Федеральное государственное образовательное бюджетное учреждение высшего образования   
 **«Финансовый университет при Правительство Российской Федерации»** **(Финансовый университет)**   
 Колледж информатики и программирования

**ОТЧЁТ**

**По лабораторной работе №11**

Дисциплина/Профессиональный модуль: Информационные системы и сети

Выполнил:

студент группы 3 ПКС-120

Колбаса Д.В.

Преподаватель: Сибирев И.В.

Оценка за работу :\_\_\_\_\_\_\_

**Москва 2022г.**

**Лабораторная работа № 11**

Цель: Ознакомиться с программным обеспечением для удаленного доступа к машине

Задание:

RDP - Разобрать

Выполнение работы

**Что такое RDP**

Удалённый рабочий стол позволяет подключиться к другому компьютеру, видеть его экран, запускать программы на нём и работать за ним так, будто бы вы сидите перед ним.

Протокол удалённого рабочего стола (Remote Desktop Protocol, RDP) — это проприетарный протокол Microsoft, который предоставляет пользователю графический интерфейс для подключения к другому компьютеру через сетевое соединение. Для этого пользователь запускает клиентское программное обеспечение RDP, а на другом компьютере должно быть запущено программное обеспечение сервера RDP.

Клиенты для подключения по RDP существуют для большинства версий Microsoft Windows (включая Windows Mobile), Linux, Unix, macOS, iOS, Android и других операционных систем. RDP-серверы встроены в операционные системы Windows; RDP-сервер для Unix и OS X также существует. По умолчанию сервер прослушивает TCP-порт 3389 и UDP-порт 3389.

В настоящее время Microsoft называет своё официальное клиентское программное обеспечение RDP «Подключение к удалённому рабочему столу» (Remote Desktop Connection), которое ранее называлось «Клиент служб терминалов» (Terminal Services Client).

Файл клиента называется **mstsc.exe**.

## Как включить удалённый рабочий стол RDP

Клиент и сервер присутствуют по умолчанию во всех версиях Windows. Для запуска клиента не требуется дополнительная настройка.

Что касается сервера, то он может быть отключён и/или доступ к порту RDP может быть заблокирован файерволом.

### Как включить удалённый рабочий стол на Windows 10 и Windows 11 с помощью SystemPropertiesRemote

Это универсальный способ включения RDP, работающих в большинстве Windows.

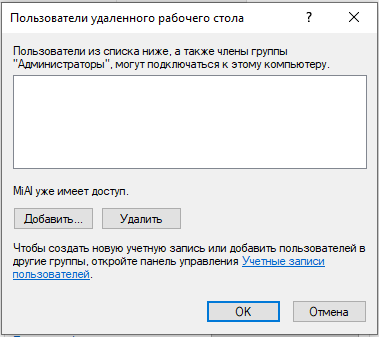
Нажмите **Win+r** и введите:

**SystemPropertiesRemote**

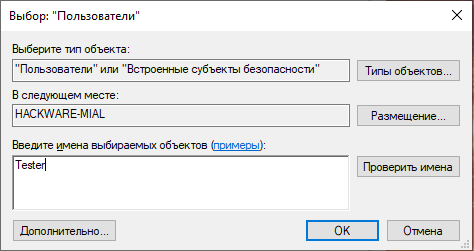
В открывшемся окне выберите «**Разрешить удалённые подключения к этому компьютеру**»:

[](https://hackware.ru/wp-content/uploads/2020/04/SystemPropertiesRemote-settings.png)

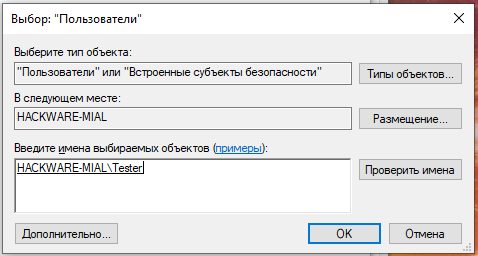
При необходимости добавьте пользователей, которые могут удалённо подключиться, щёлкнув «**Выбрать пользователей**». Члены группы «Администраторы» получают доступ автоматически:

[](https://hackware.ru/wp-content/uploads/2020/04/SystemPropertiesRemote-users.png)

Чтобы правильно добавить пользователя, введите его имя:

[](https://hackware.ru/wp-content/uploads/2020/04/SystemPropertiesRemote-users-2.png)

И нажмите кнопку «**Проверить имена**»:

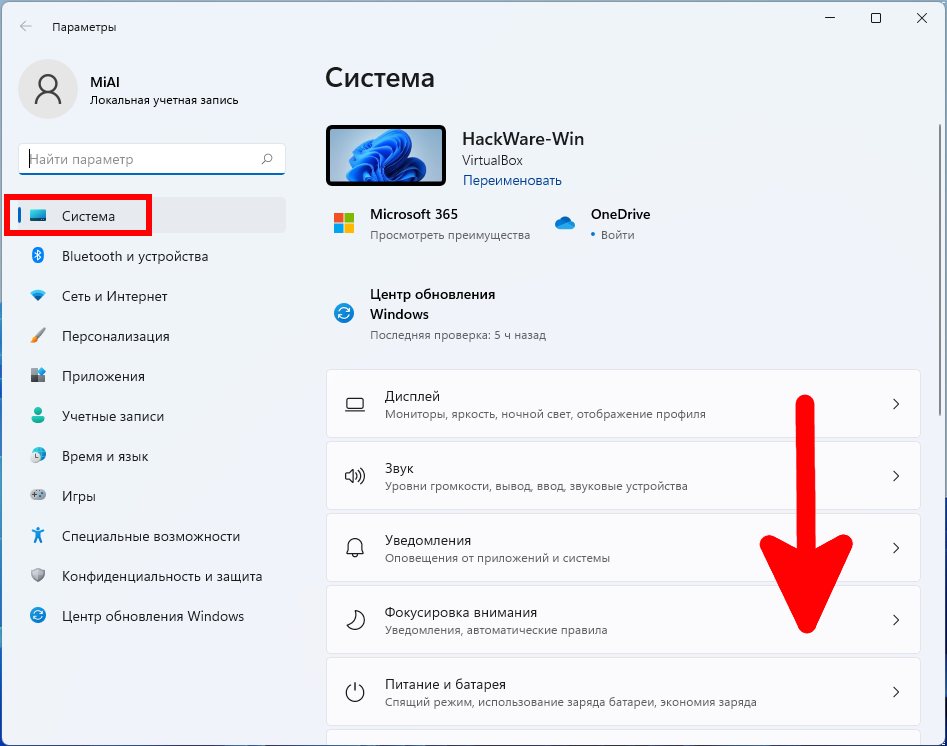
[](https://hackware.ru/wp-content/uploads/2020/04/SystemPropertiesRemote-users-3.png)

Команду **SystemPropertiesRemote** также можно запустить в командной строке, либо в PowerShell.

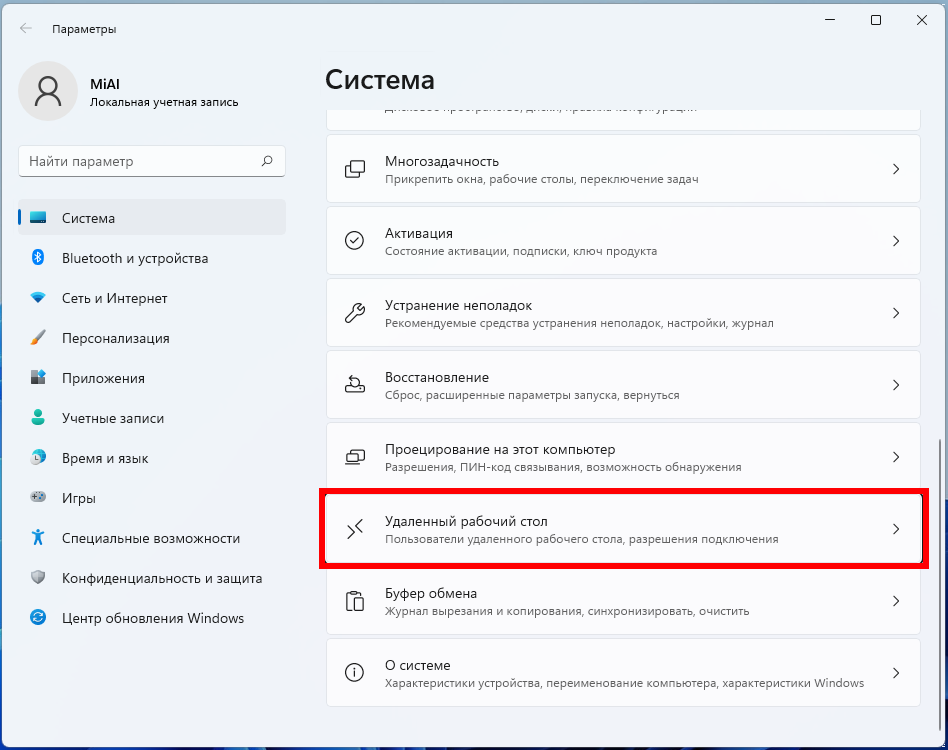
### Как включить удалённый рабочий стол на Windows 11 в графическом интерфейсе

Откройте «**Параметры**», для этого нажмите **Win+i**.

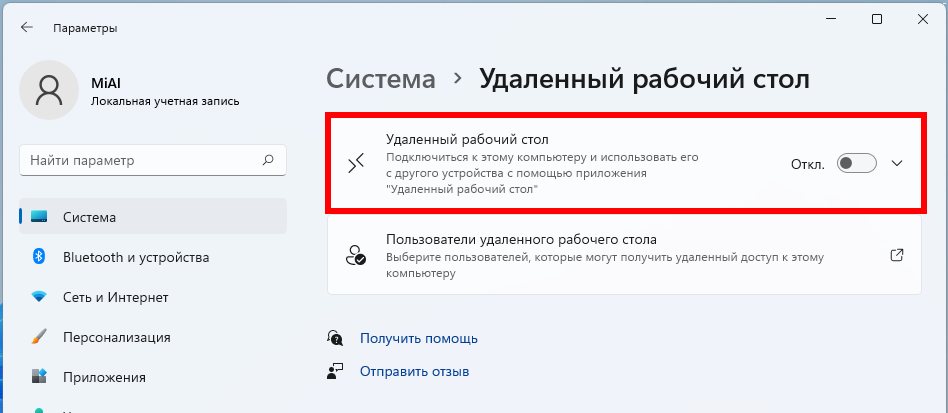
На вкладке «**Система**» прокрутите список пунктов вниз.

[](https://zawindows.ru/wp-content/uploads/2020/04/rdp.png)

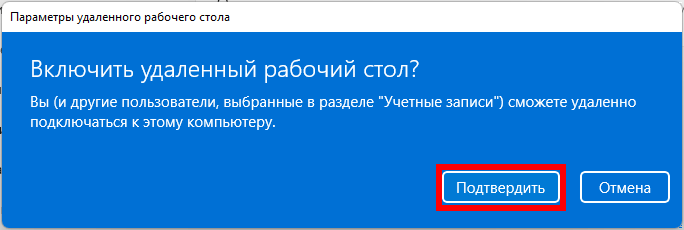
Найдите и кликните «Удалённый рабочий стол».

[](https://zawindows.ru/wp-content/uploads/2020/04/rdp-2.png)

На вкладке «Удалённый рабочий стол» включите соответствующий ползунок.

[](https://zawindows.ru/wp-content/uploads/2020/04/rdp-3.png)

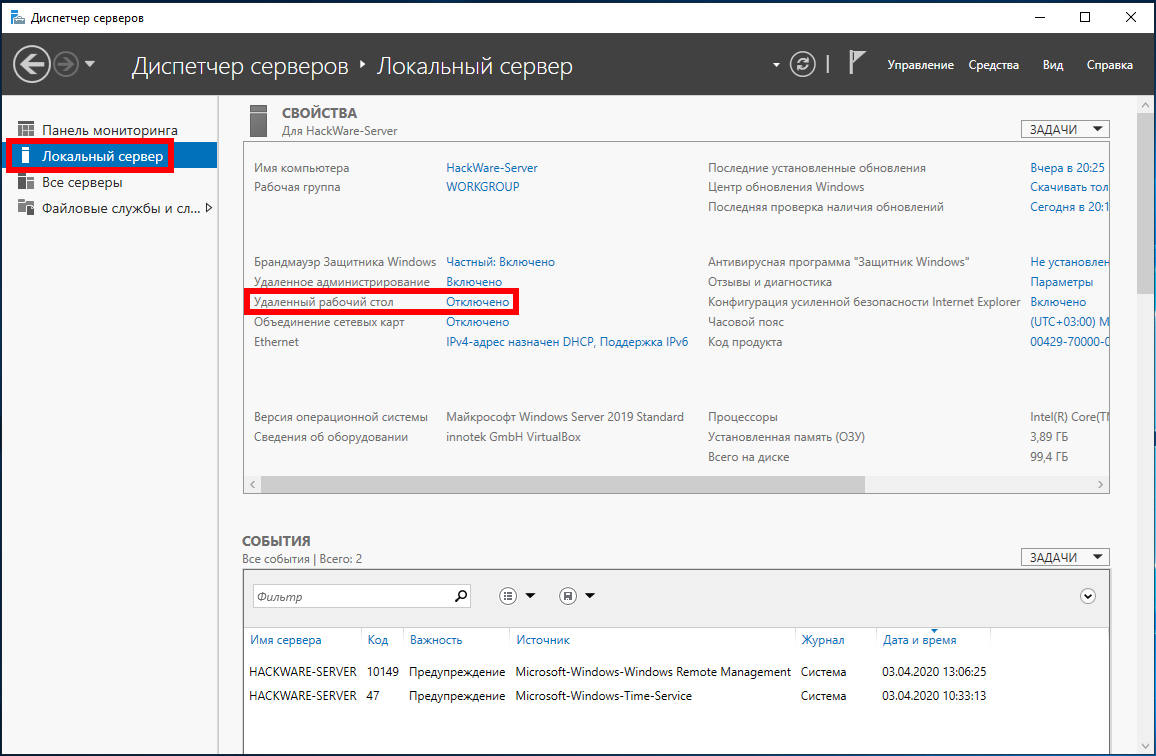
Подтвердите выбранное действие:

[](https://zawindows.ru/wp-content/uploads/2020/04/rdp-4.png)

Также вы можете выбрать пользователей, которые могут подключаться удалённо к компьютеру.

### Как включить удалённый рабочий стол на Windows Server 2019/2022 в настройках (графический интерфейс)

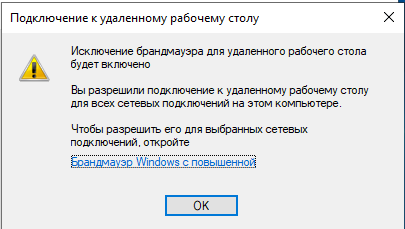
Если вы не дружите с терминалом, вы также можете включить службу RDP из графического интерфейса сервера. Откройте **Диспетчер серверов** из меню «**Пуск**» и нажмите на «**Локальный сервер**» в левой части. Найдите пункт «**Удалённый рабочий стол**» и кликните по слову «**Отключено**»:

[](https://hackware.ru/wp-content/uploads/2020/04/ServerManager.png)

В открывшемся окне выберите «**Разрешить удалённые подключения к этому компьютеру**»:

[](https://hackware.ru/wp-content/uploads/2020/04/SystemPropertiesRemote-settings.png)

Согласитесь с изменением правила файервола:

[](https://hackware.ru/wp-content/uploads/2020/04/windows-server-firewall-rdp.png)

## Как настроить подключение к RDP из Интернета

RDP разрешает любые подключения, будь то из локальной сети или из Интернета. Для подключения из Интернета требуется, чтобы у вашего компьютера был [белый IP](https://hackware.ru/?p=11589).

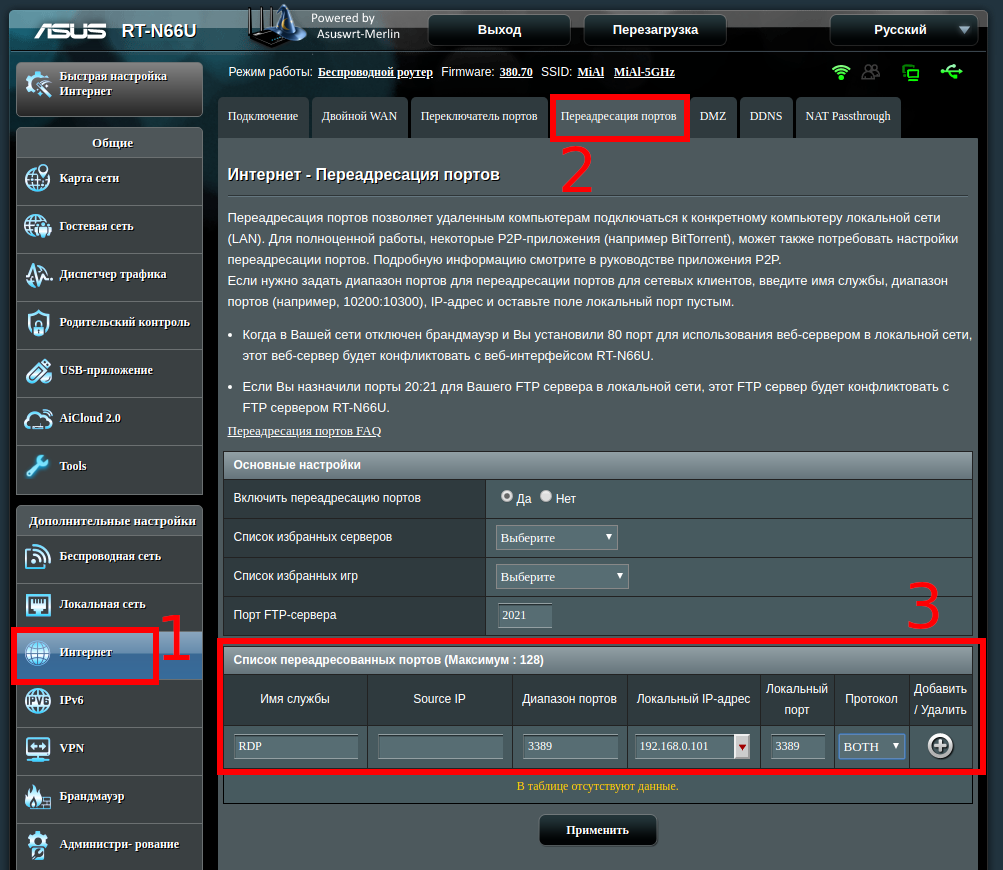
Если же ваш Интернет-провайдер использует [NAT](https://apache-windows.ru/apache-forwarding-%D0%BF%D1%80%D0%BE%D0%B1%D1%80%D0%BE%D1%81%D0%BA%D0%B0-%D0%BF%D0%BE%D1%80%D1%82%D0%BE%D0%B2-%D0%B2%D0%B5%D0%B1-%D1%81%D0%B5%D1%80%D0%B2%D0%B5%D1%80%D0%B0/#nat), то вам нужно арендовать внешний (белый) IP адрес.

Если вы подключены к роутеру (они тоже всегда используют NAT), то вам нужно настроить проброску (форвардинг, переадресацию) портов следующим образом:

1. Начать нужно с «[Настройки постоянного IP в Windows](https://hackware.ru/?p=4780#windows-static-ip)».

2. Последующие настройки нужно делать в роутере. Поскольку у всех разные модели роутеров, то конкретные действия и названия вкладок в панели администрирования роутеров могут различаться. Главное понять суть и найти соответствующую вкладку в роутере. Помните, что нужно перенаправить порты TCP и UDP с номером 3389.

Перейдите в панель управления роутером. В настройках роутера перейдите в раздел «**Интернет**» (может называться **WAN**), затем во вкладку «**Переадресация портов**» (может называться «**Перенаправление портов**», «**Port Forwarding**»):

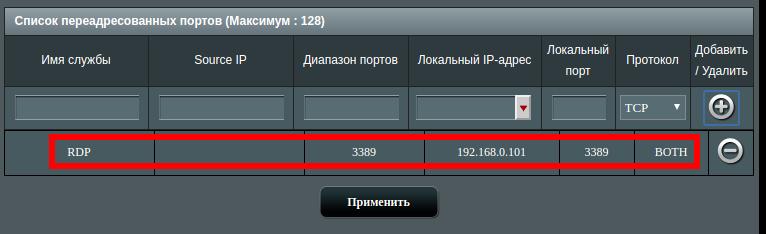
[](https://hackware.ru/wp-content/uploads/2020/04/rdp-router.png)

3. Добавьте новое правило:

* **Имя службы** — введите любое
* **Source IP** (исходный IP адрес) оставьте пустым
* **Диапазон портов** — укажите порт 3389
* **Локальный IP адрес** — укажите IP адрес компьютера Windows, к которому будет выполняться подключение по RDP
* **Локальный порт** — укажите порт 3389
* **Протокол** — укажите Both (оба)

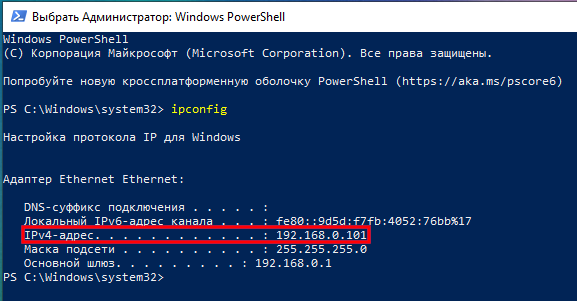
4. И нажмите кнопку «**Добавить**».

5. Сохраните сделанные изменения.

[](https://hackware.ru/wp-content/uploads/2020/04/router-forwarding-3389.png)

IP адрес компьютера Windows можно посмотреть командой:

|  |  |
| --- | --- |
| 1 | ipconfig |

[](https://hackware.ru/wp-content/uploads/2020/04/ipconfig.png)

Про переадресацию портов, о том, что это такое (на примере веб сервера), дополнительно читайте в статье «Apache Forwarding — проброска портов веб-сервера».

Ещё одним вариантом является использование VPN (виртуальной частной сети), в которой каждому компьютеру присваивается локальный адрес, но сама виртуальная частная сеть включает компьютеры которые могут быть размещены за пределами реальной частной сети. Подробности о VPN смотрите в статье «Доступ к службам компьютера через NAT и с серым IP с помощью OpenVPN».

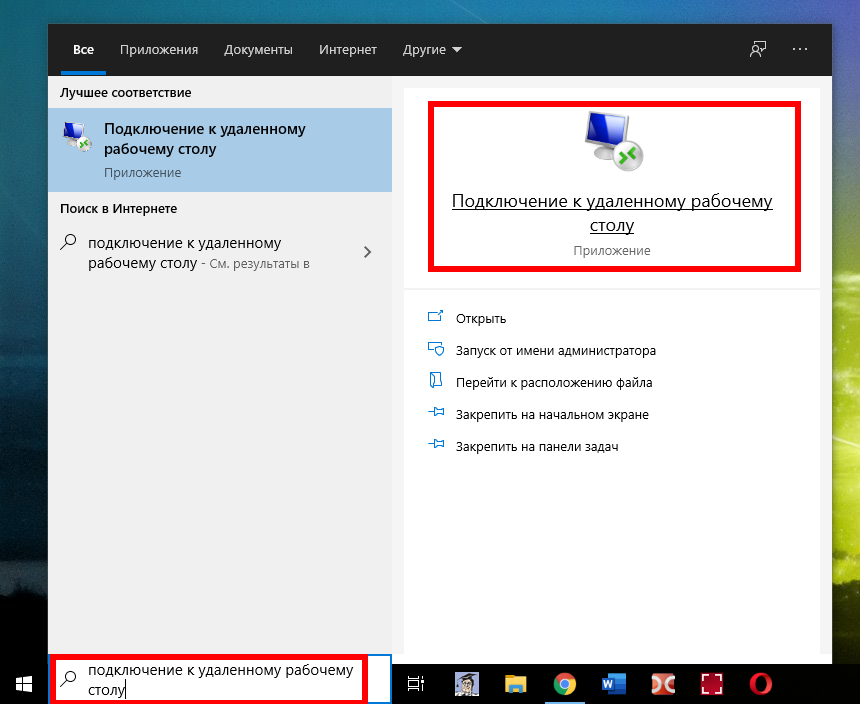
## Как подключиться к другому компьютеру и видеть его экран по RDP

Удалённый рабочий стол можно использовать для подключения к Windows 10 Pro и Windows 10 Корпоративная, Windows 8.1, Windows 8 Корпоративная и Windows 8 Pro, Windows 7 Pro, Windows 7 Корпоративная и Windows 7 Максимальная, а также для подключения к версиям выше Windows Server 2008. Подключиться к компьютерам под управлением выпуска "Домашняя" (например, Windows 10 Домашняя) нельзя.

Предварительная настройка или включение клиента RDP не требуется. Откройте командную строку (либо **Win+r**) и запустите:

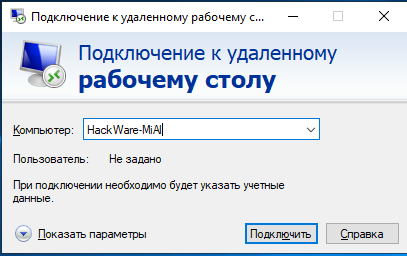
|  |  |
| --- | --- |
| 1 | mstsc |

Либо нажмите кнопку «**Пуск**» и начните набирать «**подключение к удаленному рабочему столу**»:

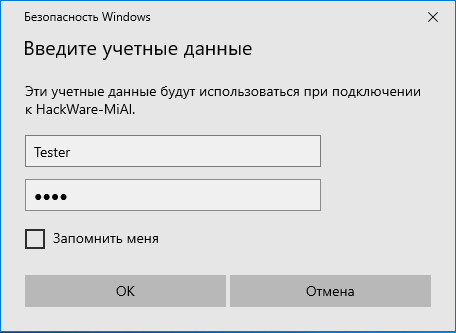
[](https://hackware.ru/wp-content/uploads/2020/04/rdp-gui.png)

Для подключения можно использовать IP либо имя компьютера. Если вы не знаете, что это такое, то смотрите статью «[Имя компьютера Windows: как изменить и использовать](https://zawindows.ru/%d0%b8%d0%bc%d1%8f-%d0%ba%d0%be%d0%bc%d0%bf%d1%8c%d1%8e%d1%82%d0%b5%d1%80%d0%b0-windows-%d0%ba%d0%b0%d0%ba-%d0%b8%d0%b7%d0%bc%d0%b5%d0%bd%d0%b8%d1%82%d1%8c-%d0%b8-%d0%b8%d1%81%d0%bf%d0%be%d0%bb%d1%8c/)».

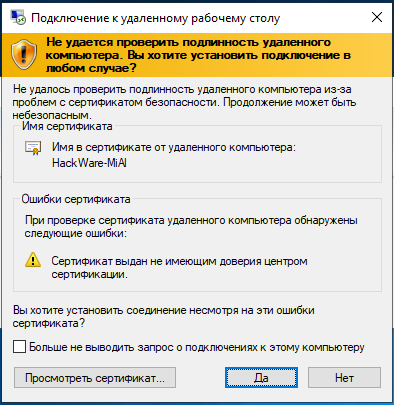
Введите IP либо имя компьютера, я буду использовать имя компьютера и подключусь к **HackWare-MiAl**:

[](https://hackware.ru/wp-content/uploads/2020/04/rdp-connect.png)

Вводим имя пользователя и пароль учётной записи на удалённом компьютере, то есть на том, к которому мы подключаемся. Можете поставить галочку «**Запомнить меня**», чтобы не вводить эти учётные данные в следующий раз:

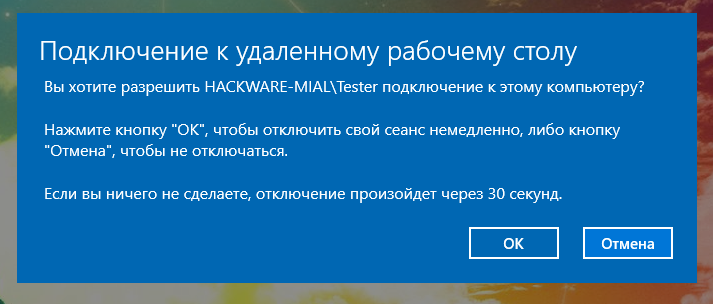
[](https://hackware.ru/wp-content/uploads/2020/04/rdp-connect-username.png)

Нажимаем «**Да**»:

[](https://hackware.ru/wp-content/uploads/2020/04/rdp-cert.png)

Система пишет, что в систему вошёл другой пользователь. Дело в том, что при подключении к удалённому компьютеру выполняется выход всех пользователей (в том числе того, от чьего имени мы подключаемся).

Если на удалённом компьютере выполнил вход какой-либо другой пользователь, то для него будет показано следующее сообщение:

[](https://hackware.ru/wp-content/uploads/2020/04/rdp-2-users.png)

Дело в том, что на одном компьютере Windows не могут одновременно работать несколько пользователей (имеется в виду по RDP, либо обычный вход и вход по RDP).

Теперь мы видим экран удалённого компьютера: работа с ним ничем не отличается, можно запускать программы, выполнять настройки и любые другие действия:

Обратите внимание на панель вверху в центре экрана:

[https://hackware.ru/wp-content/uploads/2020/04/remote-desctop-panel.png](https://hackware.ru/wp-content/uploads/2020/04/remote-desctop-panel.png)

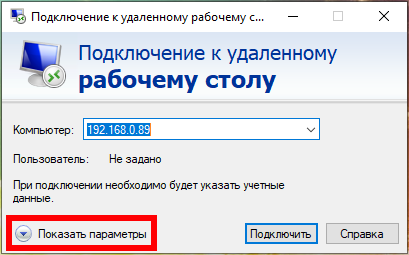
С помощью этой панели можно:

* проверить качество подключения до удалённого компьютера;
* свернуть удалённый рабочий стол без отключения (работает как с любым приложением — для открытия рабочего стола достаточно кликнуть на его иконку на панели приложений);
* изменить размер экрана удалённого компьютера (то есть выйти из полноэкранного режима, либо войти в полноэкранный режим снова);
* закрыть подключение к удалённому рабочему столу.

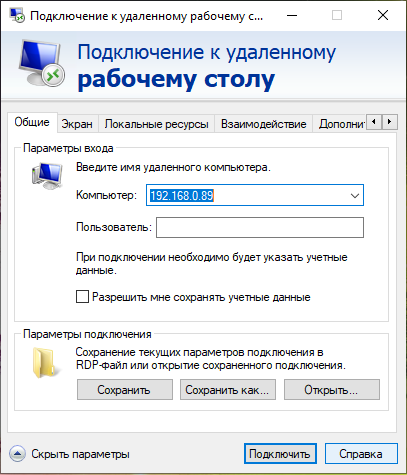
На следующем скриншоте удалённый рабочий стол не в полный экран на фоне основного рабочего стола сервера, с которого выполнено подключение:

## Настройки mstsc

Рассмотрим дополнительные настройки программы mstsc, которые открываются при нажатии на кнопку «**Показать параметры**»:

[](https://hackware.ru/wp-content/uploads/2020/04/mstsc.png)

На вкладке «**Общие**» вы можете указать имя пользователя.

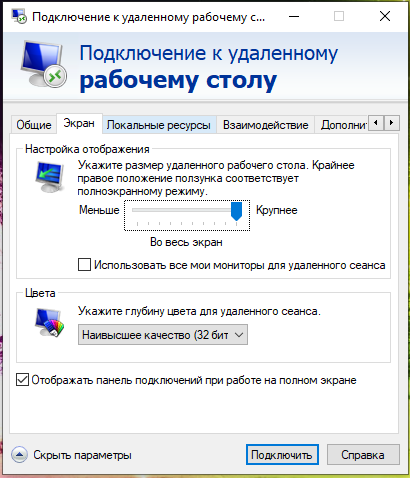
[](https://hackware.ru/wp-content/uploads/2020/04/mstsc-2.png)

Вы можете поставить галочку «**Разрешить мне сохранять учётные данные»** чтобы не вводить каждый раз имя пользователя и пароль.

При желании вы можете сохранить настройки в RDP файл или выбрать сохранённый ранее файл с настройками RDP.

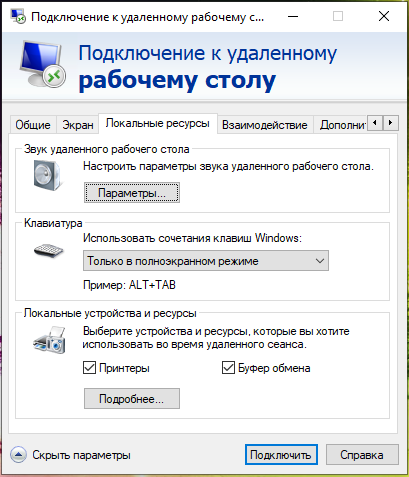
На вкладке «**Экран**» доступны настройки:

* **Укажите размер удалённого рабочего стола. Крайнее правое положение ползунка соответствует полноэкранному режиму.**
* **Использовать все мои мониторы для удалённого сеанса**
* **Укажите глубину цвета для удалённого сеанса.**
* **Отображать панель подключений при работе на полном экране**

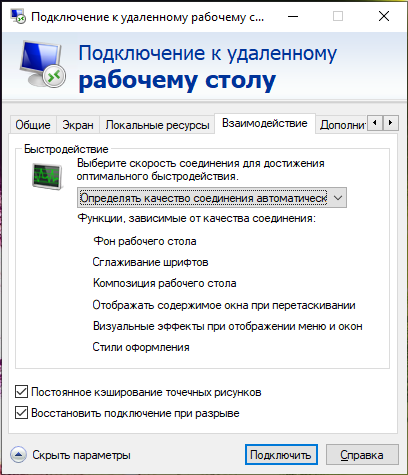
[](https://hackware.ru/wp-content/uploads/2020/04/mstsc-3.png)

На вкладке «**Локальные ресурсы**» вы найдёте настройки:

* **звука** (где проигрывать и записывать звуки удалённого рабочего стола)
* **клавиатуры** (где будут работать сочетания клавиш — на текущем или удалённом рабочем столе)
* **локальные ресурсы** (использовать ли принтеры, буфер обмена, смарт-карты, порты, диски, устройства видеозахвата и PnP устройства)

[](https://hackware.ru/wp-content/uploads/2020/04/mstsc-4.png)

Вкладка «**Взаимодействие**»:

[](https://hackware.ru/wp-content/uploads/2020/04/mstsc-5.png)

В разделе «**Быстродействие**» вы можете выбрать тип подключения и включить или отключить второстепенные функции, чтобы при любой скорости Интернета работа с удалённым столом была комфортной.

По умолчанию качество соединения определяется автоматически и также автоматически включаются или отключаются второстепенные функции.

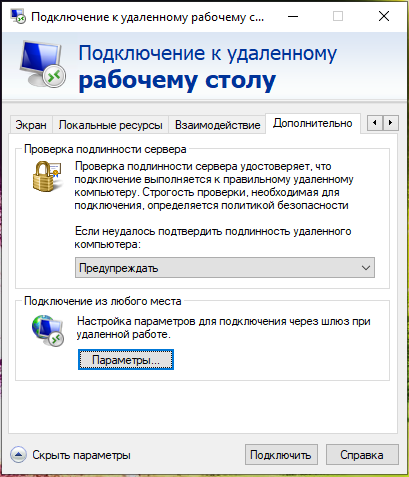
Вручную можно включить или отключить (функции, зависимые от качества соединения):

* Фон рабочего стола
* Сглаживание шрифтов
* Композиция рабочего стола
* Отображать содержимое окна при перетаскивании
* Визуальные эффекты при отображении меню и окон
* Стили оформления

Также вы есть настройки:

* Постоянное кэширование точечных рисунков
* Восстановить подключение при разрыве

Вкладка «**Дополнительно**»:

[](https://hackware.ru/wp-content/uploads/2020/04/mstsc-6.png)

**Проверка подлинности сервера**: Проверка подлинности сервера удостоверяет, что подключение выполняется к правильному удалённому компьютеру. Строгость проверки, необходимая для подключения, определяется политикой безопасности

Если не удалось подтвердить подлинность удалённого компьютера, то доступны варианты:

* Предупреждать
* Подключаться без предупреждения
* Не соединять

**Подключение из любого места**: Настройка параметров для подключения через шлюз при удалённой работе.

## Опции mstsc

Хотя mstsc является утилитой с графическим интерфейсом, вы можете запускать программу в командной строке с опциями. Далее рассмотрены эти опции.

Использование mstsc:

|  |  |
| --- | --- |
| 1 | MSTSC [<файл подключения>] [/v:<сервер[:порт]>] [/g:<шлюз>] [/admin] [/f[ullscreen]] [w:<ширина> /h:< высота>] [/public] | [/span] [/multimon] [/edit "файл подключения"] [/restrictedAdmin] [/remoteGuard] [/prompt] [/shadow:<ИД\_сеанса> [/control] [/noConsentPrompt]] |

Опции:

* **"файл подключения"** — имя RDP-файла для подключения.
* **/v:<сервер[:порт]>** —удалённый компьютер, к которому нужно подключиться.
* **/g:<шлюз>** — сервер шлюза удалённых рабочих столов, который следует использовать для подключения. Этот параметр считывается, только если удалённый компьютер конечной точки указан с использованием **/v**.
* **/admin** — подключает вас к сеансу администрирования удалённого компьютера.
* **/f** — запускает удалённый рабочий стол в полноэкранном режиме.
* **/w:<ширина>** — ширина окна удалённого рабочего стола.
* **/h:<высота>** — высота окна удалённого рабочего стола.
* **/public** — запускает удалённый рабочий стол в общем режиме.
* **/span** — сопоставляет ширину и высоту удалённого рабочего стола с соответствующими характеристиками локального виртуального рабочего стола и развёртывает изображение на несколько мониторов при необходимости. Для этого все мониторы должны быть размещены так, чтобы образовался прямоугольник.
* **/multimon** — задаёт расположение элементов на мониторах, используемых для сеанса служб удалённого рабочего стола, так, чтобы оно соответствовало текущей конфигурации на стороне клиента.
* **/edit** — открывает указанный RDP-файл подключения, чтобы его можно было изменить.
* **/restrictedAdmin** — подключает вас к удалённому компьютеру в режиме ограниченного администрирования. В этом режиме учётные данные не отправляются на удалённый компьютер, что обеспечивает защиту при подключении к скомпрометированному компьютеру. Но подключения с удалённого компьютера могут не проходить проверку подлинности со стороны других компьютеров, и это может влиять на функциональность и совместимость приложений. Этот параметр подразумевает наличие параметра **/admin**.
* **/remoteGuard** — подключает текущее устройство к удалённому устройству с помощью Remote Guard. Remote Guard предотвращает отправку учётных данных на удалённый компьютер, обеспечивая защиту при подключении к скомпрометированному удалённому компьютеру. В отличие от режима ограниченного администрирования Remote Guard также поддерживает соединения с удалённого устройства, перенаправляя все запросы обратно на ваше устройство.
* **/prompt**— запрашивает учётные данные пользователя при подключении к удалённому компьютеру.
* **/shadow:<ИД\_ceaнca>** идентификатор сеанса, для которого требуется теневое управление.
* **/control** — разрешает управление сеансом при теневом управлении.
* **/noConsentPrompt** — разрешает теневое управление без согласия пользователя.

Вывод: Я изучал работу RDP и приобрел практические навыки в использовании.