто бывают случаи когда конкретному устройству в сети необходимо назначить статический IP адрес, например файловому серверу, сетевому принтеру или IP камере. Это легко сделать вручную,

однако при этом важно учесть, что адрес, заданный таким способом, не должен входить в диапазон DHCP, PPTP, L2TP сервисов, но при этом такой адрес должен принадлежать соответствующей подсети.
Прочие сетевые настройки, которые необходимо задавать вручную: как то:

шлюз – локальный IP VPN сервера, либо IP адрес модема, в зависимости от режима работы
маска – всегда 255.255.255.0),
адреса DNS серверов – 8.8.8.8 либо 8.8.4.4 либо те которые назначил интернет провайдер

В приложении, пункт «Настройка сети», вы можете узнать как изменить сетевые настройки для операционной системы Windows.

Последним пунктом локальных настроек являются настройки VPN. Здесь необходимо задать диапазон IP адресов выдаваемых удалённым пользователям, а также изменить статус соответствующих сервисов.
VPN сервер поддерживает подключение удалённых пользователей по двум протоколам PPTP и L2TP. За поддержку каждого отвечает соответствующий сервис. Для большей совместимости рекомендуется оставить включёнными оба сервиса.
В зависимости от того по какому именно протоколу подключается удалённый пользователь, будет зависеть из какого диапазона он получит адрес. Соответственно, диапазоны PPTP и L2TP не должны пересекаться, также они не должны пересекаться с диапазоном DHCP а также в него не должны попадать адреса других устройств локальной сети.
Для каждого из протоколов возможно независимое включение и отключение шифрования передаваемых данных с использованием протокола MPPE.
При включённом шифровании, будут поддерживаться только шифрованные подключения, а при отключённом, только не шифрованные. Рекомендуется использовать шифрованные подключения. Не шифрованные подключения, необходимо использовать только в том случае если удалённый клиент не поддерживает протокол шифрования MPPE.
При необходимости измените настройки аналогично пред идущим (рис. 3.13).

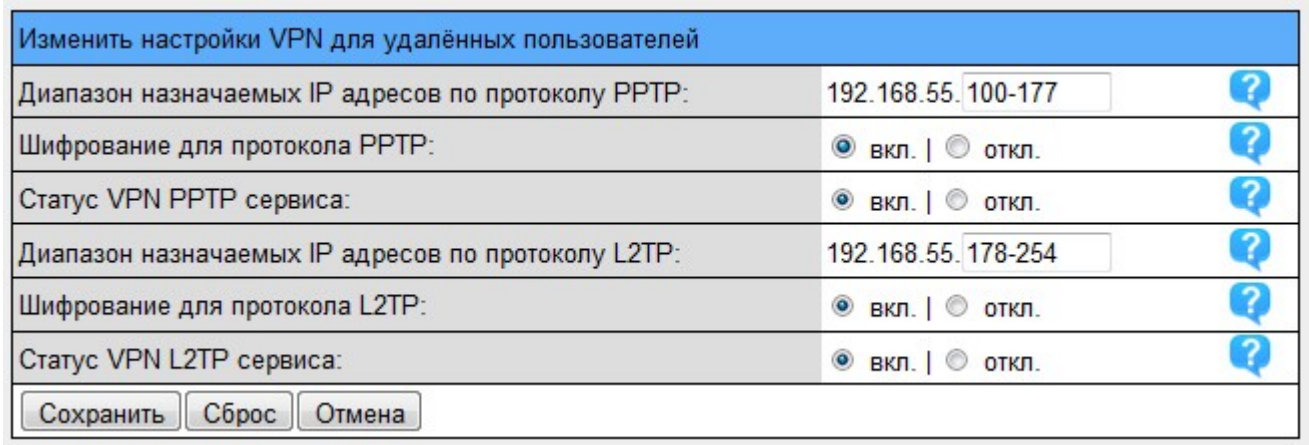


Рисунок 3.13.

После сделанных изменений ещё раз проверьте правильность локальных сетевых настроек, особенно на предмет не пересечения различных диапазонов IP адресов. Это довольно просто сделать, поскольку все они представлены на одной странице.

На этом предварительная настройка сервера завершена. Если сервер необходимо перенести в другое место, **обязательно выключайте его нажатием кнопкой питания**. После нажатия кнопки, сервер выключиться автоматически (~15сек.). Никогда не выключайте сервер простым выдёргиванием провода питания из сети.
Теперь вы можете отсоединить его от компьютера с помощью которого производилась настройка и подключить его к локальной сети, соединив «LAN» порт сервера с свободным портом коммутатора локальной сети.
Дальнейшие управление сервером возможно с любого компьютера локальной сети, по IP адресу который вы задали ранее.
Удалённое управление сервером возможно только в случае если вы подключены к нему через VPN соединение. Для обеспечения большей безопасности, удалённое управление сервером без VPN подключения запрещено.

4. Управление сервером

После того как первоначальная настройка выполнена и сервер подключен к внутренний (локальной) сети, а также, в случае необходимости, остальные участники сети настроены, подключитесь к нему используя IP адрес который был задан ранее.

4.1 Смена пароля администратора

Прежде чем продолжать дальнейшую настройку сервера необходимо изменить пароль для доступа к настройкам VPN сервера. Для этого выберите в меню - "Пользователи: Администратор" (рис. 4.1).

Рисунок 4.1.

Для изменения пароля администратора введите в соответствующие поля текущий пароль, а также новый пароль который вы будите использовать, после чего нажмите Сохранить. При этом имя администратора сервера всегда **vpn_admin** и не может быть изменено. Будьте внимательны к регистру и раскладке клавиатуры. Пароль может состоять из символов английского алфавита (от A-z) , цифр и символа подчеркивания (_).
В дальнейшем для получения доступа к серверу необходимо использовать новый пароль.
Если по каким-то причинам вы забыли пароль администратора, необходимо выполнить сброс настроек, о том как это сделать читайте в пункте «Сброс настроек».

4.2 Операции с VPN пользователями

Для добавления, удаления, редактирования а также изменения статуса удалённых VPN пользователей выберите в меню - "Пользователи: Пользователи VPN" (рис. 4.2).

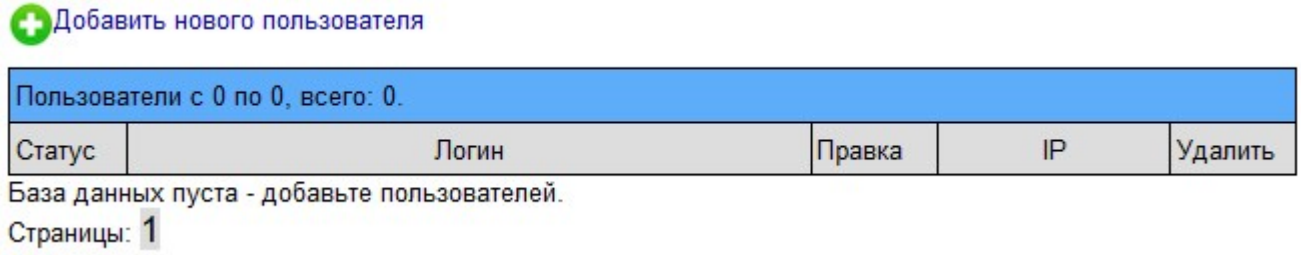


Рисунок 4.2.

Изначальна база данных с VPN пользователями пуста, и их необходимо добавить. Для этого нажмите на иконку "Добавить нового пользователя". В ответ на это вы увидите форму добавления нового пользователя (рис. 4.3).

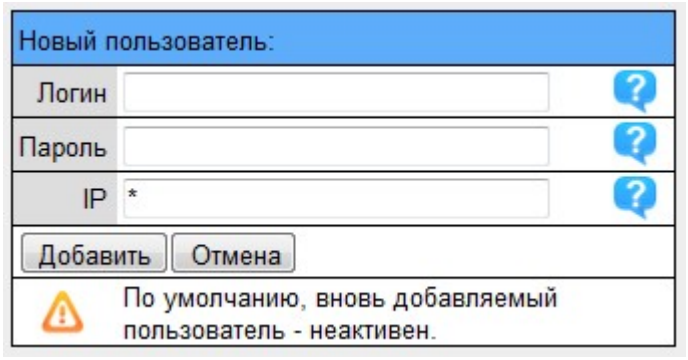


Рисунок 4.3.

"Логин" или иначе говоря имя пользователя, это уникальный набор символов, который будет отличать учетные записи пользователей между собой. Логин может состоять из символов английского алфавита (от A-z) , цифр и символа подчеркивания (_). При этом заглавные и строчные символы различаются т.е. «User» и «user» будут являться различными логинами.
При этом на сервере не может присутствовать двух пользователей с одинаковыми логинами, в противном случае он выдаст сообщение об ошибке, и предложит ввести другой логин.

"Пароль", это набор символов, который является секретным ключом для учётной записи пользователя. Пароль может состоять из символов английского алфавита (от A-z) , цифр и символа подчеркивания (_). При этом заглавные и строчные символы различаются т.е. «PassWord» и «password» будут являться различными паролями. При этом не рекомендуется использовать пароли менее 5-ти символов а также использовать в качестве паролей словарные слова.

Поле IP позволяет привязать определённому пользователю свой IP. Как правило это не требуется, и рекомендуется использовать автоматическую выдачу адреса из диапазона PPTP и L2TP сервисов, в зависимости от того по какому протоколу подключается клиент. Для автоматического назначения IP оставьте в поле символ "*" (звёздочка).

Данные введённые вами (Логин и Пароль) будут использоваться для VPN подключения.
После заполнения всех полей нажмите "Добавить", после чего перед вами вновь появится список пользователей, в котором будет присутствовать только что добавленный пользователь (рис. 4.4).

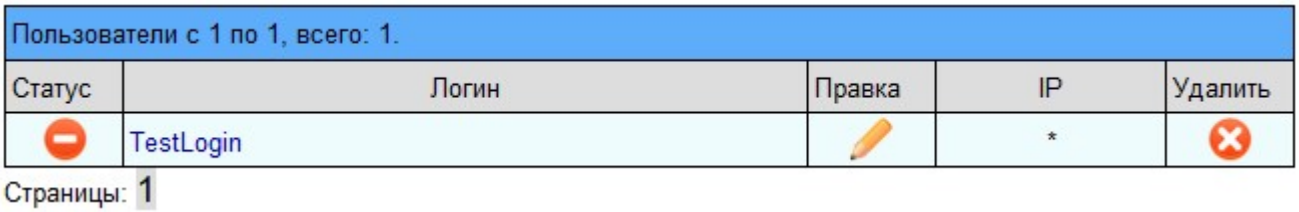


Рисунок 4.4.

По умолчанию вновь добавленному пользователю доступ закрыт, и он не может подключиться.
Для открытия ему доступа кликните мышкой на значок статуса напротив соответствующего пользователя. Это вызовет изменение статуса, о чём будет свидетельствовать соответствующий значок напротив пользователя (рис. 4.5).

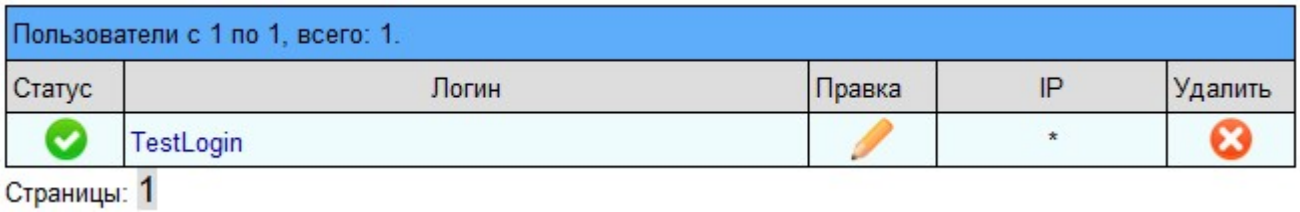


Рисунок 4.5.

Повторите данные действия для добавления других пользователей.

При большом числе пользователей используется постраничная навигация по всему списку, для чего необходимо выбрать соответствующую страницу щёлкнув на ней мышкой, при этом текущий номер страницы выделен серым цветом (рис. 4.6).

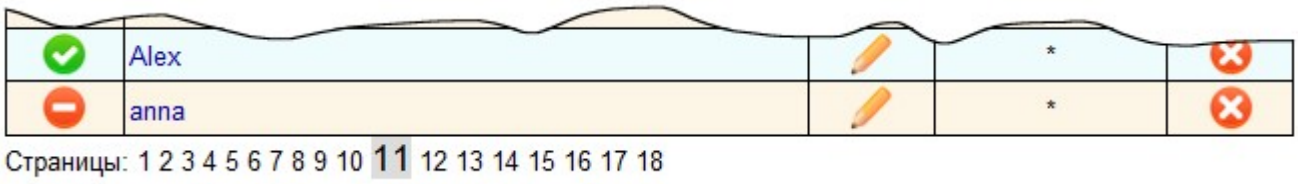


Рисунок 4.6.

Аналогичным образом происходит редактирование существующих пользователей, для этого достаточно кликнуть на иконку "Правка" либо кликнуть мышкой по имени пользователя (логину) данные которого необходимо изменить.
Для удаления пользователей кликните на иконку "Удалить" напротив необходимого пользователя.
При этом если необходимо заблокировать доступ пользователю на какое-то время, то для этого целесообразнее изменить его статус, а не удалять его.
После того как новые пользователи добавлены, а доступ необходимым пользователям открыт, можно осуществлять удалённые подключения. О том как это сделать читайте в пункте «Настройка клиентов».

4.3 Просмотр статуса

Для просмотра информации по текущему состоянию сервера, выберите в меню - "Информация: Статус".
При этом вы увидите страницу с информацией по текущему состоянию сервера (рис. 4.7).

Текущий статус Интернет адаптера	
Статус:	Подключен
IP-адрес:	94.25.191.
Маска подсети:	255.255.255.0
Отправленно:	35.4 Кбайт
Принято:	37.3 Кбайт

Текущий статус Локального адаптера	
Статус:	Подключен
IP-адрес:	192.168.55.1
Маска подсети:	255.255.255.0
Отправленно:	10.2 Кбайт
Принято:	11.5 Кбайт

Общая сетевая информация	
Статус соединения с Интернет:	Подключен
Режим работы сервера:	Маршрутизатор и VPN
Способ подключения к Интернет:	Беспроводное, 4G Yota
Используемый шлюз:	94.25.191.1
Диапазон назначаемых IP адресов по протоколу DHCP:	192.168.55.40-99
Диапазон назначаемых IP адресов по протоколу PPTP:	192.168.55.100-177
Диапазон назначаемых IP адресов по протоколу L2TP:	192.168.55.178-254
Сетевое имя DDNS:	dyndns.org

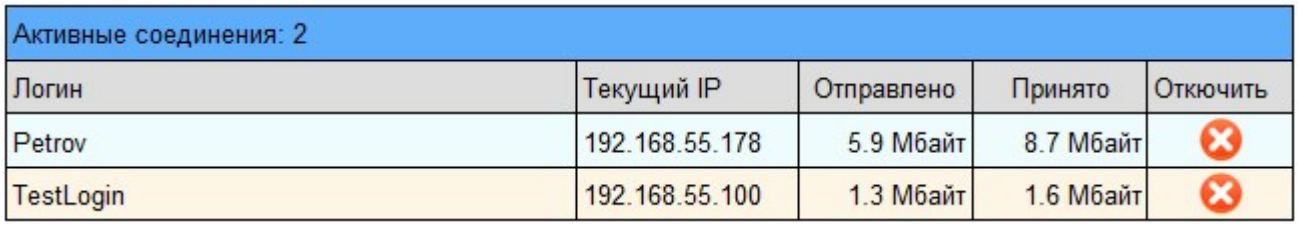
Статус сервисов:	
Статус DDNS сервиса:	Включен
Статус DHCP сервиса:	Включен
Статус VPN PPTP сервиса:	Включен
Шифрование для протокола PPTP:	Включено
Статус VPN L2TP сервиса:	Включен
Шифрование для протокола L2TP:	Включено
Текущая дата и время на сервере:	2011-06-27 1:52
Время непрерывной работы после включения:	10 мин.

Рисунок 4.7.

Здесь вы можете узнать текущее состояние для Интернет и Локального адаптеров, получить информацию о текущем режиме работы сервера, а также информацию по настройкам сервисов и их статус.

4.4 Просмотр текущих подключений

Узнать о том, какие удалённые пользователи подключены к серверу в данный момент можно выбрав в меню - "Информация: Текущие подключения" (рис. 4.8).



Активные соединения: 2				
Логин	Текущий IP	Отправлено	Принято	Откючить
Petrov	192.168.55.178	5.9 Мбайт	8.7 Мбайт	
TestLogin	192.168.55.100	1.3 Мбайт	1.6 Мбайт	

Рисунок 4.8.

При этом будет показана информация о Логине пользователя, какой IP адрес им сейчас используется, а также сколько данных было принято и отправлено им на текущий момент времени.
На против каждого подключения существует специальная иконка "Отключить", нажатие на которую вызовет отключение выбранного удалённого пользователя.

4.5 Просмотр журнала соединений

Для просмотра информации о том кто подключался к VPN серверу выберите в меню - "Информация: Журнал подключений". В ответ на это сервер выдаст информацию о том кто и когда подключался к серверу, а также какой IP адрес использовался пользователем. При этом моменты подключения и отключения представлены как отдельные события, и выделены разным цветом. (рис. 4.9).

Журнал соединений за: 2011-02-28						
Время	Событие	Логин	Выданный IP	Длит.	Отправлено	Принято
02:34:13	подкл.	TestLogin	192.168.55.100			
02:34:32	подкл.	Petrov	192.168.55.178			
02:34:48	откл.	TestLogin	192.168.55.100	35 сек.	328 байт	656 байт
02:34:51	подкл.	TestLogin	192.168.55.100			
02:50:35	откл.	TestLogin	192.168.55.100	15 м. 44 с.	1.6 Мбайт	1.3 Мбайт
02:50:49	откл.	Petrov	192.168.55.178	16 м. 17 с.	8.7 Мбайт	5.9 Мбайт

Рисунок 4.9.

Для отключений, дополнительно отображается информация по количеству переданных данных, а также длительность подключения.
По умолчанию выводиться журнал за текущий день. Для того чтобы посмотреть журнал за предыдущие дни, воспользуйтесь выпадающими вкладками, указав интересующую вас дату, после чего нажмите кнопку "Показать" (рис. 4.10).

Рисунок 4.10.

Если в выбранный день подключения будут отсутствовать, то сервер выдаст соответствующее сообщение об этом.

4.6 Просмотр лицензии

У каждого сервера существует свой уникальный серийный номер, а также лицензионный ключ соответствующий этому номеру. Для его просмотра выберете в меню - "Информация: Лицензия" (рис. 4.11).

Рисунок 4.11.

Техническая поддержка пользователей осуществляется только после проверки уникального серийного номера и в случае необходимости лицензионного ключа.

4.7 Сброс настроек

Если по тем или иным причинам необходимо сбросить настройки, вы всегда сможете это сделать воспользовавшись функцией сброса настроек. Всего существуют два способа сброса.
Первый способ это воспользоваться Web интерфейсом сервера.
Однако если по каким-то причинам вы не имеете доступа к Web интерфейсу, например вы забыли пароль администратора или сервис DHCP, выключен а вы не знаете IP сервера, необходимо воспользоваться вторым способом, который предоставляет возможность сделать это в начальный момент загрузки сервера.

4.7.1 Сброс через Web интерфейс

Для сброса настроек через Web интерфейс выберете в меню - "Настройка: Сброс настроек", после чего на открывшейся странице выберете желаемое действие кликнув мышкой по соответствующей иконке (рис. 4.12).

Рисунок 4.12.

После этого в открывшемся окне введите пароль администратора для подтверждения выбранного действия, и нажмите "Ok" (рис. 4.13 а,б).

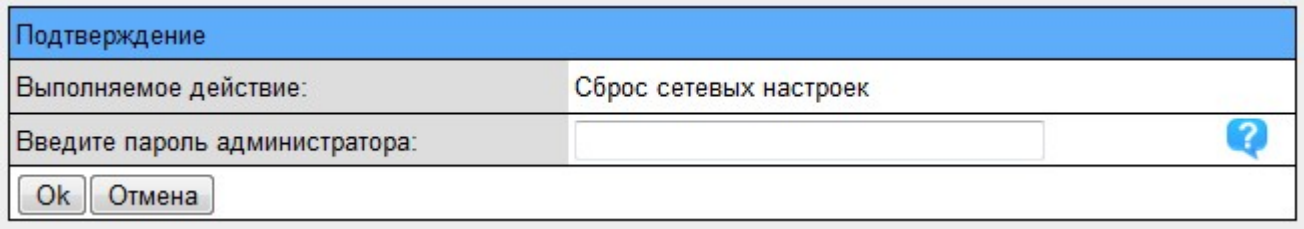


Рисунок 4.13а.

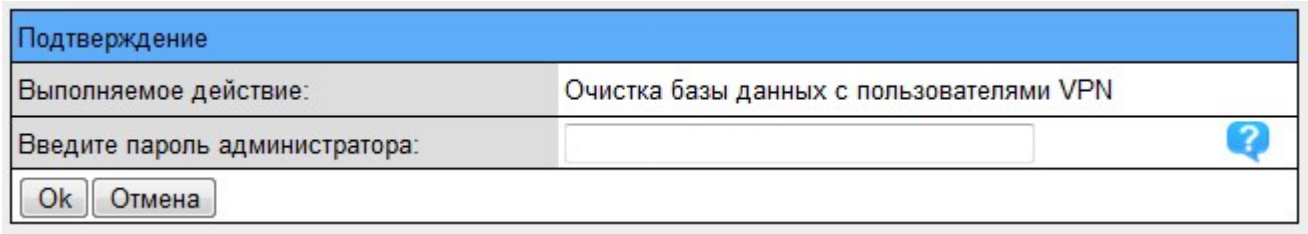


Рисунок 4.13б.

Если вы выбрали сброс сетевых настроек, то при этом при этом произойдёт перезагрузка сервера (рис 4.14).

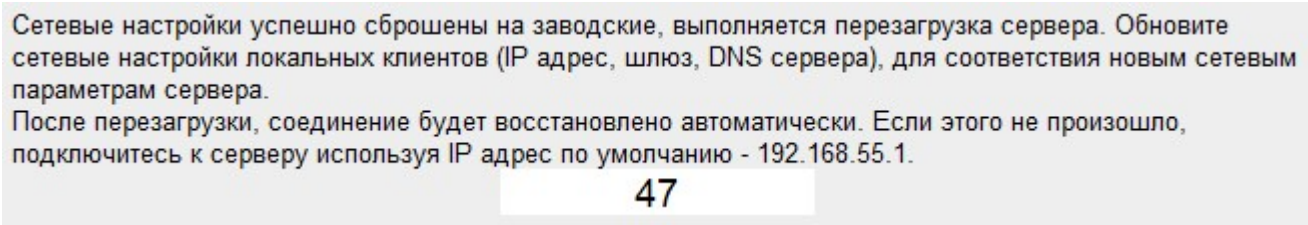


Рисунок 4.14.

4.7.2 Сброс во время загрузки

Перед сбросом настроек необходимо выключить сервер нажатием кнопки питания.
После того как сервер выключен, подсоедините стандартную USB клавиатуру (не входит в комплект поставки) в соответствующий порт, расположенный на лицевой либо задней панели. Также необходимо подключить сервер к монитору по средствам VGA кабеля (не входит в комплект поставки). Убедитесь что используемый вами монитор поддерживает разрешение 800x600 или более.
Когда необходимые приготовления сделаны, включите сервер. Через несколько секунд после включения вы должны увидеть таблицу с выбором вариантов загрузки (рис. 4.15).

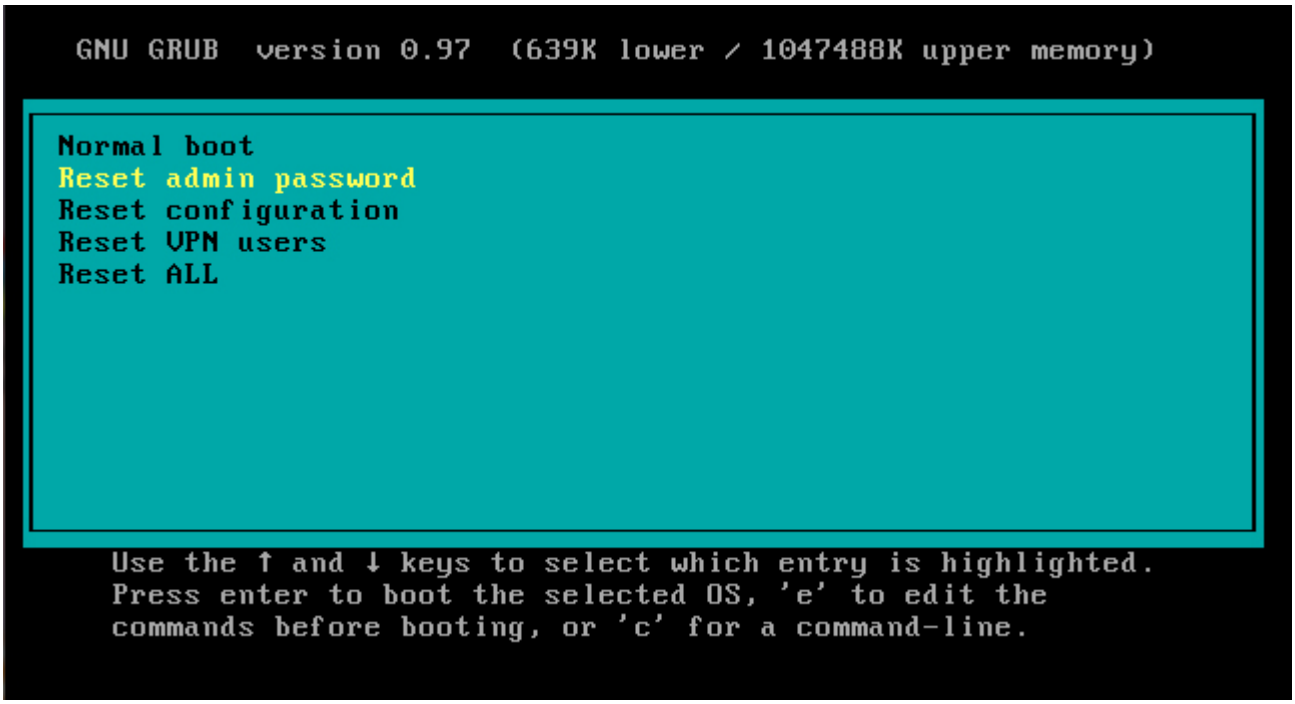


Рисунок 4.15.

У вас будет 5 секунд для выбора, если по истечению этого времени никакая клавиша на клавиатуре не была нажата сервер продолжит обычную загрузку.
Клавишами вверх и вниз выберете пункт меню, соответствующий требуемому действию (таб. 4.1)

Таблица 4.1

Пункт меню	Описание действия
Normal boot	Продолжить нормальную загрузку сервера
Reset admin password	Сбросить пароль администратора
Reset configuration	Сбросить сетевые настройки
Reset VPN users	Очистить базу данных с удалёнными пользователями VPN
Reset ALL	Сброс всех настроек

После того как выбор сделан, подтвердите его нажатием клавиши "Enter (Ввод)". В ответ на это по монитору побегут строки с служебной информацией в конце которой будет надпись "reset done", свидетельствующая об успехе, после чего сервер перезагрузится.
Отключите клавиатуру и монитор. На этом сброс настроек завершён.

5. Настройка клиентов

После того как VPN сервер полностью настроен (и сторонний маршрутизатор в случае необходимости) а также заведены новые пользователи, можно приступать к настройке удалённых клиентов. Весь процесс настройки, сводиться к созданию VPN подключения встроенными средствами операционных систем и устройств.

5.1 Создание VPN подключений

В зависимости от операционной системы, а также используемого протокола, процесс создания подключения несколько различается. Вне зависимости от клиентской системы для установления соединения используются следующие параметры:

Имя пользователя (Логин) — пользователь в VPN сервере доступ которому открыт
Пароль — его пароль
IP адрес – IP адрес VPN сервера, или сетевое имя если включён DDNS, для режима «Маршрутизатор и VPN», либо IP стороннего маршрутизатора для режима «Только и VPN»
Протокол — L2TP либо PPTP
Авторизация — MSCHAP либо MSCHAPv2
Шифрование (если включено на сервере) — MPPE

Для большего удобства рекомендуется сразу создать два подключения, первое для соединения по протоколу PPTP а второе по L2TP.
Дело в том что некоторые провайдеры не поддерживают маршрутизацию протокола GRE, который необходим для соединения по протоколу PPTP. Также не все домашние маршрутизаторы корректно работают с GRE. Протокол PPTP работает несколько быстрее, однако не всегда применим, L2TP напротив несколько медленнее но обладает большей совместимостью.
В приложении, пункт «Примеры создания и использования VPN подключений» показаны примеры настройки для Windows 2000/XP и Windows Vista/7.

5.2 Соединение и отсоединение с удалённой сетью

Для соединения с удалённой сетью необходимо воспользоваться созданными ранее подключениями. Если вы последовали рекомендации, и создали два подключения, одно по протоколу PPTP а другое по L2TP, то это позволит вам более оперативно пользоваться удалённым соединением, в зависимости от конкретных условий. Выбор того или иного протокола зависит от выбранного провайдера, используемого сетевого оборудования, а также других факторов.
При подключении к VPN серверу, надо следовать простому правилу: если соединение успешно устанавливается по протоколу PPTP то следует использовать данный тип подключения, если нет, то использовать подключение по протоколу L2TP.
В приложении, пункт «Примеры создания и использования VPN подключений» показаны примеры установления соединений в Windows 2000/XP и Windows Vista/7.

6. Технические характеристики

Максимальное число пользователей VPN – 5.000
Максимальное число одновременных VPN подключений — 100
Поддерживаемые протоколы VPN – PPTP, L2TP (без сертификата)
Протоколы авторизации — MSCHAP либо MSCHAPv2
Протоколы шифрования — MPPE
Сервис системы динамичных доменных имен (DDNS) — dyndns.com, no-ip.com
Максимальное число устройств в сети — 254
Используемые внутренние адреса — 192.168.x
Поддерживаемые клиентские операционный системы — Windows 2000/XP/Vista/7, Android (2.1 и выше), MacOS, Linux, и др.
Сетевые адаптеры — Ethernet 10/100/1000 Мбит/с, 2шт
Пропускная способность — до 750 Мбит/с
Поддерживаемые беспроводные USB адаптеры — Samsung SWC-U200 (Yota)
Процессор — x86 совместимый
Оперативная память — 2Гб
Тип накопителя — HDD.
Питание — 220 вольт.
Энергопотребление (типичное/максимальное) — 27/40Вт
Рабочий диапазон температур — +5…+40 °C
Размеры* (ширина x высота x глубина) — 265 x 90 x 270 мм

*может отличаться в зависимости от ревизии.

7. Приложение

7.1 Поддерживаемые провайдеры

В таблице 7.1 приведён список провайдеров работа с которыми VPN сервера была проверена.

Таблица 7.1

Провайдер (торговая марка)	Официальный сайт	Технология предоставления услуг	Поддерживаемые протоколы
СТРИМ	dom.mts.ru	ADSL	PPTP,L2TP
Домолинк	www.domolink.ru	ADSL	PPTP,L2TP
АКАДО	www.akado.ru	Ethernet	L2TP
QWERTY	www.qwerty.ru	Ethernet	PPTP,L2TP
Yota	www.yota.ru	4G	L2TP, L2TP
Skylink	www.skylink.ru	3G	PPTP,L2TP
МТС	www.mts.ru	3G	PPTP,L2TP
Мегафон	www.megafon.ru	3G	PPTP,L2TP
Гран При Телеком	www.gptel.ru	Ethernet	PPTP,L2TP
ПраймЛинк Телекоммуникации	www.primelink.ru	Ethernet	PPTP,L2TP

Информация представленная в таблице носит справочный характер и в реальности может отличаться в зависимости от местоположения, времени и др. факторов.
Вне зависимости от выбранного способа подключения и выбранного поставщика услуг, соединение должно удовлетворять следующим требованиям:

1. Наличие реального IP адреса (только на стороне VPN сервера).
2. Отсутствия фильтрации трафика: PPTP (GRE), 1723TCP, 1723UDP, 1701UDP, 1522TCP
3. Для соединения по протоколу PPTP требуется корректная поддержка протокола GRE
4. Стабильное соединение, обеспечивающие необходимую пропускную способность.

О возможности предоставления услуг, отвечающим этим требованиям, уточняйте у вашего провайдера.

7.2 Примеры планирования сети

Проще всего показать планирование сети на примере.
Пусть у нас имеется сеть состоящая из множества устройств подключенных к коммутатору (рис. 7.2.1).

Рисунок 7.2.1.

Для такой сети можно использовать IP адреса представленные в таблице. 7.2.

Таблица 7.2.

Устройство(а)	IP адрес(а)
VPN сервер	192.168.55.1
Файловый сервер	192.168.55.2
Принтер	192.168.55.3
Точка доступа	192.168.55.4
IP камеры	192.168.55.5-6
Рабочие станции	192.168.55.7-9
Резерв под статические адреса	192.168.55.10-39
Автоматическое назначение IP адресов для локальных клиентов по DHCP	192.168.55.40-99
Автоматическое назначение IP адресов для удалённых клиентов подключившихся по протоколу PPTP	192.168.55.100-177
Автоматическое назначение IP адресов для удалённых клиентов подключившихся по протоколу L2TP	192.168.55.178-254

Статические IP адреса лучше использовать для устройств которые не перемещаются, и к которым происходит обращение от других устройств сети, например сервера, IP камеры, Wi-Fi точки доступа, принтеры и т. д.
Для таких устройств адрес шлюза будет локальный IP адрес VPN vервера (либо модема для режима «Только VPN»), а адреса DNS серверов будут теми которые назначил провайдер, либо если вы их не знаете, просто впишите значения 8.8.8.8 и 8.8.4.4, маска подсети всегда 255.255.255.0.
Использование автоматического назначения адресов по DHCP удобно для устройств которые

перемещаются, например ноутбуки, планшеты, и т.д.
При этом следует обратить внимание на то что адреса не повторяются, и находятся в одной и то же подсети.

7.3 Настройка сети

7.3.1 Настройка сети в в Windows Vista/7

1. Справа внизу, рядом с часами, щелкните по значку в виде монитора с кабелем и выберите **Центр управления сетями и общим доступом** (рис. 7.3.1).

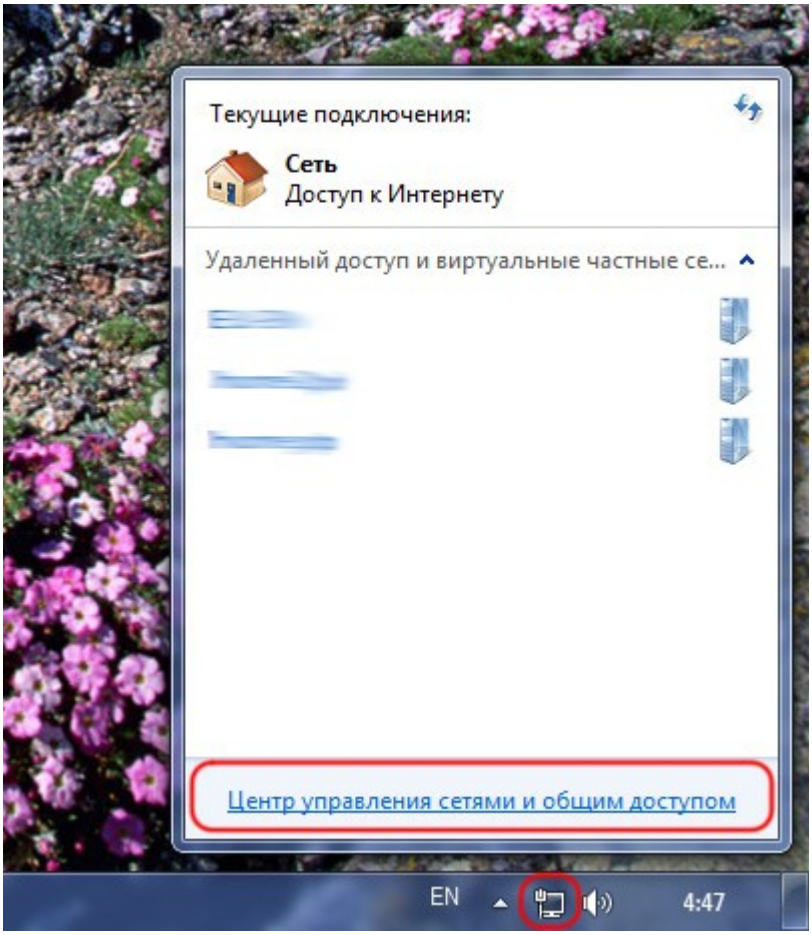


Рисунок 7.3.1.

2. В открывшемся окне выберете **Изменение параметров адаптера** (рис. 7.3.2).

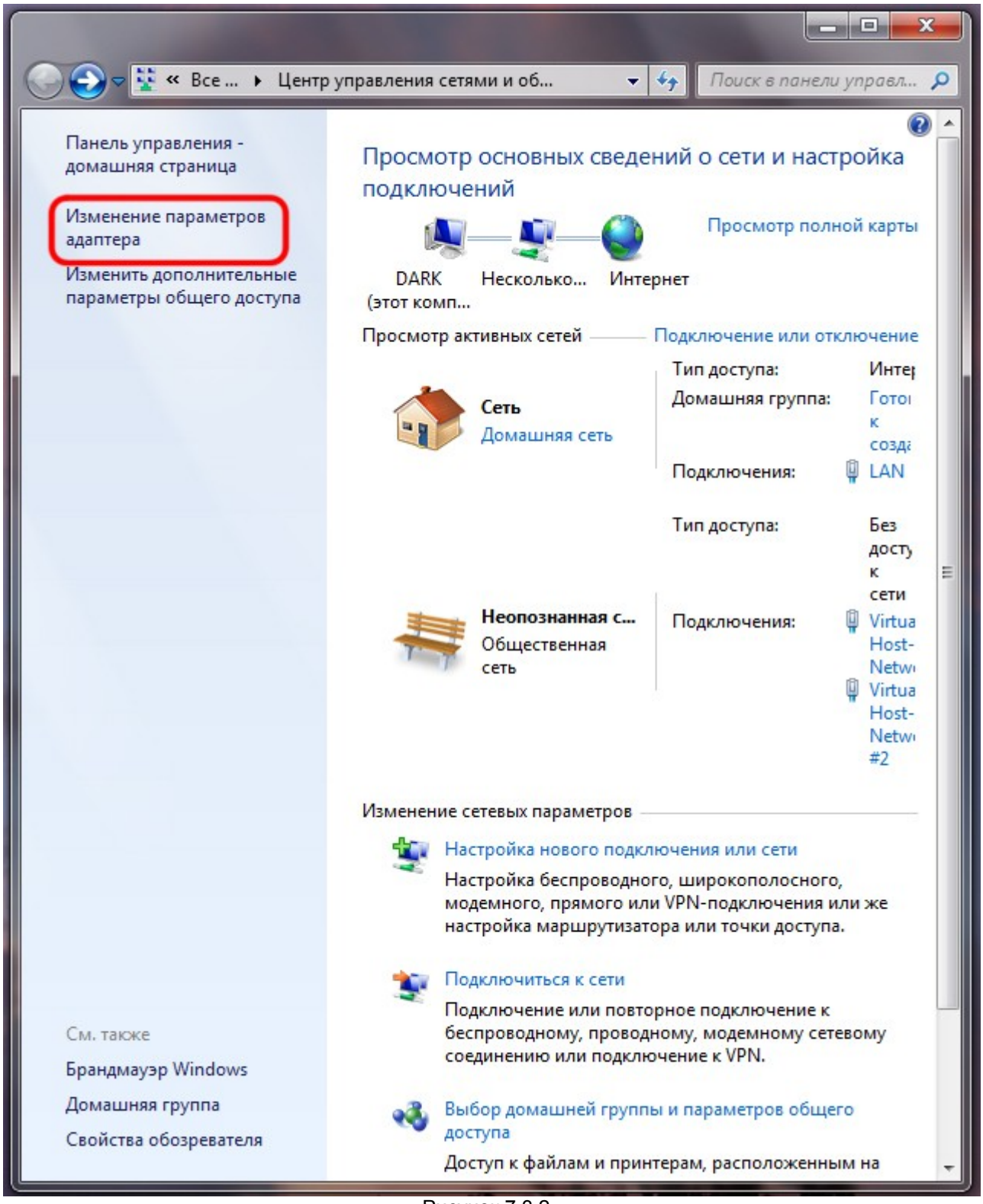


Рисунок 7.3.2.

3. Щёлкните правой клавишей мыши на сетевом адаптере локальной сети и выберете **Свойства** (рис. 7.3.3).

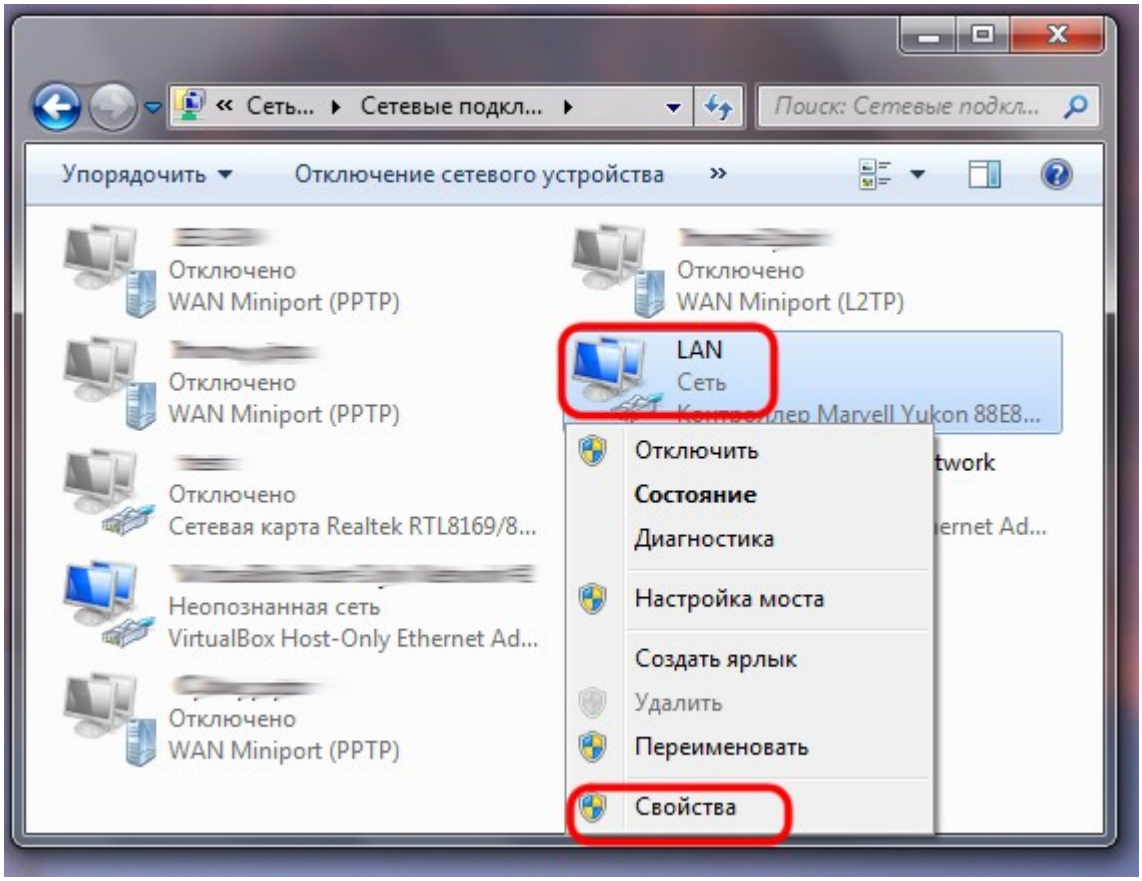


Рисунок 7.3.3.

4. Выберете **Протокол интернета версии 4 (TCP/IPv4)** и нажмите **Свойства** (рис. 7.3.4).

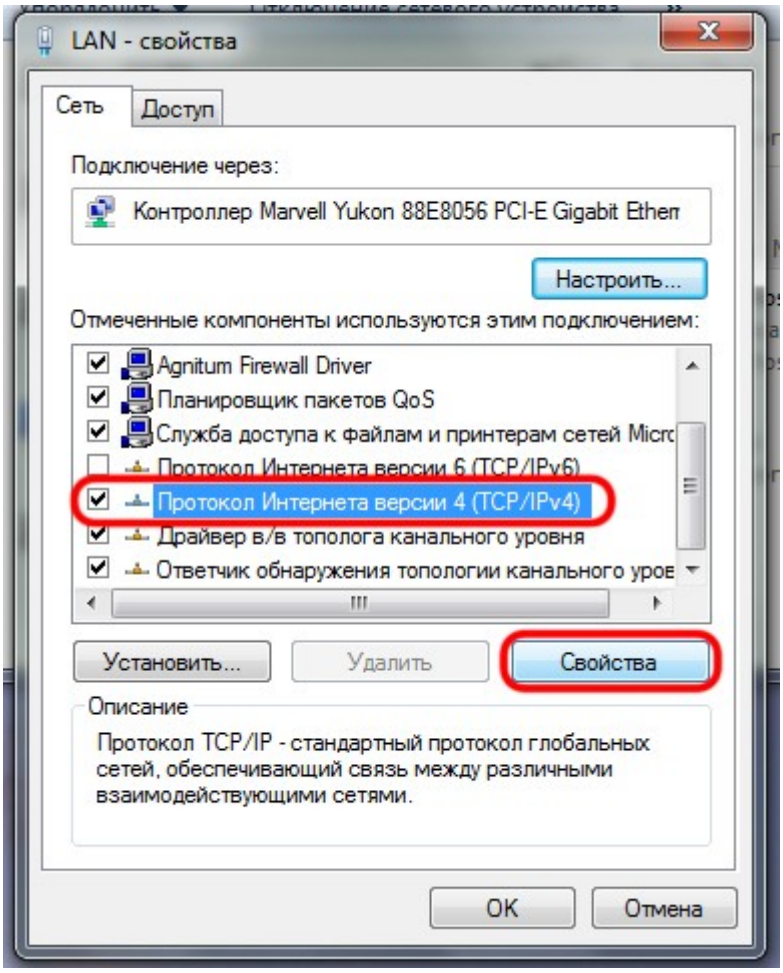


Рисунок 7.3.4.

6. В открывшемся окне заполните поля **IP-адрес**, **Маска подсети**, **Основной шлюз**, **Альтернативный** и **Предпочитаемый DNS-сервер**, для ручной настройки (статического) IP адреса (рис. 7.3.5), либо для автоматического назначения сетевых параметров по DHCP выберете **Получить IP-адрес автоматически** и **Получить адрес DNS-сервера автоматически** (рис. 7.3.6).

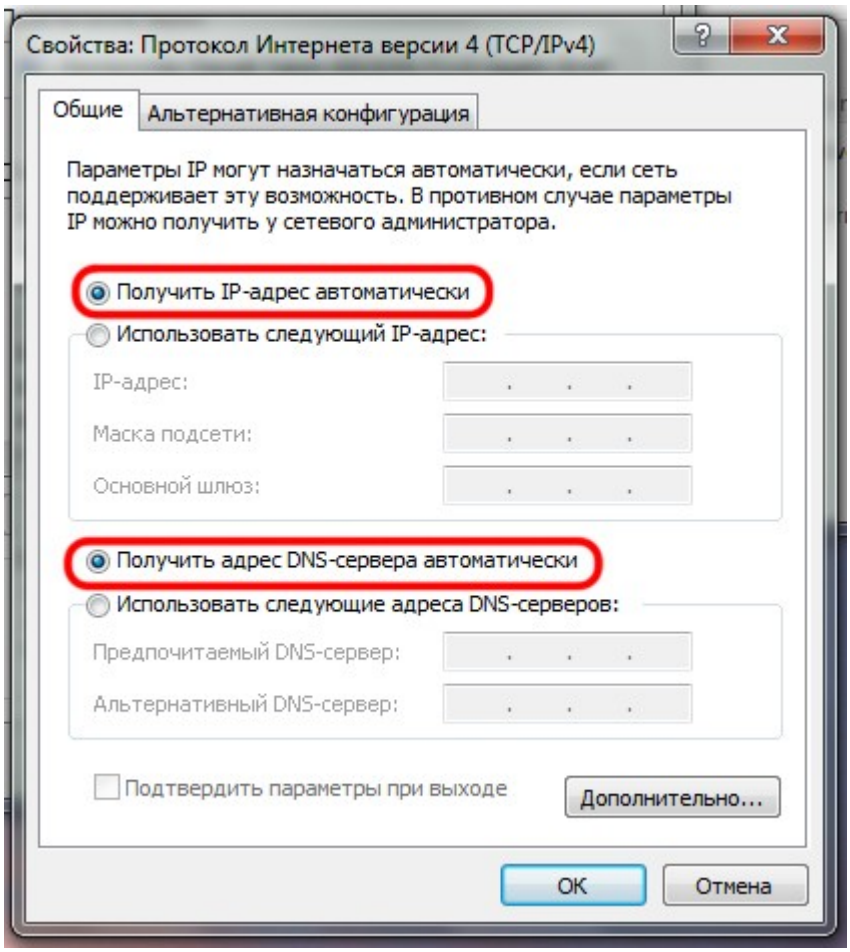

Свойства: Протокол Интернета версии 4 (TCP/IPv4)
Общие
Альтернативная конфигурация
Параметры IP могут назначаться автоматически, если сеть поддерживает эту возможность. В противном случае параметры IP можно получить у сетевого администратора.
Получить IP-адрес автоматически
Использовать следующий IP-адрес:
IP-адрес:
Маска подсети:
Основной шлюз:
Получить адрес DNS-сервера автоматически
Использовать следующие адреса DNS-серверов:
Предпочитаемый DNS-сервер:
Альтернативный DNS-сервер:
Подтвердить параметры при выходе
Дополнительно...
OK
Отмена

Рисунок 7.3.5.

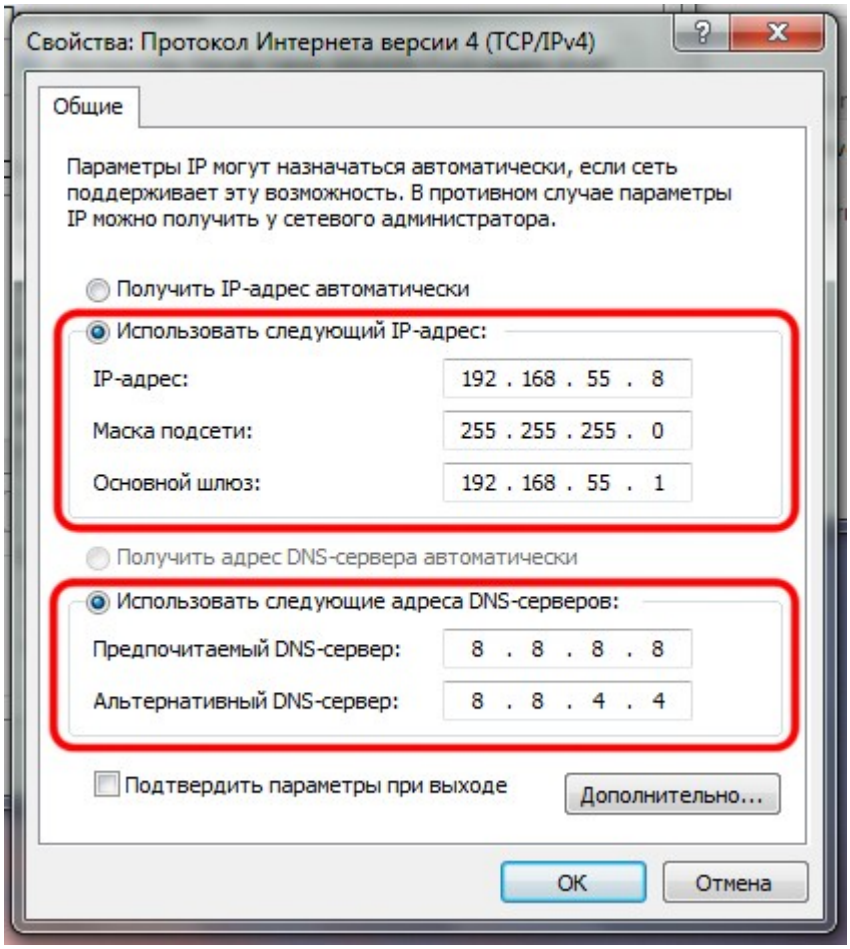


Рисунок 7.3.6.

7. Подтвердите свой выбор нажав **OK**, и затем снова **OK**.

7.3.2 Настройка сети в в Windows 2000/XP

1. Нажмите **Пуск** и выберете **Панель управления** (рис. 7.3.7а), либо **Пуск** -> **Настройка** -> **Панель управления** (рис. 7.3.7б), в зависимости от настроек представления меню Пуск.

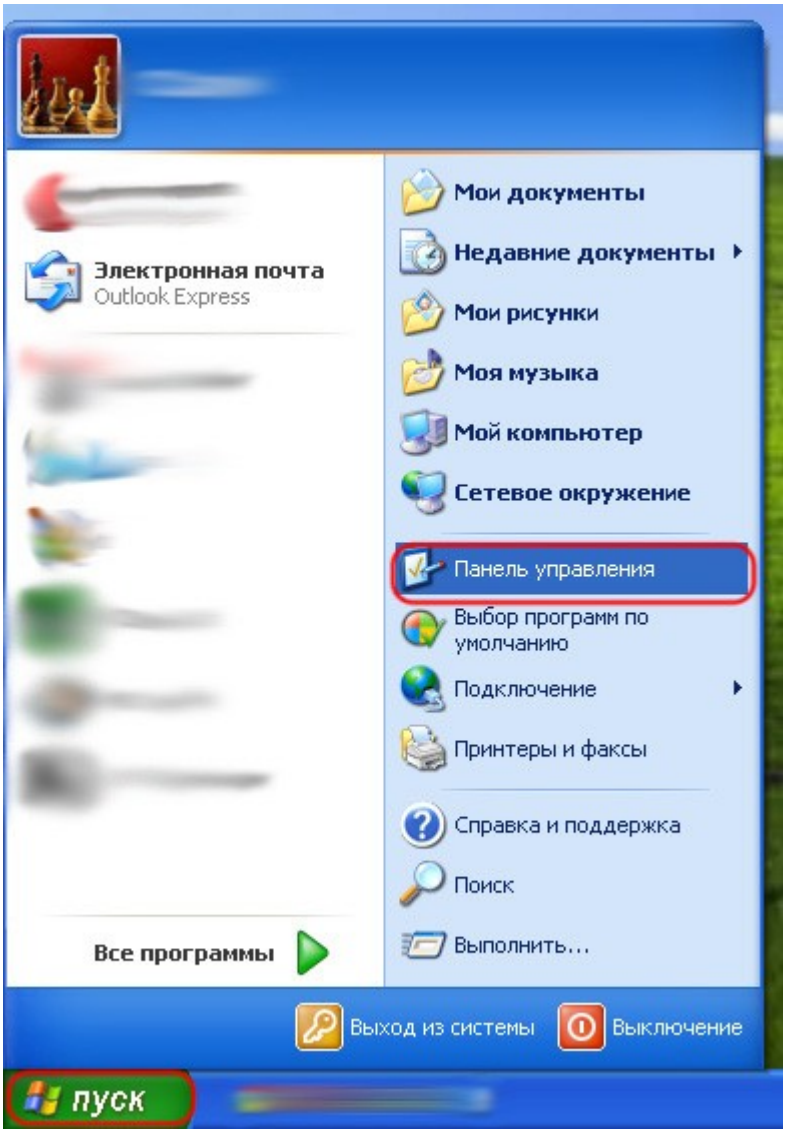


Рисунок 7.3.7а.

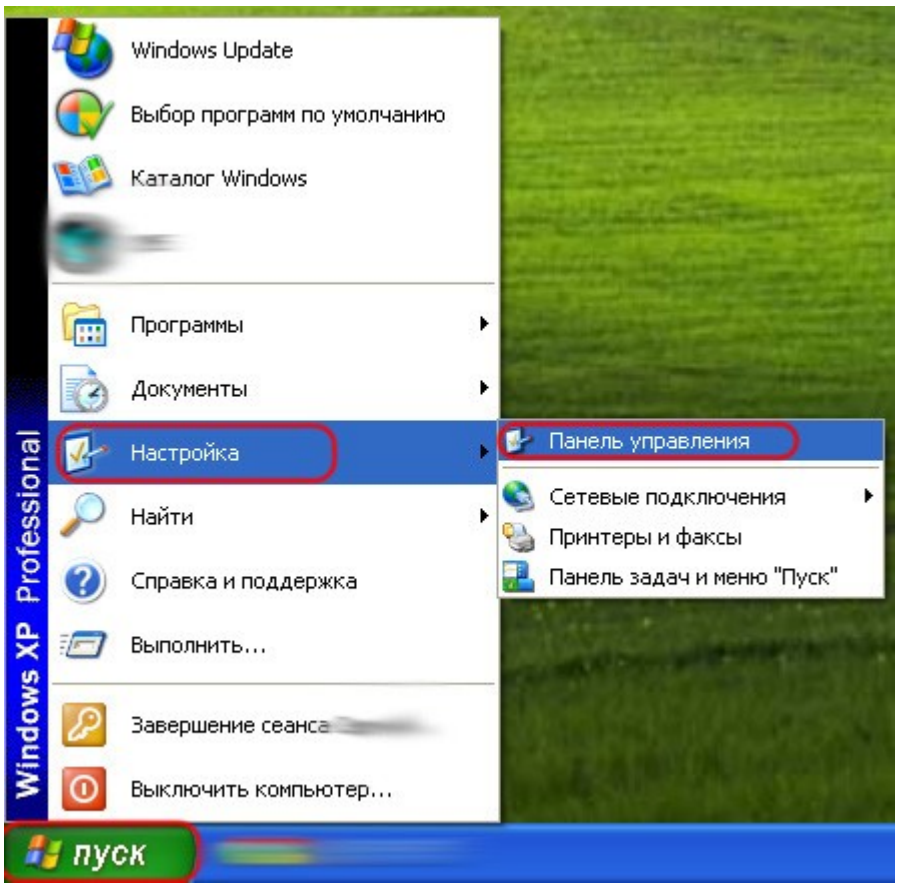


Рисунок 7.3.7б.

2. Далее, в случае необходимости, нажмите в левом верхнем углу открывшегося окна **Переключение к классическому виду**, и выберете **Сетевые подключения** (рис. 7.3.8).

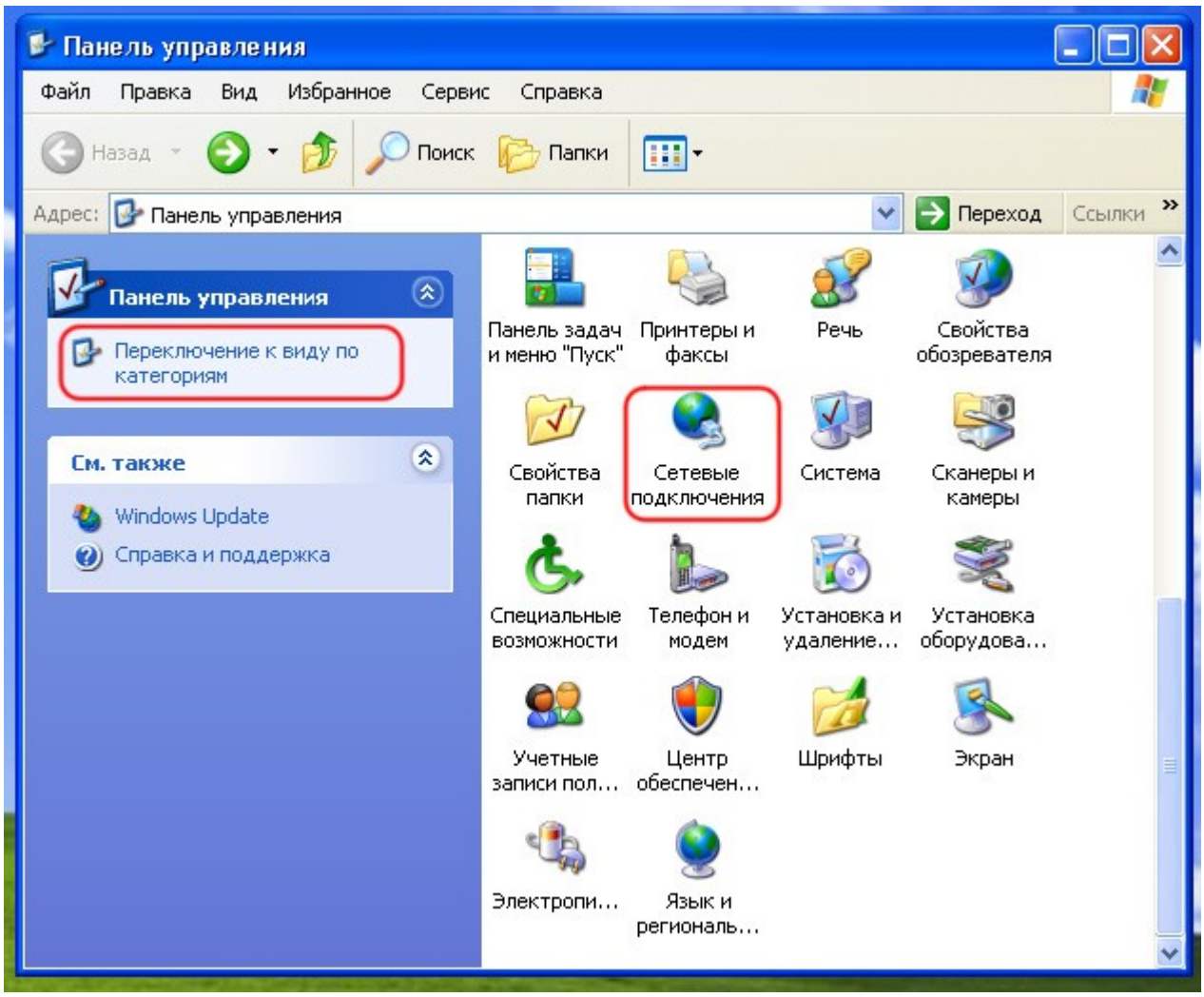


Рисунок 7.3.8.

3. Щёлкните правой клавишей мыши на сетевом адаптере локальной сети и выберете **Свойства** (рис. 7.3.9).

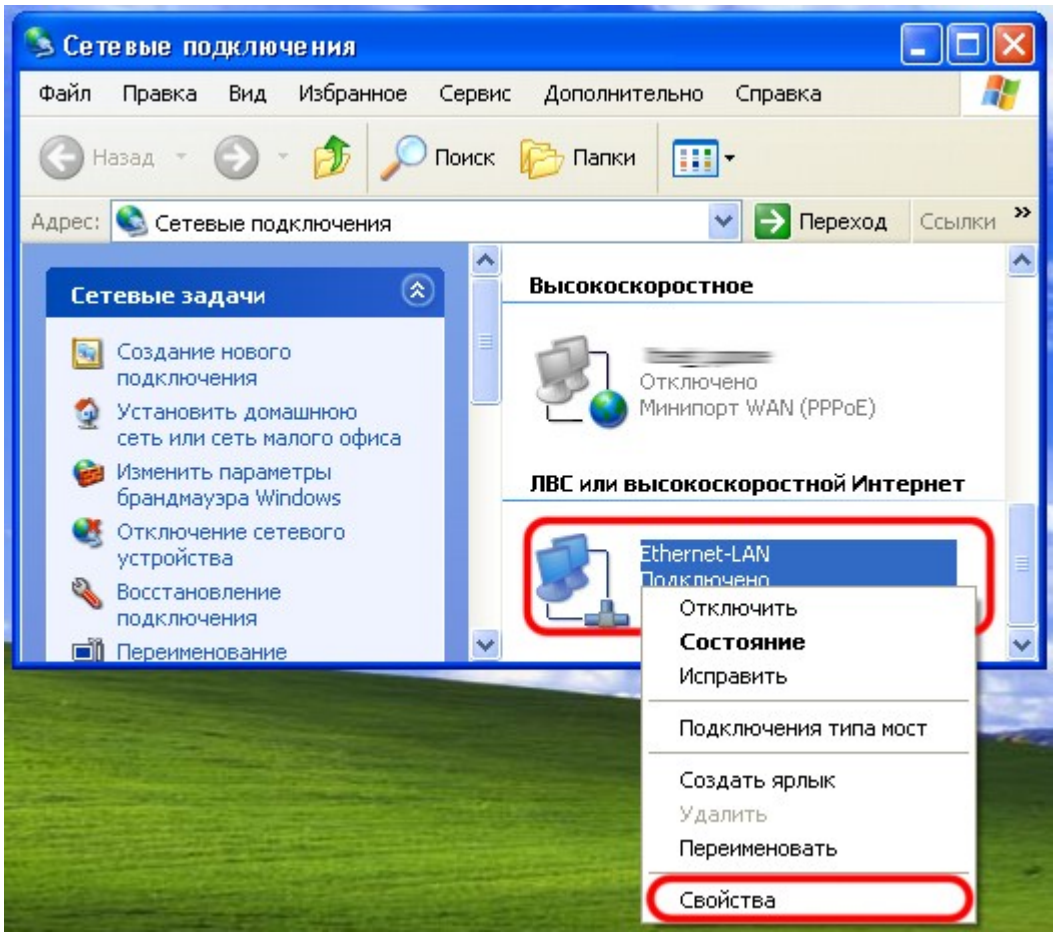


Рисунок 7.3.9.

4. Выберете **Протокол Интернета TCP/IP** и нажмите **Свойства** (рис. 7.3.10).

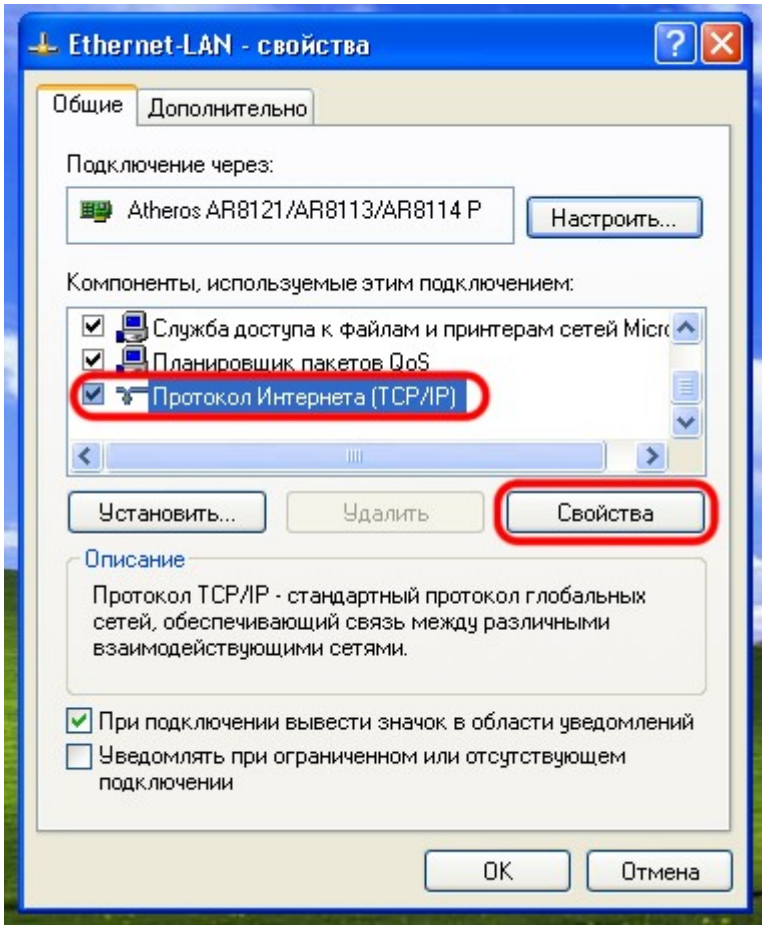


Рисунок 7.3.10.

6. В открывшемся окне заполните поля **IP-адрес**, **Маска подсети**, **Основной шлюз**, **Альтернативный** и **Предпочитаемый DNS-сервер**, для ручной настройки (статического) IP адреса (рис. 7.3.11), либо для автоматического назначения сетевых параметров по DHCP выберете **Получить IP-адрес автоматически** и **Получить адрес DNS-сервера автоматически** (рис. 7.3.12).

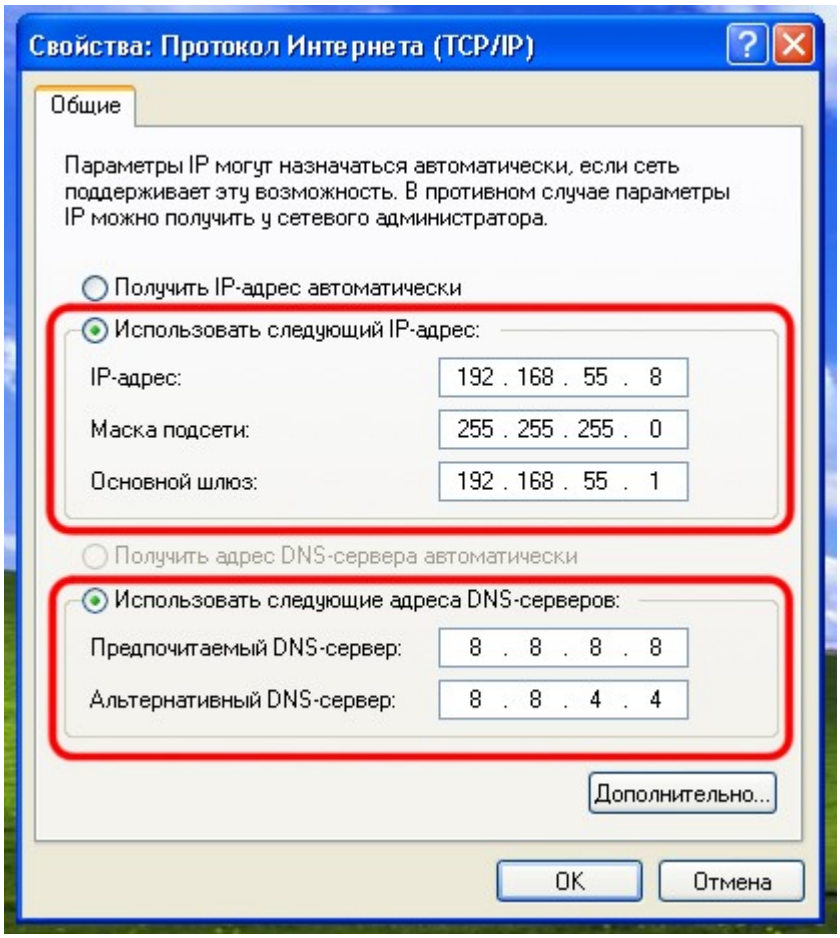


Рисунок 7.3.11.

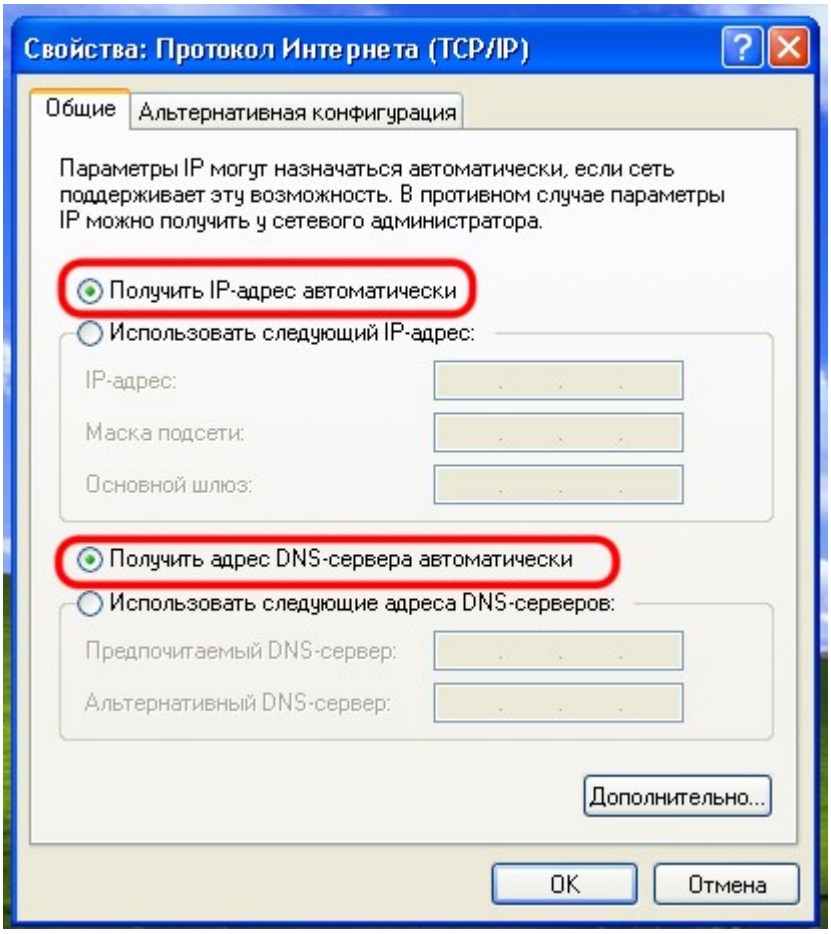


Рисунок 7.3.12.

7. Подтвердите свой выбор нажав **OK**, и затем снова **OK**.

7.4 DDNS

7.4.1 dyndns.com (условно бесплатный провайдер)

1. Откройте удобный вам браузер и перейдите на сайт www.dyndns.com, после чего выберете на открывшейся странице **Sign in** далее **Create an Accaunt** (рис. 7.4.1).

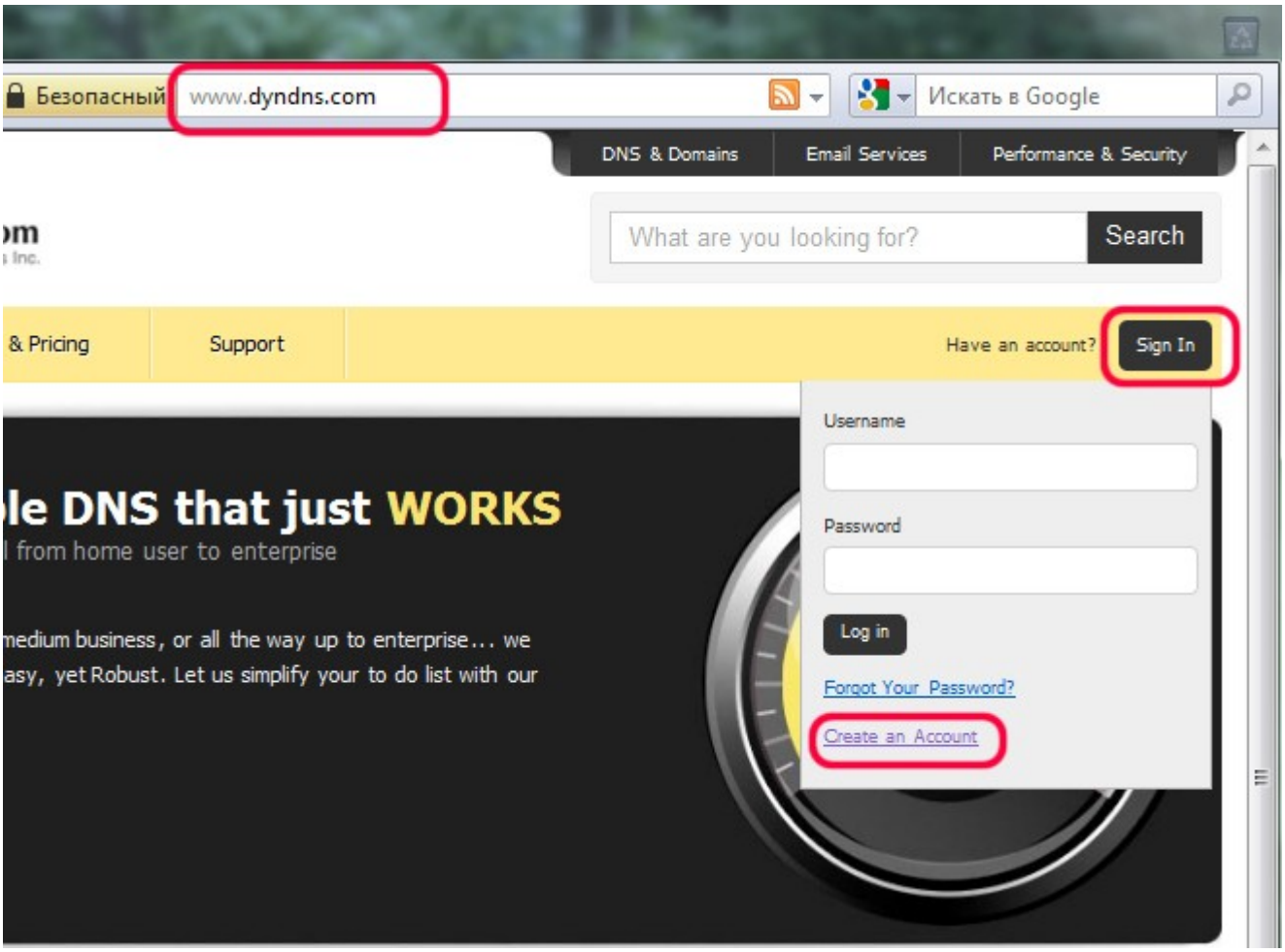


Рисунок 7.4.1.

2. Заполните соответствующие поля, **Username** – имя пользователя (Логин), **Password** – пароль, **Confirm Password** – повторите ваш пароль, **Email** – электронный почтовый ящик, **Confirm Email** – проворите адрес электронного почтового ящика, **Enter the numbers from the above image** – введите числа показанные на картинке выше, поставьте галочку напротив **I agreewith the acceptable use policy (AUP) and privacy policy**, и нажмите **Create Account** (рис. 7.4.2).

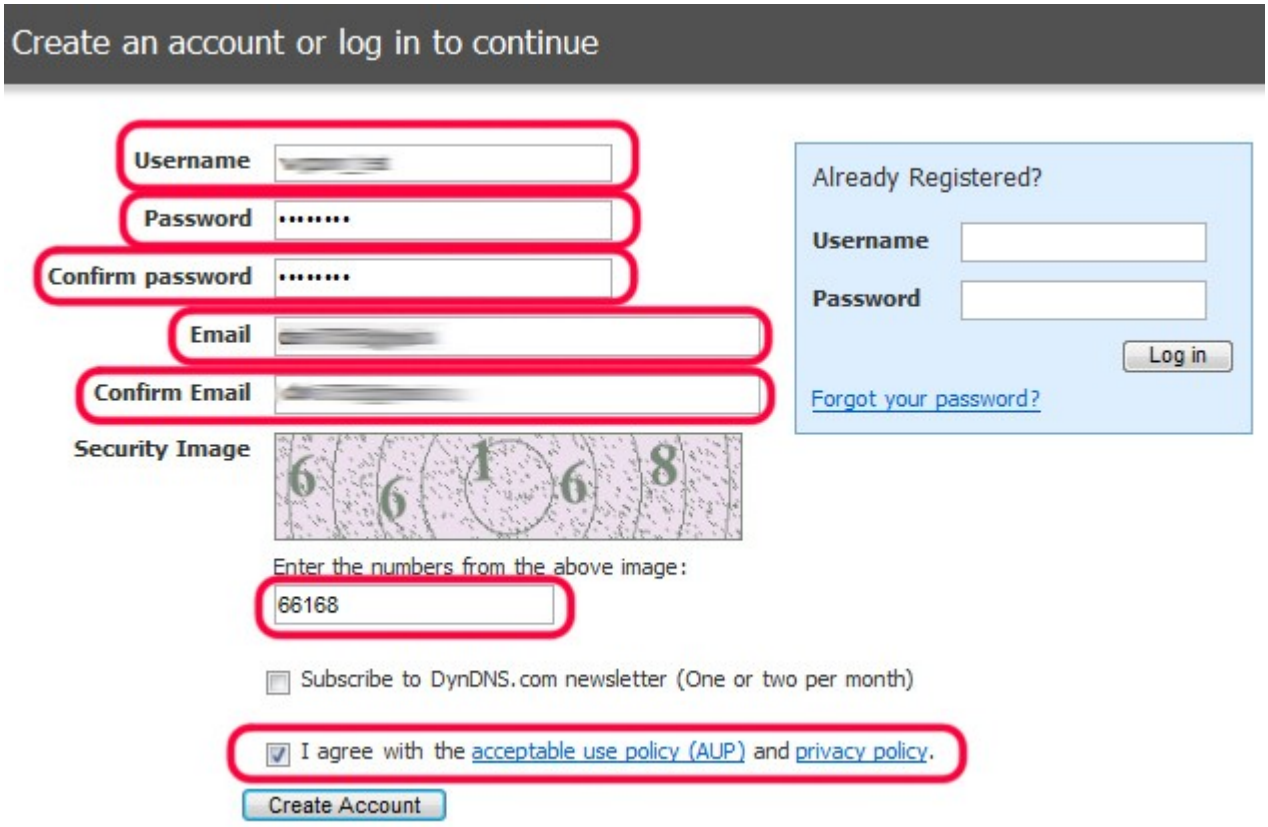


Рисунок 7.4.2.

3. Если вы сделали всё верно, то в ответ на это вы увидите сообщение о том, что на ваш почтовый ящик было направлено письмо для подтверждения процедуры регистрации (рис. 7.4.3).

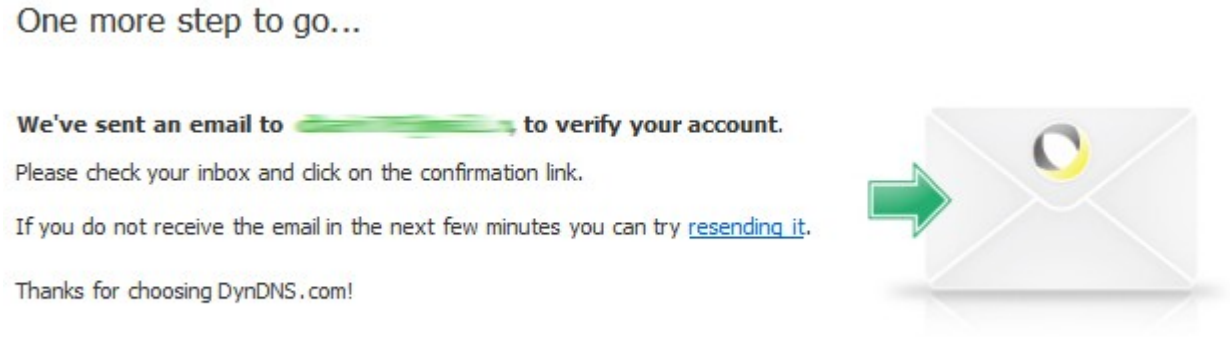


Рисунок 7.4.3.

4. Откройте в вашем почтовом ящике письмо от dyndns.com, и кликните по верхней ссылке (рис. 7.4.4).

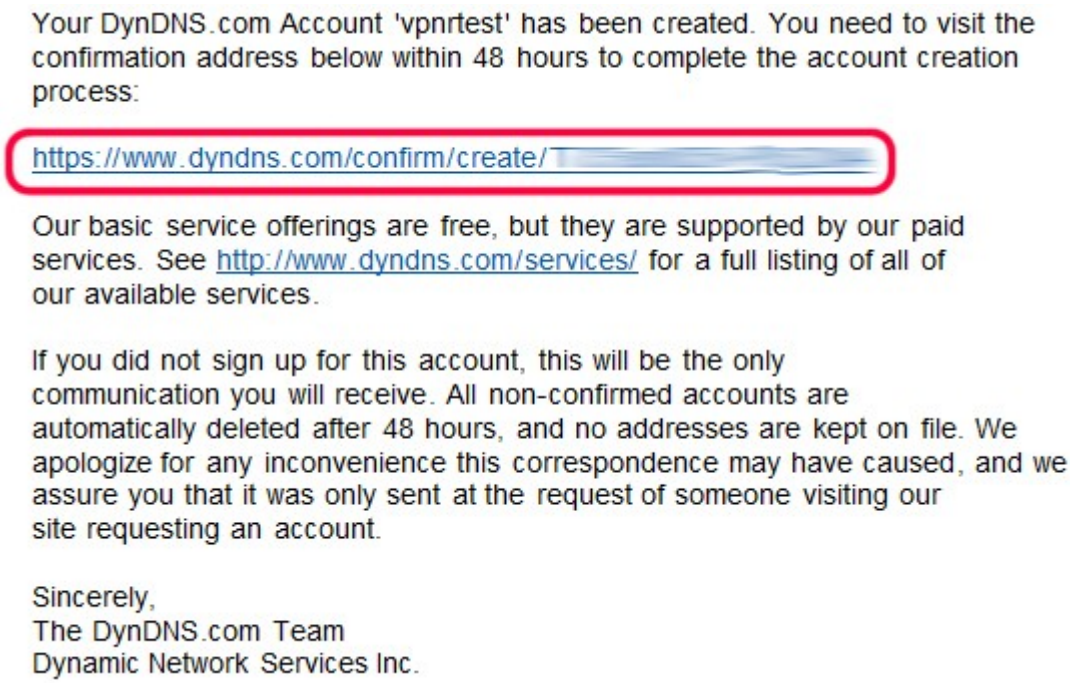


Рисунок 7.4.4.

5. В ответ на это откроется страница, на которой вам потребуется снова ввести пароль, который вы указывали при регистрации, после этого нажмите **Confirm Account** (рис. 7.4.5).

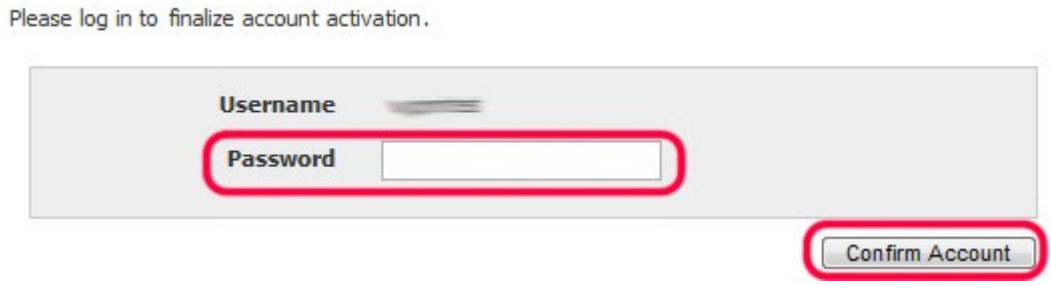


Рисунок 7.4.5.

На этом процедура регистрации завершена, и можно переходить к настройке сетевого имени.

6. Если вы ещё не зашли на сайт www.dyndns.com, сделайте это, выберав **Sign in** на главной странице и введите логин и пароль которые вы указали при регистрации, после чего выберете пункт **My Account** (рис. 7.4.6).

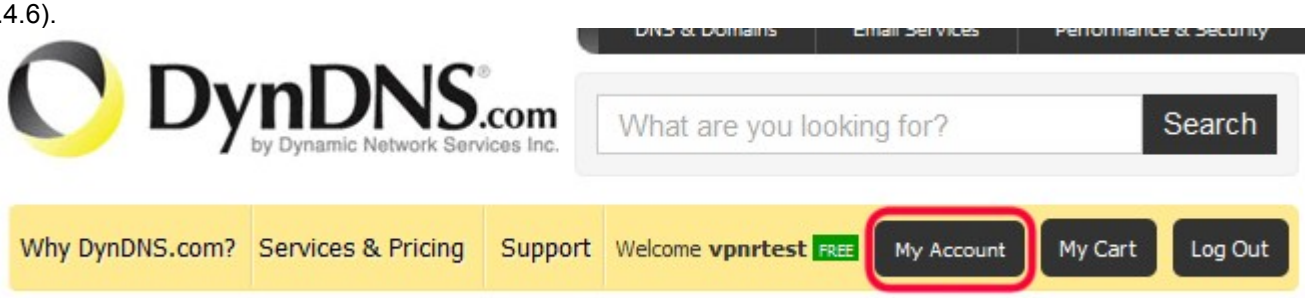


Рисунок 7.4.6.

7. Далее выберете **My Hosts** и **Add Host Services** (рис. 7.4.7).

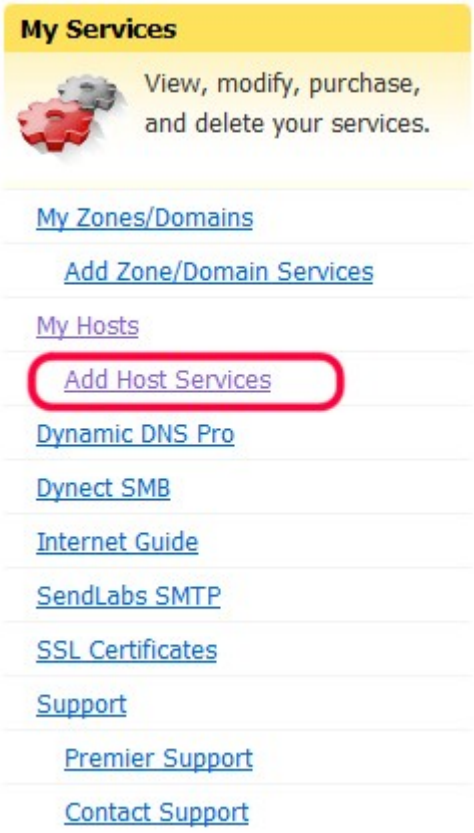


Рисунок 7.4.7.

8. В открывшемся окне заполните поле **Hostname** и выберете любой из доменов присутствующих в списке, придумав тем самым сетевое имя, которое будет ассоциироваться с сервером удалённого доступа и использоваться при создании удалённых подключений. Щёлкните по ссылке **Your current location's IP address is …**, после чего кликните по **Add to Cart** (рис. 7.4.8).

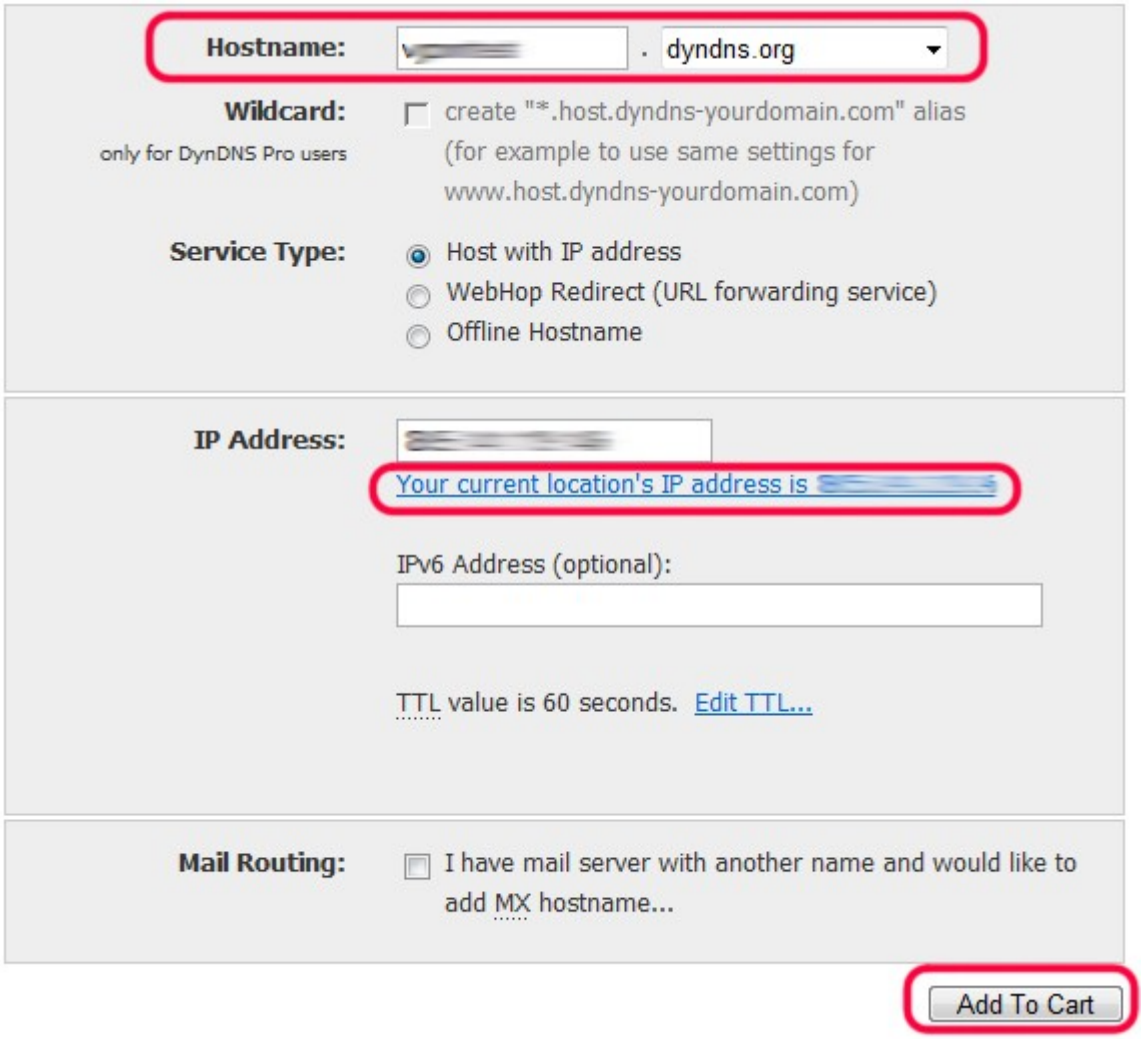


Рисунок 7.4.8.

9. Если всё было сделано верно, вы увидите соответствующее сообщение в котором необходимо нажать **Proceed to checkout** (рис. 7.4.9).

Рисунок 7.4.9.

10. В ответ на это вы увидите новое окно, в котором необходимо нажать **Activate Services** (рис. 7.4.10).

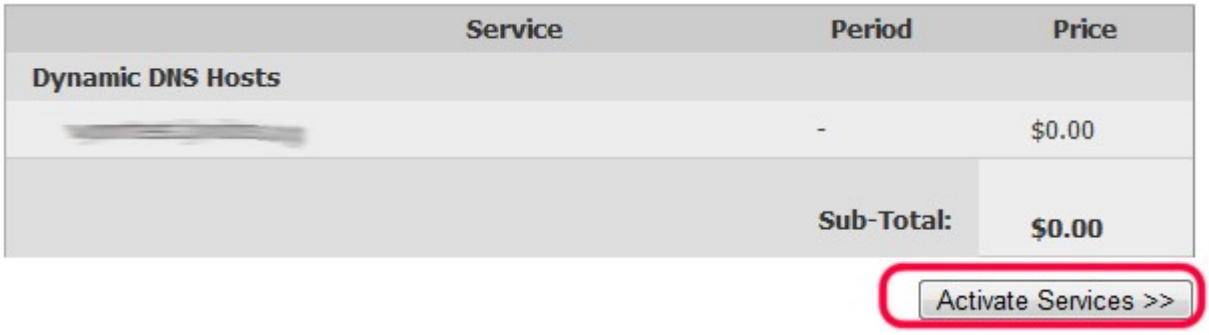


Рисунок 7.4.10.

11. После этого откроется страница с вашем, только что добавленным, сетевым именем (рис. 7.4.11).

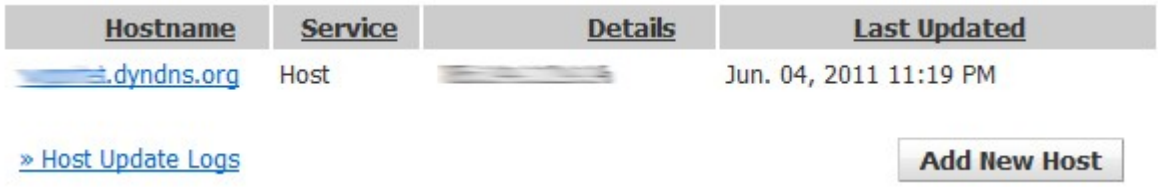


Рисунок 7.4.11.

На этом процедура создания сетевого имени завершена, и вы можете использовать его для удалённых подключений, предварительно включив и настроив DDNS сервис на сервере удалённого доступа, используя для этого Логин, Пароль, Сетевое имя вашего аккаунта, а также выбрав в качестве провайдера DDNS - dyndns.com.

7.4.2 no-ip.com (бесплатный провайдер)

1. Откройте удобный вам браузер и перейдите на сайт www.no-ip.com, после чего выберете на открывшейся странице **No-IP Free** (рис. 7.4.12).

Рисунок 7.4.12.

2. На открывшейся странице заполните поле, **Email Address** – адрес электронного почтового ящика, после чего нажмите **Sign Up Now!**. Обратите внимание на то, что некоторые почтовые системы, например mail.ru и yandex.ru, не поддерживаются, по этому рекомендуется использовать зарубежные почтовые системы, например gmail.com (рис. 7.4.13).

Рисунок 7.4.13.

3. Заполните соответствующие поля, **First Name** – ваше имя, **Last Name** – фамилия, **Email** – электронный почтовый ящик, **Username** – имя пользователя (Логин), **Password** – пароль, **Confirm Password** – повторите ваш пароль, **Security Question** – секретный вопрос на случай утраты пароля, **Your Answer** – ответ на секретный вопрос, **Birthday** – день рождения, **Type the twowords above** – введите два слова показанные на картинке выше, поставьте галочку напротив **I agree that I will only create one free No-IP account.**, и нажмите **I Accept, Create my Account** (рис. 7.4.14).

Рисунок 7.4.14.

4. Если вы сделали всё верно, то в ответ на это вы увидите сообщение о том, что на ваш почтовый ящик было направлено письмо для подтверждения процедуры регистрации (рис. 7.4.15).

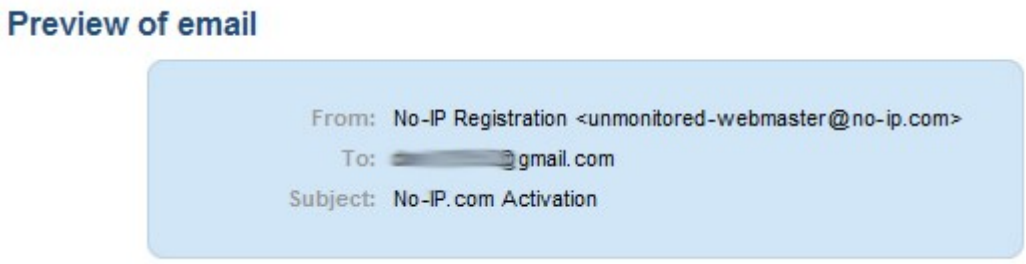


Рисунок 7.4.15.

5. Откройте в вашем почтовом ящике письмо от no-ip.com, и кликните по ссылке (рис. 7.4.16).

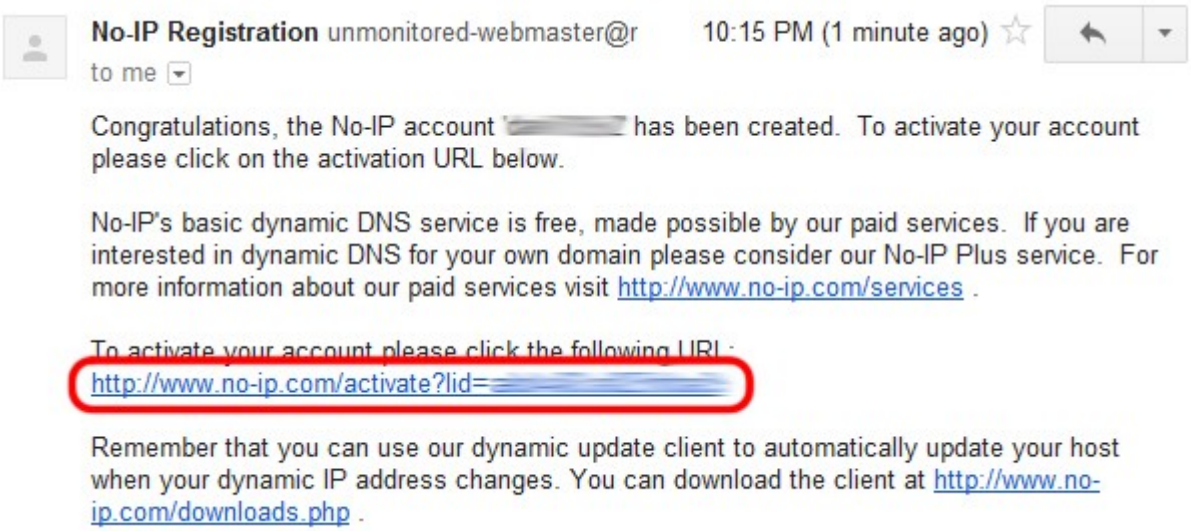


Рисунок 7.4.16.

6. В ответ на это откроется страница, на которой вы увидите сообщение об успешной активации(рис. 7.4.17).

Рисунок 7.4.17.

На этом процедура регистрации завершена, и можно переходить к настройке сетевого имени.

7. Если вы ещё не зашли на сайт www.no-ip.com, сделайте это введя в поля **Username** и **Password** логин (или email) и пароль, соответственно, которые вы указали при регистрации, и нажмите **Login** (рис. 7.4.18).

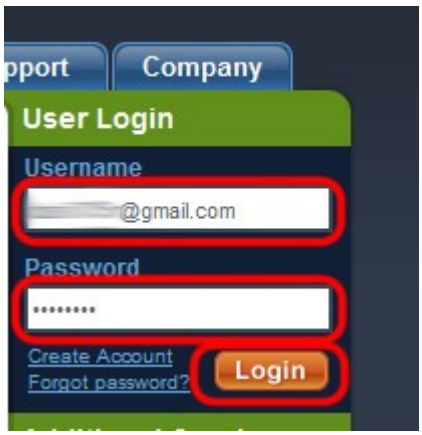


Рисунок 7.4.18.

8. Далее выберете **Add Host** (рис. 7.4.19).

Рисунок 7.4.19.

9. В открывшемся окне заполните поле **Hostname** и выберете любой из доменов присутствующих в списке (после строки No-IP Free Domains), придумав тем самым сетевое имя, которое будет ассоциироваться с сервером удалённого доступа и использоваться при создании удалённых подключений. Щёлкните по **Create host** (рис. 7.4.20).

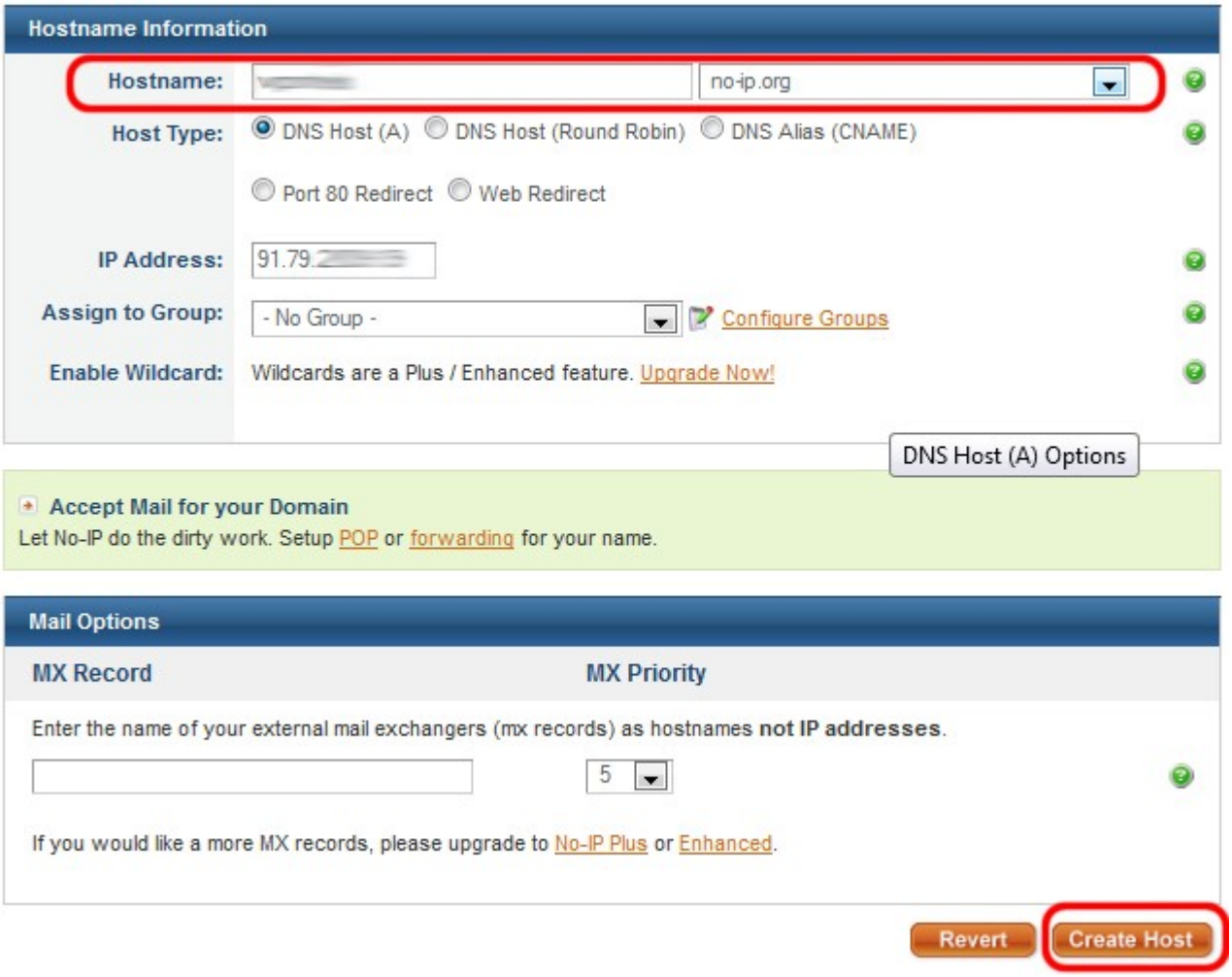


Рисунок 7.4.20.

10. После этого откроется страница с вашем, только что добавленным, сетевым именем (рис. 7.4.21).

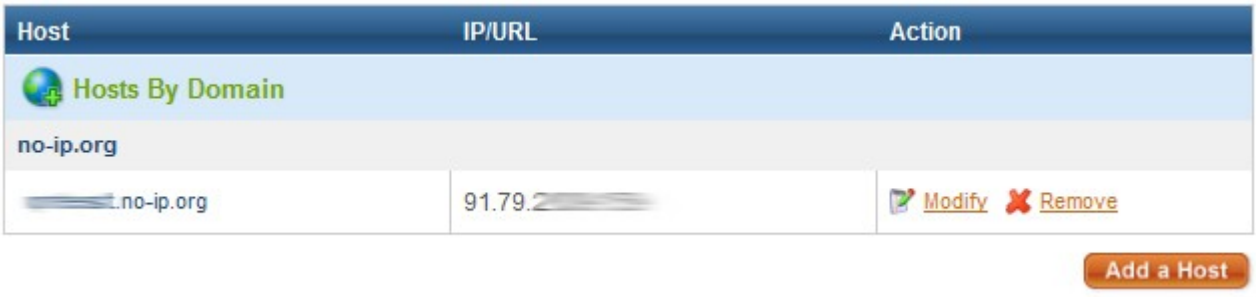


Рисунок 7.4.21.

На этом процедура создания сетевого имени завершена, и вы можете использовать его для удалённых подключений, предварительно включив и настроив DDNS сервис на сервере удалённого доступа, используя для этого Логин (e-mail), Пароль, Сетевое имя вашего аккаунта, а также выбрав в качестве провайдера DDNS - no-ip.com.

7.5 Примеры создания и использования VPN подключений

7.5.1 Создание VPN подключения в Windows Vista/7 по протоколу PPTP

1. Справа внизу, рядом с часами, щелкните по значку в виде монитора с кабелем и выберите **Центр управления сетями и общим доступом** (рис. 7.5.1).

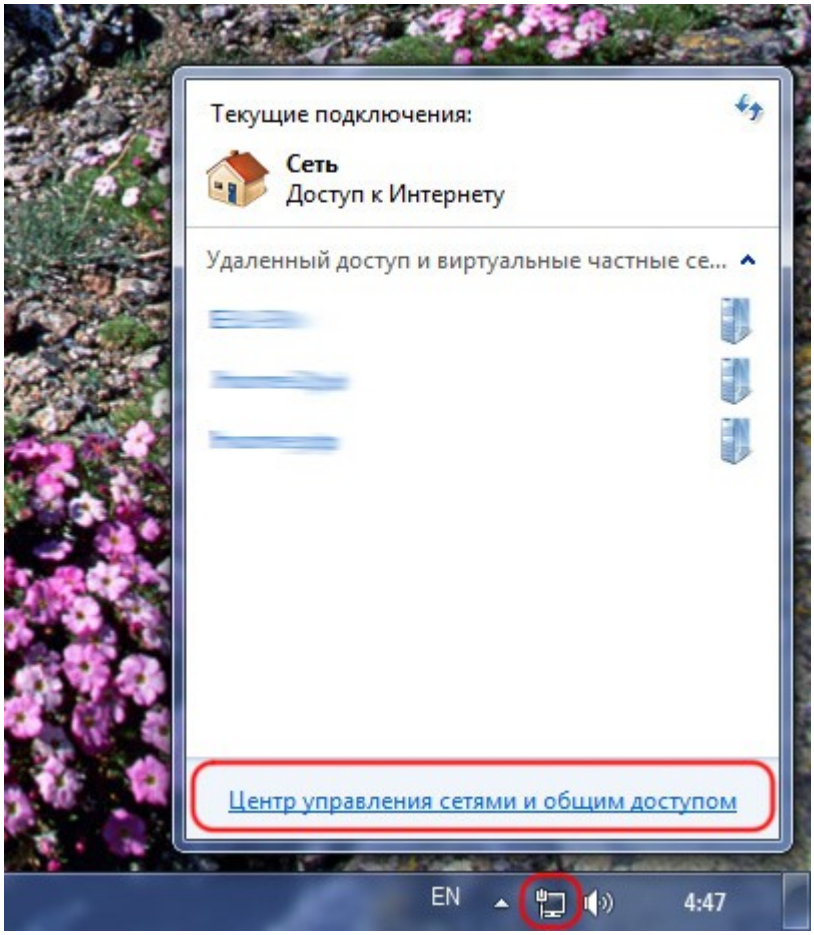


Рисунок 7.5.1.

2. В открывшемся окне выберите **Настройка нового подключения или сети** (рис. 7.5.2).

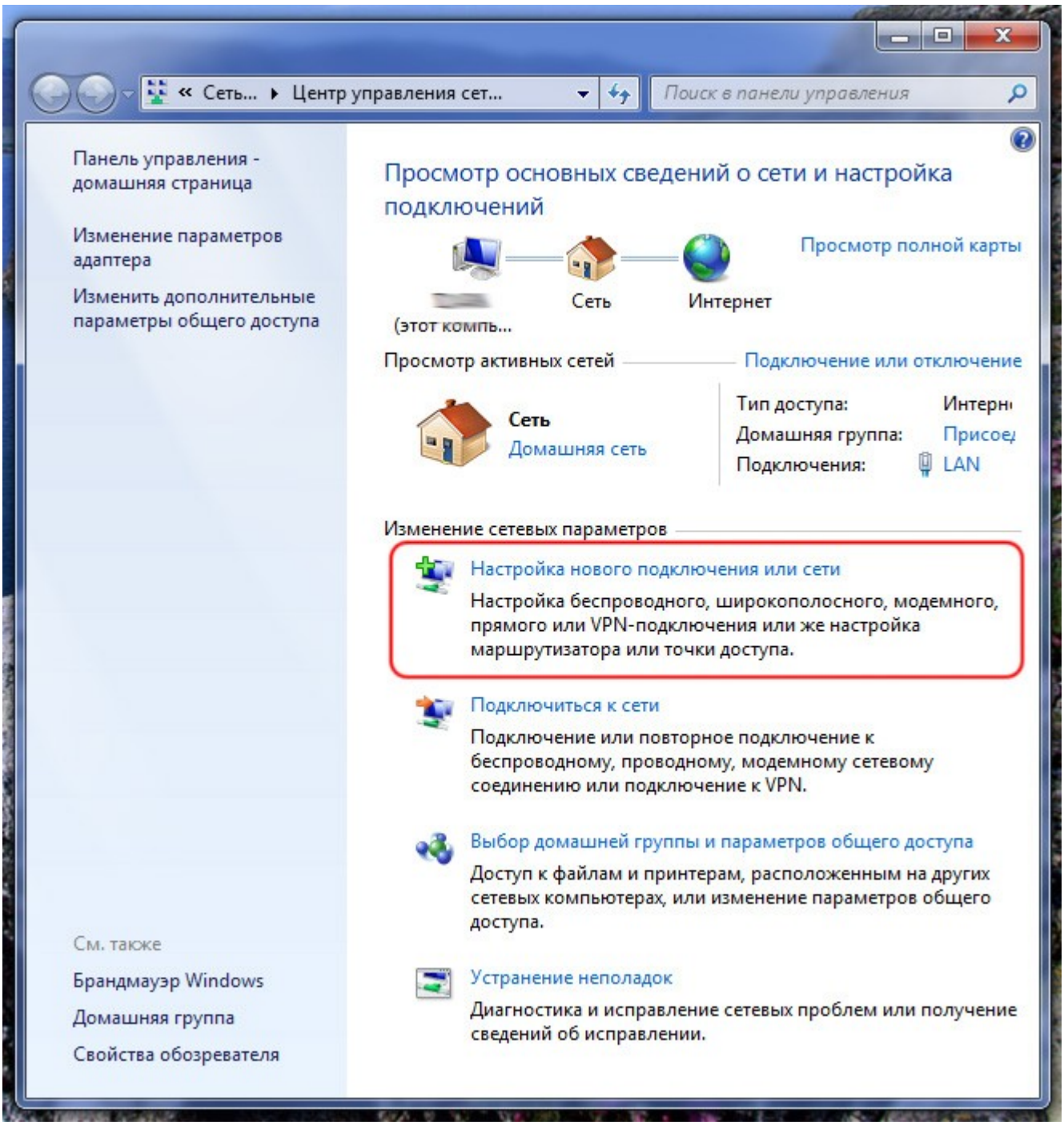


Рисунок 7.5.2.

3. Выберите **Подключение к рабочему месту**. Нажмите **Далее** (рис. 7.5.3).

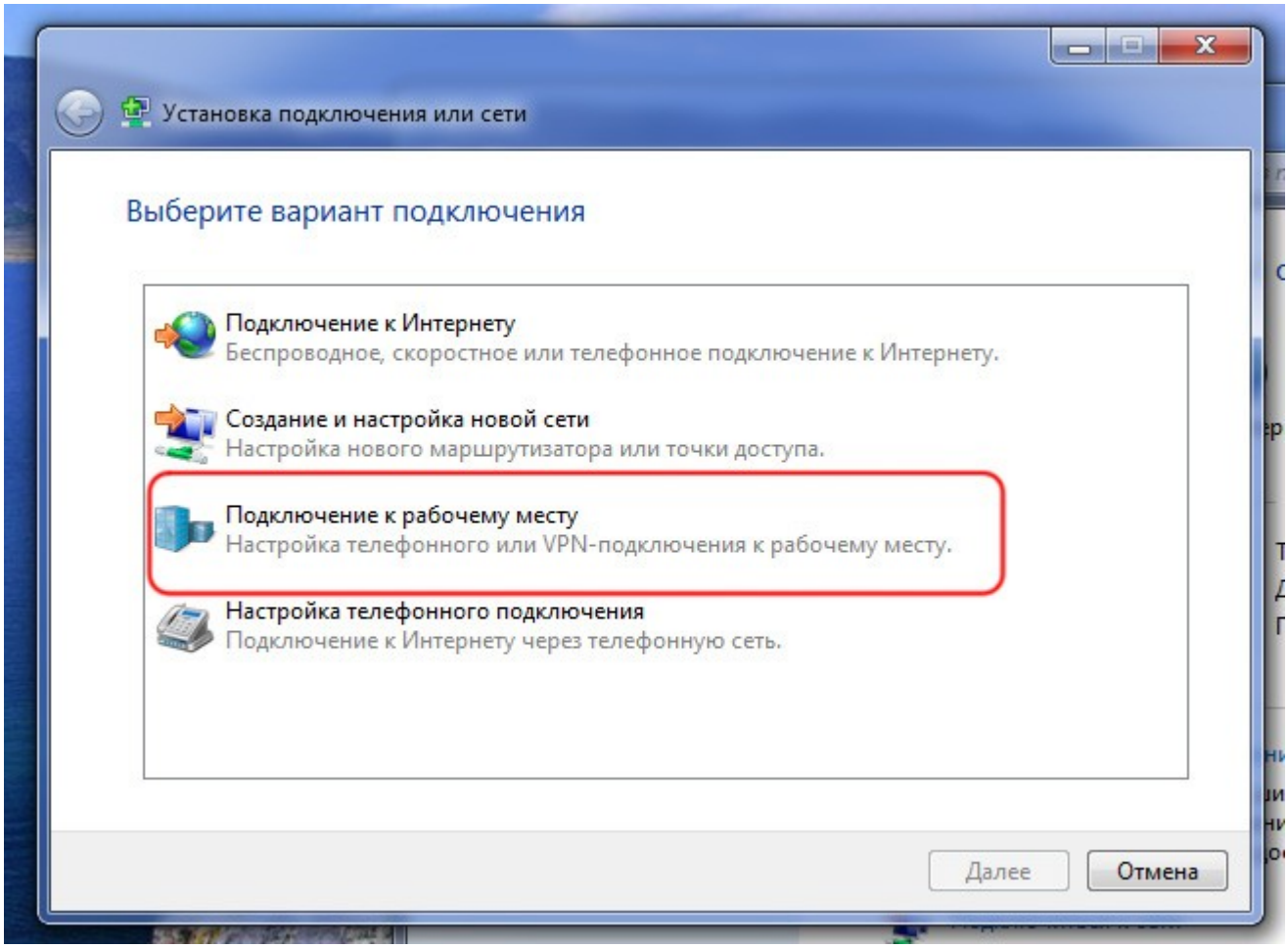


Рисунок 7.5.3.

4. Если появиться окно с предложением использовать имеющееся подключение выберете пункт **Нет, создать новое подключение** и нажмите **Далее** (рис. 7.5.4).

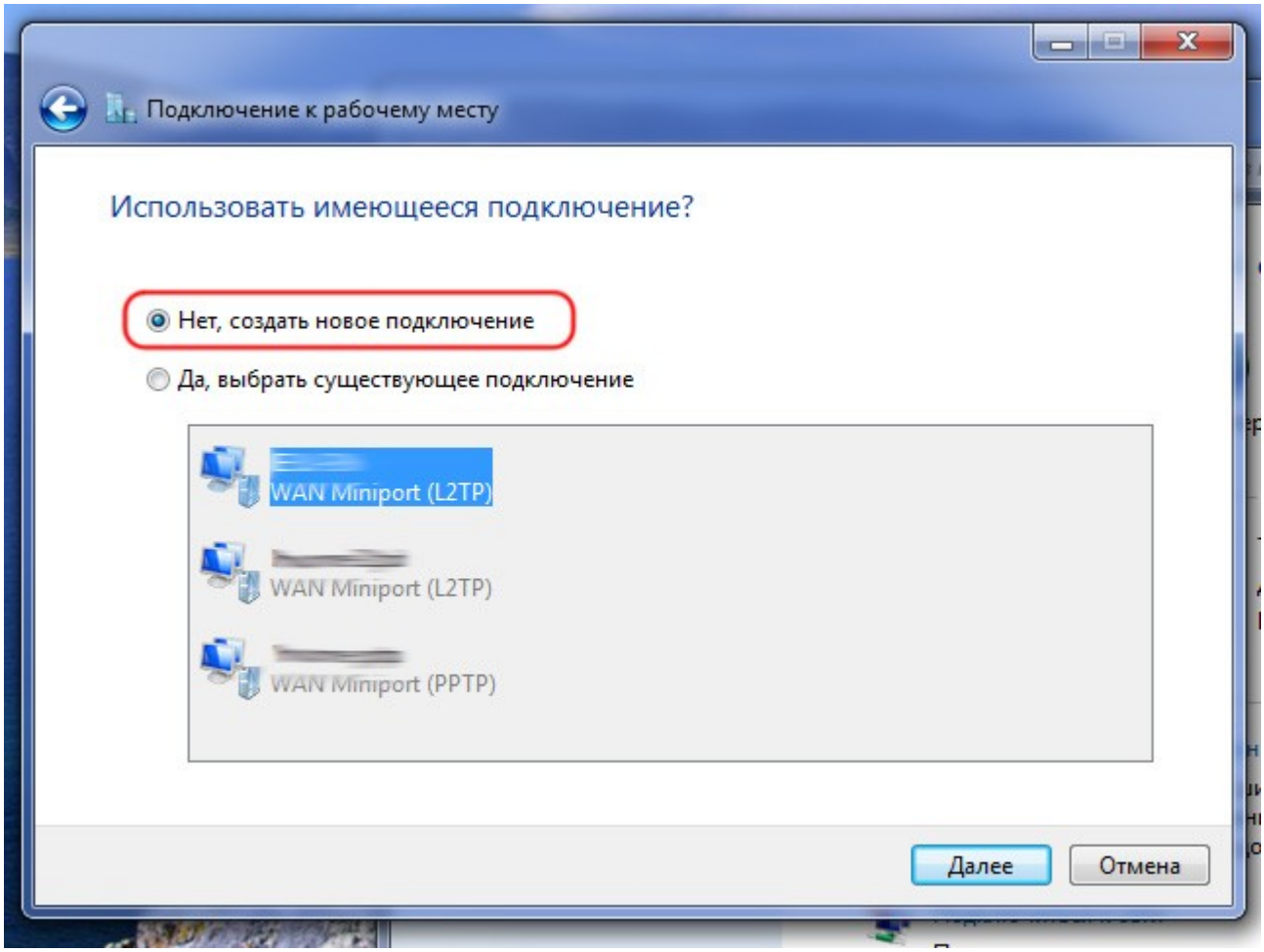


Рисунок 7.5.4.

5. Выберите **Использовать мое подключение к Интернету (VPN)** (рис. 7.5.5).

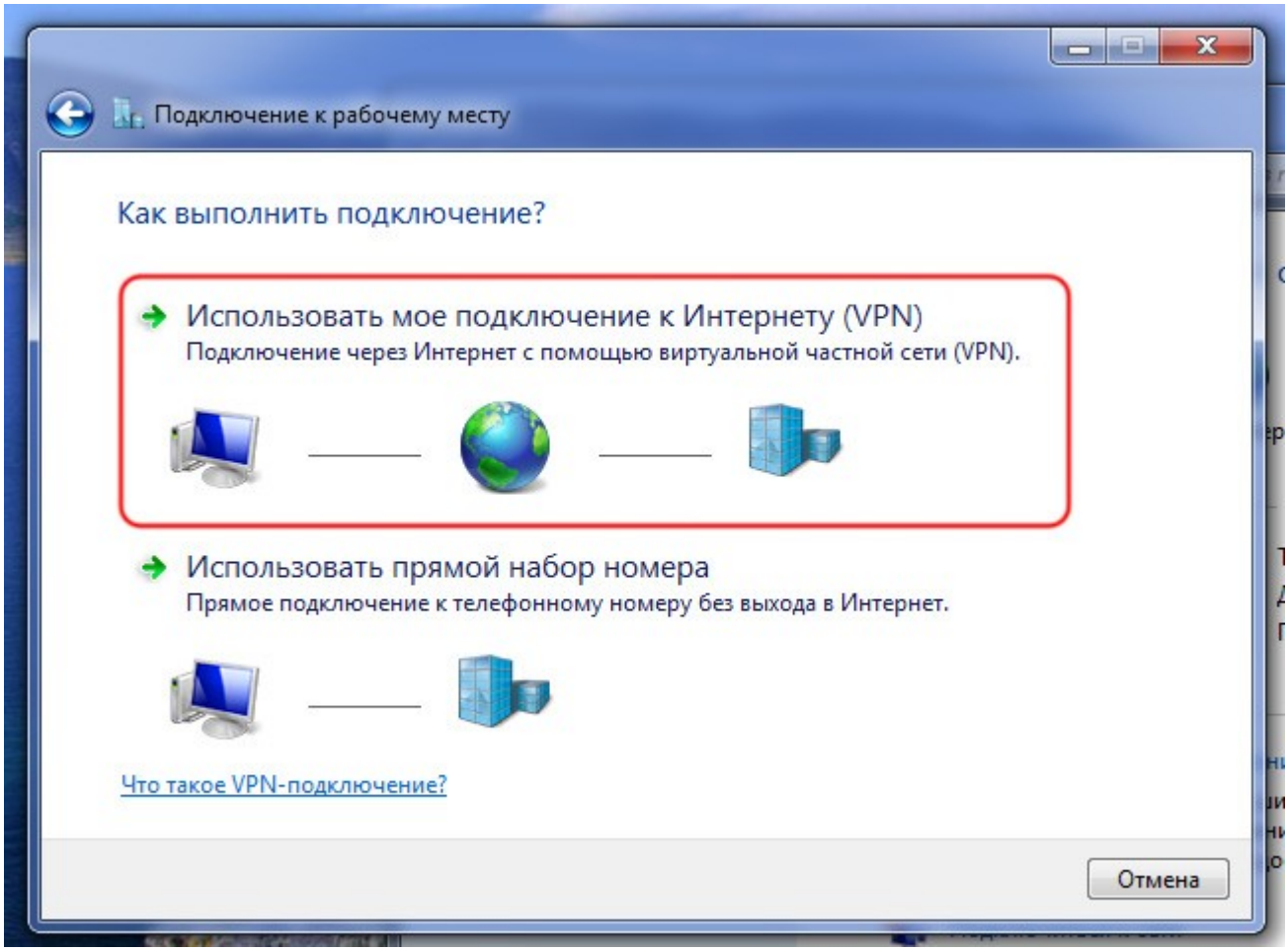


Рисунок 7.5.5.

6. В открывшемся окне заполните поле **Интернет-адрес**, введя в него IP адрес Интернет адаптера сервера VPN или сетевое имя если у вас настроен сервис DDNS, если сервер работает в режиме «Маршрутизатор и VPN», либо IP адрес стороннего маршрутизатора, если сервер работает в режиме «Только VPN».
В поле **Имя местоназначения**, введите имя которое будет ассоциироваться с этим подключением, например ”Офис pptp”. Также необходимо поставить галочку на против пункта **Не подключаться сейчас, только выполнить установку для подключения в будущем**, и нажмите **Далее** (рис. 7.5.6).

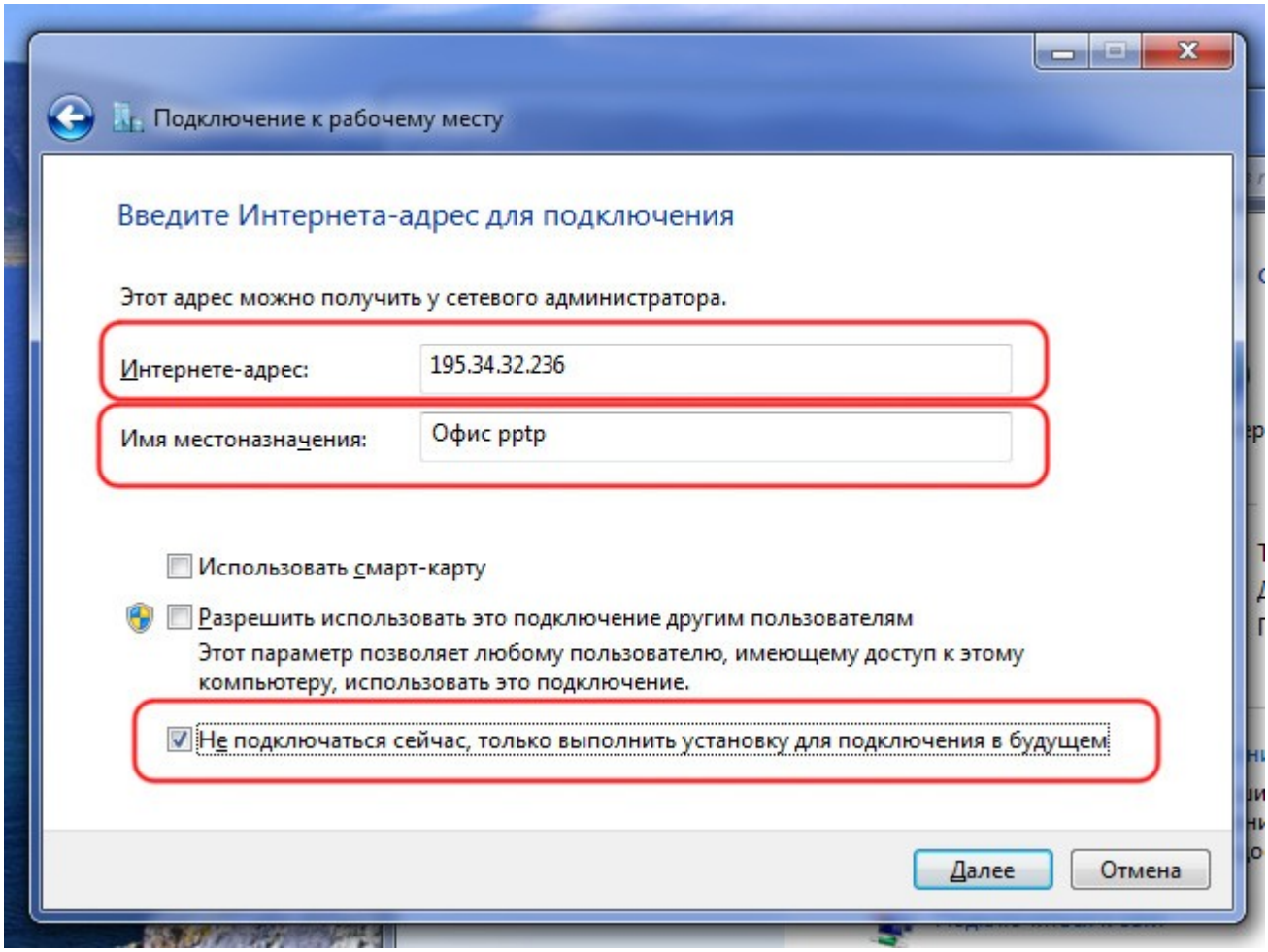


Рисунок 7.5.6.

7. В соответствующих полях введите ваши логин (имя пользователя) и пароль, которые были заведены на VPN сервере.
Будьте внимательны при заполнении, заглавные и строчные символы различаются, также удостоверьтесь что активна англоязычная раскладка. Для удобства можете поставить галочку для отображения вводимых символов. В целях обеспечения большей безопасности не рекомендуется использовать автоматическое запоминание пароля.
Нажмите **Создать** (рис. 7.5.7). После создания подключения, в появившемся окне, нажмите **Закрыть**.

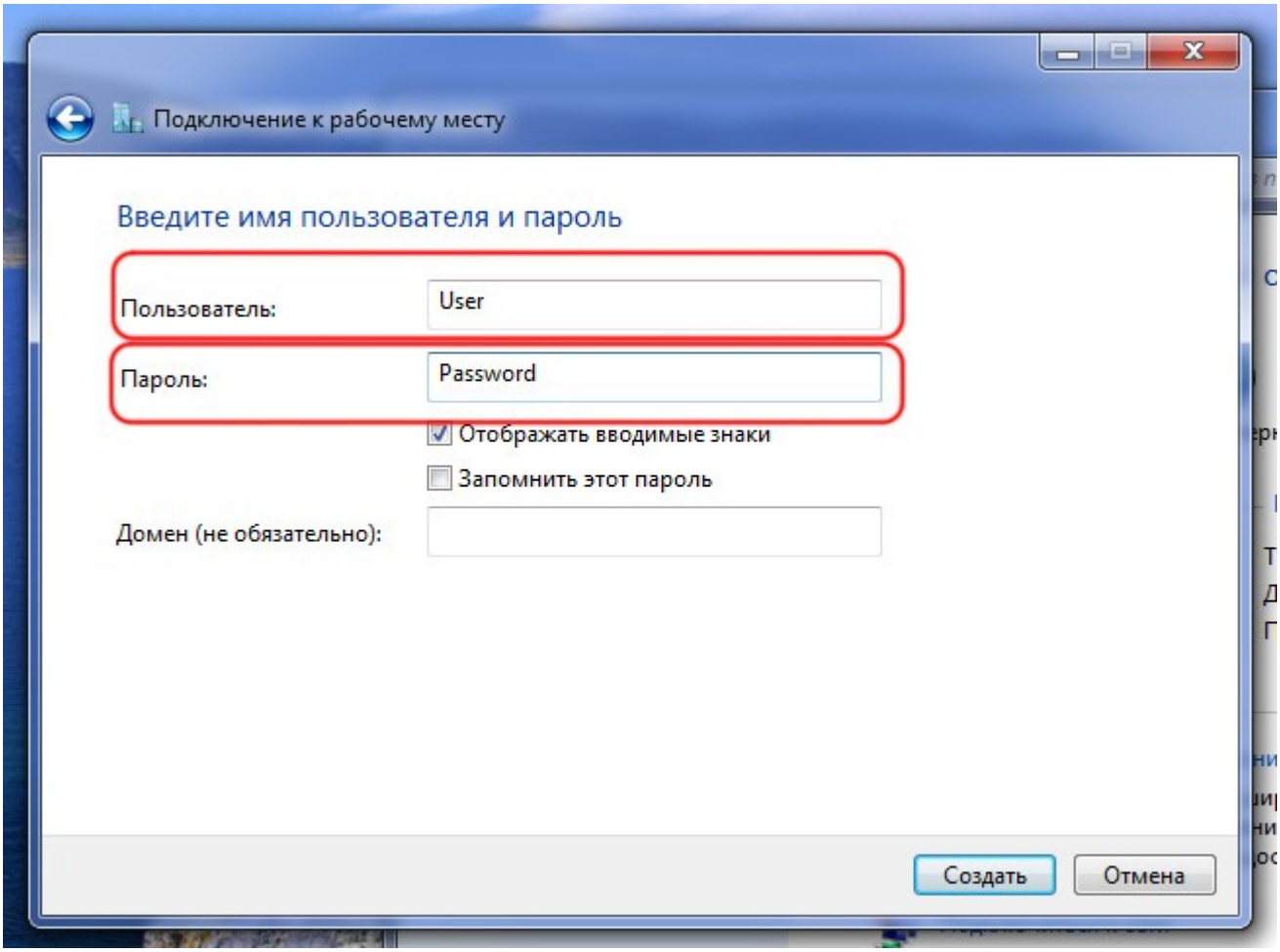


Рисунок 7.5.7.

8. Справа внизу, рядом с часами, щелкните по значку в виде монитора с кабелем. Затем щелкните правой кнопкой мыши по только что созданному подключению, например ”**Офис pptp”**, и нажмите **Свойства** (рис. 7.5.8).

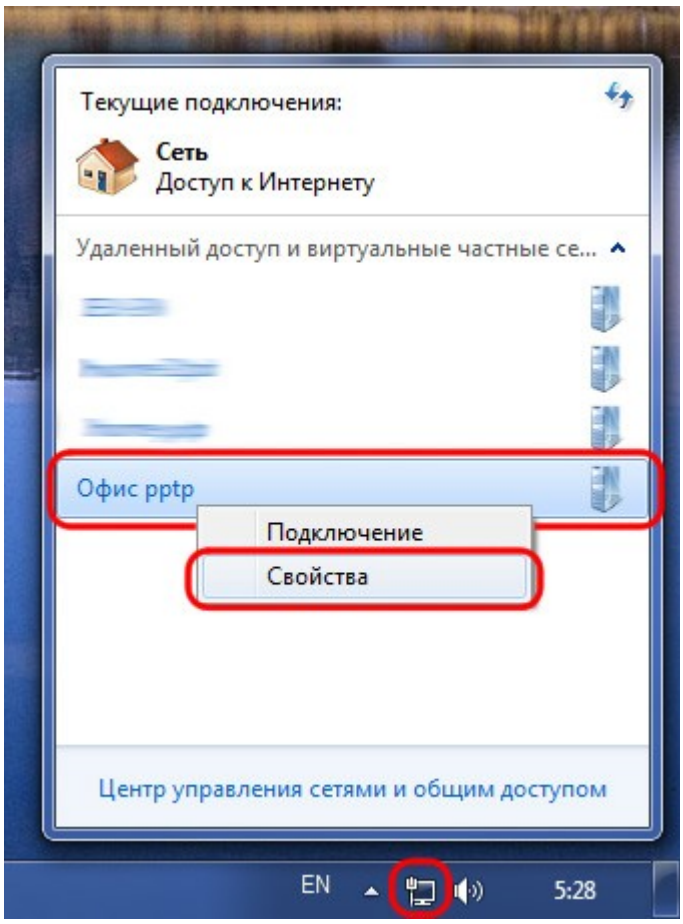


Рисунок 7.5.8.

9. Откройте вкладку **Безопасность**, и укажите **Тип VPN: Туннельный протокол точка-точка (PPTP).** Установите **Шифрование данных: необязательное (подключиться даже без шифрования)** (рис. 7.5.9). При этом если на сервере будет включено шифрование для протокола PPTP, то будет установлено шифрованное соединение, если отключено, то не шифрованное. После этого откройте вкладку **Сеть**.

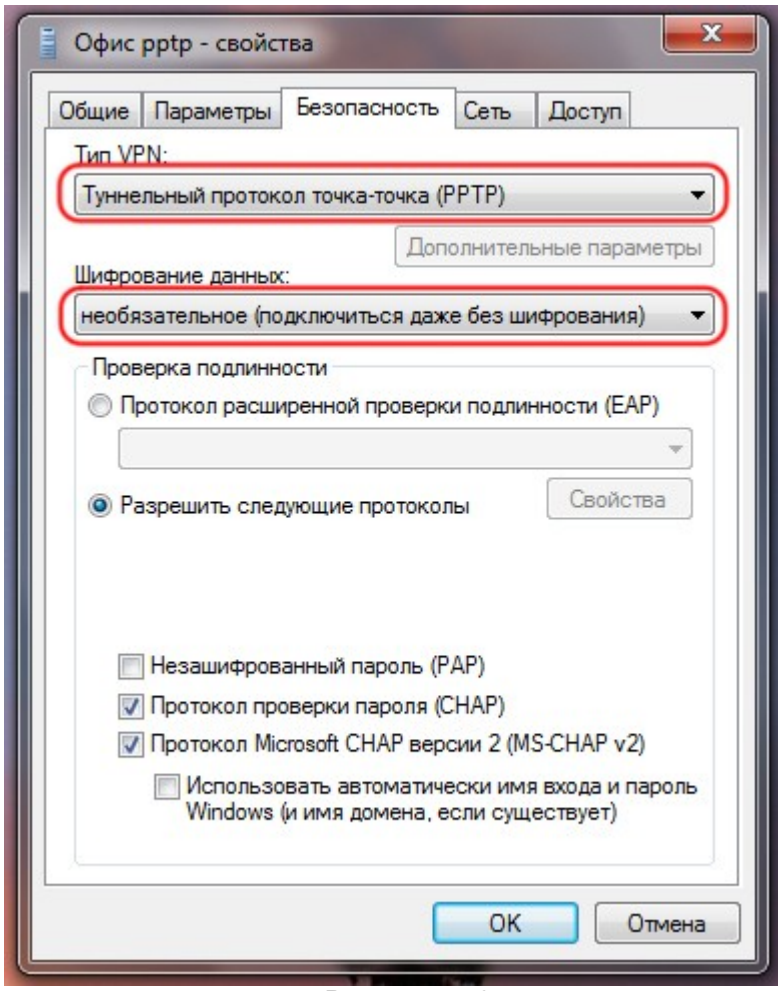


Рисунок 7.5.9.

10. Выберете **Протокол Интернета версии 4 (TCP/IPv4)**, и нажмите **Свойства** (рис. 7.5.10). Далее нажмите **Дополнительно**, и в появившемся окне снимите галочку **Использовать основной шлюз в удалённой сети** (рис. 7.5.11), и нажмите **Ok**. Далее **Ok** и снова **Ok**.

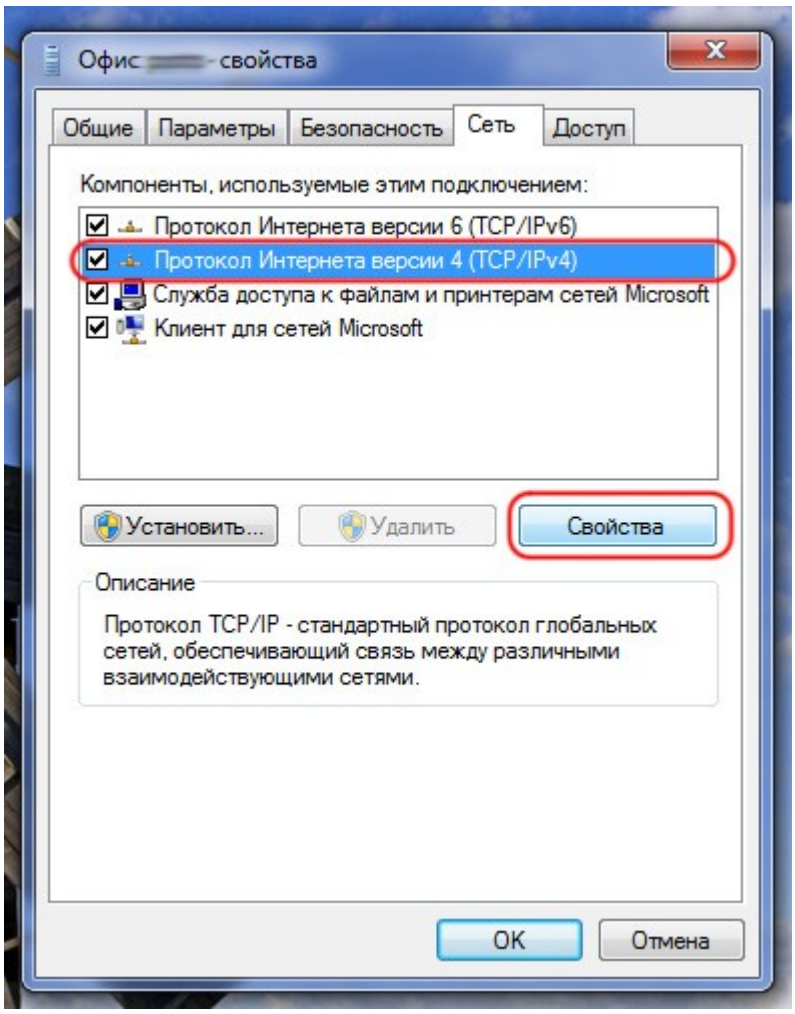


Рисунок 7.5.10.

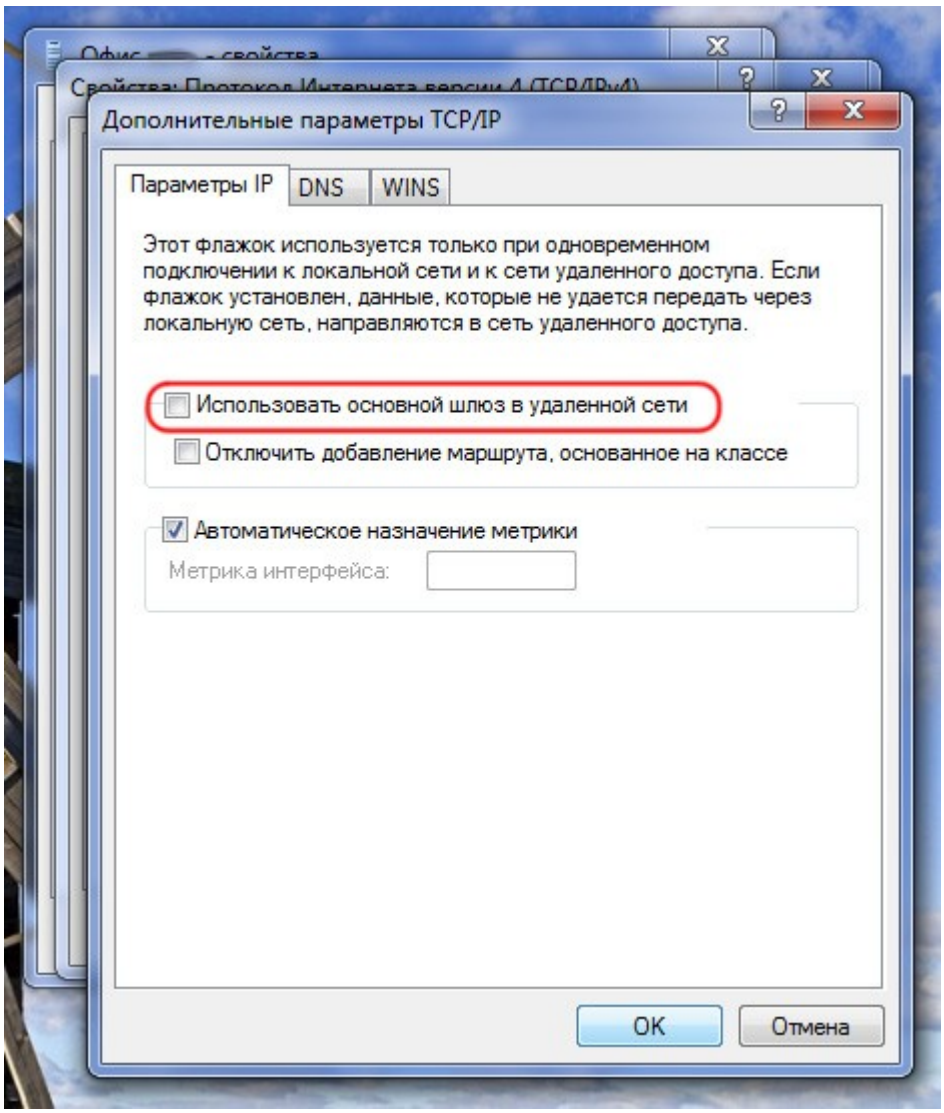


Рисунок 7.5.11.

На этом создание подключения завершено, и его можно использовать для подключения по протоколу PPTP.

7.5.2 Создание VPN подключения в Windows Vista/7 по протоколу L2TP

1. Справа внизу, рядом с часами, щелкните по значку в виде монитора с кабелем и выберите **Центр управления сетями и общим доступом** (рис. 7.5.12).

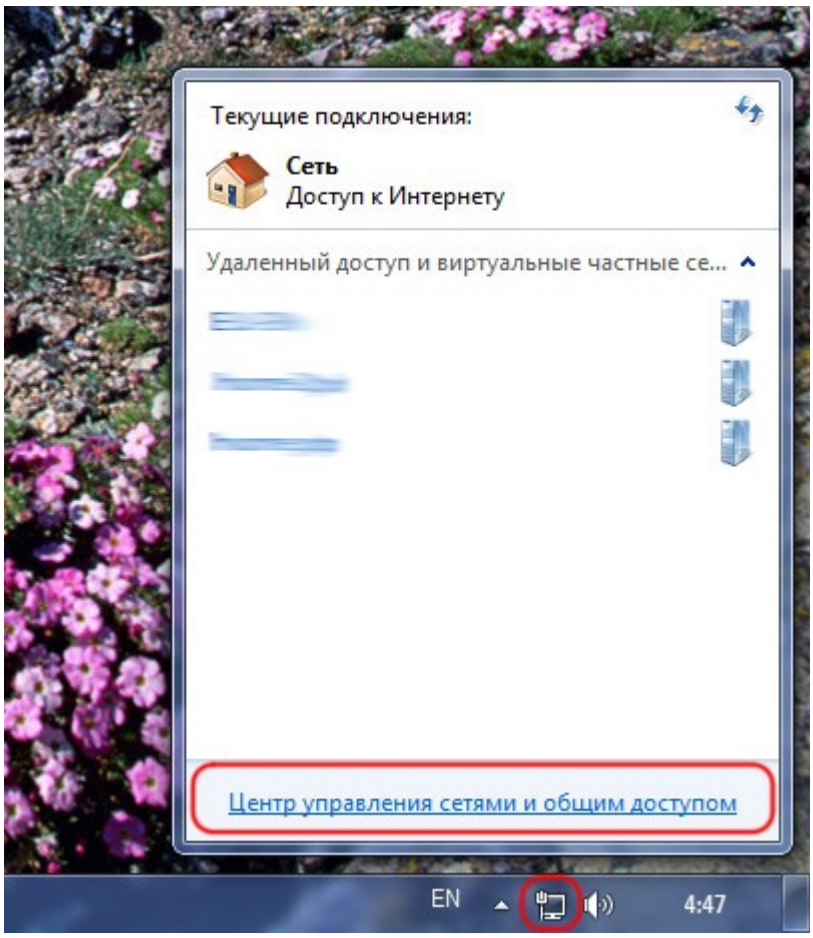


Рисунок 7.5.12.

2. В открывшемся окне выберите **Настройка нового подключения или сети** (рис. 7.5.13).

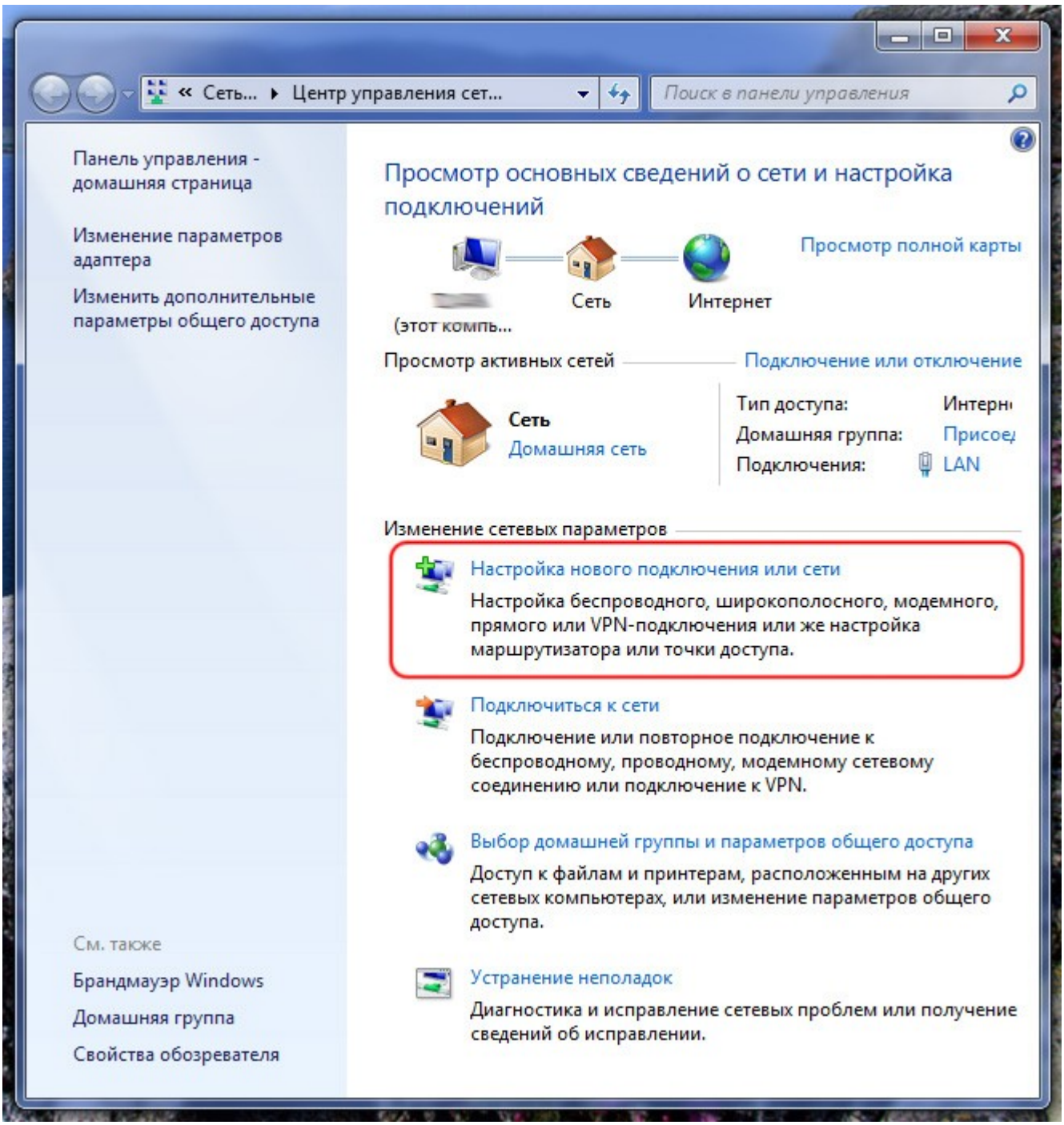


Рисунок 7.5.13.

3. Выберите **Подключение к рабочему месту**. Нажмите **Далее** (рис. 7.5.14).

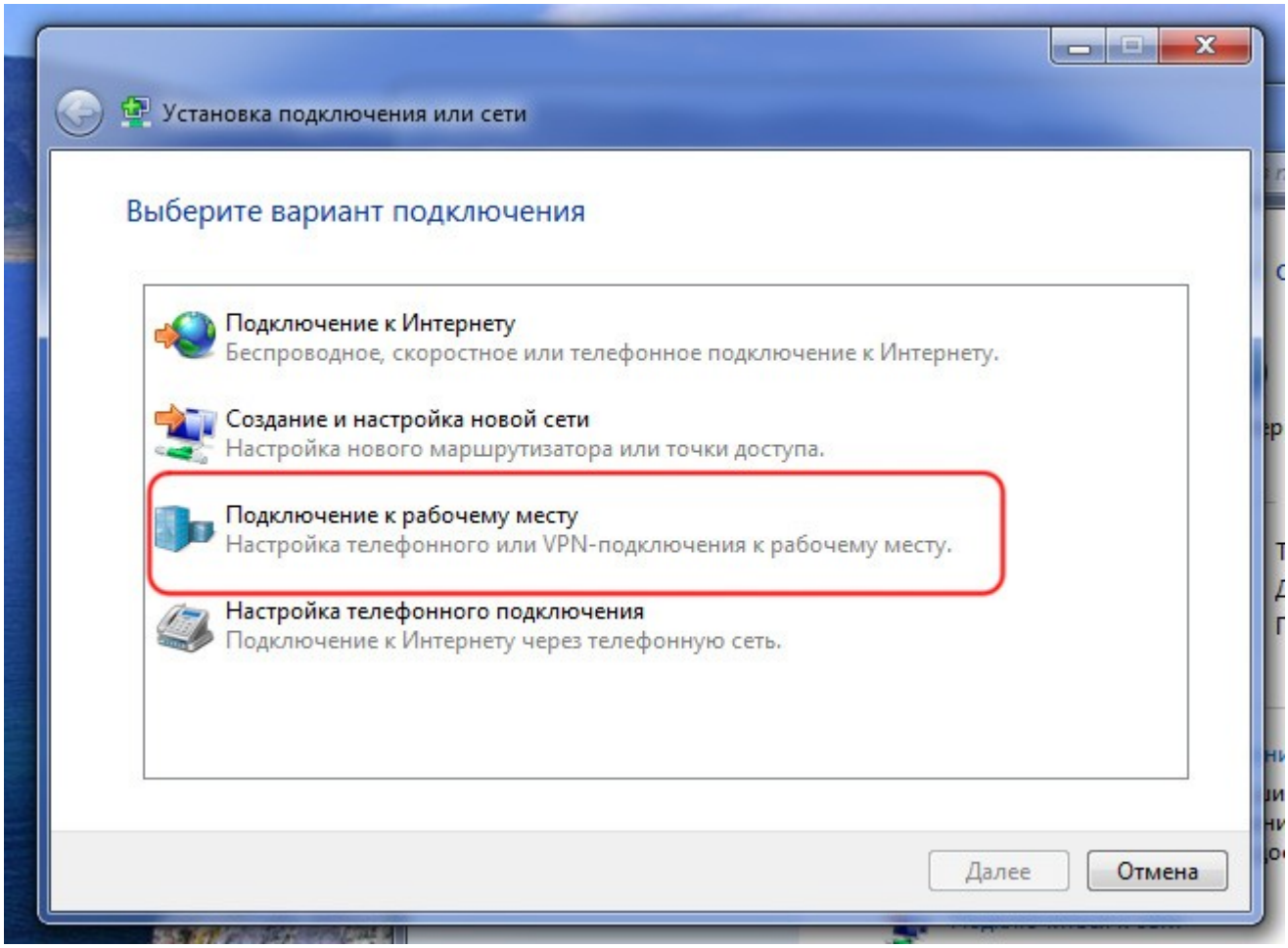


Рисунок 7.5.14.

4. Если появиться окно с предложением использовать имеющееся подключение выберете пункт **Нет, создать новое подключение** и нажмите **Далее** (рис. 7.5.15).

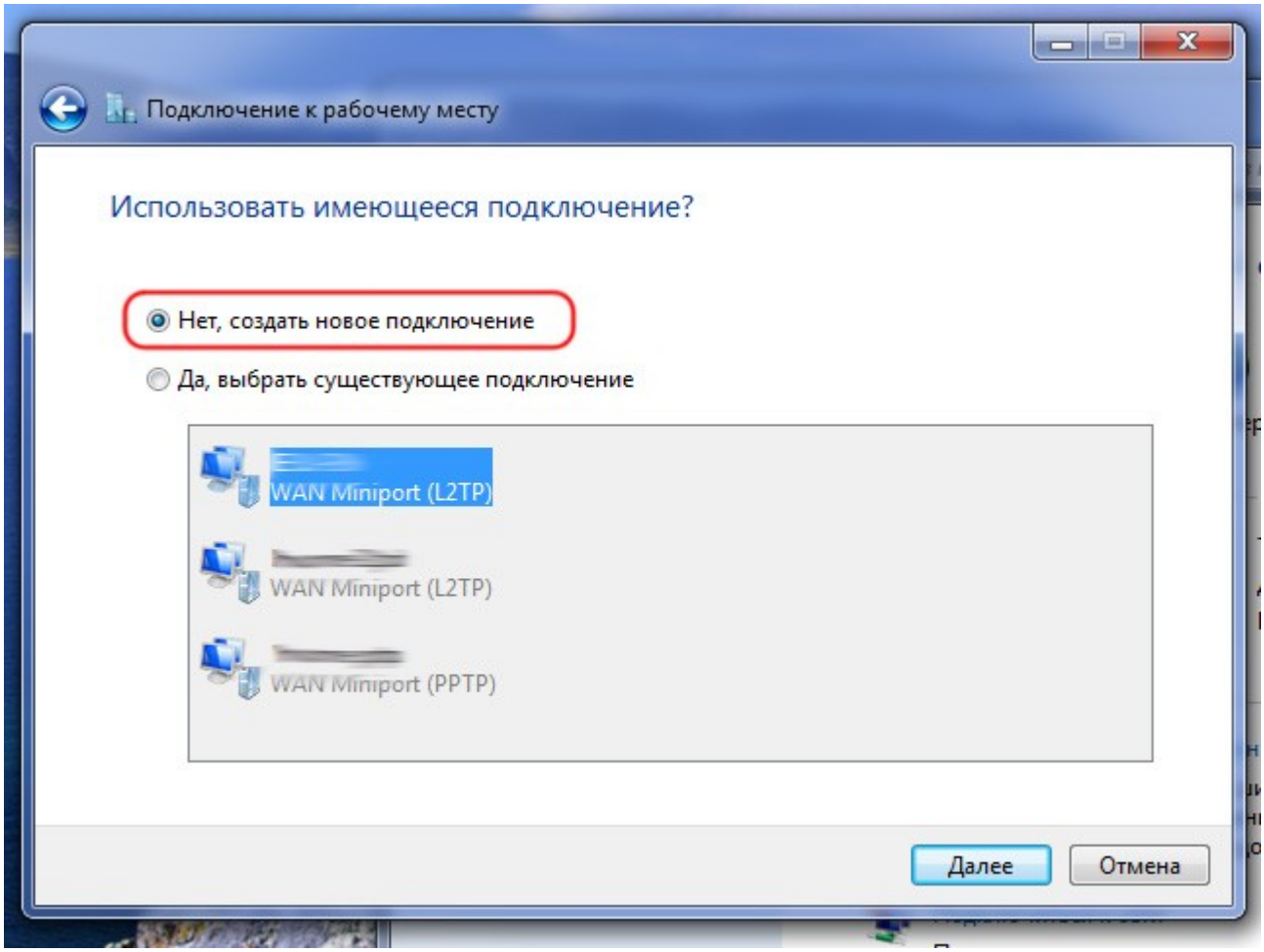


Рисунок 7.5.15.

5. Выберите **Использовать мое подключение к Интернету (VPN)** (рис. 7.5.16).

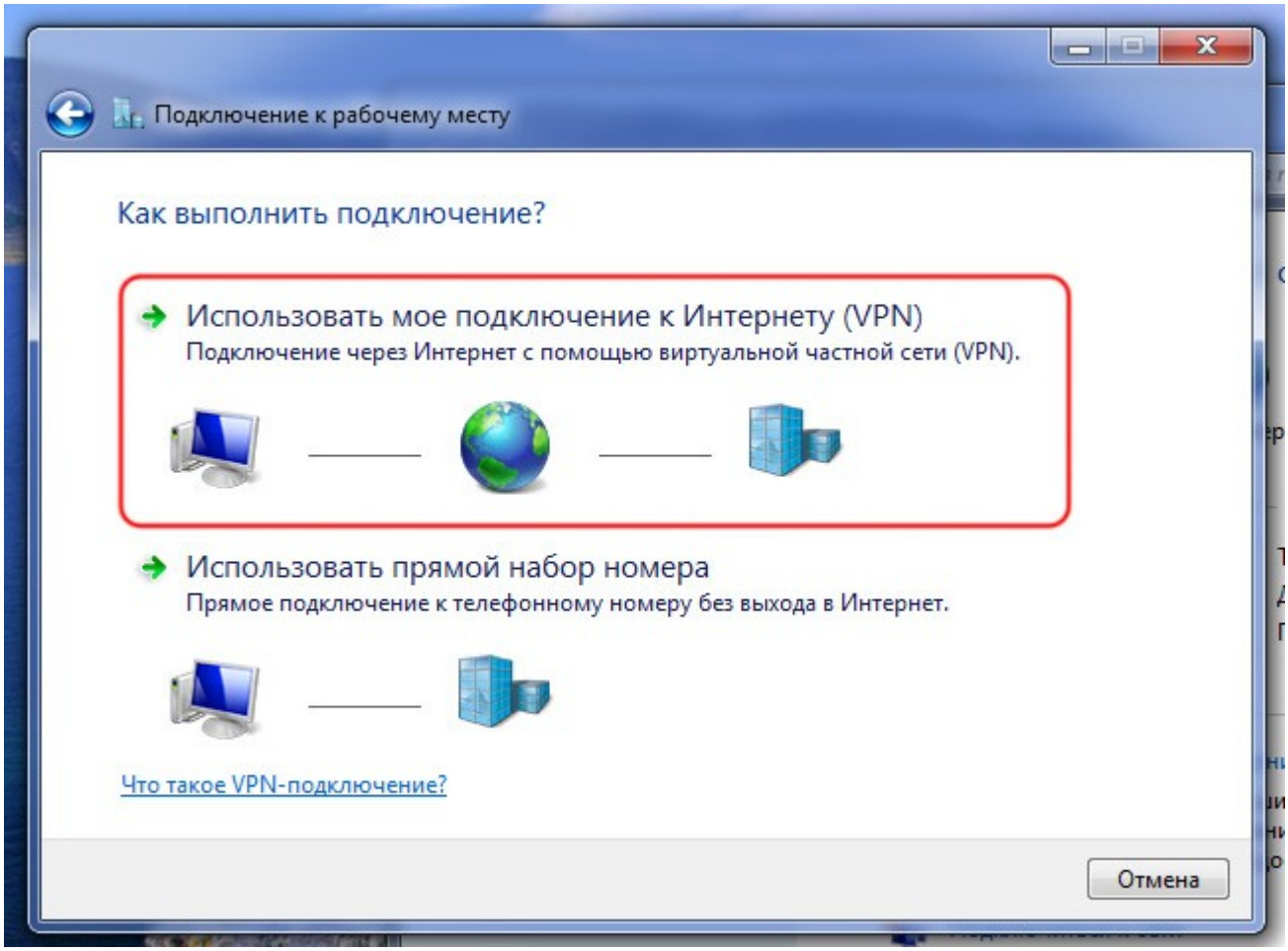


Рисунок 7.5.16.

6. В открывшемся окне заполните поле **Интернет-адрес**, введя в него IP адрес Интернет адаптера сервера VPN или сетевое имя если у вас настроен сервис DDNS, если сервер работает в режиме «Маршрутизатор и VPN», либо IP адрес стороннего маршрутизатора, если сервер работает в режиме «Только VPN».
В поле **Имя местоназначения**, введите имя которое будет ассоциироваться с этим подключением, например ”Офис l2tp”. Также необходимо поставить галочку на против пункта **Не подключаться сейчас, только выполнить установку для подключения в будущем**, и нажмите **Далее** (рис. 7.5.17).

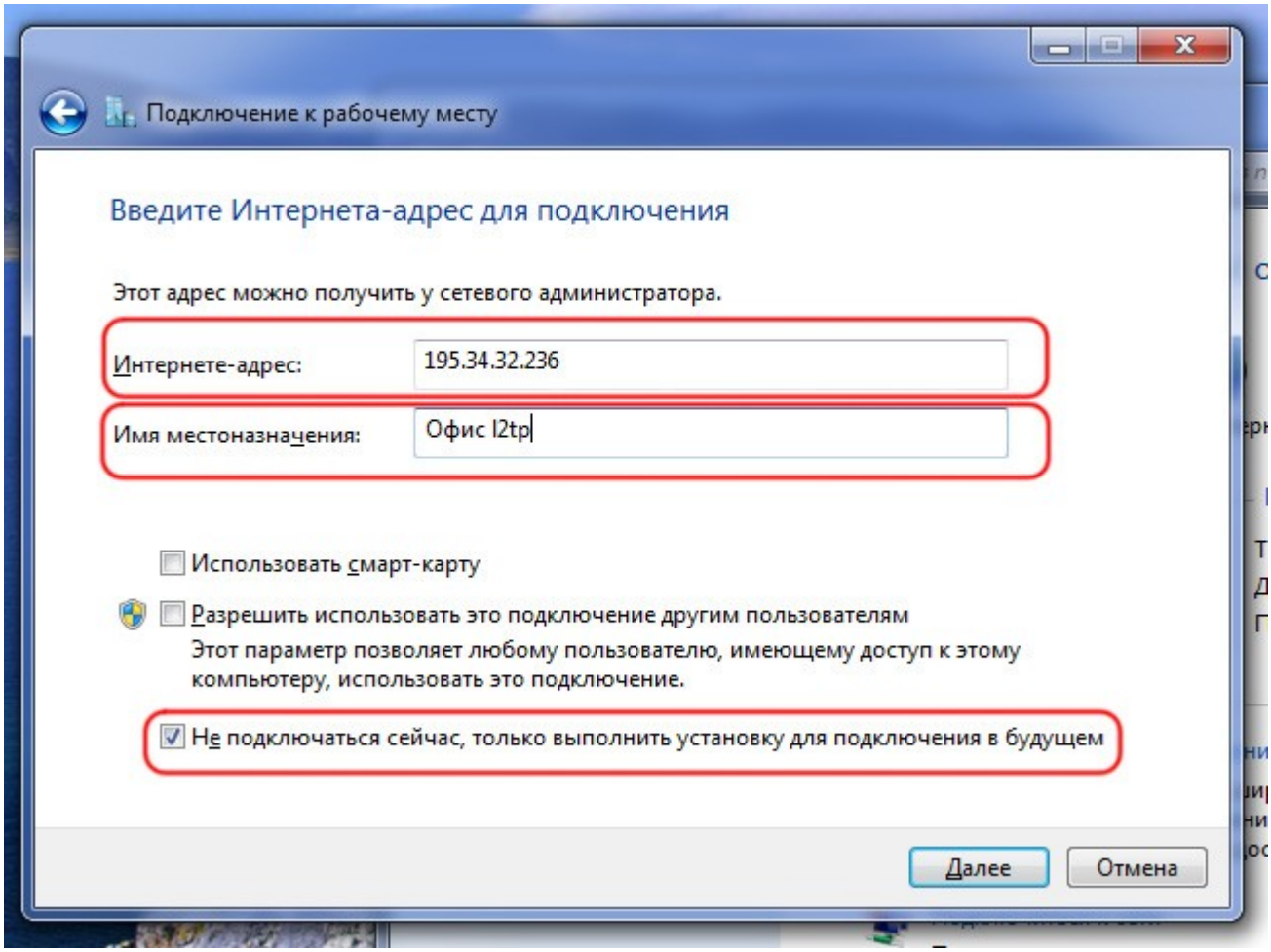


Рисунок 7.5.17.

7. В соответствующих полях введите ваши логин (имя пользователя) и пароль, которые были заведены на VPN сервере.
Будьте внимательны при заполнении, заглавные и строчные символы различаются, также удостоверьтесь что активна англоязычная раскладка. Для удобства можете поставить галочку для отображения вводимых символов. В целях обеспечения большей безопасности не рекомендуется использовать автоматическое запоминание пароля.
Нажмите **Создать** (рис. 7.5.18). После создания подключения, в появившемся окне, нажмите **Закрыть**.

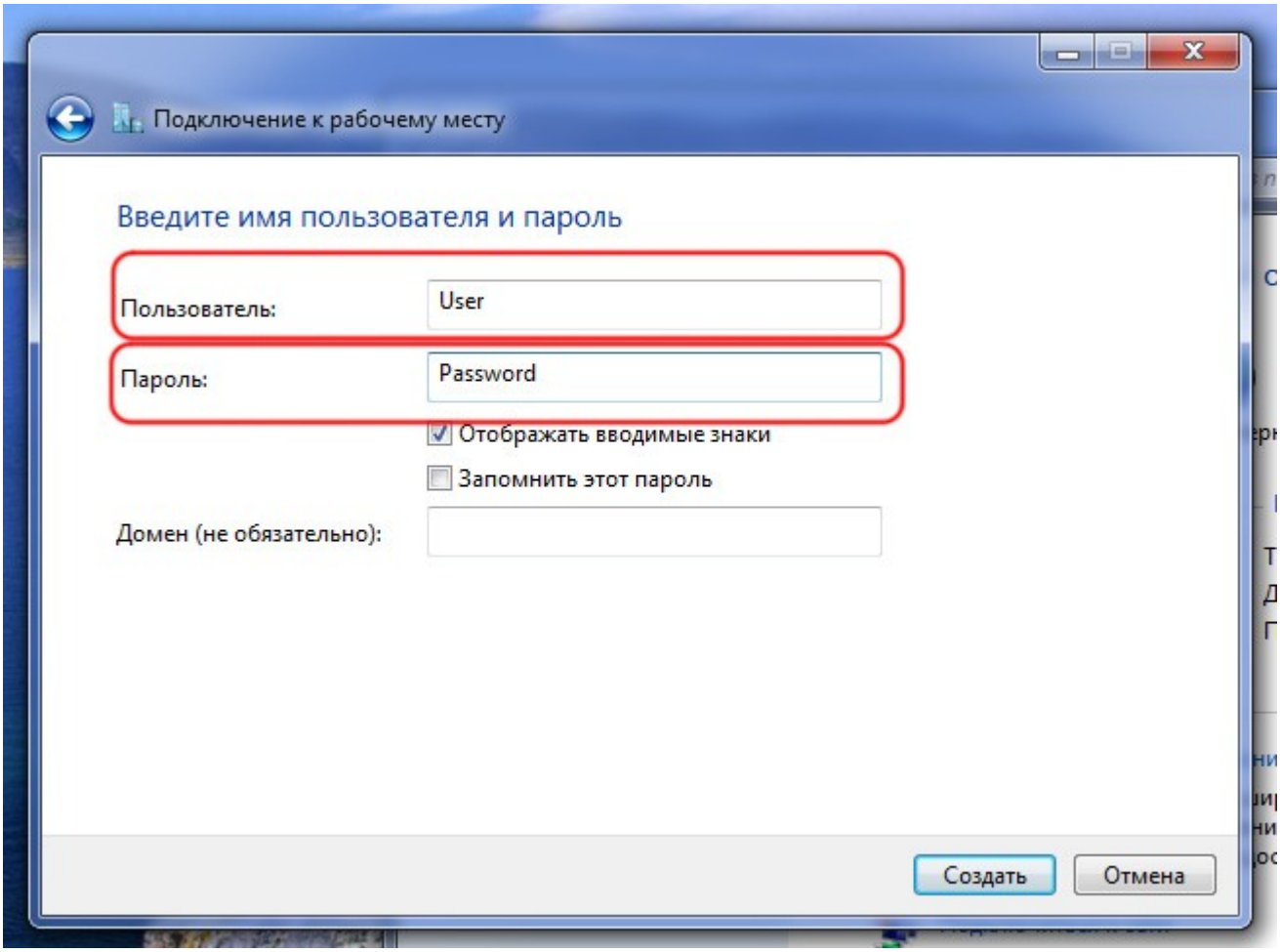


Рисунок 7.5.18.

8. Справа внизу, рядом с часами, щелкните по значку в виде монитора с кабелем. Затем щелкните правой кнопкой мыши по только что созданному подключению, например ”**Офис l2tp”**, и нажмите **Свойства** (рис. 7.5.19).

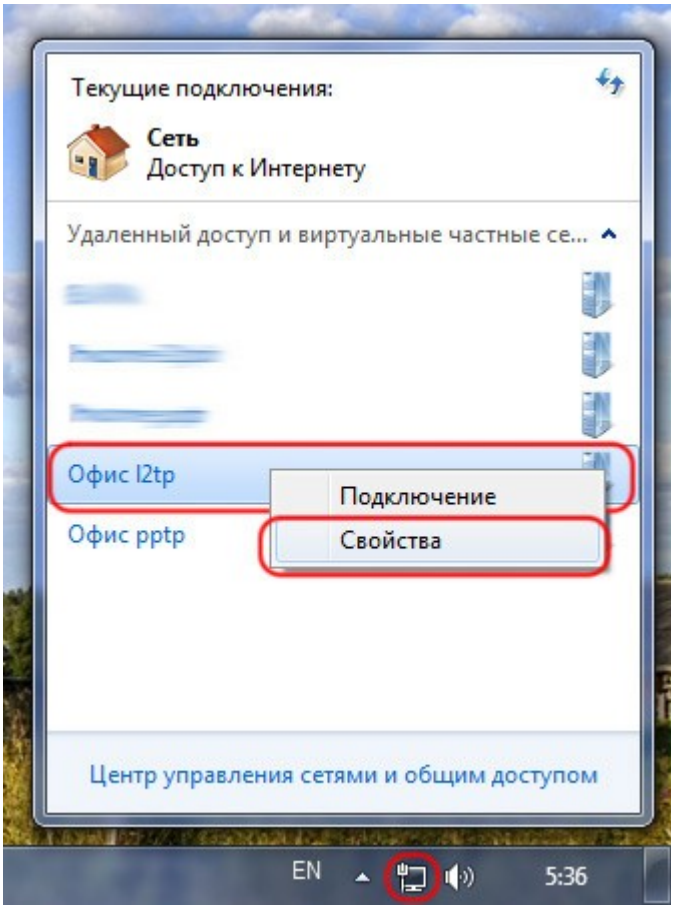


Рисунок 7.5.19.

9. Откройте вкладку **Безопасность**, и укажите **Тип VPN: L2TP IPsec VPN**. Установите **Шифрование данных: необязательное (подключиться даже без шифрования)** (рис. 7.5.20). При этом если на сервере будет включено шифрование для протокола L2TP, то будет установлено шифрованное соединение, если отключено, то не шифрованное. После этого откройте вкладку **Сеть**.

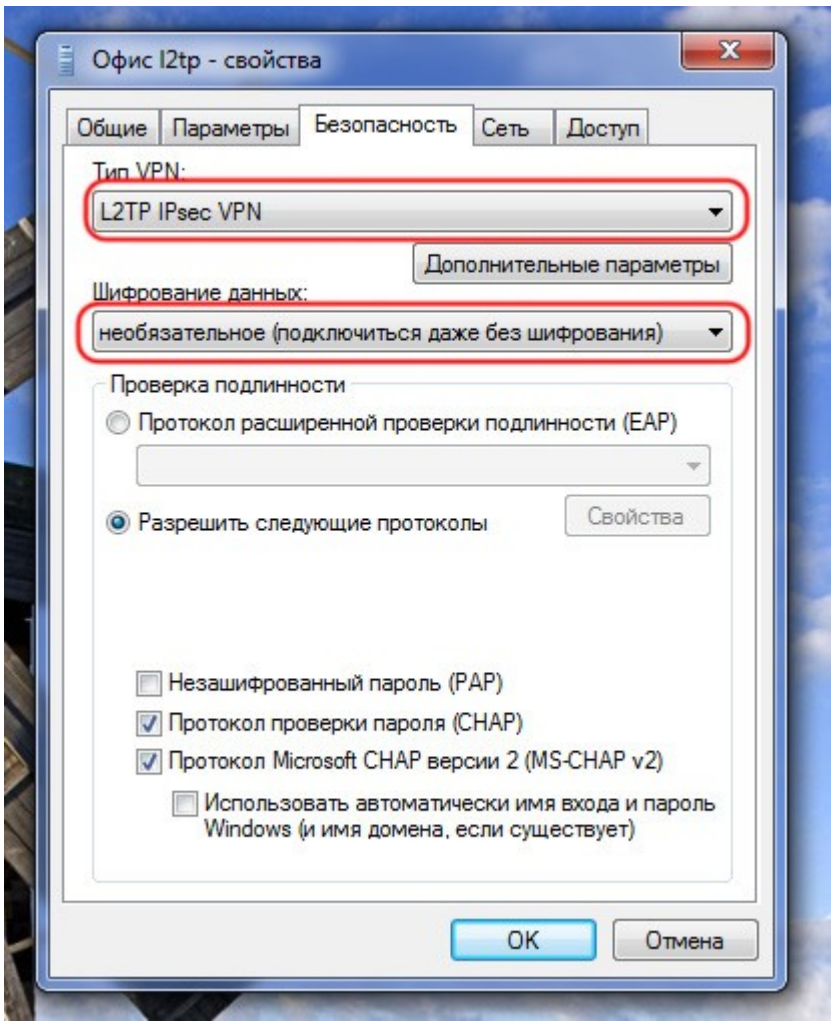


Рисунок 7.5.20.

10.Выберете **Протокол Интернета версии 4 (TCP/IPv4)**, и нажмите **Свойства** (рис. 7.5.21). Далее нажмите **Дополнительно**, и в появившемся окне снимите галочку **Использовать основной шлюз в удалённой сети** (рис. 7.5.22), и нажмите **Ok**. Далее **Ok** и снова **Ok**.

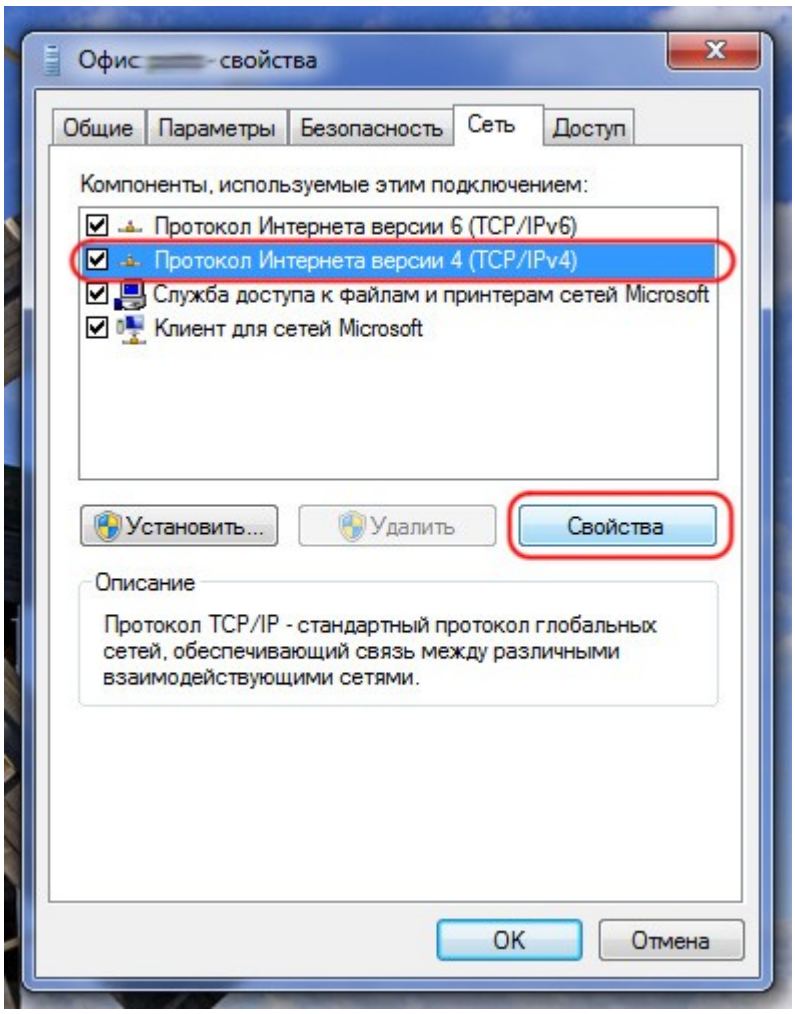


Рисунок 7.5.21.

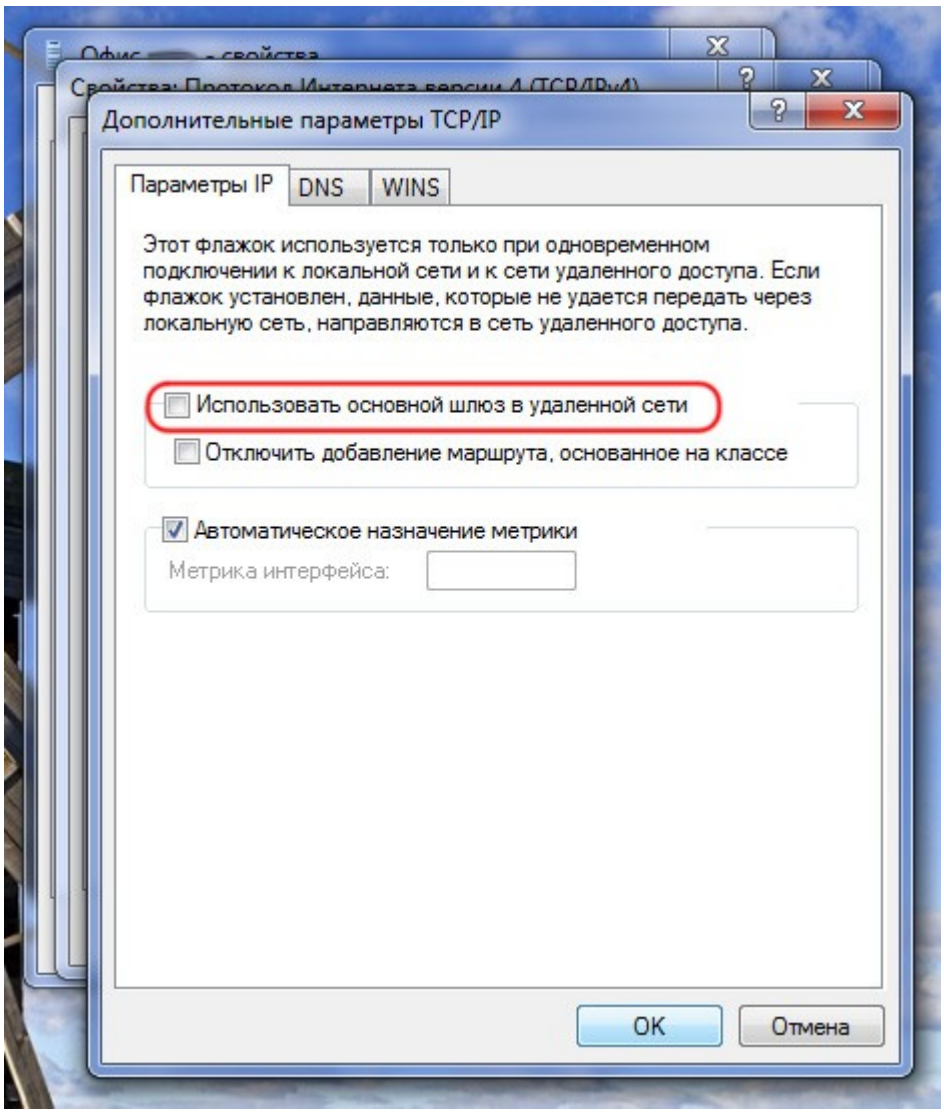


Рисунок 7.5.22.

На этом создание подключения завершено, и его можно использовать для подключения по протоколу L2TP.

7.5.3 Подключение и отключение в Windows Vista/7

Подключение

1. Справа внизу, рядом с часами, щелкните по значку в виде монитора с кабелем и выберите из списка соответствующее подключение, щелкнув по нему мышью а затем нажав **Подключение** (рис. 7.5.23).

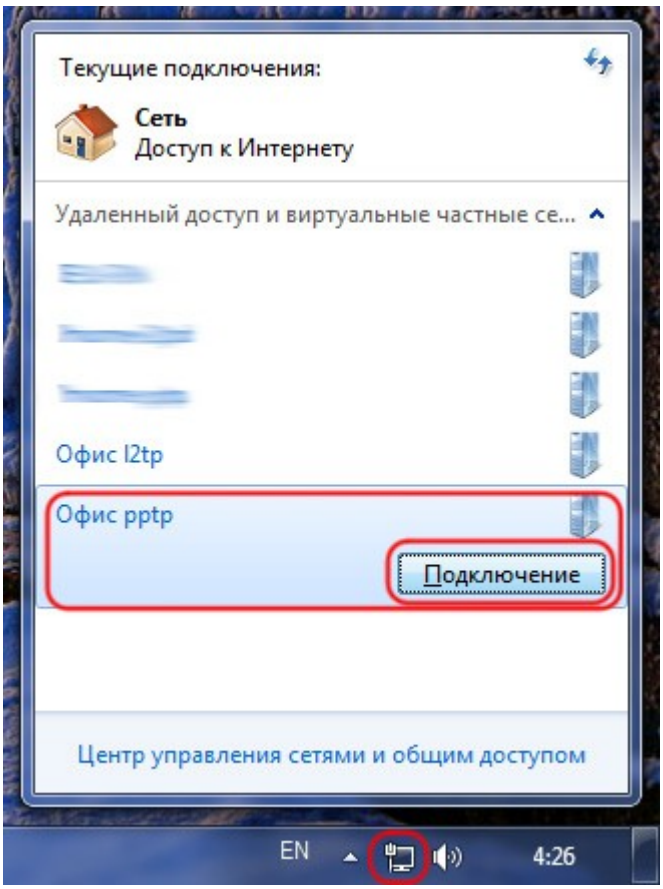


Рисунок 7.5.23.

2. В появившемся окне заполните соответствующие поля.
Если вы следовали рекомендации то вам будет достаточно ввести только пароль, и нажать **Подключение** (рис. 7.5.24).
Будьте внимательны при заполнении, заглавные и строчные символы различаются, также удостоверьтесь что активна англоязычная раскладка. В целях обеспечения большей безопасности не рекомендуется использовать автоматическое запоминание пароля.

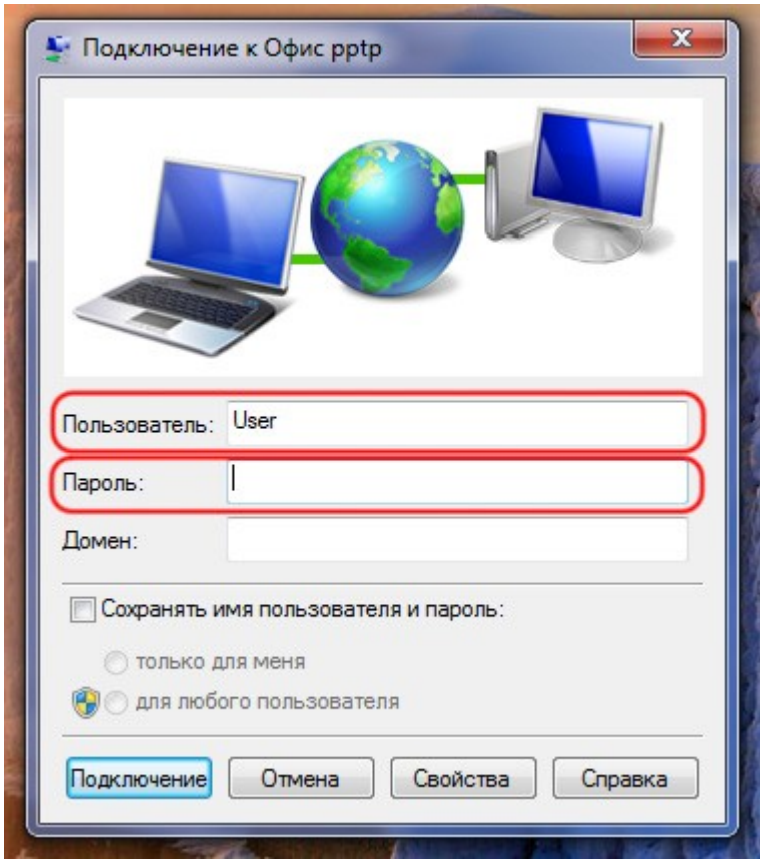


Рисунок 7.5.24.

В ответ на это вы увидите процесс соединения (рис. 7.5.25, 7.5.26).

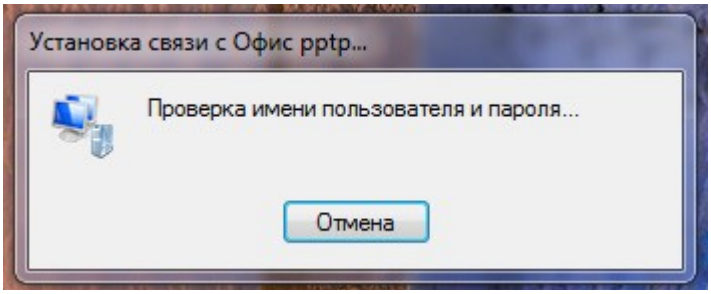


Рисунок 7.5.25.

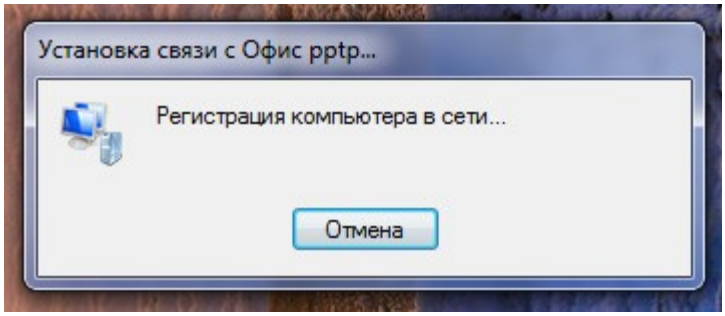


Рисунок 7.5.26.

Теперь вы подключены к удалённой сети, и можете пользоваться всеми её внутренними ресурсами, так если бы вы были подключены локально.
После того как вы выполните все необходимые вам действия обязательно выполните процесс отключения.

Отключение

1. Справа внизу, рядом с часами, щелкните по значку в виде монитора с кабелем и выберите из списка соответствующее активное подключение, щелкнув по нему мышью а затем нажав **Отключение** (рис. 7.5.27).

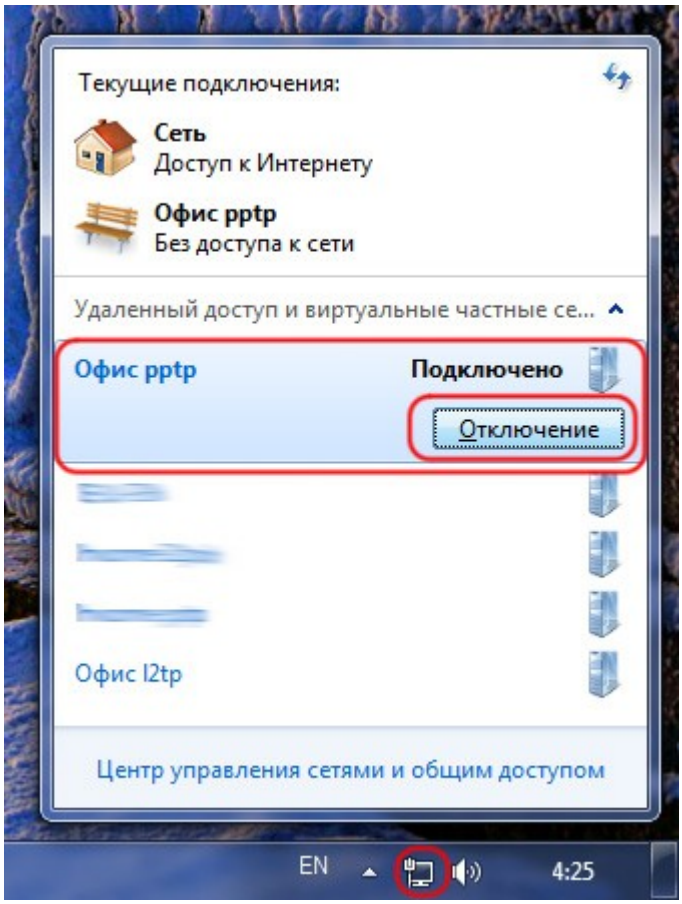


Рисунок 7.5.27.

7.5.4 Создание VPN подключения в Windows 2000/XP по протоколу PPTP

1. Нажмите **Пуск** и выберете **Панель управления** (рис. 7.5.28а.), либо **Пуск** -> **Настройка** -> **Панель управления** (рис. 7.5.28б.), в зависимости от настроек представления меню Пуск.

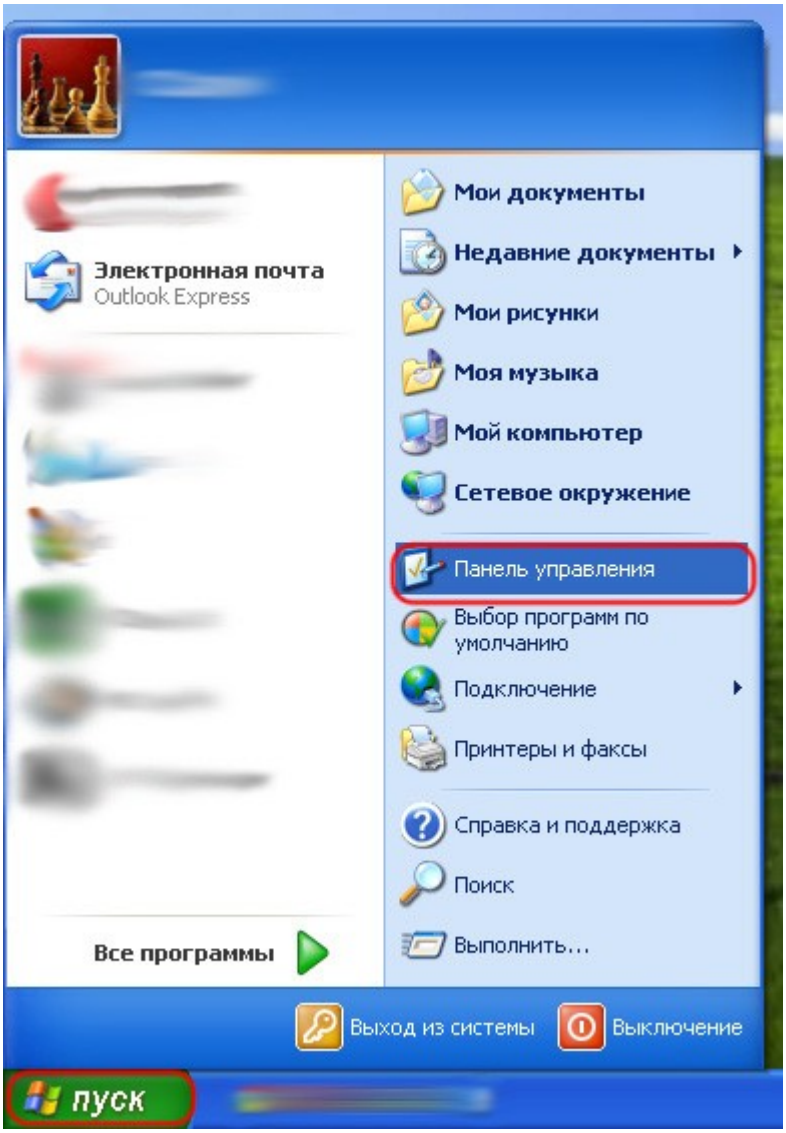


Рисунок 7.5.28а.

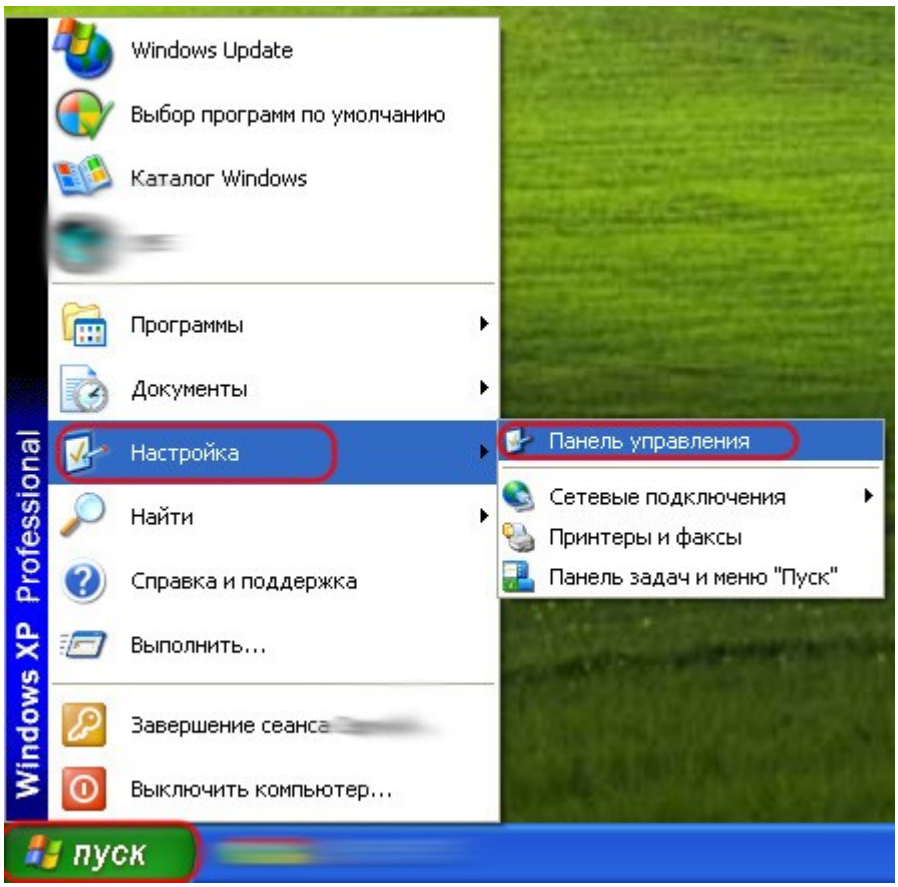


Рисунок 7.5.28б.

2. Далее, в случае необходимости, нажмите в левом верхнем углу открывшегося окна **Переключение к классическому виду**, и выберете **Сетевые подключения** (рис. 7.5.29).

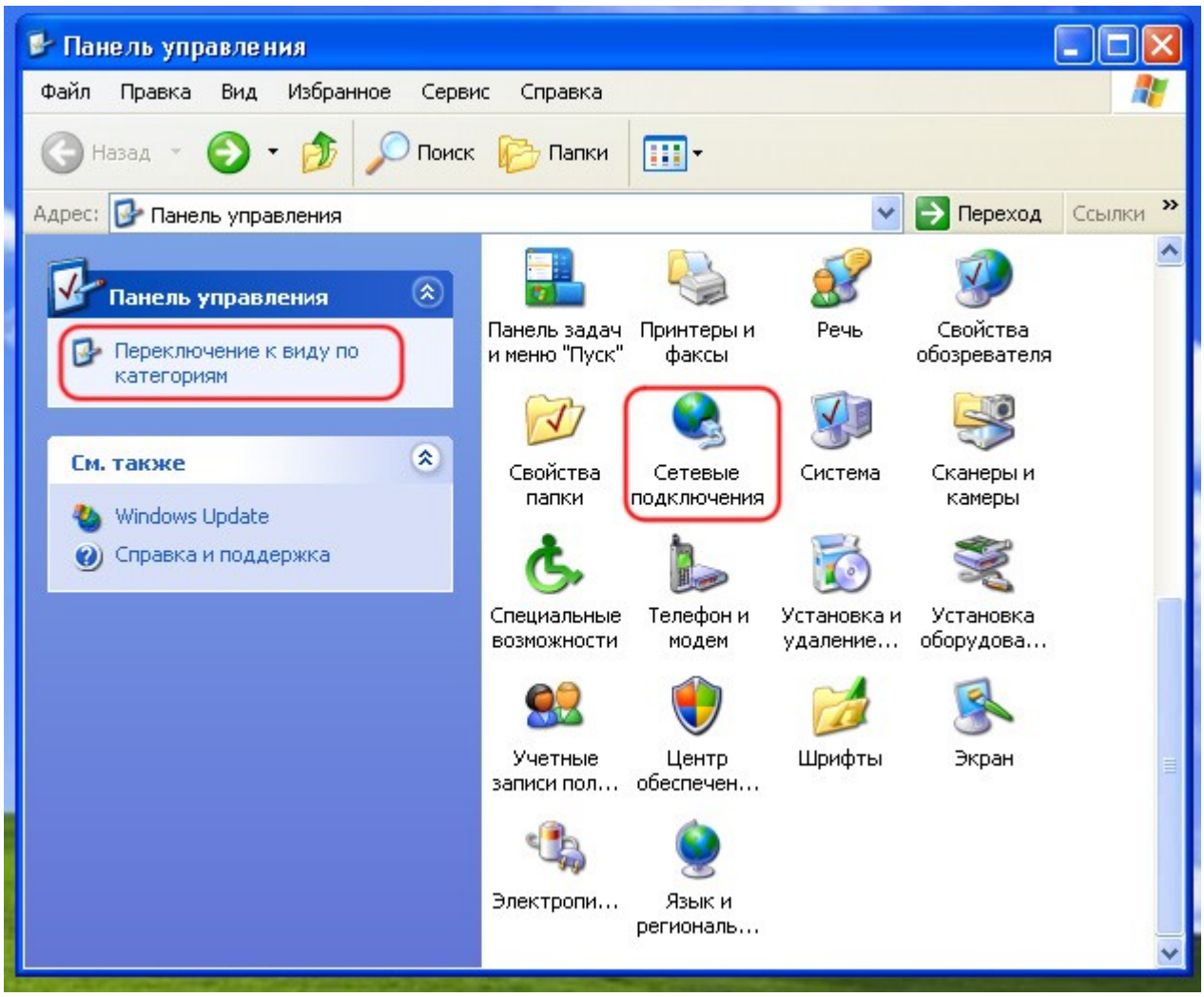


Рисунок 7.5.29.

3. Щёлкните мышкой по **Создание нового подключения**, и в появившемся окне нажмите **Далее** (рис. 7.5.30).

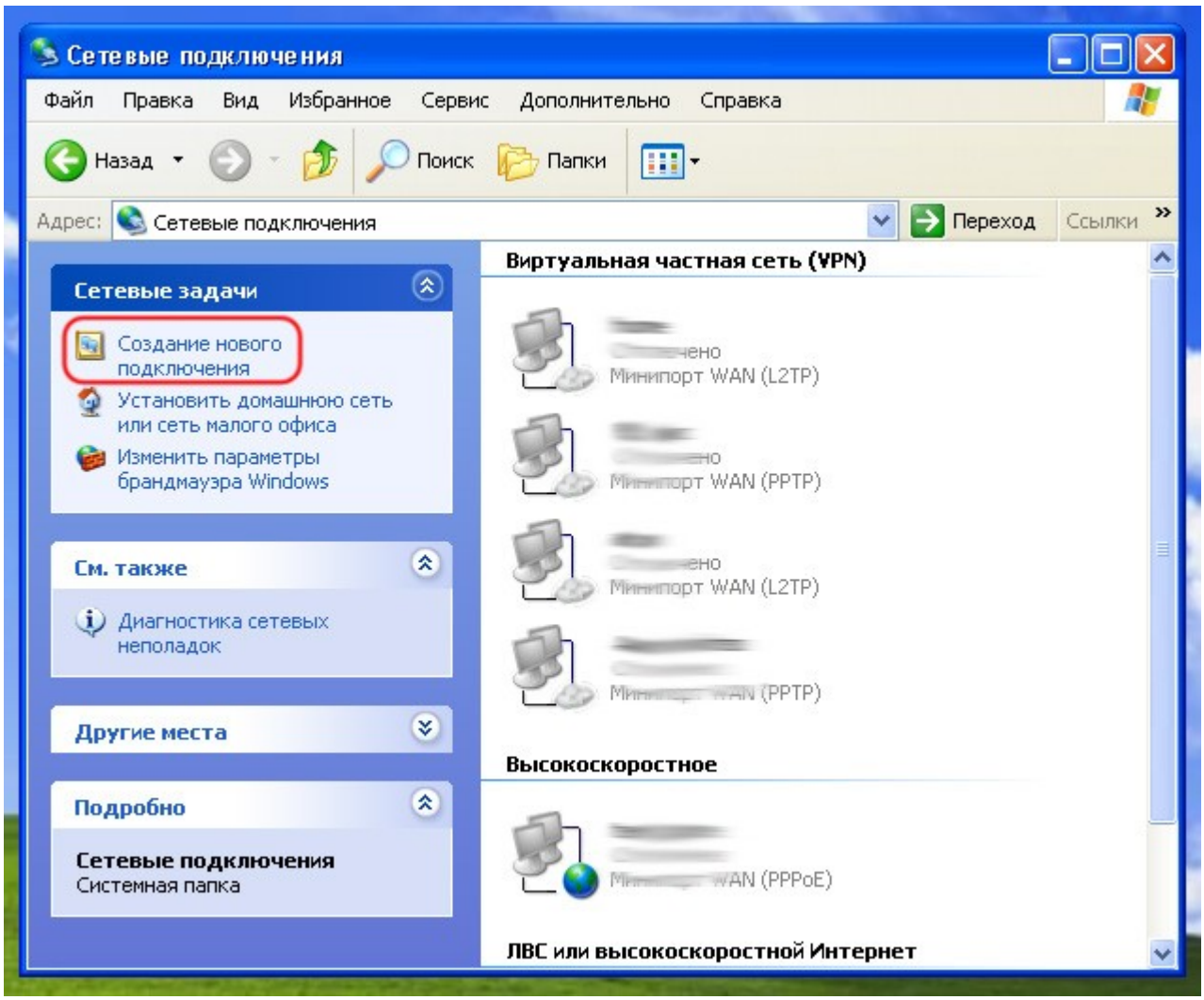


Рисунок 7.5.30.

4. В открывшемся окне выберете **Подключить к сети на рабочем месте**, и нажмите **Далее** (рис. 7.5.31).

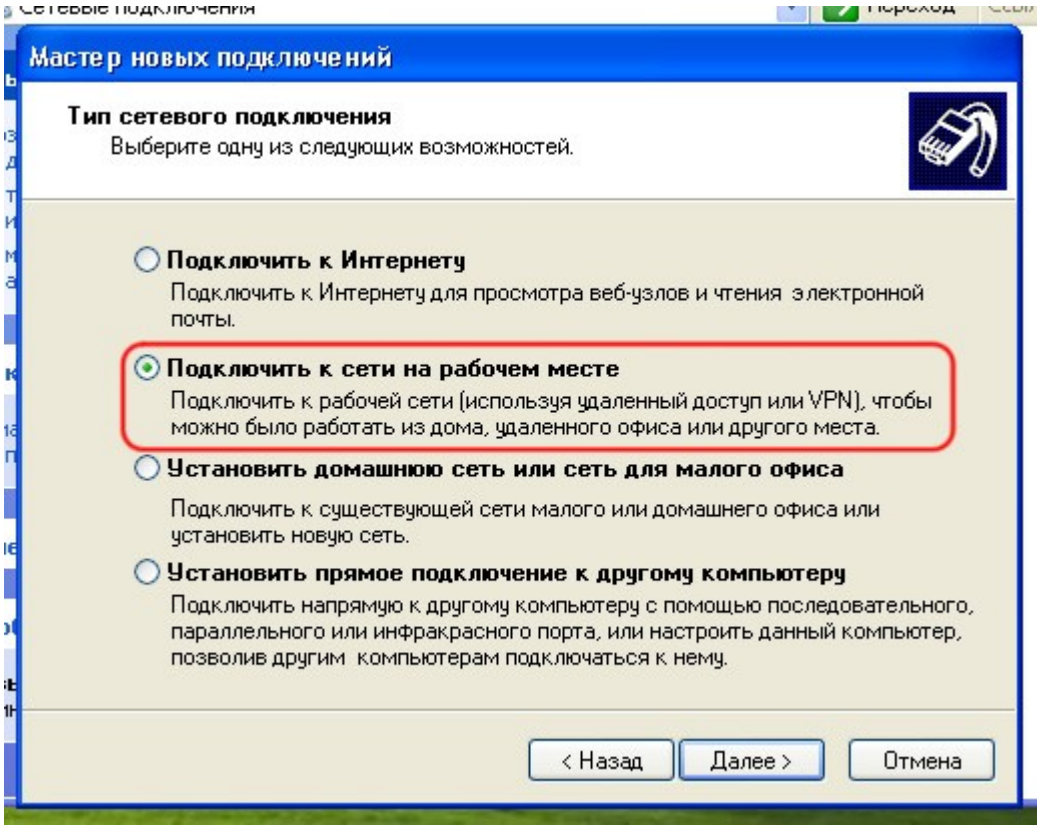


Рисунок 7.5.31.

5. Выберете **Подключение к виртуальной частной сети** и нажмите **Далее** (рис. 7.5.32).

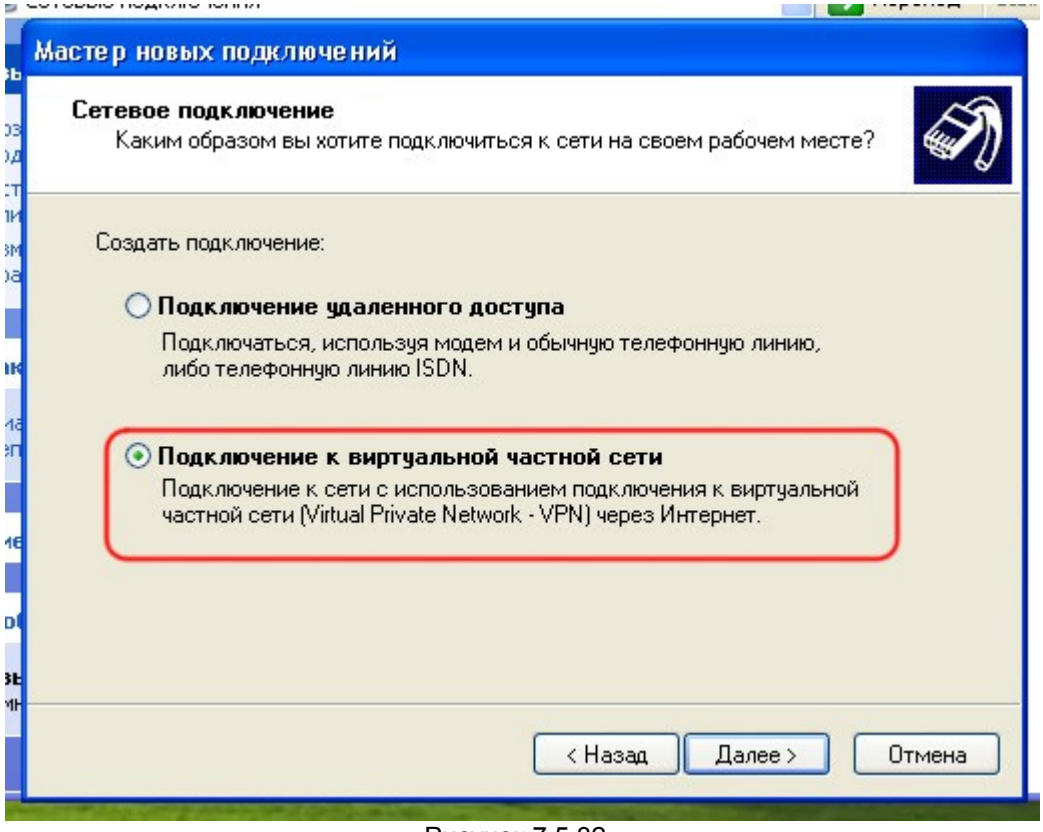


Рисунок 7.5.32.

6. В поле **Организация**, введите имя которое будет ассоциироваться с этим подключением, например

”Офис pptp” и нажмите **Далее** (рис. 7.5.33).

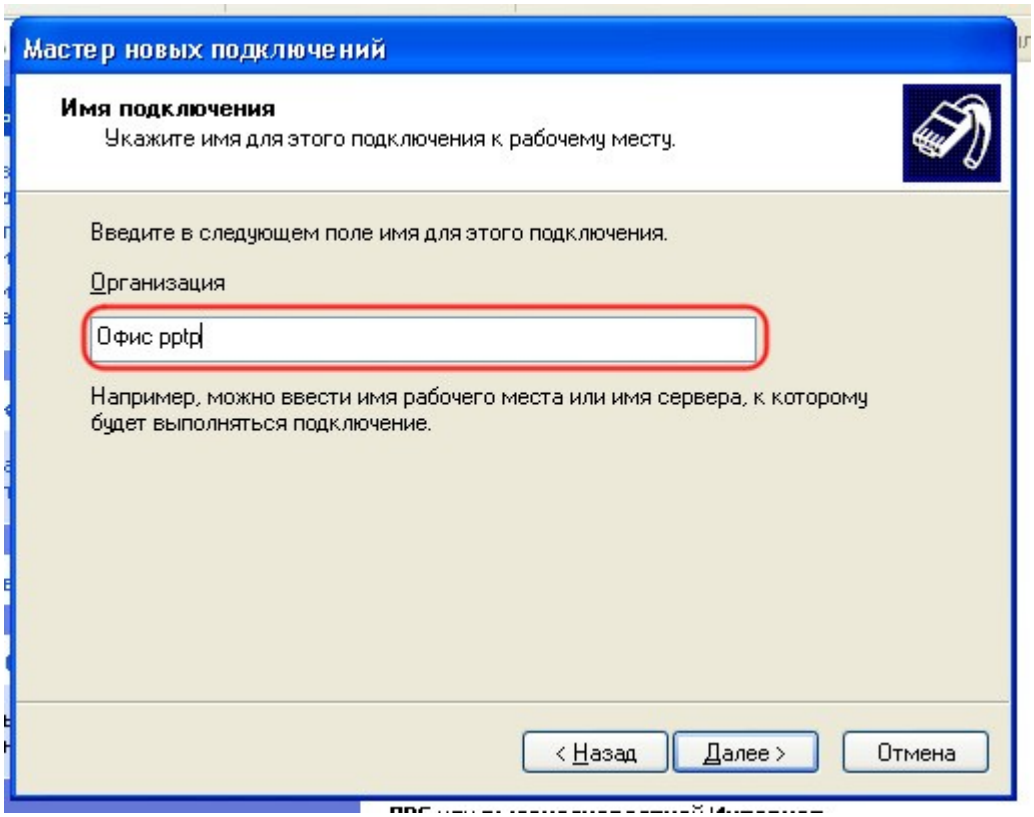


Рисунок 7.5.33.

7. Если появиться окно с предложением набора номера, выберете **Не набирать номер для предварительного подключения** и нажмите **Далее** (рис. 7.5.34).

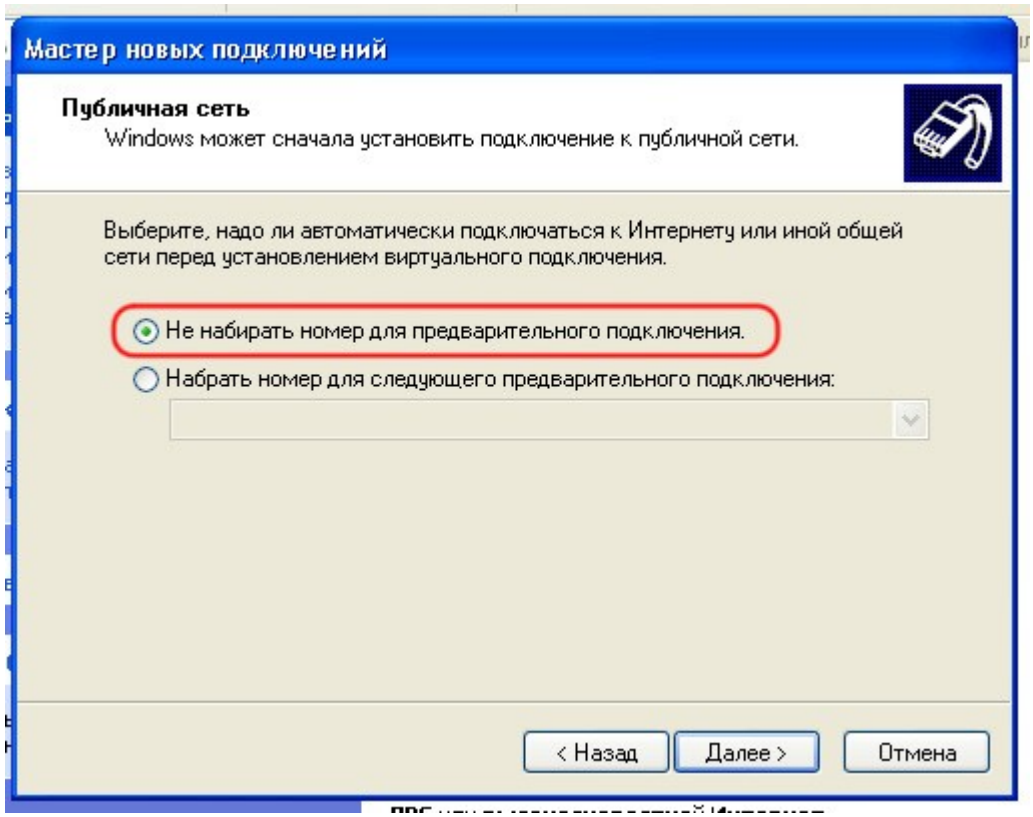


Рисунок 7.5.34.

8. В открывшемся окне заполните поле **Имя компьютера или IP-Адрес**, введя в него IP адрес Интернет адаптера сервера VPN или сетевое имя если у вас настроен сервис DDNS, если сервер работает в режиме «Маршрутизатор и VPN», либо IP адрес стороннего маршрутизатора, если сервер работает в режиме «Только VPN», нажмите **Далее** (рис. 7.5.35).

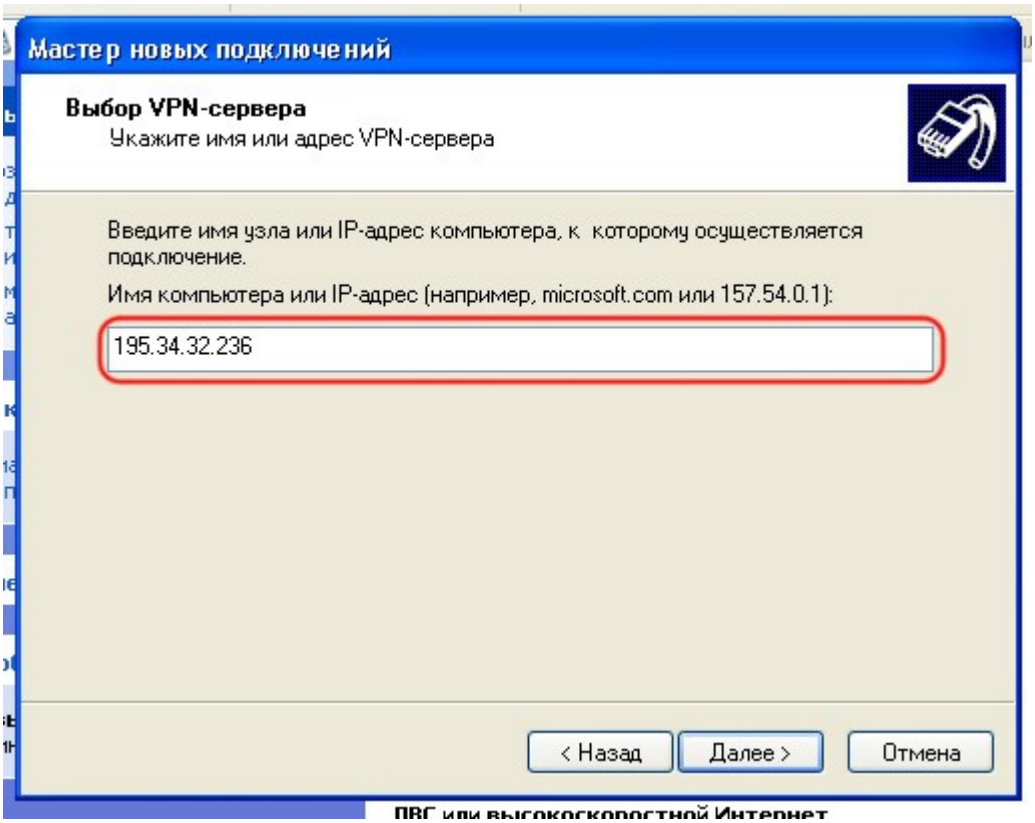


Рисунок 7.5.35.

9. Для большего удобства, во вновь открывшемся окне, рекомендуется поставить галочку напротив **Добавить ярлык подключения на рабочий стол**, нажмите **Готово**.
10. После успешного создания подключения, автоматически откроется окно с предложением подключиться. Нажмите **Свойства** (рис. 7.5.36).

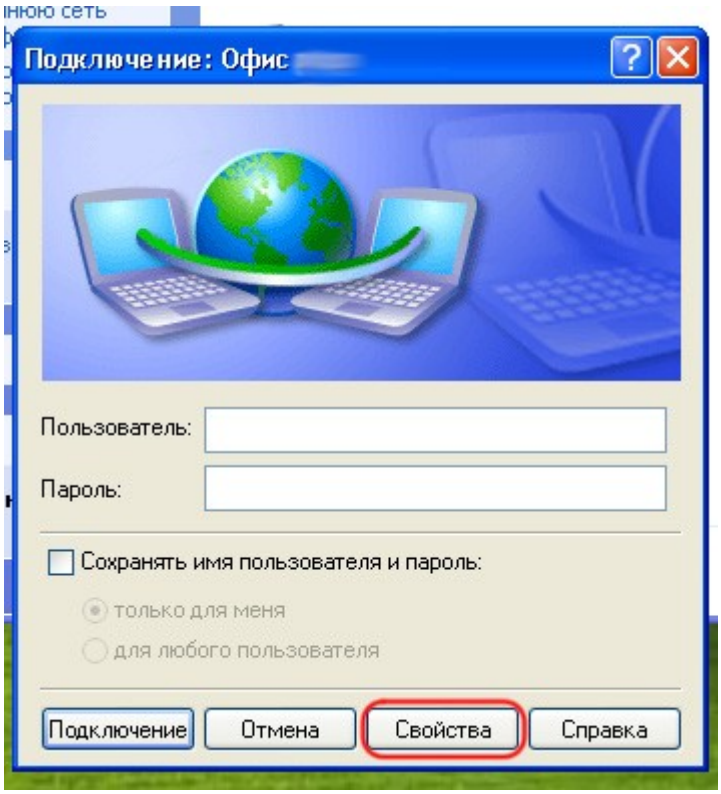


Рисунок 7.5.36.

11. Перейдите на вкладку **Безопасность**, и снимите галочку на против **Требуется шифрование данных (иначе отключаться)** (рис. 7.5.37) При этом если на сервере будет включено шифрование для протокола PPTP, то будет установлено шифрованное соединение, если отключено, то не шифрованное.

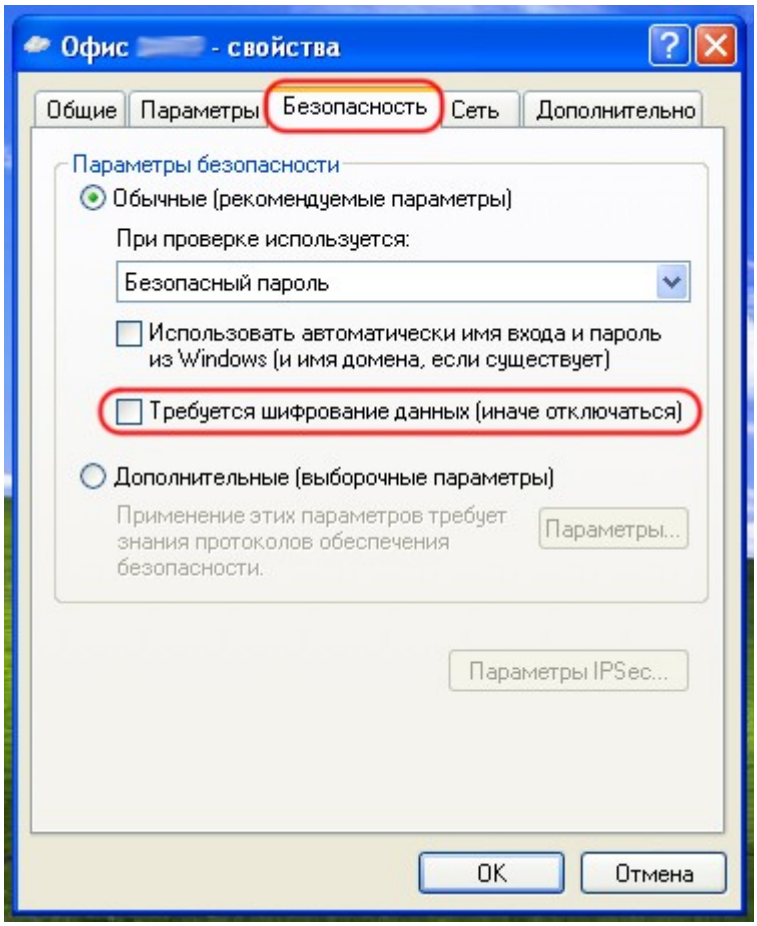


Рисунок 7.5.37.

12. Перейдите на вкладку **Сеть**, далее выберете **Тип VPN: PPTP VPN**, после чего выберете **Протокол Интернета (TCP/IP)** и нажмите **Свойства** (рис. 7.5.38).

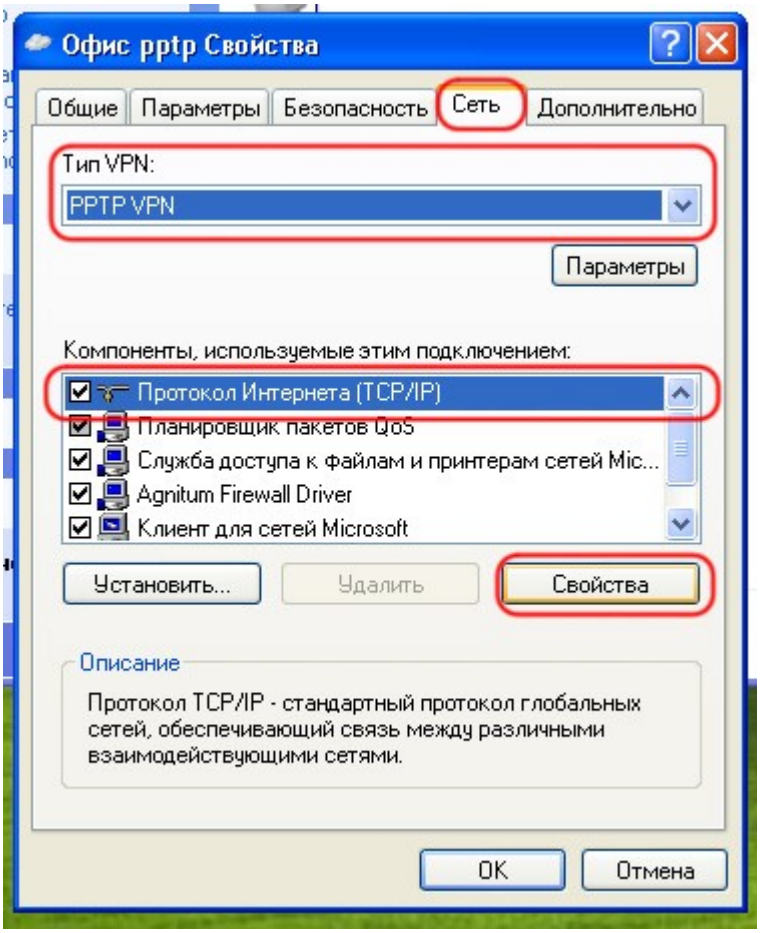


Рисунок 7.5.38.

13. В появившемся окне нажмите **Дополнительно**. Далее снимите флажок напротив **Использовать основной шлюз в удалённой сети** и нажмите **Ok**, далее **Ok** и **Ok** (рис. 7.5.39).

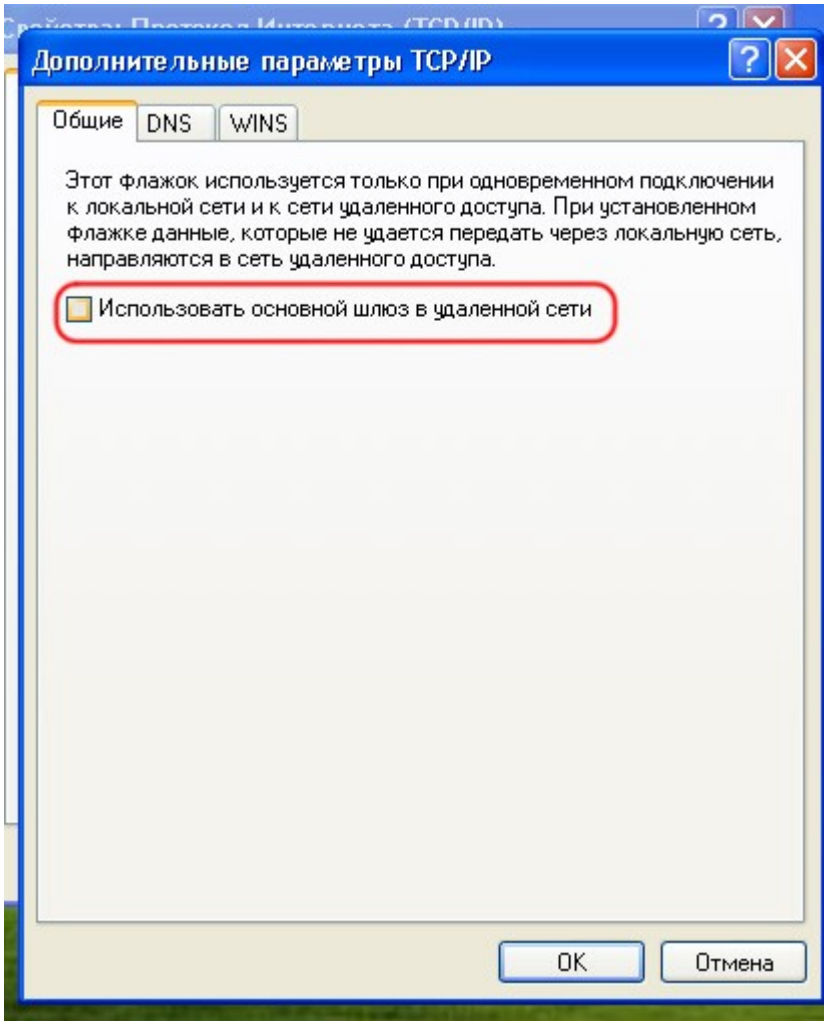


Рисунок 7.5.39.

На этом создание подключения завершено, и его можно использовать для подключения по протоколу PPTP.

7.5.5 Создание VPN подключения в Windows 2000/XP по протоколу L2TP

Прежде чем создавать новое подключение по протоколу L2TP, необходимо внести изменения в реестр. Это необходимо сделать в виду того, что Windows 2000/XP не умеют устанавливать соединение при отсутствии сертификата. Внести изменения в реестр можно двумя способами: запустив специальный патч (находиться на диске в каталоге path) (рис. 7.5.40), либо вручную изменив в реестре параметр

"ProhibitIpSec"=dword:00000001
в ветке
[HKEY_LOCAL_MACHINE\System\CurrentControlSet\Services\Rasman\Parameters]

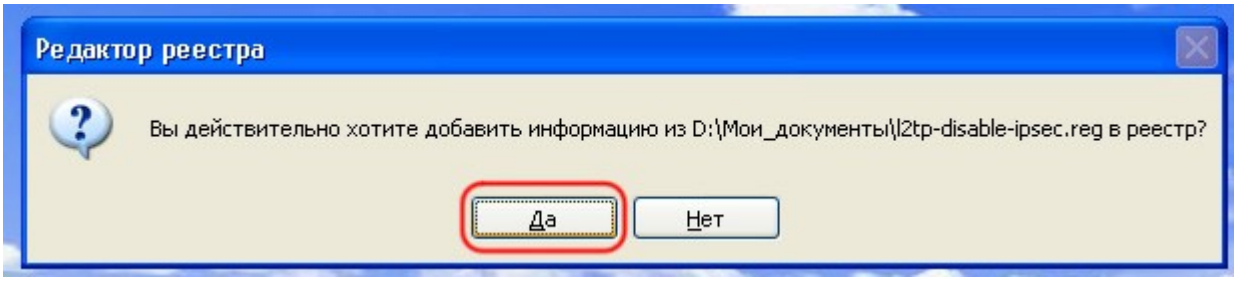


Рисунок 7.5.40.

После того как изменения внесены в реестр **ОБЯЗАТЕЛЬНО перезагрузите компьютер**, в противном случае установление соединения будет невозможно.

1. Нажмите **Пуск** и выберете **Панель управления** (рис. 7.5.41а), либо **Пуск** -> **Настройка** -> **Панель управления** (рис. 7.5.41б), в зависимости от настроек представления меню Пуск.

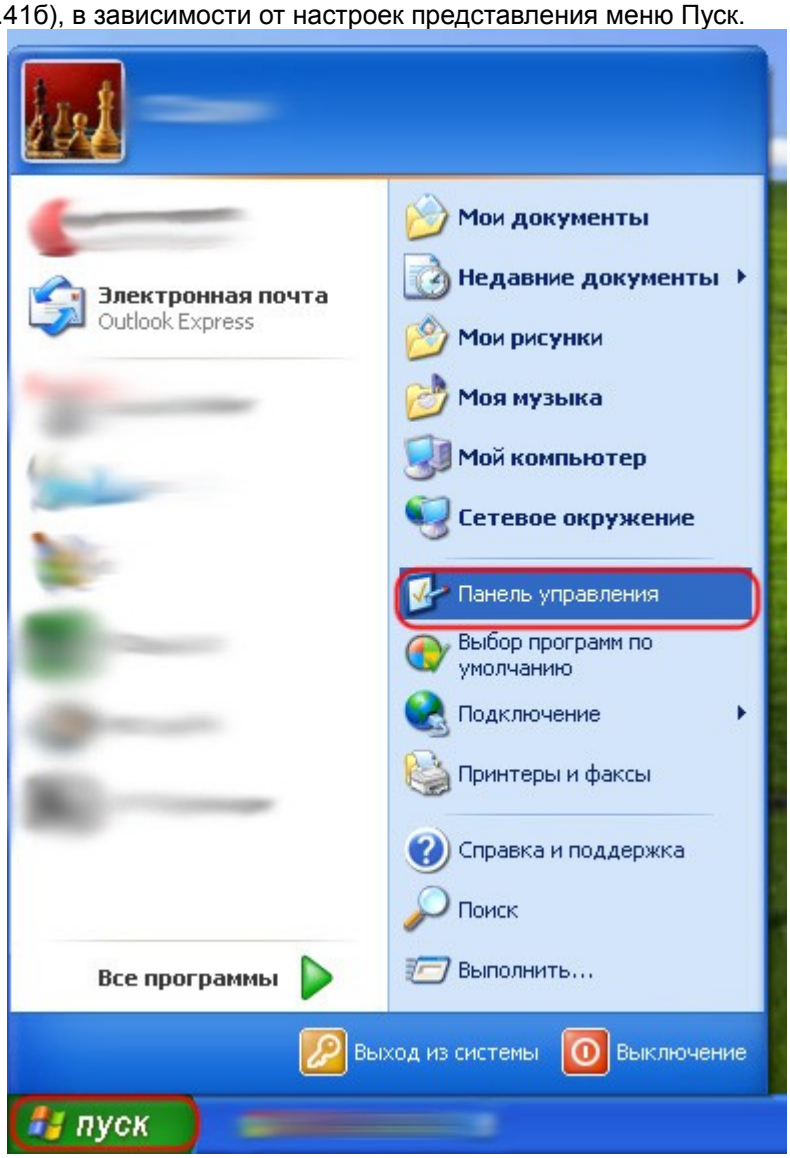


Рисунок 7.5.41а.

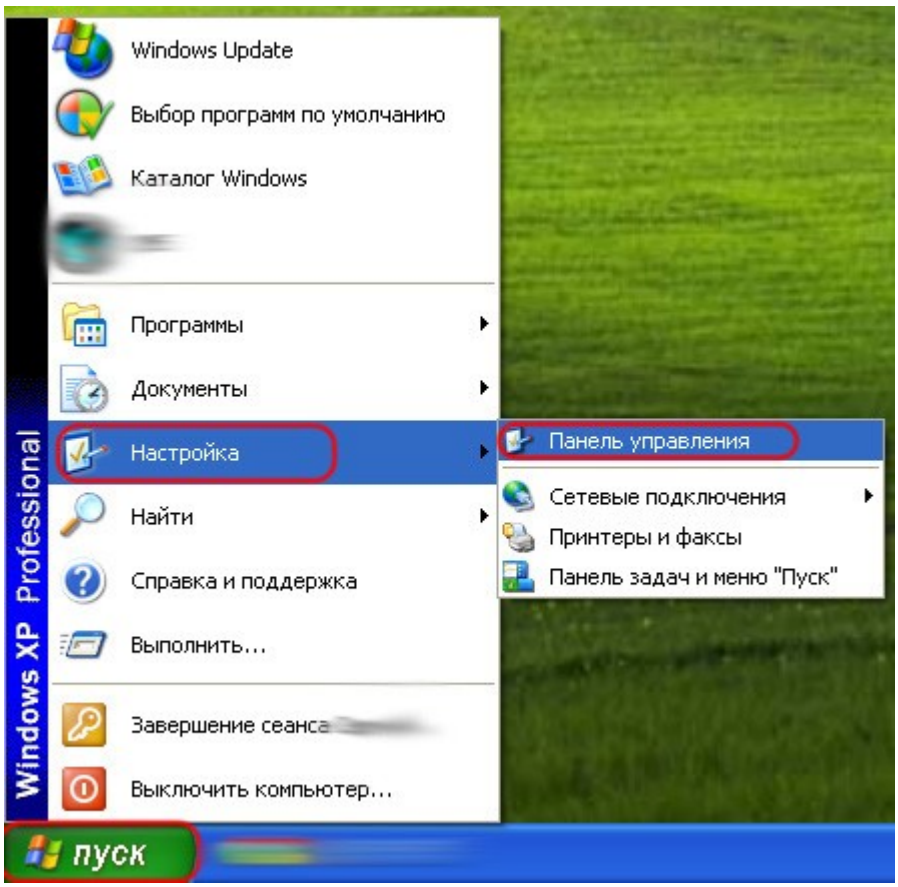


Рисунок 7.5.41б.

2. Далее, в случае необходимости, нажмите в левом верхнем углу открывшегося окна **Переключение к классическому виду**, и выберете **Сетевые подключения** (рис. 7.5.42).

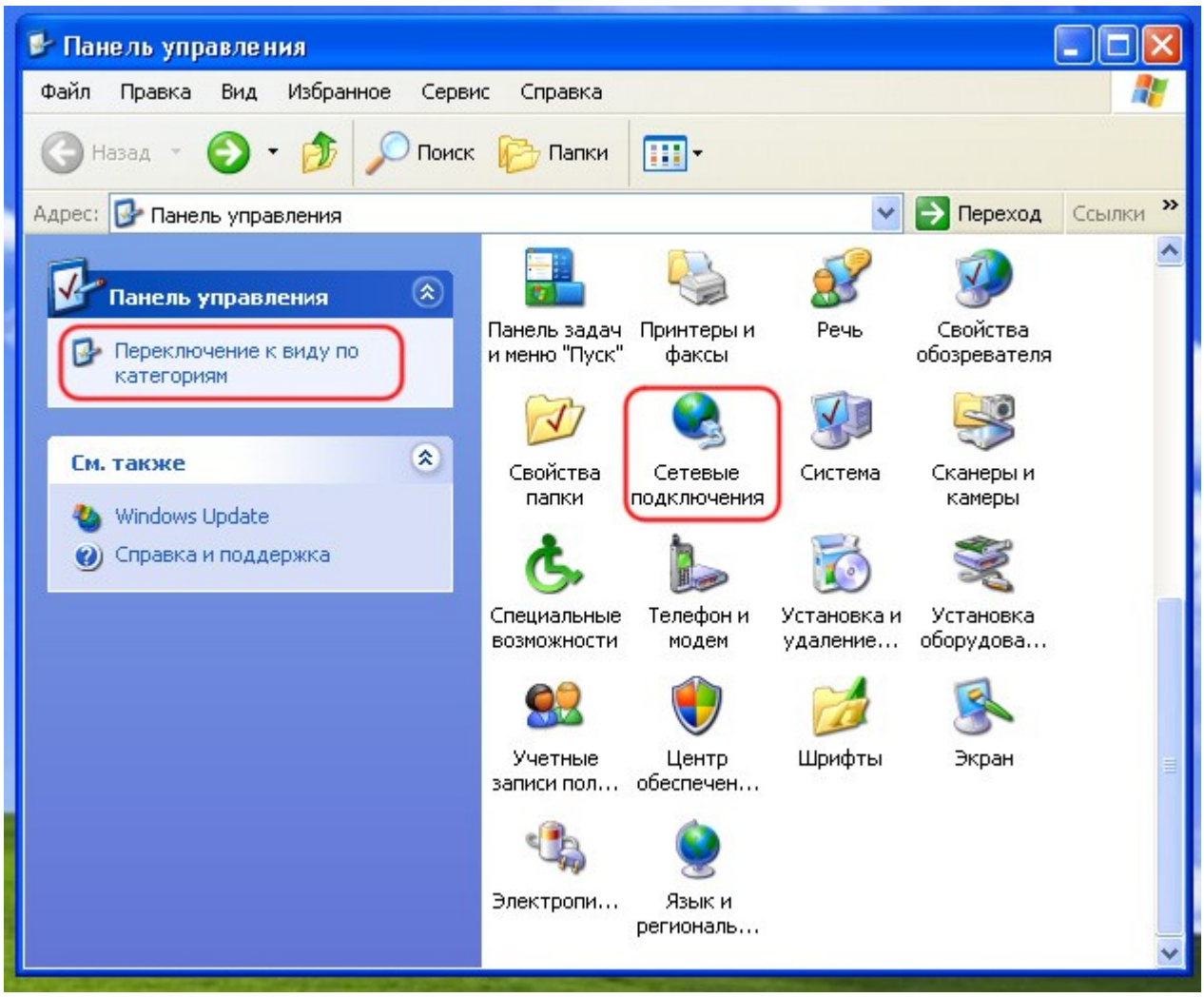


Рисунок 7.5.42.

3. Щёлкните мышкой по **Создание нового подключения**, и в появившемся окне нажмите **Далее** (рис. 7.5.43).

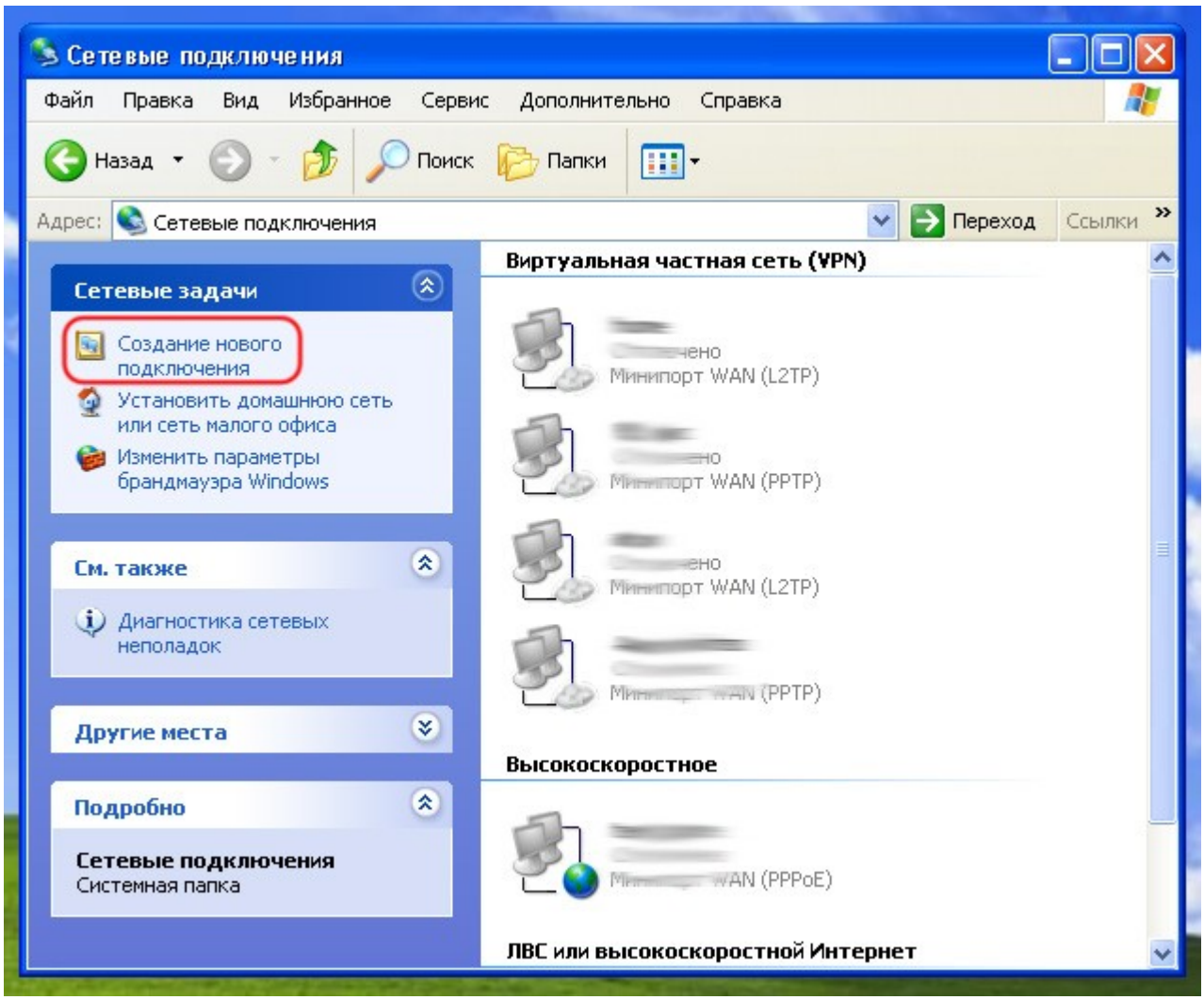


Рисунок 7.5.43.

4. В открывшемся окне выберете **Подключить к сети на рабочем месте**, и нажмите **Далее** (рис. 7.5.44).

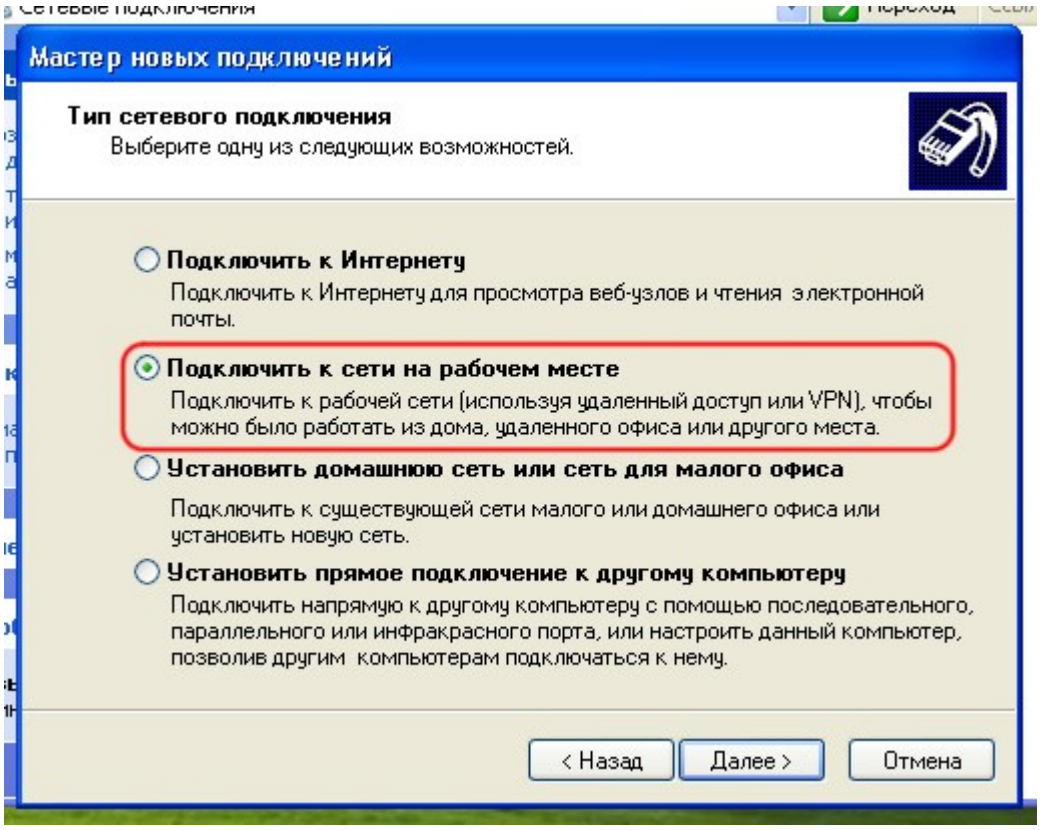


Рисунок 7.5.44.

5. Выберете **Подключение к виртуальной частной сети** и нажмите **Далее** (рис. 7.5.45).

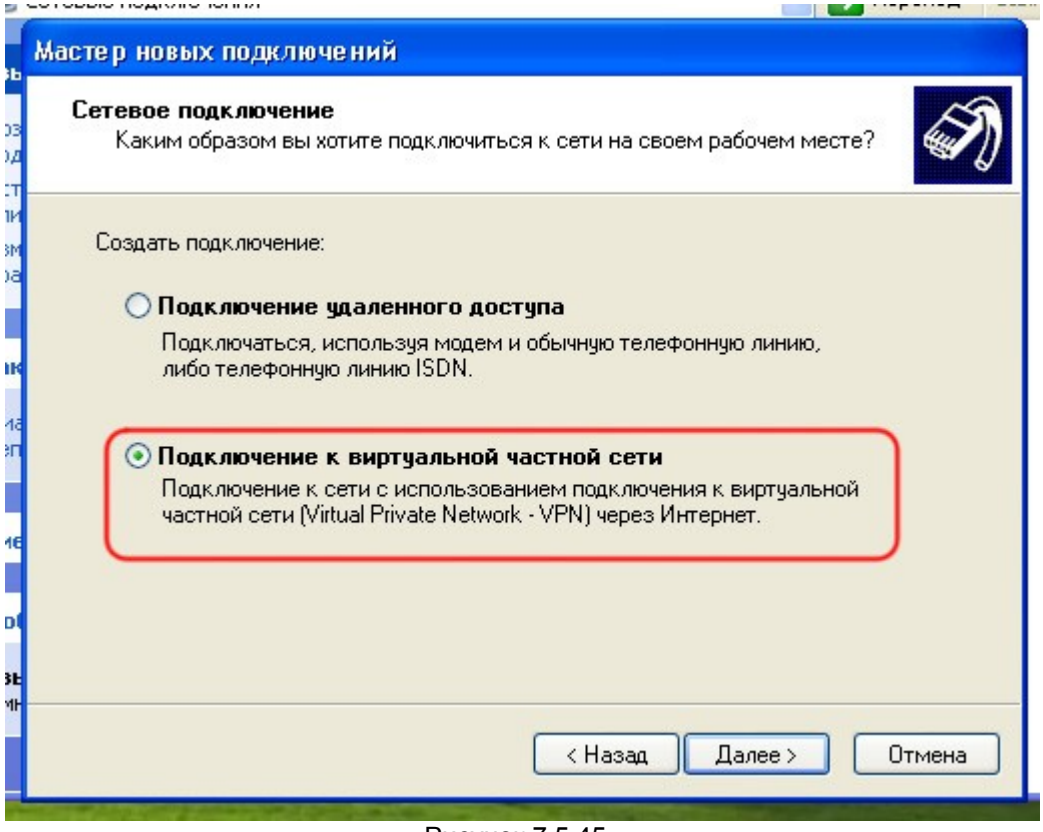


Рисунок 7.5.45.

6. В поле **Организация**, введите имя которое будет ассоциироваться с этим подключением, например

”Офис l2tp” и нажмите **Далее** (рис. 7.5.46).

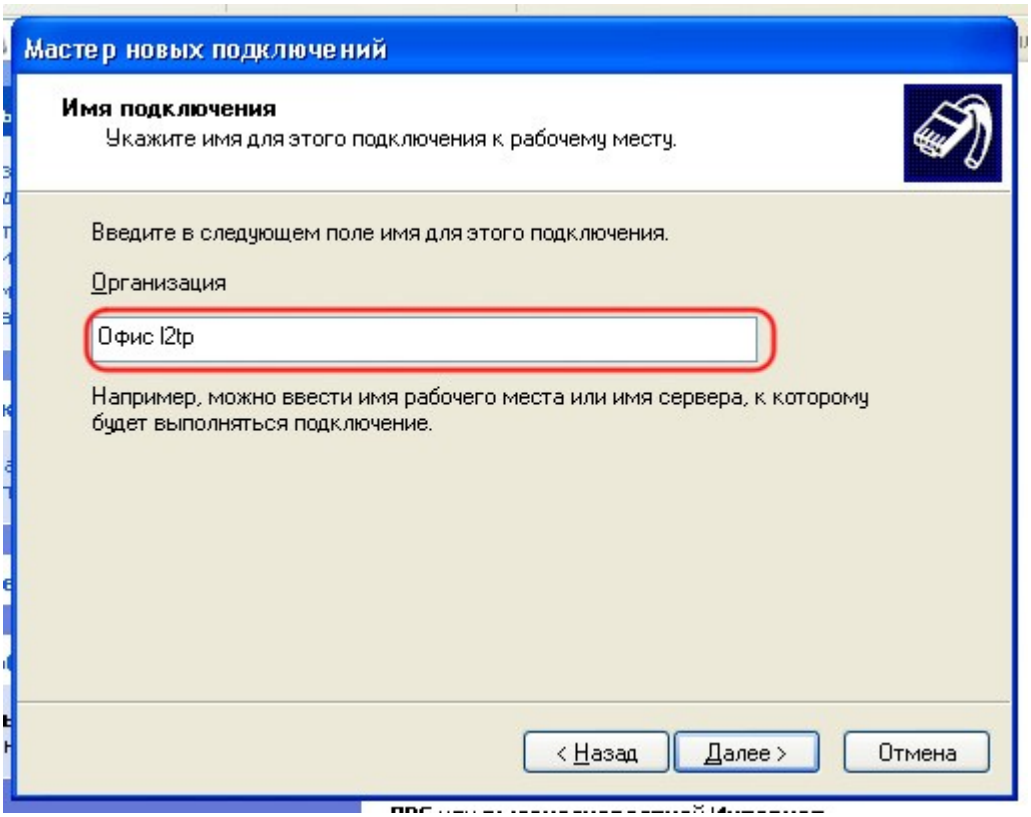


Рисунок 7.5.46.

7. Если появиться окно с предложением набора номера, выберете **Не набирать номер для предварительного подключения** и нажмите **Далее** (рис. 7.5.47).

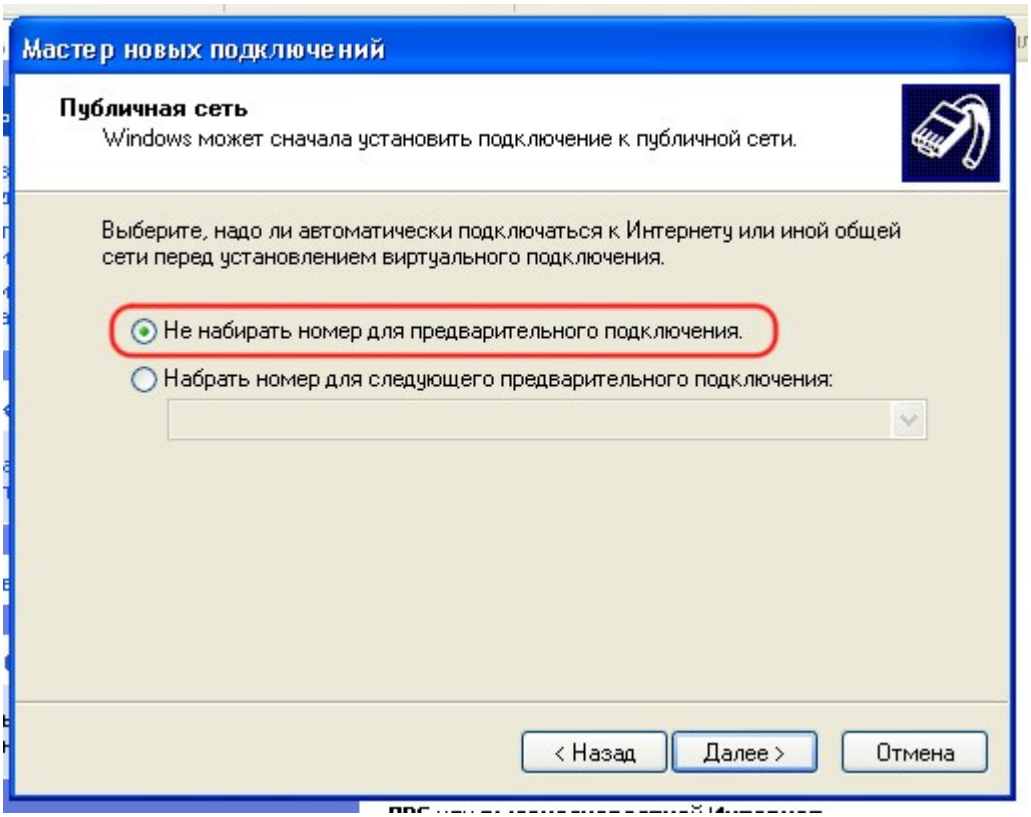


Рисунок 7.5.47.

8. В открывшемся окне заполните поле **Имя компьютера или IP-Адрес**, введя в него IP адрес Интернет адаптера сервера VPN или сетевое имя если у вас настроен сервис DDNS, если сервер работает в режиме «Маршрутизатор и VPN», либо IP адрес стороннего маршрутизатора, если сервер работает в режиме «Только VPN», нажмите **Далее** (рис. 7.5.48).

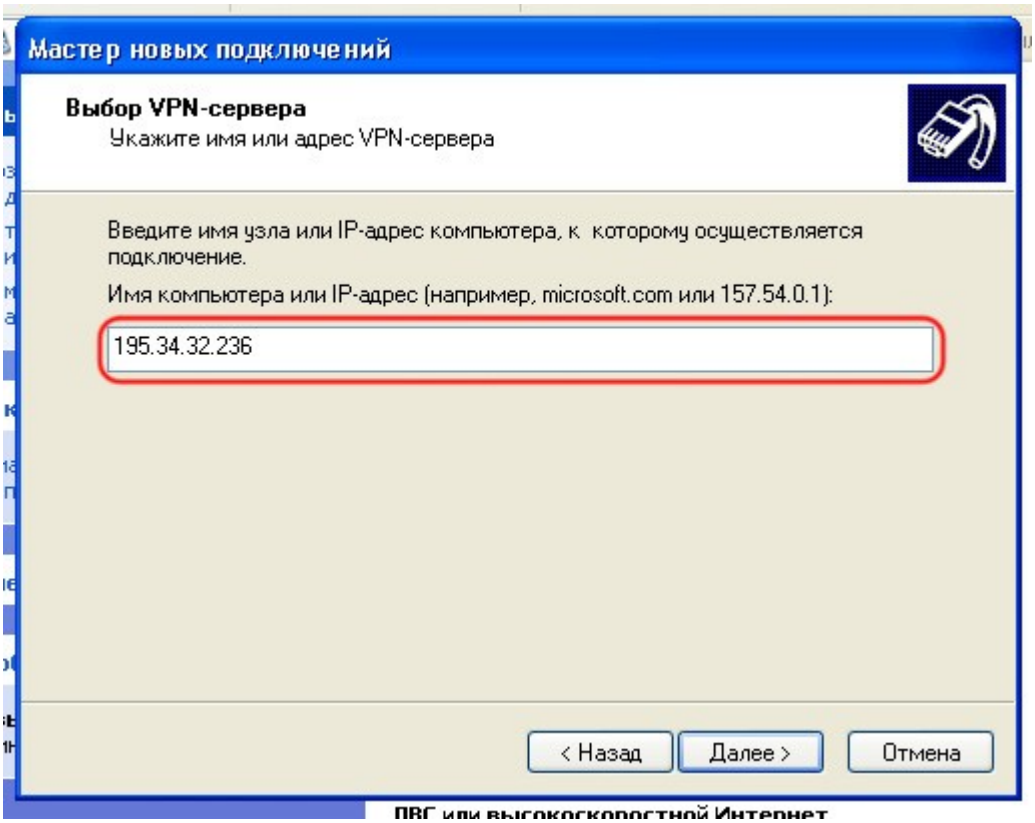


Рисунок 7.5.48.

9. Для большего удобства, во вновь открывшемся окне, рекомендуется поставить галочку напротив **Добавить ярлык подключения на рабочий стол**, нажмите **Готово**.

10. После успешного создания подключения, автоматически откроется окно с предложением подключиться. Нажмите **Свойства** (рис. 7.5.49).

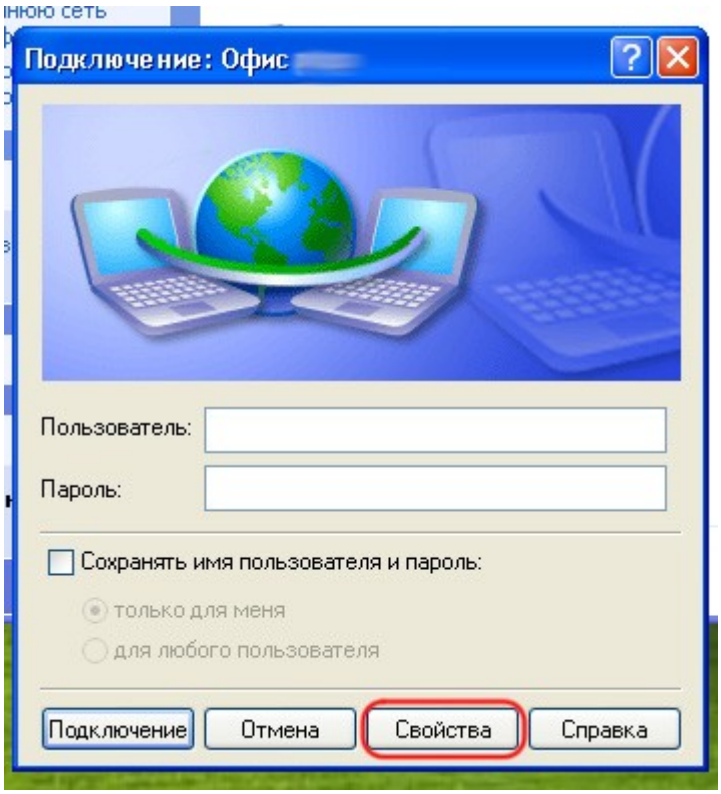


Рисунок 7.5.49.

11. Перейдите на вкладку **Безопасность**, и снимите галочку на против **Требуется шифрование данных (иначе отключаться)** (рис. 7.5.50) При этом если на сервере будет включено шифрование для протокола L2TP, то будет установлено шифрованное соединение, если отключено, то не шифрованное.

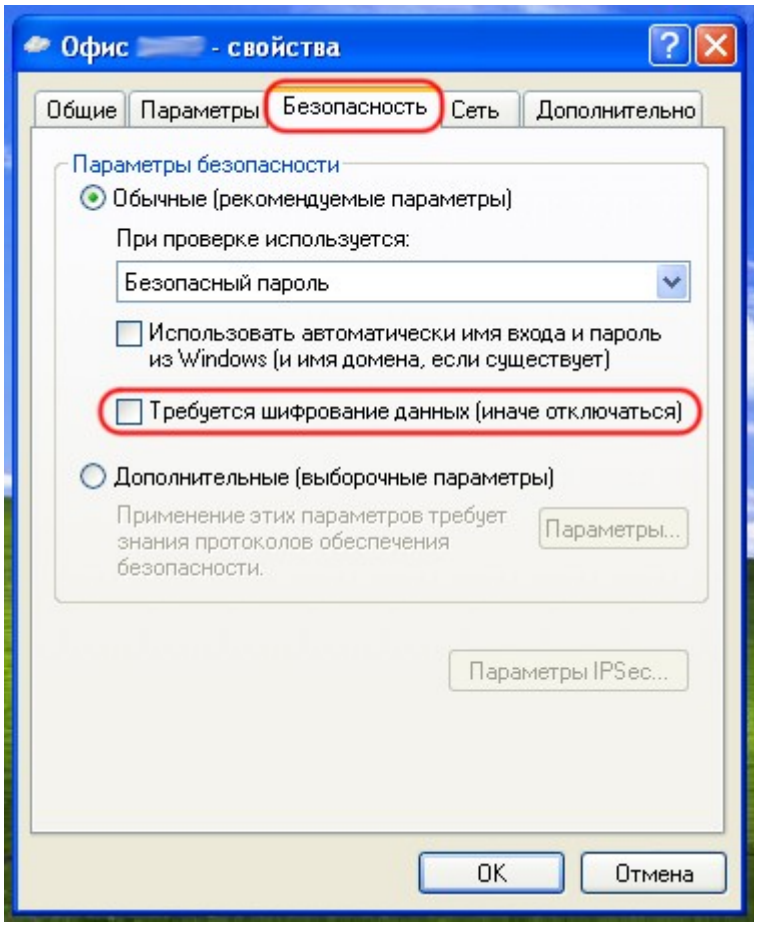


Рисунок 7.5.50.

12. Перейдите на вкладку **Сеть**, далее выберете **Тип VPN: L2TP IPSec VPN**, после чего выберете **Протокол Интернета (TCP/IP)** и нажмите **Свойства** (рис. 7.5.51).

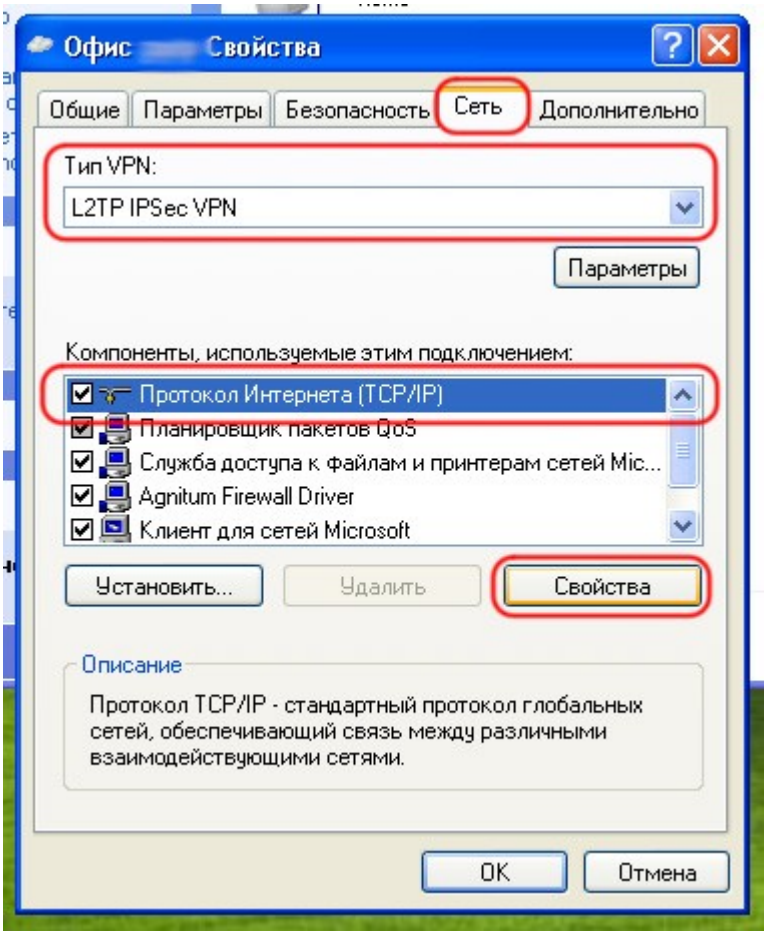


Рисунок 7.5.51.

13. В появившемся окне нажмите **Дополнительно**. Далее снимите флажок напротив **Использовать основной шлюз в удалённой сети** и нажмите **Ok**, далее **Ok** и **Ok** (рис. 7.5.52).

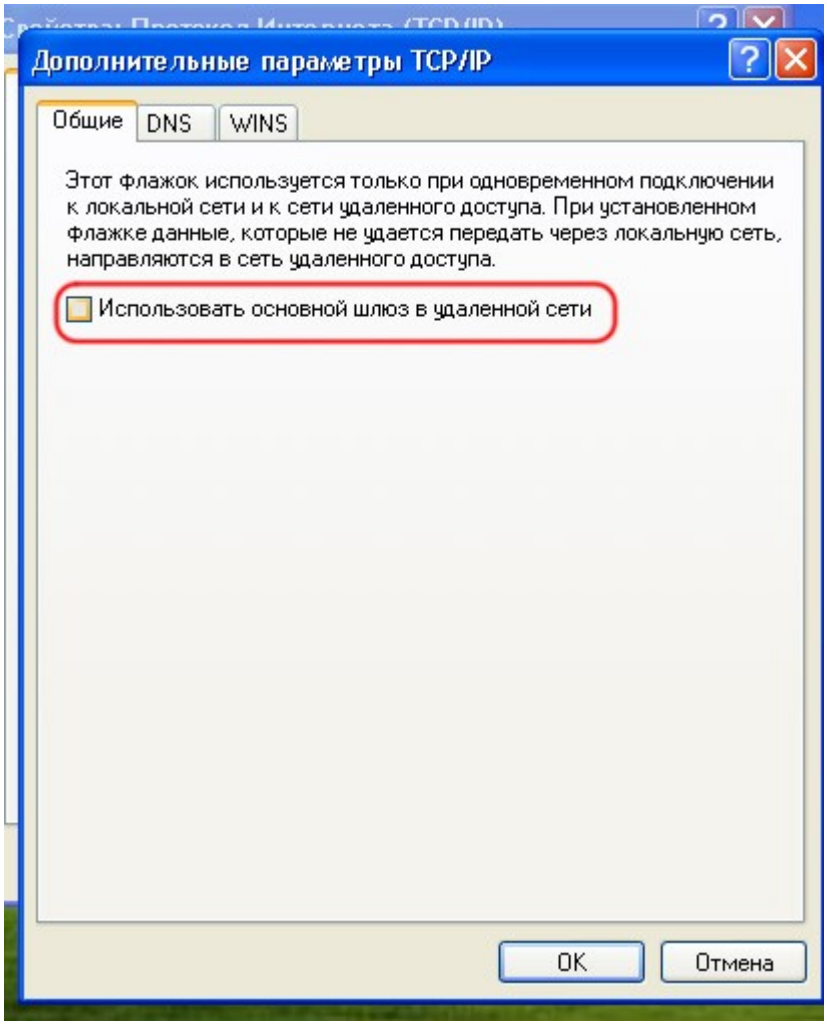


Рисунок 7.5.52.

На этом создание подключения завершено, и его можно использовать для подключения по протоколу L2TP.

7.5.6 Подключение и отключение в Windows 2000/XP

Подключение

1. Нажмите **Пуск** и выберете **Подключение** (рис. 7.5.53а), либо **Пуск** -> **Настройка** -> **Сетевые подключения** (рис. 7.5.53б), в зависимости от настроек представления меню Пуск, выберете из списка необходимое подключение.
Также вы можете воспользоваться соответствующим ярлыком на рабочем столе, если вы сделали его в процессе создания подключения.

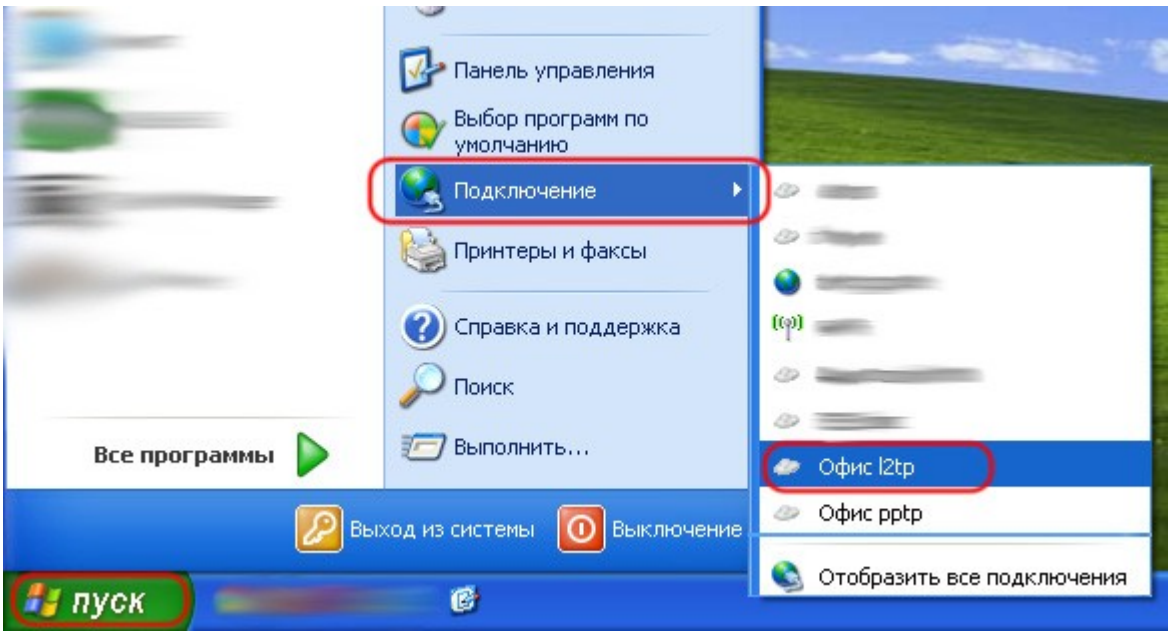


Рисунок 7.5.53а.

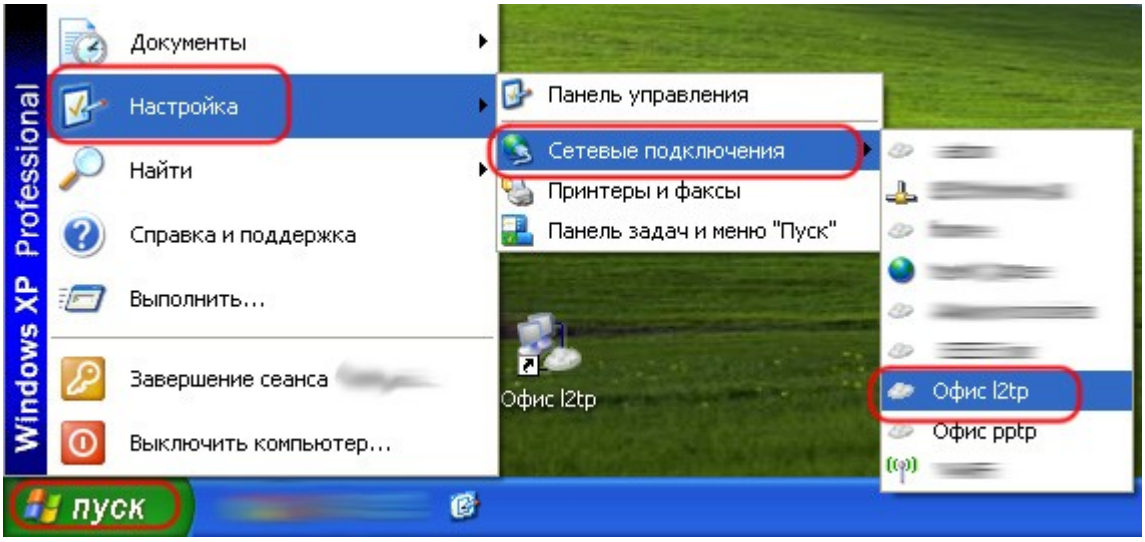


Рисунок 7.5.53б.

2. В появившемся окне заполните соответствующие поля, после чего нажмите **Подключение** (рис. 7.5.54). Будьте внимательны при заполнении, заглавные и строчные символы различаются, также удостоверьтесь что активна англоязычная раскладка. В целях обеспечения большей безопасности не рекомендуется использовать автоматическое запоминание пароля.

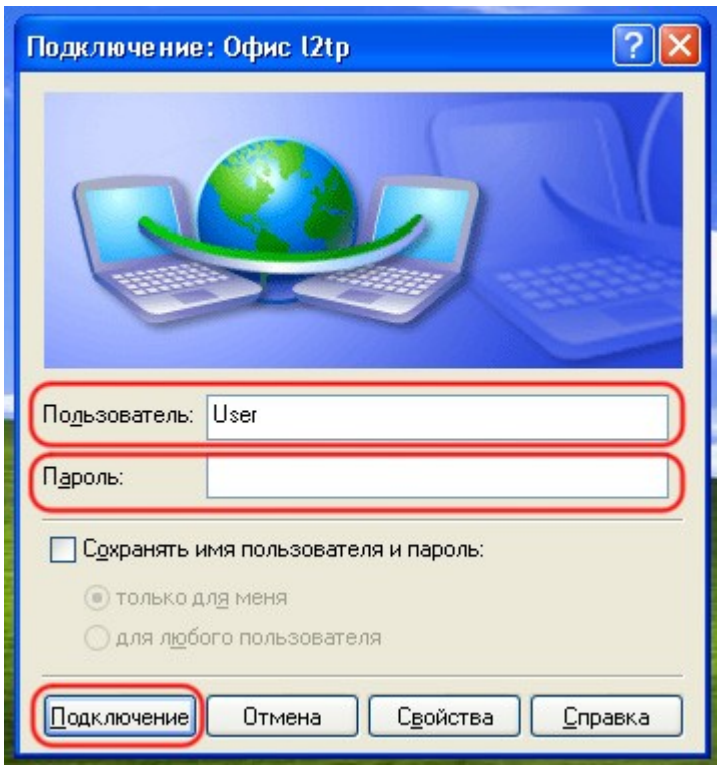


Рисунок 7.5.54.

В ответ на это вы увидите процесс соединения (рис. 7.5.55).

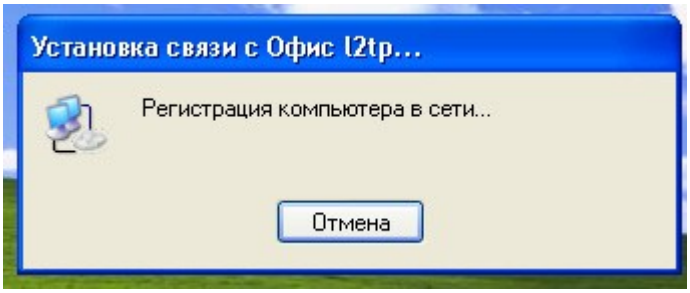


Рисунок 7.5.55.

Теперь вы подключены к внутренний сети, и можете пользоваться всеми её внутренними ресурсами, так если бы вы были подключены локально.
После того как вы выполните все необходимые вам действия обязательно выполните процесс отключения.

Отключение

1. Справа внизу, рядом с часами, поднесите мышку к одному из сетевых подключений, в ответ на это вы увидите всплывающую подсказку в которой будет указано имя подключения (рис. 7.5.56). Таким образом вы сможете найти из нескольких подключений необходимое.

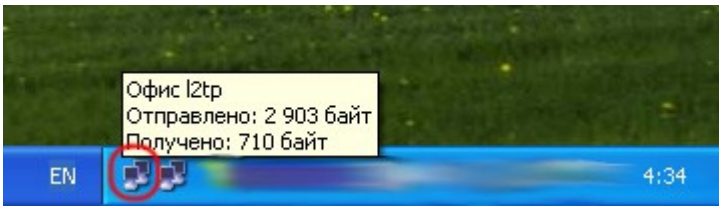


Рисунок 7.5.56.

После того как вы нашли необходимое подключение, щёлкните на нём правой клавишей мыши и выберете **Разъединить** (рис. 7.5.57).

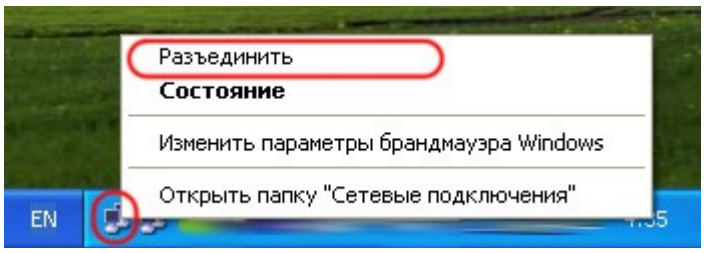


Рисунок 7.5.57.