Удаленный доступ к ресурсам корпоративной сети БИН РАН

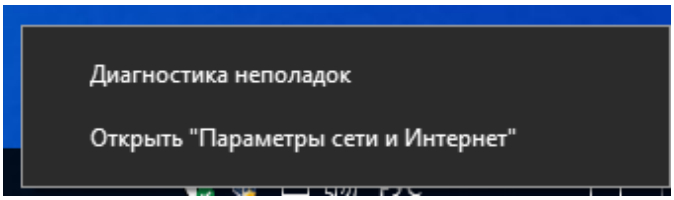
Внутренние ресурсы корпоративной сети (серверы и рабочие станции) надежно изолированы от несанкционированного доступа извне. Вместе с тем, возможность удаленного доступа к внутренним ресурсам может быть чрезвычайно полезна для пользователей в самых разных ситуациях. Для обеспечения безопасного удаленного доступа внутрь корпоративной сети используется технология **VPN** (**Virtual Private Network** — виртуальная частная сеть) на основе протоколов **PPTP** и **L2TP**.

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 протоколов PPTP/L2TP 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 протоколы PPTP/L2TP закрыты на уровне прокси-сервера, через который осуществляется доступ с рабочих компьютеров в Интернет.

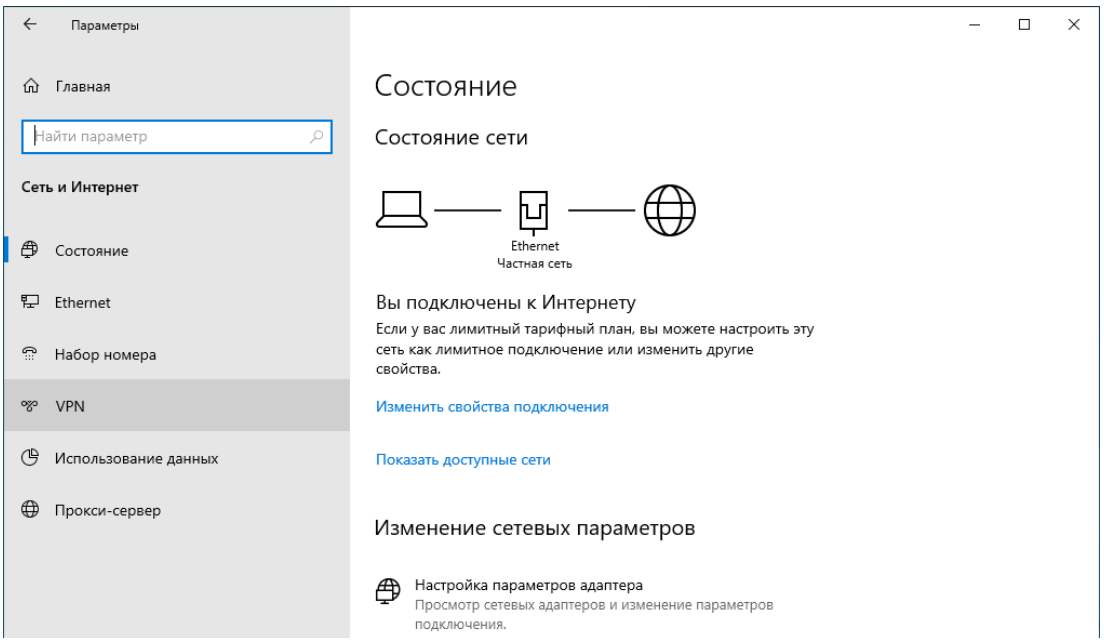
Если вы не можете получить доступ в сеть БИН РАН после выполнения всех шагов настоящего руководства — это однозначно указывает на то, что протоколы PPTP/L2TP закрыты вашим провайдером или требуется перенастройка используемого вами сетевого оборудования.

Порядок настройки VPN-соединения на компьютере под управлением Windows

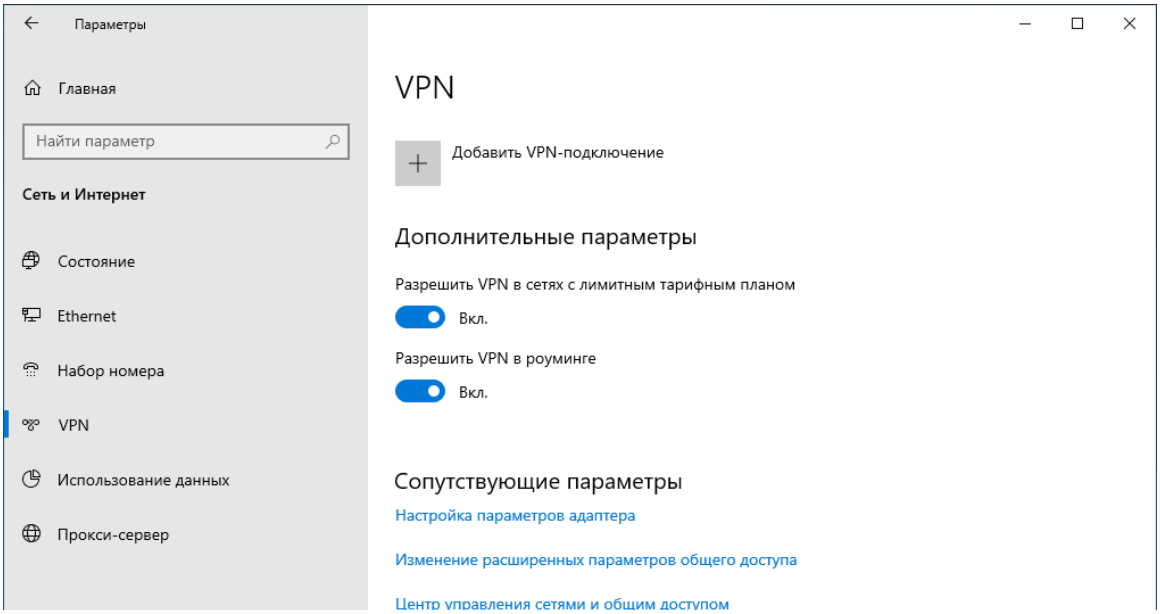
- Откройте **«Параметры сети и Интернет»**:
  щелкните правой кнопкой мыши по значку сетевых подключений в правом нижнем углу экрана и в открывшемся меню выберите соответствующий пункт:



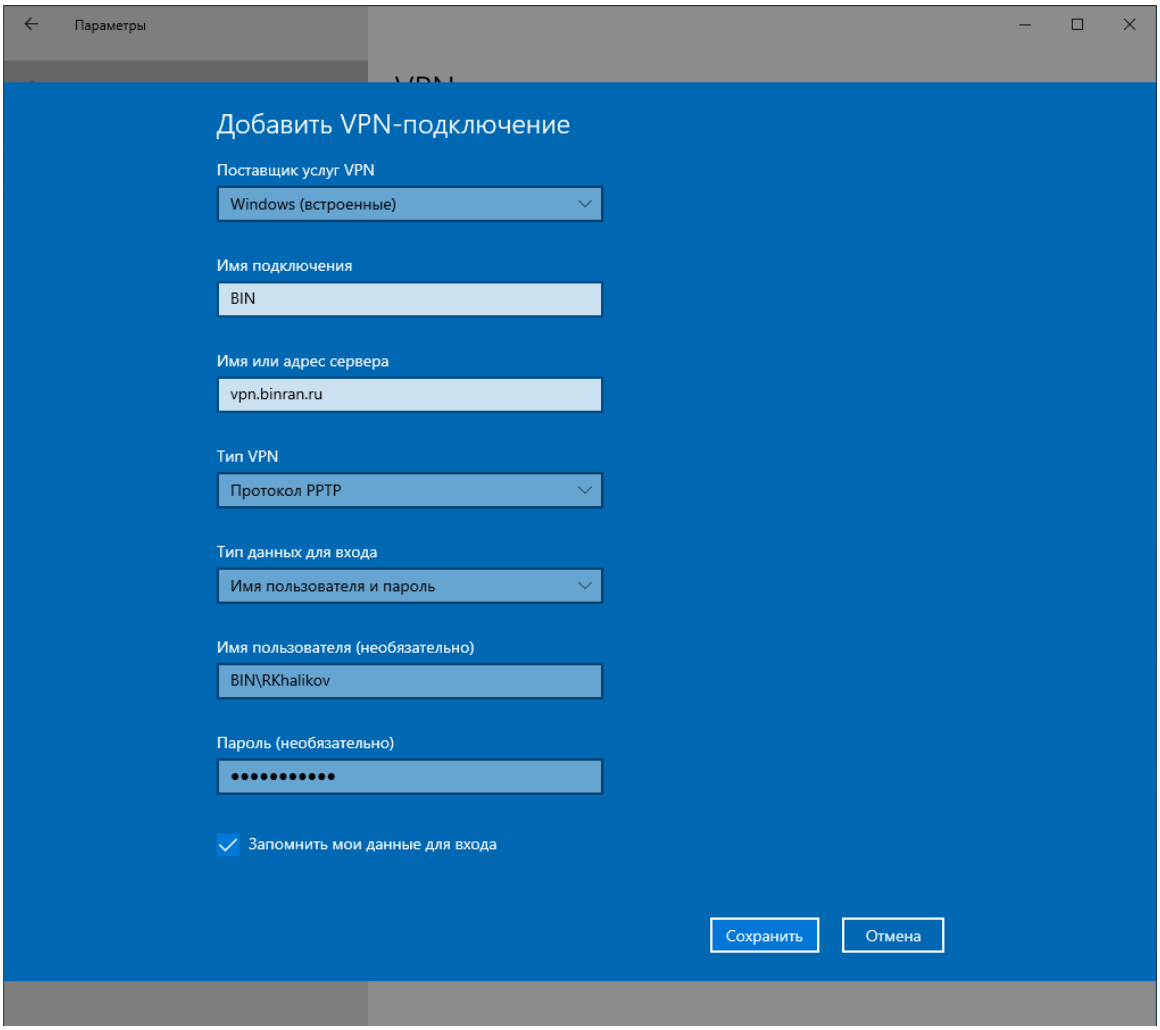
- В открывшемся окне нажмите **«VPN»**:



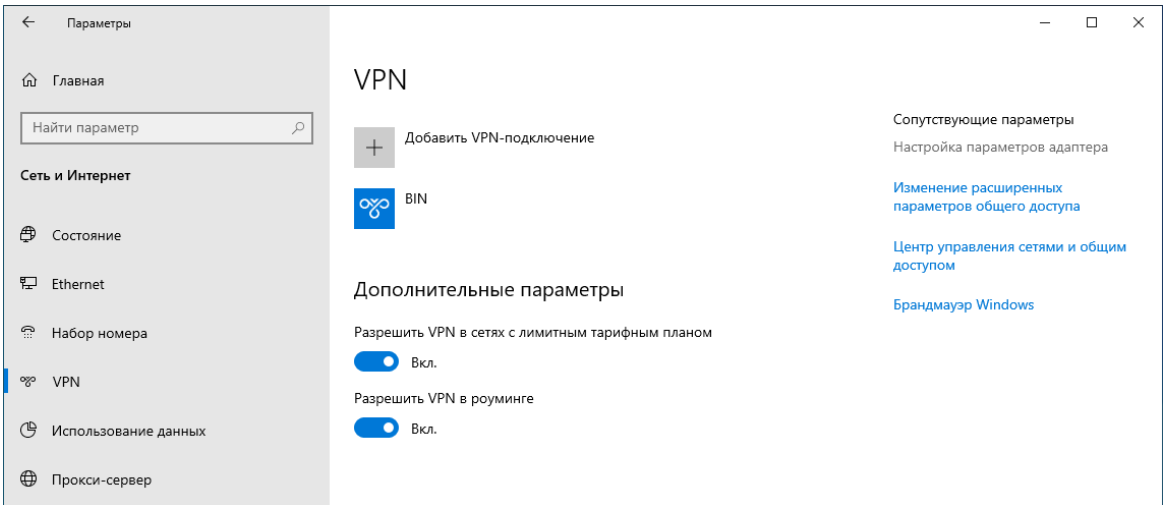
- В открывшемся окне нажмите «**Добавить VPN-подключение**»:



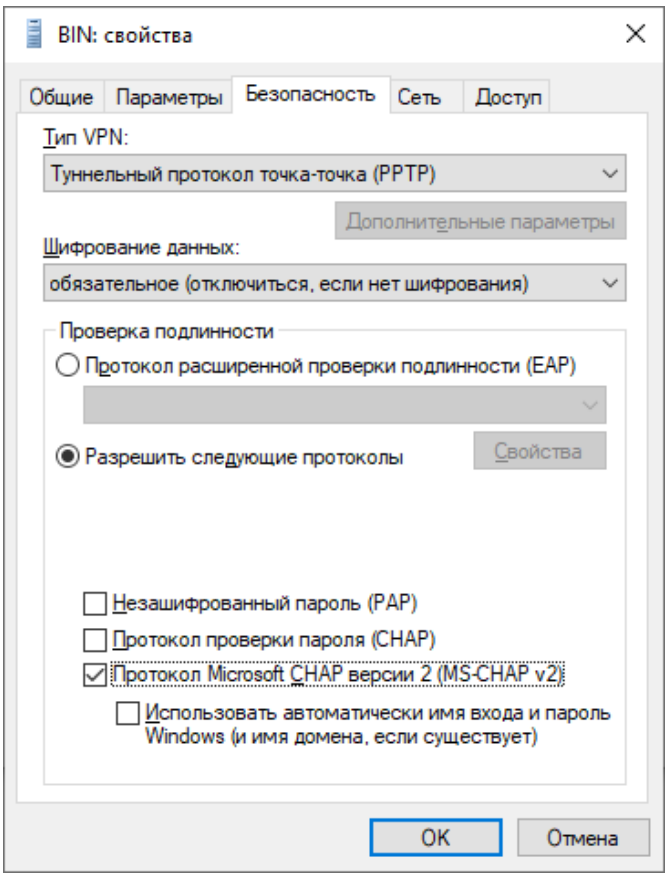
- В окне настройки VPN-подключения введите адрес сервера **vpn.binran.ru**, название подключения, например, **BIN**, данные вашей персональной учетной записи пользователя в сети БИН РАН и другие параметры в точности как показано ниже и сохраните их:



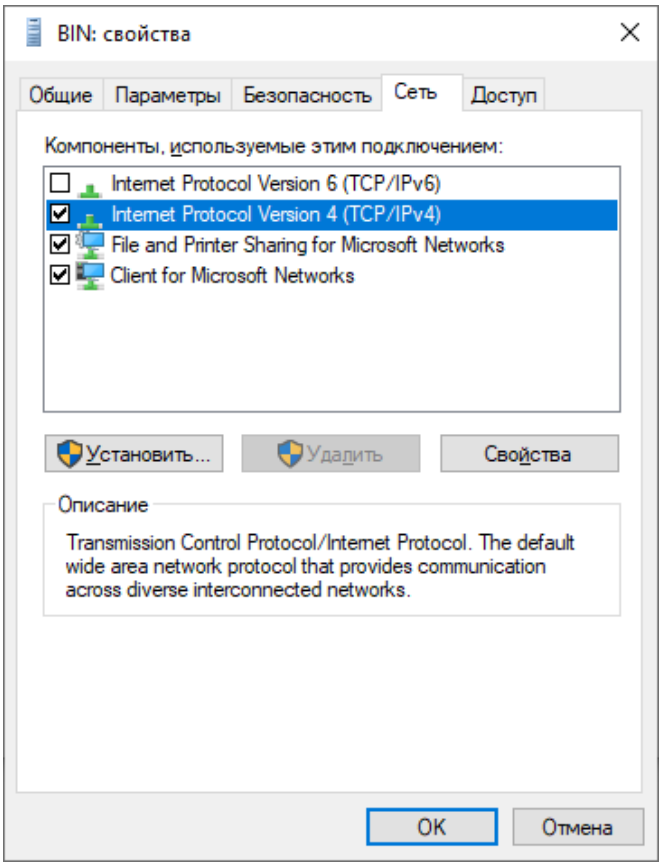
- Включать опцию **«Запомнить мои данные для входа»** рекомендуется только в том случае, если вы устанавливаете VPN-соединение со своего личного компьютера (домашний компьютер, ноутбук во время командировки и пр.), а не используете чужой служебный компьютер или рабочую станцию в публичной точке доступа.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



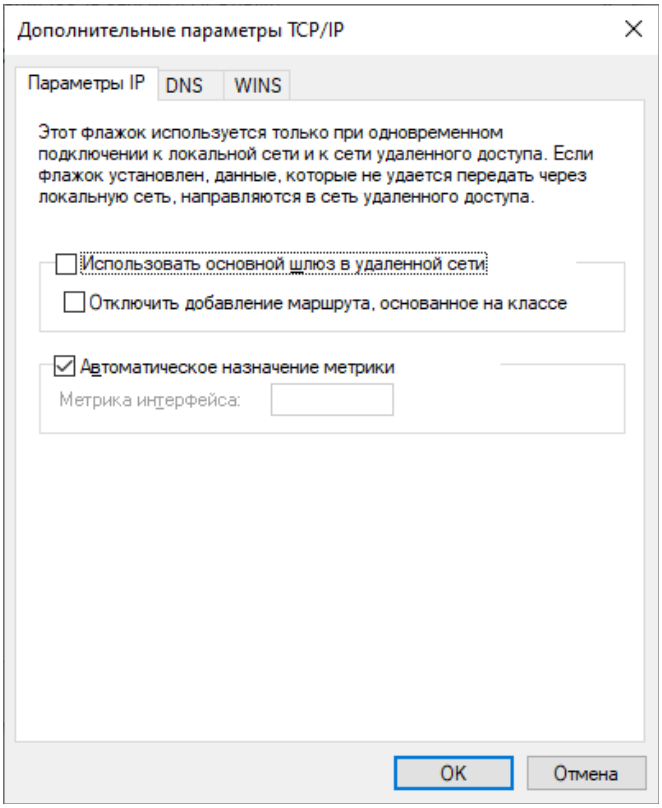
- В открывшемся окне Сетевых подключений щелкните правой кнопкой по созданному VPN-подключению и в открывшемся меню выберите **«Свойства»**;
- Настройте свойства VPN-соединения в точности как показано ниже:



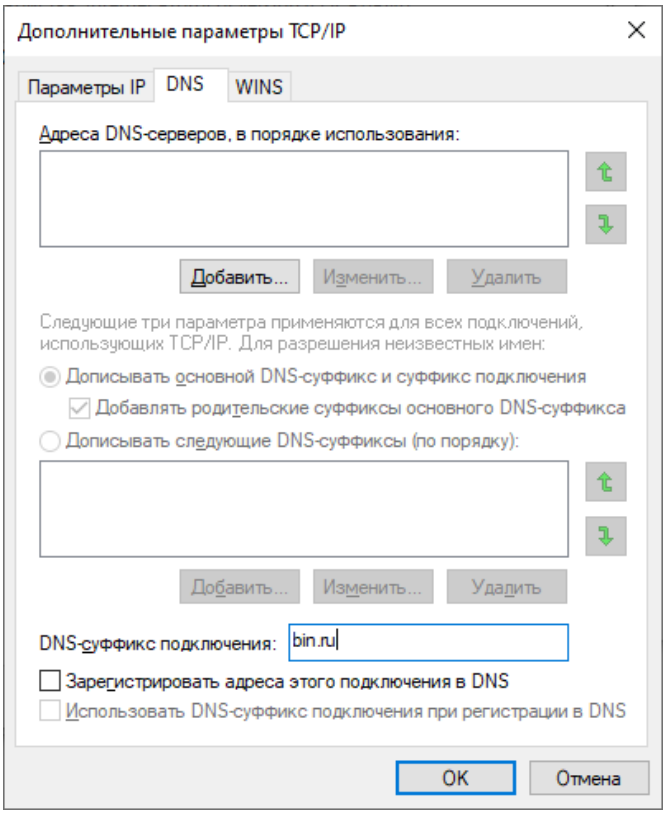
- На закладке Сеть выберите **«Протокол Интернета версии 4»** и нажмите **«Свойства»**:



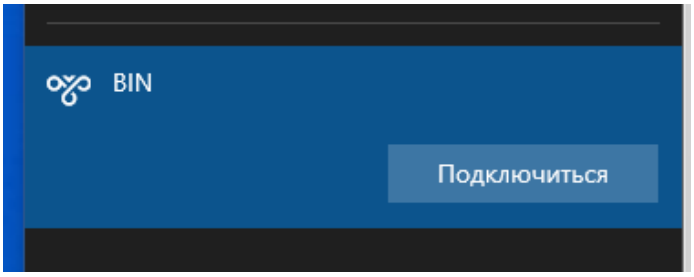
- В открывшемся окне нажмите **«Дополнительно...»** и в следующем окне на закладке Параметры IP снимите галочку использования основного шлюза в удаленной сети как показано ниже:



- 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.

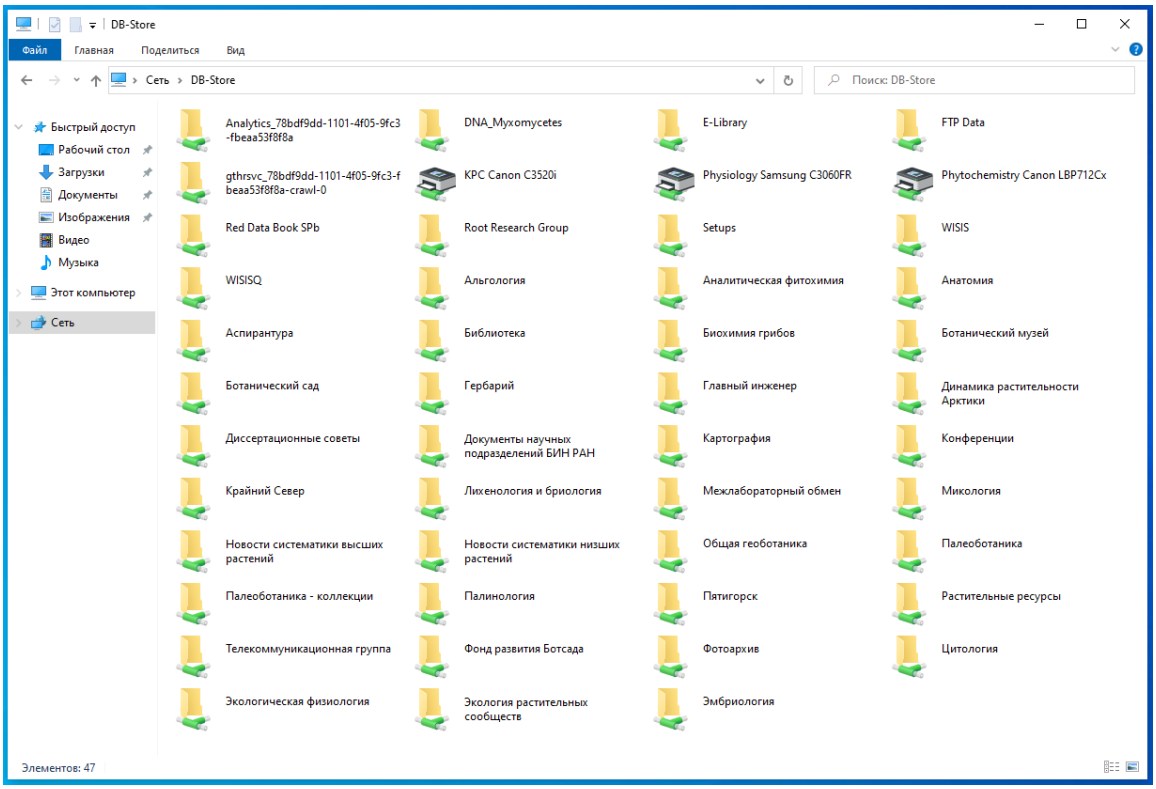
Общая информация о работе с VPN-соединением

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.

Помните — вы несете полную ответственность за свои действия, выполняя VPN-подключение к сети института. В режиме удаленного доступа категорически недопустимо использование программного обеспечения и сетевых сервисов, создающих избыточную нагрузку и генерирующих значительный сетевой трафик — торрент-клиентов, стриминговых сервисов, онлайн кинотеатров, социальных сетей и т. п. Подобного рода деятельность не требует VPN-подключения к ресурсам сети института!

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:



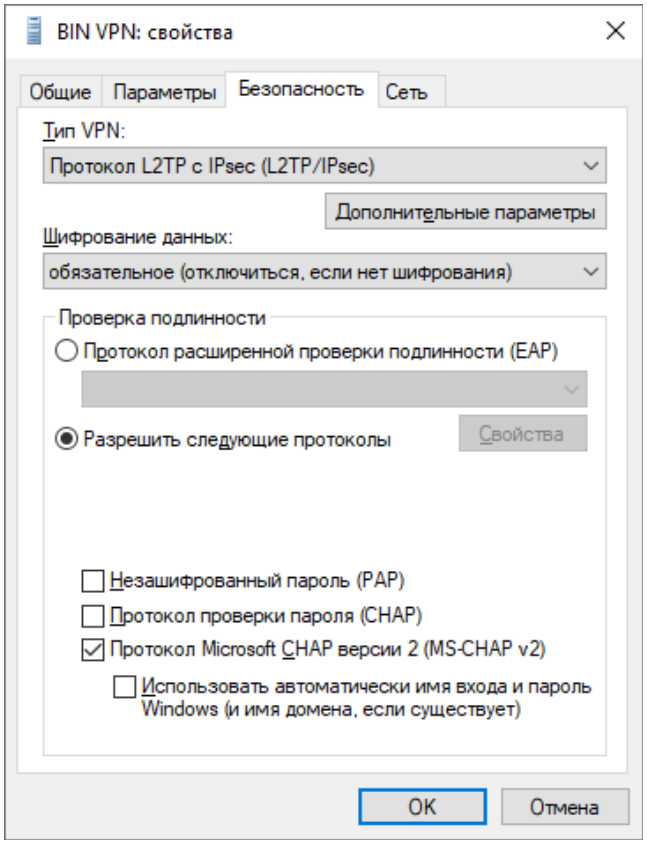
  Указав в адресной строке имя компьютера кого-нибудь из ваших коллег, вы получите список каталогов этого компьютера, для которых открыт доступ по сети.
- Доступ к сетевым каталогам определяется правами вашей персональной учетной записи — если у вас есть права на доступ к сетевым ресурсам, вы можете работать 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.

Порядок изменения протокола VPN-соединения

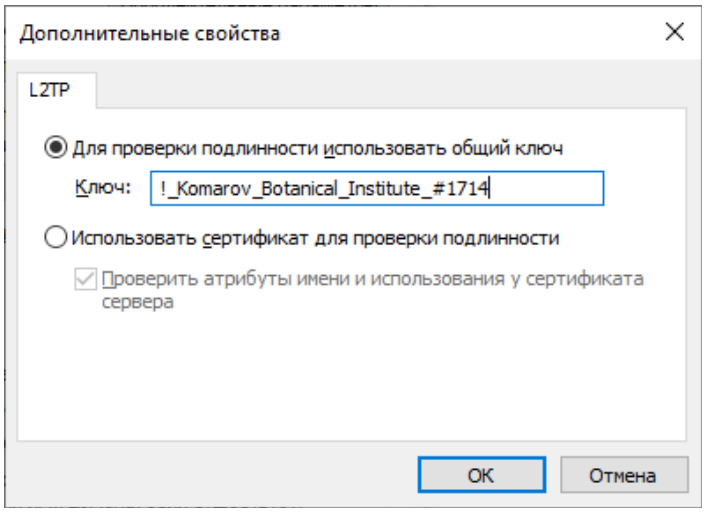
В последнее время многие провайдеры отключают поддержку протокола PPTP. При этом утрачивается возможность VPN-подключения к серверу института. В такой ситуации вы можете изменить протокол VPN-подключения, переключив его с PPTP на L2TP.

Для изменения протокола VPN-соединения выполните следующие действия:

- Откройте свойства VPN-соединения и выберите в списке Тип VPN протокол L2TP с IPsec как показано ниже:



- Нажмите «Дополнительные параметры» и в открывшемся окне введите общий ключ **!_Komarov_Botanical_Institute_#1714** как показано ниже:



- Сохраните настройки, последовательно нажимая «**ОК**» и закрывая окна.