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: Кшнякин Владислав

Дисциплина/Профессиональный модуль: Инфокоммуникационные системы и сети

Группы: 3ПКС-220

Преподаватель

Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва – 2022г.**

**Цель:** RDP – разобрать

**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.

Согласно условиям лицензирования, ОС Windows Server допускает по умолчанию не более 2-х одновременных подключений по RDP к серверу, если нужно больше, то понимается терминальный сервер и лицензируется либо количество пользователей, либо количество подключаемых устройств. Но, подключившись к серверу по RDP, вы также можете поставить любое удобное вам решение для удалённого управления рабочим столом: TeamViewer, RAdmin и прочие.

## Режим подключений

RDP используют в 3 режимах:

1. Подключение через протокол к серверной ОС для настройки или управления. Это связано с тем, что Windows Server поддерживает параллельно два удаленных подключения и один локальный вход, а рабочие станции – только один вариант.
2. RDP служит транспортом для соединения с терминальным сервером. Такой режим доступен только для серверных ОС. Количество подключений безлимитное, но потребуется установка сервера лицензий.
3. Подключение к рабочей станции. Пользователь, используя RDP, соединяется со своим офисным либо домашним компьютером для дальнейшей работы.

Если требуется установить соединение между ОС семейства Windows и Linux, то для второй используют приложения, которые поддерживают работу с протоколом RDP, например, Remmina, Rdesktop, Vinagre и др.

## Принцип работы

Принцип работы RDP базируется на протоколе TCP. Соединение клиент-сервер происходит на транспортном уровне. После инициализации пользователь проходит аутентификацию. В случае успешного подтверждения сервер передает клиенту управление.

Протокол RDP внутри себя поддерживает виртуальные каналы, через которые пользователю передаются дополнительные функции операционной системы, например, можно распечатать документ, воспроизвести видео или скопировать файл в буфер обмена.

## Безопасность

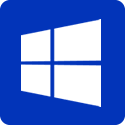
Технология обеспечивает безопасность подключения двумя способами. В первом используется внутренняя подсистема (Standard RDP Security). На удаленной машине генерируется пара ключей RSA и сертификат открытого ключа, который подписывается одним из них.

Во время подключения клиент получает подписанный сертификат и открытый ключ, который используется для выбора технологии шифрования данных. Длина ключа шифрования зависит от версии операционной системы, в старых версиях Windows Server 2008 значение составляло 168 бит. Авторизация происходит после подтверждения сертификата и ввода пароля.

Второй способ предлагает использовать внешние средства обеспечения безопасности (Enhanced RDP Security). В качестве примера расскажем про протокол TLS. Во время инициализации подключения он шифрует соединение и проверяет разрешение пользователя на вход. Такой подход снижает нагрузку на терминальный сервер при большом количестве одновременных подключений. Принцип работы аналогичен первому варианту. Как правило, крупные компании используют второй вариант, а небольшие – первый.

Протокол RDP используется для удаленного подключения только в среде Windows. Соединение полностью безопасно, так как использует шифрование и процедуру аутентификации пользователей. Для других операционных систем существует специальное ПО, которое поддерживает работу с RDP.

**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:

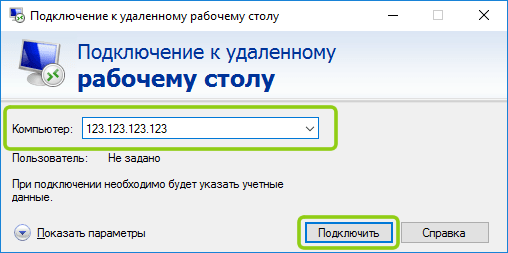
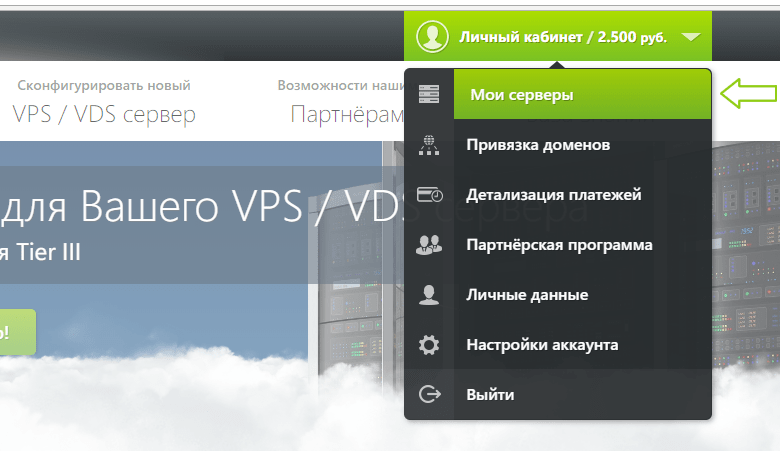
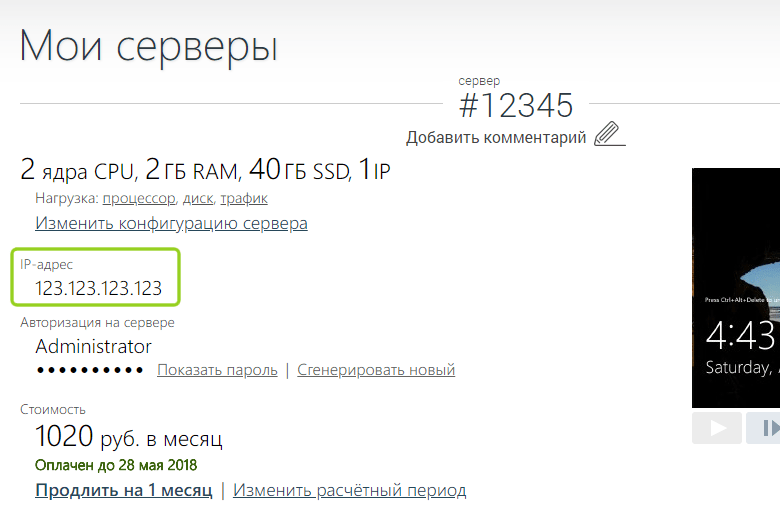
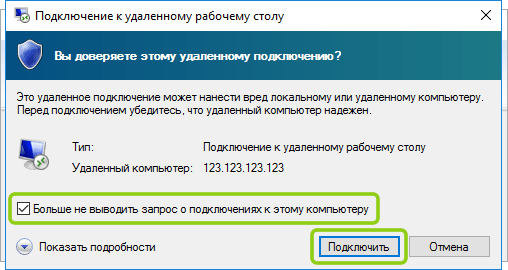
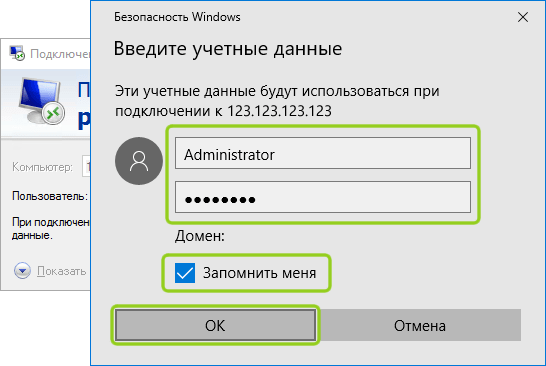
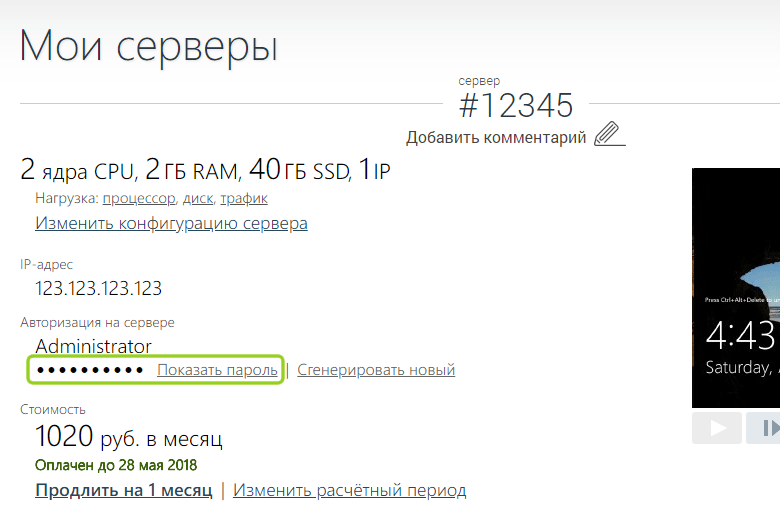
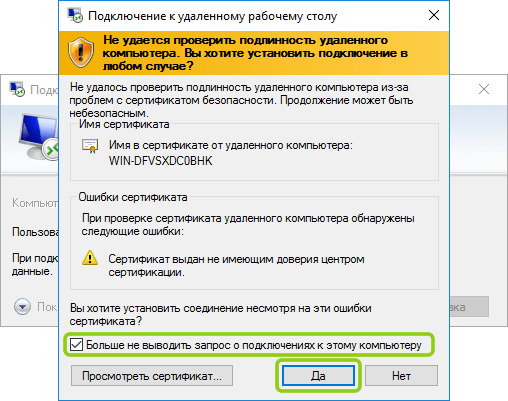
Пуск -> Программы -> Стандартные -> Подключение к удалённому рабочему столу

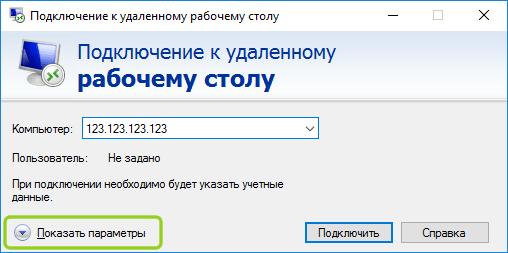
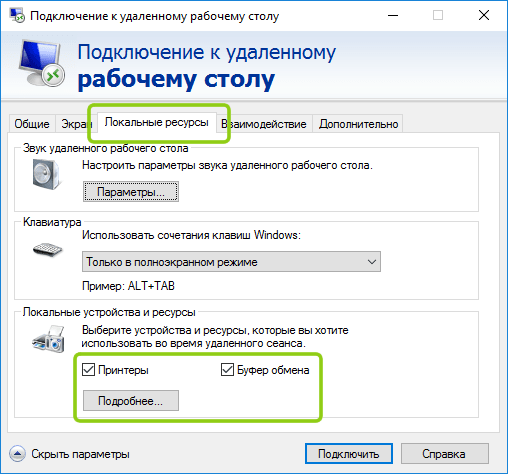
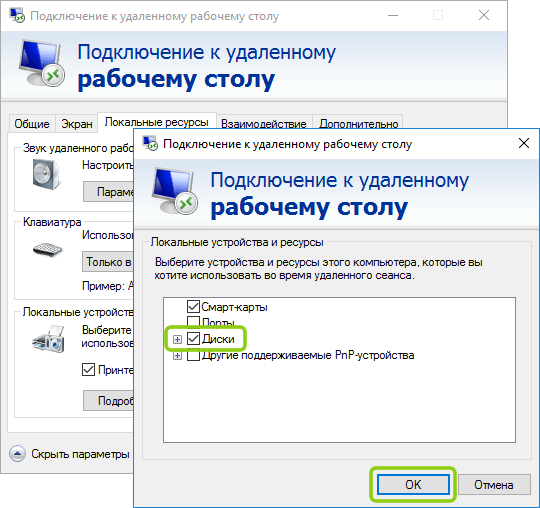
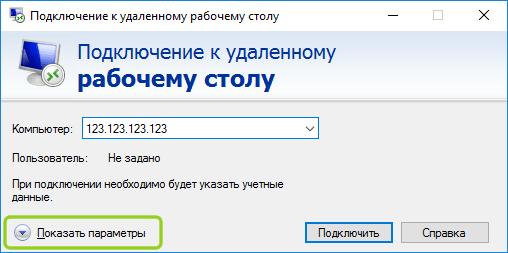
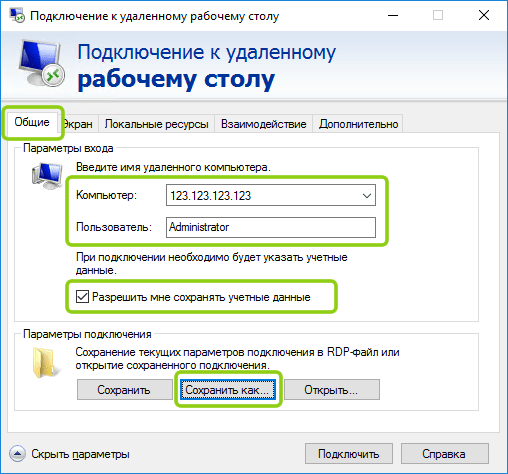
Если вы используете Windows 8, тогда:

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».

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

**Вывод:** RDP - разобрал