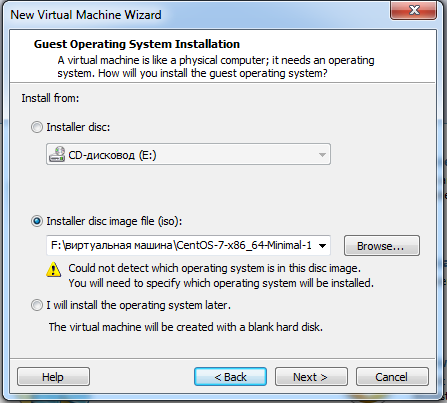
Кудрявцев Николай, отчет.

**Задание 1:** создать виртуальную машину с операционной системой CentOS.

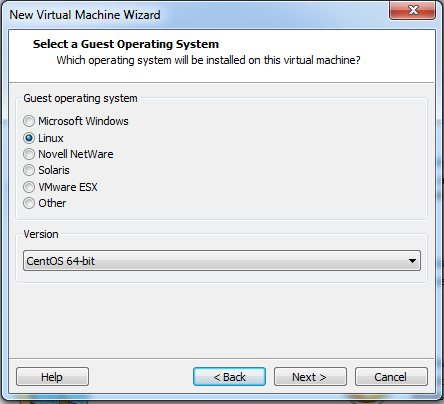
**Виртуальная машина** — программная и или аппаратная система, эмулирующая аппаратное обеспечение некоторой платформы (target — целевая, или гостевая платформа) и исполняющая программы для target-платформы на host-платформе (host — хост-платформа, платформа-хозяин) или виртуализирующая некоторую платформу и создающая на ней среды, изолирующие друг от друга программы и операционные системы.

1) Для начала необходимо скачать и установить программу виртуализации VMware Workstation 10 (либо ее аналог), а также скачать образ установочного диска операционной системы CentOS в минимальной комплектации с официального сайта: http://www.centos.org/download/

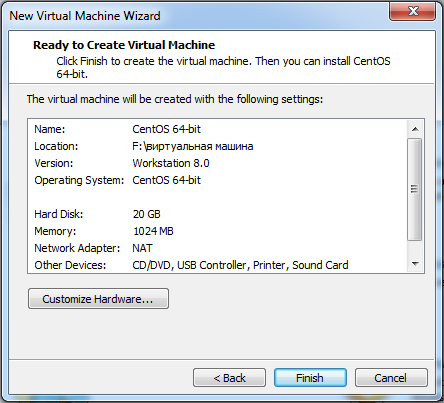
2) Затем нужно создать виртуальную машины. Сначала нужно указать путь к расположению образа CentOs:



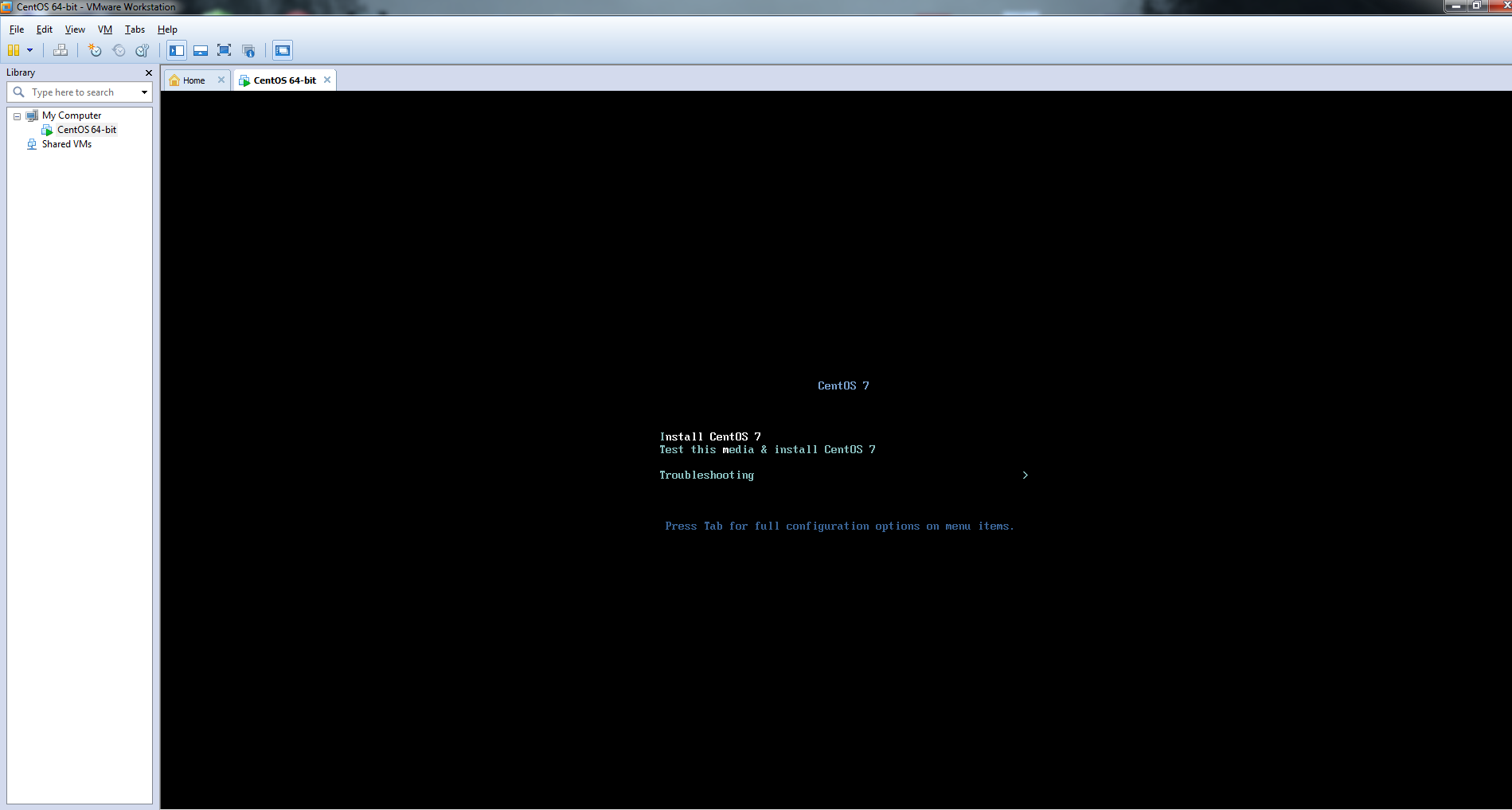
Затем вручную определить операционную систему:



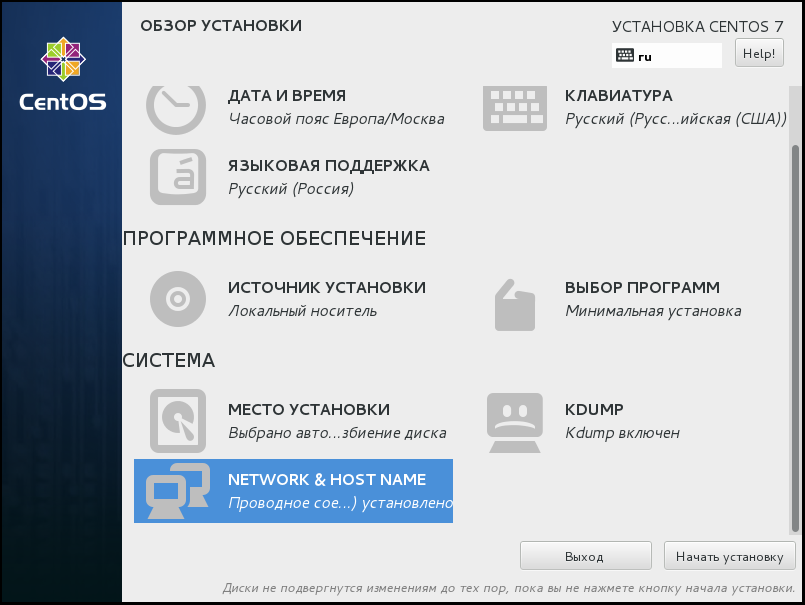
В результате настроек получится виртуальная машина со следующими характеристиками:



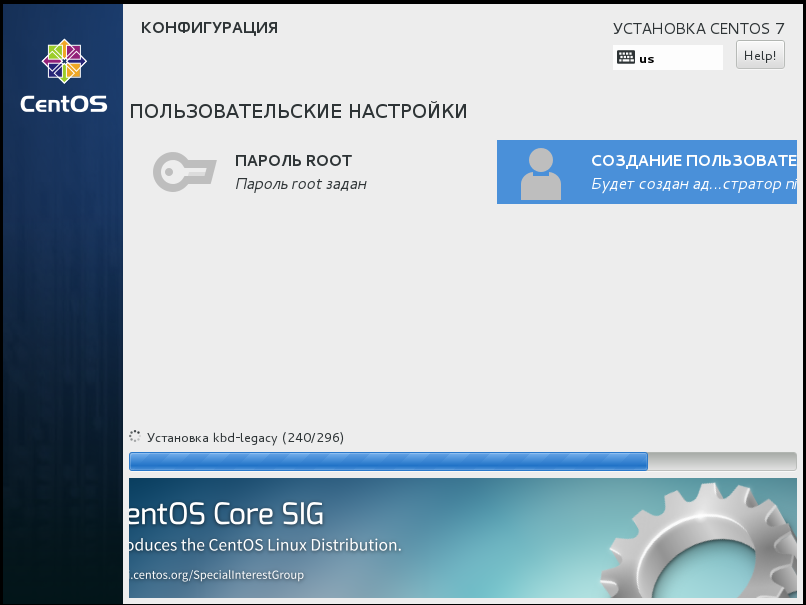
Затем виртуальная машинаможет быть запущена, запустится установка ОС:



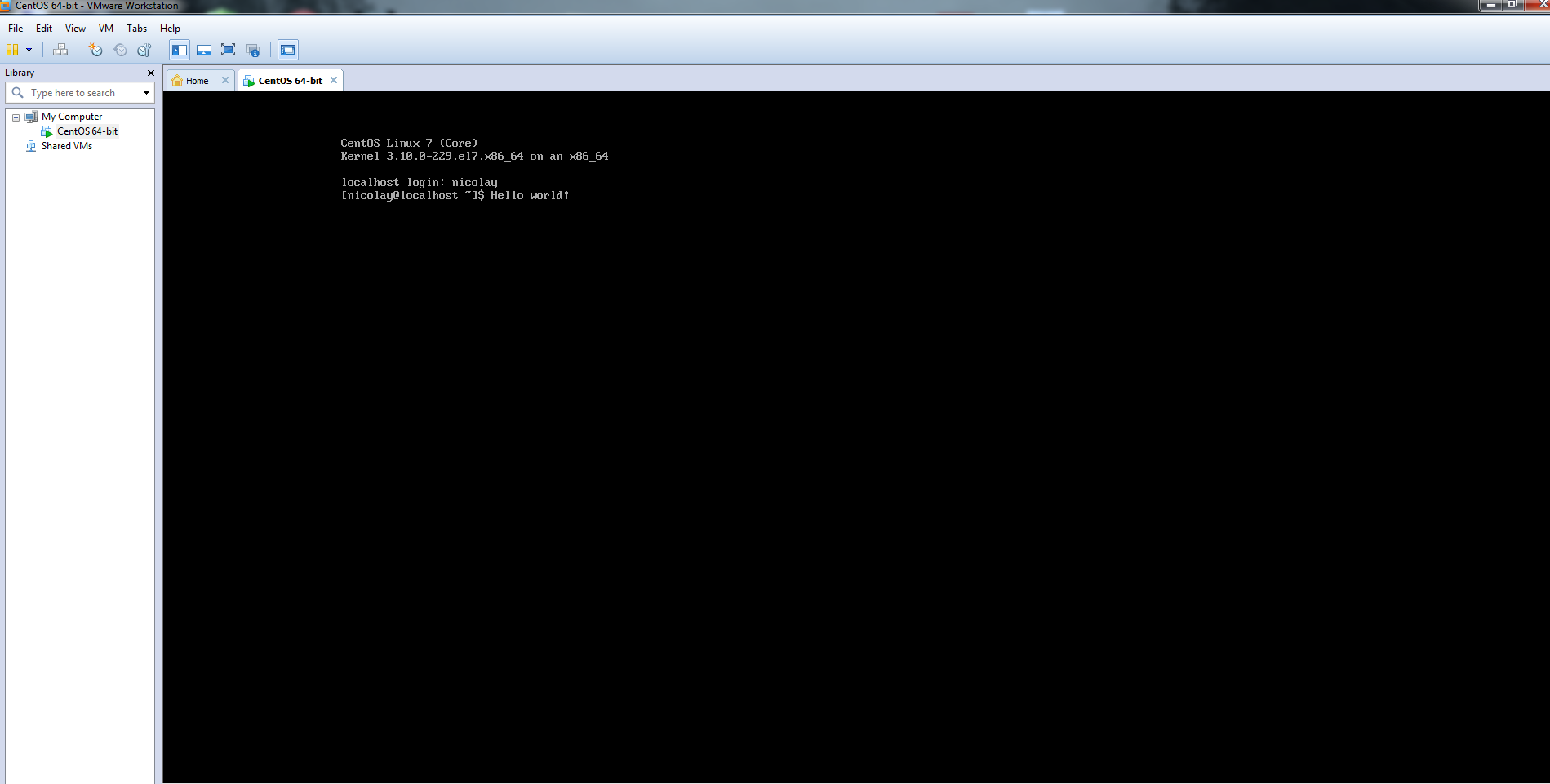
Далее следует выбрать тип установки ОС, а также виртуальный жесткий диск и подключение к интернету:



Затем необходимо выбрать пароль для получения root-прав доступа, а также создать пользователь с правами администратора:



Виртуальная машина готова к работе.



**Задание 2:** научиться работать в консоли CentOS и настроить сеть.

**Основные команды для работы в консоли:**

*cd* Переход в заданную папку

*ls* Вывод всех файлов и каталогов по порядку

*cp* Копирование файлов/папок

*mkdir* Создать папку  
 *rmdir* Удаление пустой папки

*ps* Показывает текущие активные процессы

*vi* Редактирование текстовых файлов

*cat* Получение информации о файле/процессе

*poweroff* Завершение работы системы

*reboot* Перезагрузка

Root, или суперпользователь - специальный аккаунт, владелец которого обладает правами на выполнение всех без исключения операций.

Чтобы совершить действие с правами суперпользователя, можно воспользоваться командой *sudo*, например:

*sudo mkdir /home/primer*

**Настройка сети**

*ip a -* проверить текущие сетевые настройки.

В данном способе сетевой интерфейс будет настроен путем редактирования конфигурационного файла, который расположен в директории /etc/sysconfig/network-scripts/

Нужно отредактировать файл /etc/sysconfig/network-scripts/ifcfg-[\*\*\*], где [\*\*\*] - название сетевого адаптера в системе.

Если сеть имеет статический IP-адрес, то следует в редактируемом файле дописать следующие строчки:

DEVICE=»eth0″  
 BOOTPROTO=»none»  
 ONBOOT=»yes»  
 IPADDR=»192.168.1.100″ - IP-адрес  
 NETMASK=»255.255.255.0″  
 GATEWAY=»192.168.1.1″ - IP-адрес шлюза

Для сети с использованием DHCP (протокол динамической настройки узла, позволяющий компьютерам автоматически получать IP-адрес и другие параметры, необходимые для работы в сети):

DEVICE=»eth0″  
 BOOTPROTO=»dhcp»  
 ONBOOT=»yes»

Затем нужно в сетевой конфигурационный файл vi /etc/sysconfig/network дописать следующие данные:

NETWORKING=»yes»  
 HOSTNAME=»имя\_вашего\_сервера»

После этого следует перезапустить сеть (для корректного применения новых настроек):

/etc/init.d/network restart

Проверка работы сети:



**Установка дополнительных пакетов (nano, elinks, mc)**

**YUM** - средство установки пакетов. Чтобы с помощью него установить какой-либо пакет, необходимо написать в консоли

*yum install \*название\_пакета\**

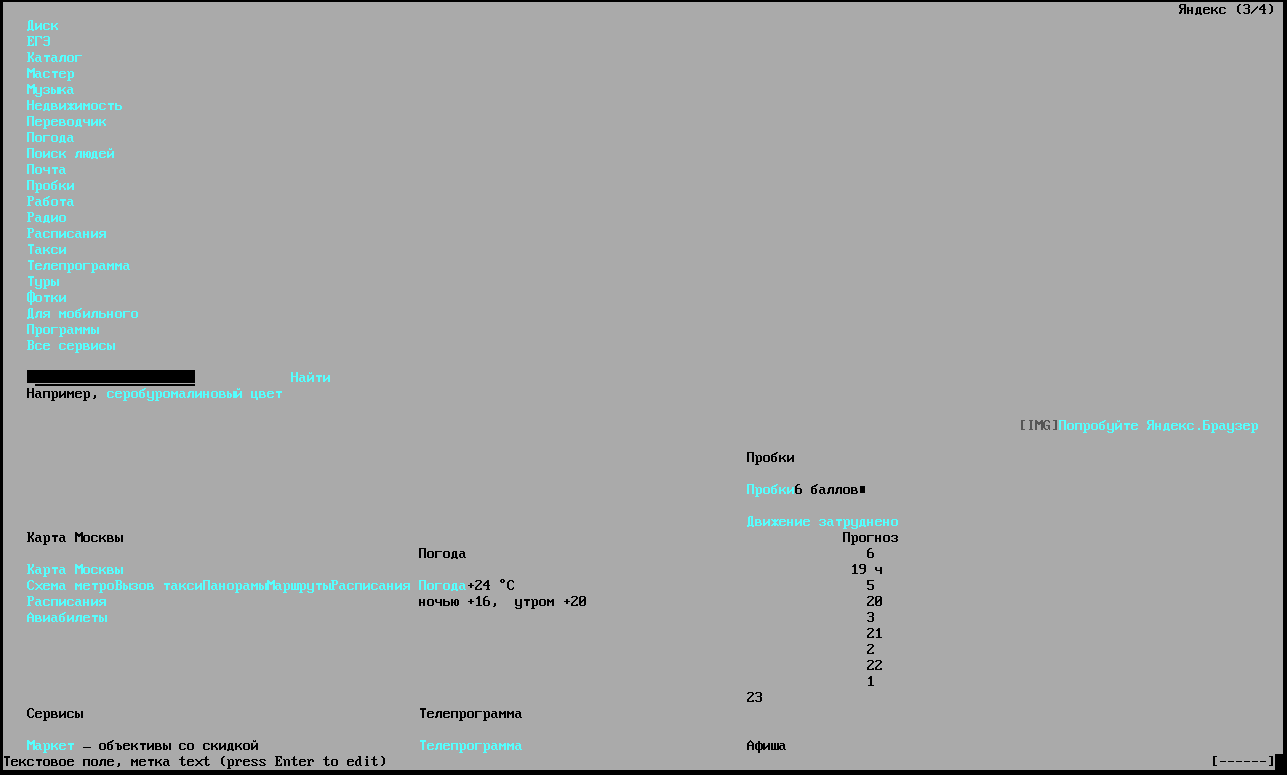
Также командой *yum update* можно обновить все установленные пакеты. Команда *yum list* выводит список всех установленных пакетов.

С помощью команды *yum install nano* устанавливается текстовый редактор nano.



С помощью команды *yum install elinks* устанавливается вэб-браузер elinks. Пользоваться им можно, введя URL нужного сайта в специальное окно, либо из консоли с помощью команды

*elinks \*адрес\_сайта\*.*



С помощью команды *yum install mc* устанавливается файловый менеджер mc.



**Задание 3**

**SSH** — сетевой протокол прикладного уровня, позволяющий производить удалённое управление операционной системой и туннелирование TCP-соединений (например, для передачи файлов). Шифрует весь траффик, включая и передаваемые пароли. SSH допускает выбор различных алгоритмов шифрования. SSH-клиенты и SSH-серверы доступны для большинства сетевых операционных систем.

Установить ssh-сервер можно командой *yum install ssh-server*. Настройки ssh-сервера находятся в файле /etc/ssh/sshd\_config. Настройки по умолчанию довольно небезопасны, поэтому лучше изменить некоторые из их.

**PermitRootLogin no**

Этот параметр разрешает или запрещает вход по SSH под суперпользователем.

**AllowUsers user@host**

Это означает, что доступ разрешён пользователю user с компьютера host.

**PermitEmptyPasswords no**

Параметр PermitEmptyPasswords разрешает или запрещает вход с пустым паролем.

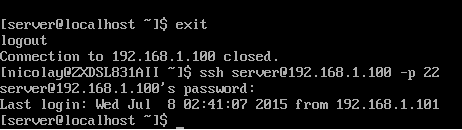
**Port 22**

Этот параметр устанавливает порт, по которому будет подключаться клиент. Для повышения безопасности следует заменить порт на нестандартный.

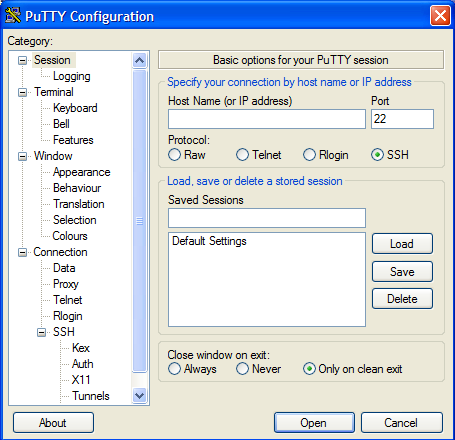
Чтобы подключиться к ssh-серверу, понадобится вторая виртуальная машина, на которую нужно установить ssh-клиент. На виртуальной машине с сервером нужно создать пользователя, к которому будет подключаться клиент. Чтобы подключиться к пользователю server на компьютере localhost через порт 22, необходимо написать следующую строчку:

*ssh server@localhost  –p 22*

Название компьютера можно заменить на его IP-адрес.



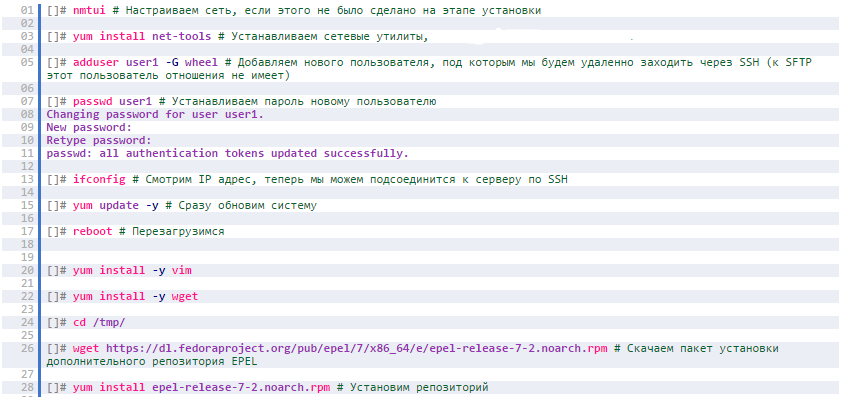
**PuTTy** - это популярный **SSH-клиент** и **Telnet** , то есть программа для безопасного подключения к удаленному компьютеру (или к серверу) и выполнения на нем различных команд. **PuTTY** ведет логи, позволяет настраивать шрифты, цвета и разрешение консоли, допускает сохранение в своей памяти ключей авторизации, поддерживает работу через прокси-сервер.

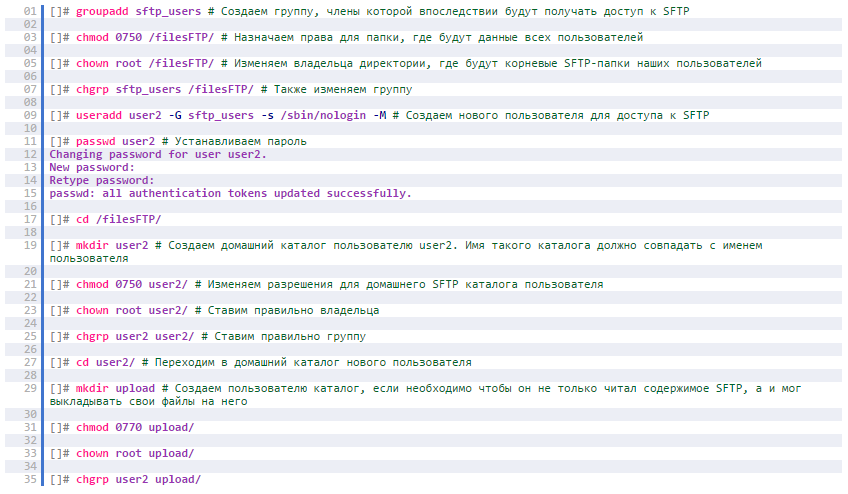


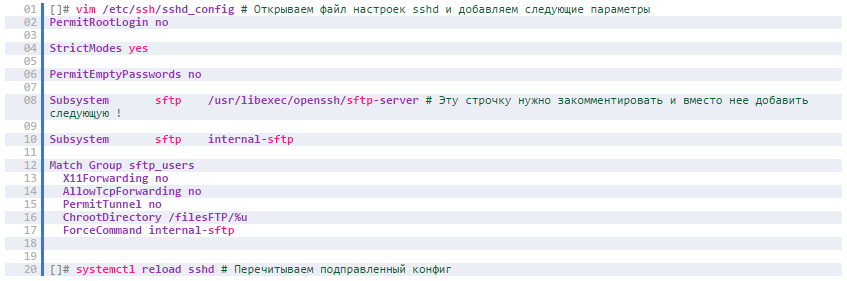
В поле **Host Name (or IP address)** нужно ввести имя вашего домена или IP. Затем нажать "открыть", и в появившемся окне ввести имя пользователя и его пароль. После этого вы сможете управлять данным пользователем.

**SFTP** — протокол прикладного уровня, предназначенный для копирования и выполнения других операций с файлами поверх надёжного и безопасного соединения.

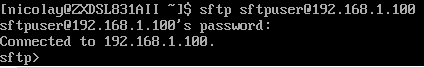
Чтобы настроить SFTP-сервер, необходимо выполнить следующие действия:







На вторую виртуальную машину нужно установить SFTP-клиент. Подключение к пользователю sftpuser сервера 192.168.1.100 производится с помощью команды *sftp sftpuser@192.168.1.100.*

**

**Tripwire** – свободная программа для мониторинга которая сообщает и предупреждает о любых изменениях в ваших файлах на сервере.

**Первым шагом, нужно установить репозиторий EPEL. Затем нужно скачать и установить Tripwire. Затем нужно создать для Tripwire локальный и для сайта ключи:** *tripwire-setup-keyfiles.*

Cледующим шагом нужно инициализировать Tripwire: *tripwire --init.*

В файле vim /etc/tripwire/twpol.txt находятся конфигурации программы, список проверяемых файлов. Добавим в список файлов для проверки файл /home/server/test, а затем, зайдя со второй машины с помощью ssh-соединения, изменим этот файл. В результате проверки, tripwire сообщит об изменении этого файла.

