Программа профессиональных проб по специальности «Сетевое и системное администрирование»

План

1. Изготовление и тестирование патч-корда Ethernet
2. Настройка IP-адресации на сетевом интерфейсе.
3. Проверка скорости интернет соединения.
4. Настройка общего публичного каталога на Windows 10
5. Создание VPN соединения с удаленным сервером.
6. Работа с виртуальными машинами на удаленном сервере.

Теоретические сведения

Витая пара — это несколько проводников, которые «завиты» в определенном порядке как между собой, так и вместе. Так как цифровая техника понимает только цифровой язык, по проводам приходится передавать огромное количество разнообразных сигналов: с разной длиной волны, разным напряжением и формой. Все это кодируется и декодируются специальными «приемниками» как с одной стороны, так и с другой. На качество и целостность битов в проводе могут влиять разные факторы. Например, любые источники магнитных волн и радиосигналов — как микроволновые печи или роутеры с частотой 5 ГГц.

Для чего нужна витая пара

Несмотря на то, что беспроводные технологии давно окутывают корпоративные сети, старая добрая проводка все еще остается актуальной, если нужно создать безопасную, быструю и стабильную сеть. И даже в домашних условиях иногда «полезно» подключаться по кабелю. Например, чтобы провести быстрый канал на несколько этажей в большом доме или просто подключить умный телевизор по проводу, когда просмотр любимых кинофильмов прерывается из-за слабого WiFi-приемника. А если захочется организовать видеонаблюдение в доме и за его пределами — без витой пары и PoE просто физически не обойтись.

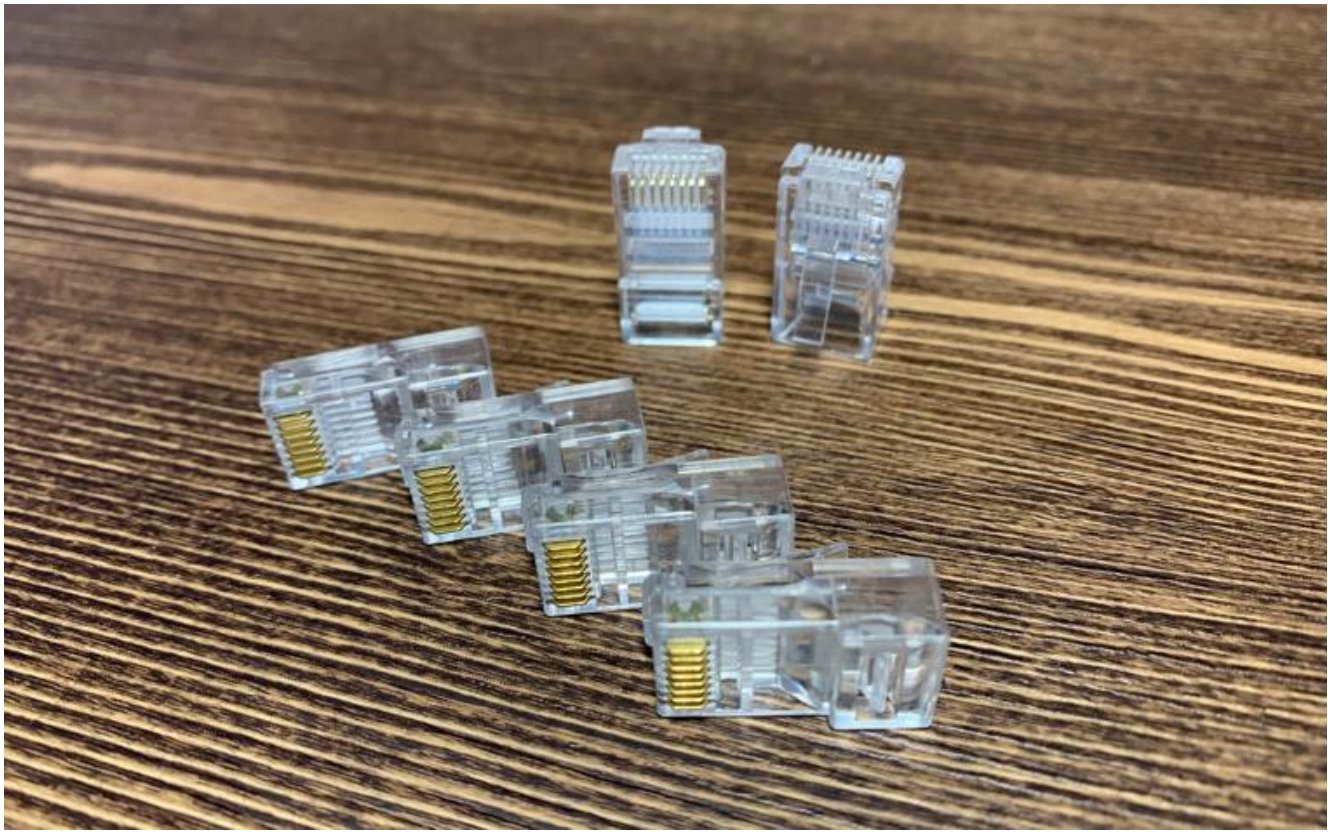
1. Изготовление и тестирование патч-корда Ethernet

Подготовка к обжиму

Перед обжимом нужно подготовить витую пару. Пусть это будет отрезок с небольшим запасом:

Обычного Cat. 5e кабеля с медными жилами и мягкой качественной оболочкой хватит для домашних задач с головой.

Даже опытный мастер может «запороть» процесс, поэтому коннектор — это расходный материал. Пусть и они тоже будут в запасе:



Простые коннекторы типа 5e — золотые и бутафорские.

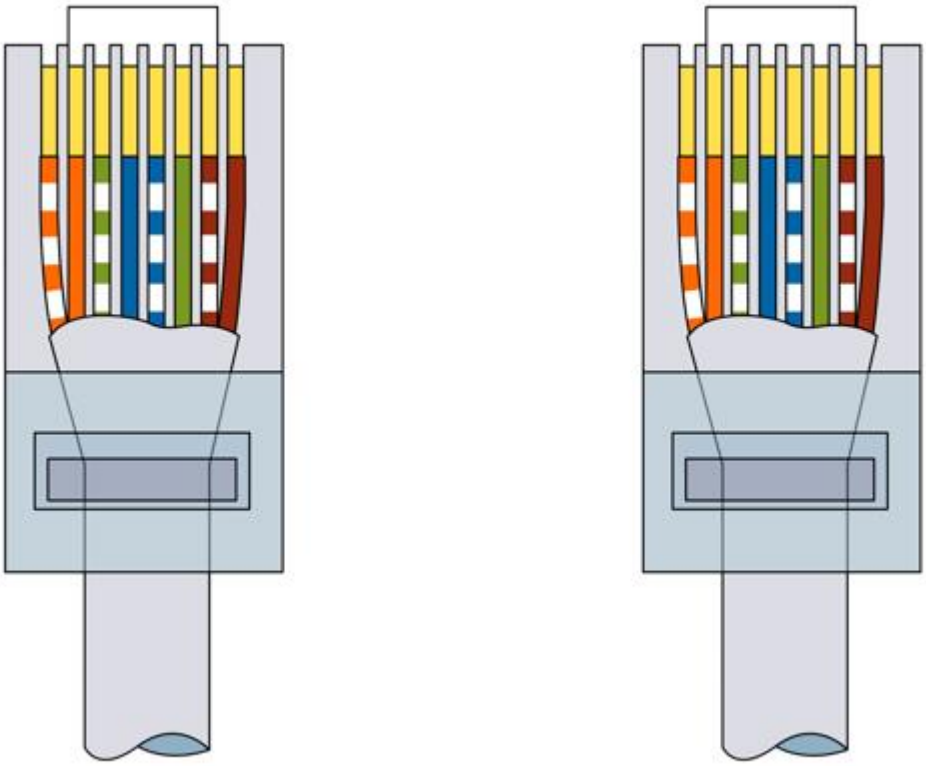
Для реализма будем использовать самый простой кримпер из доступных на рынке:

Такого инструмента хватит для нужд домашнего мастера и даже специалиста.

Отвертка с плоским жалом:

Секретный инструмент.

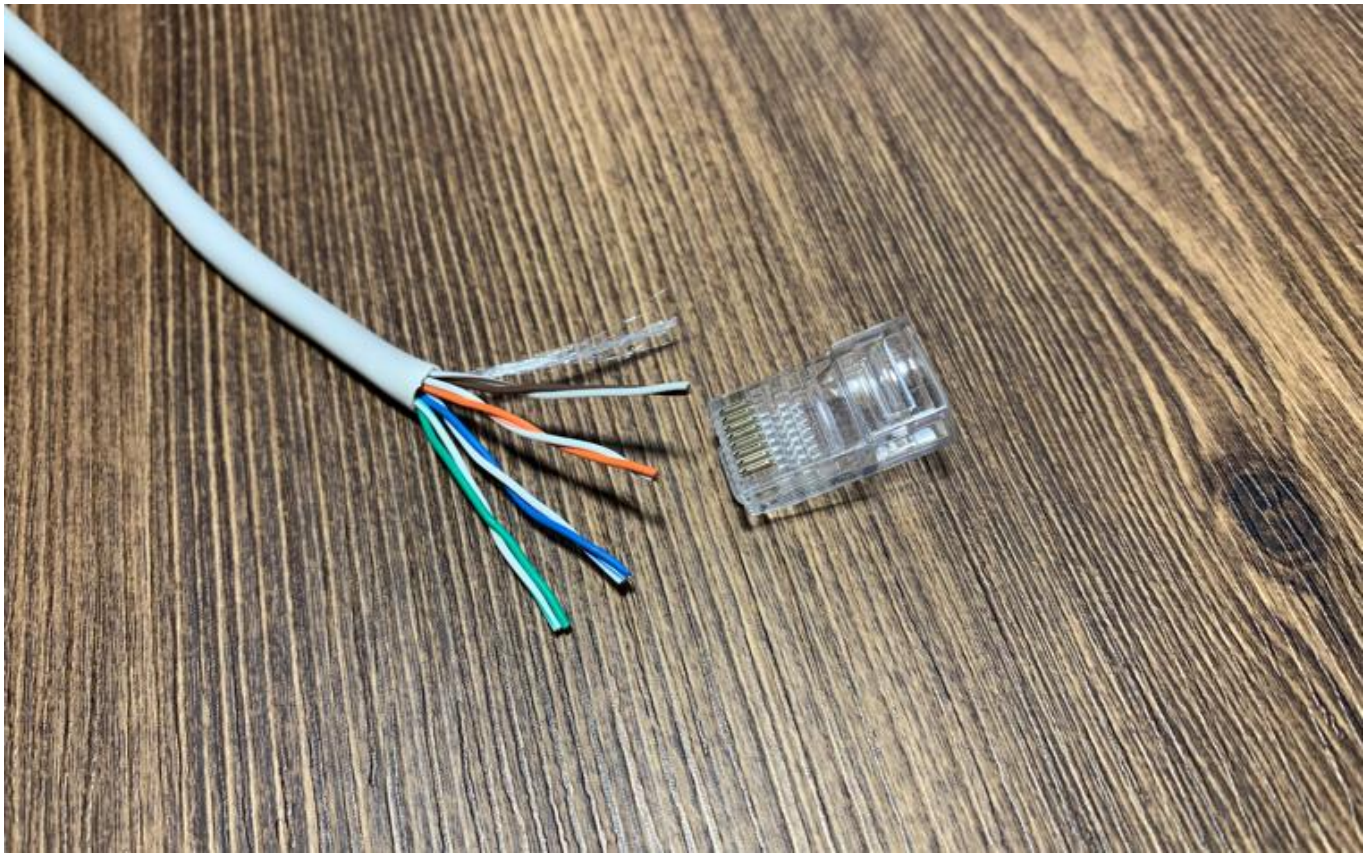
Определяемся со способом обжима витой пары. Например, для соединения типа компьютер-компьютер раньше использовали перекрестное расположение пар в коннекторе. А для соединения компьютера с роутером — прямую распиновку. Сейчас вся техника автоматически перекидывает нужные пары местами и для стандартных задач можно всегда использовать прямой способ обжима:



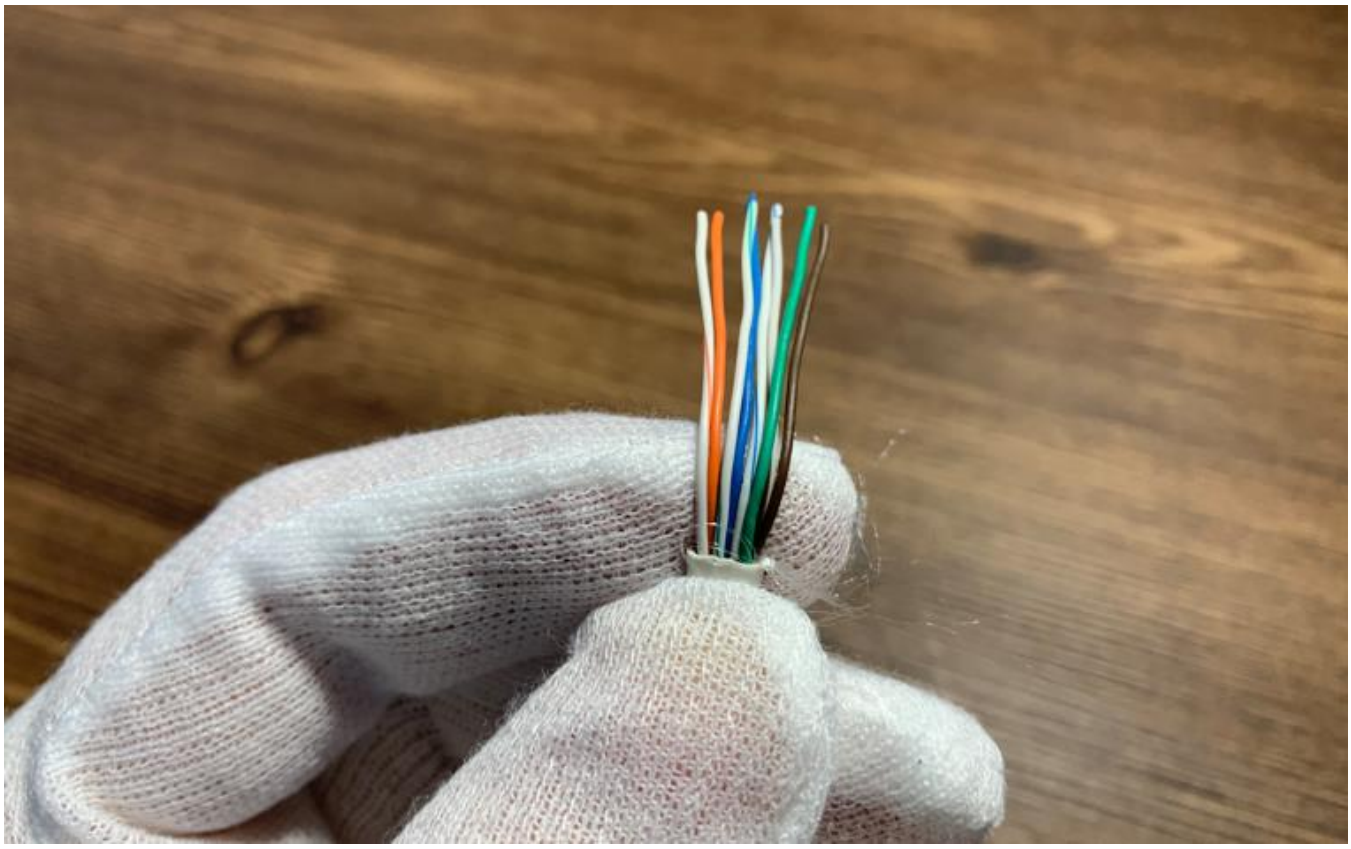
Оба коннектора обжимаются идентично.

Подготовка провода и коннектора

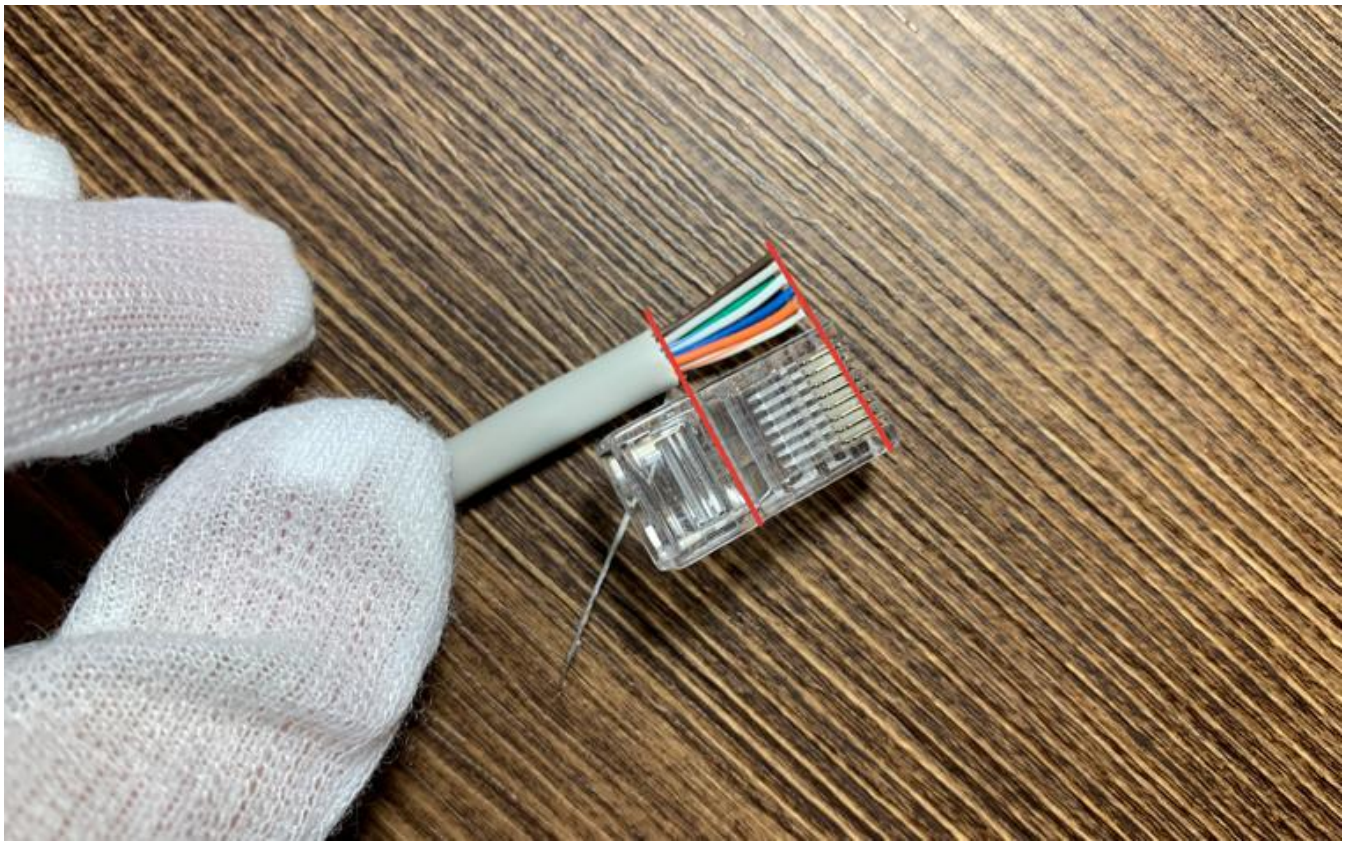
Зачищаем провод примерно на полторы длины коннектора. Стараемся сделать максимально аккуратно, чтобы не повредить оболочку самих жил:



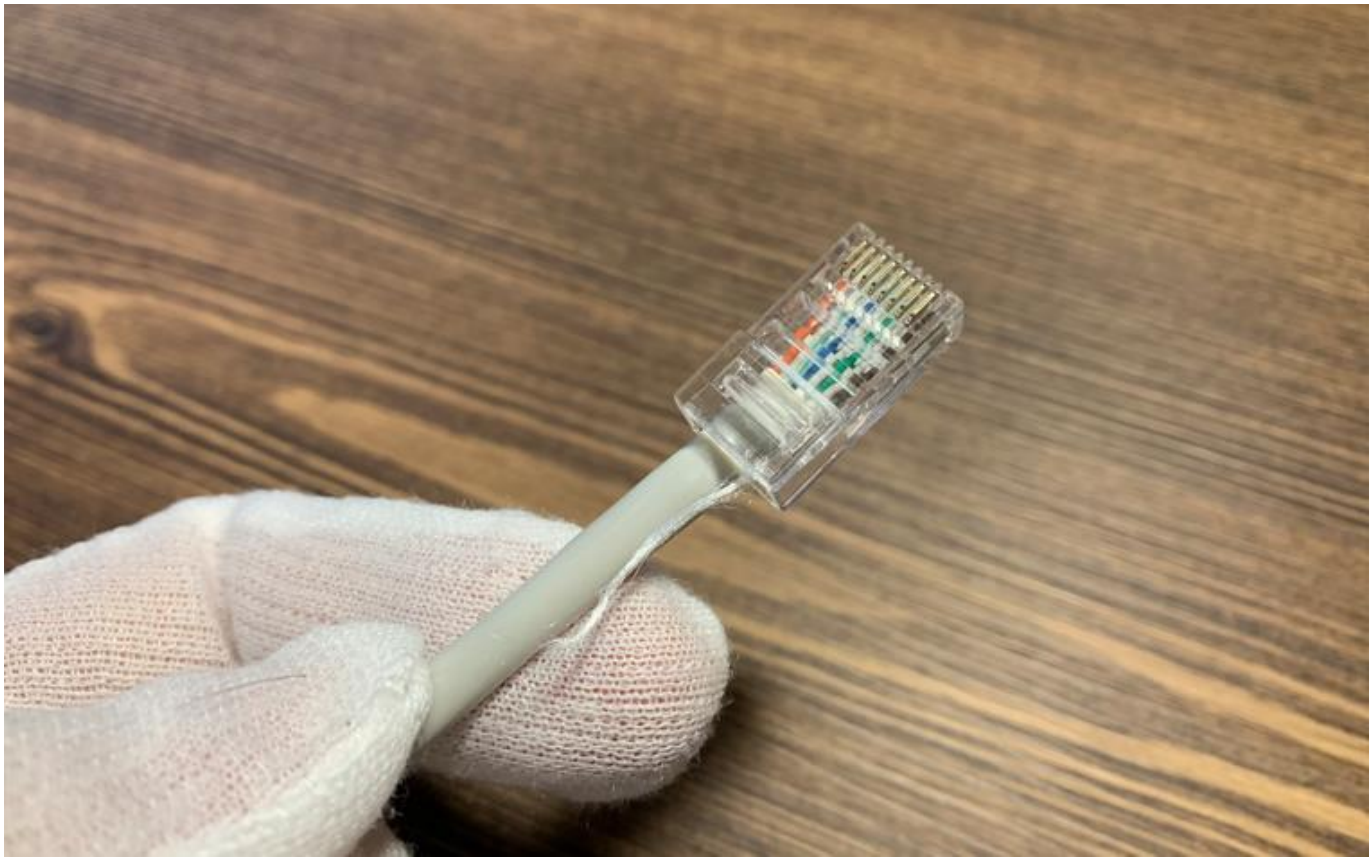
Каждая пара различается по цветам и скручена в определенном порядке. Необходимо раскрутить проводники, но так, чтобы скрытая часть провода под оболочкой оставалась в заводском скрученном виде. Это необходимо для сохранения помехоустойчивости на всех участках провода, вплоть до коннекторов. Не забываем распределить провода по цветам, как показано на схеме распиновки:



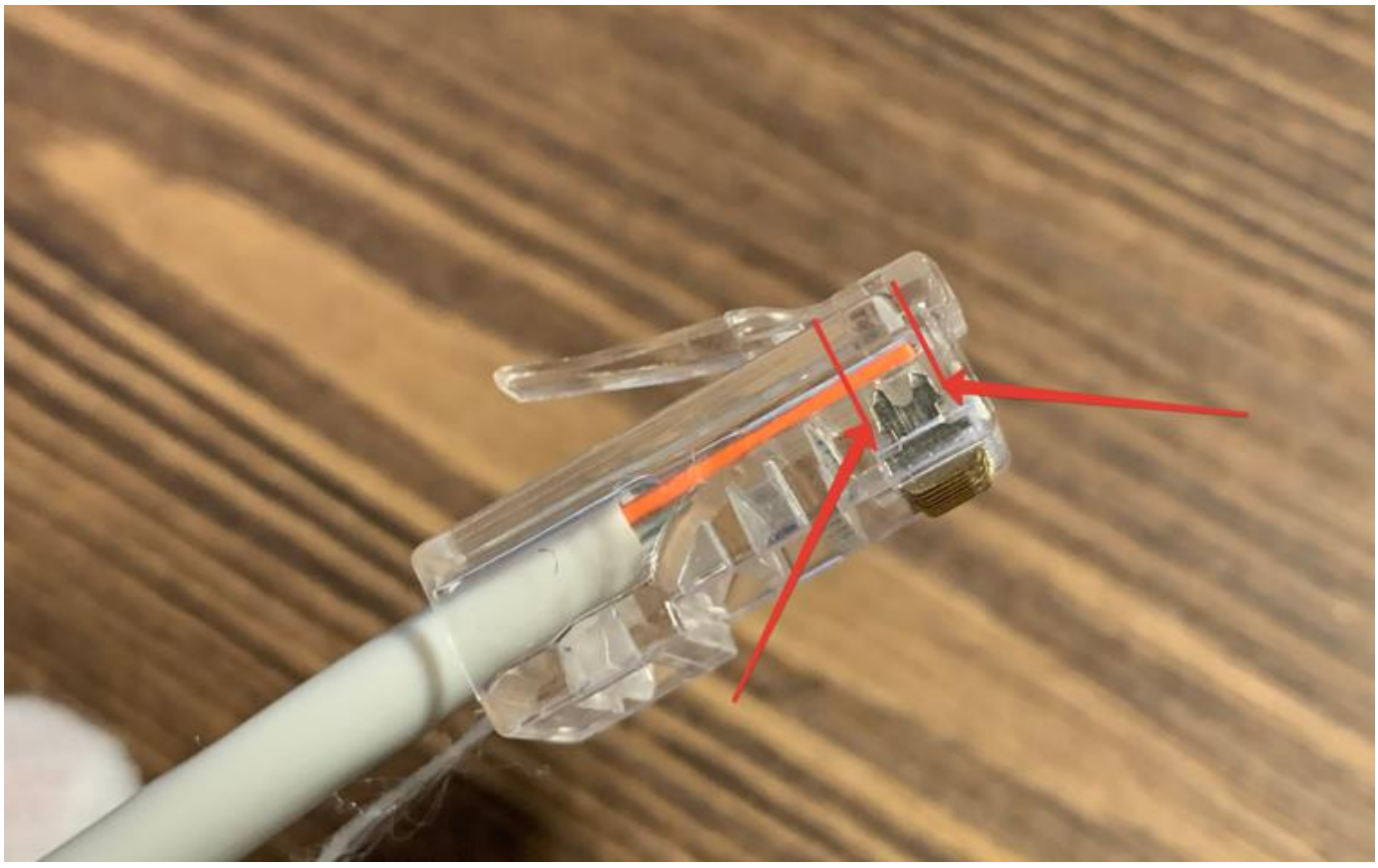
Примеряем провод к коннектору, чтобы определиться с нужной длиной проводников. Красными линиями на фото обозначены границы для оболочки и самих витых пар:



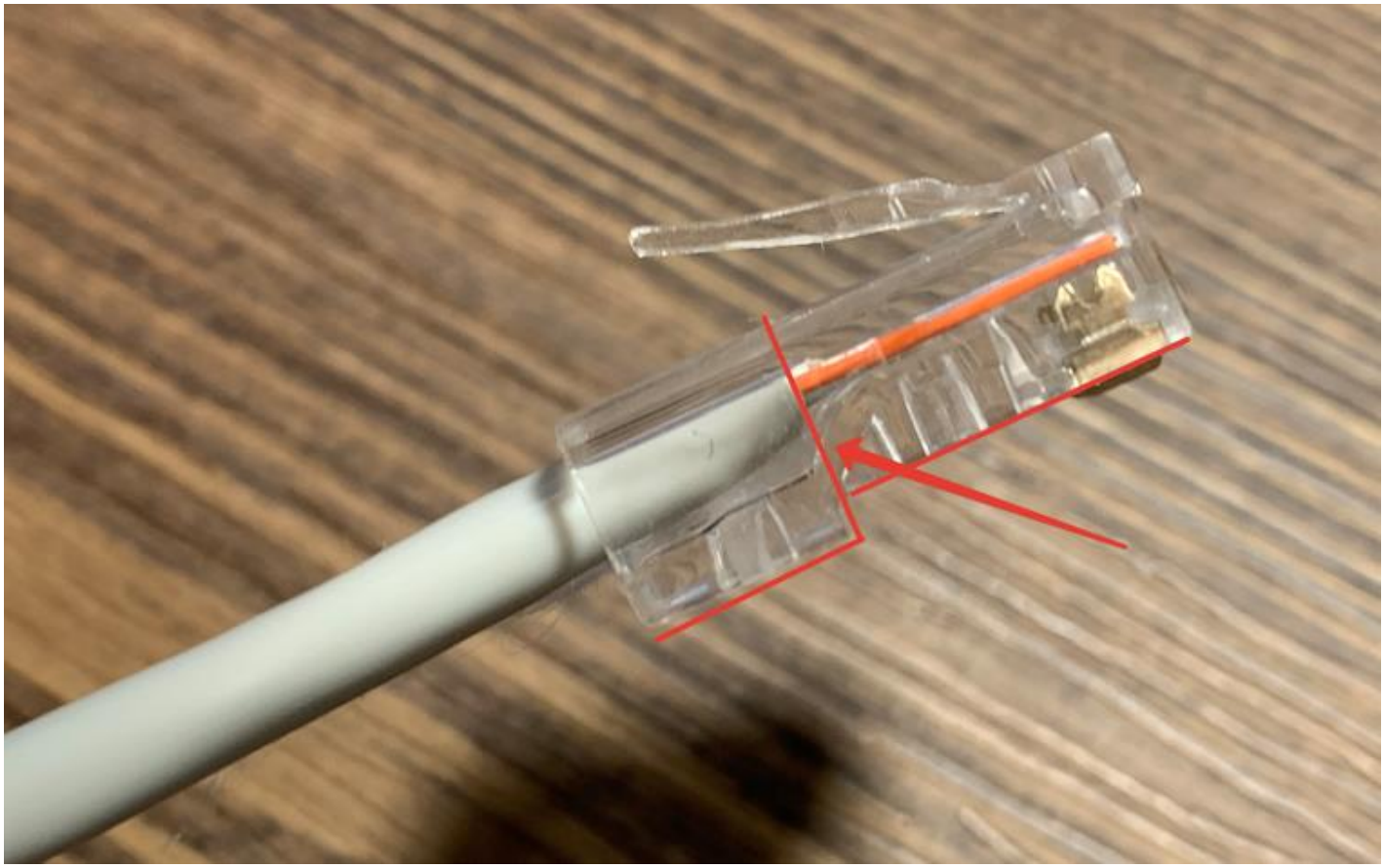
Чтобы удержать пучок в правильном порядке, можно прижать их пальцем возле края оболочки, а затем аккуратно перенести хлипкую конструкцию в коннектор. В нем есть специальные салазки для каждого провода — поэтому после того, как каждый проводник попадет на свою дорожку, просто вставляем кабель до упора. Не забываем отвести в сторону нейлоновую нить:



Обязательно следим, чтобы все пары достигли крайних точек в салазках и полностью накрылись ножами контактов:



Оболочка провода должна также достигнуть сужения в месте, где начинаются салазки, чтобы одноразовая защелка полностью накрыла своей плоскостью широкую часть провода:

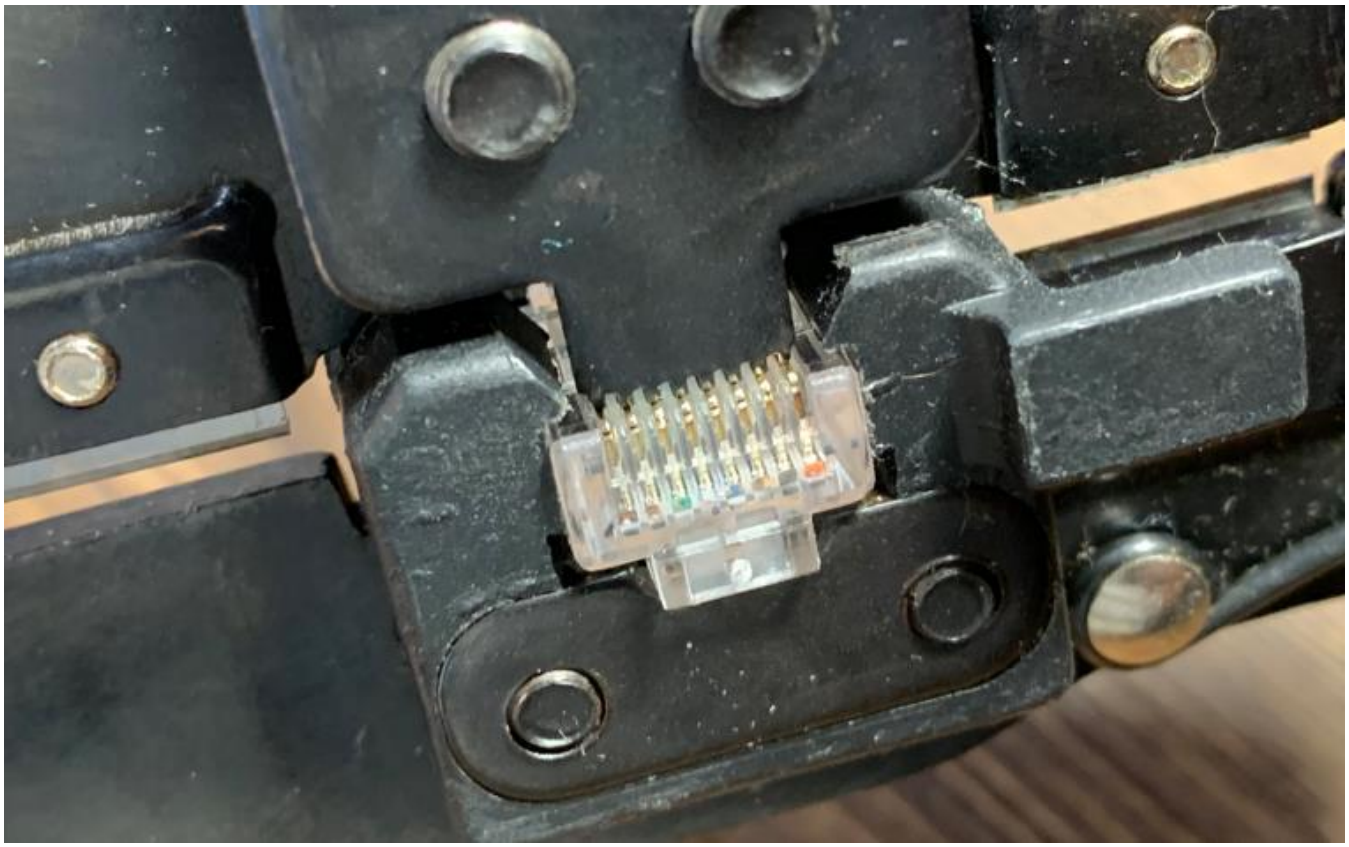


Обжим

Убеждаемся в качестве подготовки конструкции и переносим ее в рабочий паз инструмента. В обжимной каретке присутствуют ограничитель и защита от неправильного положения коннектора — не спешим и делаем внимательно:

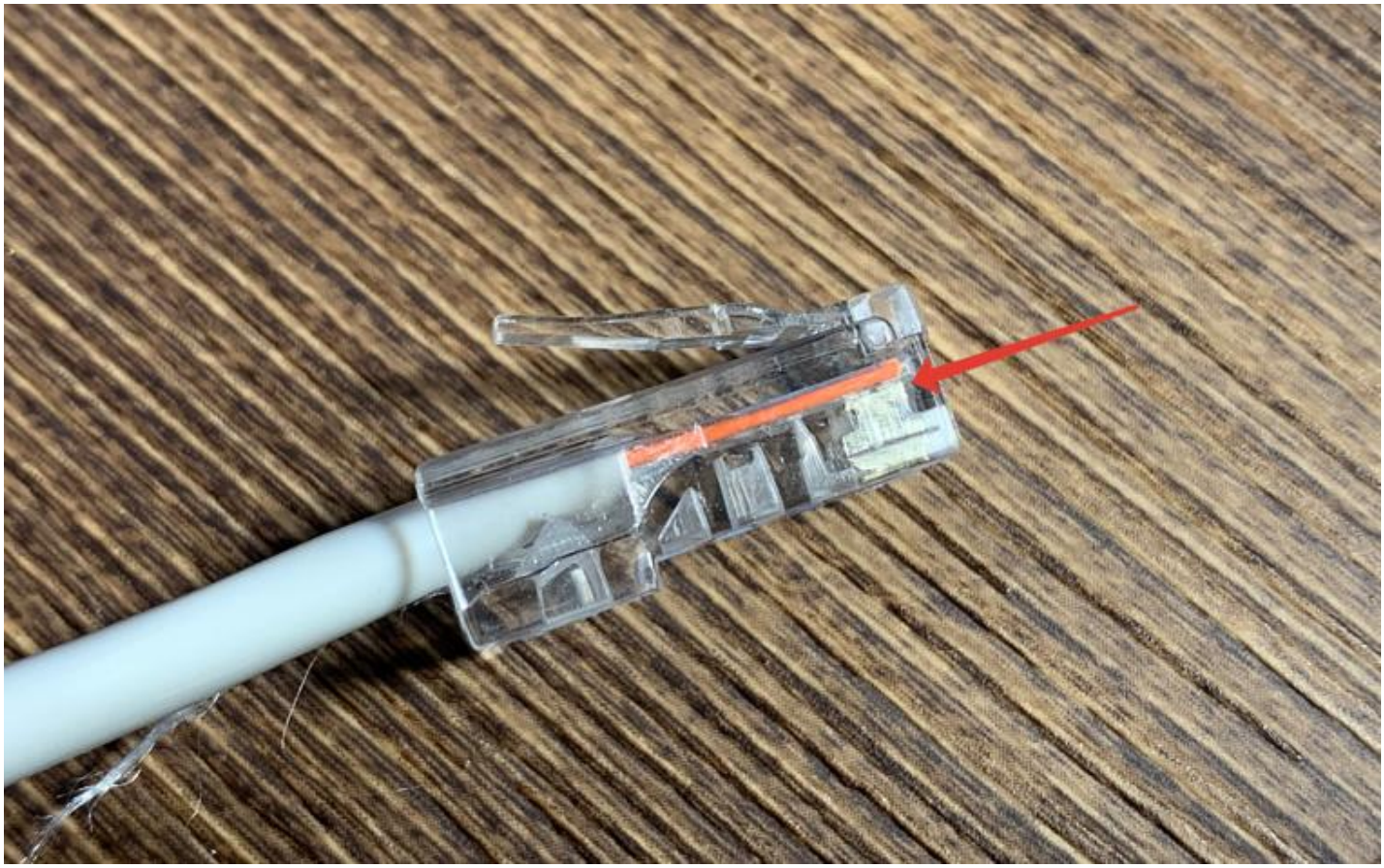
Когда коннектор окажется в правильном положении в инструменте, сжимаем ручки кримпера практически до упора, после чего будет слышен щелчок — сработает стопор оболочки в коннекторе:

Зубцы кримпера имеют одинаковый шаг и соответствуют контактам в коннекторе. При сжатии ручек они попадают в пазы с контактами и продавливают их через оболочку проводников:

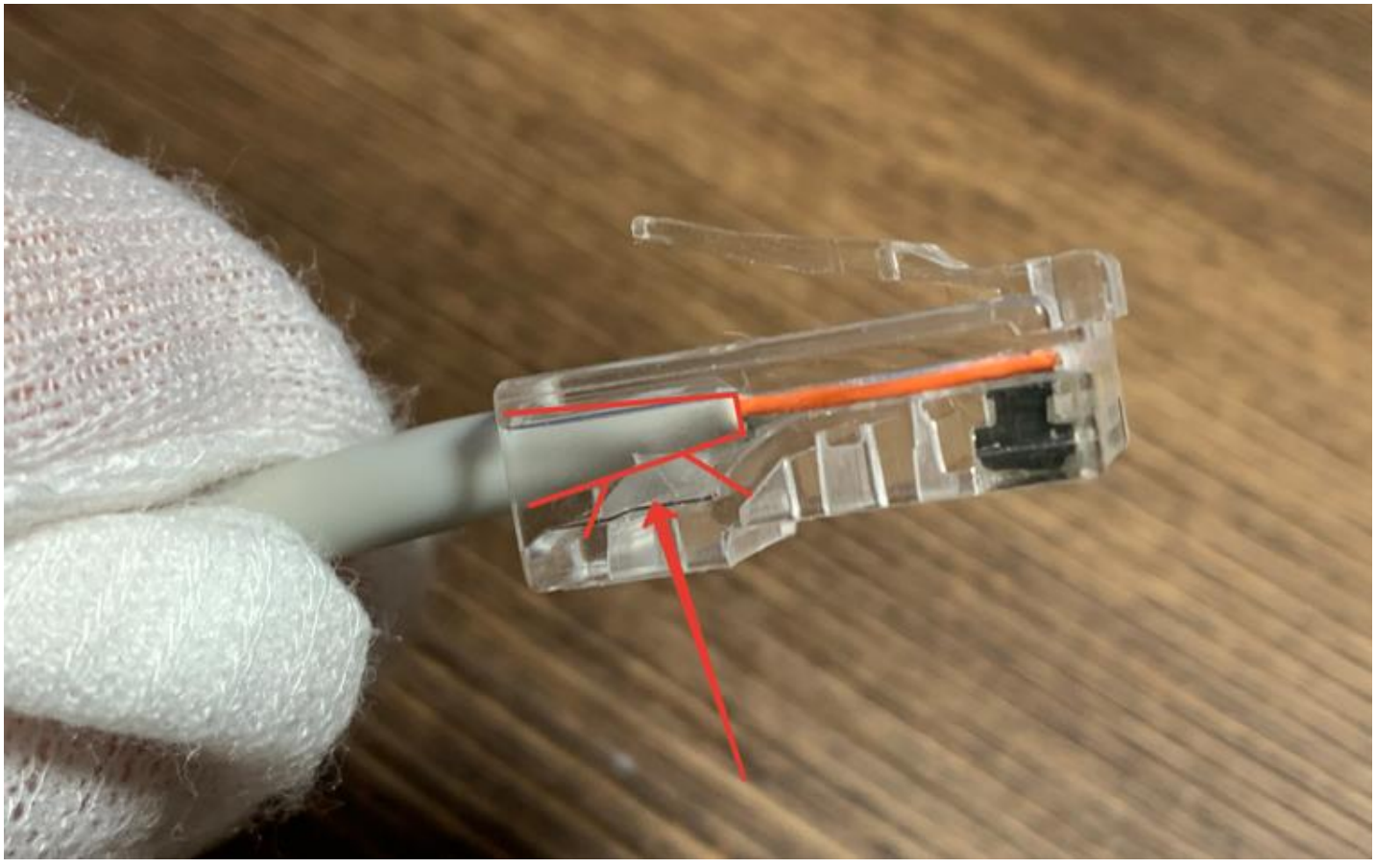


Проверка качества

Вынимаем готовый провод и проверяем качество обжима. Во-первых, убеждаемся в том, что ножи полностью «врезались» в провода:



Во-вторых, проверяем качество фиксации оболочки провода в коннекторе:

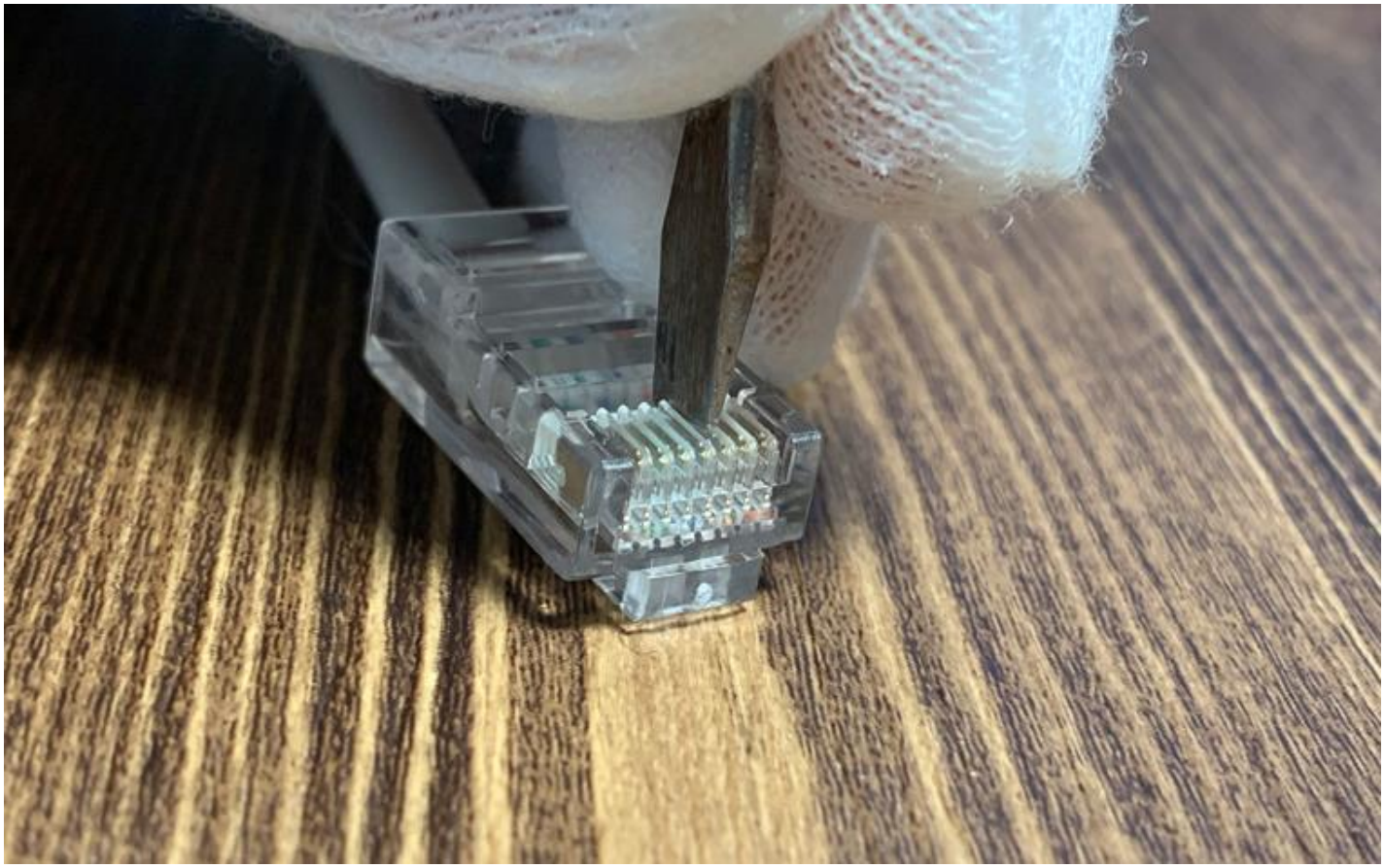


Если один из контактов не достает до проводника, то можно сделать «контрольный» обжим в кримпере или использовать секретный инструмент.

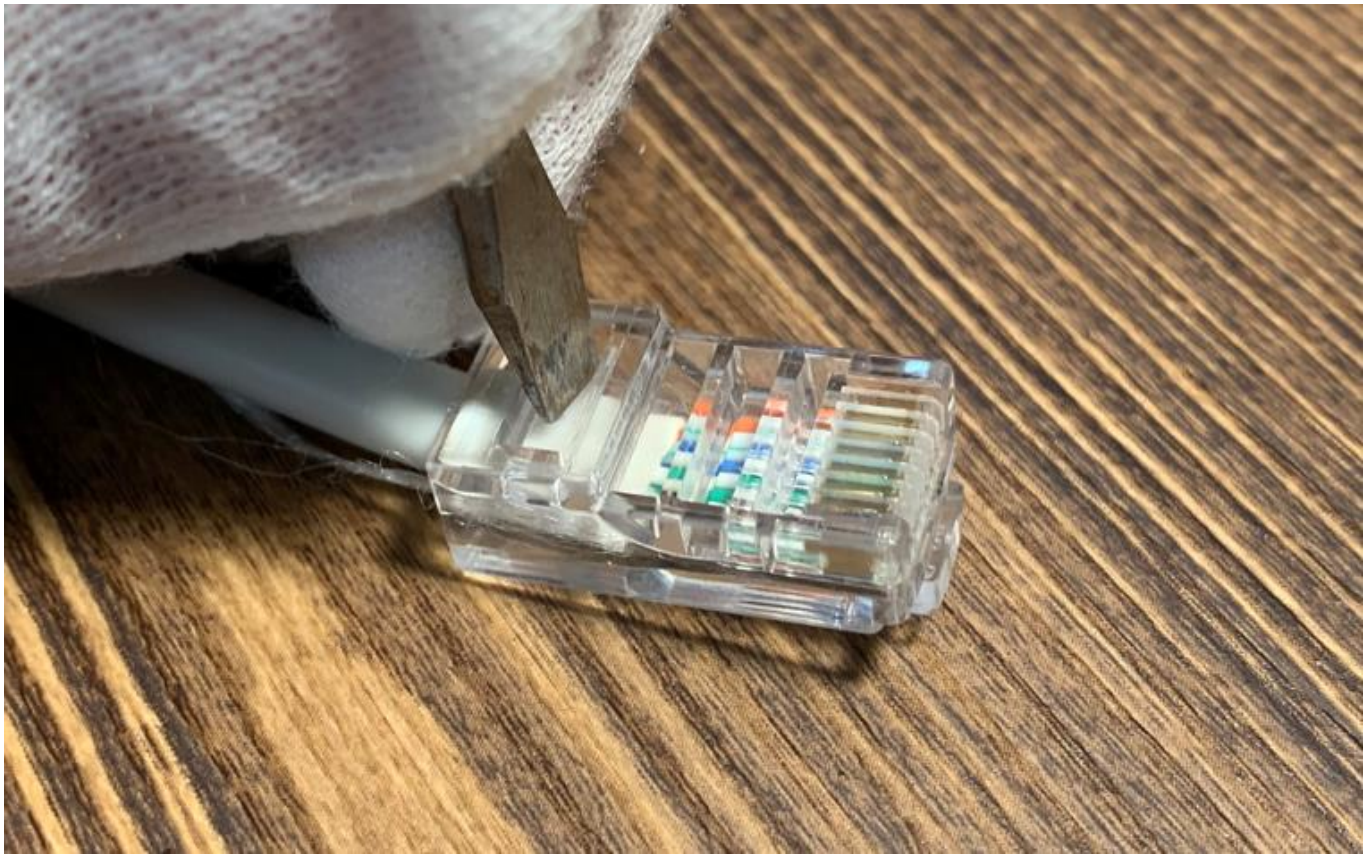
Доработка

Бывает, что некоторые зубцы кримпера не достают до каждого контакта в одинаковой степени и оставляют часть пар без контакта. Для этого необходимо настроить обжимную каретку, которая подвижна и регулируется с помощью фиксирующих болтов. Однако, можно быстро исправить положение с помощью секретного инструмента — отвертки. Просто дожимаем нужный контакт плоскостью:

Нажимаем с силой, аккуратно, без ударов по отвертке, не расшатывая контакт, чтобы ножи прорезали оболочку проводника и соединились с медными проводниками. Впрочем, так можно обжать весь провод, если под рукой нет кримпера. Долго и неудобно, но осуществимо:



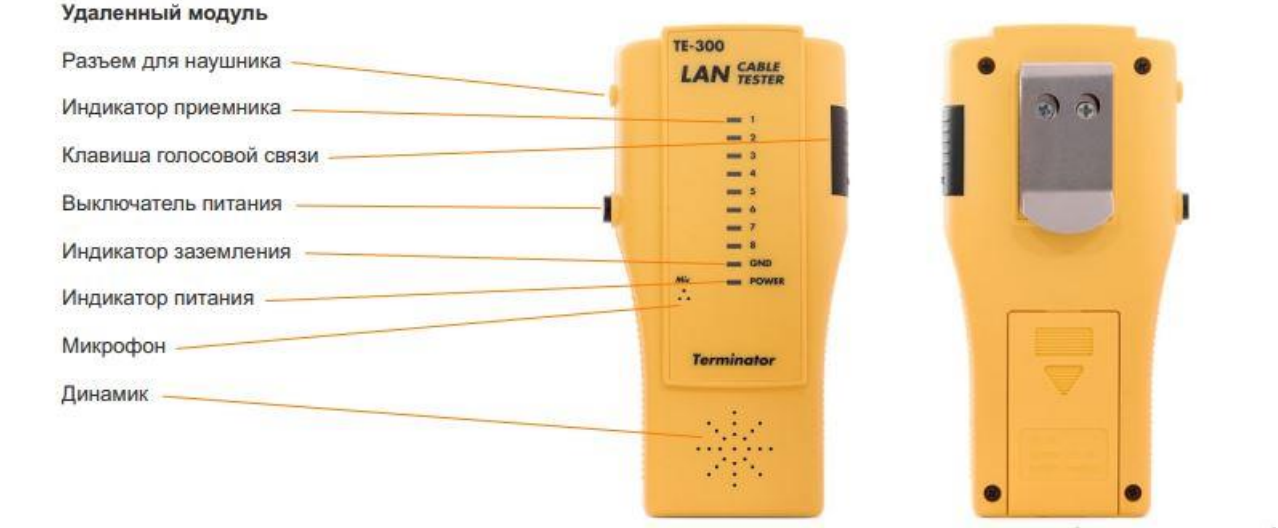
То же самое с защелкой для оболочки — давим до щелчка:



Проверяем работу

Для проверки можно использовать специальный тестер, который находит обрывы, короткое замыкание и проверяем распиновку обжима.

Удаленный модуль

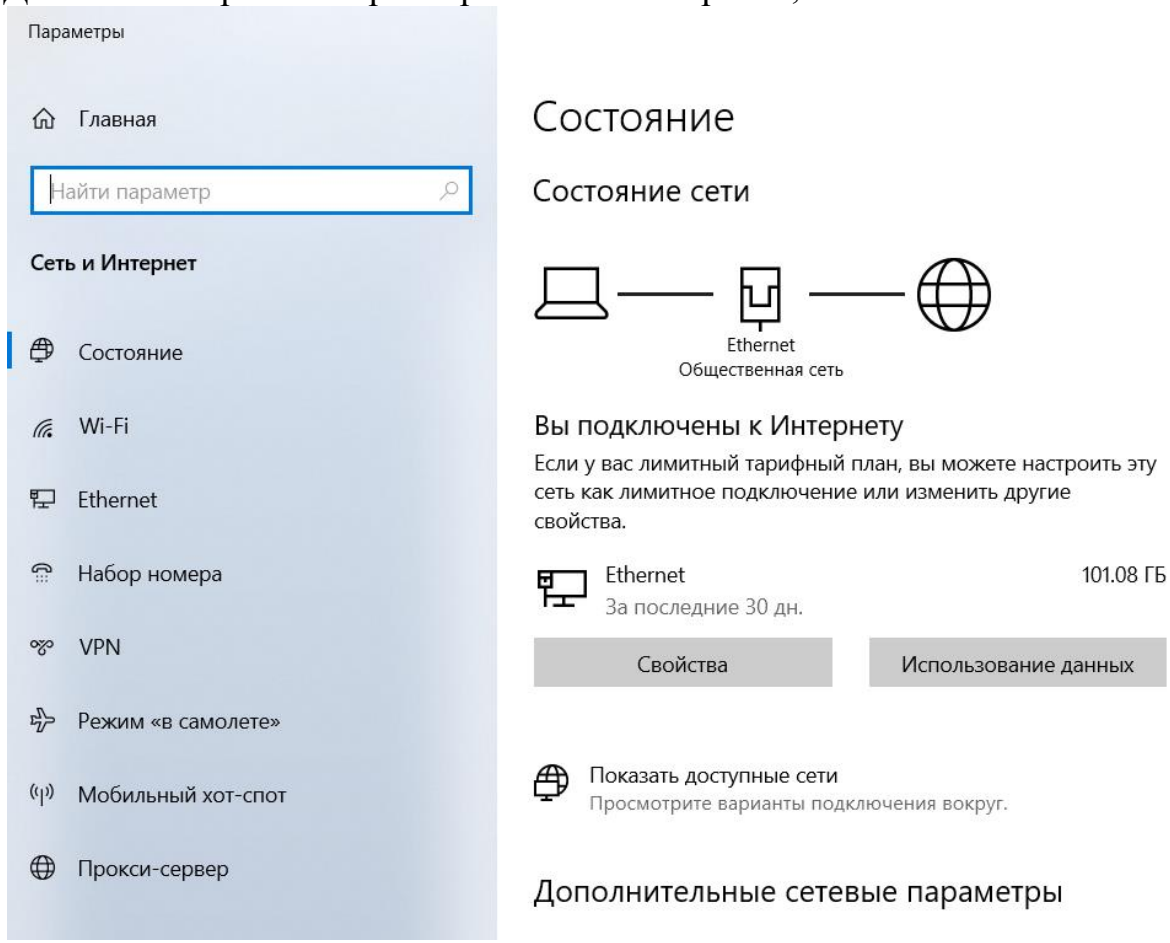


Без спецтехники тоже можно обойтись — подключаем компьютер к роутеру с помощью нового кабеля и ждем подключения:


4
3
2
1
0
0
SFP

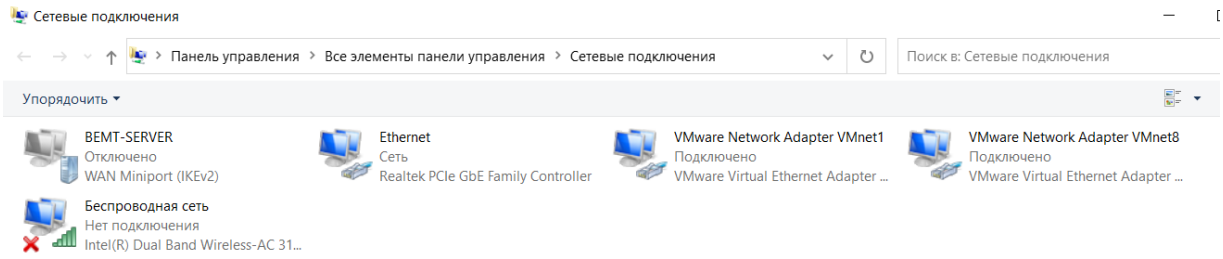
2. Настройка IP-адресации на сетевом интерфейсе.

Для функционирования сети необходимо задать правильные сетевые параметры. Для этого открыть «Параметры сети и Интернет»,

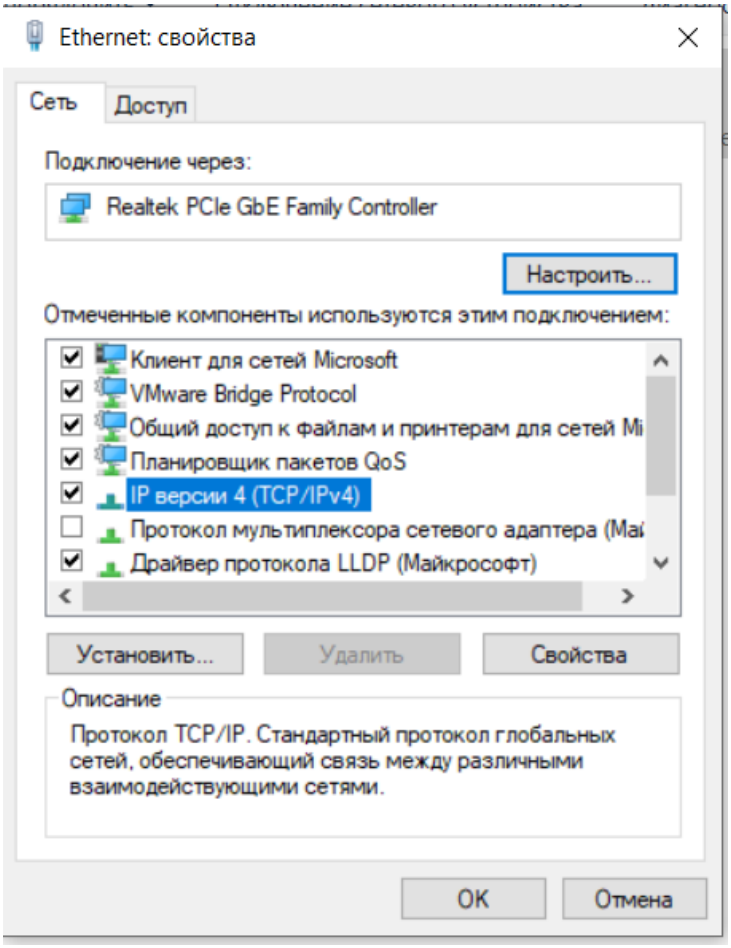


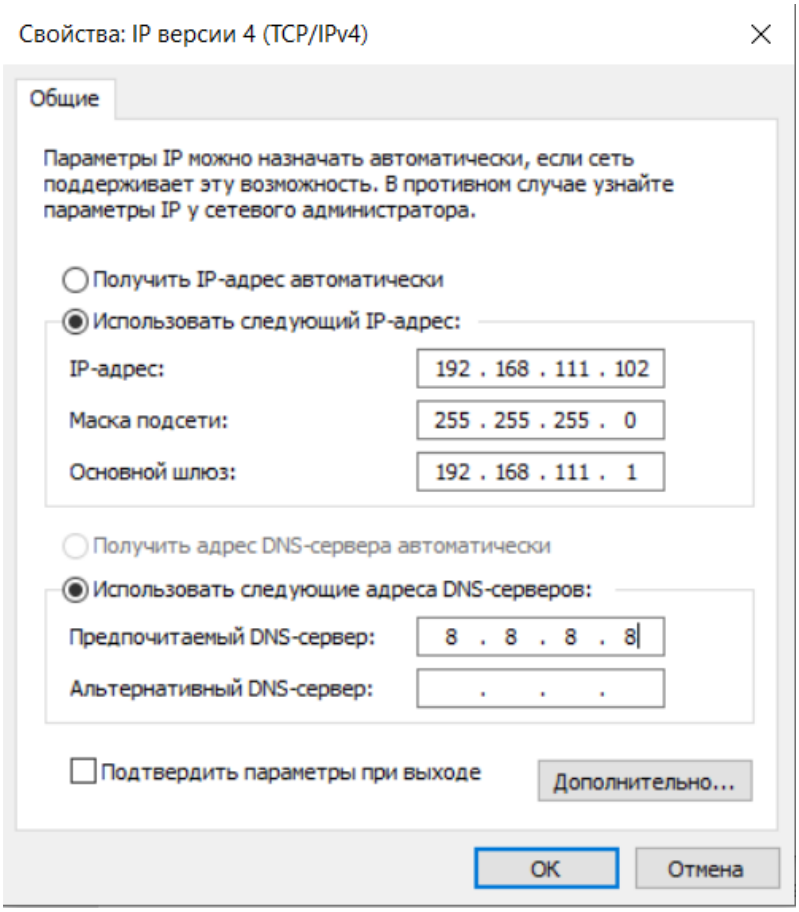
далее выбрать пункт «Настройка параметров адаптера»

Выбрать нужный сетевой адаптер и открыть его свойства.

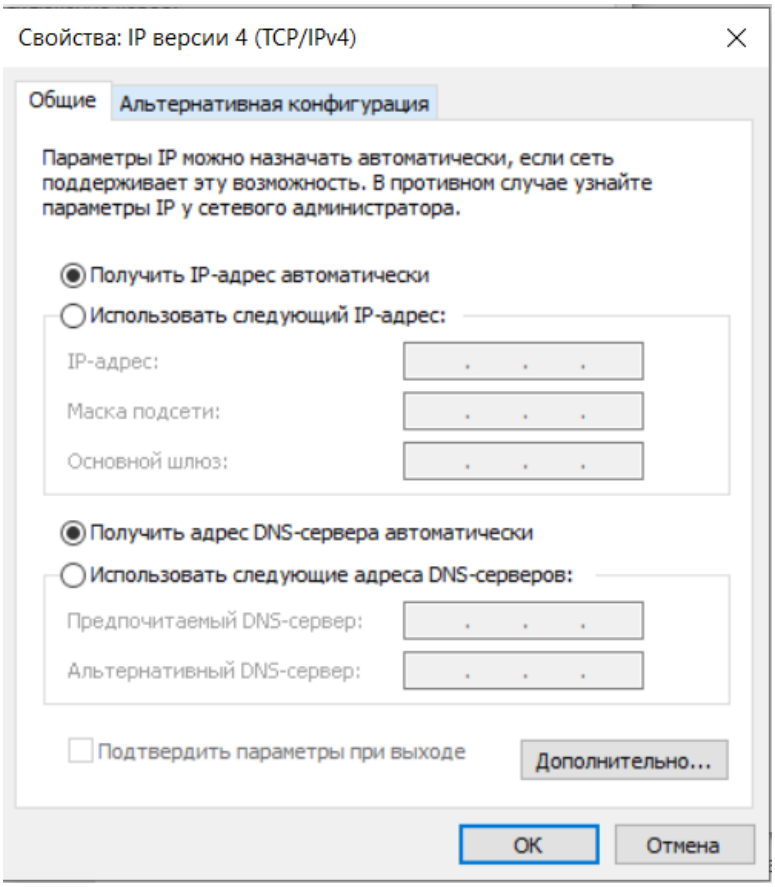


Кликнуть дважды в пункте IP версии 4(TCP/IPv4)





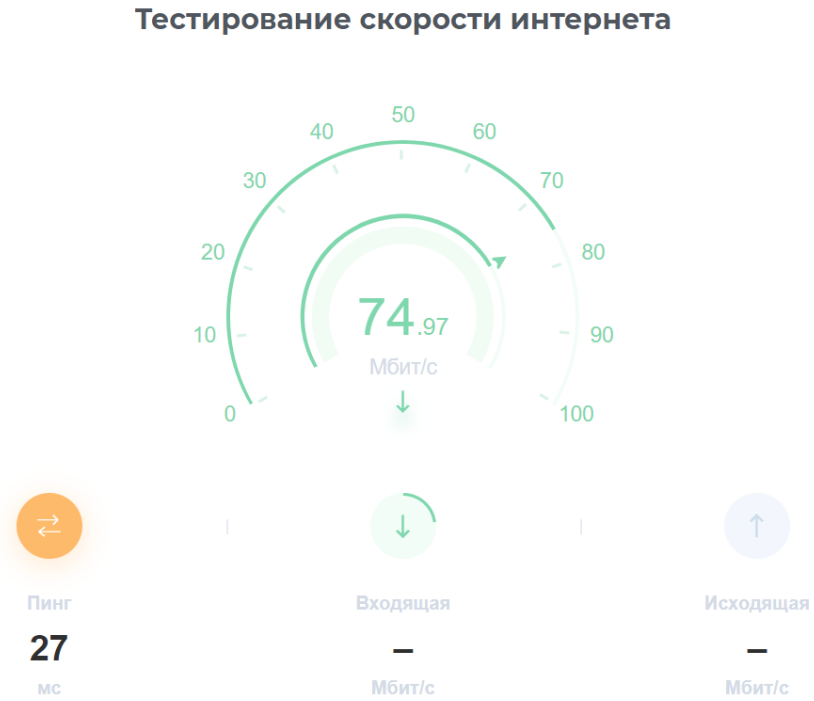
Для получения корректных сетевых параметров включить пункты «Получить IP адрес автоматически» и «Получить адрес DNS-сервера автоматически»



Далее везде нажать кнопку OK и убедиться что сетевой интерфейс получил правильные сетевые параметры. Значок  внизу экрана.

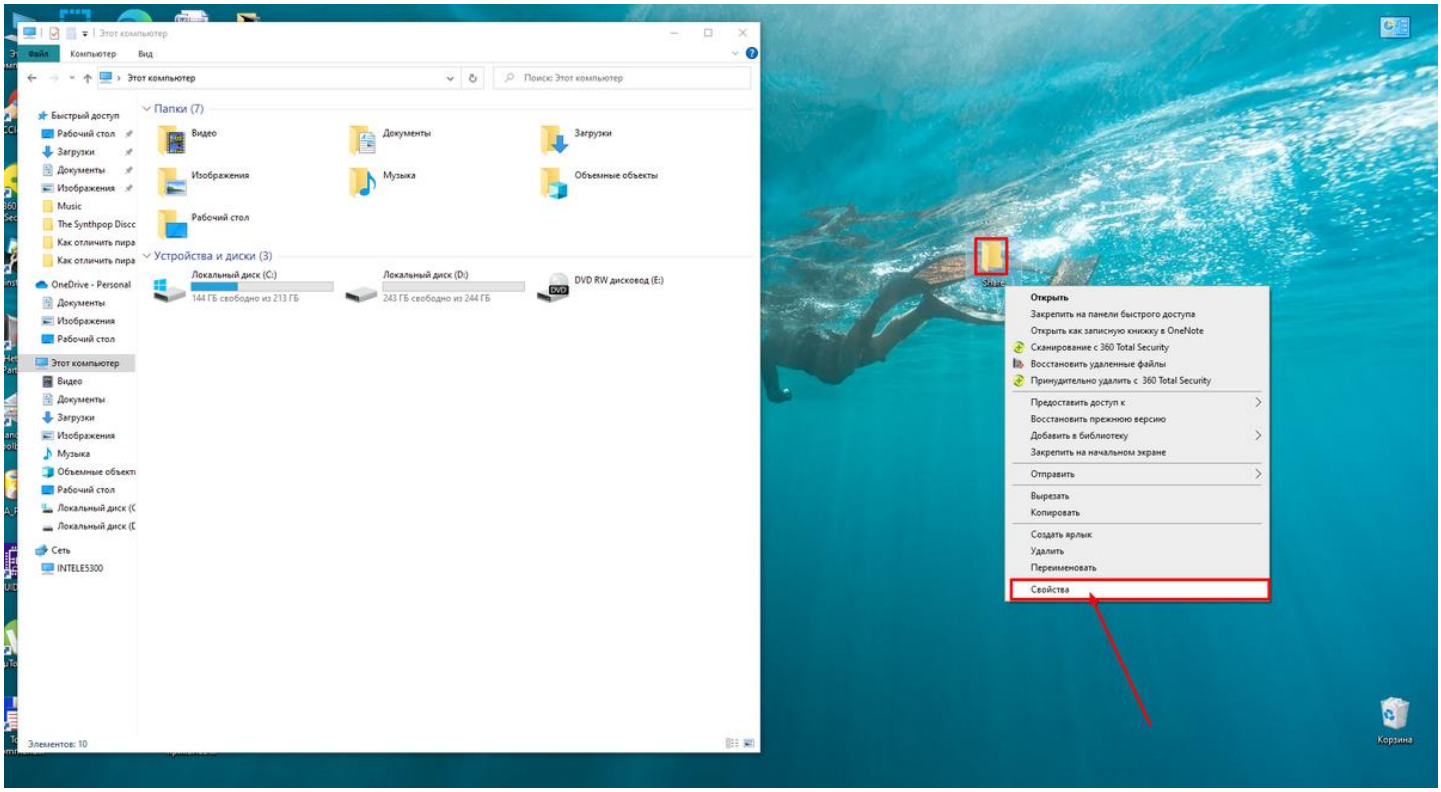
3. Проверка скорости интернет соединения.

Затем открываем браузер и проверяем скорость интернет соединения на сайте 2ip.ru в разделе Тесты – Скорость интернет соединения.



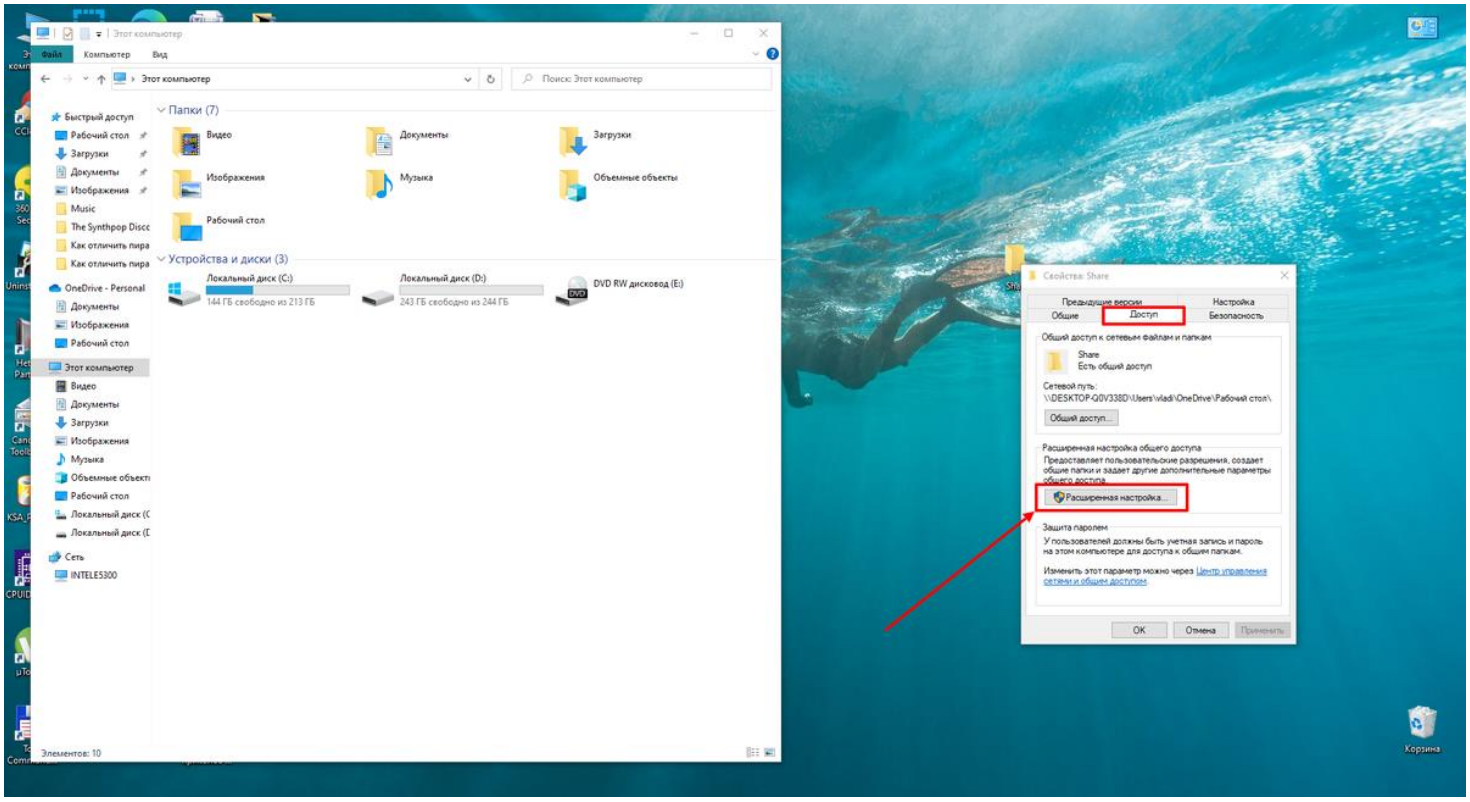
4. Настройка общего публичного каталога на Windows

Придумываем название нашей папке и наделяем полномочиями пользователей



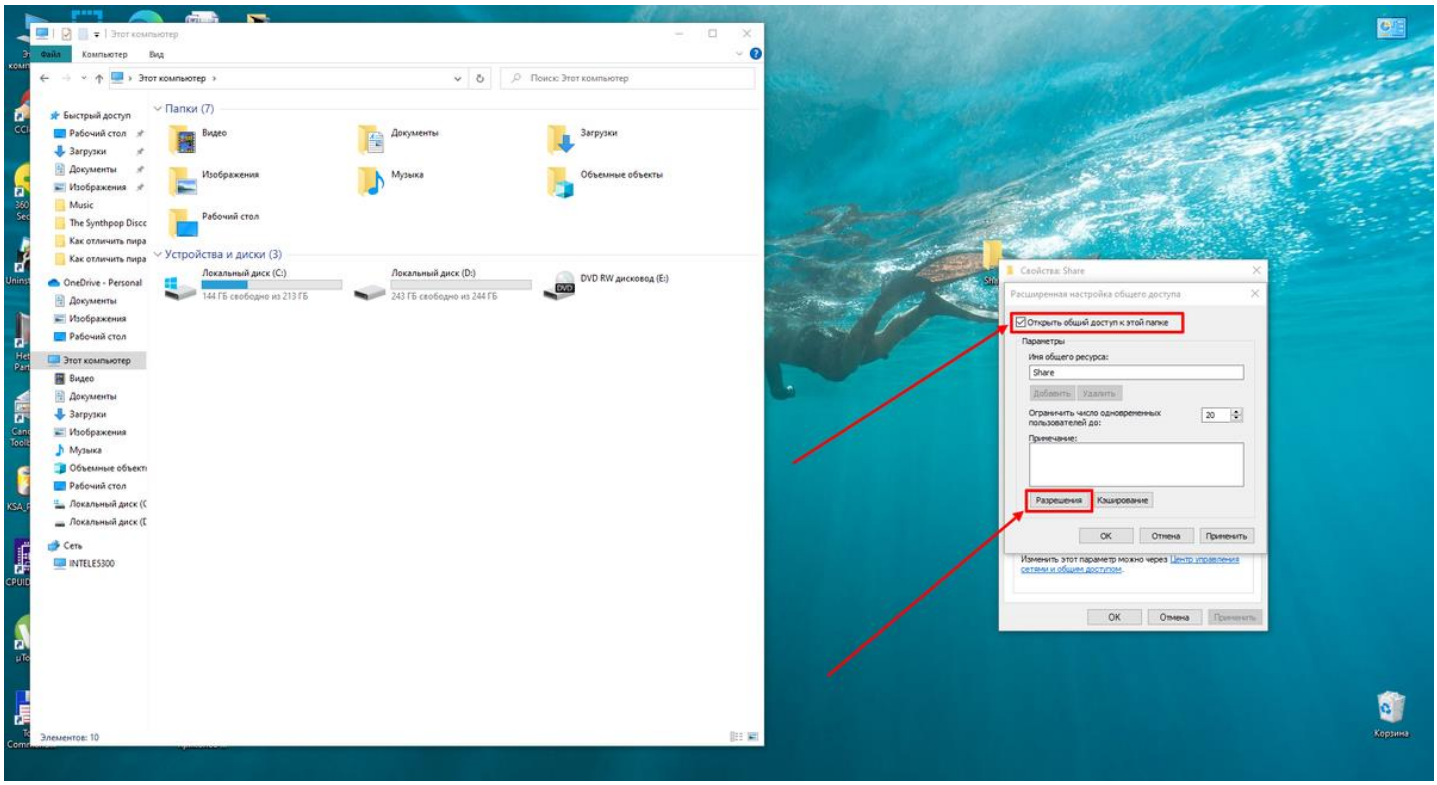
Переходим в свойства нашей новой папки

- В открывшемся меню идём во вкладку "Доступ", далее в "Расширенные настройки".



Переходим в "Расширенные настройки" нашей новой папки

- Ставим отметку в виде галочки напротив пункта "Открыть общий доступ к этой папке" и дальше отправляемся в директорию "Разрешения".

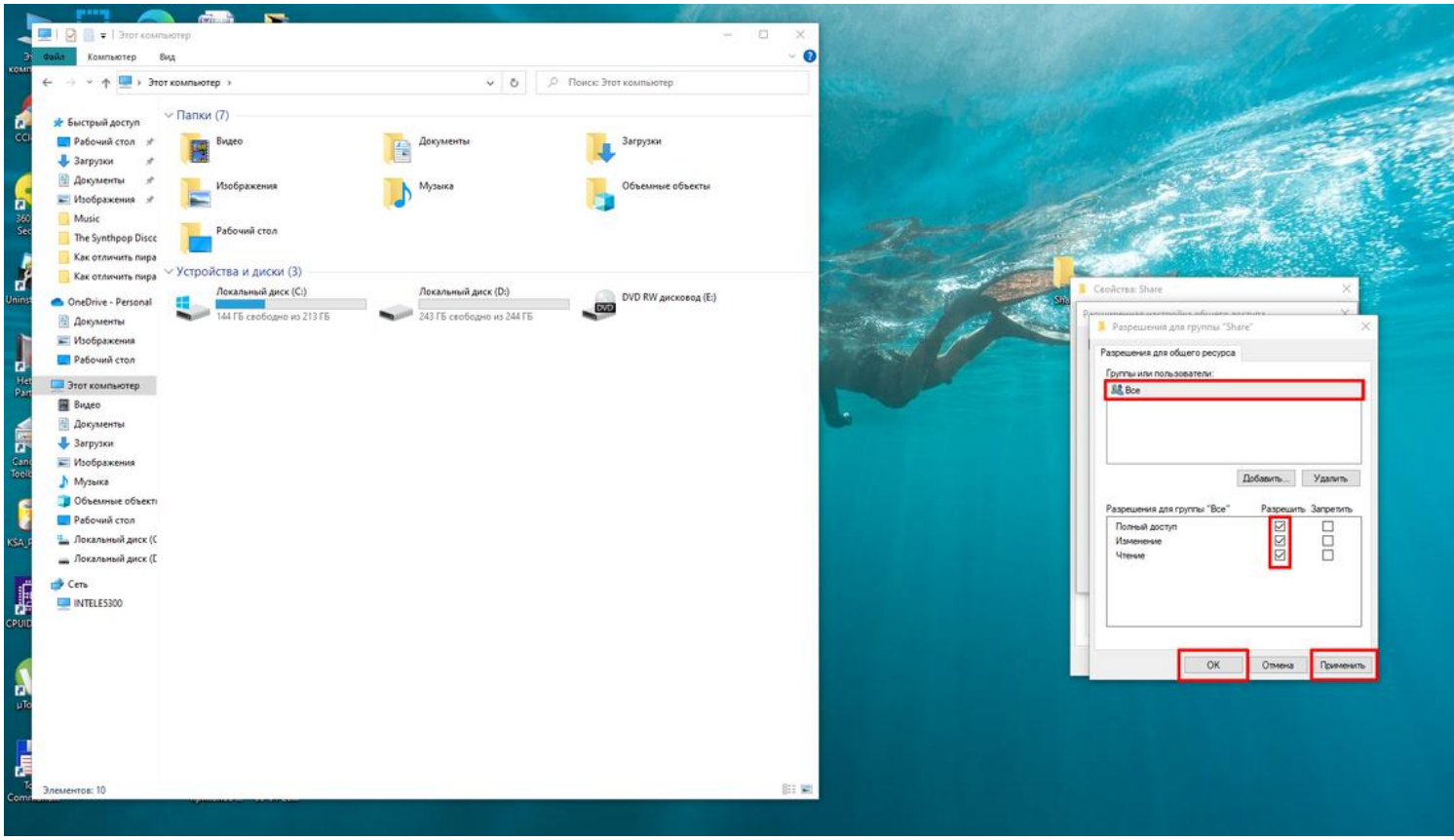


Открываем общий доступ к нашей папке и переходим в "Разрешения"

По умолчанию стоят пользователи "Все". И разрешено им пока только "Чтение". Установив галочки на следующих пунктах — "Изменение" и "Полный доступ", вы откроете для всех участников уже полные возможности. Участники - это пользователи и мы показываем просто на примере

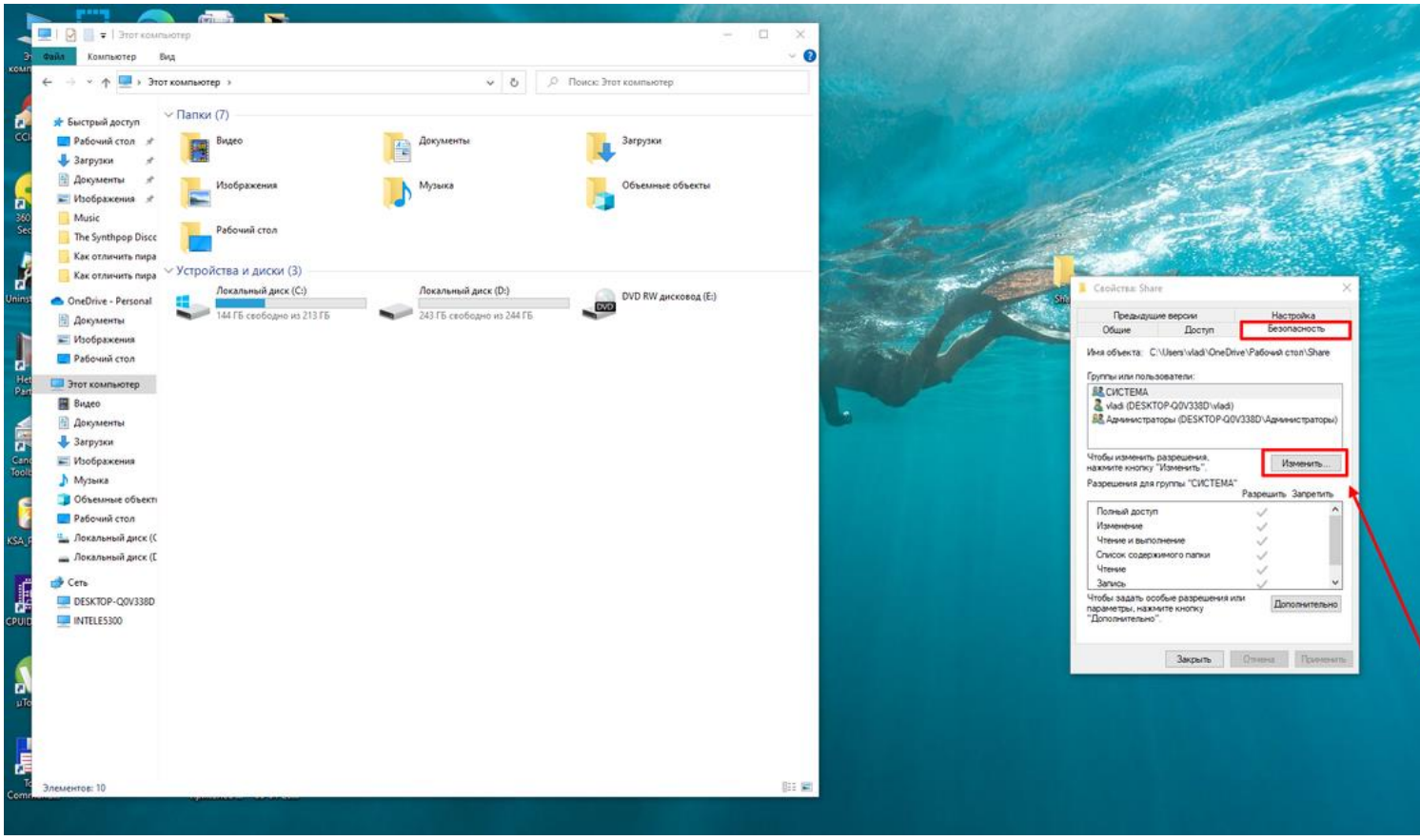
пользователя "Все", а вы можете наделять полномочиями именно ваших пользователей, ведь их имена известны только Вам.

Через кнопки "Добавить" и "Удалить" вы сможете добавлять новых пользователей и удалять тех, кто уже не является участником группы и вы не хотите, чтобы они имели доступ к этой папке. Также можно и ограничить их возможности, оставив галочку только напротив пункта "Чтение" или вовсе запретить через соответствующие окошки. Везде подтверждайте свои действия кнопками "Применить" и "ОК".



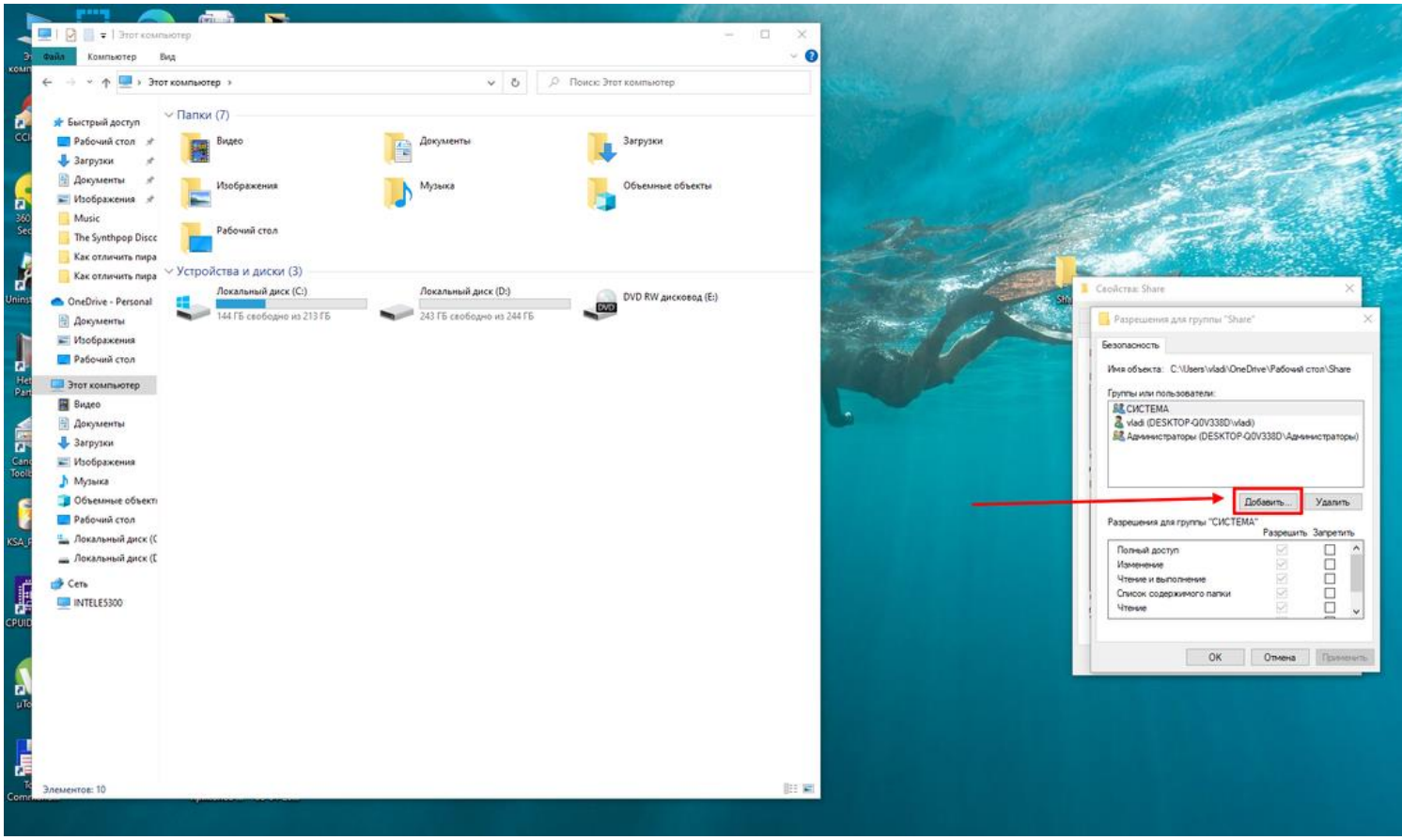
Даем полный доступ на примере пользователя "Все"

- Теперь, подтвердив всё, возвращаемся к своей папке, но переходим уже во вкладку "Безопасность". И там нам надо нажать на кнопку "Изменить".

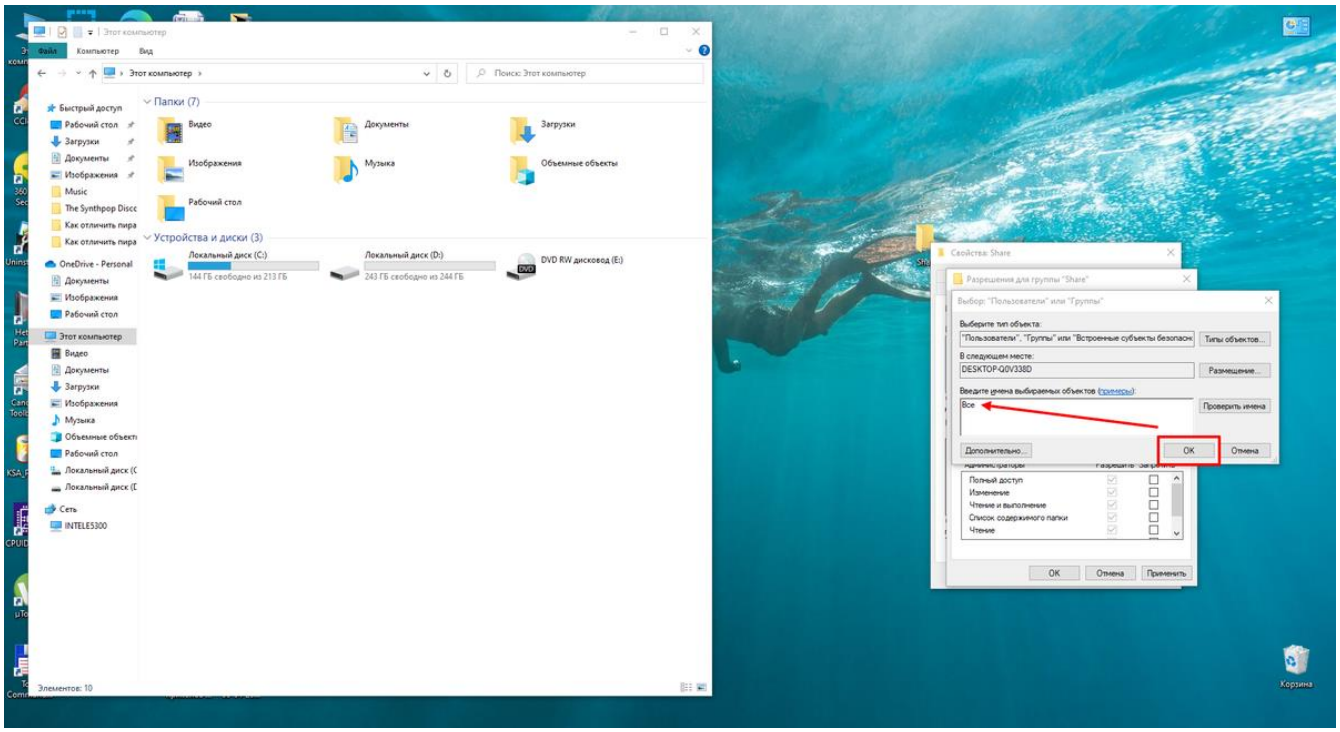


Переход к изменениям разрешений выбранного нами пользователя

- Там нужно добавить нашего пользователя под именем "Все". Вы же добавляете своего.
- Пишем вручную слово "Все" (только без кавычек и с большой буквы). После нажимаем "ОК".

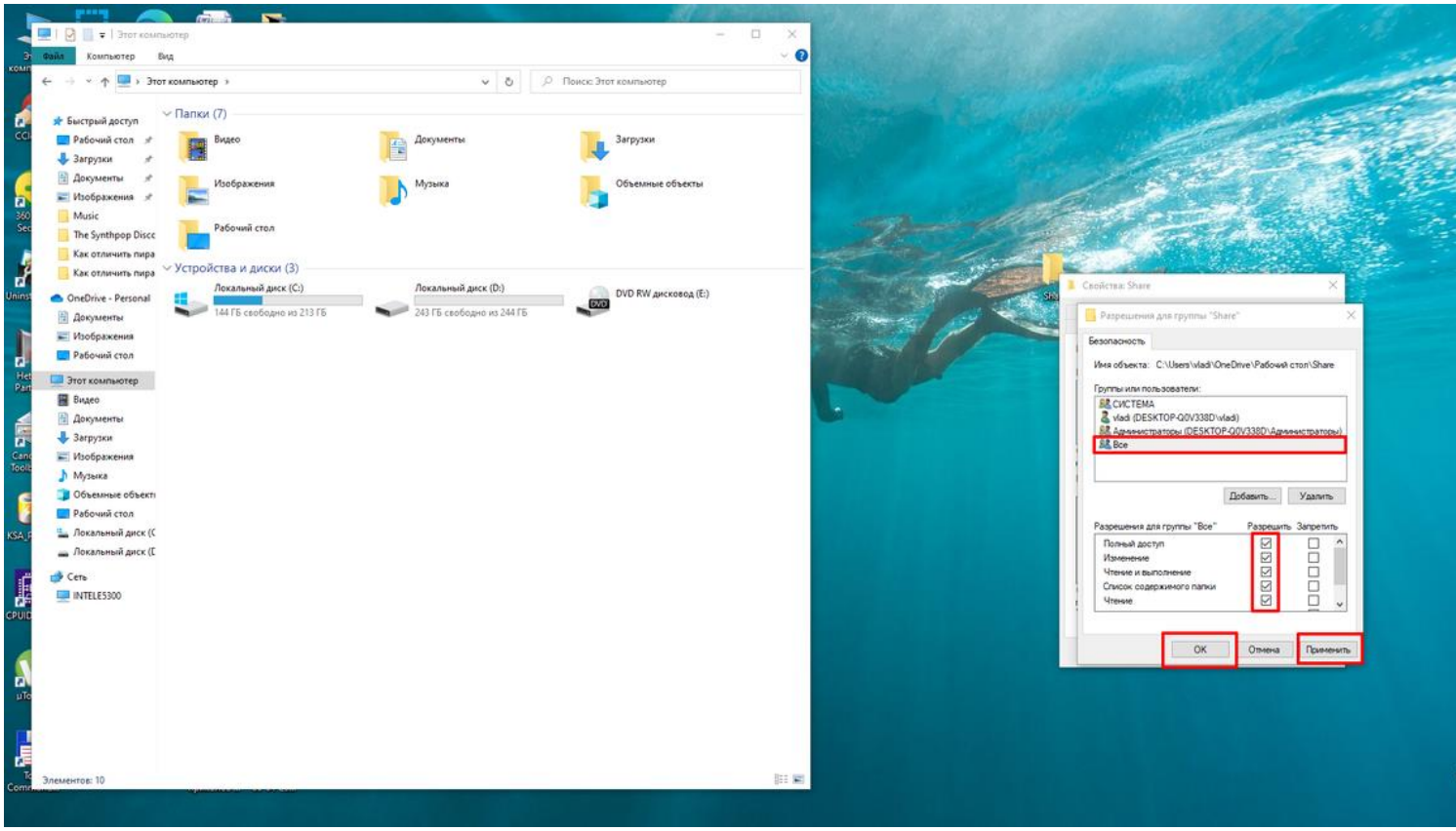


Добавляем необходимого нам пользователя

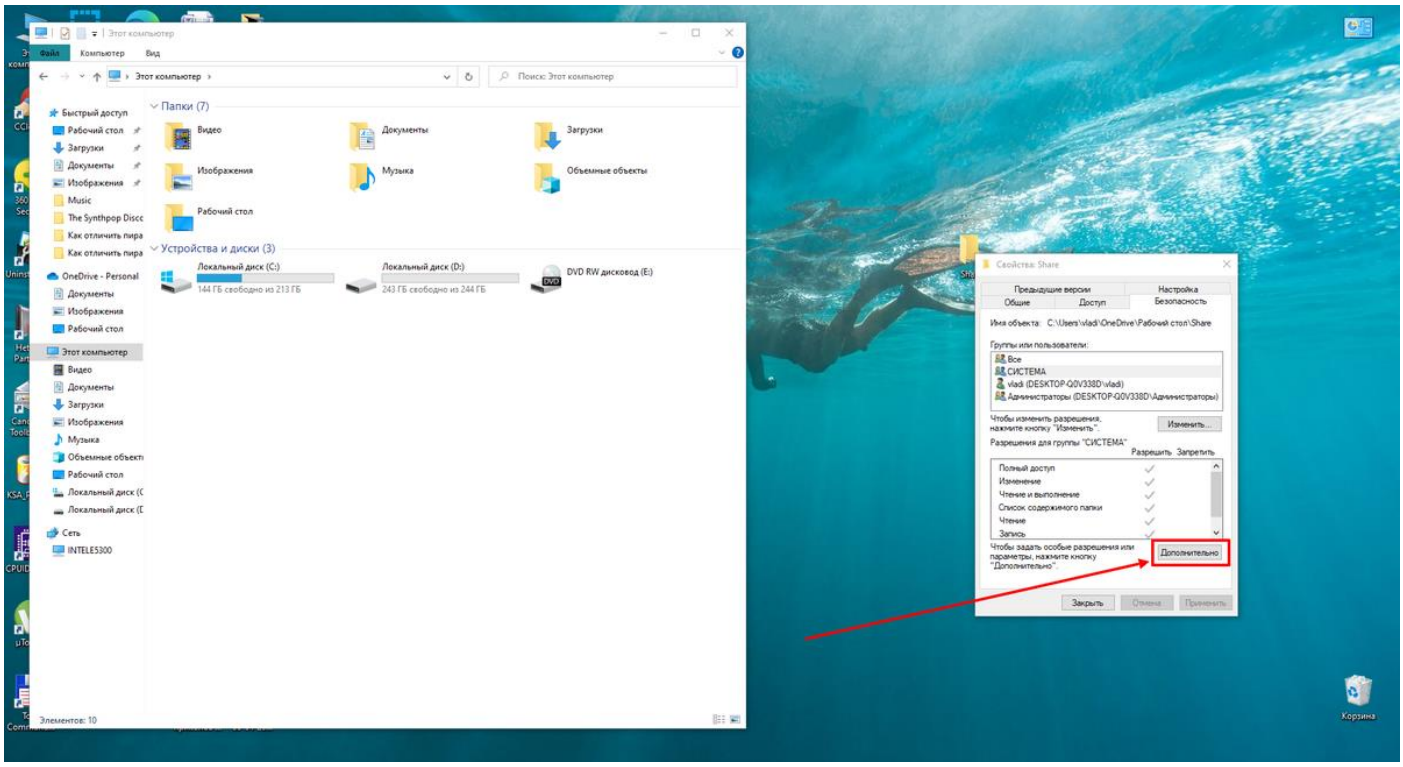


Вводим имя пользователя, которого Вы хотите добавить

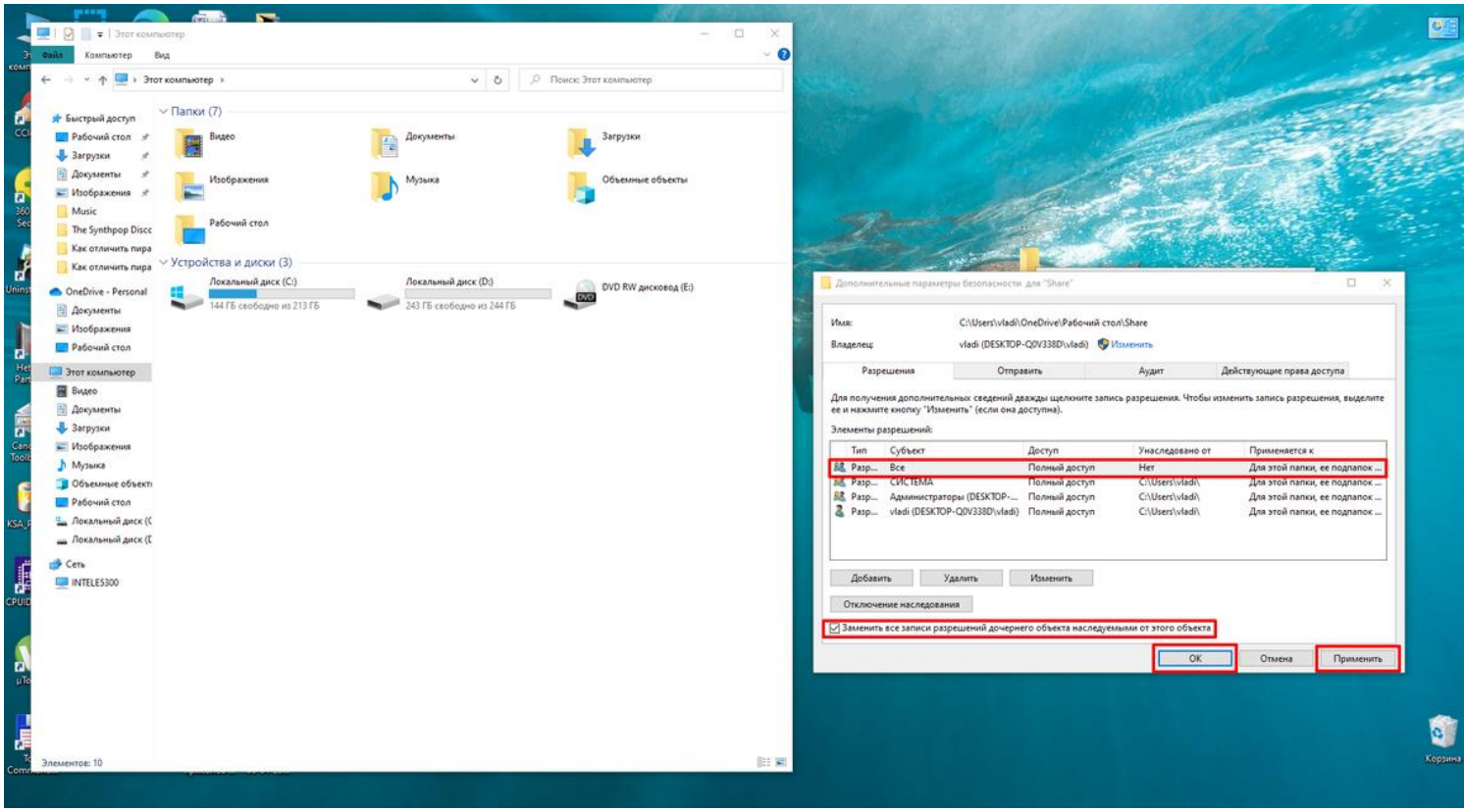
Даём те права, которыми вы хотите наделить эту группу. Подтверждаем и возвращаемся во вкладку "Безопасность", ещё раз проверьте какие права вы даёте для файлов, расположенных в папке "Share" и переходим в раздел "Дополнительно". Здесь нужно установить галочку напротив "Заменить все записи разрешений дочернего объекта наследуемыми от этого объекта". Далее "ОК". На всплывающий запрос от "Безопасности Windows" отвечайте кнопкой "Да".



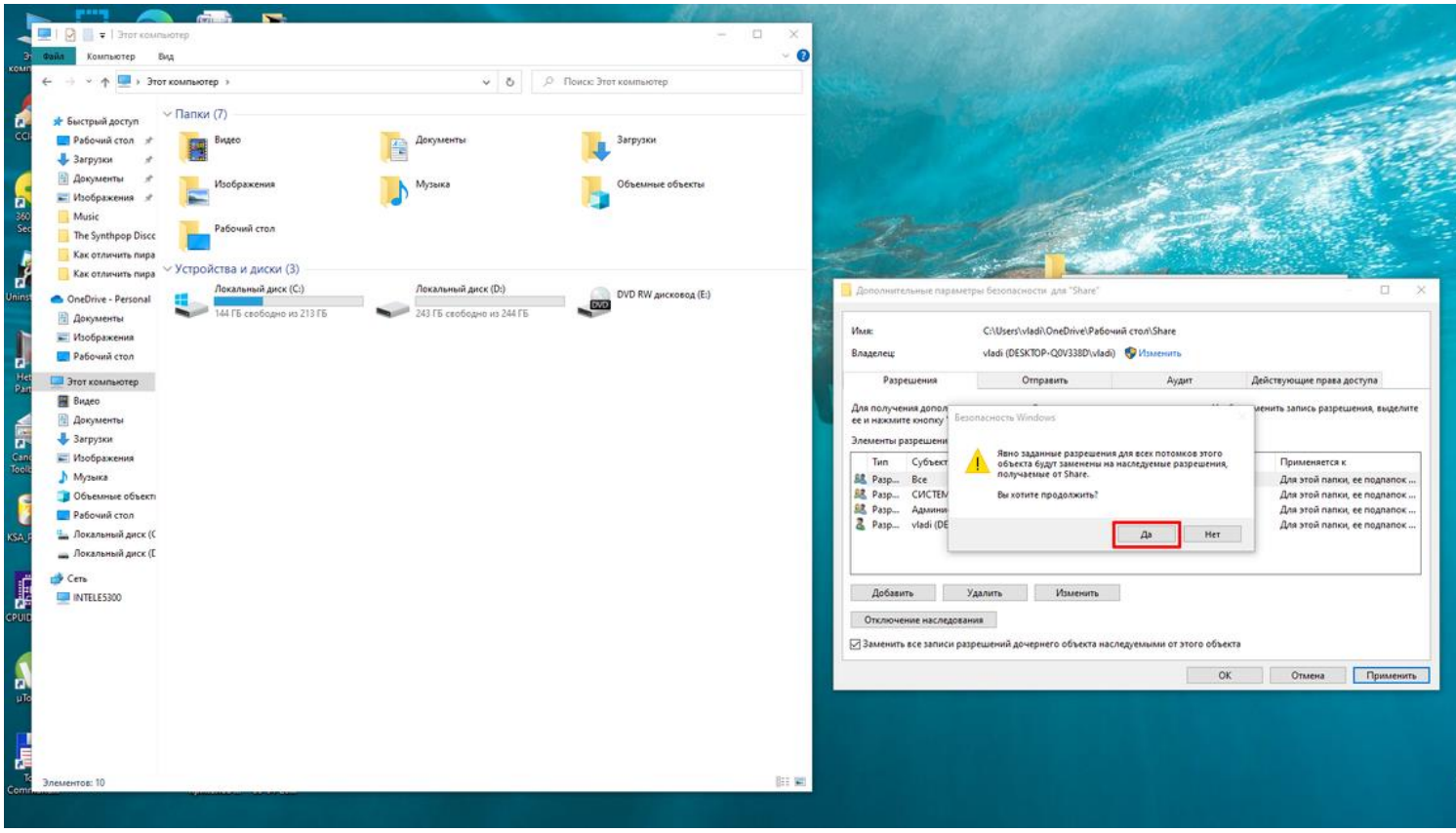
Наделяем выбранного пользователя правами, установив галочки напротив необходимых пунктов



Переход в раздел "Дополнительно" свойств папки



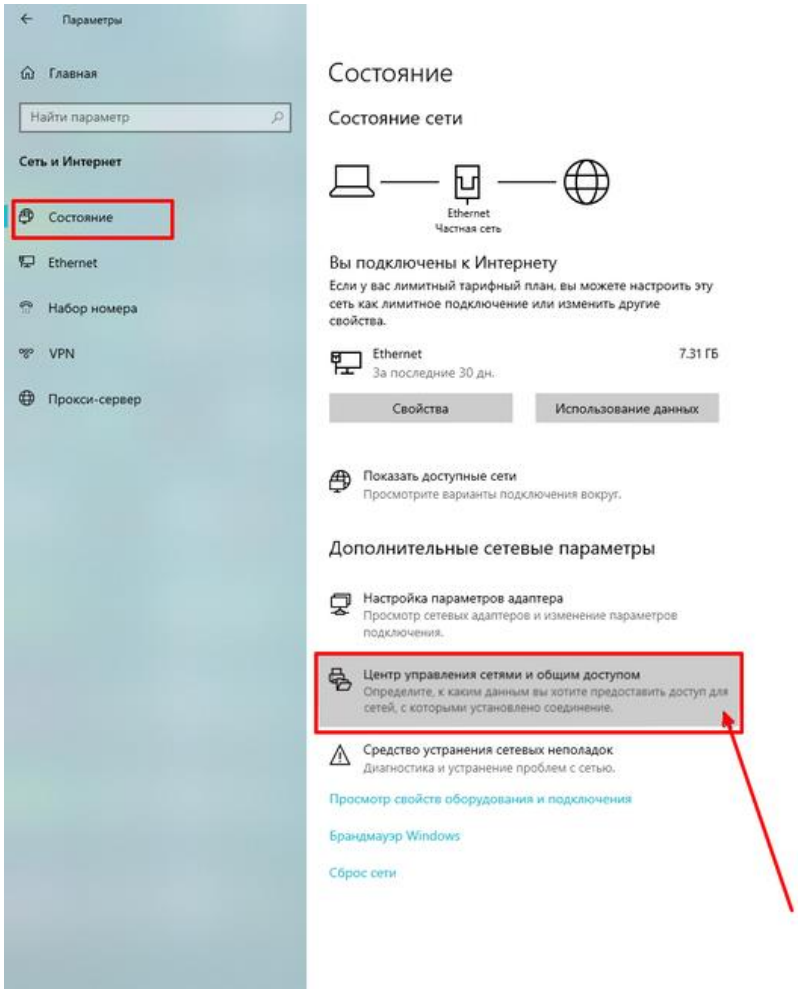
Заменяем все записи разрешений дочернего объекта наследуемыми от этого объекта



Подтверждаем все свои предыдущие действия через кнопку "Да" в появившемся окне

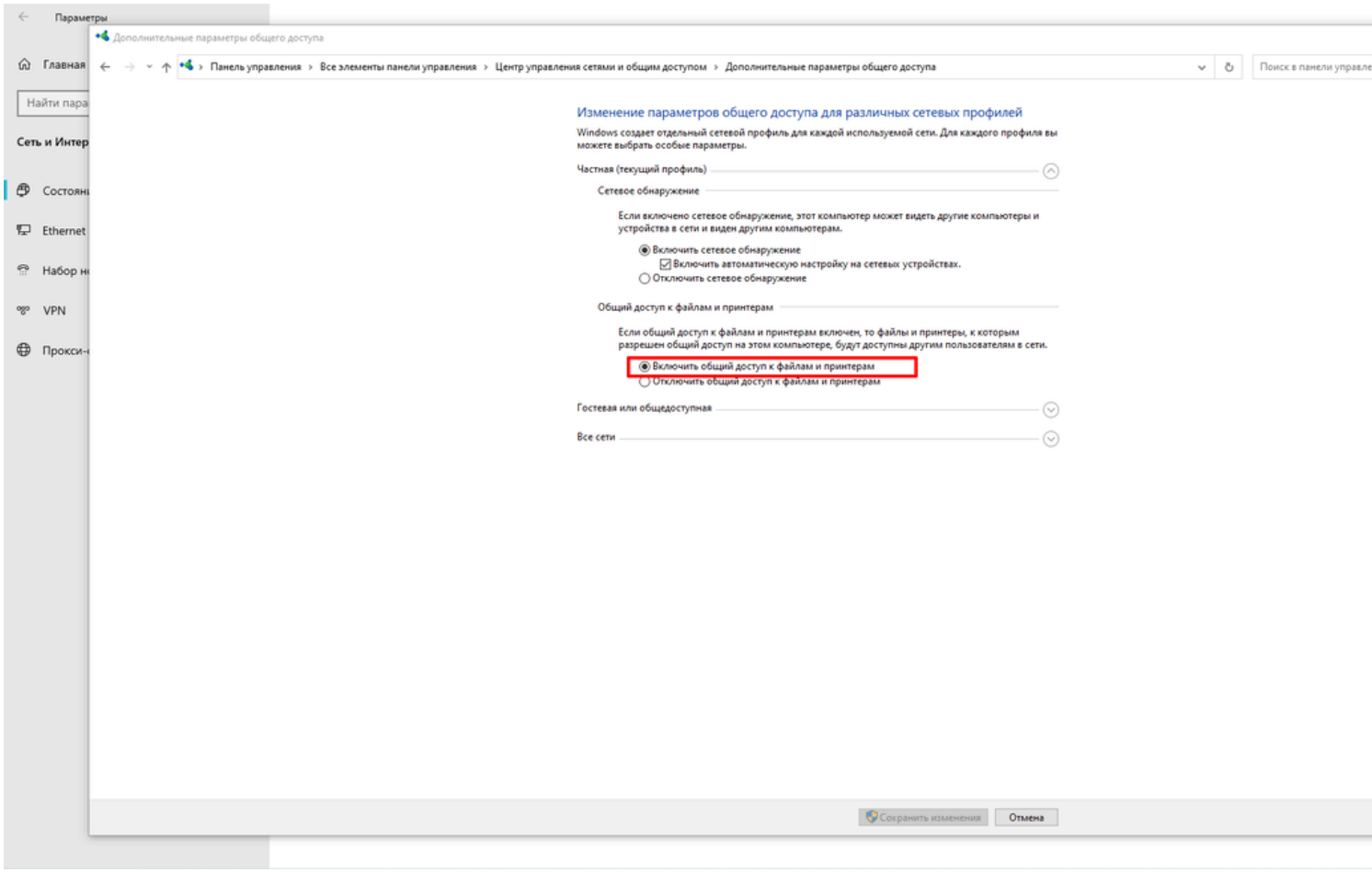
Теперь нам нужно попасть в "Параметры". Делайте переход так, как вам удобно. Один из лучших способов — нажать комбинацию клавиш Win+I. В "Параметрах" зайдём в раздел "Сеть и интернет".

- Далее проходим в "Состояние" и "Центр управления сетями и общим доступом".

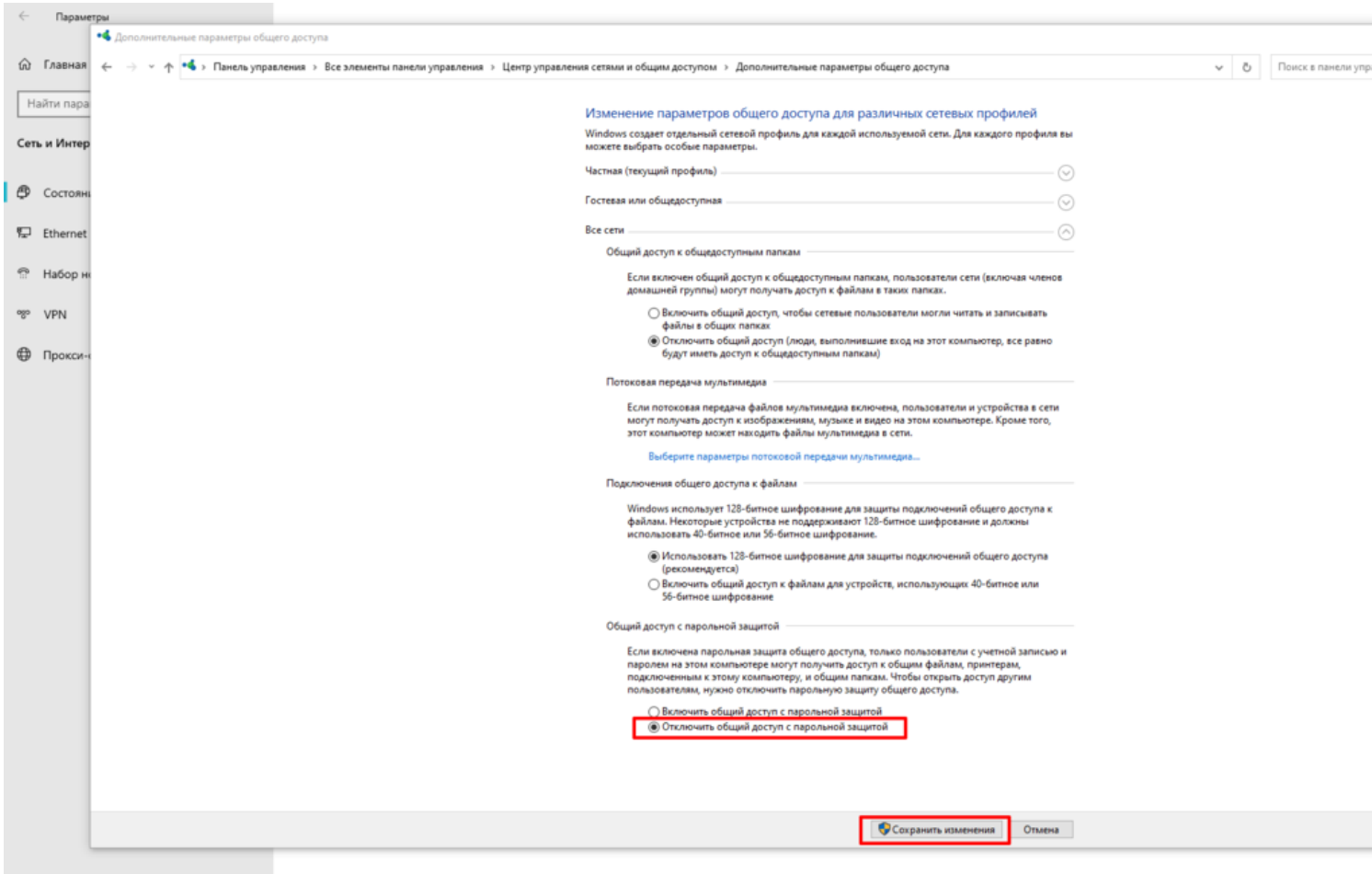


Переход в "Центр управления сетями и общим доступом"

- Нам нужно включить "Общий доступ к файлам и принтерам", установив маркер напротив, затем чуть ниже раскрыть вкладку "Все сети" и там установить маркер на "Отключить общий доступ с парольной защитой", чтобы не вводить пароль при входе в дальнейшем. Подтверждаем всё кнопкой "Сохранить изменения".



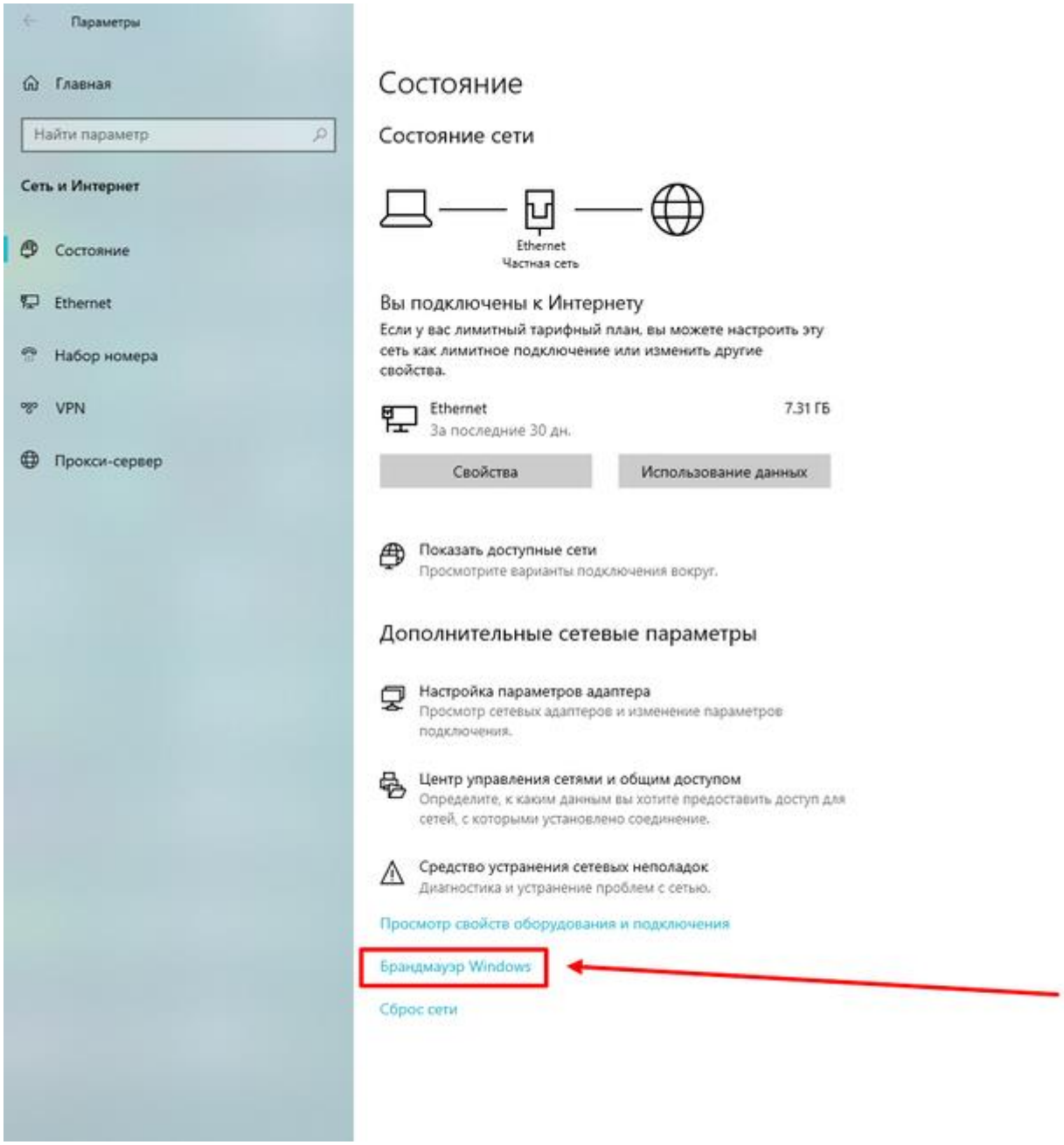
Включаем общий доступ к файлам и принтерам



Отключаем общий доступ с парольной защитой

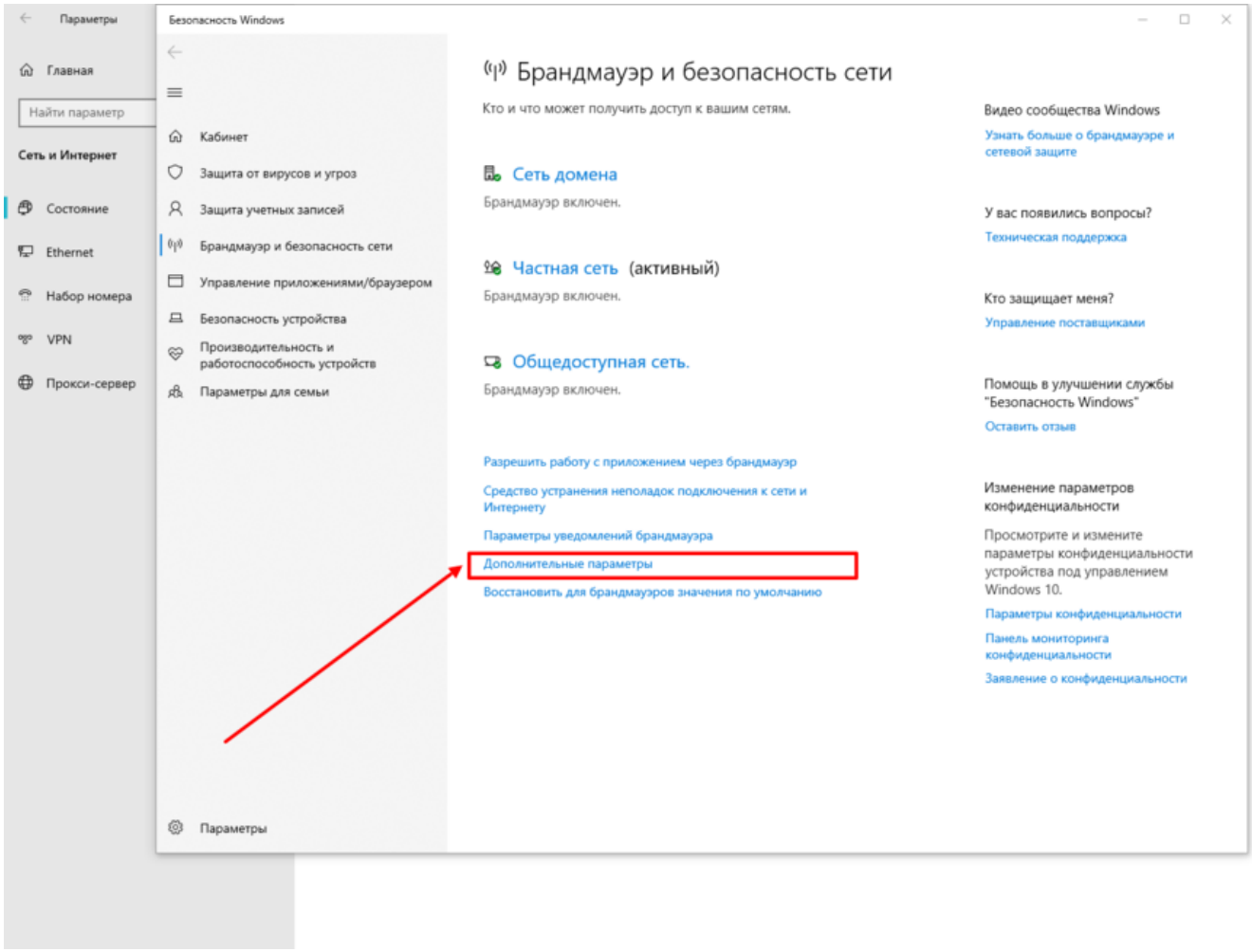
Настраиваем брандмауэр Windows

Чтобы брандмауэр Windows не строил нам козни при подключении внешних соединений, мы перейдём в брандмауэр через поле поиска в "Параметрах" или снова находим его в разделе "Сеть и интернет" и вкладке "Состояние".



Переход к "Брандмауэру Windows"

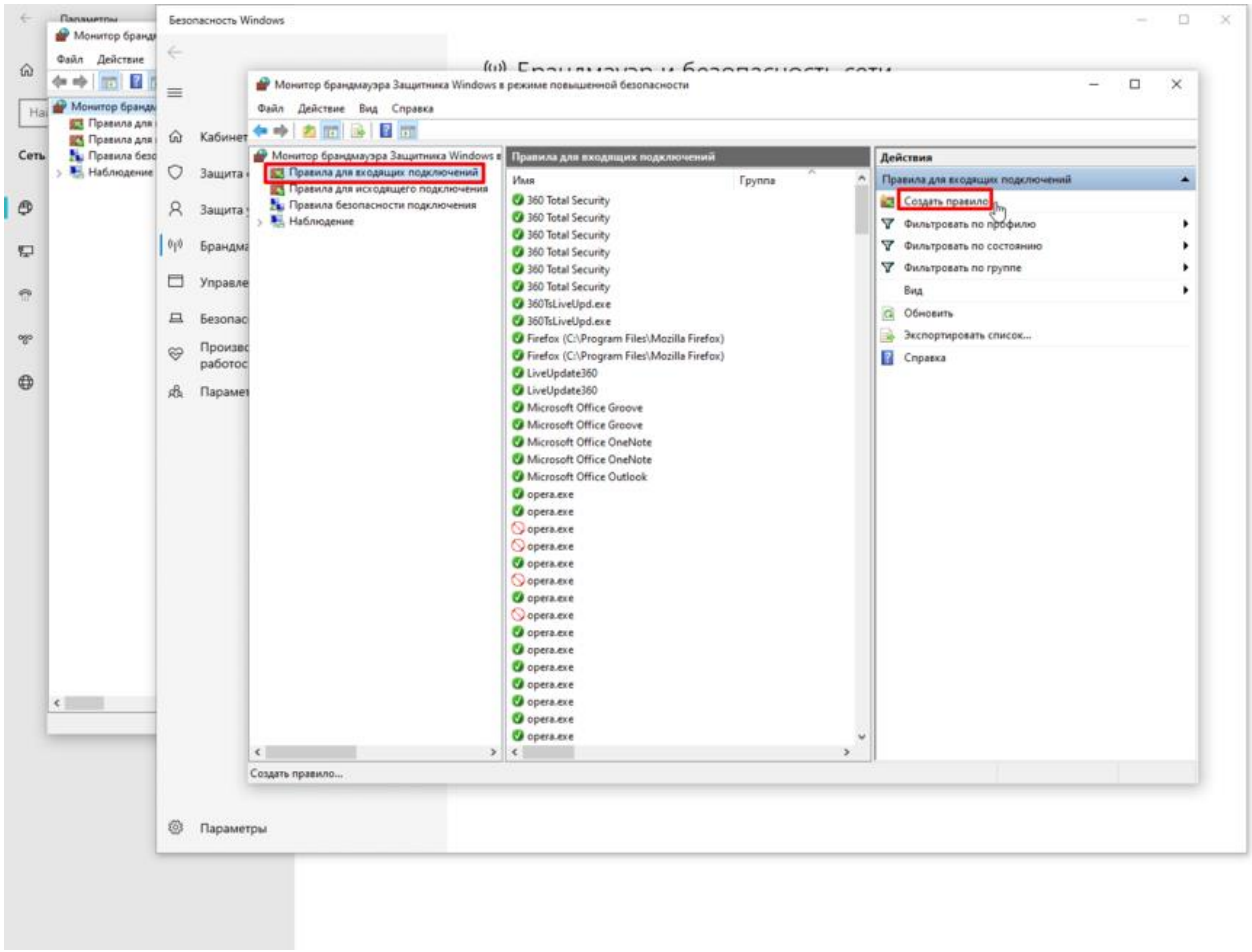
- Далее войдём в "Дополнительные параметры".



Переход в "Дополнительные параметры" брандмауэра Windows

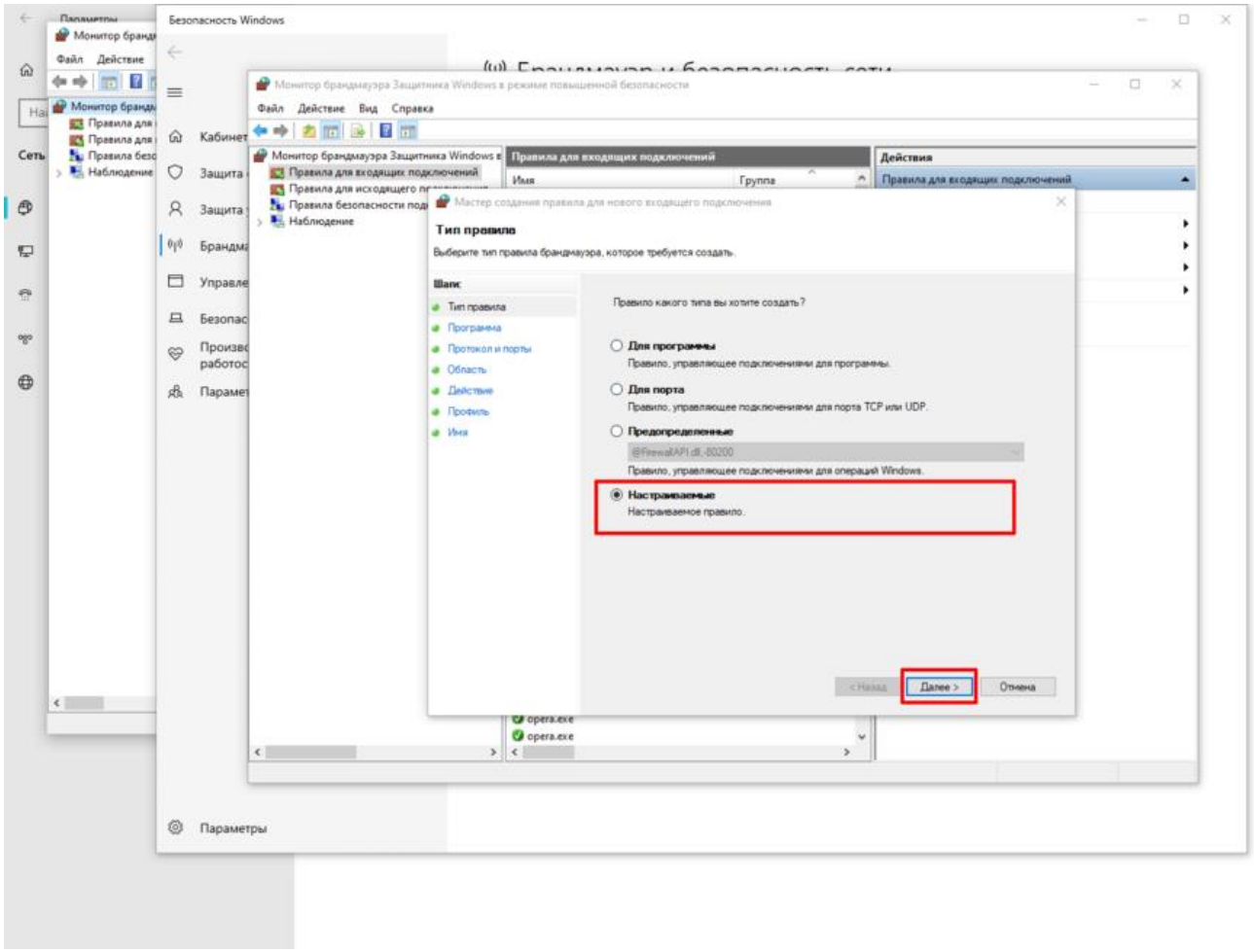
На всплывающее окно ответьте кнопкой "Да".

- Нам нужна вкладка "Создать правило" в разделе "Правило для входящих подключений".



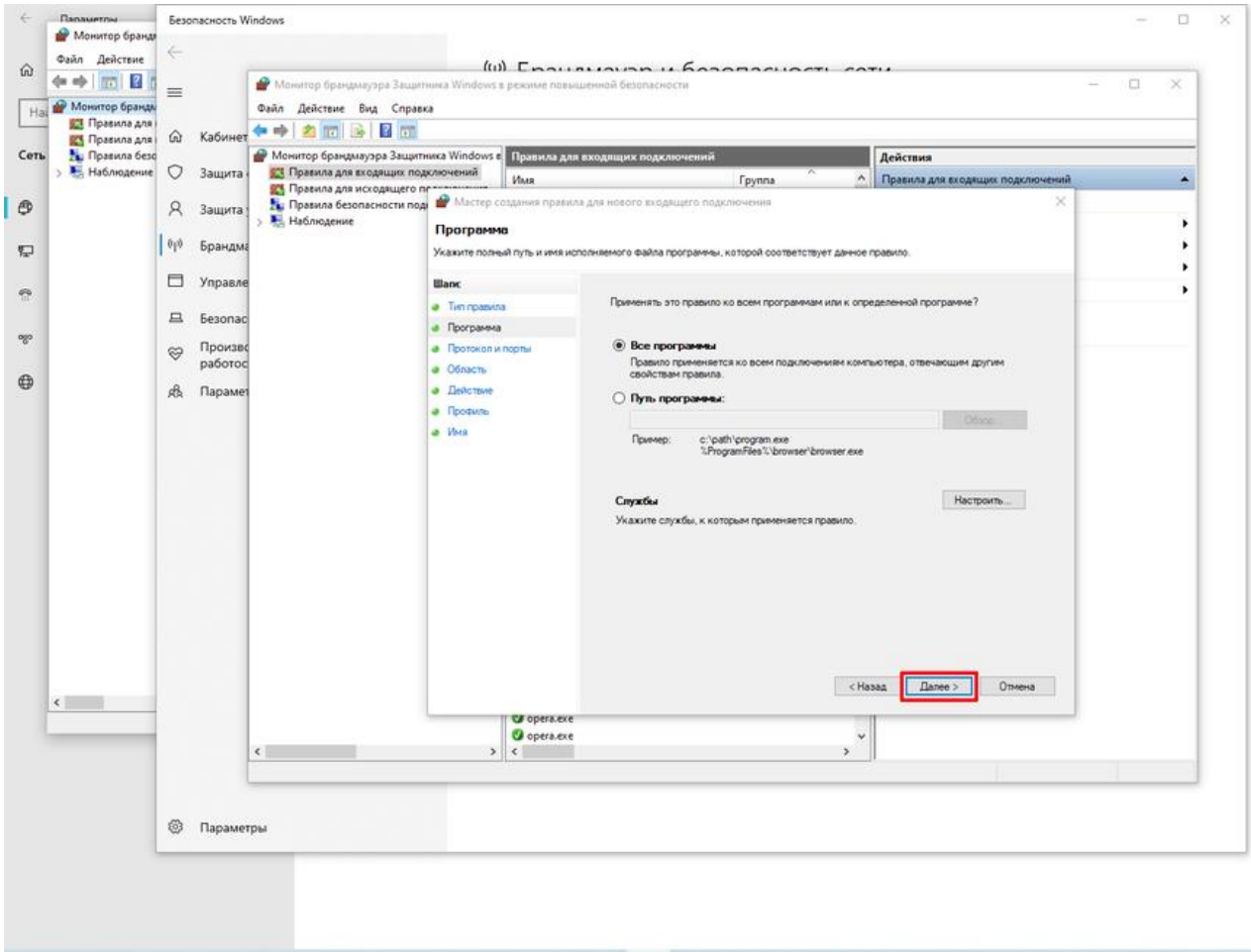
Создаём новое правило для брандмауэра Windows

- Тип правила выбираем "Настраиваемые", поставив маркер напротив. Жмём "Далее".



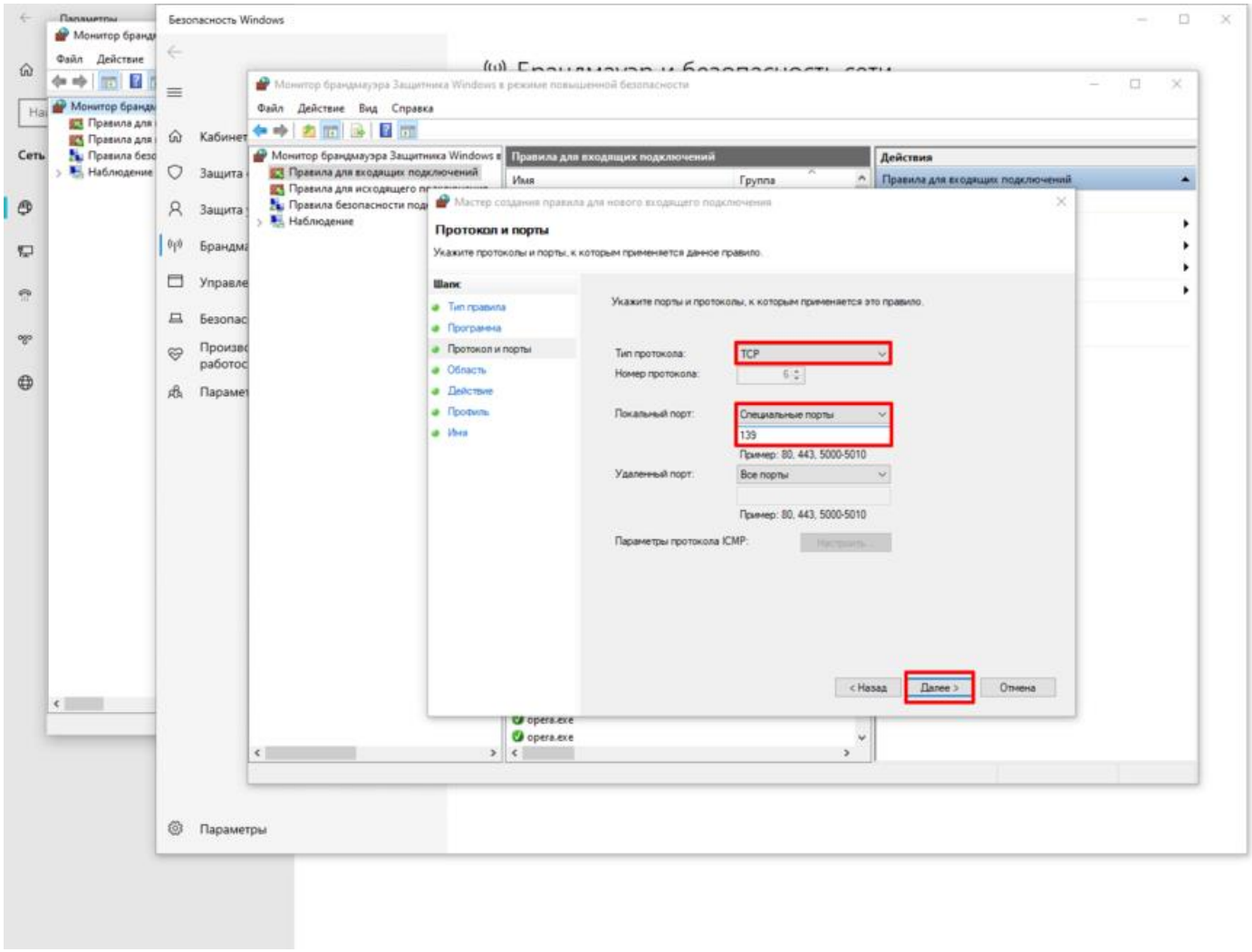
Устанавливаем новое правило настраиваемого типа

- На следующей странице всё оставляем без изменений и просто переходим дальше.



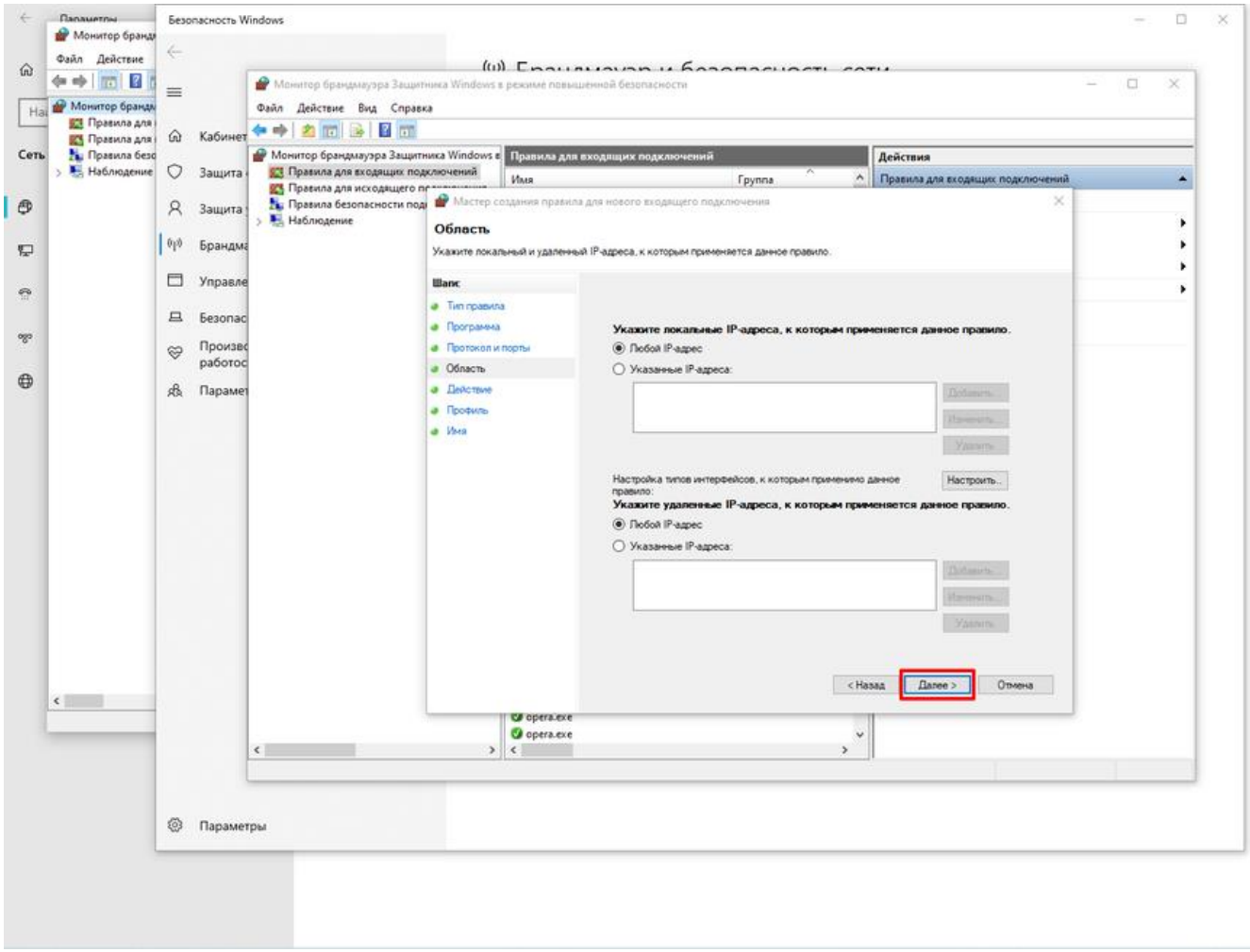
На этой странице ничего не меняем и нажимаем сразу на кнопку "Далее"

- На следующей странице указываете, что тип протокола "TCP", а напротив пункта "Локальный порт" у вас должен быть выбран "Специальный порт" и 139. Жмите "Далее".



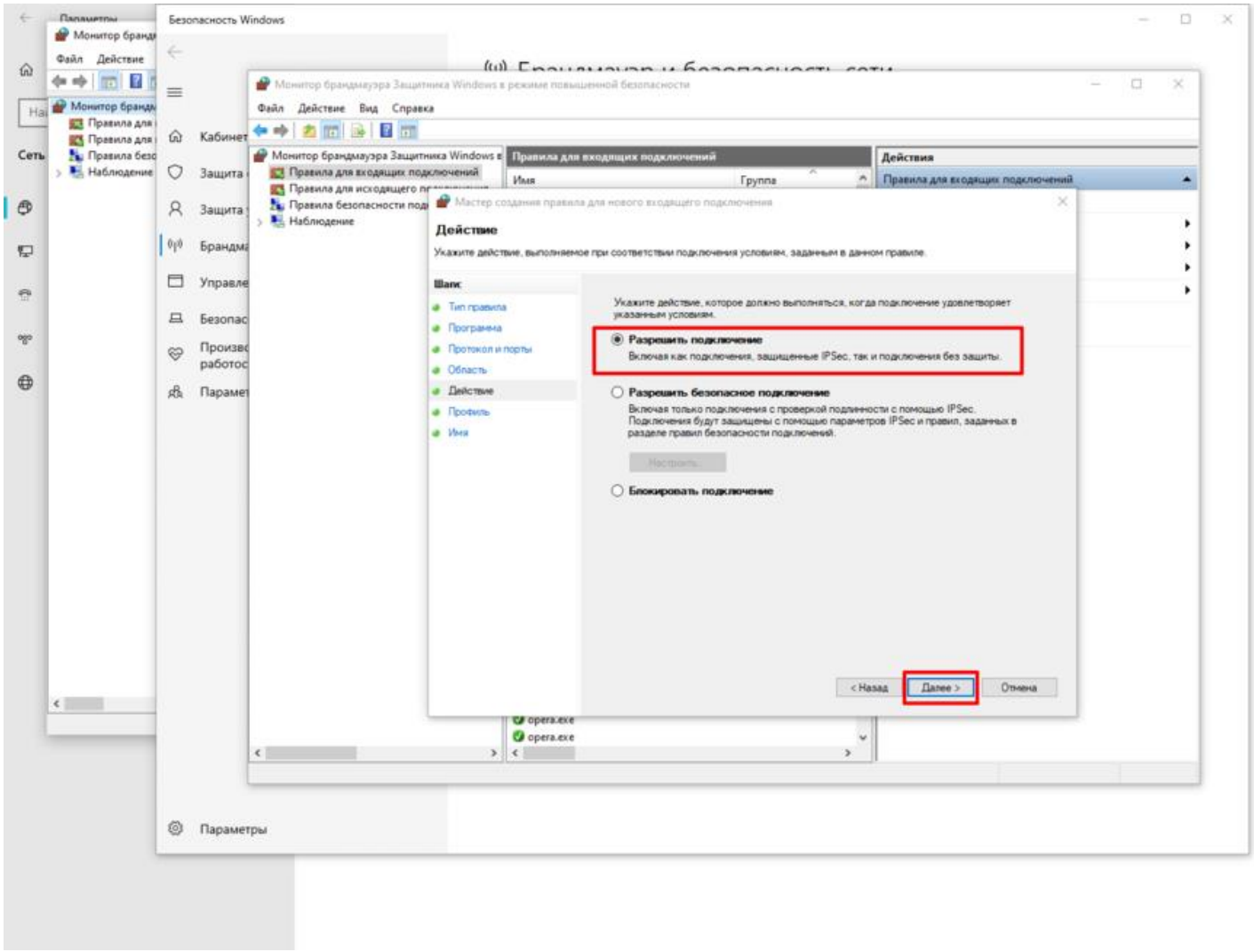
Выставляем тип протокола TCP и выделяем локальному порту специальный порт 139

- В следующем окошке мы можем прописать конкретные IP-адреса для подключения или оставляем разрешения для всех.



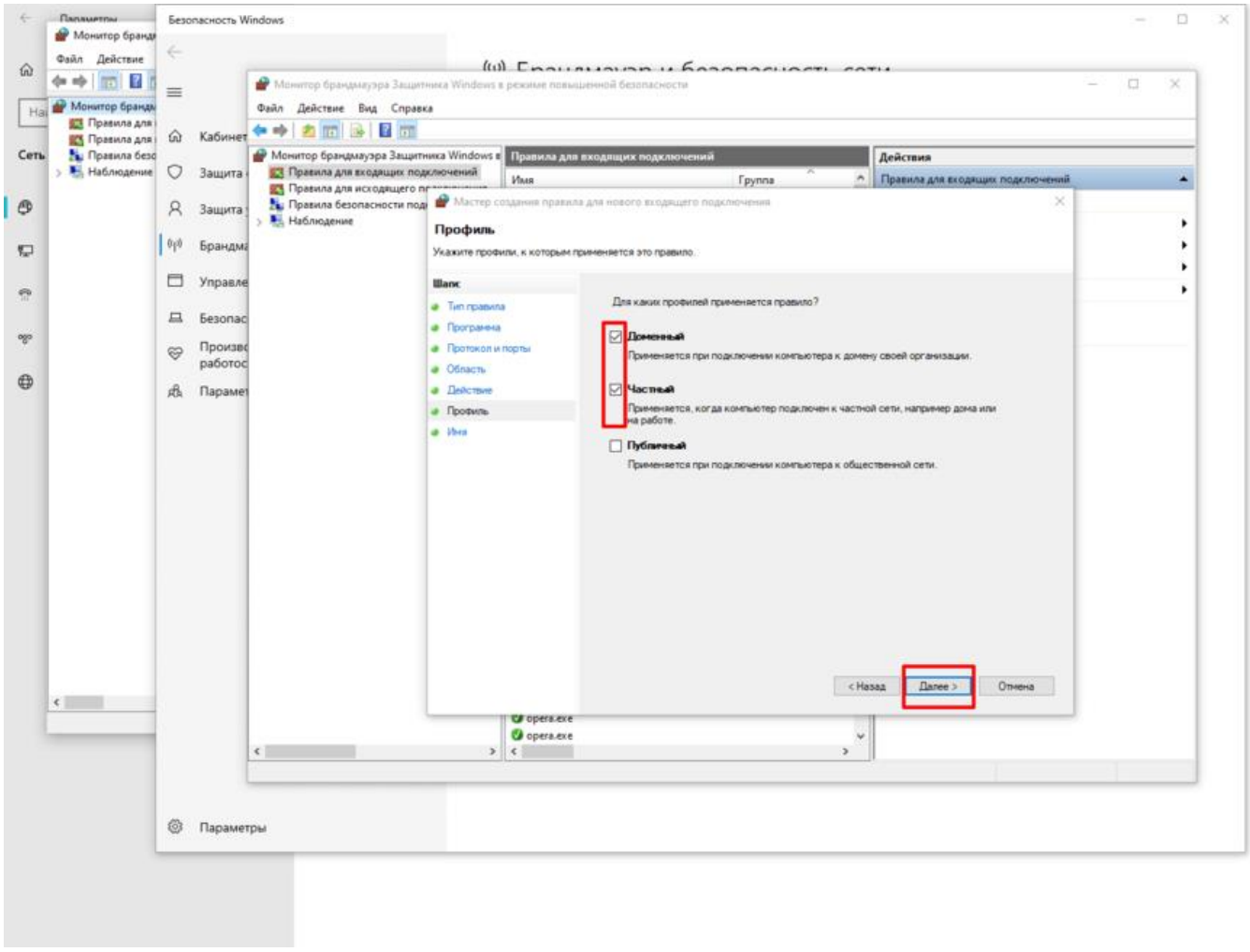
Заполняем при необходимости поля конкретными IP-адресами или оставляем всё по умолчанию

- Далее выставляем разрешение на подключение в виде маркера и идём дальше.



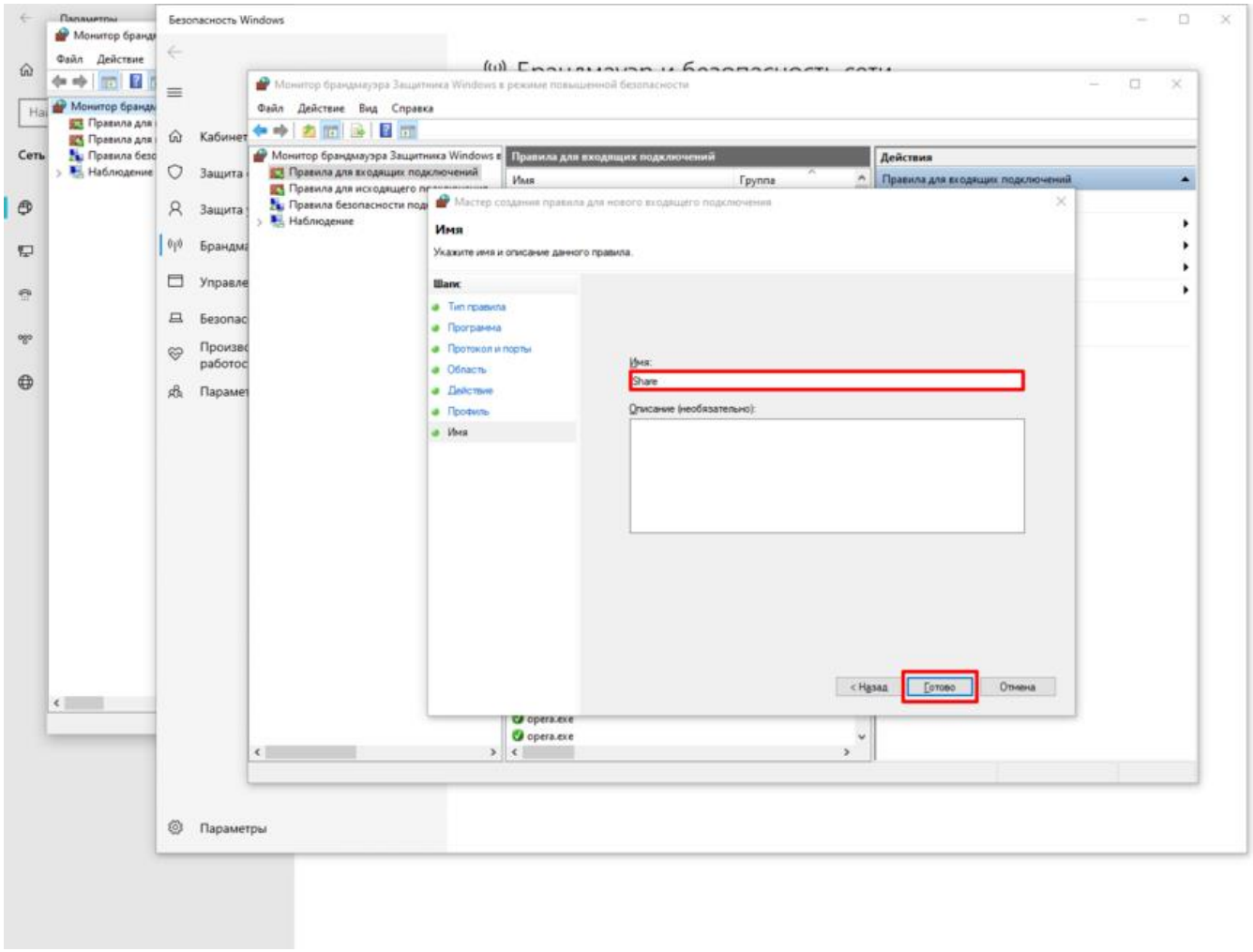
Даём разрешение на подключение с помощью маркера

- Применяем правило для доменных и частных профилей. Публичные не отмечаем.



Отмечаем доменные и частные профили

- Вписываете любое имя и жмёте "Готово".



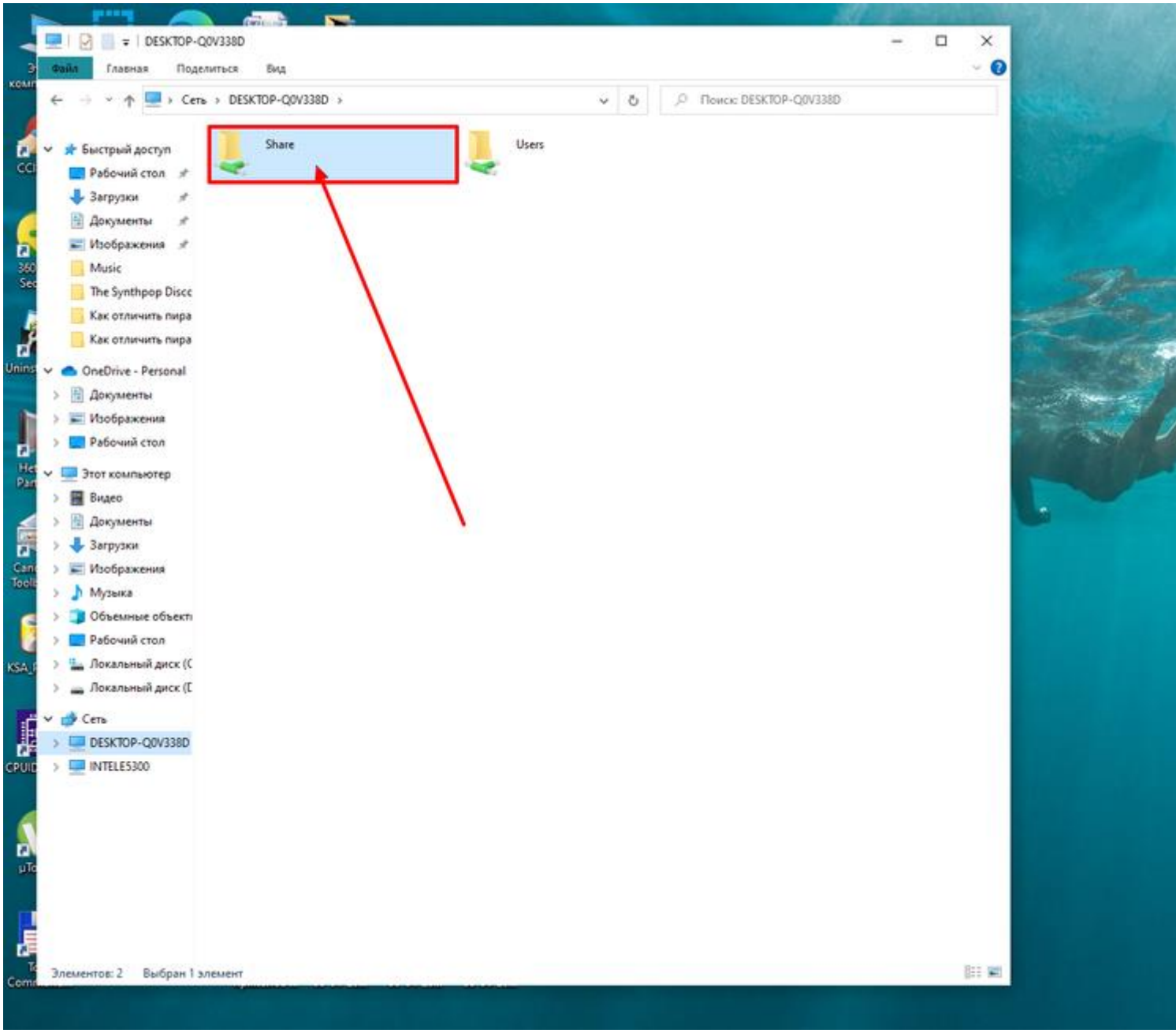
Придумываете новому правилу имя и нажимаете на кнопку "Готово"

Всё, что было проделано нами с брандмауэром Windows, являет собой настройку доступа без отключения самого брандмауэра, так как он важен для системы и для нас также очень важно было получить от него разрешения на доступ, не отключая его самого.

Как создать сетевую папку Windows 10, дать ей общий доступ и наделить определёнными правилами мы научились, а теперь осталось только отыскать её.

Где всегда можно отыскать созданную папку в Windows

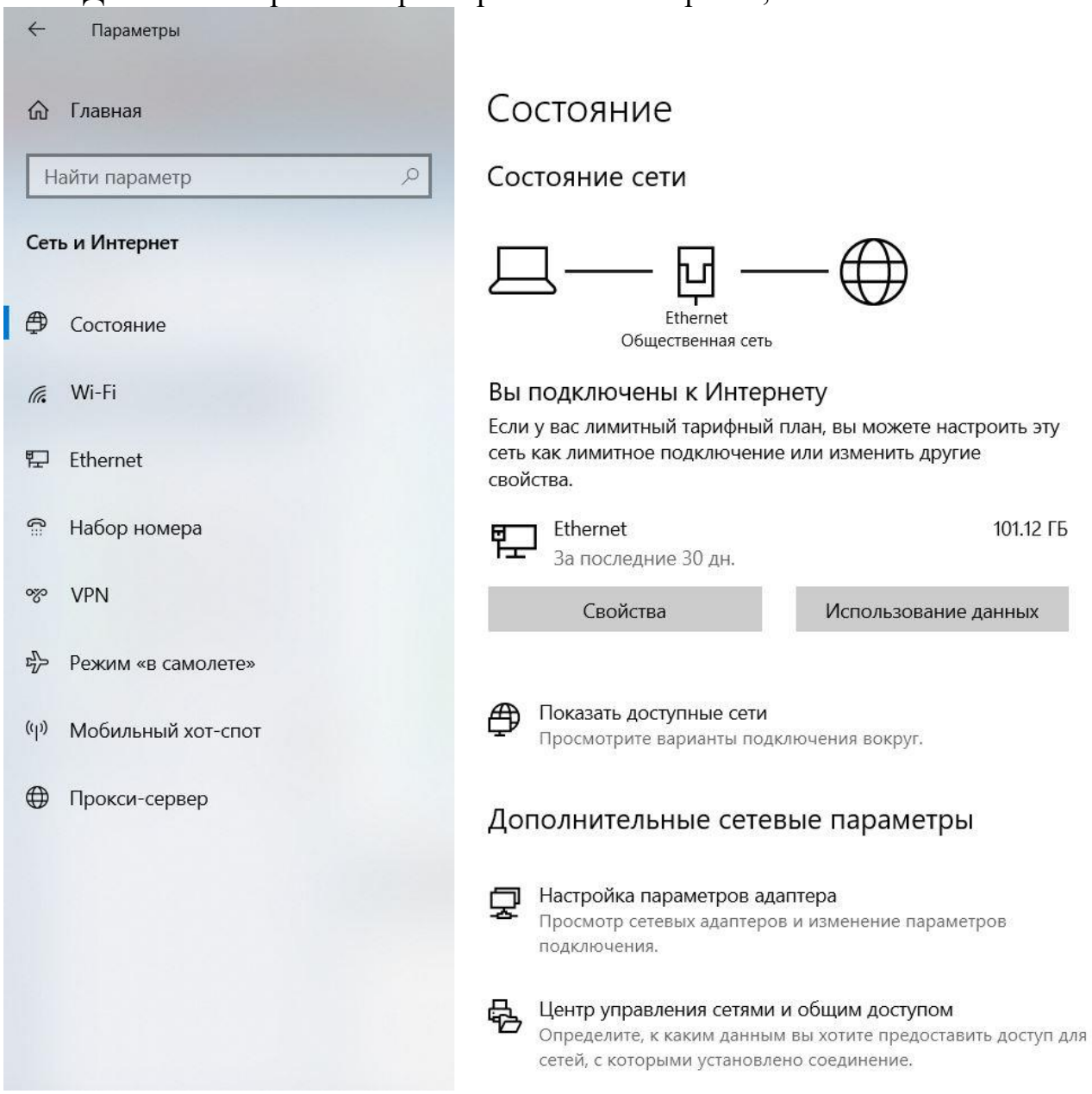
Теперь можете попробовать поискать через "Проводник" или "Этот компьютер" вашу сетевую папку с общим доступом. Просто перейдите для этого во вкладку "Сеть".



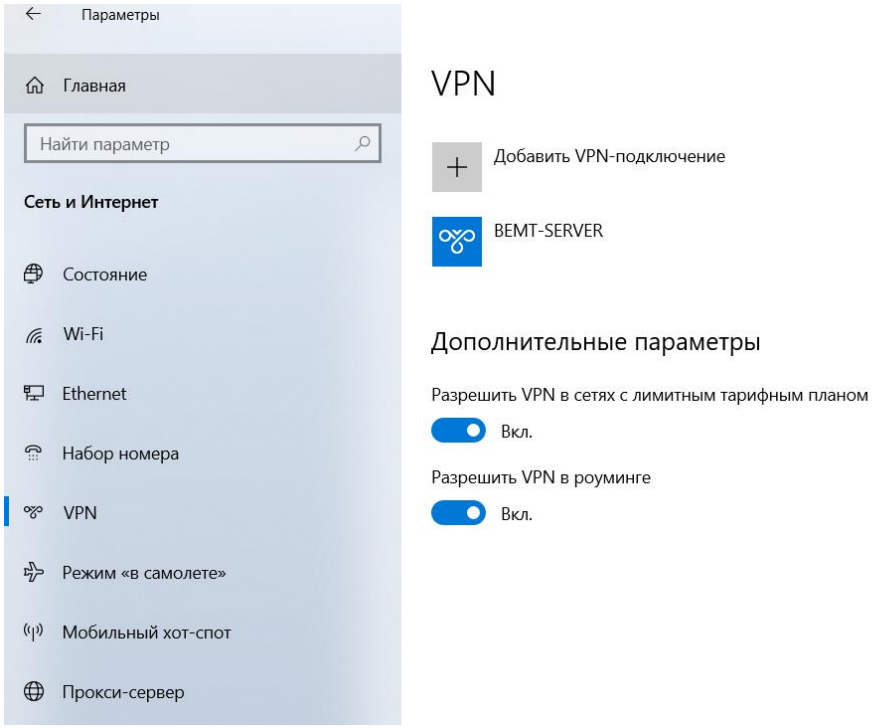
Созданная папка всегда доступна в "Проводнике" - во вкладке "Сеть", где нужно щёлкнуть только по названию вашего ПК для её отображения

5. Создание VPN соединения с удаленным сервером.

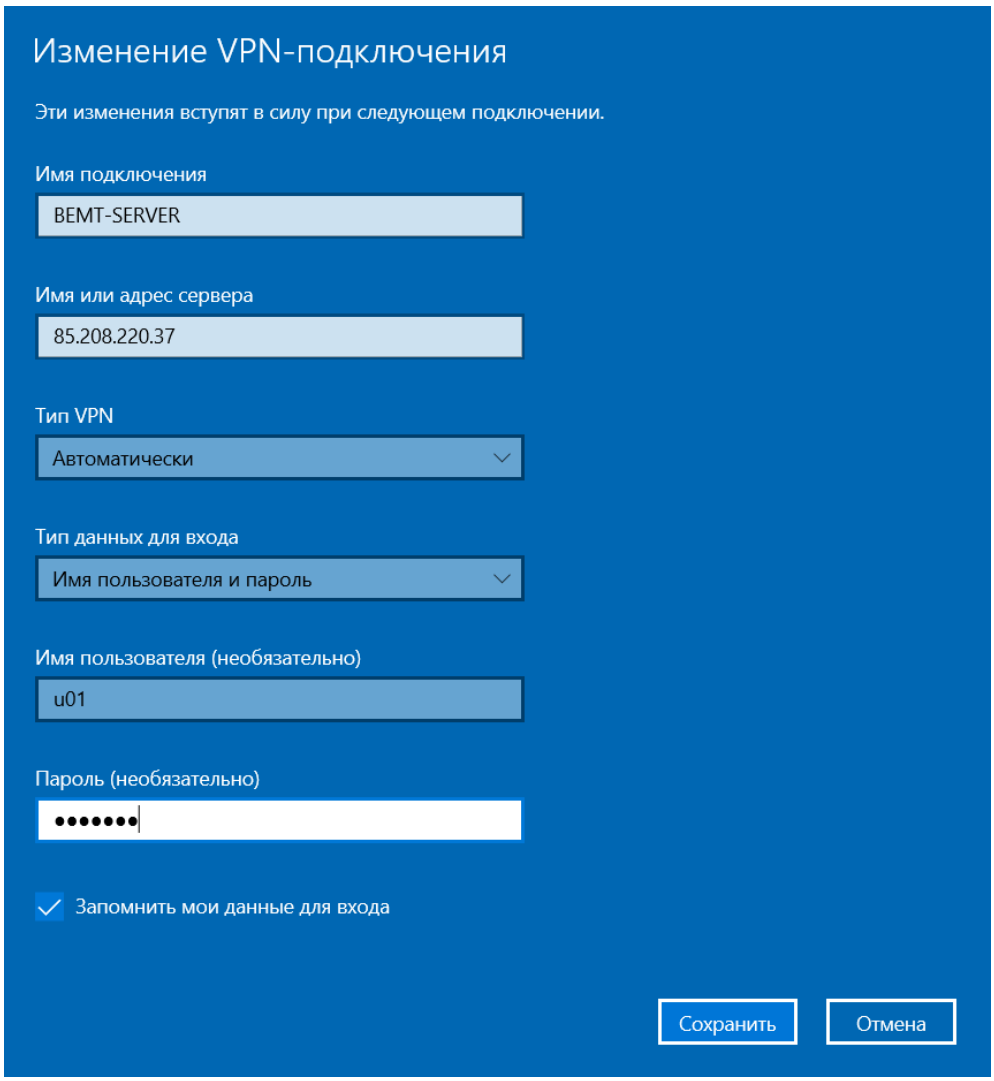
Для этого открыть «Параметры сети и Интернет»,



Далее выбрать раздел VPN



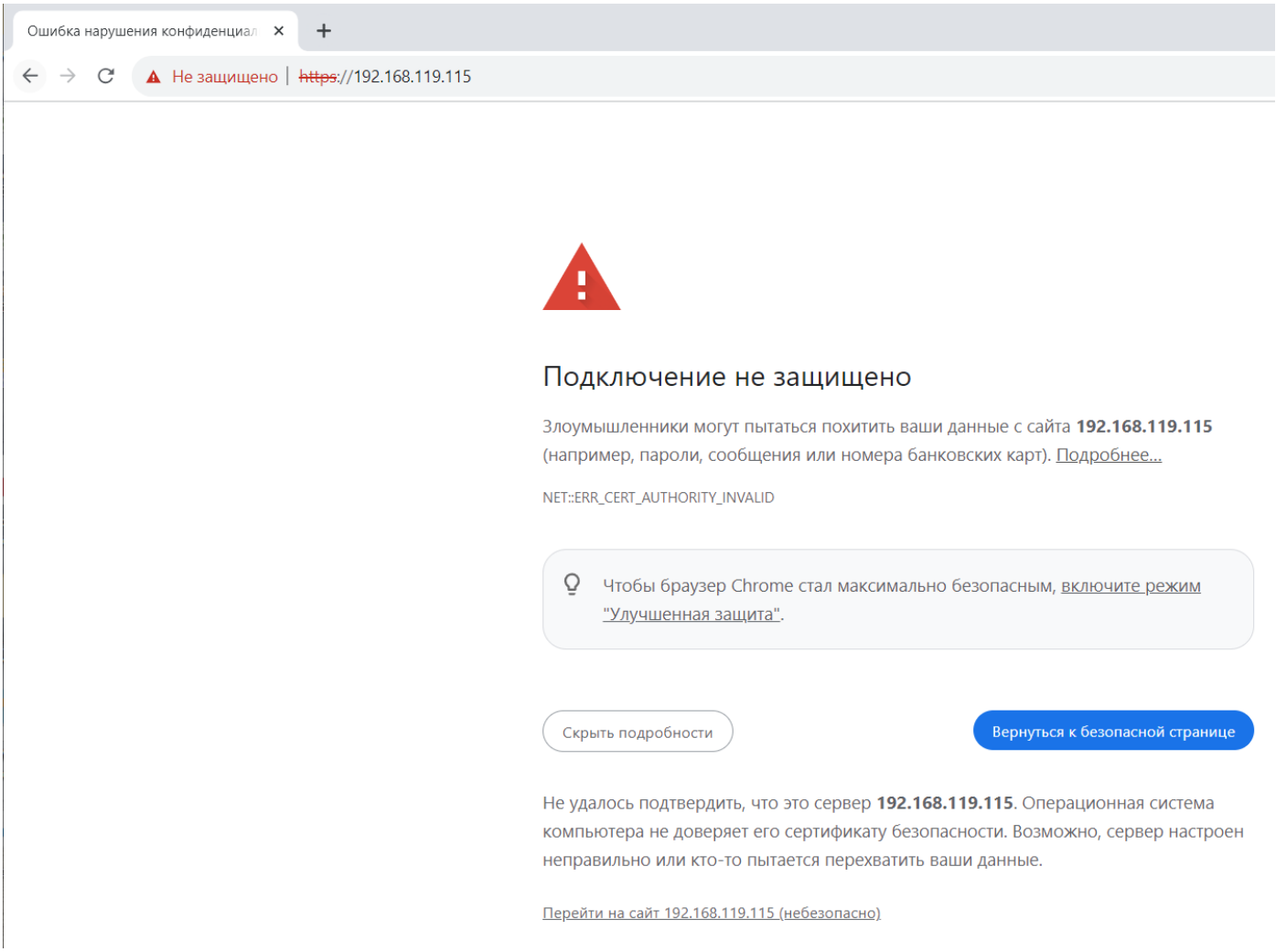
Нажать «Добавить VPN-подключение» и ввести следующие параметры



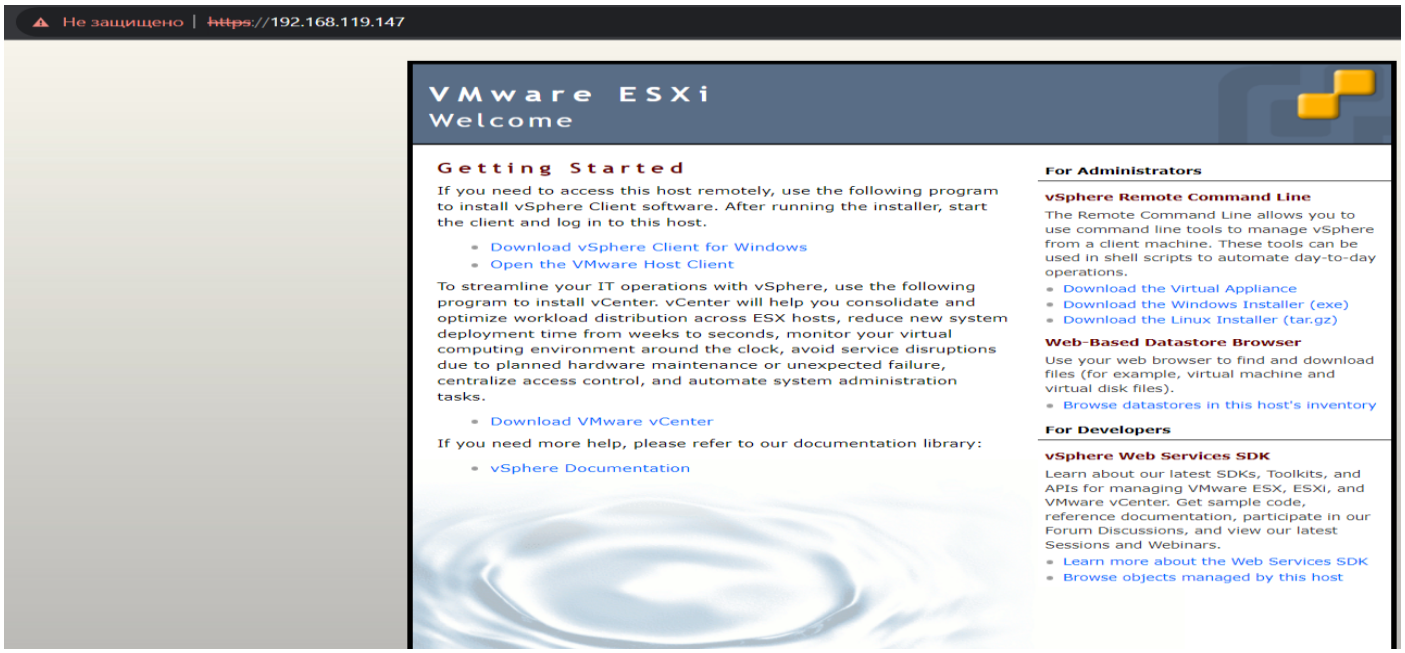
Нажать Сохранить. И проверить подключение.

6. Работа с виртуальными машинами на удаленном сервере.

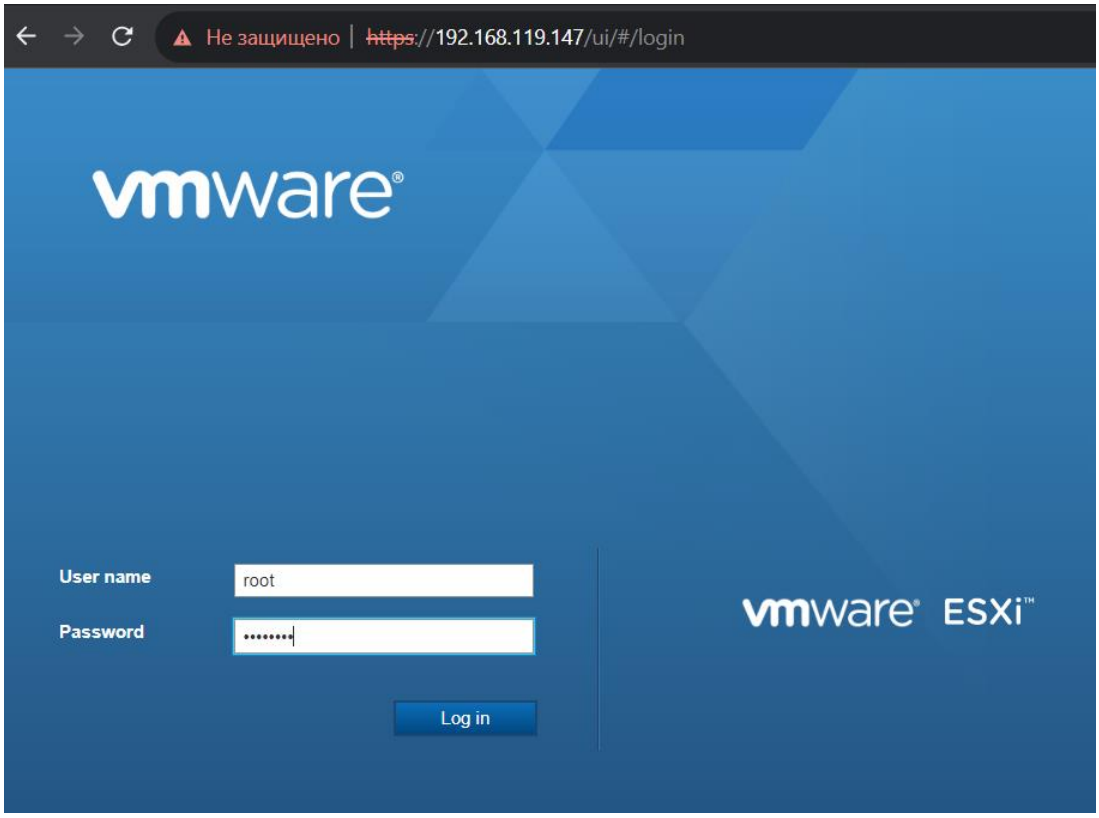
После успешного подключения по VPN, открыть браузер и в адресной строке ввести указанный преподавателем IP адрес виртуальной машины.



На вкладке дополнительно внизу, нажать перейти на сайт. Далее нажать Open the VMware Host Client



В появившемся окне ввести логин root и пароль P@ssw0rd



Далее выбираем из списка виртуальную машину и делаем запуск.