Федеральное государственное образовательное бюджетное

учреждение высшего образования

**«Финансовый университет при Правительстве Российской Федерации»**

**(Финансовый университет)**

Колледж информатики и программирования

**ОТЧЁТ**

**По лабораторной работе №11**

Студент: Глазков Никита Павлович

Дисциплина/Профессиональный модуль: Инфокоммуникационные системы и сети

Группа: 3ПКС-220

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2022г.**

**Лабораторная работа №11**

**Цель работы:**

Описать технологию RPD, для чего нужна, как применить, для кого пригодиться.

**Задание:**

RDP (Remote Desktop Protocol) – специальный протокол, разработанный компанией Microsoft для удаленного управления ОС Windows (протокол удалённого рабочего стола). Изначально, разумеется, как и многие вещи под Windows, этот протокол разработали другие люди, но в настоящее время поддерживает его и развивает Microsoft.  
Протокол RDP основан на семействе стандартов протокола T-120 и является его расширением. Протокол, поддерживающий несколько каналов, позволяет использовать отдельные виртуальные каналы для передачи следующих сведений:

* данные презентации
* последовательная связь с устройством
* сведения о лицензировании
* строго зашифрованные данные, такие как активность клавиатуры и мыши

RDP — это расширение основного протокола T.Share. Некоторые другие возможности сохраняются как часть RDP, например, архитектурные особенности, необходимые для поддержки многоточечных (многосторонних) сеансов. Доставка данных из нескольких точек позволяет в реальном времени доставлять данные из приложения нескольким сторонам, таким как виртуальные доски. Не требуется отправлять одинаковые данные в каждый сеанс по отдельности.

В этом первом выпуске Windows Terminal Server мы будем концентрироваться на обеспечении надежного и быстрого обмена данными «точка–точка» (один сеанс). В первоначальном выпуске Terminal Server 4.0 используется только один канал данных. Однако гибкость протокола RDP предоставляет достаточно места для функциональных возможностей в будущих продуктах.

Одна из причин, по которой корпорация Майкрософт решила реализовать RDP в целях подключения в Windows NT Terminal Server, заключается в том, что он предоставляет расширяемую базу для создания множества дополнительных возможностей. RDP предоставляет 64 000 отдельных каналов для передачи данных. Однако в настоящее время для передачи данных используется только один канал (для клавиатуры, мыши и данных презентации).

Протокол RDP предназначен для поддержки различных типов сетевых топологий, таких как ISDN и POTS. Протокол RDP также предназначен для поддержки многих протоколов локальной сети, таких как IPX, NetBIOS и TCP/IP. Текущая версия RDP будет работать только по протоколу TCP/IP. Благодаря отзывам клиентов в будущих версиях может быть добавлена поддержка других протоколов.

Действия, связанные с отправкой и получением данных через стек RDP, по сути, аналогичны стандартам семиуровневой модели OSI для распространенных сегодня сетей LAN. Данные от приложения или службы, которые необходимо передать, передаются через стеки протоколов. Они разделяются, направляются в канал (через MCS), шифруются, структурируются и упаковываются в сетевой протокол и, наконец, обрабатываются и отправляются клиенту по сети. Возвращение данных выполняется так же, только в обратном направлении. Пакет удаляется из адреса, а затем распаковывается, расшифровывается и т. д. Наконец, данные представляются приложению для использования. Основные части изменений стека протокола происходят между четвертым и седьмом уровнями, где данные являются:

* зашифрованными;
* упакованными;
* систематизированными;
* направленными в канал;
* приоритезированными.

Одним из ключевых моментов для разработчиков приложений является то, что при использовании RDP корпорация Майкрософт абстрагируется от сложностей работы со стеком протоколов. Это позволяет им создавать 32-разрядные продуманные, корректно написанные приложения. Затем стек RDP, реализованный сервером терминалов и его клиентскими подключениями, берет на себя остальные операции.

Дополнительные сведения о взаимодействии приложений на сервере терминалов и о том, что необходимо знать при разработке приложений для инфраструктуры Windows Terminal Server, см. в следующем техническом документе:  
Оптимизация приложений для Windows NT Server 4.0, Terminal Server Edition

В составе стека RDP стоит рассмотреть четыре компонента:

* Служба связи Multipoint (MCSMUX)
* Общее управление конференцией (GCC)
* Wdtshare.sys
* Tdtcp.sys

MCSmux и GCC являются частью семейства T.120 Международного союза электросвязи (ITU). MCS состоит из двух стандартов:

* T.122: определяет службы multipoint
* T.125: указывает протокол передачи данных.

MCSMux управляет:

* назначением каналов путем мультиплексирования данных на предопределенные виртуальные каналы в протоколе
* уровнями приоритета
* сегментацией отправляемых данных

По сути, MCSMux объединяет несколько стеков RDP в единую сущность с точки зрения GCC. GCC отвечает за управление этими каналами. GCC позволяет создавать и удалять сеансы подключения и управляет ресурсами, предоставляемыми MCS. Для каждого протокола сервера терминалов (в настоящее время поддерживаются только ICA Citrix и RDP) будет загружен экземпляр стека протоколов (стек прослушивателя, ожидающий запроса на подключение). Драйвер устройства сервера терминалов координирует действия протокола RDP и управляет ими. Он состоит из более мелких компонентов:

* драйвер RDP (Wdtshare.sys) для передачи с помощью пользовательского интерфейса, сжатия, шифрования, кадрирования и т. д.
* транспортный драйвер (Tdtcp.sys) для упаковки протокола в базовый сетевой протокол TCP/IP.

Протокол RDP был разработан для полной независимости от базового транспортного стека, в данном случае TCP/IP. Это обеспечивает возможность добавлять другие транспортные драйверы для других сетевых протоколов, которые по мере их роста могут понадобиться клиентам, без внесения значительных изменений в основные части протокола. Они являются ключевыми элементами производительности и расширяемости RDP в сети.

**Подключение в VPS серверу из десктопной Windows**

Данная инструкция проверена и работает успешно на всех популярных версиях Windows для персональных компьютеров: XP, Vista, Windows 7, 8, 8.1 и 10.  
В каждой операционной системе Windows есть встроенное приложение для подключения по RDP – это программа «Подключение к удалённому рабочему столу» (Remote Desktop Connection в англоязычных ОС).  
Для запуска ее зайдите по пути:

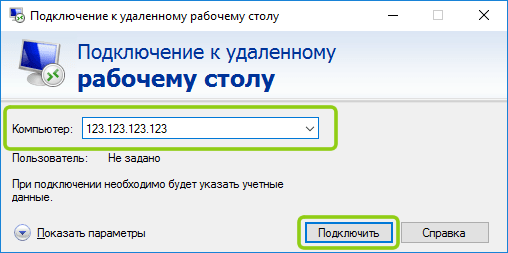
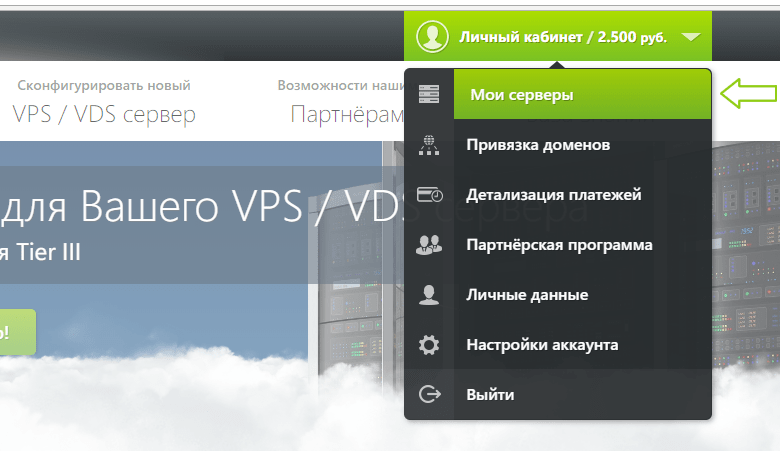
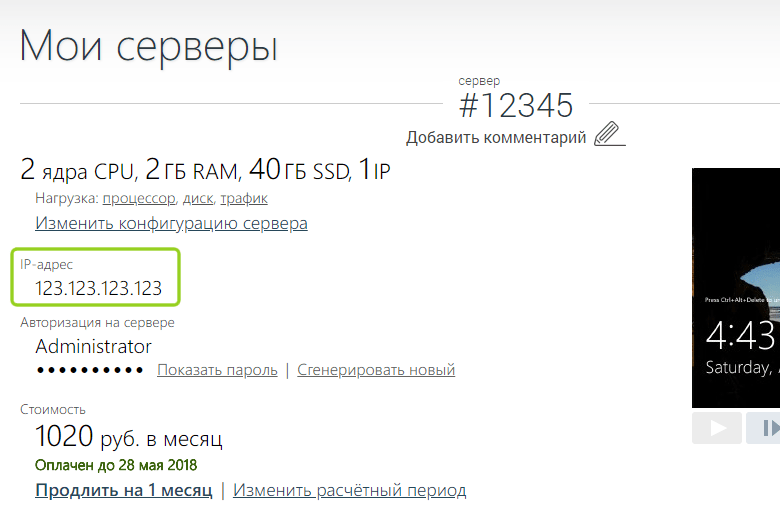
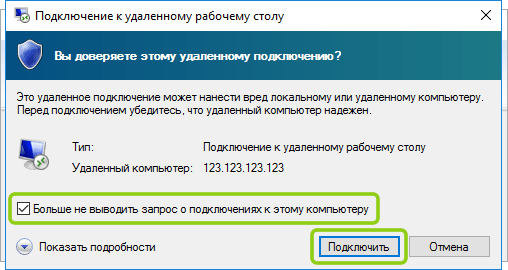
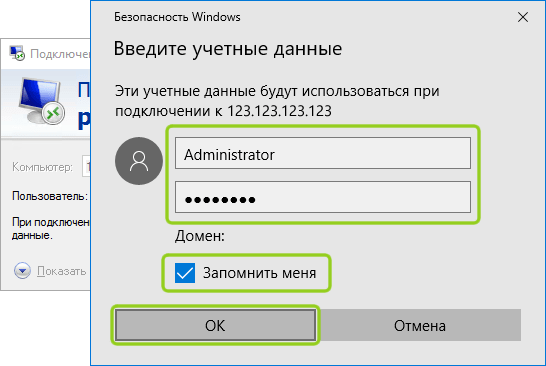
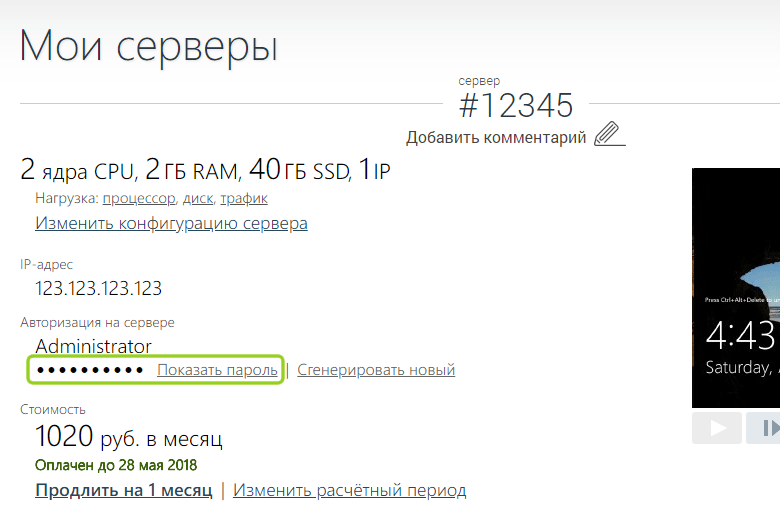
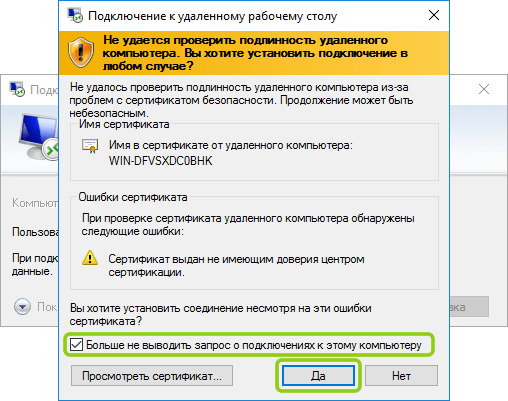
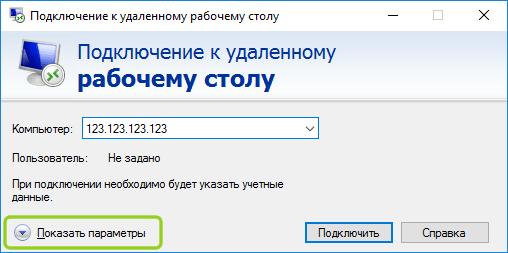
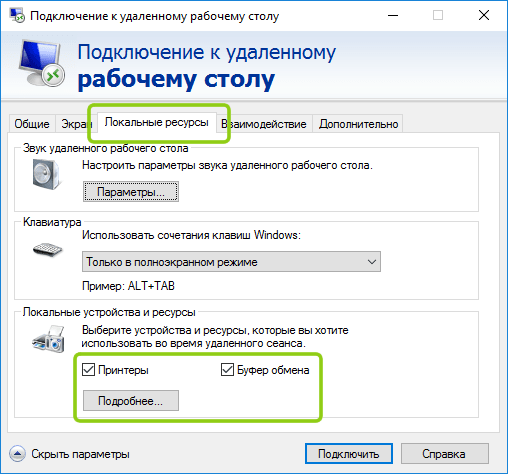
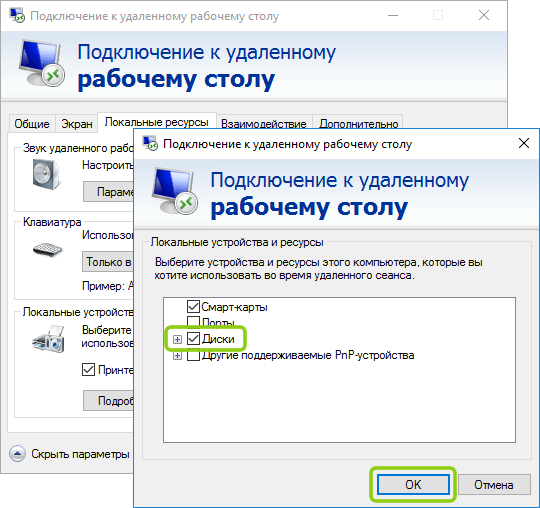
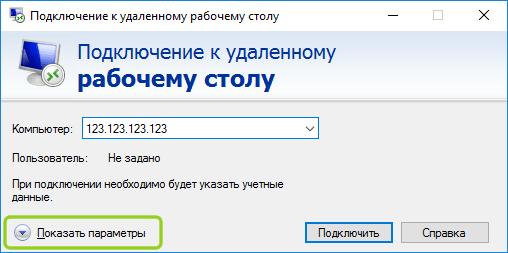
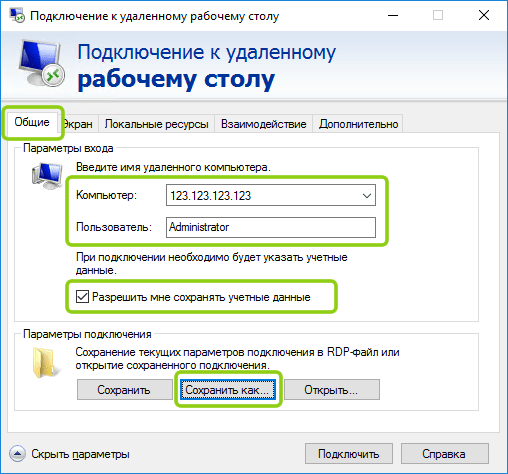
Пуск -> Программы -> Стандартные -> Подключение к удалённому рабочему столу

Если вы используете Windows 8, тогда:

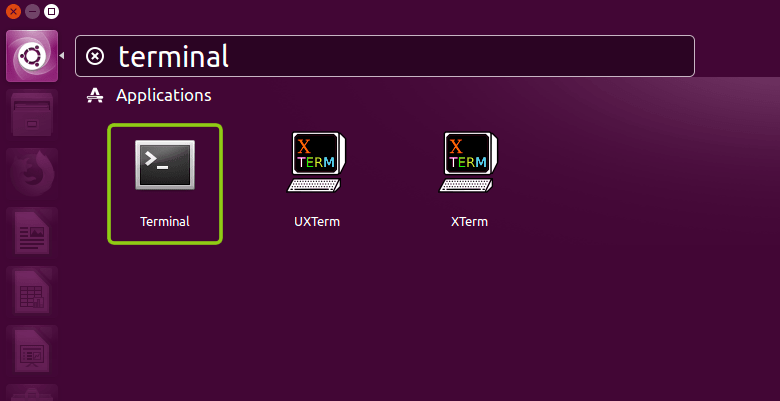
Пуск -> Приложения -> Подключение к удалённому рабочему столу

Если вы используете Windows 10, тогда:

Пуск -> Все приложения (может этого пункта не быть!) -> Стандартные Windows -> Подключение к удалённому рабочему столу

Или же просто нажмите комбинацию клавиш **Win+R** и в открывшемся окне наберите **mstsc**  
  
  
  
В открывшемся окне наберите IP-адрес вашего виртуального сервера и нажмите кнопку «Подключить». IP-адрес сервера вы можете видеть в вашем личном кабинете в разделе «Мои серверы»:  
  
  
  
****  
  
Если вы заказали сервер с 2-я или большим количеством IP-адресов, то для подключения к серверу вы можете использовать любой из них – это ни на что не влияет.  
  
Те, кто впервые стакиваются с созданием удалённого рабочего стола, часто задаются вопросом «Зачем нужны эти IP-адреса и сколько нужно именно им», часто также путают количество IP-адресов с количеством рабочих столов или учётных записей, или полагают, что если зайти на сервер по одному адресу, то открывая браузер именно этот адрес будет браузер использовать. Нас самом же деле это всего лишь список внешних адресов, по которому можно подключиться к серверу, сама работа на сервере уже после подключения никаким образом не меняется.  
  
Чаща всего при подключении по умолчанию настроена автоматическая передача данных из буфера обмена, а также подключаются к серверу и становятся на нём видны локальные диски устройства, с которого вы подключаетесь. При сразу после нажатия на кнопку «Подключить» вы можете увидеть уведомление о возможном вреде, который может нанести как удалённый компьютер вашему, так и ваш удалённому. Такое вполне возможно если вы подключаетесь к чужому серверу, на котором могут быть вирусы или вы подключаетесь к своему проведенному серверу с чужого заражённого ПК.  
  
  
  
Подключаясь к только что созданному и чистому серверу можно смело отключить дальнейшие уведомления и продолжить процесс подключения.  
  
Далее вы увидите окно с вводом авторизационных данных:  
  
  
  
При создании каждого нового сервера система VPS.house автоматически генерирует новый уникальный пароль для него, при этом на всех серверах Windows по умолчанию остаётся имя пользователя **Administrator**. Пароль от сервера отображается также в личном кабинете возле вашего сервера на странице «Мои серверы»:  
  
  
  
В целях безопасности, по умолчанию пароль от сервера скрыт и отображается только по нажатию на ссылку «Показать пароль», при этом сайт попросит вас ввести пароль от вашей учётной записи на VPS.house.  
  
Обратите, пожалуйста, внимание на то, что очень часто при попытке подключения с Windows 7 если копировать и вставлять пароль, система показывает ошибку о неверно введённых учетных данных, тоже самое может возникать и в других версиях. Если вы с этим столкнулись, просто **введите пароль вручную** и обязательно с учётом регистра (заглавные буквы вводите заглавными, а строчные строчными и строго в английской раскладке клавиатуры).  
  
После успешной авторизации перед началом сессии вы получите уведомление о **неуспешной проверке подлинности удаленного компьютера**. Причина этого уведомления в том, что сессия на стороне сервера шифруется по умолчанию с помощью SSL-сертификата, который сгенерировал сам же сервер, а не тем, что мог быть выдан авторизованным центром сертификации.  
  
  
  
Данное уведомление не говорит о проблемах безопасности, и вы смело можете отключить его для будущих подключений к этому же серверу, отметив галочкой «Больше не выводить запрос о подключениях к этому компьютеру».  
  
Если вы используете для работы **Windows XP** и при подключении система выдает ошибку с текстом *«Удаленный компьютер требует проверку подлинности на уровне сети, которую данный компьютер не поддерживает»*, значит на ваш ПК очень сильно устарел и нужно дополнительно установить небольшое обновление, где его взять и как установить [мы подробно расписали здесь](https://vps.house/help/credSSP).  
  
Встроенная программа подключения к удалённому рабочему столу позволяет с лёгкостью передавать файлы на сервер, копируя их на вашем ПК и вставляя в любую папку уже на самом сервере и наоборот. Помимо этого, можно включить передачу на сервер практически любых USB-устройств и сетевых принтеров и сканеров.  
  
Для включения этих возможностей перед подключением к серверу нажмите на кнопку «Показать параметры»:  
  
  
  
Откроется режим расширенных настроек подключения к вашему VDS серверу. Перейдите на вкладку «Локальные ресурсы» и отметьте галочкой требуемые для вас устройства:  
  
  
  
  
  
Еще одна очень полезная и популярная функция – это возможность **создать готовый файл подключения (так называемый «ярлык»)**, в котором уже сохранены все нужные вам настройки и данные авторизации на сервере. Это особенно удобно если вы хотите дать доступ сотруднику, который не является опытным пользователем ПК.  
  
  
  
Для этого также в расширенных настройках подключения на вкладке «Общие» введите имя пользователя (на серверах VPS.house это всегда по умолчанию Administrator), отметьте галочкой «Разрешить мне сохранять учетные данные», чтобы не приходилось вводить пароль каждый раз и, по завершению внесения всех нужных вам остальных параметров подключения (если таковые есть), нажиме кнопку «Сохранить как»:  
  
  
  
В итоге вы получите готовый файл с подключением, который вы можете отправить вашему коллеге и тот в свою очередь подключится к серверу 2-я простыми кликами по нему мышкой.  
  
В целях безопасности по умолчанию в данный файл не будет добавлен пароль от учётной записи, он будет запрошен при первом подключении.

**Как подключиться к серверу по RDP если вы работаете с Ubuntu**

Протокол подключения к уделённому рабочему столу Windows (RDP) – это закрытый протокол компании Microsoft, официальных служб под операционные системы Linux Microsoft не выпускает, но так или иначе уже давно существуют стабильно работающие решения, которые в последних редакциях Ubuntu даже включены в изначальную сборку.  
Речи идет о клиенте под названием **Remmina**  
По умолчанию если Remmina включена в вашу сборку, вы можете найти ее в Поиске по запросу «Remote Desktop Client», если ее нет, то установите ее при помощи следующих команд в Терминале.  
  


1. Устанавливаем пакет Remmina

sudo apt-add-repository ppa:remmina-ppa-team/remmina-next

1. Устанавливаем обновления

sudo apt-get update

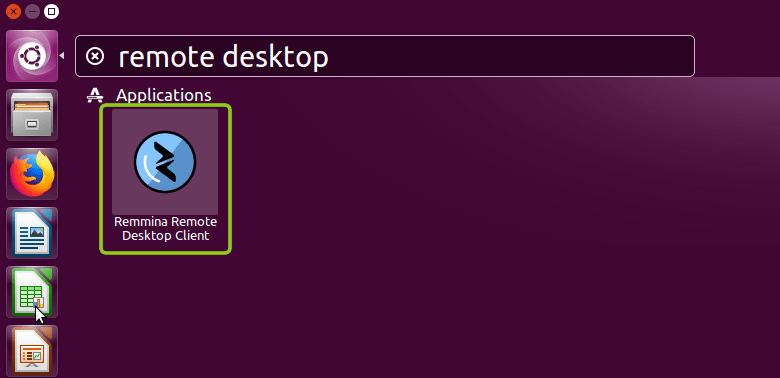
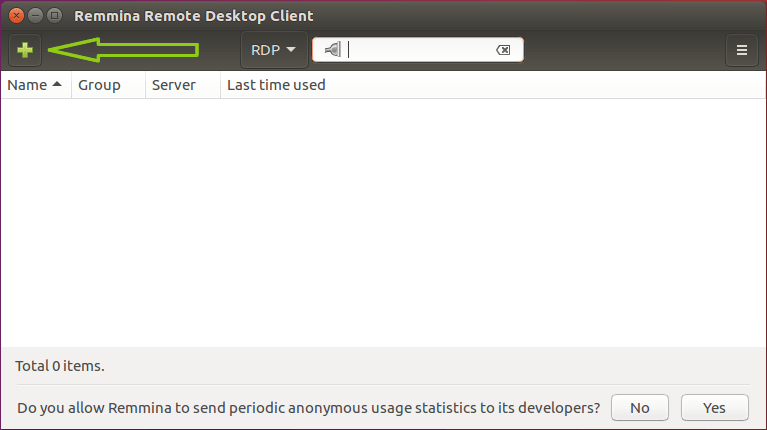
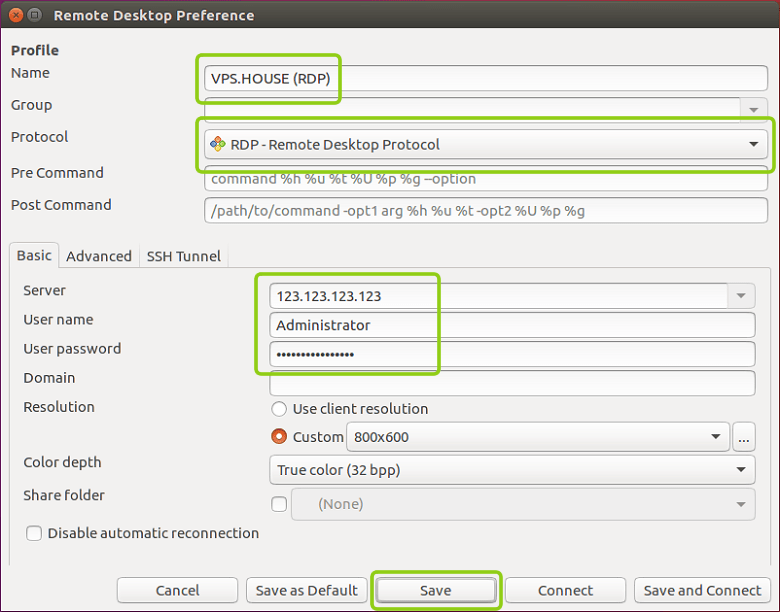
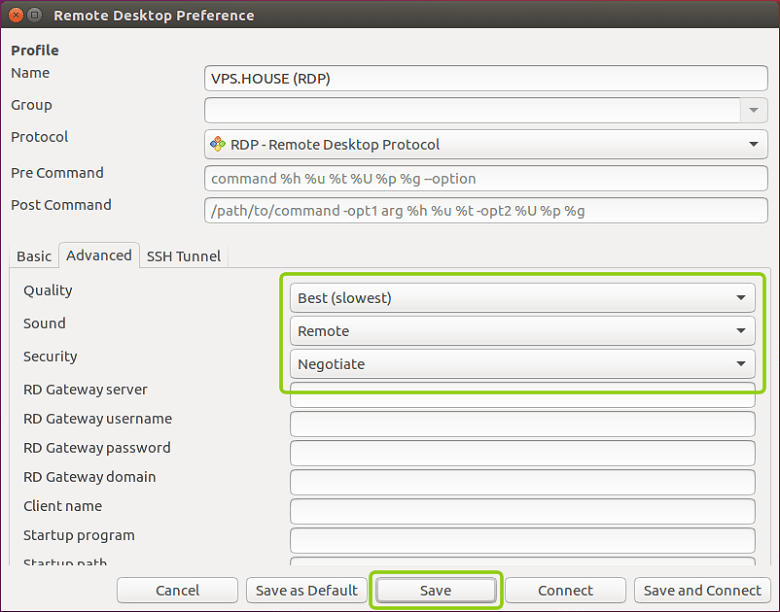
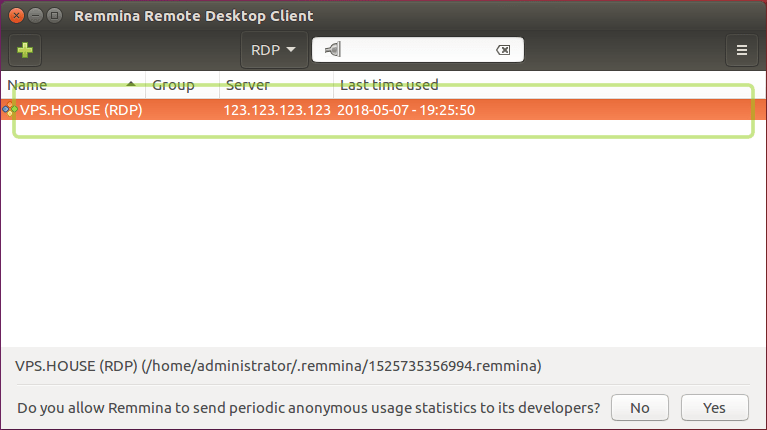
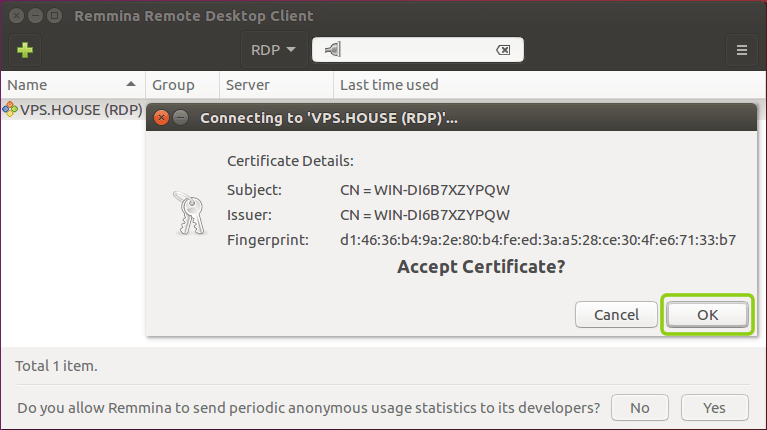
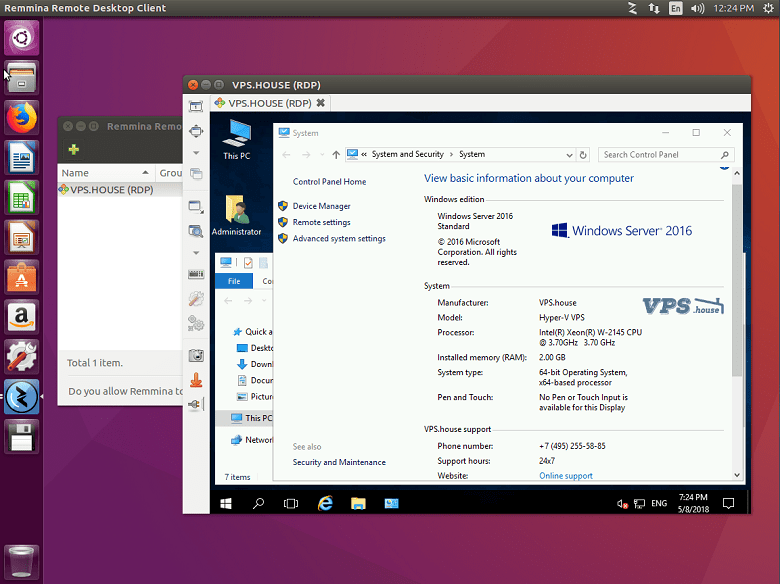
1. Устанавливаем плагин протокола RDP

sudo apt-get install remmina remmina-plugin-rdp libfreerdp-plugins-standard

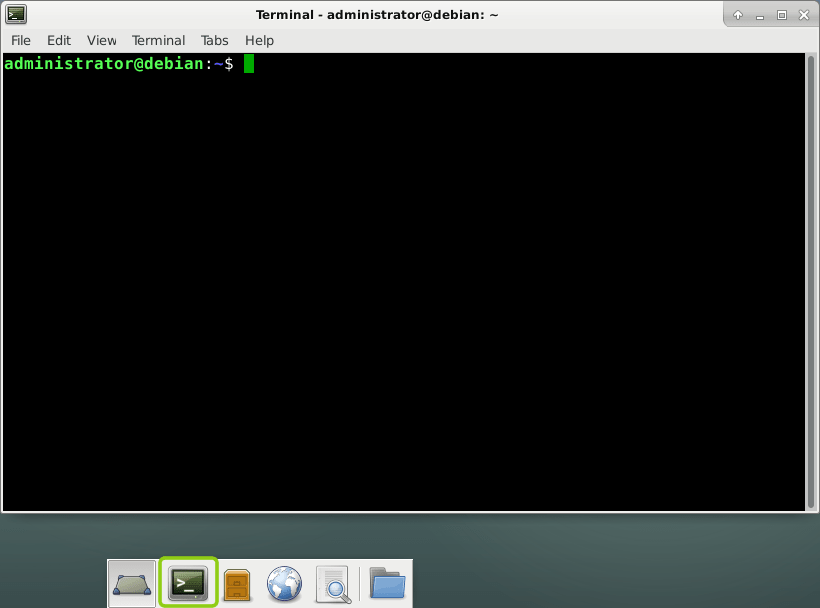
1. Если ранее у вас уже была установлена какая-либо версия Remmina или была запущена до установки, то ее необходимо перезапустить. Это лучше всего сделать перезагрузкой компьютера или с помощью команды:

udo killall remmina

Если после её выполнения вы получили сообщение об ошибке типа «процесс не найден», значит и так все хорошо и можно было команду и не выполнять.

В меню поиска наберите «remote desktop» или «remmina», чтобы найти установленное приложение:  
  
  
Remmina позволяет добавлять и сохранять список подключений для быстрого доступа к тому или иному серверу. Для сознания нового нажмите на «+», как показано на изображении:  
  
Заполните поля авторизационными данными, которые [указаны в вашем личном кабинете](https://habr.com/ru/company/vps_house/blog/358488/#account):  
  
  
  
На вкладке «Advanced» вы можете также указать качество подключения к серверу и детализации при передаче изображений:  
  
  
  
После сохранения данных вы всегда сможете найти ваш сервер в списке подключений Remmina. Для подключения к серверу теперь достаточно просто кликнуть дважды мышкой по строке сервера:  
  
  
  
Если вы подключаетесь к серверу впервые с этого приложения, то оно может показать информацию о ошибке в сертификате безопасности. Почему это происходит [мы описали выше в блоке подключения к серверу из десктопной Windows](https://habr.com/ru/company/vps_house/blog/358488/#ssl).  
Достаточно нажать «ОК» и программа продолжит подключение к вашему серверу:  
  
  
  


**Как подключиться к серверу по RDP если вы работаете с Debian**

Протокол RDP (Remote Desktop Protocol) – это закрытый протокол удалённого рабочего стола Microsoft. К сожалению, они не выпускают официальных клиентов для работы подключения к серверам Windows с операционных систем, работающих на базе Linux. Однако уже довольно давно существуют стабильно работающие решения.  
Одно из самых популярных – это клиент для всевозможных удалённых **Remmina**, именно его мы и рекомендуем использовать для включения к серверам VPS.house или любым другим под управлением ОС Windows.  


1. Указываем путь к установочным файлам

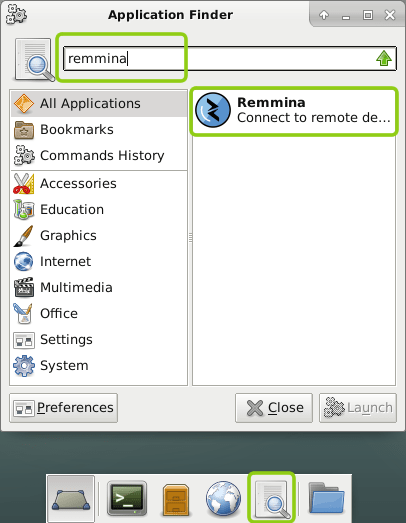
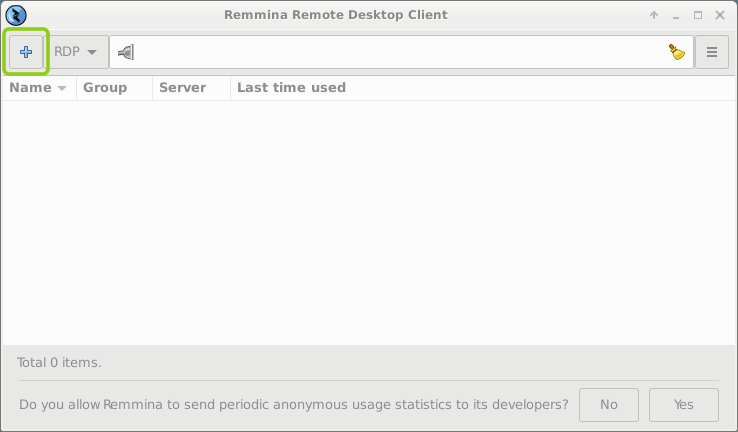
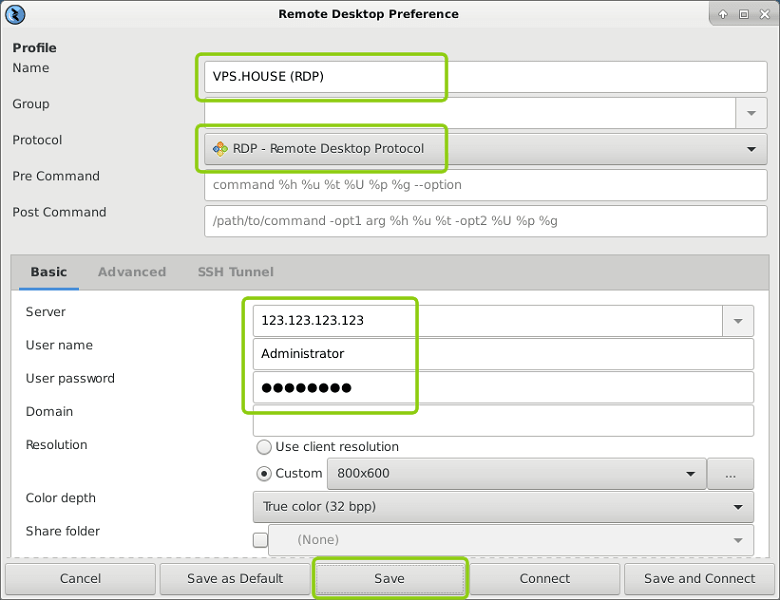
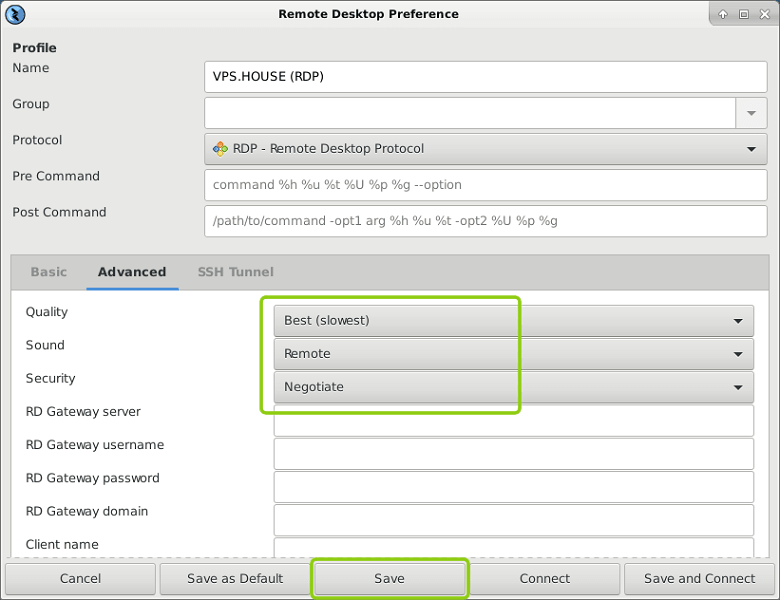
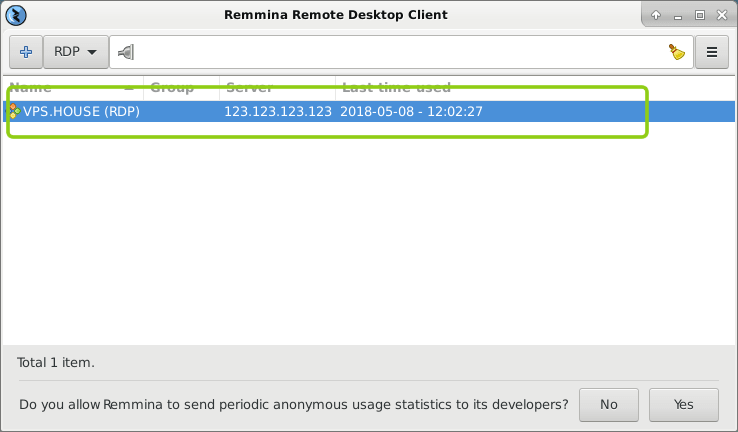
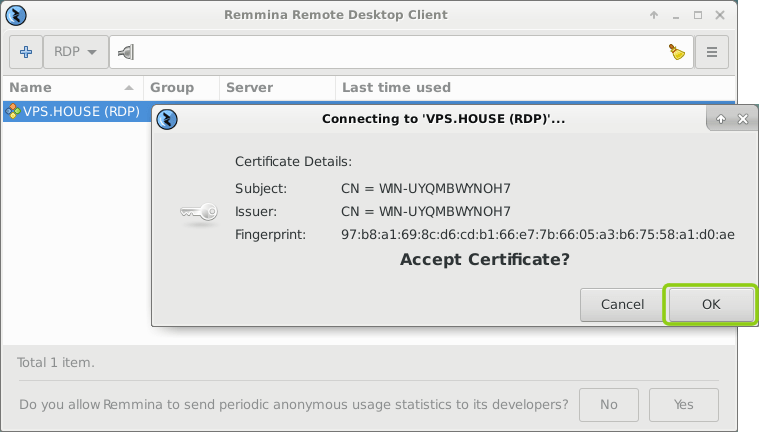
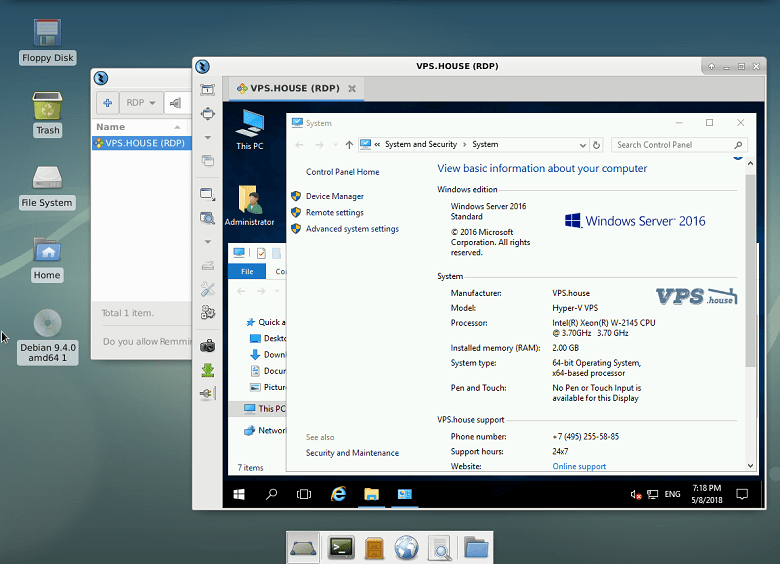
echo 'deb http://ftp.debian.org/debian stretch-backports main' | sudo tee --append /etc/apt/sources.list.d/stretch-backports.list >> /dev/null

1. Запускаем процесс установки

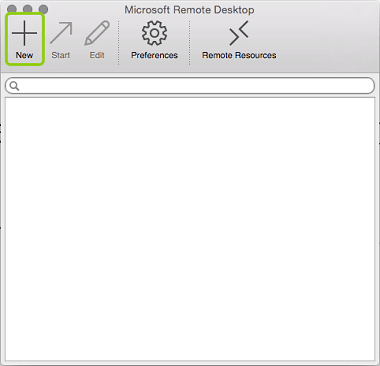
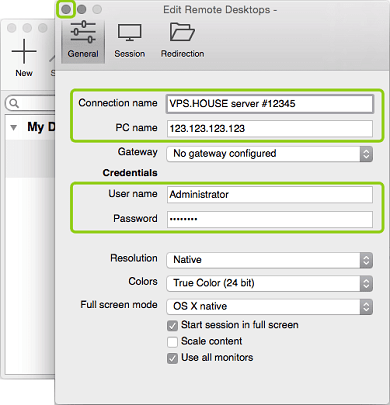
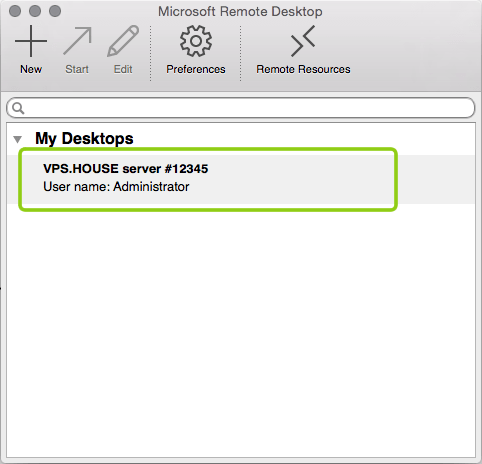
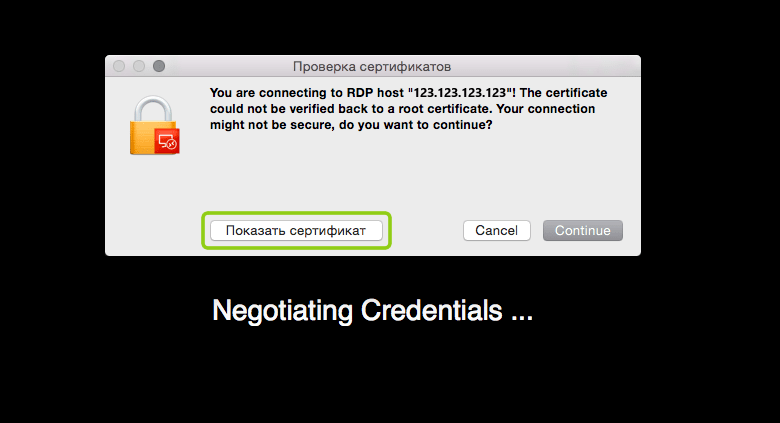
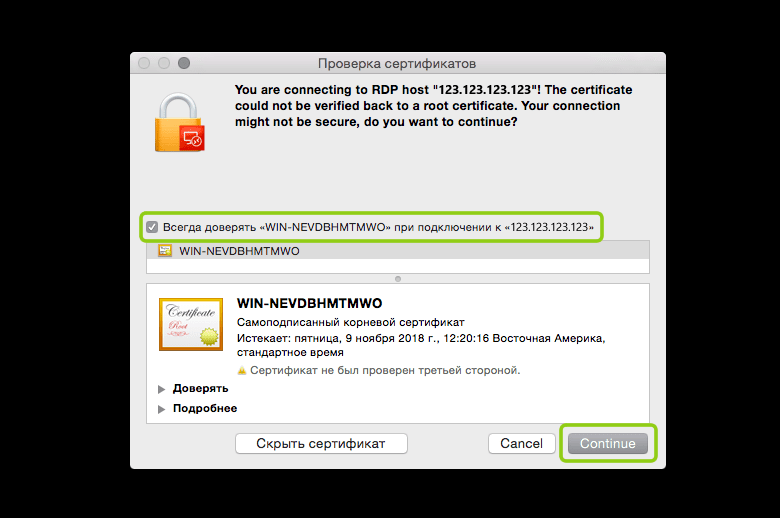
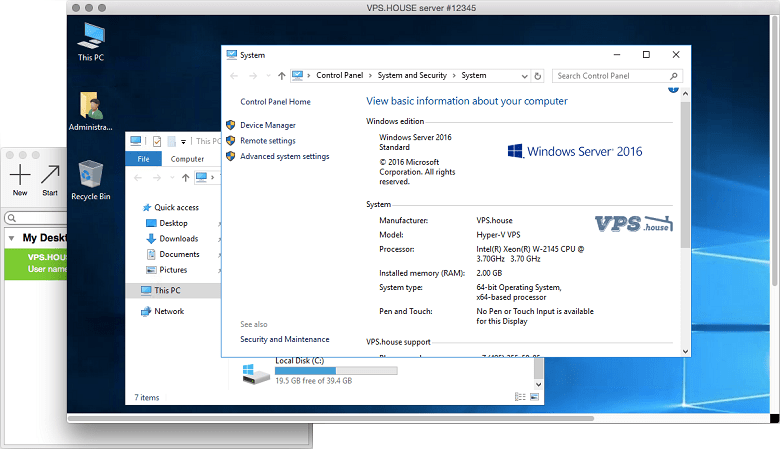
sudo apt update

1. Устанавливаем плагин протокола RDP

sudo apt install -t stretch-backports remmina remmina-plugin-rdp remmina-plugin-secret libfreerdp-plugins-standard

Сразу после установки приложение можно найти через поиск программ:  
  
  
В отличие стандартного от RDP-клиента ОС Windows, Remmina позволяет сохранять в список все свои подключения к различным серверам и осуществлять моментальный доступ к ним. Для добавления первого сервера в список нажмите «+» в левом верхнем углу:  
  
  
  
В открывшемся окне задайте параметры подключения к вашему серверу и введите удобное для запоминания имя сервера. Все необходимые для подключения данных [указаны в вашем личном кабинете](https://habr.com/ru/company/vps_house/blog/358488/#account):  
  
  
На вкладке «Advanced» («Дополнительные») вы можете задать параметры передачи звука с сервера на ваш ПК, а также качество передаваемого изображения при подключении:  
  
  
  
После сохранения я настроек вы увидите новую строку в списке подключений. Для начала работы с сервером достаточно просто дважды кликнуть по нему мышкой:  
  
  
  
В момент первого подключения к серверу Remmina покажет уведомление у недоверенном сертификате шифрования. Это не является какой-либо ошибкой или проблемой безопасности. Причину этого сообщения [мы описали выше](https://habr.com/ru/company/vps_house/blog/358488/#ssl). Просто нажмите «ОК» и вы увидите рабочий стол вашего сервера, при условии, разумеется, что все данные для подключения ранее были введены корректно.  
  
  
  


**Подключение серверу по RDP из Mac OS**

Для подключения к удалённому рабочему столу для Mac OS компания Microsoft разработала и поддерживает официальный RDP-клиент. Он стабильно работает с любыми версиями ОС Windows.  
  
Программа обладает интуитивно понятным интерфейсом и позволяет создавать список серверов для дальнейшего моментального подключения к ним.  
Для добавления нового сервера в список нажмите «New», как показано на скриншоте:  
  
   
  
В открывшемся окне укажите авторизационные данные, как указано [в вашем личном кабинете](https://habr.com/ru/company/vps_house/blog/358488/#account) (IP-адрес сервера, логин Administrator и его пароль), и укажите произвольное название для нового подключения (Connection Name).  
  
По завершению ввода нажмите на кнопку закрытия окна – все данных сохранятся и появится строчка с вашим сервером в списке подключений:  
  
  
  
Кликните на эту строчку дважды мышкой, и вы подключитесь к серверу.  
  
При попытке подключения к вашему VPS серверу если он работает на Windows Server 2008 или более новой версии, программа покажет уведомление о том, что не удалось проверить сертификат шифрования. Это не является проблемой безопасности, а всего лишь говорит о том, что сертификат выдан не сертифицированным центром, а сгенерирован самим же сервером.  
  
Для того, чтобы это сообщение в будущем не возникало для этого сервера, нажмите «Показать сертификат».  
  
  
  
Отметьте галочкой «Всегда доверять…» и нажмите «Continue».  
  
  
  
Если в настройках подключения все параметры были введены без ошибок (IP-адрес, логин и пароль), то вы сразу же увидите рабочий стол вашего Windows Server:  
  


**Вывод:** разобрался, как работает протокол RDP, где используется и как подключаться с различных систем.