

Московский государственный технический университет
имени Н.Э. Баумана
(национальный исследовательский университет)

Факультет «Информатика и системы управления»
Кафедра «Компьютерные системы и сети»

В.Ю. Мельников, Е.К. Пугачев

Исследование способов удалённого управления Windows и Linux.

Электронное учебное издание

Методические указания по выполнению лабораторных работ
по дисциплине "Операционные системы"

2017

Введение

Цель работы: получение теоретических и практических сведений об удалённом управлении linux и Windows серверами а так же методах взаимодействия Windows и Linux.

Время выполнения - 2 часа.

Серверы располагаются в серверной. Там созданы все условия для серверов. К сожалению, для людей эти условия мало пригодны. В серверной очень шумно, очень холодно, маленький монитор, неудобная клавиатура и работать приходится стоя. К счастью, сразу после инсталляции ОС, и настройки сетевых интерфейсов можно покинуть это негостеприимное место и продолжить настройку сервера по сети.

Так же легко, находясь в Москве установить и настроить разработанную Вами программу в Нижнем Новгороде, Владивостоке, Америке — в любом месте где доступен Интернет.

Удалённое управление Linux

Установка сервиса *sshd* на сервере

Дайте команду «apt-get install ssh»

```
root@Pavel:~# apt-get install ssh
Чтение списков пакетов... Готово
Построение дерева зависимостей
Чтение информации о состоянии... Готово
Будут установлены следующие дополнительные пакеты:
  openssh-server openssh-sftp-server
Предлагаемые пакеты:
  ssh-askpass rssh molly-guard ufw monkeysphere
НОВЫЕ пакеты, которые будут установлены:
  openssh-server openssh-sftp-server ssh
обновлено 0, установлено 3 новых пакетов, для удаления отмечено 0 пакетов, и 66
пакетов не обновлено.
Необходимо скачать 532 kB архивов.
После данной операции, объём занятого дискового пространства возрастёт на 1 285
кВ.
Хотите продолжить? [д/н]
```

Будут установлены пакеты сервера ssh и запущен сервис sshd

Из соображений безопасности, в настройках запрещено подключаться по сети пользователем root (с аутентификацией по паролю). Но можно подключиться любым другим пользователем, и использовать команды sudo, или su для получения привилегий суперпользователя (которое в свою очередь надо разрешить в файле /etc/sudoers).

Во внутренней сети, если у вас сложный пароль и вы его надёжно храните, можно рискнуть разрешить прямое подключение суперпользователем по сети. Для этого, надо в файле «etc/ssh/sshd_config» найти параметр «PermitRootLogin» и задать «PermitRootLogin yes». Затем надо рестартовать сервис командой «service sshd restart».

Подключение к Linux из Linux

Удалённое выполнение команд

Поскольку наша виртуальная машина не имеет пока доступа к другим компьютерам, для начала установим сетевое соединение с localhost – значит со своей - же виртуальной машиной. Но работа с удалённым компьютером будет происходить так же.

Дайте команду «ssh root@localhost»

```
root@debian:~# ssh root@localhost
The authenticity of host 'localhost (::1)' can't be established.
ECDSA key fingerprint is d4:37:e3:d7:31:4e:fe:fe:cc:f5:2c:14:8e:10:c4:73.
Are you sure you want to continue connecting (yes/no)? y
Please type 'yes' or 'no': yes
Warning: Permanently added 'localhost' (ECDSA) to the list of known hosts.
```

При первом обращении к новому серверу, команда ssh спрашивает, доверяете ли вы этому серверу.

Затем запрашивается пароль пользователя, указанного в нашей команде

```
root@localhost's password:
The programs included with the Debian GNU/Linux system are free software;
the exact distribution terms for each program are described in the
individual files in /usr/share/doc/*/copyright.

Debian GNU/Linux comes with ABSOLUTELY NO WARRANTY, to the extent
permitted by applicable law.
Last login: Thu Nov 17 22:34:28 2016
root@debian:~#
```

Чтобы убедиться, что мы подключились действительно по ssh дайте команду «pstree»

```
root@debian:~# pstree
systemd--acpid
         |
         |--atd
         |--cron
         |--dbus-daemon
         |--2*[dhclient]
         |--exim4
         |--login--bash--ssh
         |--rpc.idmapd
         |--rpc.statd
         |--rpcbind
         |--rsyslogd--{|in:imklog}
                   |--{|in:imuxsock}
                   |--{rs:main Q:Reg}
         |--sshd--sshd--bash--pstree
         |--systemd-journal
         |--systemd-logind
         |--systemd-udevd
root@debian:~#
```

Мы в строке login—bash—ssh мы видим, что выполняется команда ssh в которой мы вводим команды. Далее стандартный поток ввода передаётся по сети сервису sshd, который передаёт его интерпретатору команд bash, который выполняет команду pstree (строка sshd—sshd—bash—pstree). Стандартный поток вывода команды pstree передаётся по цепочке сервису sshd, который в свою очередь, передает его обратно по сети команде ssh, которая выводит этот поток на экран. Точно так же работала бы команда, и если бы сервер был далеко

от нас. Все передаваемые данные шифруются, так что удалённое администрирование безопасно.

По ssh прекрасно будут работать и интерактивные команды, работающие в текстовом режиме. Для примера установим текстовый файловый менеджер «Midnight Commander», командой «`apt-get install mc`». И запустите его командой «`mc`»

```
Левая панель      Файл      Команда      Настройки      Правая панель
< ~ .[^]>         < ~ .[^]>
.и  Имя          Размер  Время правки  .и  Имя          Размер  Время правки
/..  -ВВЕРХ-        сен 8 22:04  /..  -ВВЕРХ-        сен 8 22:04
/.cache  4096 сен 8 22:40  /.cache  4096 сен 8 22:40
/.config  4096 сен 8 22:33  /.config  4096 сен 8 22:33
/.local   4096 сен 8 22:33  /.local   4096 сен 8 22:33
/.ssh     4096 ноя 17 23:01  /.ssh     4096 ноя 17 23:01
/.w3m     4096 сен 8 22:44  /.w3m     4096 сен 8 22:44
.Xauthority  0 сен 8 22:49  .Xauthority  0 сен 8 22:49
.bash_history  68 ноя 17 23:38  .bash_history  68 ноя 17 23:38
.bashrc     568 сен 8 22:34  .bashrc     568 сен 8 22:34
.profile    140 ноя 19 2007  .profile    140 ноя 19 2007
.selected_editor  72 сен 8 22:33  .selected_editor  72 сен 8 22:33
.xsession-errors 1232 сен 8 22:45  .xsession-errors 1232 сен 8 22:45

-ВВЕРХ-        -ВВЕРХ-
6512M/7555M (86%) 6512M/7555M (86%)
Совет: На медленных терминалах может помочь флаг -s.
root@debian:~#
1Помощь 2Меню 3Про~тр 4Правка 5Копия 6Пер~ос 7Нвк~ог 8Уда~ть 9МенюМС 10Выход
```

Цвет, рамки! И как всё это проходит через stdout?

Дело в том, что терминал обрабатывает ESC последовательности. Это последовательности символов, начинающиеся с символа ESC (33₁₆), управляющие терминалом. Например, команда «`echo -e "\033[42;33m Hello"`» выведет текст «Hello» красными буквами на зелёном фоне. Есть управляющие последовательности для перемещения курсора в нужную позицию терминала, очистки экрана и так далее.

Но вернёмся к `mc`.

Перейдём в каталог «`/etc`». Для этого, используя клавиши стрелок вверх и вниз выберите каталог «`..`» и нажмите «`Enter`». Мы перешли на уровень выше. В нашем случае это корневой каталог. используя клавиши стрелок вверх и вниз выберите каталог «`..`» и нажмите «`Enter`» текущим каталогом стал «`/etc`» и мы видим его содержимое.

«Midnight Commander» позволяет вводить выполнять команды, так, что для перехода можно было бы воспользоваться командой «`cd /etc`»

`Ctrl+O` — Скрывает панели. В этом режиме удобно выполнять команды как в терминале. Повторное нажатие `Ctrl+O` — показывает панели.

С помощью «`mc`» можно копировать и перемещать файлы и каталоги. Для этого перейдите клавишей «`Tab`» на вторую панель, выберите нужный файл в нужном каталоге и

нажмите «F5» или «F6» (подсказка в нижней строке).

Клавиша «Ins» позволяет выделить несколько файлов и каталогов.

Клавиша «F8» их удалит (осторожнее)

Клавиша «F4» открывает довольно мощный редактор с привычным интерфейсом.

Клавиша «F9» выведет меню в котором много других команд.

Если привыкнуть, то работать так же удобно, как и в графическом файловом менеджере.

При этом, нагрузка на сеть и процессор минимальная,

Для выхода нажмите клавишу F10

Для завершения работы с удалённым компьютером дайте команду exit.

Подключение с аутентификацией по ключу

Если вам приходится много раз в день подключаться к разным серверам (и по несколько раз), удобно можно настроить ssh на подключение без ввода пароля. Может показаться, что этот подход — дыра в безопасности. Но не забывайте, что , вводимый вами пароль будет передаваться по сети (пусть и зашифрованный), а если злоумышленник подберёт пароль к вашему компьютеру, он сможет перехватить вводимый вами пароль. Подключаться желательно не root, а обычным пользователем, при необходимости можно получить полномочия суперпользователя командой sudo.

Сначала сформируем на вашем рабочем компьютере пару ключей командой «ssh-keygen». Путь к файлу пароля оставим по умолчанию (нажмите Enter), пароль не задаём.

```
Generating public/private rsa key pair.
Enter file in which to save the key (/root/.ssh/id_rsa):
Enter passphrase (empty for no passphrase):
Enter same passphrase again:
Your identification has been saved in /root/.ssh/id_rsa.
Your public key has been saved in /root/.ssh/id_rsa.pub.
The key fingerprint is:
3c:f1:9d:2f:4e:27:73:52:b0:55:9d:42:f0:b3:8d:b5 root@debian
The key's randomart image is:
+---[RSA 2048]---+
  .O. +
   .. 0.
    . .00.
   . 0 . =* .
  S . +0.E
    . 0
     * +
    0 B
     .
+-----+

```

Передадим открытый ключ на удалённый компьютер (снова для тренировки подойдёт наша же виртуальная машина localhost)

```
ssh-copy-id user1@localhost
```

Последний раз вводим пароль пользователя user1

```
root@debian:~# ssh-copy-id user1@localhost
/usr/bin/ssh-copy-id: INFO: attempting to log in with the new key(s), to filter
out any that are already installed
/usr/bin/ssh-copy-id: INFO: 1 key(s) remain to be installed -- if you are prompt
ed now it is to install the new keys
user1@localhost's password:
Number of key(s) added: 1
Now try logging into the machine, with:  "ssh 'user1@localhost'"
and check to make sure that only the key(s) you wanted were added.
```

Теперь команда «ssh user1@localhost» установит подключение от имени пользователя user без ввода пароля.

Копирование файлов на удалённый компьютер

Сервис sshd позволяет не только выполнять команды, но и безопасно копировать файлы на удалённый сервер. Для этого используется команда «scp» (secure copy).

Синтаксис этой команды «scp [[user1@]host1:]file1 [[user2@]host2:]file2»

Например, для тренировки, скопируем файл «xx.txt» на наш же компьютер (но по сети)

```
scp /root/xx.txt user1@localhost:~/yy.txt
```

В данной команде копирование осуществляется от имени пользователя user1 в его домашний каталог, в чём мы можем убедиться дав команду «ls -l /home/user1»

Если надо скопировать несколько файлов, можно использовать знак групповой операции. В качестве file2 укажите каталог. Например,

```
scp /root/*.txt user1@localhost:~/
```

Если понадобится скопировать систему каталогов, можно воспользоваться конвейером с командой tar. Попробуйте понять, как работает следующая команда:

```
MBP-Ekaterina:~ ekaterina$ tar -c /Users/ekaterina/Desktop/cat.jpg /Users/ekaterina/Desktop/wall.jpg | gzip -c - | ssh kate@10.37.129.6 'gunzip -c | tar x'
tar: Removing leading '/' from member names
kate@10.37.129.6's password:
tar: Removing leading '/' from member names
```

Резервное копирование больших каталогов

При необходимости копировать много файлов лучше воспользоваться мощной командой «rsync»

```
apt-get install rsync
```

Скопируем с рабочего компьютера каталог /root на удалённый компьютер (снова для тренировки подойдёт наша же виртуальная машина localhost)

```
rsync -vrtplze ssh --progress --stats --delete /root user1@localhost:~/backup
```

Разберите по справке «man rsync» опции этой команды

```

root/.config/mc/mcedit/
root/.local/
root/.local/share/
root/.local/share/mc/
root/.local/share/mc/filepos
      122 100%   7,94kB/s   0:00:00 (xfr#13, to-chk=5/32)
root/.local/share/mc/history
      455 100%  29,62kB/s   0:00:00 (xfr#14, to-chk=4/32)
root/.local/share/mc/mcedit/
root/.ssh/
root/.ssh/id_rsa
      1,679 100% 109,31kB/s   0:00:00 (xfr#15, to-chk=2/32)
root/.ssh/id_rsa.pub
      393 100%   25,59kB/s   0:00:00 (xfr#16, to-chk=1/32)
root/.ssh/known_hosts
      222 100%   14,45kB/s   0:00:00 (xfr#17, to-chk=0/32)
root/./w3m/

Number of files: 32 (reg: 17, dir: 15)
Number of created files: 32 (reg: 17, dir: 15)
Number of deleted files: 0
Number of regular files transferred: 17
Total file size: 9,718 bytes
Total transferred file size: 9,718 bytes
Literal data: 9,718 bytes
Matched data: 0 bytes
File list size: 0
File list generation time: 0,001 seconds
File list transfer time: 0,000 seconds
Total bytes sent: 6,858
Total bytes received: 414

sent 6,858 bytes received 414 bytes 14,544.00 bytes/sec
total size is 9,718 speedup is 1.34

```

Если мы повторим эту команду снова будет скопированы только новые и изменившиеся файлы (в отличии от команды scp).

Настройка соединения виртуальной машины с реальной.

Студенты, которые выполняют данную работу в зале 809 через терминалы сервера АИС, должны ознакомиться с этим и следующим разделами теоретически, по причине отсутствия необходимых прав доступа. Просьба не пытаться выполнять описанные ниже действия.

При создании виртуальной машины в первой лабораторной работе мы оставили тип сетевого подключения по умолчанию — «NAT». В этом режиме наша виртуальная машина имеет подключение к Интернет (вашего реального компьютера) но доступа к реальному компьютеру и другим виртуальным машинам не имеет. Так же, нет возможности установить соединение в вашей виртуальной машиной извне. До сих пор нам этого было достаточно.

Теперь мы хотим научиться подключаться по сети с реальной машины к виртуальной и наоборот.

Завершите работу вашей виртуальной машины (если она запущена). Выделите вашу виртуальную машину и выберите из контекстного меню команду «настроить». Выделите элемент «сеть».

Кроме NAT, имеются следующие типы подключений:

В режиме «Сетевой мост» виртуальная машина подключается напрямую к сети, к которой подключён реальный компьютер, получает свой IP адрес и становится одним из устройств этой сети.

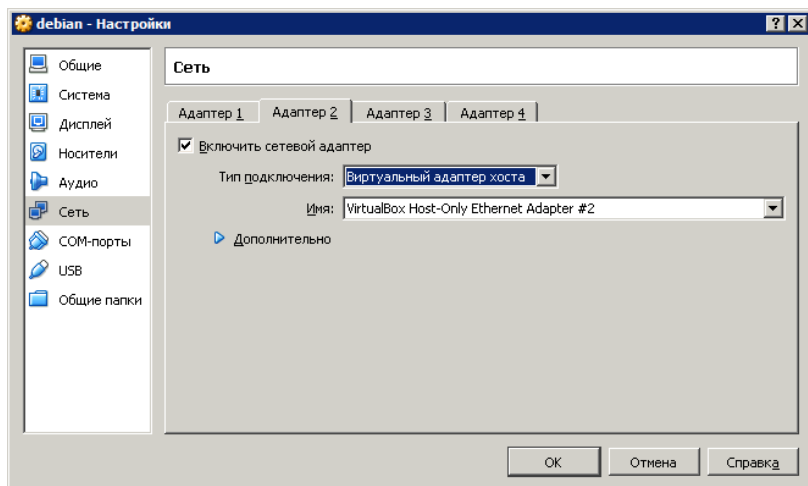
В режиме «Виртуальный адаптер хоста» создаётся новая сеть, к которой подключены виртуальные машины и реальный компьютер. VirtualBox сам назначает этим устройствам IP адреса.

В режиме «Внутренняя сеть» создаётся новая сеть, к которой подключены только выбранные виртуальные машины, но не связанная ни с реальным компьютером ни с реальной сетью. Этот режим хорош при написании вирусов и других опасных программ.

| Тип подключения | Доступ VM к локальной сети и интернет | Доступ VM к реальному компьютеру | Доступ к VM из локальной сети | Доступ с реального компьютера |
|---------------------------|---------------------------------------|----------------------------------|-------------------------------|-------------------------------|
| NAT | да | нет | Требуется «проброс портов» | Требуется «проброс портов» |
| Сетевой мост | да | да | да | да |
| Виртуальный адаптер хоста | нет | да | нет | да |
| Внутренняя сеть | нет | нет | нет | нет |

Нам надо не лишиться доступа к интернет и при этом установить соединение с реальным компьютером. Согласно приведённой выше таблице можно попробовать режим «Сетевой мост». Но в нашей локальной сети напряжённая ситуация со свободными адресами, поэтому мы пойдём другим путём. Добавим второй сетевой адаптер на нашу виртуальную машину и установим режим «Виртуальный адаптер хоста». Для виртуальной машины это будет соответствовать установке второй сетевой карты. Через первый сетевой интерфейс мы будем иметь доступ в интернет, а через второй — к реальному компьютеру.

Выберите в настройках виртуальной машины вкладку «Адаптер 2», поставьте отметку «Включить» и выберите тип подключения «Виртуальный адаптер хоста».



Сохраняем настройки и запускаем виртуальную машину.

Войдите в систему как «root» и дайте команду «ifconfig -a»

```
eth0      Link encap:Ethernet  HWaddr 08:00:27:5f:c6:00
          inet addr:10.0.2.15  Bcast:10.0.2.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fe5f:c600/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:14 errors:0 dropped:0 overruns:0 frame:0
          TX packets:25 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:2736 (2.6 KiB)  TX bytes:2480 (2.3 KiB)

eth1      Link encap:Ethernet  HWaddr 08:00:27:c6:99:32
          BROADCAST MULTICAST  MTU:1500  Metric:1
          RX packets:0 errors:0 dropped:0 overruns:0 frame:0
          TX packets:0 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:0 (0.0 B)  TX bytes:0 (0.0 B)
```

Наш старый сетевой интерфейс имеет имя «eth0». Он получил IP адрес и работает. Наш новый сетевой интерфейс получил имя «eth1» но IP адрес не получил. Настроим этот интерфейс. Для этого, отредактируем файл «/etc/network/interfaces»

По аналогии с настройками интерфейса «eth0» добавим строки

```
allow-hotplug eth1
iface eth1 inet dhcp
```

Согласно этой настройке интерфейс должен будет получить IP адрес автоматически. На нашей виртуальной машине, в сети типа «виртуальный адаптер хоста», адреса будет назначать VirtualBox.

Для сети в которой нет DHCP сервера, (в частности, сеть типа «Внутренняя сеть» VirtualBox), придётся назначить вручную статический адрес. Например:

```
auto eth1
iface eth1 inet static
    address 192.168.56.100
    netmask 255.255.255.0
```

«Поднимем» интерфейс «eth1» командой «ifup eth1»

```
root@debian:~# ifup eth1
Internet Systems Consortium DHCP Client 4.3.1
Copyright 2004-2014 Internet Systems Consortium.
All rights reserved.
For info, please visit https://www.isc.org/software/dhcp/

Listening on LPF/eth1/08:00:27:c6:99:32
Sending on   LPF/eth1/08:00:27:c6:99:32
Sending on   Socket/fallback
DHCPDISCOVER on eth1 to 255.255.255.255 port 67 interval 3
DHCPREQUEST on eth1 to 255.255.255.255 port 67
DHCPOFFER from 192.168.56.100
DHCPACK from 192.168.56.100
bound to 192.168.56.102 -- renewal in 1780 seconds.
```

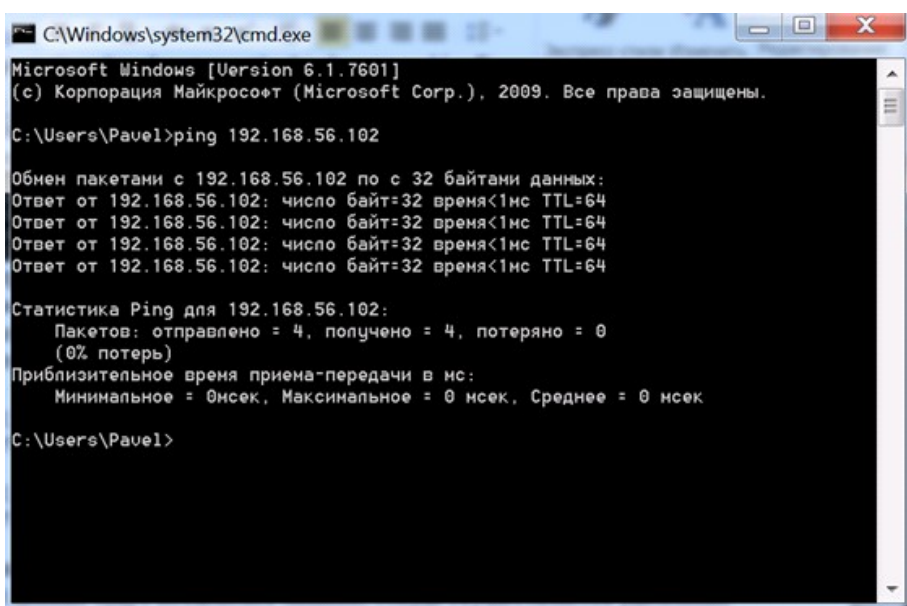
Дайте команду «ifconfig»

```
eth1      Link encap:Ethernet  HWaddr 08:00:27:c6:99:32
          inet addr:192.168.56.102  Bcast:192.168.56.255  Mask:255.255.255.0
          inet6 addr: fe80::a00:27ff:fec6:9932/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:37 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:6981 (6.8 KiB)  TX bytes:1332 (1.3 KiB)
```

В блоке «eth1» мы видим, какой адрес получил наш сетевой интерфейс - «inet addr» = 192.168.56.102

По этому адресу мы получим доступ с реальной машины на виртуальную.

Переключитесь в вашу реальную машину, запустите терминал и дайте команду `ping <IP_адрес_VM>`



```
C:\Windows\system32\cmd.exe
Microsoft Windows [Version 6.1.7601]
(c) Корпорация Майкрософт (Microsoft Corp.), 2009. Все права защищены.

C:\Users\Pavel>ping 192.168.56.102

Обмен пакетани с 192.168.56.102 по с 32 байтани данных:
Ответ от 192.168.56.102: число байт=32 время<1мс TTL=64
Ответ от 192.168.56.102: число байт=32 время<1мс TTL=64
Ответ от 192.168.56.102: число байт=32 время<1мс TTL=64
Ответ от 192.168.56.102: число байт=32 время<1мс TTL=64

Статистика Ping для 192.168.56.102:
    Пакетов: отправлено = 4, получено = 4, потеряно = 0
    (0% потерь)
Приблизительное время приема-передачи в мс:
    Минимальное = 0нсек, Максимальное = 0 нсек, Среднее = 0 нсек

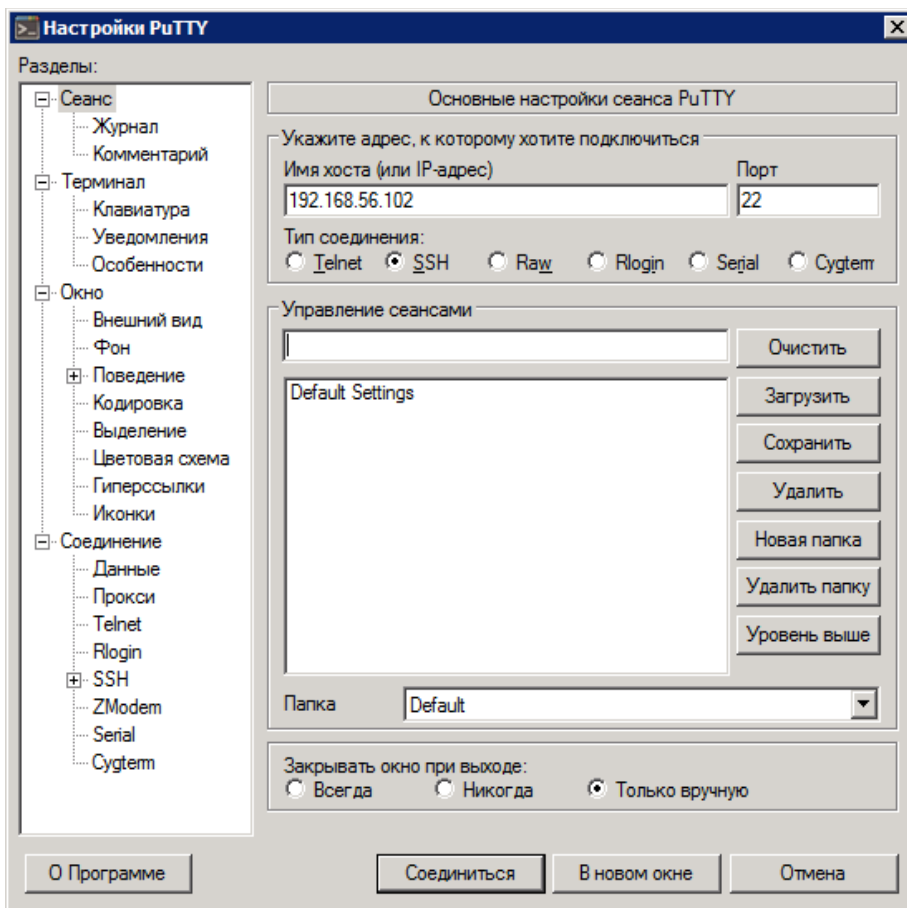
C:\Users\Pavel>
```

Ответ получен, значит соединение есть.

Подключение к Linux из Windows

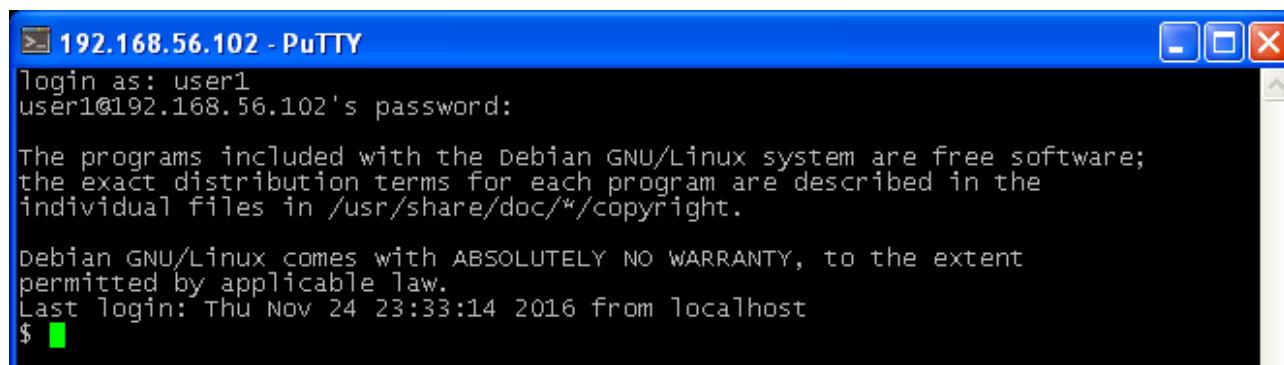
Для подключения к Linux по протоколу ssh из Windows имеется свободно распространяемая программа «putty». Скачайте её со страницы [«<http://putty.org.ru/download.html>»](http://putty.org.ru/download.html) (Жмите не большую зелёную кнопку, а незаметную ссылку «Скачать PuTTY») Загрузится архив PuTTY-0.66-RU-16.zip распакуйте его в одноимённую папку и найдите putty.exe (В принципе, можно было скачать только его и puttygen.exe)

Запустите «putty.exe» и введите IP адрес нашей виртуальной машины.



В будущем, если вы будете работать с несколькими серверами, чтобы не вводить адрес каждый раз введите имя сервера в поле «Управление сеансами» и нажмите кнопку «Сохранить».

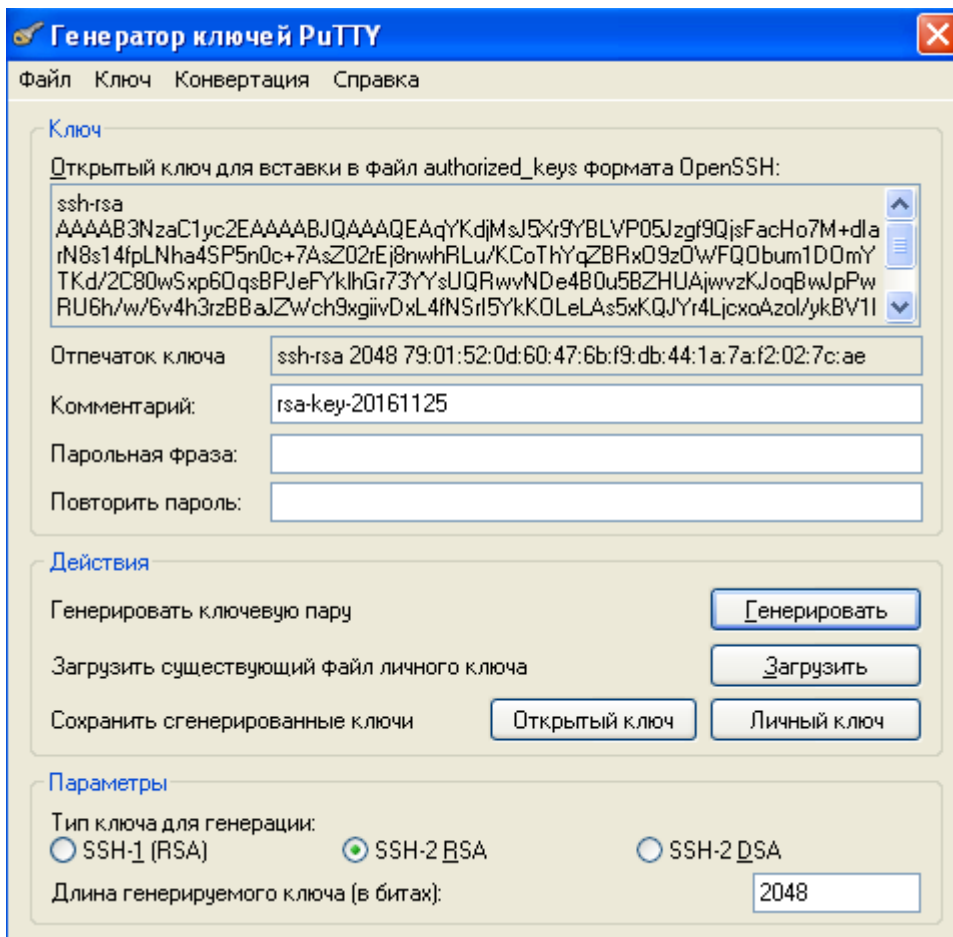
Для подключения нажмите кнопку «Соединиться».



Точно так же, как в команде ssh мы выполняем команды на удалённом сервере а результаты отображаются в окне программы PuTTY.

Настроим аутентификацию по ключу.

В том же каталоге, где лежит PuTTY.exe лежит программа «puttygen.exe» запустите её и нажмите кнопку «Генерировать».



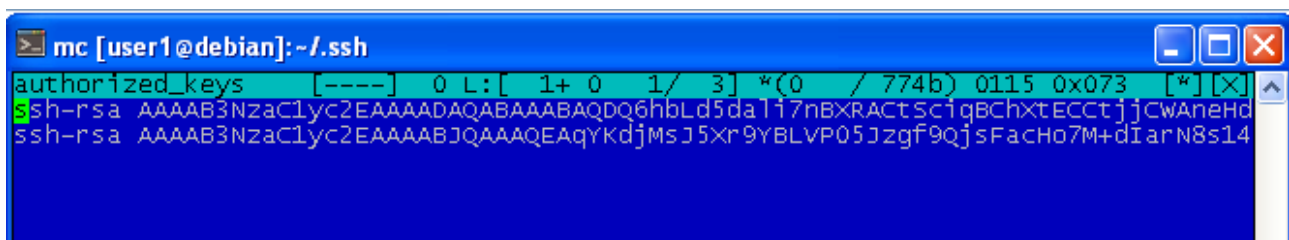
Используя кнопки «Открытый ключ» и «Личный ключ» создайте файлы открытого и закрытого ключа. А ещё скопируйте текст открытого ключа из верхнего поля в буфер обмена.

Возвращаемся в окно PuTTY запустите mc, перейдите в каталог «/user1/.ssh» (если надо — создайте его)

Перейдите на файл «authorized_keys» и откройте его в редакторе «mcedit» (клавиша F4)

Вставьте в конец файла открытый ключ из буфера обмена (Shift+Ins)

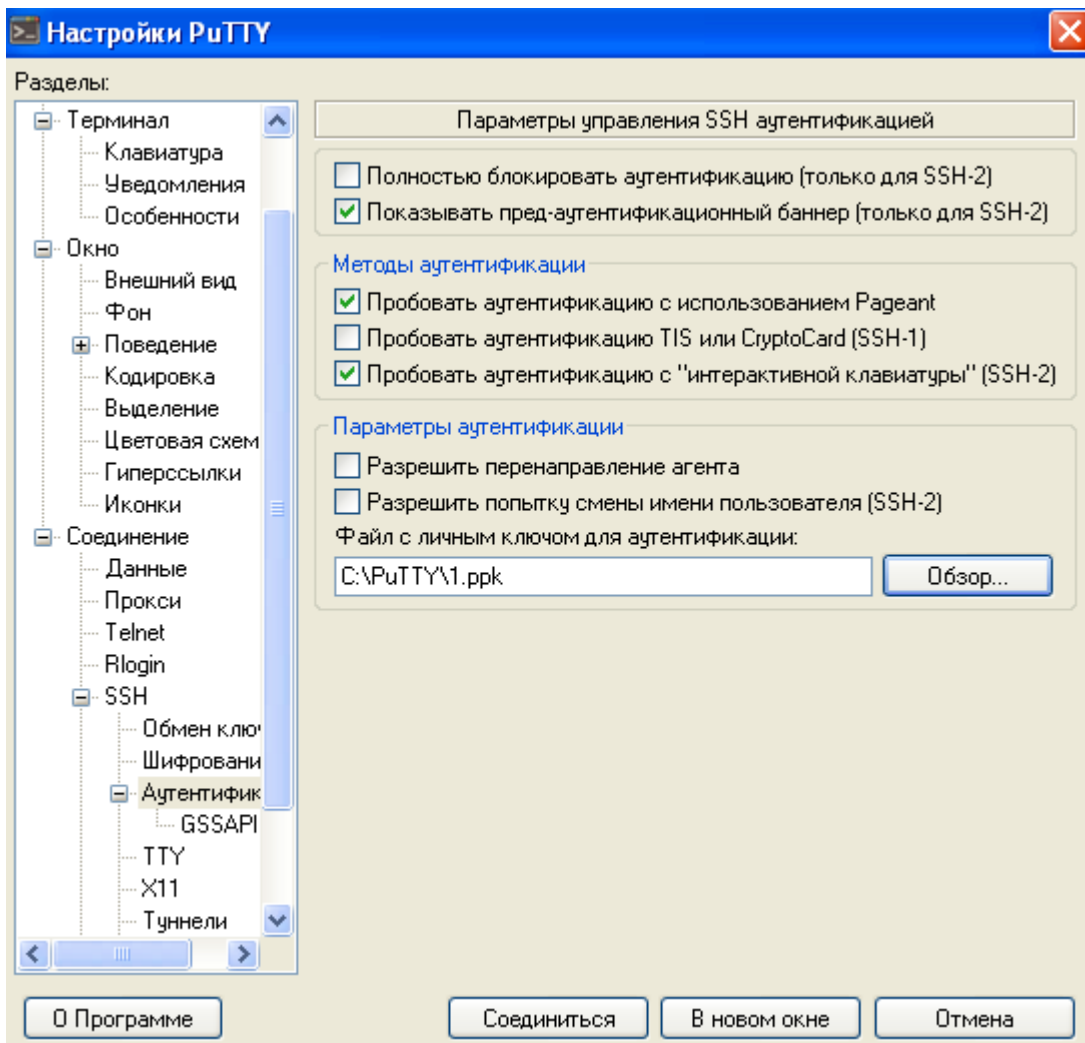
И сохраните файл (F2)



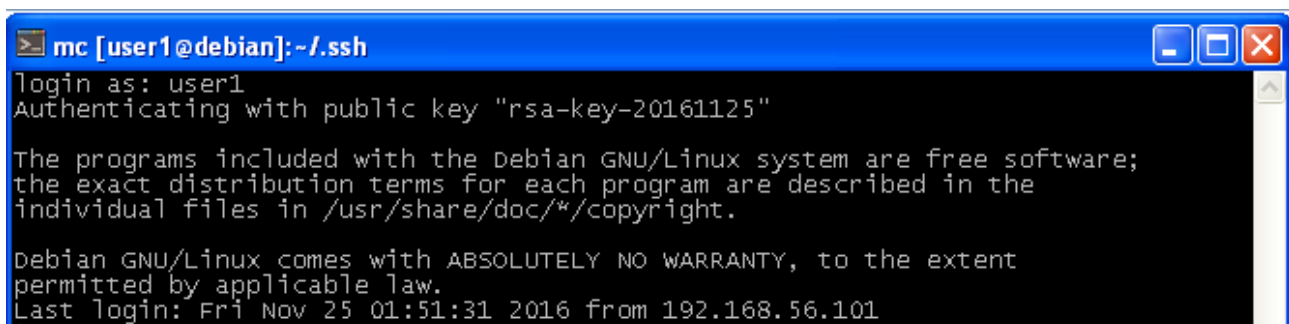
Выйдите из редактора (F10)

Закройте PuTTY и снова запустите его.

В левом окне раскройте элементы «Соединение», «SSH» и выберите элемент «Аутентификация» и задайте файл личного (закрытого ключа). Сохраните конфигурацию.

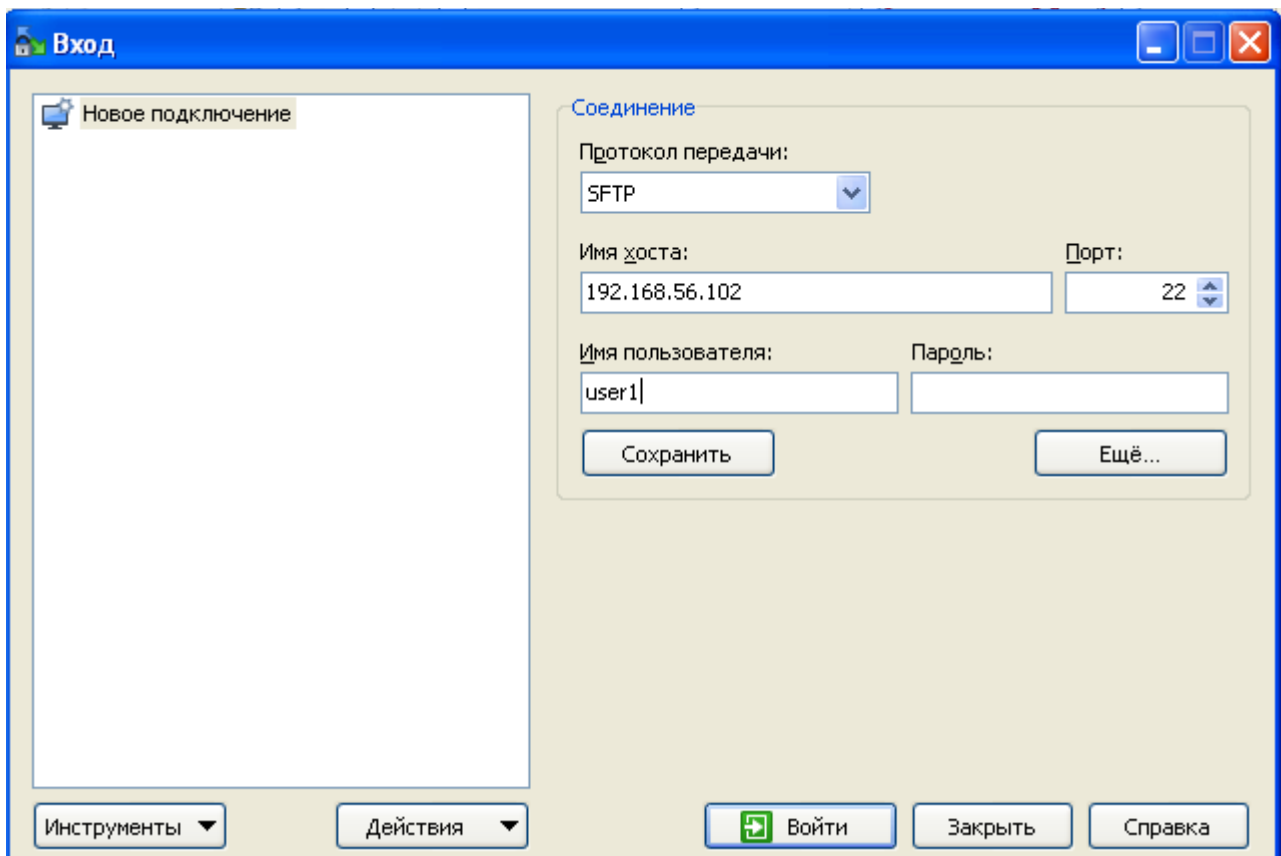


Нажмите кнопку «Соединиться», введите имя пользователя. Пароль вводить не придётся.

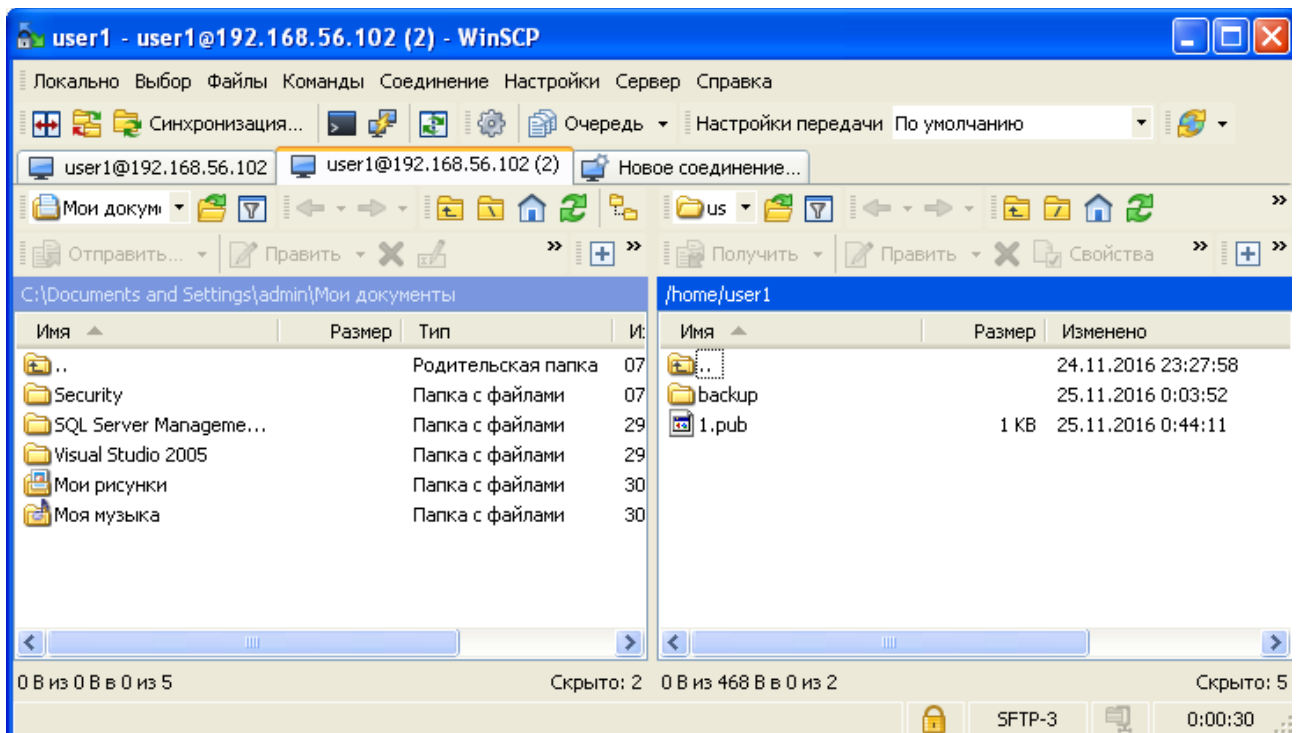


Копирование файлов на удалённый компьютер

Загрузите с сайта <https://winscp.net/eng/download.php> программу WinSCP (ссылка Installation package) и установите её. Введите адрес удалённого компьютера, имя пользователя и сохраните конфигурацию.



Нажмите кнопку «Войти» и введите пароль. Открывается окно в котором вы можете копировать файлы с локального компьютера (левая половина) на удалённый компьютер (правая половина) и обратно.



Удалённое управление Windows

Многие из рассмотренных в предыдущей работе оснасток ММС позволяют управлять не только локальным, но и удалённым компьютером, для этого, при добавлении оснастки, следует указать этот компьютер. Разумеется, ваш пользователь должен иметь права на выполнение соответствующих операций на выбранном компьютере.

Но полные возможности по управлению удалённым компьютером предоставляет программа «Подключение к удаленному рабочему столу».

Заранее, надо настроить удалённый компьютер. Пуск → Панель управления → Система.

Для Windows XP Professional — на вкладке «Удалённые сеансы»

Для Windows 7 — «Дополнительные параметры системы» → Удалённый доступ.

Для Windows - «Настройка удалённого доступа» → Удалённый доступ

Следует отметить «Разрешить удалённый доступ ...» и нажать кнопку «Применить».

В настройках брандмауера будет открыт порт 3389 и запущена служба дистанционного управления рабочим столом.

Администраторы компьютера и домена получают доступ сразу, других пользователей надо добавить, нажав кнопку «Выбрать пользователей».

На сервере АИС (195.19.33.62) подключение к удалённому рабочему столу уже настроено. В зале 809 рабочие станции автоматически подключаются к службе удалённого рабочего стола этого сервера.

На своём локальном компьютере следует запустить Пуск → Все программы → Стандартные → Подключение к удаленному рабочему столу

В поле «Компьютер» следует ввести имя или IP адрес сервера и нажать кнопку «Подключить». Затем ввести имя пользователя и пароль.

Если требуется скопировать данные на удалённый компьютер, можно открыть удалённый доступ к папке. Для этого в проводнике вызовите контекстное меню щелчком правой кнопки мыши на нужной папке, выберите команду «Общий доступ и безопасность», выбрать «Открыть общий доступ» и ввести имя, под которым папка будет доступна по сети. Если требуется разрешить запись надо поставить отметку «Разрешить изменение файлов по сети». Теперь, на локальном компьютере в строке адреса проводника следует ввести «\\IP_адрес» или «\\ИМЯ» удалённого компьютера и через несколько секунд откроется список доступных сетевых папок этого компьютера.

Если открытие сетевой папки нежелательно, можно воспользоваться программой «Подключение к удаленному рабочему столу». В этом случае надо нажать кнопку

«Параметры>>» и на вкладке «Локальные ресурсы» нажать кнопку «Подробнее», раскрыть элемент «Устройства» и отметить открываемый локальный диск вашего компьютера. Для безопасности рекомендуется использовать флешку. В этом случае, файлы надо сначала записать на локальном компьютере на флешку, а потом забрать с удалённого компьютера. Выбранный диск будет доступен на удалённом компьютере через проводник.