Удаленный доступ к ресурсам корпоративной сети БИН РАН

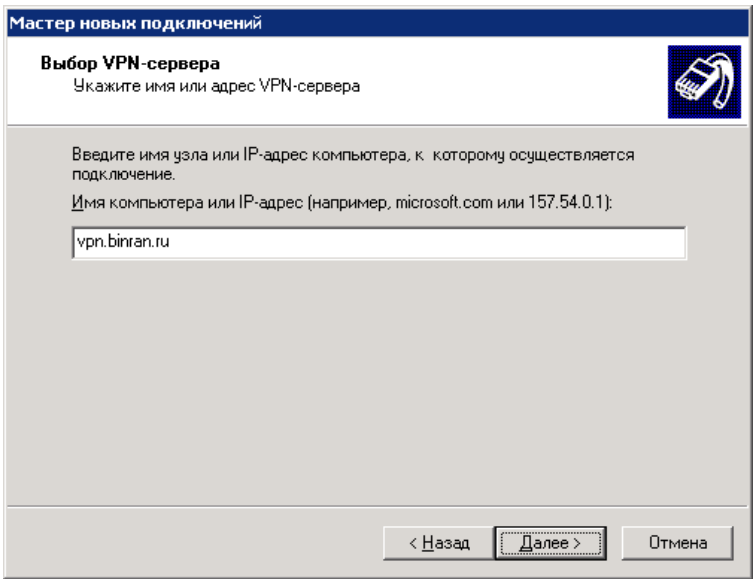
Внутренние ресурсы корпоративной сети (серверы и рабочие станции) надежно изолированы от несанкционированного доступа извне. Вместе с тем, возможность удаленного доступа к внутренним ресурсам может быть чрезвычайно полезна для пользователей в самых разных ситуациях. Для обеспечения безопасного удаленного доступа внутрь корпоративной сети используется технология **VPN** (**Virtual Private Network** — виртуальная частная сеть) на основе протокола **PPTP** (**Point-to-Point Tunneling Protocol** — туннельный протокол типа точка-точка).

В самом общем виде VPN — это совокупность способов обеспечения защищенного канала связи за счет создания специального туннеля в стандартной, незащищенной сети Интернет. Обращаем особое внимание, что поддержка протокола PPTP провайдерами сети Интернет нередко входит лишь в дополнительный пакет услуг или же требует специальной настройки вашего оборудования (кабельные модемы, маршрутизаторы и пр.). Кроме того, во многих организациях протокол PPTP закрыт на уровне прокси-сервера, через который осуществляется доступ с рабочих компьютеров в Интернет.

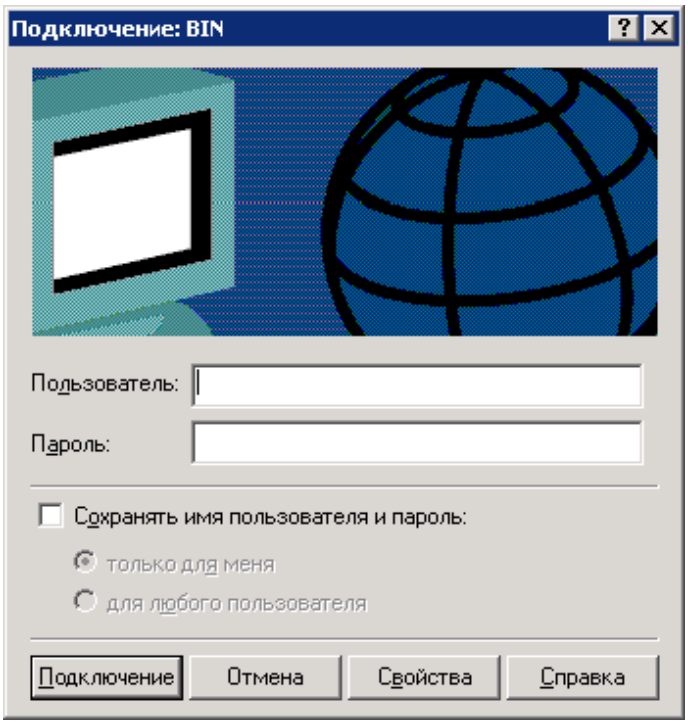
Если вы не можете получить доступ в сеть БИН РАН после выполнения всех шагов настоящего руководства — это однозначно указывает на то, что протокол PPTP закрыт вашим провайдером/ работодателем или требуется перенастройка используемого вами сетевого оборудования.

Порядок настройки VPN-соединения на компьютере под управлением Windows XP

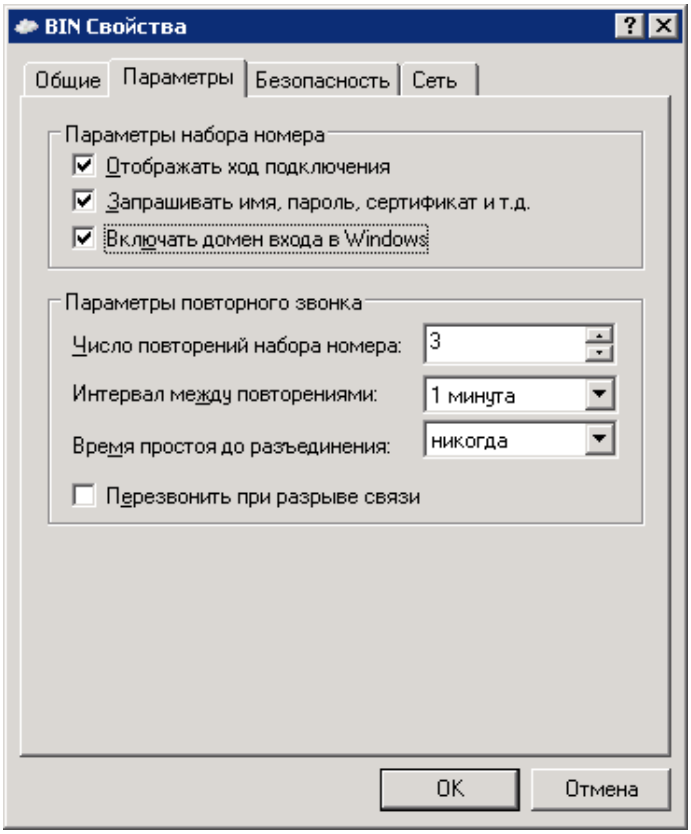
- Откройте **«Сетевые подключения»** через меню Windows:
  Пуск → Настройка → Панель управления → Сетевые подключения;
- Запустите **«Мастер новых подключений»** через меню: Файл → Новое подключение..., нажмите **«Далее»**;
- В окне выбора типа сетевого подключения укажите **«Подключить к сети на рабочем месте»**, на следующем этапе мастера — выберите **«Подключение к виртуальной частной сети»**;
- В окне указания имени подключения введите удобное вам имя, например, **BIN**, нажмите **«Далее»**;
- В окне установки подключения к публичной сети выберите **«Не набирать номер для предварительного подключения»**, нажмите **«Далее»**;
- В окне выбора VPN-сервера укажите **vpn.binran.ru** и нажмите **«Далее»**:

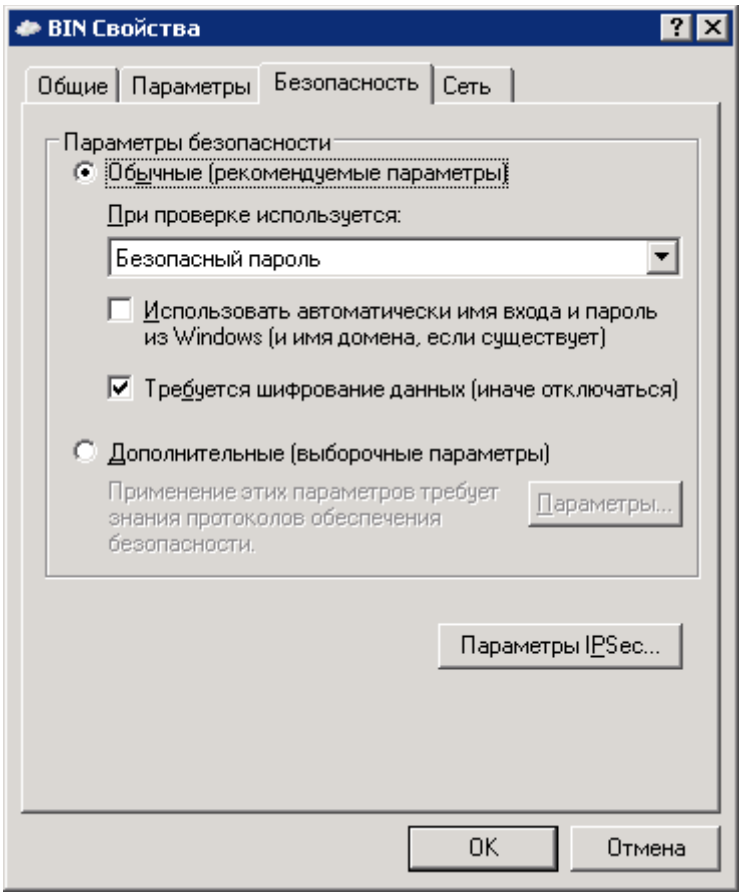


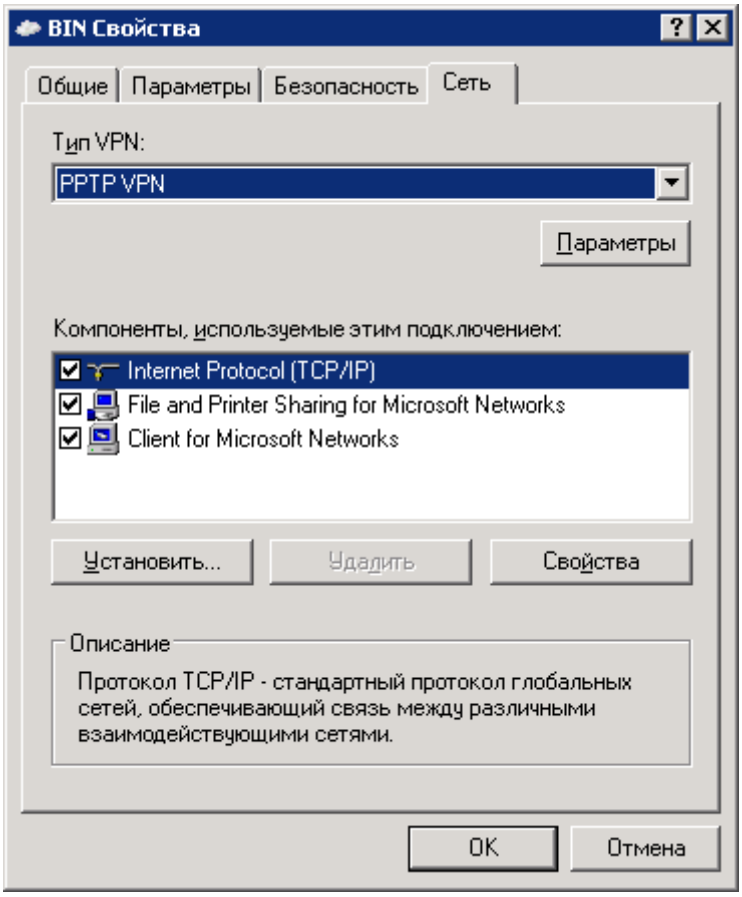
- В окне выбора доступности подключения выберите удобный вам вариант доступности нового подключения, нажмите «**Далее**»;
- Для завершения мастера новых подключений нажмите «**Готово**»;
- В открывшемся окне подключения к сети нажмите «**Свойства**»:



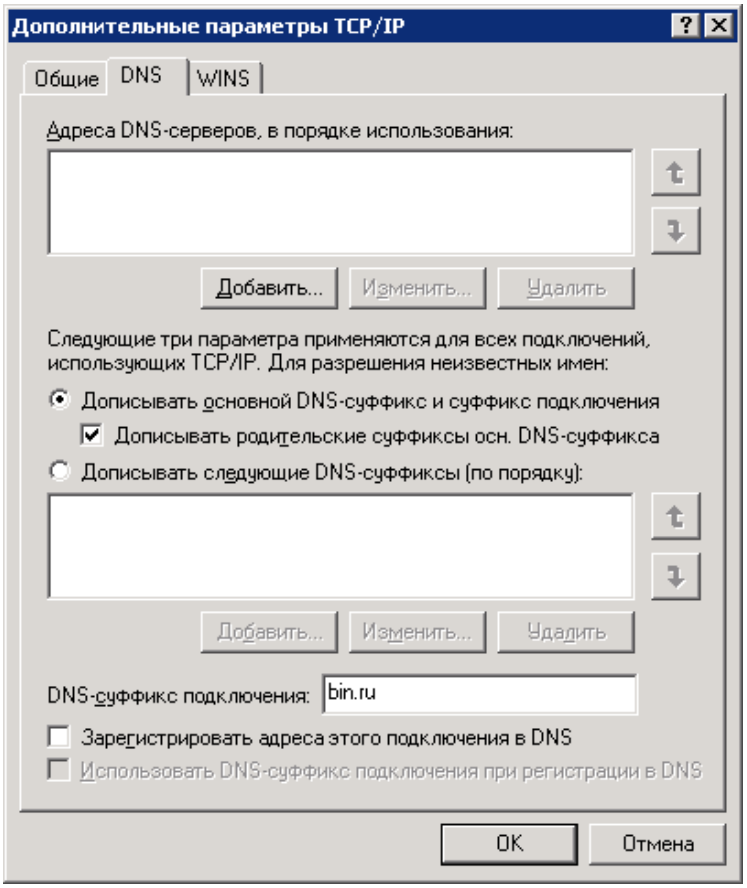
- Настройте свойства VPN-соединения как показано ниже:



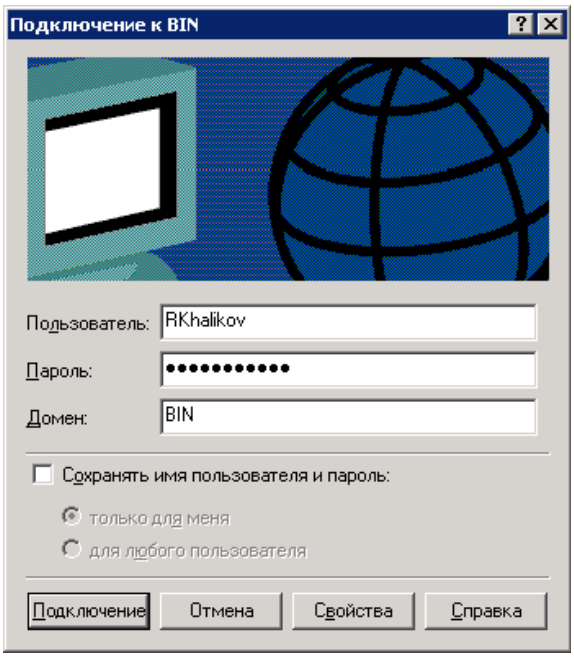

BIN Свойства
Общие
Параметры
Безопасность
Сеть
Параметры безопасности
Обычные (рекомендуемые параметры)
При проверке используется:
Безопасный пароль
Использовать автоматически имя входа и пароль из Windows (и имя домена, если существует)
Требуется шифрование данных (иначе отключаться)
Дополнительные (выборочные параметры)
Применение этих параметров требует знания протоколов обеспечения безопасности.
Параметры...
Параметры IPSec...
OK
Отмена


BIN Свойства
Общие
Параметры
Безопасность
Сеть
Тип VPN:
PPTP VPN
Параметры
Компоненты, используемые этим подключением:
Internet Protocol (TCP/IP)
File and Printer Sharing for Microsoft Networks
Client for Microsoft Networks
Установить...
Удалить
Свойства
Описание
Протокол TCP/IP - стандартный протокол глобальных сетей, обеспечивающий связь между различными взаимодействующими сетями.
OK
Отмена

- На закладке Сеть выберите «**Протокол интернета (TCP/IP)**» и нажмите «**Свойства**»;
- В открывшемся окне нажмите «**Дополнительно...**» и в следующем окне на закладке DNS укажите DNS-суффикс подключения **bin.ru** как показано ниже:



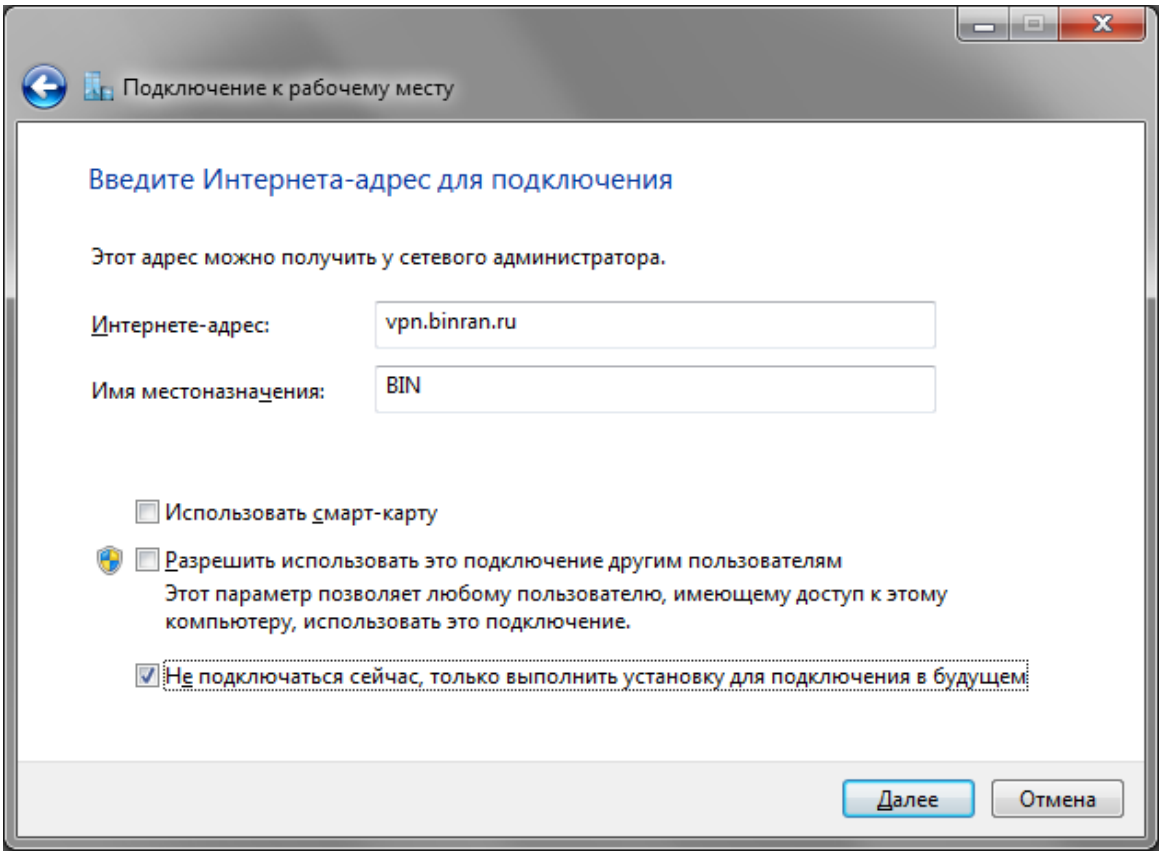
- Сохраните настройки, последовательно нажимая «**ОК**» и закрывая окна, пока не появится окно подключения VPN-соединения;
- В окне подключения введите данные вашей персональной учетной записи пользователя в сети БИН РАН как показано ниже:



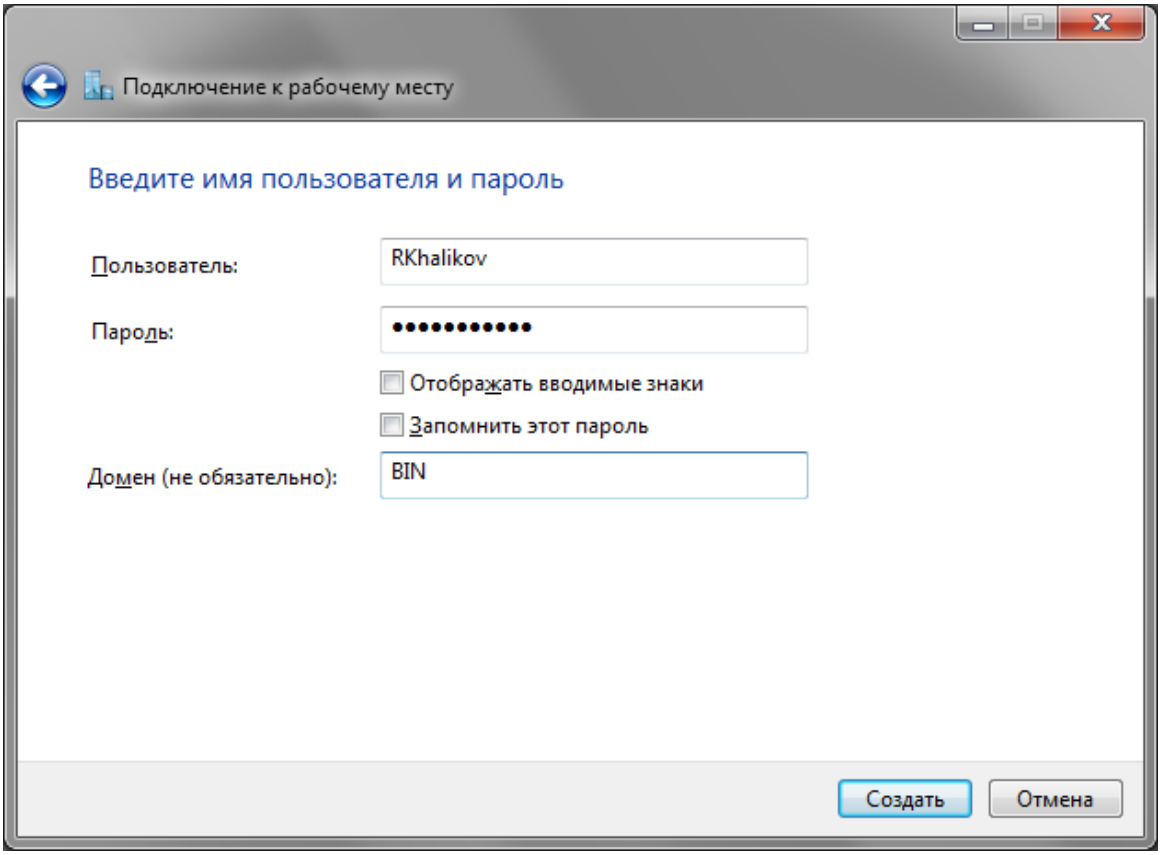
- Включать опцию «**Сохранять имя пользователя и пароль**» рекомендуется только в том случае, если вы устанавливаете VPN-соединение со своего личного компьютера (домашний компьютер, ноутбук во время командировки и пр.), а не используете чужой служебный компьютер или рабочую станцию в публичной точке доступа.
  Помните, что аккуратное использование собственной учетной записи пользователя — единственная гарантия сохранности ваших данных и данных ваших коллег как при работе внутри сети БИН РАН, так и в случае удаленного доступа к ресурсам корпоративной сети.
- Нажмите «**Подключение**» и установите VPN-соединение с сервером института.

Порядок настройки VPN-соединения на компьютере под управлением Windows 7 и Windows 8 (8.1)

- Откройте «**Центр управления сетями и общим доступом**»:
  в Windows 7: через меню, Пуск → Панель управления → Центр управления сетями и общим доступом;
  в Windows 8: переместите курсор в верхний или нижний правый угол рабочего стола → в панели меню нажмите Параметры → выберите Панель управления;
- Выберите «**Настройка нового подключения или сети**»;
- В окне установки подключения или сети выберите «**Подключение к рабочему месту**», нажмите «**Далее**»;
- В окне подключения к рабочему месту выберите «**Нет, создать новое подключение**», нажмите «**Далее**»;
- Нажмите «**Использовать мое подключение к Интернету (VPN)**»;
- В окне настройки VPN-подключения введите адрес сервера **vpn.binran.ru** и название подключения, например, **BIN**, нажмите «**Далее**»:

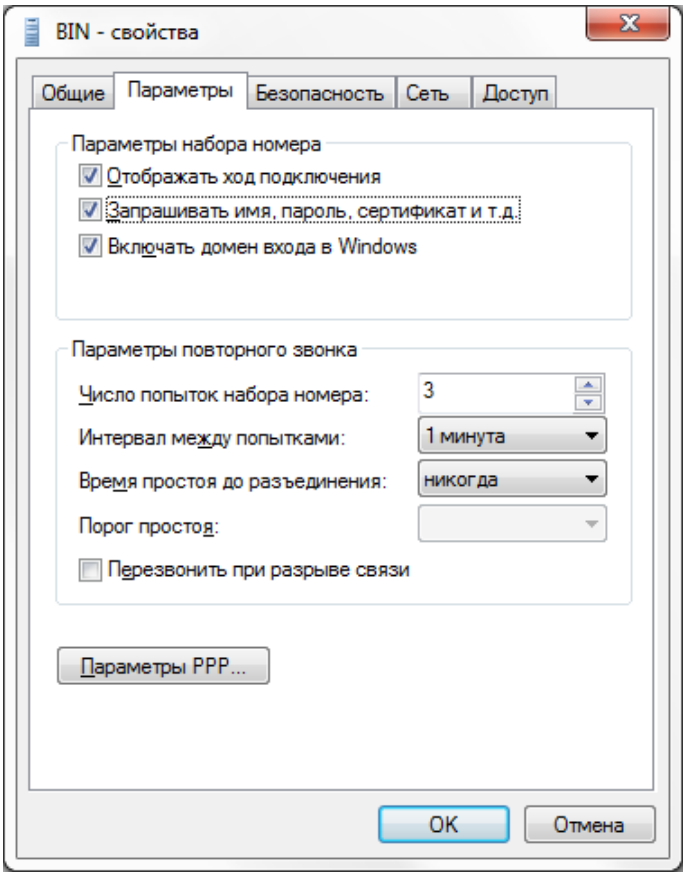


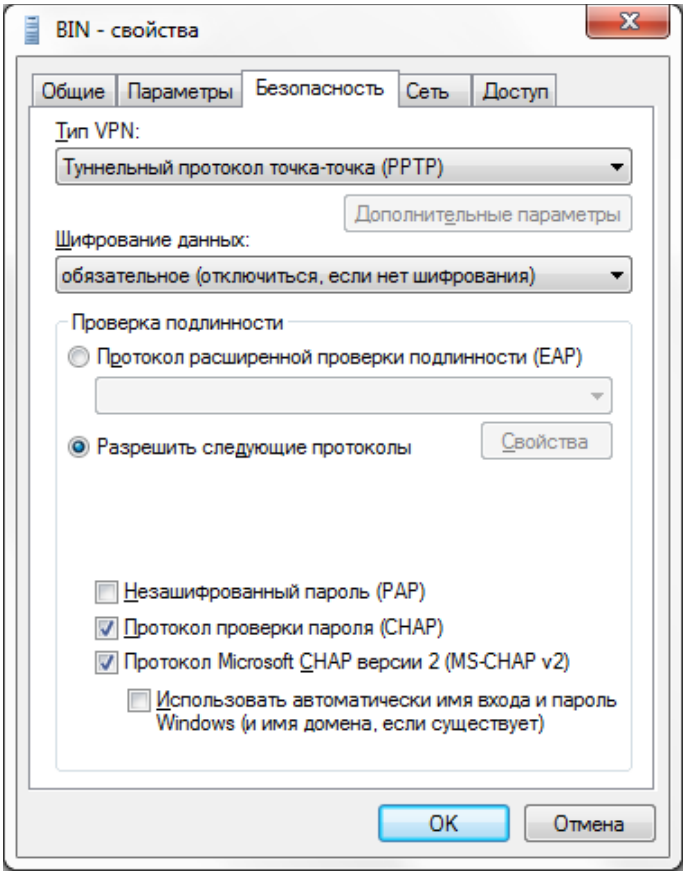
- Введите данные вашей персональной учетной записи пользователя в сети БИН РАН как показано ниже, нажмите «**Создать**»:

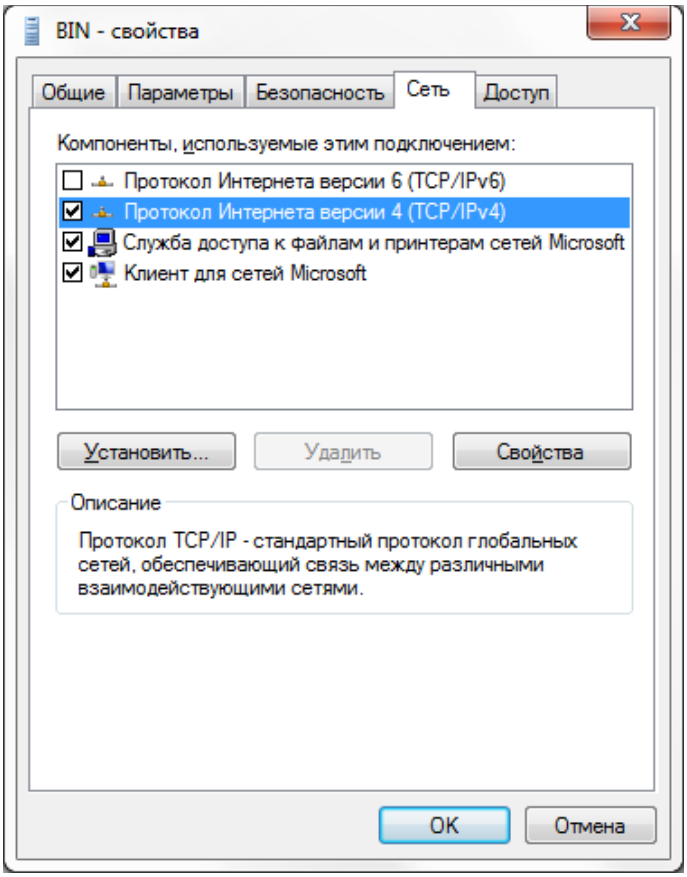


- Включать опцию «**Запомнить этот пароль**» рекомендуется только в том случае, если вы устанавливаете VPN-соединение со своего личного компьютера (домашний компьютер, ноутбук во время командировки и пр.), а не используете чужой служебный компьютер или рабочую станцию в публичной точке доступа.
  Помните, что аккуратное использование собственной учетной записи пользователя — единственная гарантия сохранности ваших данных и данных ваших коллег как при работе внутри сети БИН РАН, так и в случае удаленного доступа к ресурсам корпоративной сети.
- Дождитесь создания VPN-соединения, но **не подключайтесь** сейчас, нажмите «**Закрыть**»;
- Вернитесь в «**Центр управления сетями и общим доступом**» и выберите «**Изменение параметров адаптера**»;
- В открывшемся окне Сетевых подключений выделите созданное VPN-подключение и откройте его свойства через меню: Файл → Свойства;

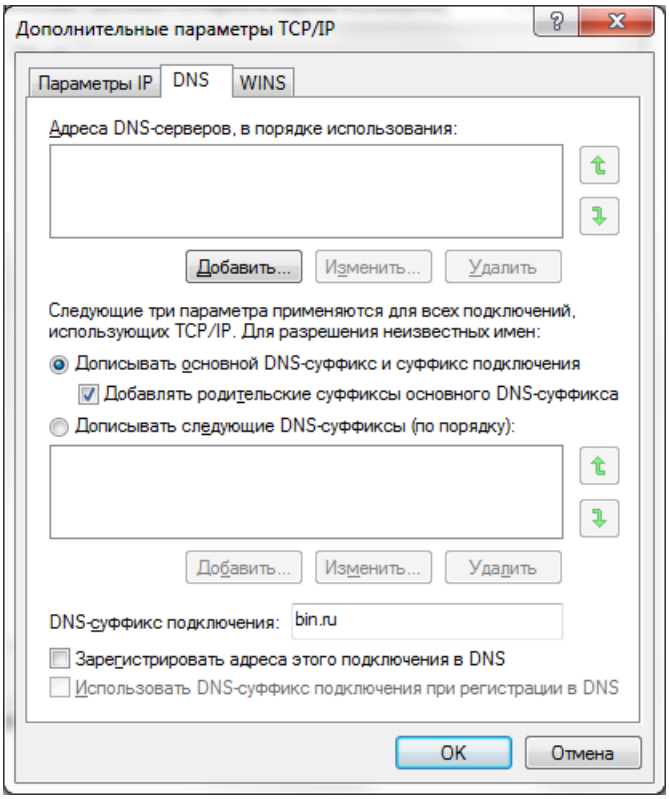
- Настройте свойства VPN-соединения как показано ниже:



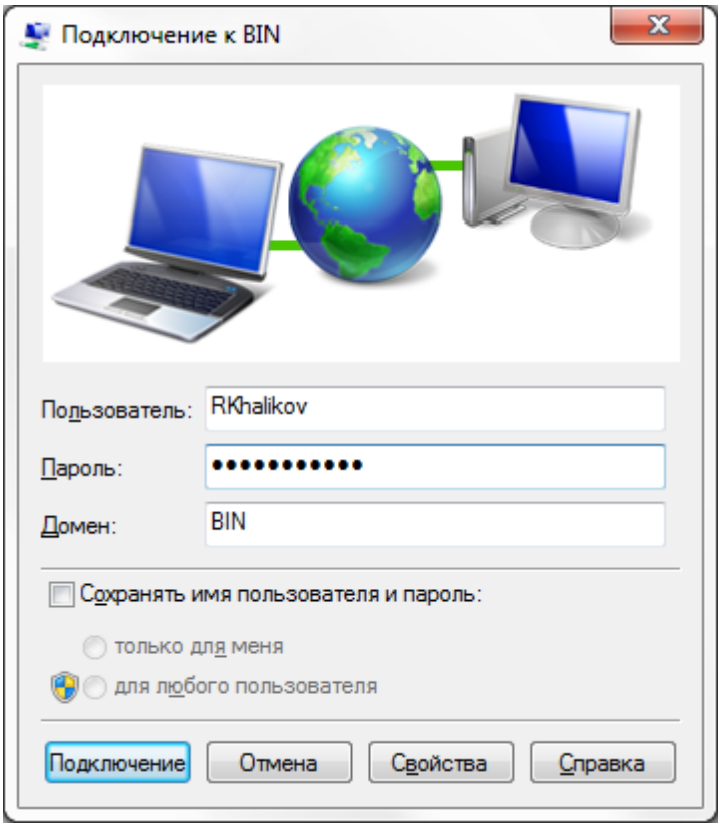




- На закладке Сеть выберите **«Протокол Интернета версии 4 (TCP/IPv4)»** и нажмите **«Свойства»**;
- В открывшемся окне нажмите **«Дополнительно...»** и в следующем окне на закладке DNS укажите DNS-суффикс подключения **bin.ru** как показано ниже:



- Сохраните настройки, последовательно нажимая «**ОК**» и закрывая окна;
- Запустите VPN-соединение, в окне подключения введите данные вашей персональной учетной записи пользователя в сети БИН РАН как показано ниже:



- Включать опцию «**Сохранять имя пользователя и пароль**» рекомендуется только в том случае, если вы устанавливаете VPN-соединение со своего личного компьютера (домашний компьютер, ноутбук во время командировки и пр.), а не используете чужой служебный компьютер или рабочую станцию в публичной точке доступа.
  Помните, что аккуратное использование собственной учетной записи пользователя — единственная гарантия сохранности ваших данных и данных ваших коллег как при работе внутри сети БИН РАН, так и в случае удаленного доступа к ресурсам корпоративной сети.
- Нажмите «**Подключение**» и установите VPN-соединение с сервером института.

Общая информация о работе с VPN-соединением

VPN-соединение предназначено для безопасного удаленного доступа к внутренним ресурсам корпоративной сети. Обращаем внимание — все прочие сетевые сервисы (доступ в Интернет, электронная почта, системы обмена сообщениями и пр.) при подключении VPN-соединения будут недоступны; их работа возобновится после отключения VPN-соединения.

Для удобной работы с VPN-соединением можно создать ярлык для него на рабочем столе Windows и с его помощью выполнять подключение/отключение VPN-соединения.

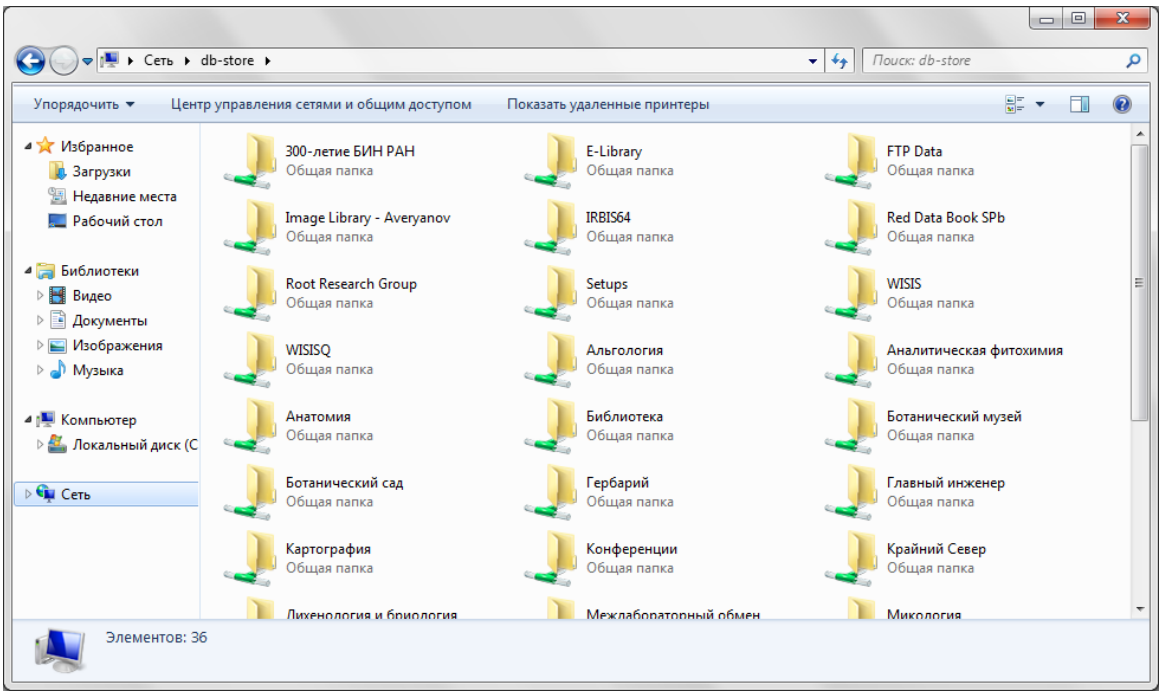
Для создания ярлыка выполните следующие действия:

- Откройте «**Сетевые подключения**» (в Windows XP: Панель управления → Сетевые подключения; в Windows 7/8: Панель управления → Центр управления сетями и общим доступом → Изменение параметров адаптера);
- Выделите VPN-соединение и перетащите его правой кнопкой мыши на рабочий стол Windows;
- Отпустите правую кнопку мыши и выберите «**Создать ярлык**» в открывшемся контекстном меню;

- Для подключения VPN-соединения дважды щелкните ярлык или щелкните по нему правой кнопкой мыши и в открывшемся меню выберите «**Подключить**»;
- Для отключения VPN-соединения щелкните по ярлыку правой кнопкой мыши и в открывшемся меню выберите «**Отключить**».

Порядок работы с внутренними ресурсами сети БИН РАН в режиме удаленного доступа

- Установите VPN-соединение с сервером института;
- Откройте Проводник Windows — «**Мой компьютер**» или любое другое окно Проводника, где есть адресная строка;
- Если адресная строка в Проводнике не отображается, включите ее через меню: Вид → Панели инструментов → Адресная строка;
- Наберите в адресной строке Проводника имя компьютера, к ресурсам которого вы хотите получить доступ, в формате **\\Имякомпьютера** и откройте его.
  Например, для доступа к серверу баз данных, на котором хранятся общие документы лабораторий и другие материалы, укажите в адресной строке имя сервера **\\Db-Store**. В Проводнике отобразится список сетевых каталогов сервера:



  Указав в адресной строке имя компьютера кого-нибудь из ваших коллег, вы получите список каталогов этого компьютера, для которых открыт доступ по сети.
- Доступ к сетевым каталогам определяется правами вашей персональной учетной записи — если у вас есть права на доступ к сетевым ресурсам, вы можете работать с ними, как если бы вы находились за своим рабочим компьютером в институте.
  Обращаем внимание — никаких дополнительных запросов на авторизацию (предложений указать имя или пароль и т.п.) при доступе к сетевым ресурсам возникать не должно, так как вы уже авторизовались в сети института, установив VPN-соединение с сервером.
- Если ваш рабочий компьютер включен и находится в сети института, вы можете получить доступ не только к его папкам, открытым для доступа по сети, но и к дискам компьютера непосредственно. Для этого необходимо указать в адресной строке не только имя компьютера, но и диск, в следующем формате — **\\Имякомпьютера\Диск$** (например, **\\Khalikov\D$**).
- После завершения работы с сетевыми ресурсами отключите VPN-соединение.