



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 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»:

Подключение к рабочему месту

Введите Интернета-адрес для подключения

Этот адрес можно получить у сетевого администратора.

Интернете-адрес:

Имя местоназначения:

Использовать смарт-карту

Разрешить использовать это подключение другим пользователям
Этот параметр позволяет любому пользователю, имеющему доступ к этому компьютеру, использовать это подключение.

Не подключаться сейчас, только выполнить установку для подключения в будущем

Далее Отмена

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

Подключение к рабочему месту

Введите имя пользователя и пароль

Пользователь:

Пароль:

Отображать вводимые знаки

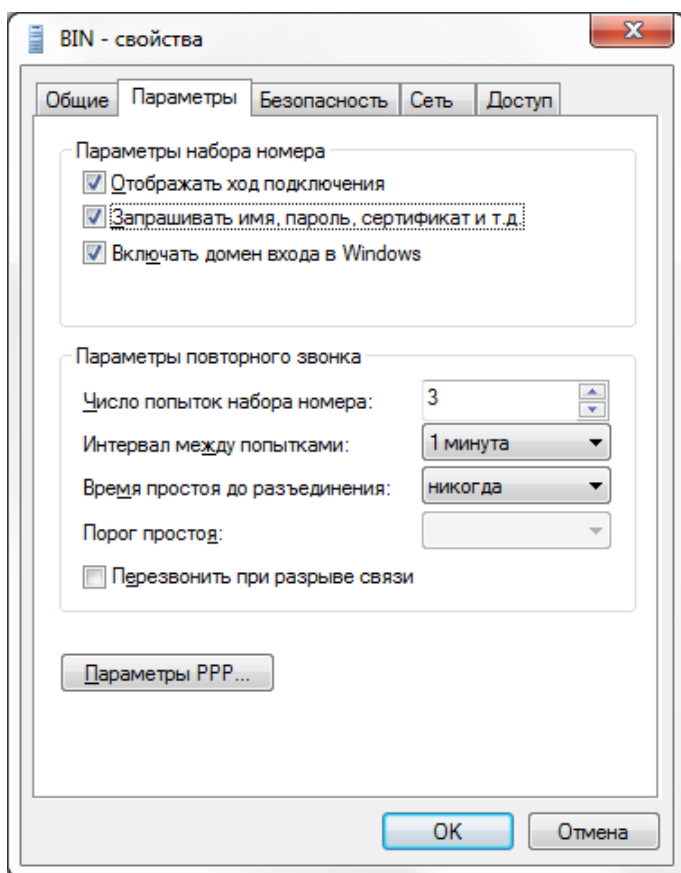
Запомнить этот пароль

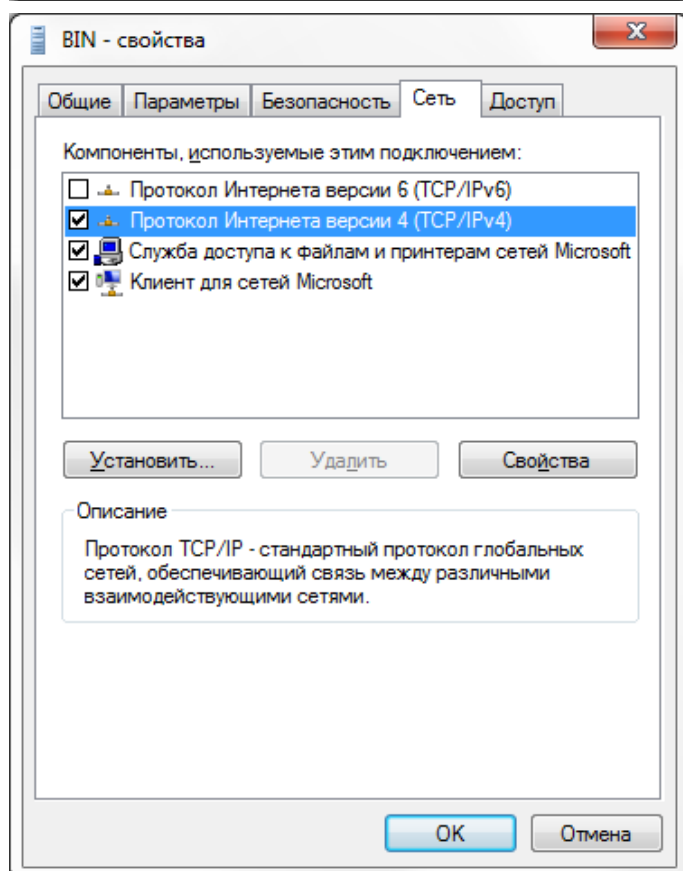
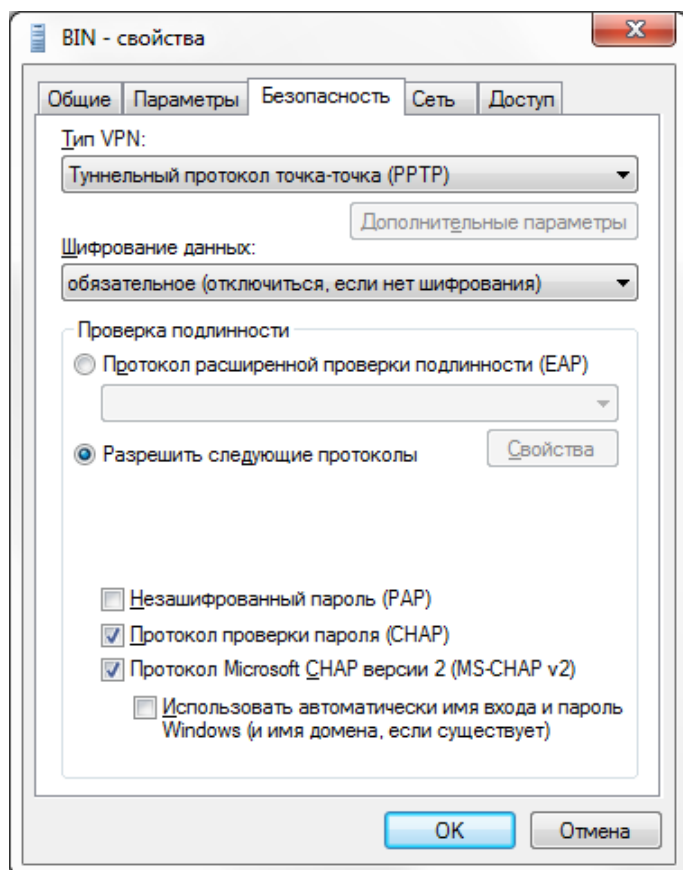
Домен (не обязательно):

Создать Отмена



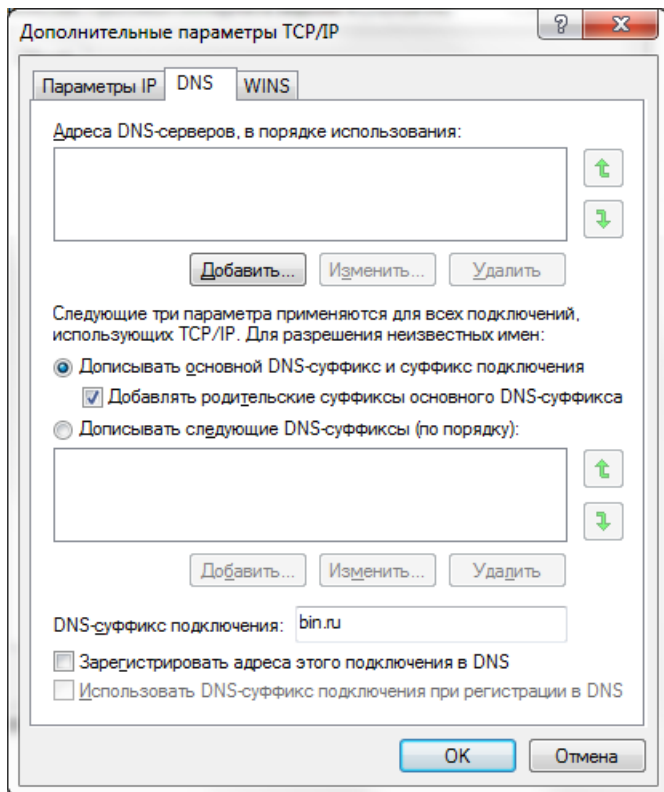
- Включать опцию «**Запомнить этот пароль**» рекомендуется только в том случае, если вы устанавливаете VPN-соединение со своего личного компьютера (домашний компьютер, ноутбук во время командировки и пр.), а не используете чужой служебный компьютер или рабочую станцию в публичной точке доступа.
Помните, 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 «**Заккрыть**»;
- 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 в точности как показано ниже:



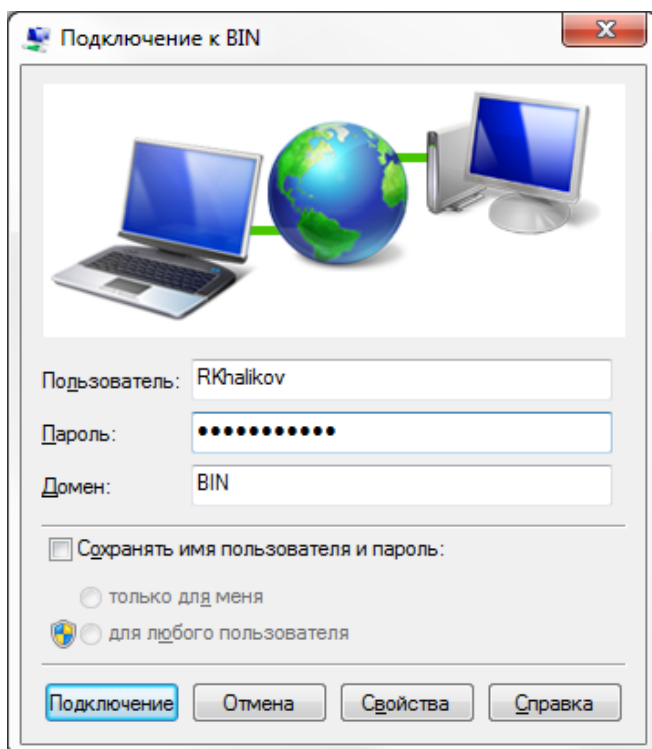




- На закладке Сеть выберите «Протокол Интернета версии 4 (TCP/IPv4)» и нажмите «Свойства»;
- В открывшемся окне нажмите «Дополнительно...» и в следующем окне на закладке DNS укажите DNS-суффикс подключения **bin.ru** как показано ниже:



- 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:

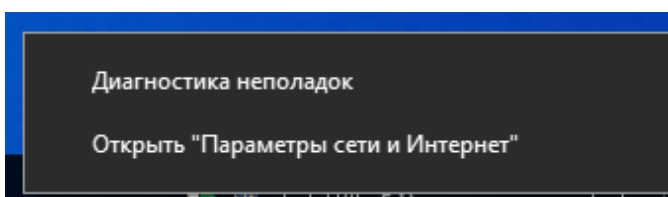




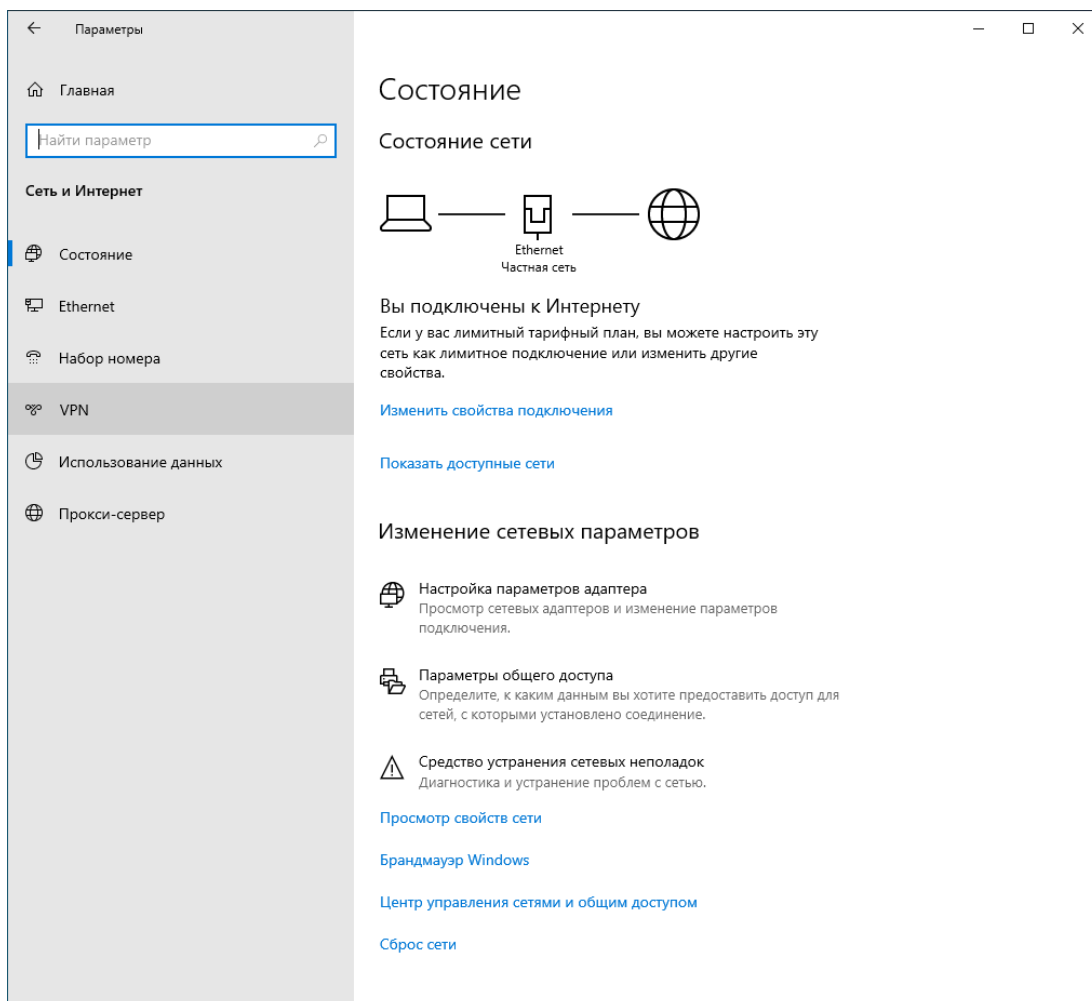
- Включать опцию «Сохранять имя пользователя и пароль» рекомендуется только в том случае, если вы устанавливаете VPN-соединение со своего личного компьютера (домашний компьютер, ноутбук во время командировки и пр.), а не используете чужой служебный компьютер или рабочую станцию в публичной точке доступа.
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.

Порядок настройки VPN-соединения на компьютере под управлением Windows 10

- Откройте «Параметры сети и Интернет»: щелкните правой кнопкой мыши по значку сетевых подключений в правом нижнем углу экрана и в открывшемся меню выберите соответствующий пункт:

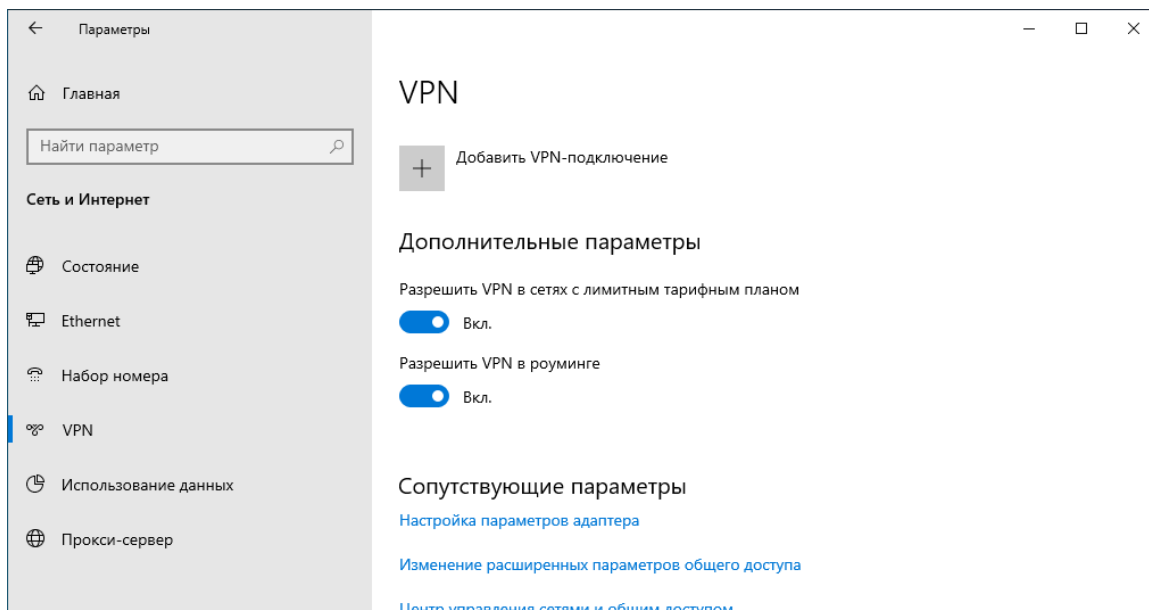


- В открывшемся окне нажмите «VPN»:

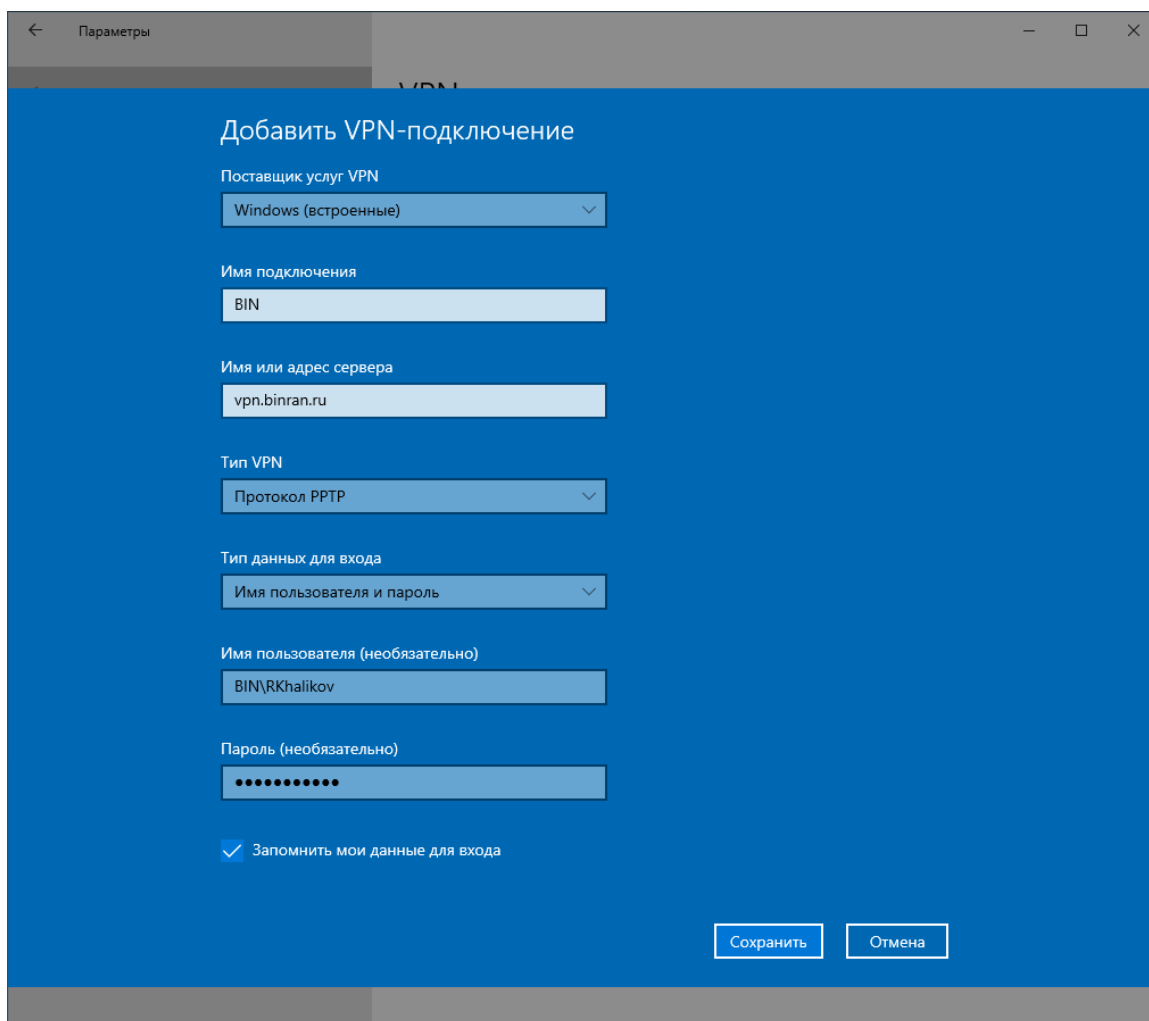




- В открывшемся окне нажмите «Добавить VPN-подключение»:

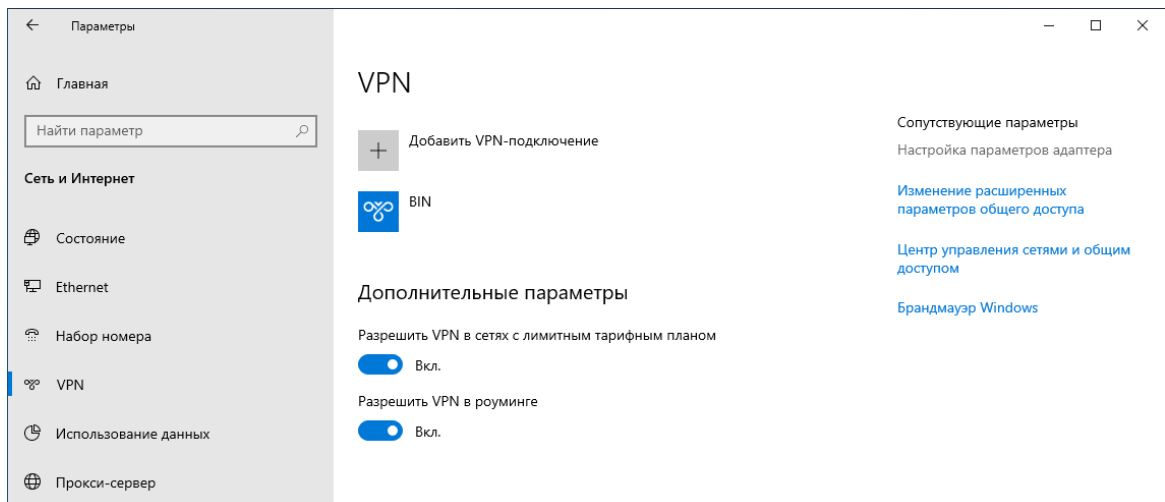


- В окне настройки VPN-подключения введите адрес сервера **vpn.binran.ru**, название подключения, например, **BIN**, данные вашей персональной учетной записи пользователя в сети БИН РАН и другие параметры в точности как показано ниже и сохраните их:

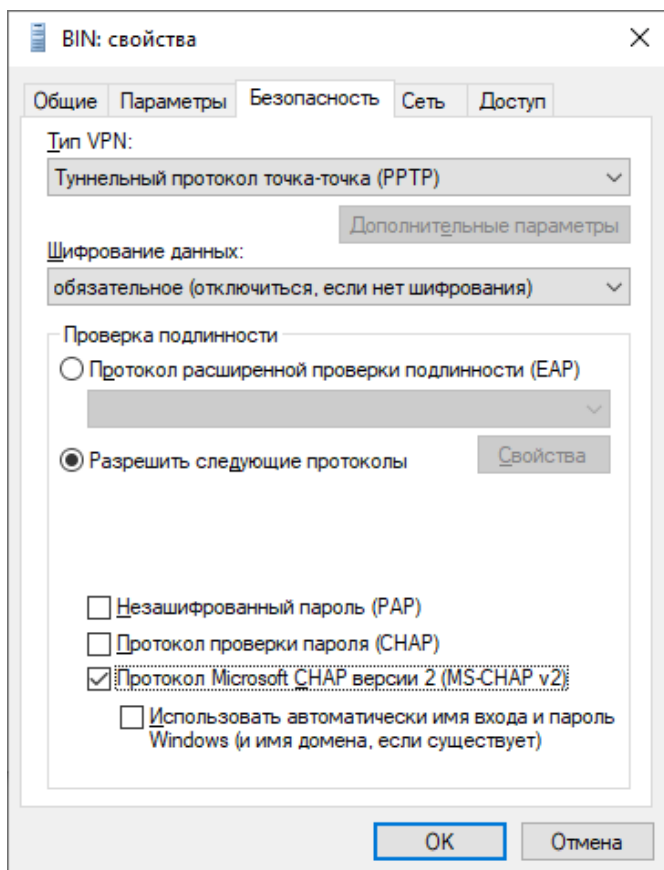


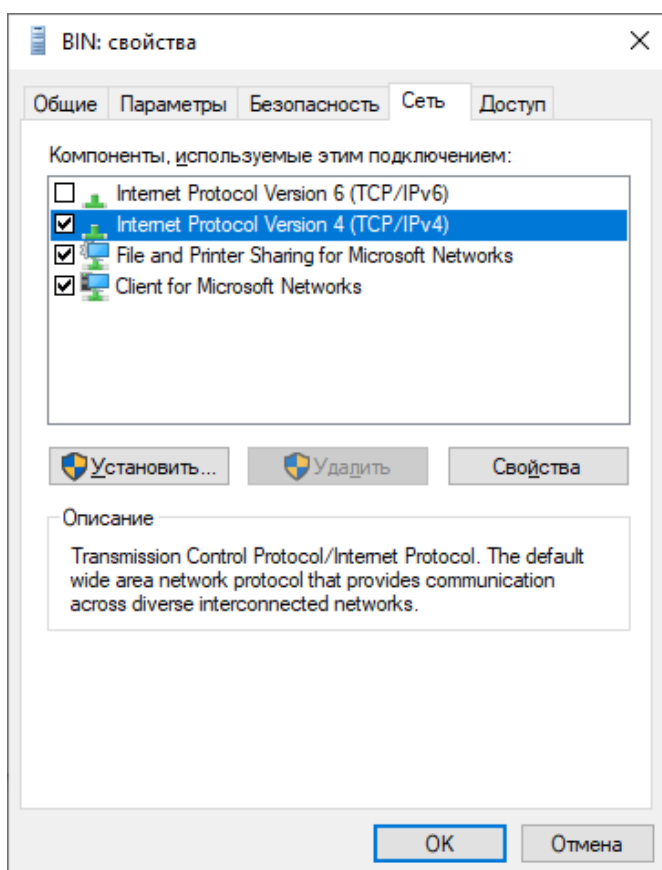


- Включать опцию «Запомнить мои данные для входа» рекомендуется только в том случае, если вы устанавливаете VPN-соединение со своего личного компьютера (домашний компьютер, ноутбук во время командировки и пр.), а не используете чужой служебный компьютер или рабочую станцию в публичной точке доступа. 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.
- В окне настройки VPN выберите «Настройка параметров адаптера»:

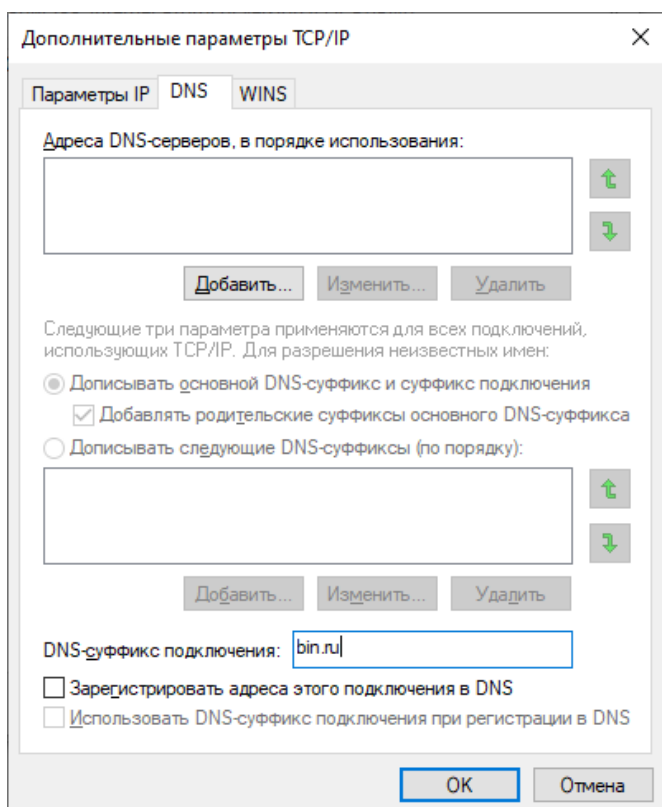


- В открывшемся окне Сетевых подключений щелкните правой кнопкой по созданному VPN-подключению и в открывшемся меню выберите «Свойства»;
- Настройте свойства VPN-соединения в точности как показано ниже:



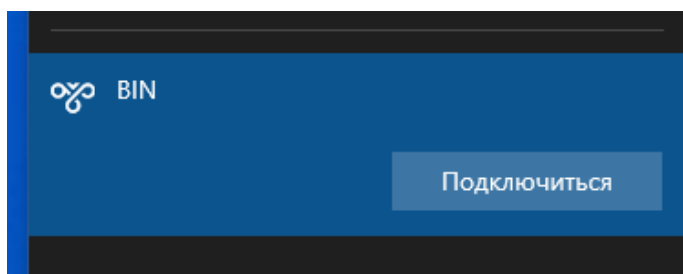


- На закладке Сеть выберите «Протокол Интернета версии 4 (TCP/IPv4)» и нажмите «Свойства»;
- В открывшемся окне нажмите «Дополнительно...» и в следующем окне на закладке DNS укажите DNS-суффикс подключения bin.ru как показано ниже:





- Сохраните настройки, последовательно нажимая «ОК» и закрывая окна;
- Щелкните левой кнопкой мыши по значку сетевых подключений в правом нижнем углу экрана и в открывшемся списке выберите созданное VPN-соединение, чтобы в нем открылась кнопка «Подключиться»:



- Нажмите «Подключиться» и установите VPN-соединение с сервером института.

Общая информация о работе с VPN-соединением

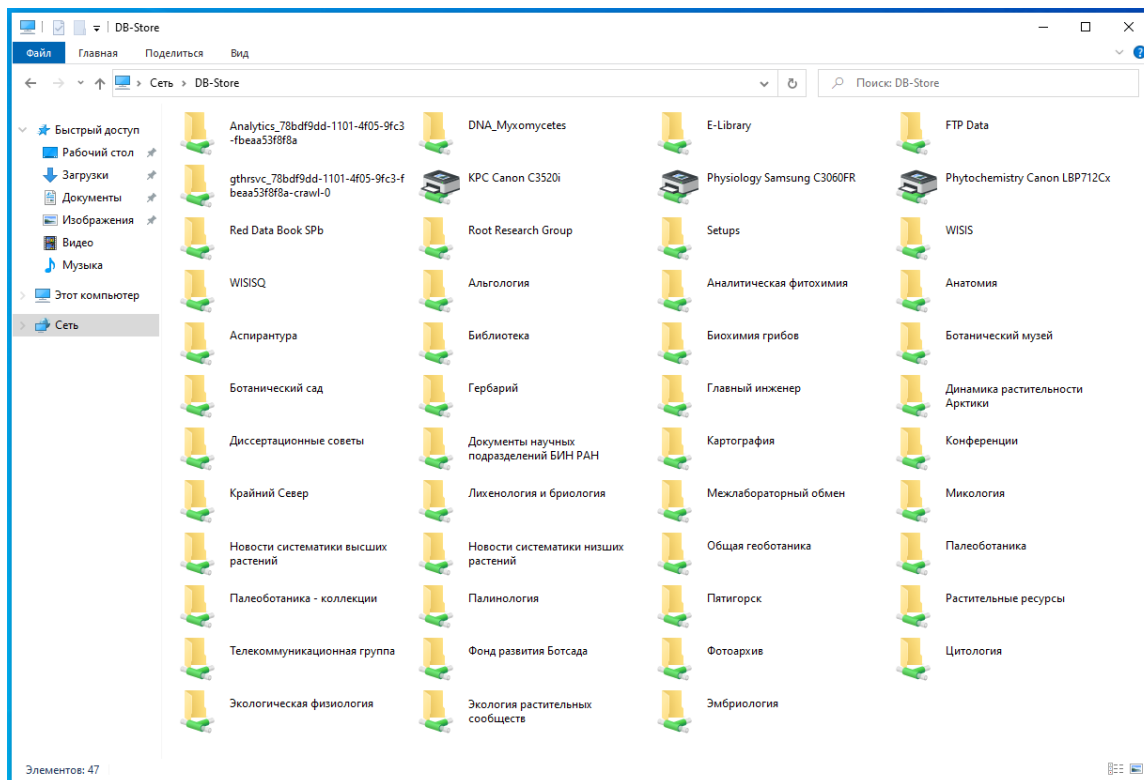
VPN-соединение предназначено для безопасного удаленного доступа к внутренним ресурсам корпоративной сети. Обращаем внимание – прочие сетевые сервисы (доступ в Интернет, электронная почта, системы обмена сообщениями и пр.) при подключении VPN-соединения могут оказаться недоступны или работать иначе, чем без VPN-соединения; корректная их работа возобновится после отключения VPN-соединения.

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;
- Наберите в адресной строке Проводника имя компьютера, к ресурсам которого вы хотите получить доступ, в формате \\Имякомпьютера и откройте его.



Например, для доступа к файловому серверу, 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.