Лабораторная работа № 1

Дисциплина: Информационная безопасность

Сулицкий Богдан Романович

Содержание

Список иллюстраций

1 Цель работы:

Целью данной работы является приобретение практических навыков установки операционной системы на виртуальную машину, настройки минимально необходимых для дальнейшей работы сервисов.

2 Выполнение лабораторной работы

1. Я запустил VirtualBox и создал новую виртуальную машину которую назвал “centOS”, оставив версию Red Hat так как она рекомендована инструкцией(2.1).

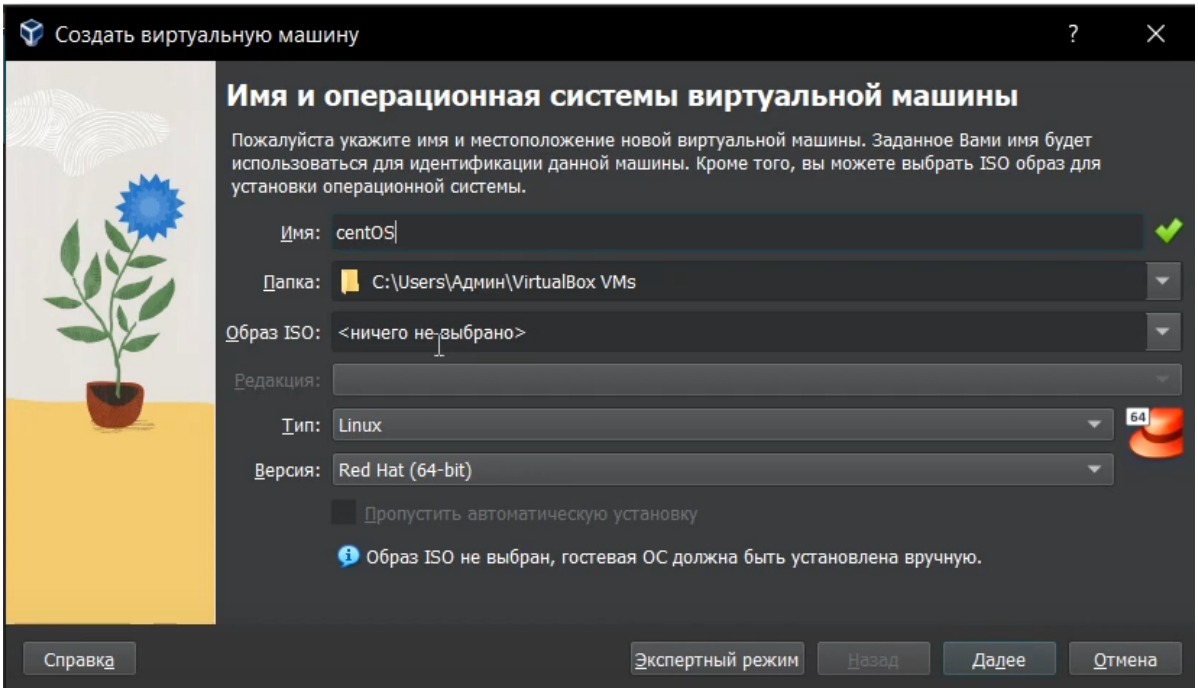

Рис. 2.1: Начало создания виртуальной машины

2. Я изменил значения параметров системы для более корректной работы в дальнейшем(2.2).

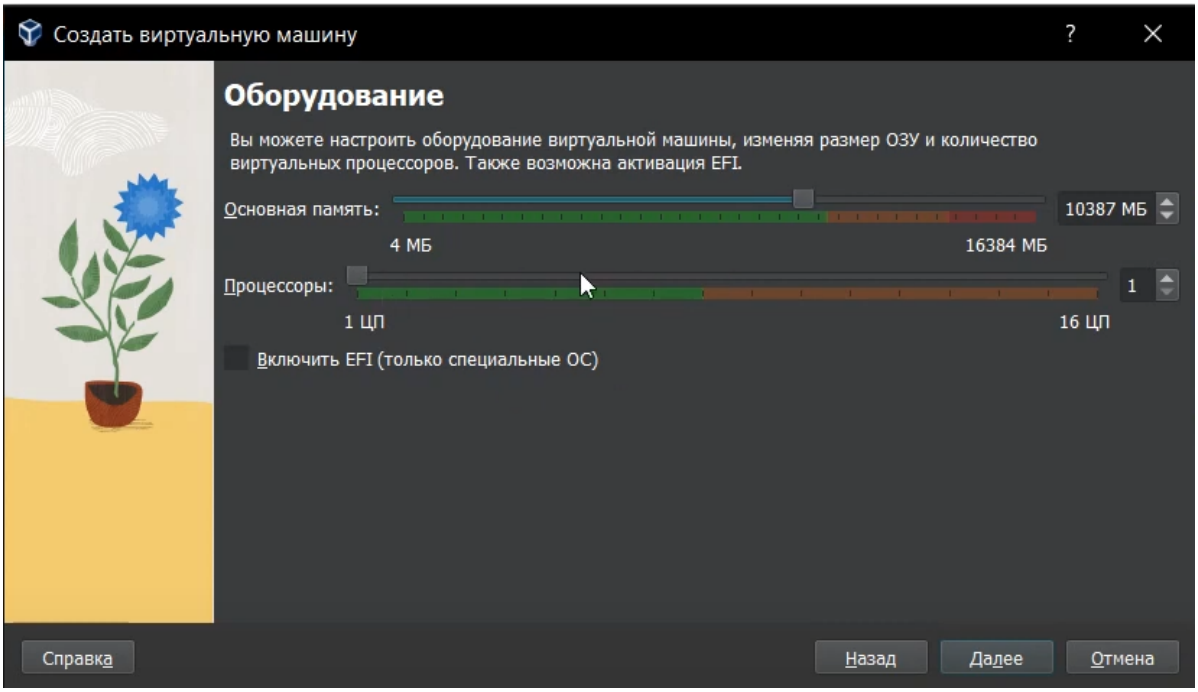

Рис. 2.2: Настройка ОЗУ

3. Я предоставил виртуальной машине 78 ГБ(2.3).

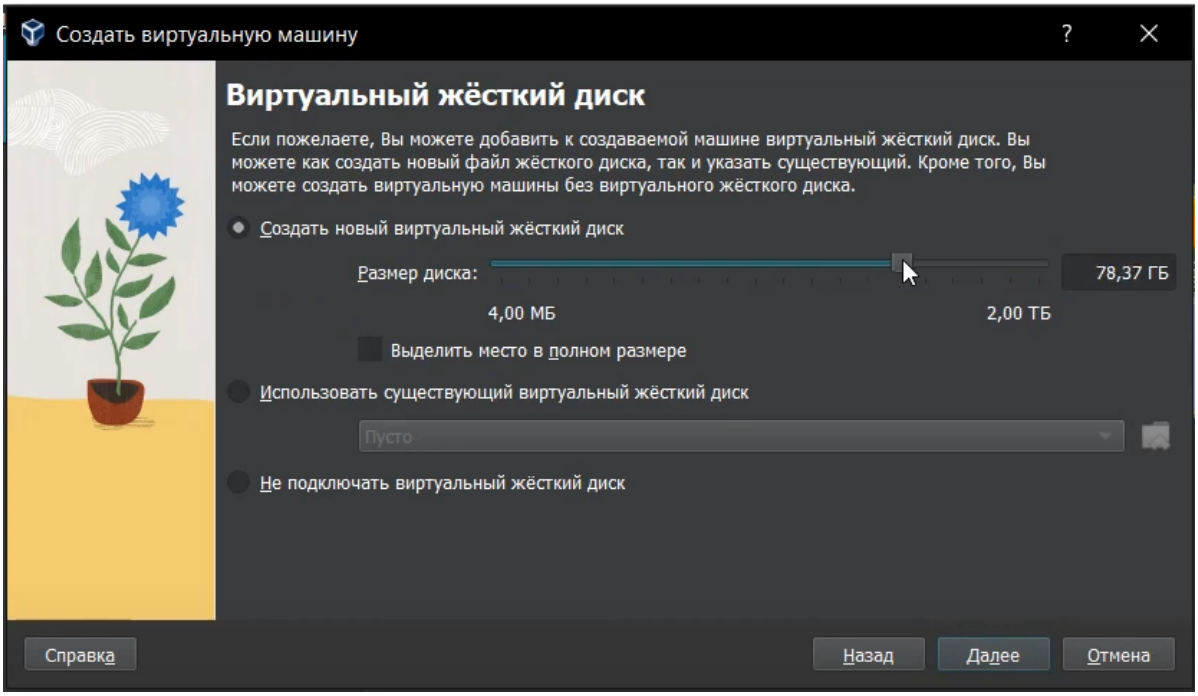

Рис. 2.3: Настройка виртуального жёсткого диска

4. Я создал виртуальную машину(2.4).

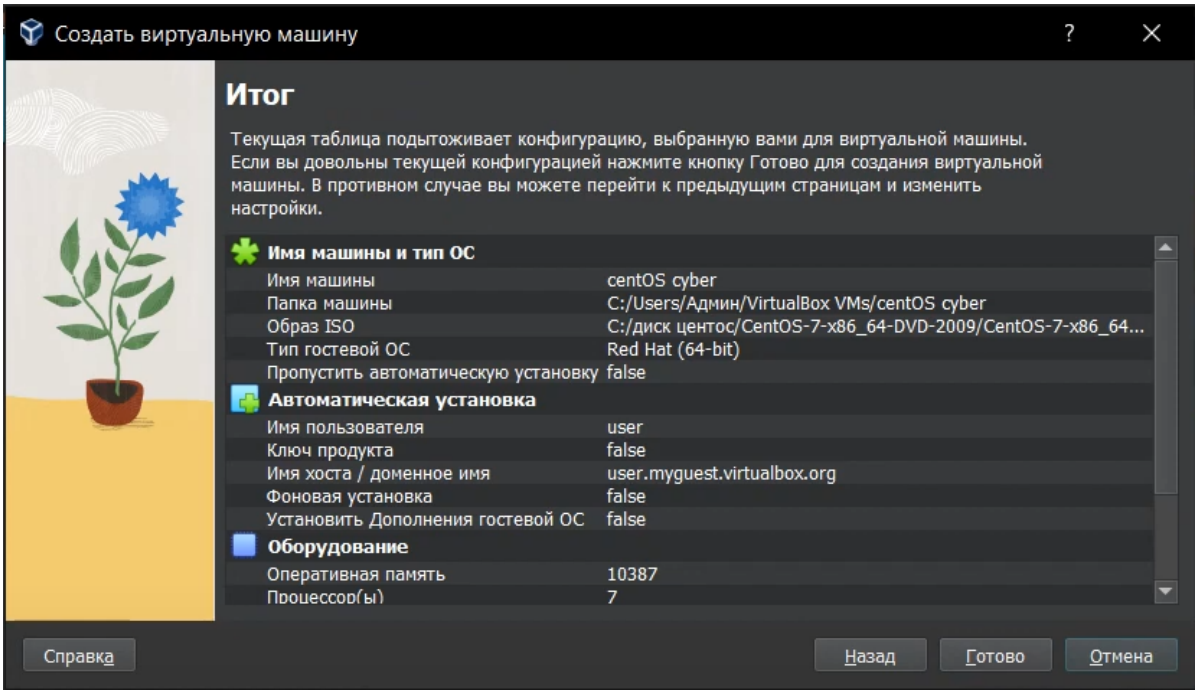

Рис. 2.4: Просмотр итога

5. Предварительно скачав подходящую версию образа CentOS 7 использую её как носителя, и запускаю виртуальную машину(2.5).

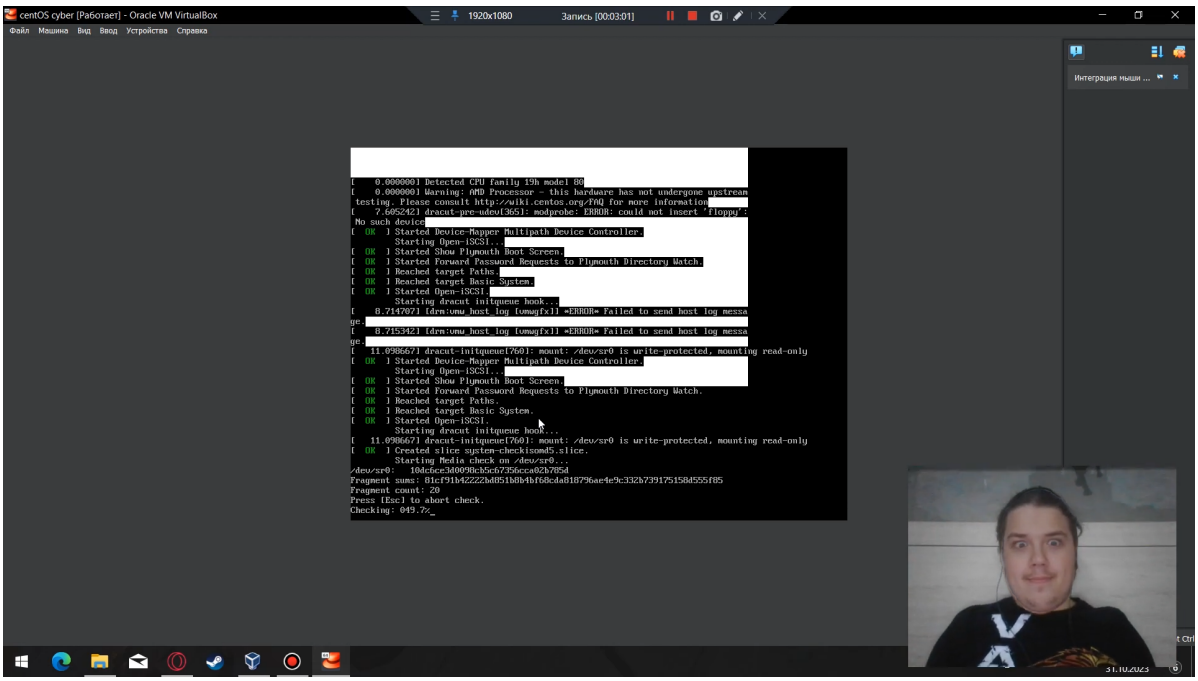

Рис. 2.5: Запуск centOS

6. Я указал дату и время(2.6).

Рис. 2.6: Дата и время

7. Я выбрал нужные дополнительные компоненты для ОС(2.7).

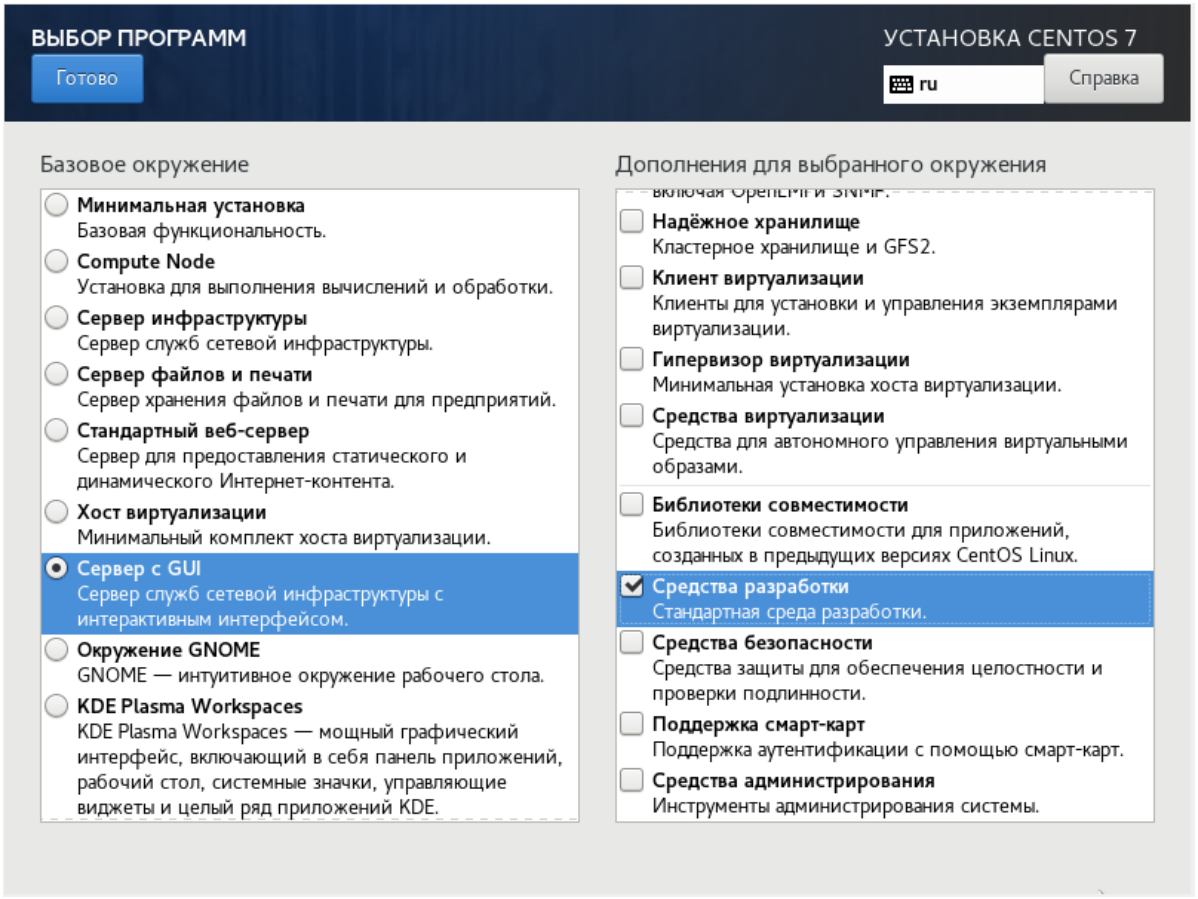

Рис. 2.7: Выбор программ

8. После настройки установки я нажал кнопку “Запустить установку”(2.8).

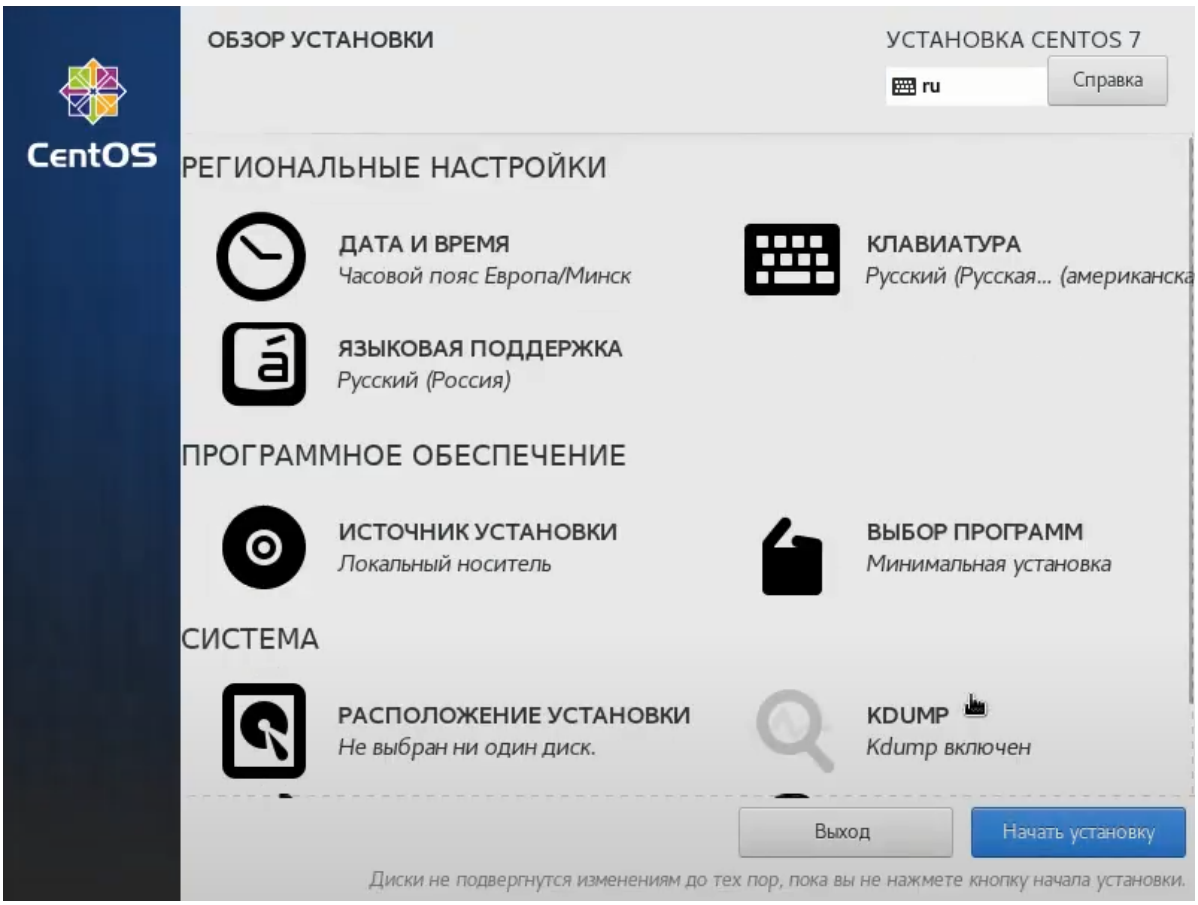

Рис. 2.8: Завершение настройки

9. Далее во время установки я задал пароль root и параметры администратора(2.9).

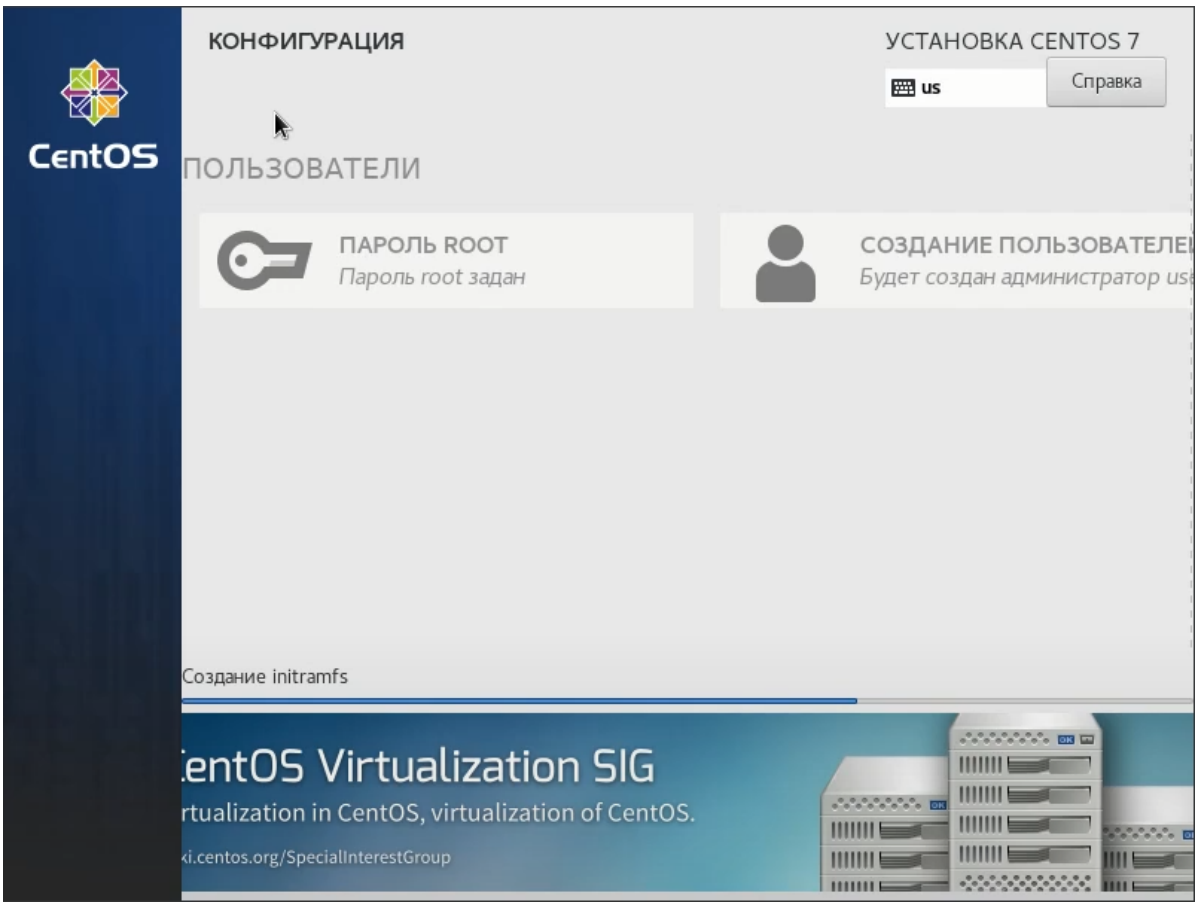

Рис. 2.9: Настройки параметров админ. учетной записи

10. После установки я запустил виртуальную машину(2.10).

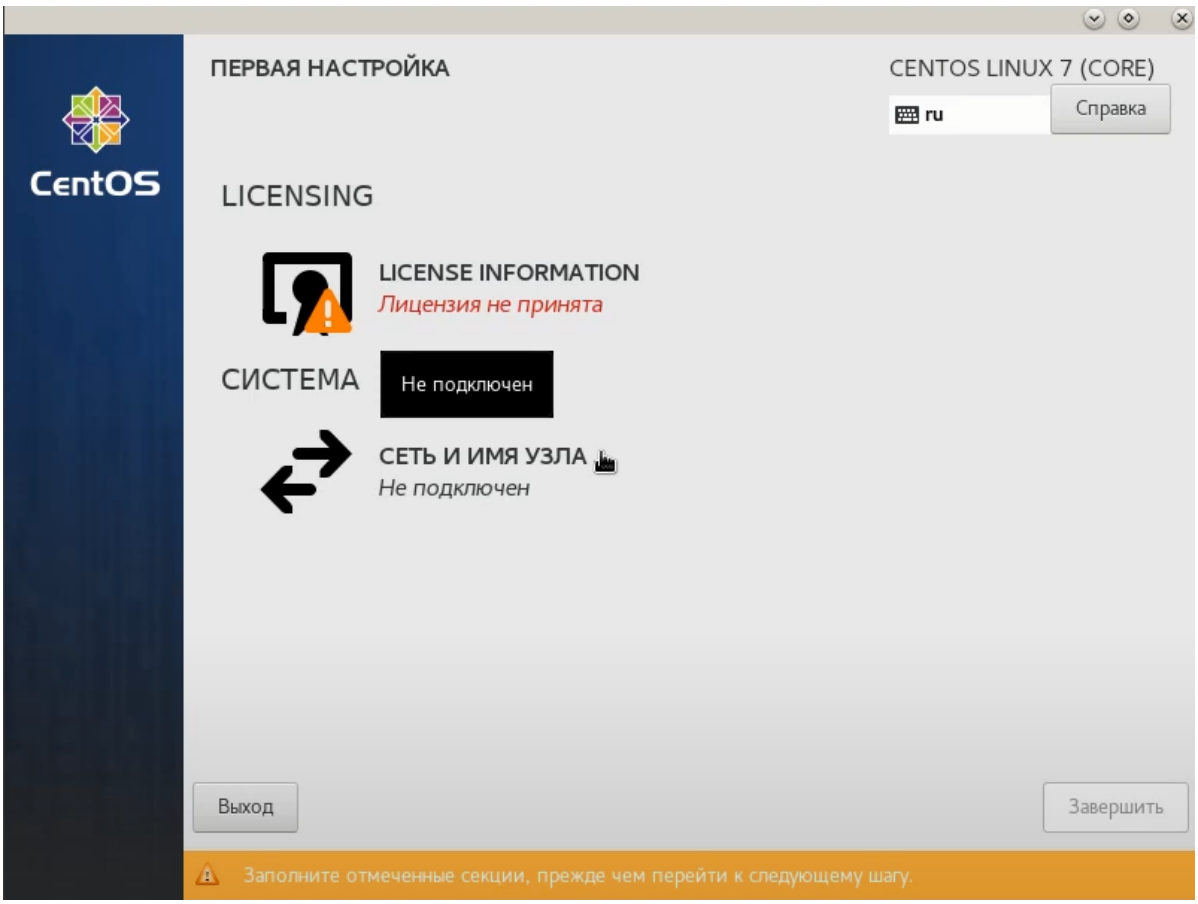

Рис. 2.10: Первая настройка ОС

И принял лицензию(2.11).

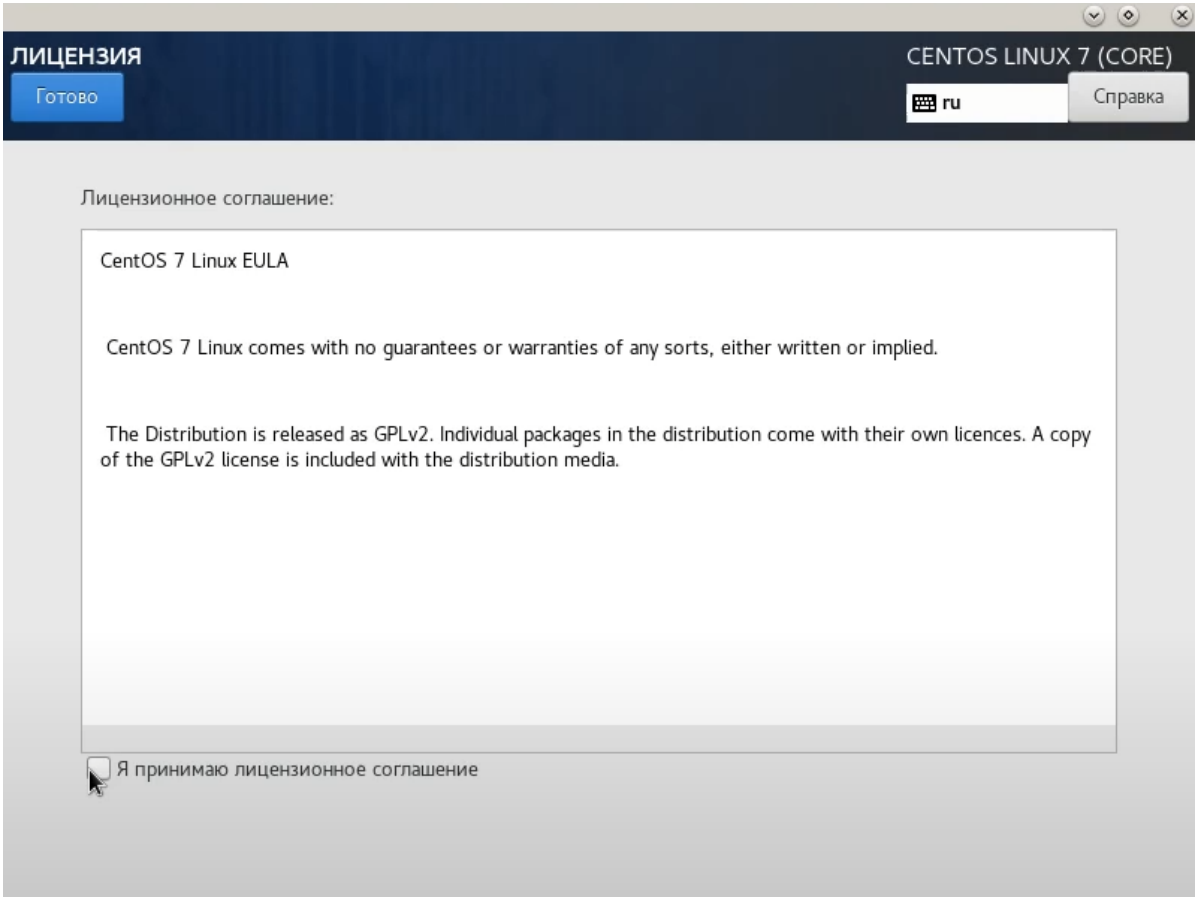

Рис. 2.11: Принятие лицензии

11. Я подключил образ диск доп. гостевой ОС(2.12).

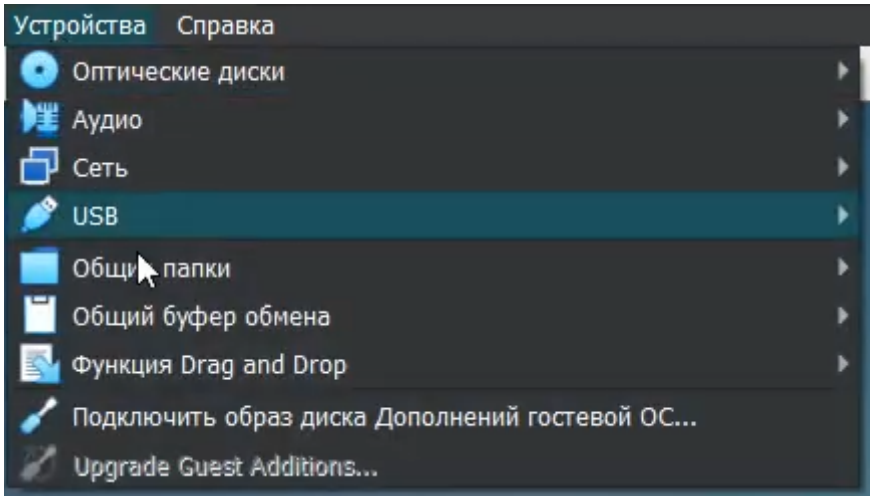

Рис. 2.12: Подключение ОС к гостевой библиотеке

12. Появляется системное окно. Я нажимаю на кнопку “Запустить”(2.13).

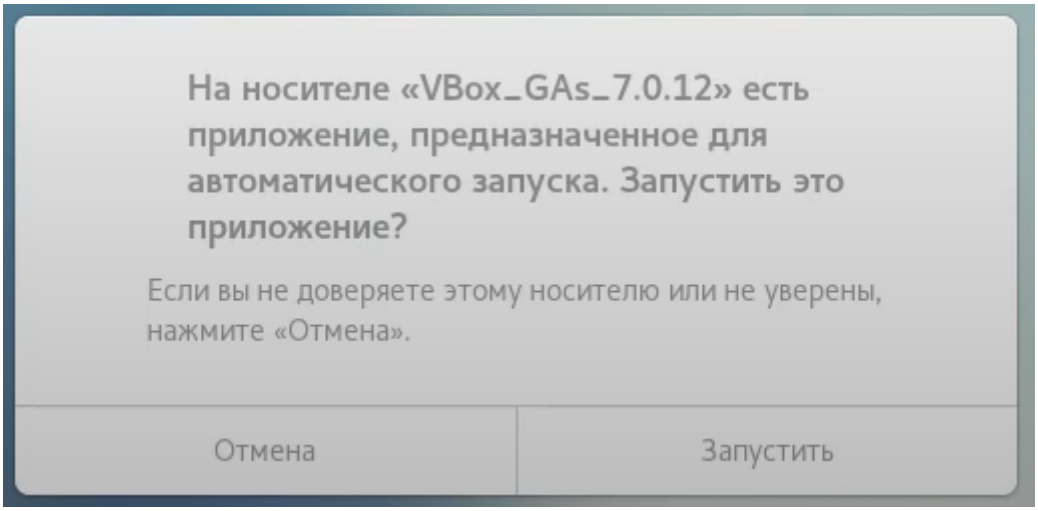

Рис. 2.13: Запуск приложения

И дожидаюсь окончания процесса(2.14).

```
Verifying archive integrity...  100%   MD5 checksums are OK. All good.
Uncompressing VirtualBox 7.0.12 Guest Additions for Linux  100%
VirtualBox Guest Additions installer
Copying additional installer modules ...
Installing additional modules ...
.VirtualBox Guest Additions: Starting.
VirtualBox Guest Additions: Setting up modules
VirtualBox Guest Additions: Building the VirtualBox Guest Additions kernel
modules.  This may take a while.
VirtualBox Guest Additions: To build modules for other installed kernels, run
VirtualBox Guest Additions:   /sbin/rcvboxadd quicksetup <version>
VirtualBox Guest Additions: or
VirtualBox Guest Additions:   /sbin/rcvboxadd quicksetup all
VirtualBox Guest Additions: Building the modules for kernel
3.10.0-1160.el7.x86_64.
VirtualBox Guest Additions: reloading kernel modules and services
VirtualBox Guest Additions: kernel modules and services 7.0.12 r159484 reloaded
VirtualBox Guest Additions: NOTE: you may still consider to re-login if some
user session specific services (Shared Clipboard, Drag and Drop, Seamless or
Guest Screen Resize) were not restarted automatically
Press Return to close this window...
```

Рис. 2.14: Процесс работы приложения

13. С помощью команды dmesg вывел нужные параметры системы(**??**).

```
[user@localhost ~]$ dmesg | grep -i "Linux version"
[    0.000000] Linux version 3.10.0-1160.el7.x86_64 (mockbuild@kbuilder.bsys.centos.org) (
[user@localhost ~]$ dmesg | grep -i "Mhz processor"
[    0.000000] tsc: Detected 2999.996 MHz processor
[user@localhost ~]$ dmesg | grep -i "CPU0"
[    0.115984] smpboot: CPU0: Intel(R) Core(TM) i7-9700 CPU @ 3.00GHz (fam: 06, model: 9e,
[user@localhost ~]$ dmesg | grep -i "memory"
[    0.000000] Base memory trampoline at [ffff94a240099000] 99000 size 24576
[    0.000000] Early memory node ranges
[    0.000000] PM: Registered nosave memory: [mem 0x0009f000-0x0009ffff]
[    0.000000] PM: Registered nosave memory: [mem 0x000a0000-0x000effff]
[    0.000000] PM: Registered nosave memory: [mem 0x000f0000-0x000fffff]
[    0.000000] Memory: 2012796k/2097088k available (7788k kernel code, 392k absent, 83900k
[    0.000000] please try 'cgroup_disable=memory' option if you don't want memory cgroups
[    0.047504] Initializing cgroup subsys memory
[    0.215337] x86/mm: Memory block size: 128MB
[    0.536506] Freeing initrd memory: 31212k freed
[    0.558399] Non-volatile memory driver v1.3
[    0.558506] crash memory driver: version 1.1
[    0.623093] Freeing unused kernel memory: 1984k freed
[    0.624004] Freeing unused kernel memory: 392k freed
[    0.624948] Freeing unused kernel memory: 536k freed
[    1.352600] [drm] Max dedicated hypervisor surface memory is 507904 kiB
[    1.352601] [drm] Maximum display memory size is 16384 kiB
[    1.352728] [TTM] Zone  kernel: Available graphics memory: 1023474 kiB
[user@localhost ~]$ dmesg | grep -i "Hypervisor detected"
[    0.000000] Hypervisor detected: KVM
[user@localhost ~]$ dmesg | grep -i "Filesystem"
[    1.935544] XFS (dm-0): Mounting V5 Filesystem
[    3.230283] XFS (sda1): Mounting V5 Filesystem
```

3 Выводы:

В результате выполнения работы ознакомился с основными этапами установки виртуальных машин и их настроек, а также создал виртуальную среду для выполнения последующих лабораторных работ.

4 Контрольные вопросы

1. Какую информацию содержит учётная запись пользователя?

Все важные данные о пользователя в систему, хранятся в файлах “/etc/passwd”, так в учётной записи хранится в первую очередь ID пользователя (где 0 это с root-правами и в системе CentOS 1-999 обычные пользователи), логин, пороль, идентификаторе группы, идентификаторе пользователя, начальный каталог и регистрационная оболочка. Если детально расмотреть структуру хранящихся данных то у нас получится такая строка данных: “User ID”:“Password”:“UID”:“GID”:“User Info”:“Home Dir”:“Shell”.

2. Укажите команды терминала и приведите примеры:

– для получения справки по команде; Для этого можно использовать команду “man”, данная команда может предоставить инструкцию или справку по использованию команды или программы. Если нужна краткая информация можно применить команду “whatis”.

– для перемещения по файловой системе; Чтобы перемещаться нужно знать где ты и куда можешь пойти для этого есть команда “ls” позволяющая просмотреть содержание нынешней папки, а также комадна “ll” позволяющая просмотреть начинку директории. И самая главная команда “cd” - меняет текущий каталог на указанный, при пустом вводе перемещает на уровень выше в древе каталога.

– для просмотра содержимого каталога; Как я указал выше для этого есть команда “ls” позволяющая просмотреть содержание нынешней папки, а также комадна “ll” позволяющая просмотреть начинку директории.

– для определения объёма каталога; В большенстве систем на linux можно использовать команду “sudo du” (особенно утилита du) она выведит занимаемое котологом место на диске.

– для создания / удаления каталогов / файлов; Стандартная команда для создание каталога или директории (файлов) “mkdir”, а также команды для взаимодействия с ними: “cp” - основная задача копирование и дублирование, “mv” - перемещение и переиминовывание, “rm” - удаление папок и файлов. Также есть команда “cat” - показывает что содержит файл или стандартный ввод, а также “ln” - создающая фактически ссылку как в windows ярлыки.

– для задания определённых прав на файл / каталог; фЕдинственная универсальная команда помимо задания прав при создании файла это “chmod”.

– для просмотра истории команд. Для этого есть стандартная команда “history”, так помимо опций указав число после команды она выведет именно столько последних команд.

3. Что такое файловая система? Приведите примеры с краткой характеристикой.

Одно из определений гласит “Файловая система связывает носитель информации (хранилище) с прикладным программным обеспечением, организуя доступ к конкретным файлам при помощи функционала взаимодействия программ API”. Тоесть файловая система это набор драйверов встроенных в систему которая при обращение программы к файлу по его имени (адресу) предостовляет информацию, касающуюся типа носителя, на котором записан файл, и структуры хранения данных. Получается на деле драйверы ФС оптимизируют запись и считывание отдельных частей файлов для ускоренной обработки запросов.

Так на система типа Linux можно увидеть много разных ФС: Ext2, Ext3, Ext4, JFS, ReiserFS, XFS, Btrfs, ZFS и т.д. А например на Windows в основном используется NTFS для внутрених файлов и FAT32 (или NTFS) для флешек и внешних насителей есть и другие, но они не так важны и универсальны. И на Android особенно более современных стоит Ext4 - внутренняя и FAT32 - внешняя.

NTFS (файловая система новой технологии) - стандарт был реализован в Windows NT в 1995 году, и по сей день является основным в Windows. Система NTFS имеет допустимый предел размера файлов до 16 гигабайт и размер диска (памяти) до 16 Эксабайт, а также Использование метод «прозрачного шифрования» (Encryption File System) разделяя доступ к файлом для разных пользователей и приложений.

4. Как посмотреть, какие файловые системы подмонтированы в ОС?

На большинстве современных систем можно легко и быстро определить это в свойствах диска. Но на разных системах Linux есть свои способы это проверить через настройки системы или команды. Так например эту информацию можно получить через утилиту Gnome Диски.

5. Как удалить зависший процесс?

В windows быстрее всего это сделать через диспечер задач или консоль (Win+R; cmd; tasklist; Taskkill “процесс”). В сестемах Linux есть несколько команд для этого с разной степень серьёзности: “SIGINT” - оправляет приложение команду правильного безопасного завершения, “SIGQUIT” - отличается от предыдущей возможностью проигнорировать сигнал и созданием dump-памяти, “SIGHUP” - сообщает процессу о разрыве соединения с терминалом (в основном связана с неполадками интернета), “SIGTERM” - немедленное завершение процесса проводимого самим процессом или дочерними, “SIGKILL” - зевершение процесса через ядро не мгновенное; и команды для убийства: “kill” - и тут многое зависит от опции если её нет то используется одна из выше указанных, если стоит “-TERM” то пытается принудительно или настойчиво закрыть процесс, и если это не помагает то испольуем “-KILL” что направляет все силы на уничтожение процесса.

Список литературы

1. Официальный сайт VirtualBox
2. Источник скачивание CentOS
3. Материал для выполнения лабораторной
4. Официальный сайт CentOS