МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное
учреждение высшего образования
«СЕВАСТОПОЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

ИНСТИТУТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
И УПРАВЛЕНИЯ В ТЕХНИЧЕСКИХ СИСТЕМАХ

Кафедра информатики и управления в технических системах

# ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ДИСЦИПЛИНЕ «АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ»

**Методические указания**
к выполнению лабораторных работ
для студентов направления подготовки
27.03.04 – Управление в технических системах

Севастополь
СевГУ
2020

УДК 004.7
ББК 32.972
О-72

**Р е ц е н з е н т**:
**В.А. Карапетьян** – доцент кафедры «Информатика и управление в технических системах», кандидат технических наук, доцент

*Составитель:* А.Е. Осадченко

**О-72 Лабораторный практикум по дисциплине «Администрирование компьютерных сетей»** : методические указания для студентов направления подготовки 27.03.04 – Управление в технических системах / Сост. А.Е. Осадченко ; Министерство науки и высшего образования РФ, Севастопольский государственный университет, Институт информационных технологий и управления в технических системах кафедра информатики и управления в технических системах. – Севастополь : СевГУ, 2020. – 82 с. – Текст : электронный.

В лабораторном практикуме приводятся описания лабораторных работ, целью которых является исследование средств виртуализации для создания и администрирования компьютерных сетей.

Лабораторный практикум предназначен для студентов направления подготовки 27.03.04 – Управление в технических системах.

УДК 004.7
ББК 32.972

Лабораторный практикум рассмотрен и утверждён на заседании кафедры «Информатика и управления в технических системах», протокол № 6 от 28 февраля 2020 г.

Лабораторный практикум рассмотрен и рекомендован к изданию на заседании ученого совета Института информационных технологий и управления в технических системах, протокол № 4 от 3 марта 2020 г.

# СОДЕРЖАНИЕ



# ВВЕДЕНИЕ

Лабораторный практикум включает пять лабораторных работ, охватывающие основные разделы изучаемой дисциплины. Первая лабораторная работа, посвящена ознакомлению с программами виртуализации и выполняется в течении двух академических часов. Остальные лабораторные работы выполняется в течение четырех академических часов. В процессе подготовки к выполнению работы студент должен ознакомиться с основными теоретическими положениями, описанием используемого программного обеспечения (ПО), последовательностью его установки и настройки.

Все лабораторные работы выполняются в виртуальных машинах(ВМ), созданных при помощи программ виртуализации, которые позволяют осуществлять установку и настройку различных операционных систем (ОС), создавать компьютерные сети, производить их администрирование.

Вторая лабораторная работа посвящена установке и настройке ОС Linux на ВМ и инсталляции дополнительного ПО.

В третьей лабораторной работе исследуются вопросы создания и администрирования компьютерной сети на основе ВМ с различными типами ОС.

В четвертой лабораторной работе исследуется ПО удаленного администрирования ОС Linux и ОС Windows.

Пятая лабораторная работа посвящена исследованию программ для шифрования, обеспечивающих безопасность и конфиденциальность важных данных[1, с. 527].

# 1. ЛАБОРАТОРНАЯ РАБОТА № 1 УСТАНОВКА И НАСТРОЙКА ВИРТУАЛЬНЫХ МАШИН

## 1.1 Виртуальные машины

Понятие виртуализации представляет собой сокрытие настоящей реализации какого-либо процесса или объекта от истинного его представления для того, кто им пользуется. Продуктом виртуализации является нечто удобное для использования, на самом деле, имеющее более сложную или совсем иную структуру, отличную от той, которая воспринимается при работе с объектом. Виртуальная ОС

– это программная реализация, эмулирующая аппаратное и (или) программное обеспечение некоторой платформы [2, с.13].

Виртуальная машина (ВМ, от англ. virtual machine) — 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.

Также спецификация некоторой вычислительной среды (например: «виртуальная машина языка программирования Си»).

Виртуальная машина исполняет некоторый машинно-независимый код или машинный код реального процессора.

Помимо процессора, ВМ может эмулировать работу, как отдельных компонентов аппаратного обеспечения, так и целого реального компьютера (включая BIOS, оперативную память, жёсткий диск и другие периферийные устройства) [2, с.13]. В последнем случае в ВМ, как и на реальный компьютер, можно устанавливать операционные системы (например, ОС Windows можно запускать в виртуальной машине под ОС Linux или наоборот).

Использование технологий виртуализации повышает безопасность информационных систем. Если какое-то приложение или компонент вызывает сомнения в его надежности и защищенности, можно использовать его на виртуальной машине без опасности повредить жизненно важные компоненты системы. Такую изолированную среду называют также «песочницей» (sandbox). Помимо этого, можно создавать виртуальные машины, ограниченные политиками безопасности (например, машина перестанет запускаться через две недели).

На одном компьютере может функционировать несколько ВМ (это может использоваться для имитации нескольких серверов на одном реальном сервере с целью оптимизации использования ресурсов сервера).

На одном физическом компьютере может быть установлено несколько ВМ, с различными операционными системами (Windows различных версий, разные варианты Linux, FreeBSD и т.д.) которые можно объединить в локальную сеть[2, с.14].

Такая особенность предоставляет возможности по созданию моделей виртуальной сети между несколькими системами на одном физическом компьютере. Особенно это необходимо, когда требуется смоделировать некую распределенную систему, состоящую из нескольких машин. Это может использоваться для имитации нескольких серверов на одном реальном сервере с целью оптимизации использования ресурсов сервера.

Также можно создать несколько изолированных пользовательских окружений (для работы, развлечений, работы в Интернет), запустить их и переключаться между ними по мере необходимости выполнения тех или иных задач.

### 1.2Возможности Oracle VM VirtualBox

Oracle VM VirtualBox[3] представляет собой систему виртуализации для ОС Windows, Linux и Mac OS и обеспечивает взаимодействие с гостевыми ОС Windows, Linux, OpenBSD, FreeBSD, OS/2 Warp.

VirtualBox поддерживает широкий набор современных аппаратных средств.

Осуществляется поддержка виртуализации аудиоустройств, виртуализации сетевых устройств. Обеспечивается высокая производительность и незначительное потребление ресурсов ПК, а также поддержка различных видов сетевого взаимодействия (NAT, Host Network, Bridge, Internal).

Имеется возможность сохранения снимков ВМ (snapshots), к которым может быть произведен откат из любого состояния гостевой системы, а также настройка и управление приложением VirtualBox и виртуальной системой из командной строки.

Программа устанавливается и запускается как обычная программа для Windows. Её можно загрузить с сайта разработчика[3].

### 1.3 Создание виртуальной машины

Для создания ВМ необходимо запустить программу Oracle VM VirtualBox. На рабочем столе откроется окно программы вид которого показан на рис. 1.1.

Если возникает необходимость изменить язык интерфейса программы необходимо использовать меню **Файл** и **Настройки** как показано на рис. 1.2 и выбрать необходимый язык интерфейса программы как показано на рис. 1.3.

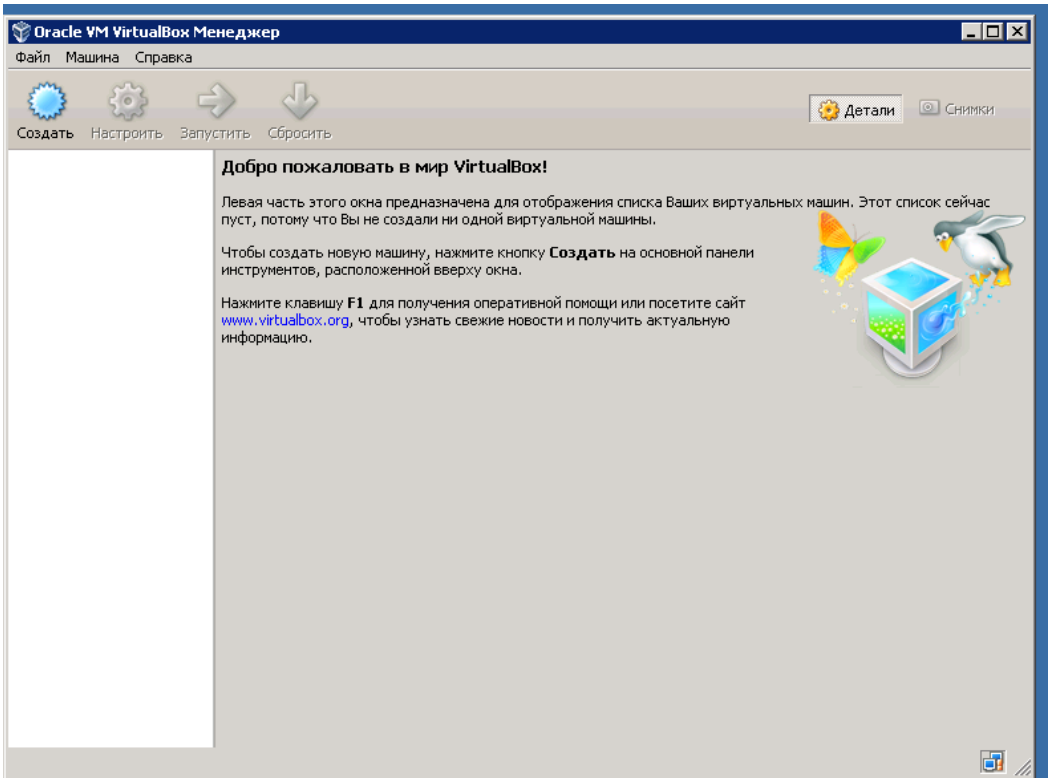


Рис. 1.1. – Программа Oracle VM VirtualBox

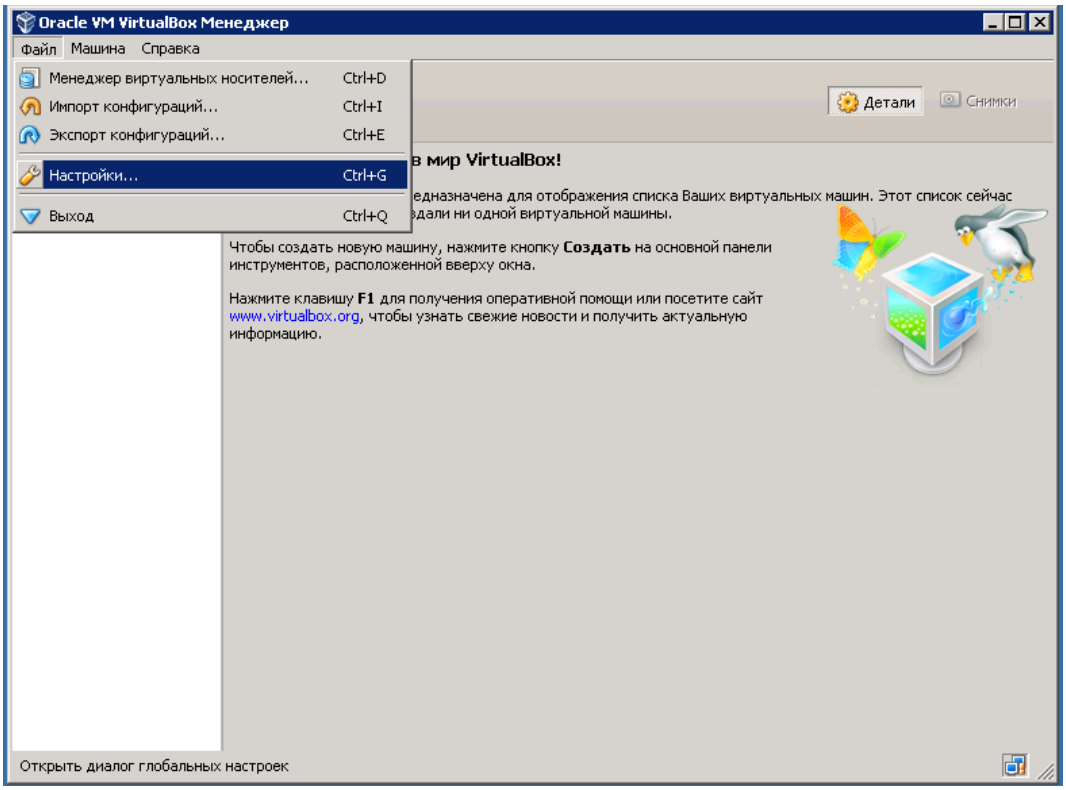


Рис. 1.2. – Настройка программы Oracle VM VirtualBox

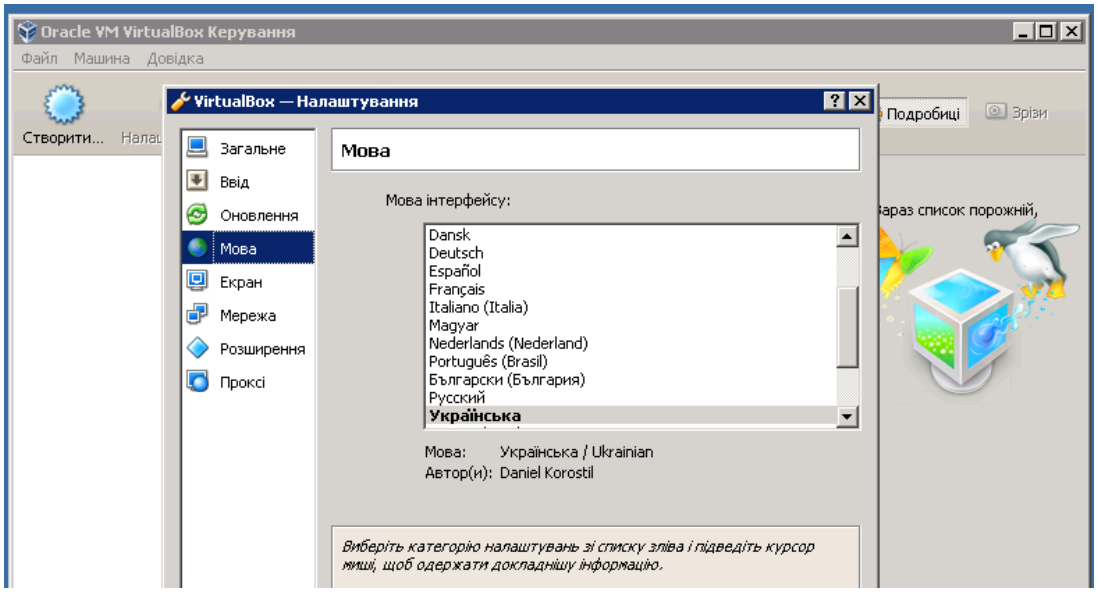


Рис. 1.3. – Выбор языка интерфейса программы

Для создания новой ВМ необходимо придумать ее имя, выбрать тип и версию операционной системы (ОС) как показано на рис. 1.4.

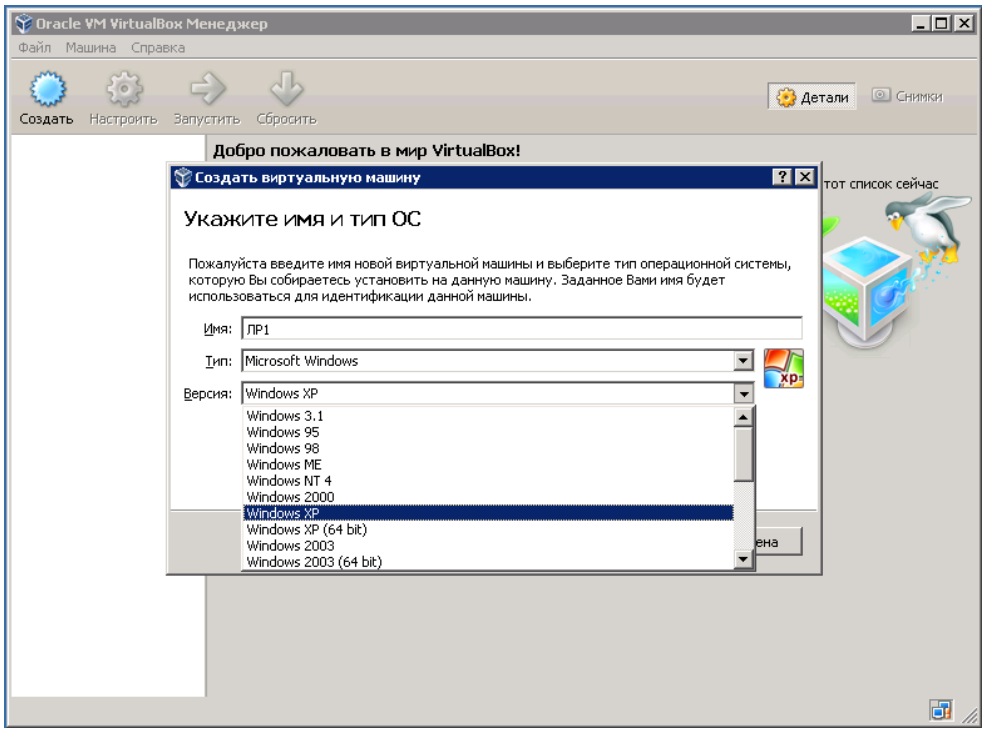


Рис. 1.4. – Имя и тип операционной системы

Если тип и версия ОС неизвестны, вводится тип **Other** как показано на рис. 1.5

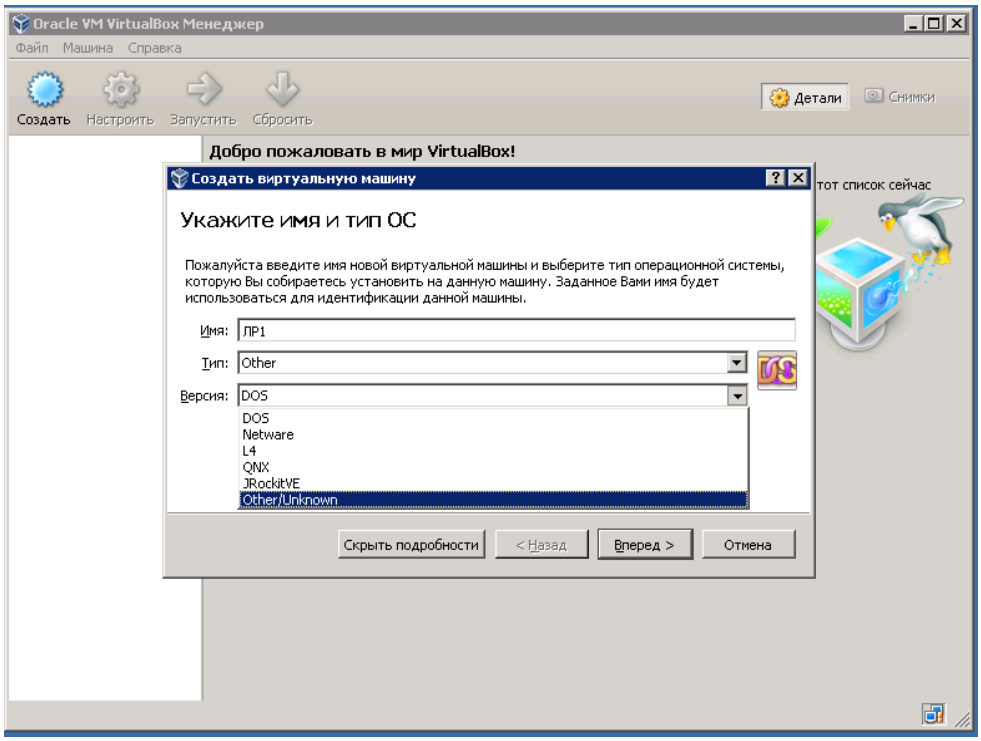


Рис. 1.5. – Неизвестный программе тип операционной системы

Далее необходимо указать объем оперативной памяти которая будет выделена ВМ как показано на рис 1.6. Величина памяти зависит от типа ОС и используемых приложений (для ОС Windows XP достаточно 192 МБ)

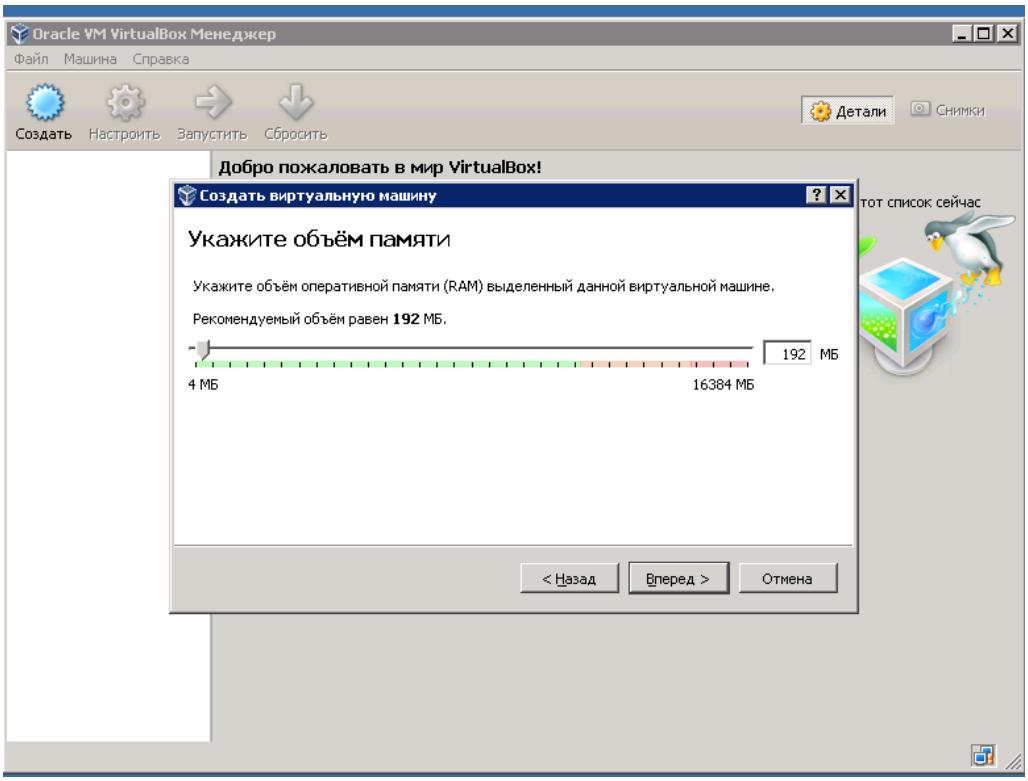


Рис. 1.6. – Указание объема памяти ВМ

На следующем этапе производится выбор, и подключение виртуального жесткого диска ВМ как показано на рис. 1.7.

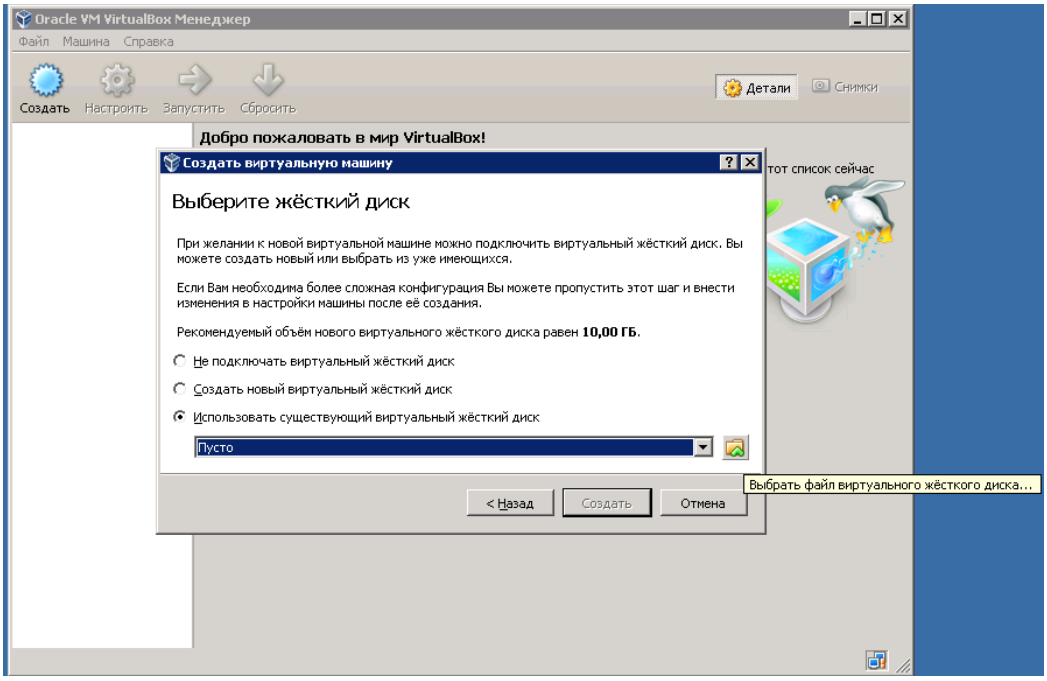


Рис. 1.7. – Подключение виртуального жесткого диска

Если имеются файлы, содержащие образы виртуальных жестких дисков (с расширением VDI) их можно выбрать, как показано на рис. 1.8.

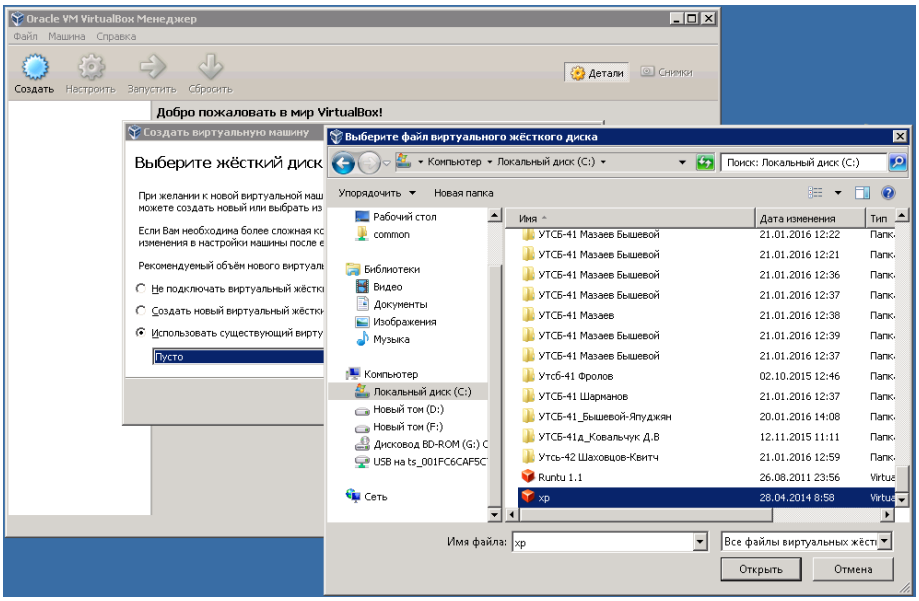


Рис. 1.8. – Выбор образа виртуального жесткого диска

После выбора виртуального жесткого диска окно программы Oracle VM VirtualBox будет содержать информацию о созданной ВМ (рис. 1.9).

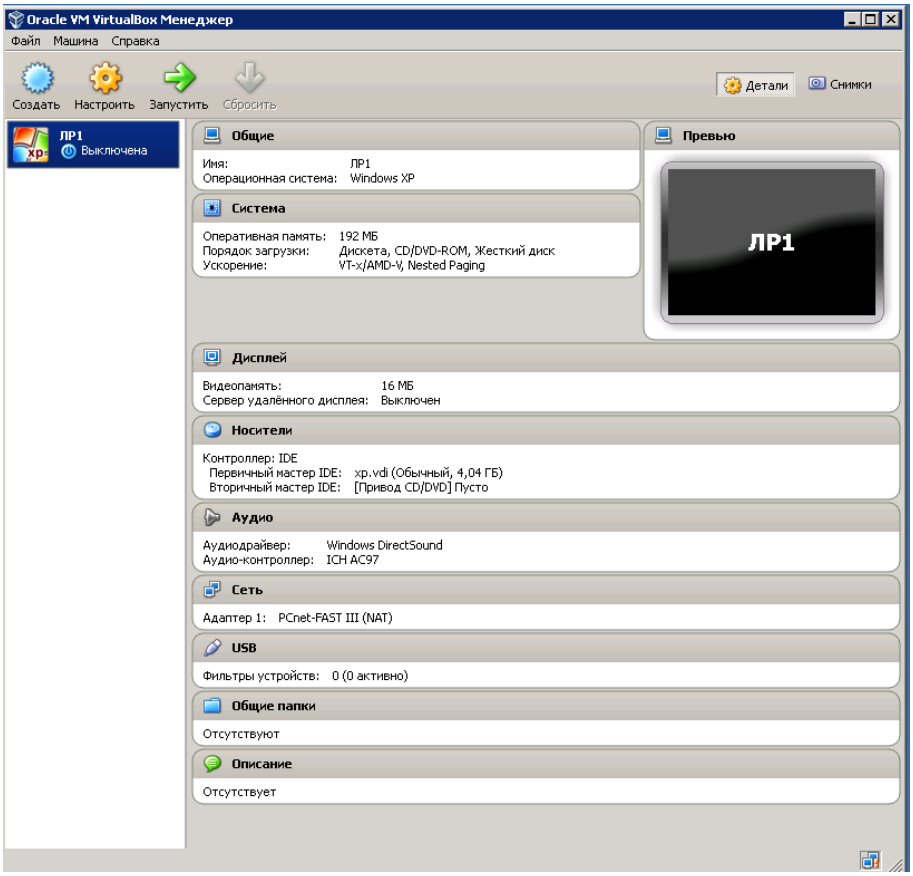


Рис. 1.9. – Параметры созданной ВМ

Если предполагается использовать один файл образа для одновременной работы нескольких ВМ (например, в компьютерном классе или на сервере) необходимо установить атрибут множественного подключения к файлу с образом виртуального жесткого диска. Для этого сначала необходимо выбрать меню настройки ВМ как показано на рис. 1.10.

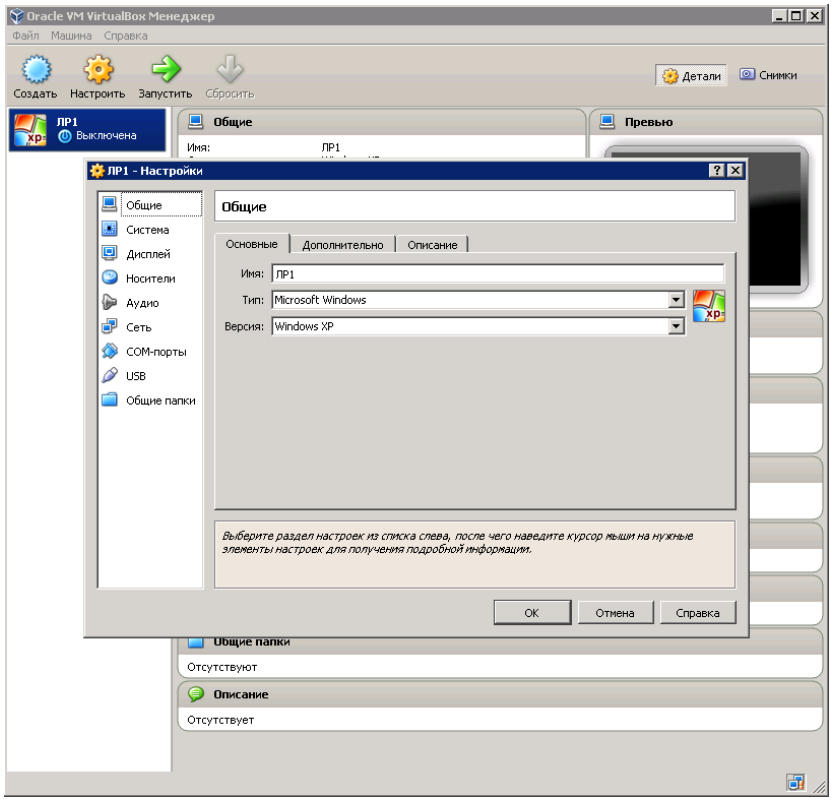


Рис. 1.10. – Настройки ВМ

Затем необходимо выбрать меню носители как показано на рис. 1.11 и при помощи значка “-” удалить из списка файл образа виртуального жесткого диска для которого будет делаться настройка множественного подключения.

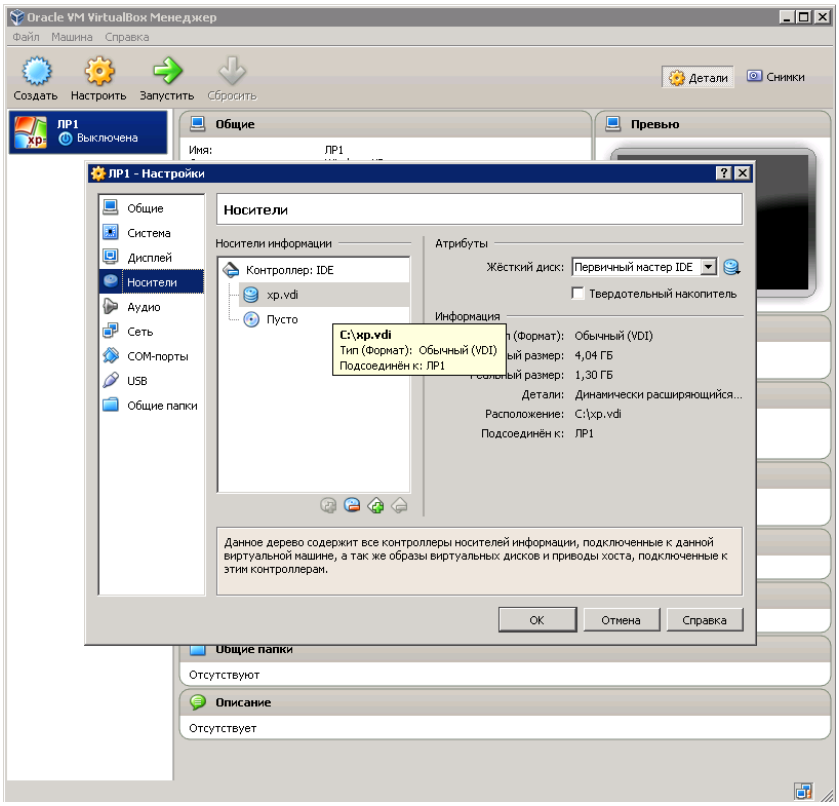


Рис. 1.11. – Носители ВМ

Далее необходимо выбрать меню **Файл** и подменю **Менеджер виртуальных носителей** как показано на рис. 1.12

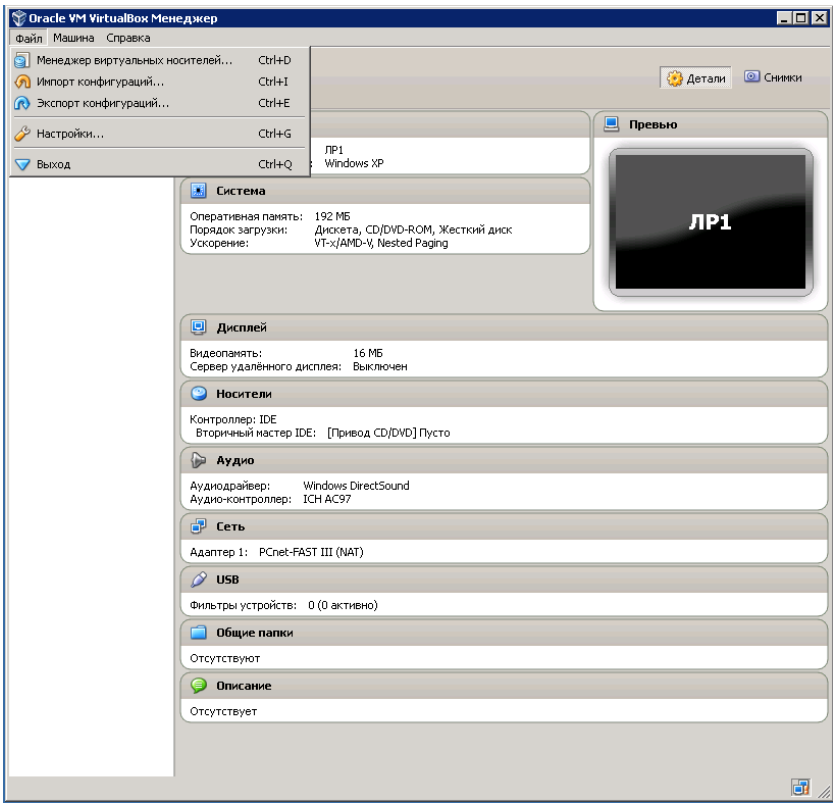


Рис. 1.12. – Менеджер виртуальных носителей

После открытия списка виртуальных носителей, можно произвести изменение их атрибутов, как показано на рис. 1.13.

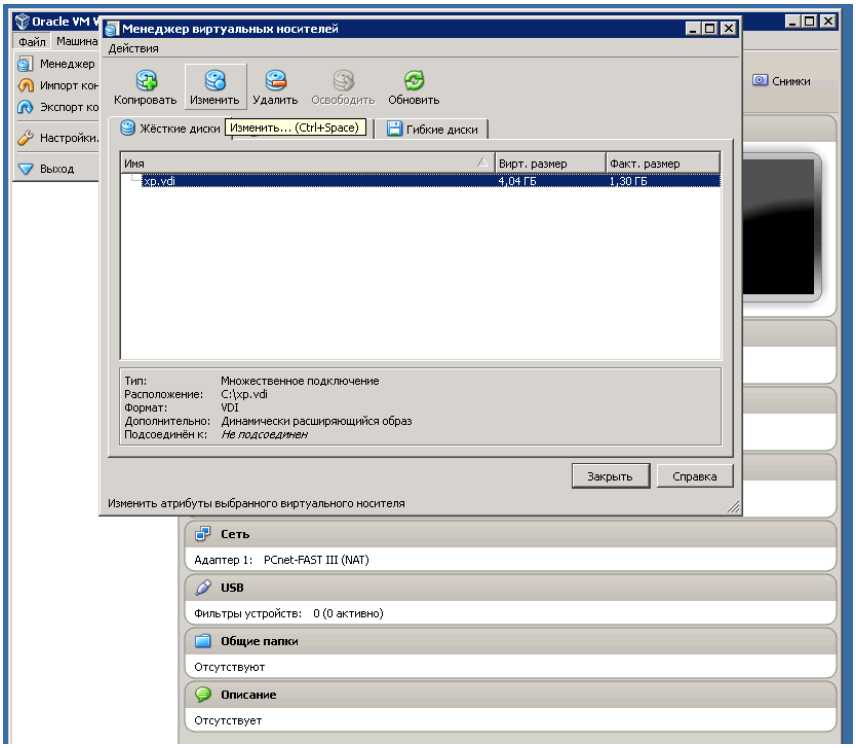


Рис. 1.13. – Изменение атрибутов виртуального носителя

Возможные варианты атрибутов носителя представлены на рис. 1.14. Если атрибут множественного подключения не был установлен, то необходимо установить его.

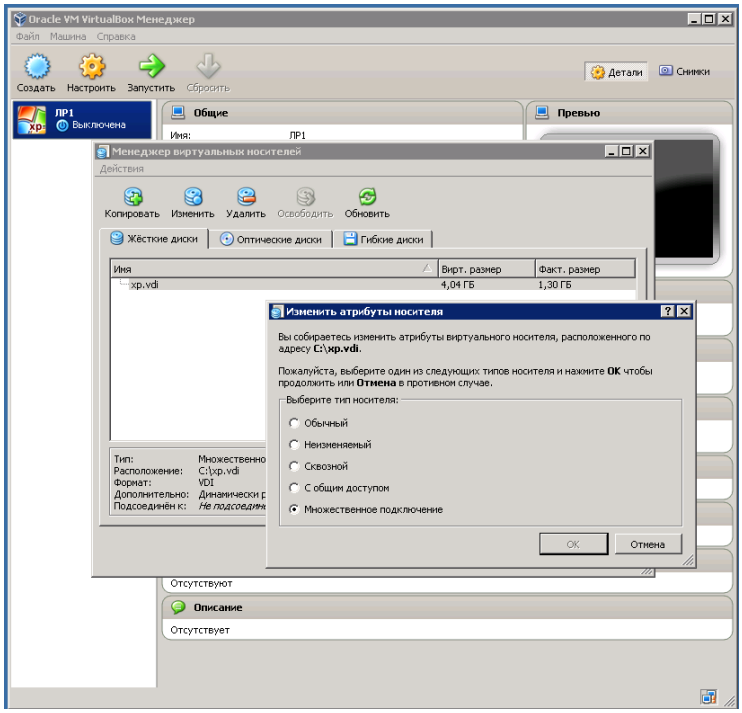


Рис. 1.14. – Выбор атрибута виртуального носителя

После установки необходимого атрибута виртуального носителя необходимо вновь подключить его к ВМ. Для этого сначала необходимо выбрать меню настройки ВМ как показано на рис. 1.10, затем необходимо выбрать меню носители как показано на рис. 1.11 и при помощи значка “+” добавить файл образа виртуального жесткого диска как показано на рис. 1.15.

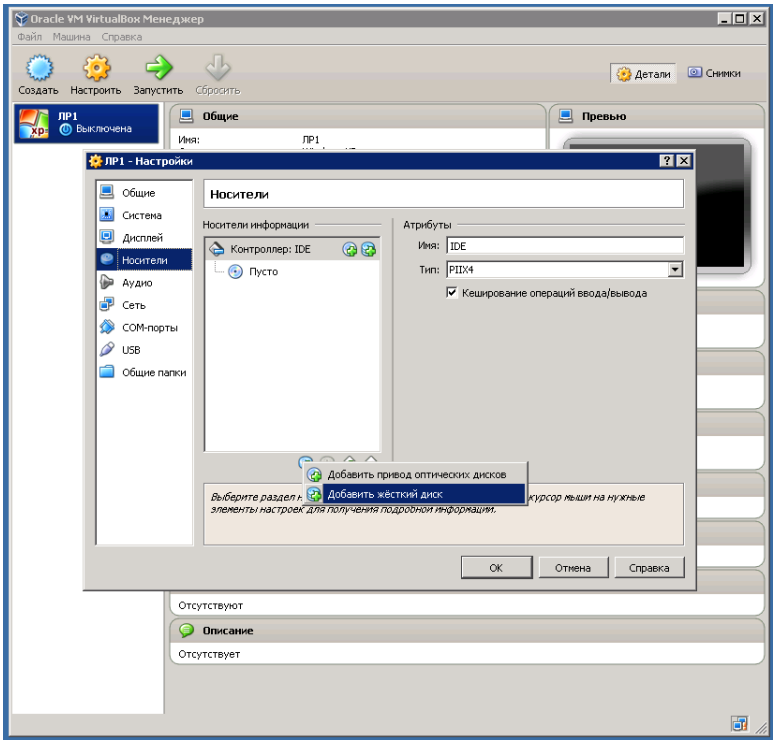


Рис. 1.15. – Добавление виртуального жесткого диска

Далее необходимо выбрать существующий жесткий диск (рис. 1.16) и имя файла образа виртуального жесткого диска как показано на рис. 1.17. Результат представлен на рис. 1.11, но у жесткого диска будет установлен атрибут множественного подключения.

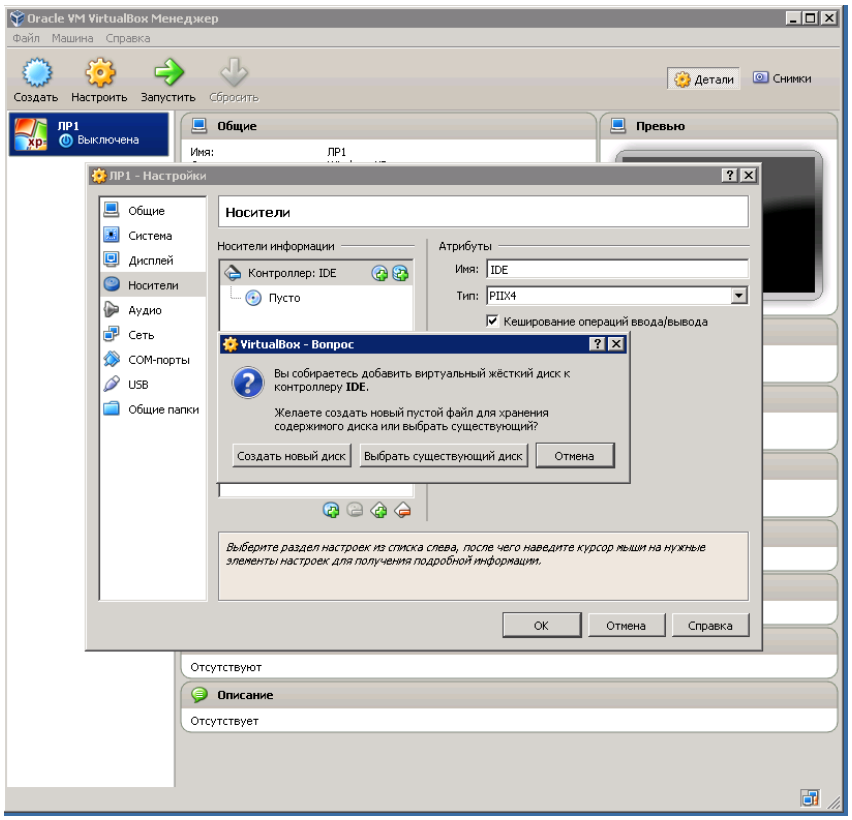


Рис. 1.16. – выбор существующего жесткого диска

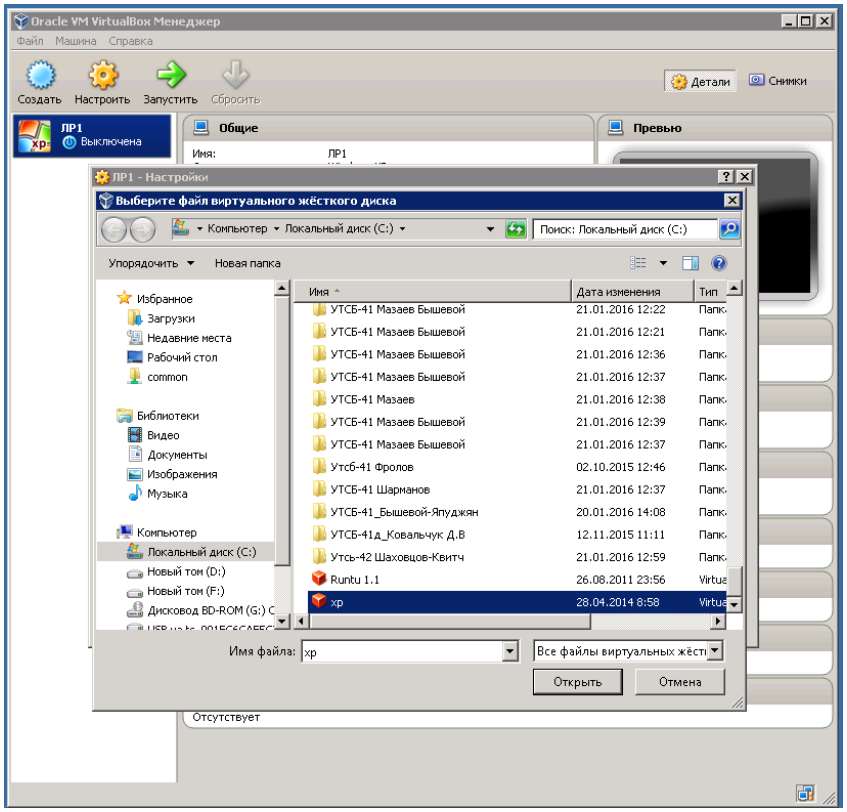


Рис. 1.17. – Выбор образа виртуального жесткого диска

После установки атрибута множественного подключения можно произвести запуск созданной ВМ. После нескольких сообщений об особенностях работы устройств ввода, на которые нужно ответить откроется окно, в котором будет отображаться рабочий стол ВМ, как показано на рис. 1.18.

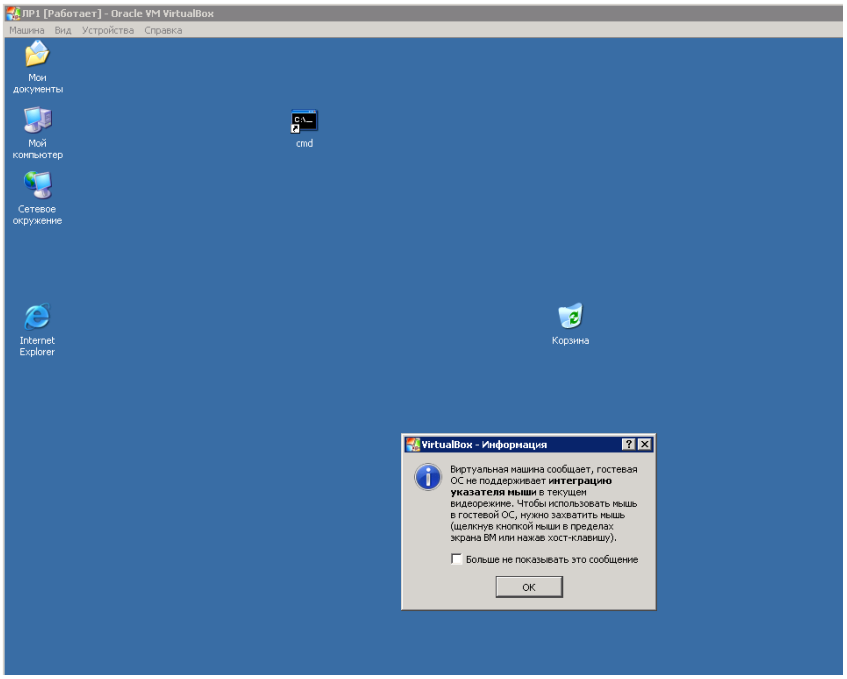


Рис. 1.18. – Рабочий стол на ВМ

Варианты закрытия ВМ представлены на рис. 1.19. Можно сохранить состояние ВМ и в любое время восстановить ее работу, при этом будет восстановлены все настройки ОС и все запущенные программы. Можно также завершить работу ОС как на персональном компьютере или выключить ВМ без сохранения данных.

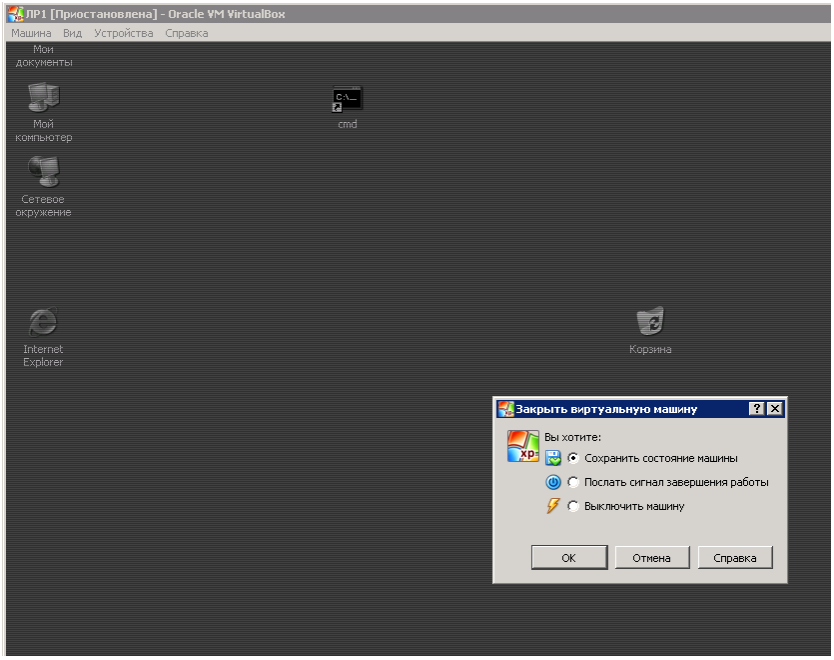


Рис. 1.19. – Закрытие ВМ

Аналогично создаются виртуальные машины с другими ОС. На рисунках 1.20 и 1.21 показаны снимки экрана при запуске ОС Runtu.


Рис. 1.20. – ОС Runtu

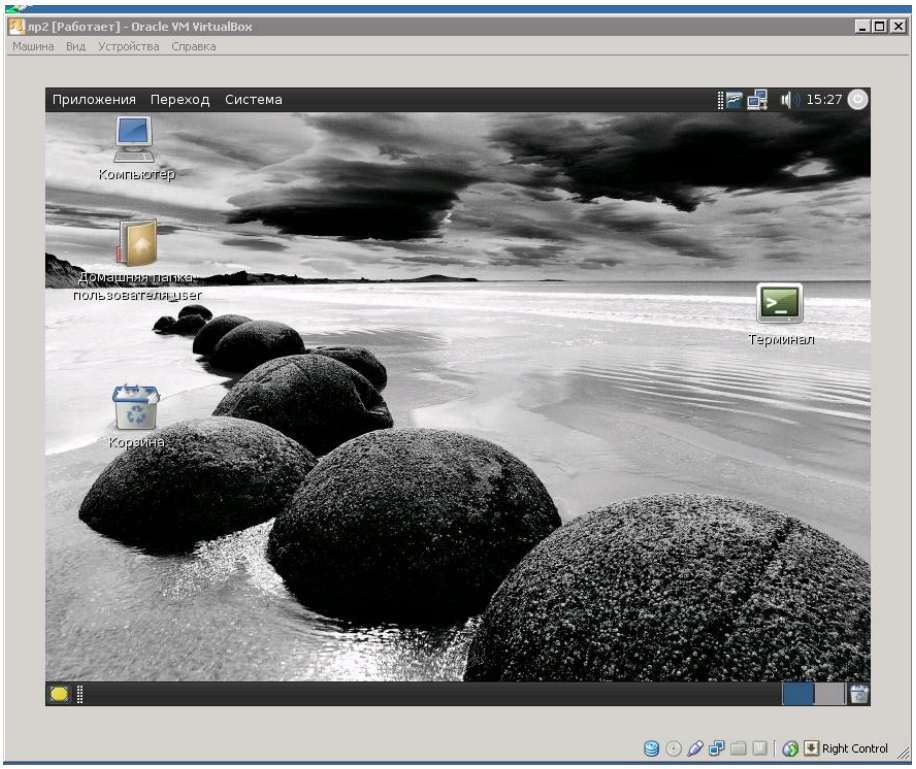


Рис. 1.21. – Рабочий стол ОС Runtu

### 1.4 Общие папки

Часто при использовании ВМ возникает задача обмена информацией с хост-платформой, например, необходимо скопировать файл. Для решения этой задачи можно использовать общие папки. Для создания общей папки необходимо в меню

**Устройства** выбрать **Общие папки** как показано на рис. 1.22, после этого станет доступно окно добавления общей папки как показано на рис. 1.23.

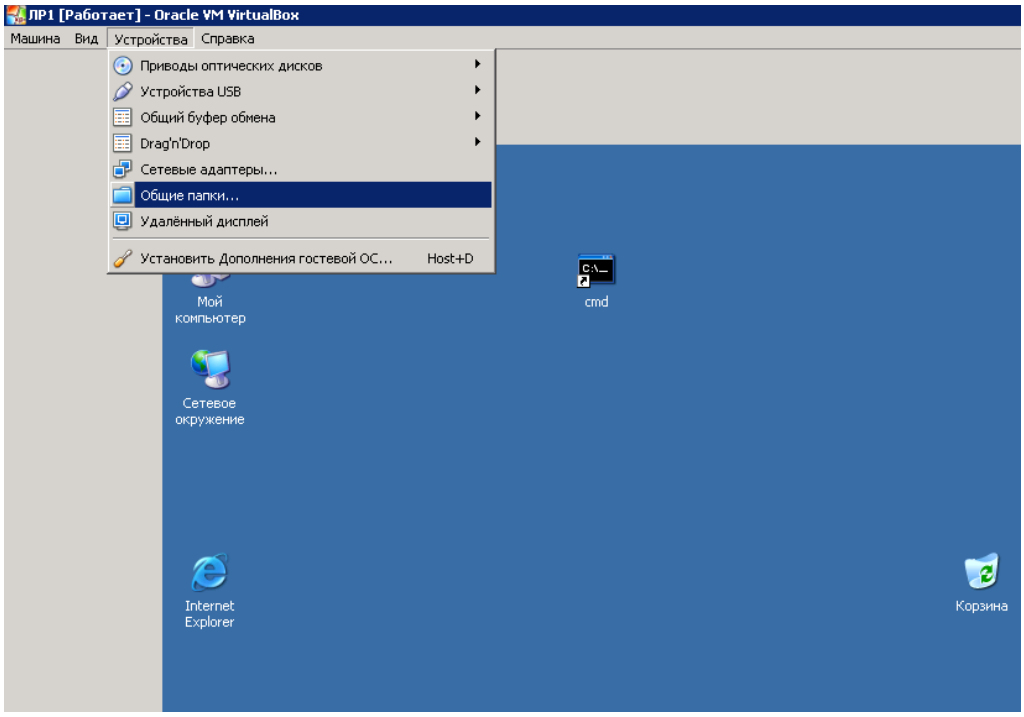


Рис. 1.22. – Общие папки

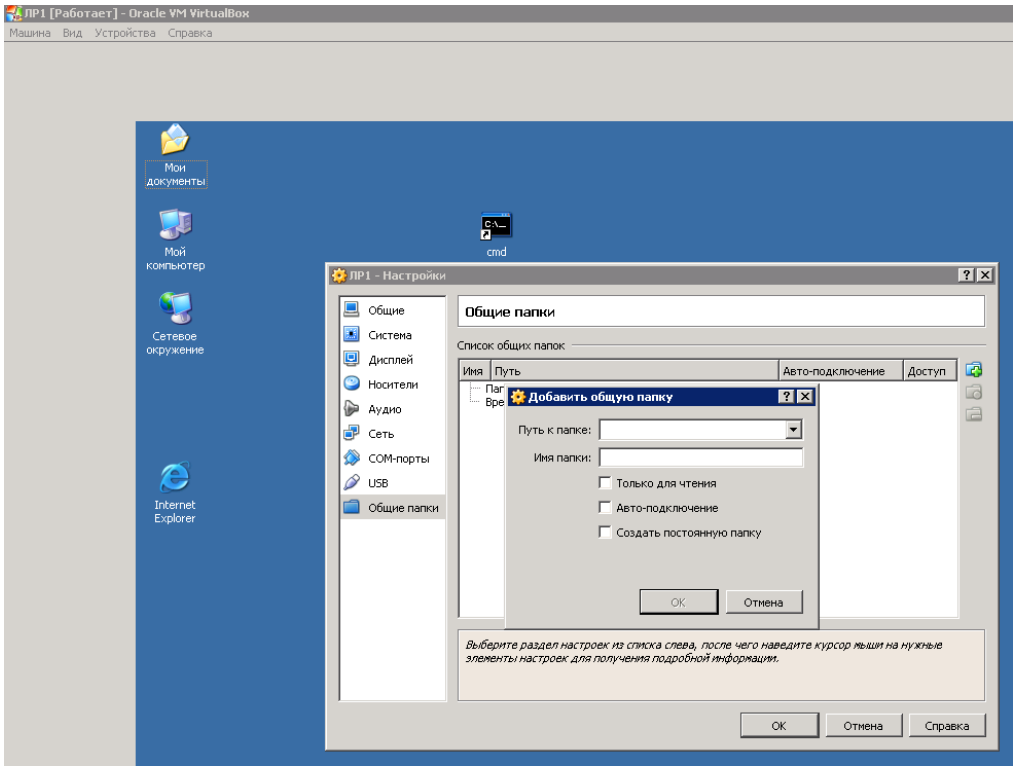


Рис. 1.23. – Добавление общей папки

Далее необходимо указать путь к общей папке на хост-платформе как показано на рис. 1.24 и выбрать общую папку (рис. 1.25).

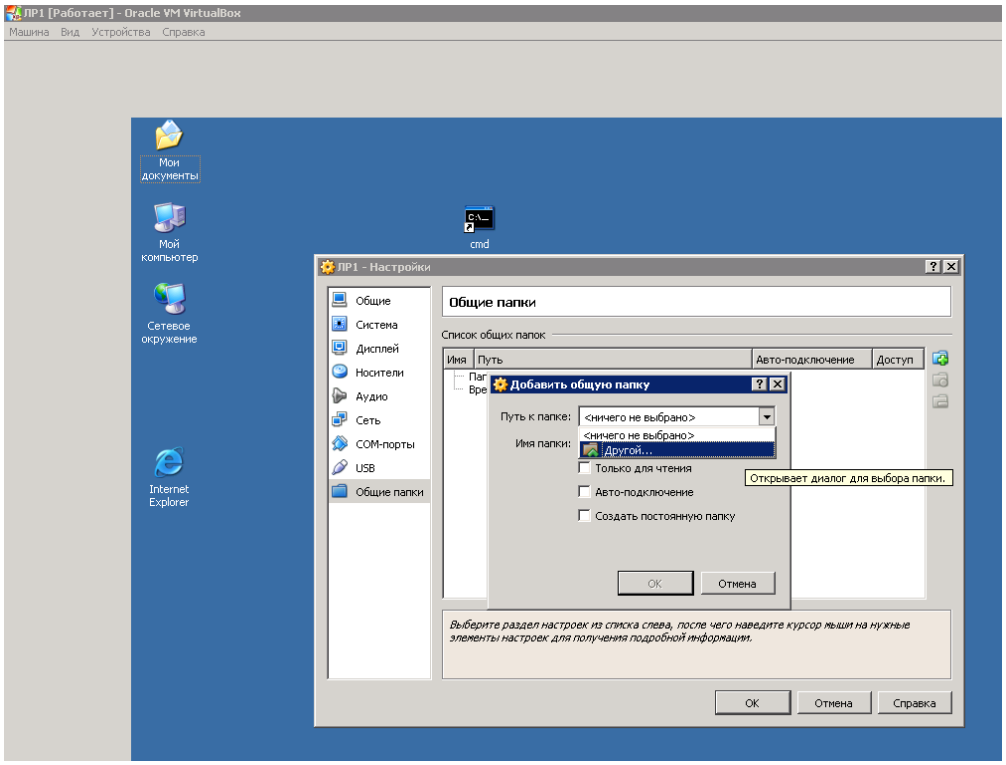


Рис. 1.24. – Путь к общей папке

При необходимости можно создать новую папку.

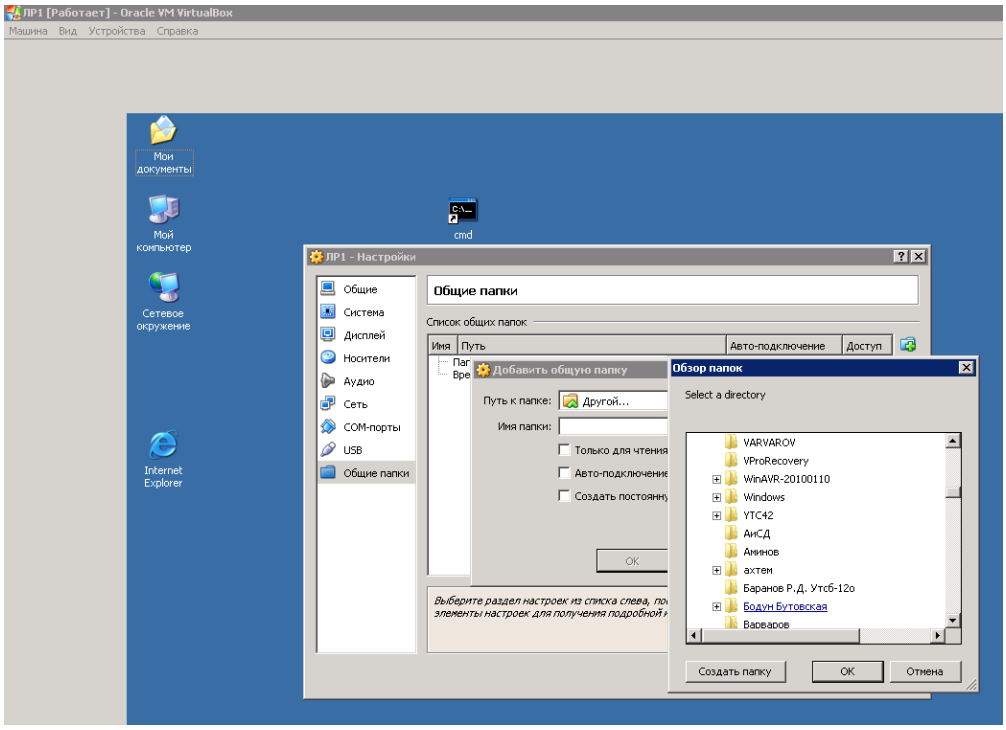


Рис. 1.25. – Выбор общей папки

Программа предложит имя для общей папки при необходимости можно изменить его, а также ее параметры (рис. 1.26).

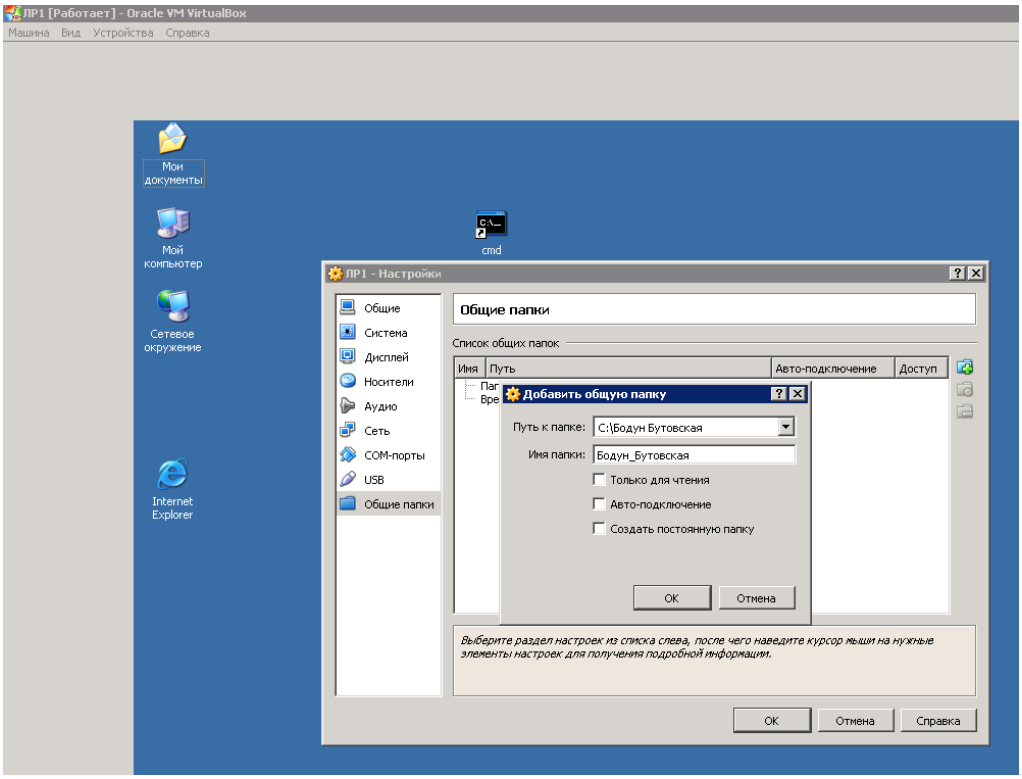


Рис. 1.26. – Имя общей папки

После создания общей папки она станет доступна в ВМ как сетевой ресурс. Можно подключить к нему сетевой диск, как показано на рис. 1.27 и рис. 1.28.

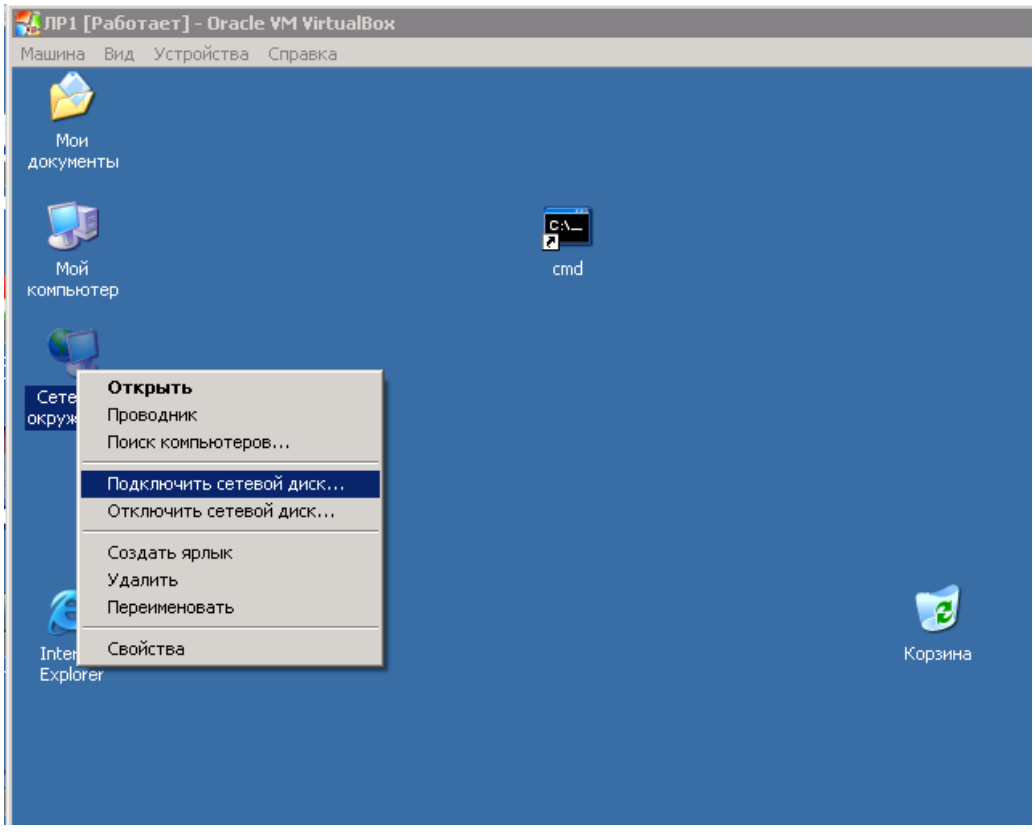


Рис. 1.27. – Подключение сетевого диска

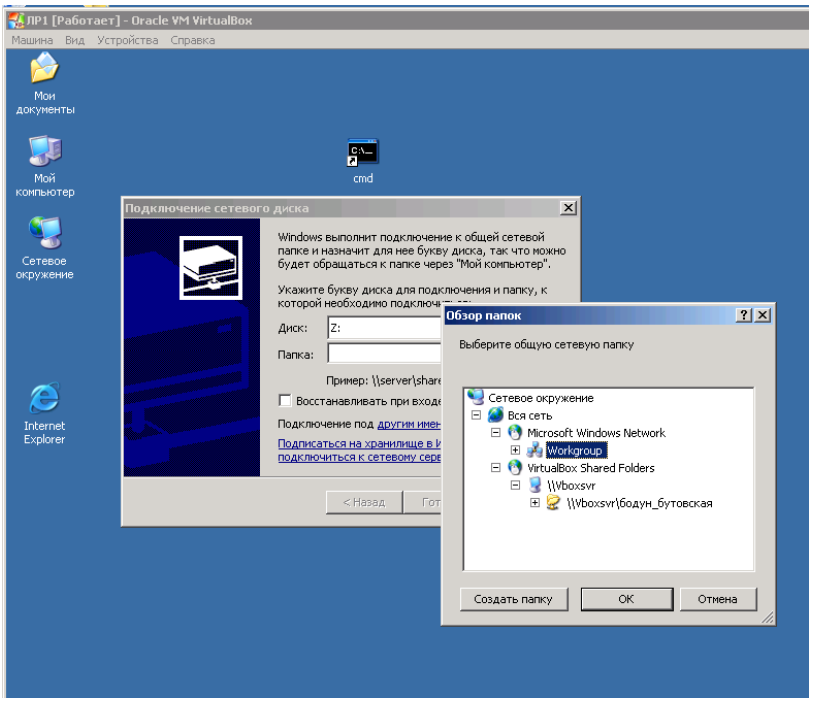


Рис. 1.28. – Выбор общей сетевой папки

Если на ВМ используется ОС Linux, то подключение общей папки делается иначе. Рассмотрим подключение общей папки на примере ОС Runtu. Этапы выбора общей папки показаны на рис. 1.22 – 1.26 и не зависят от типа ОС. Далее необходимо на рабочем столе ОС Runtu (рис. 1.21) выполнить программу **Терминал** и зарегистрироваться в ОС с правами суперпользователя при помощи команды **su**, для чего необходимо ввести пароль суперпользователя (**user**).

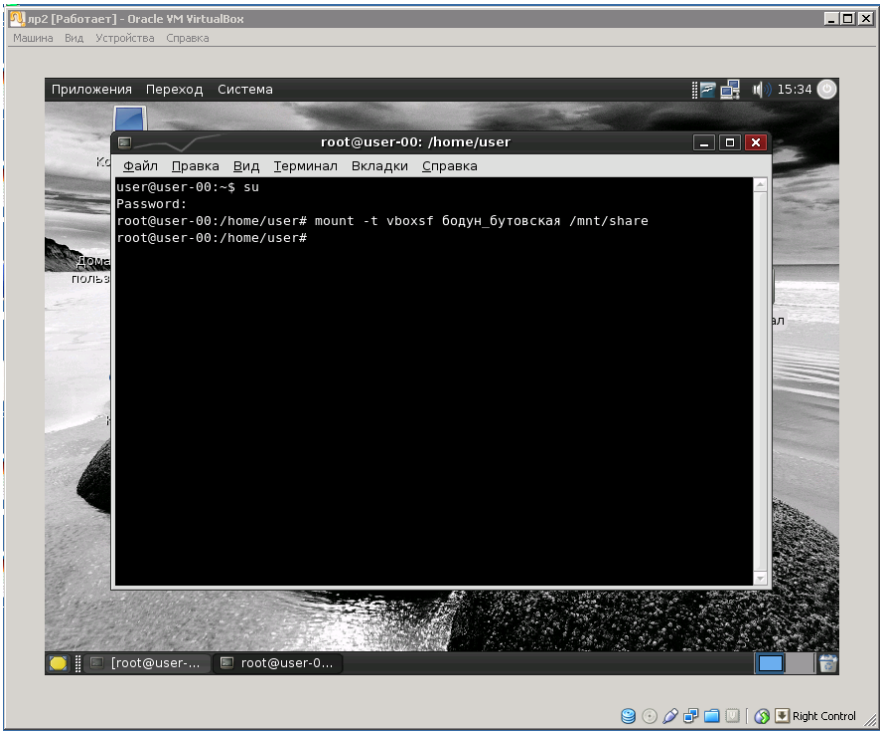


Рис. 1.29. – Монтирование общей папки

После этого можно смонтировать при помощи команды **mount –t vboxsf** общую папку на заданную папку ОС Runtu как показано на рис. 1.29.

Используя обозреватель файлов (значок **Компьютер** на рабочем столе) можно получить доступ к общим папкам через файловую систему (рис. 1.30)

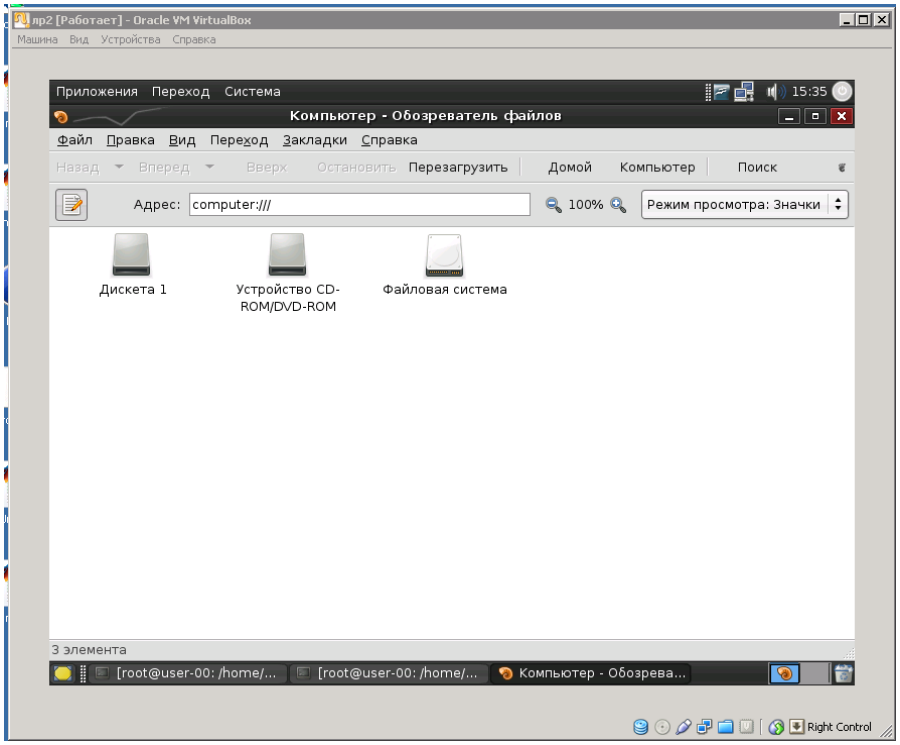


Рис. 1.30. – Обозреватель файлов

На рис. 1.31 представлен вид корневого каталога файловой системы, а на рис. 1.32 содержимое папки **mnt**. В **share** будет находится информация общей папки.

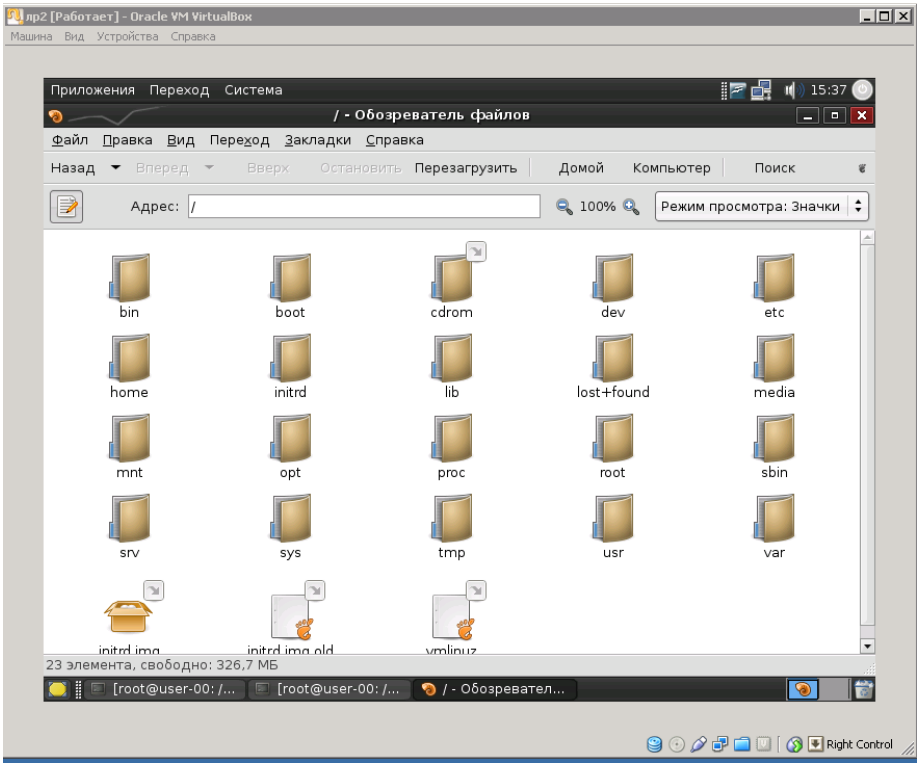


Рис. 1.31. – Корневой каталог

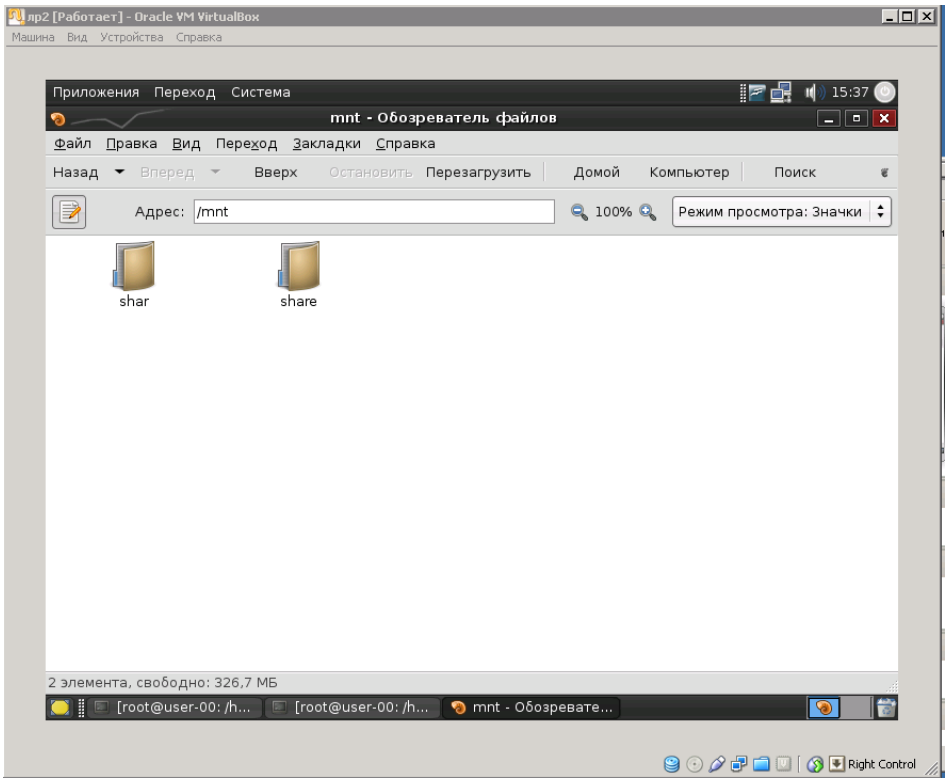


Рис. 1.32. – Содержимое папки **mnt**

### 1.5 Технические средства для выполнения работы.

Компьютерный класс с установленной **ОС Windows** и **Oracle VM VirtualBox**.

### 1.6. Порядок выполнения лабораторной работы

1. Запустить Oracle VM VirtualBox Менеджер.
2. Выбрать “создать”
3. Придумать имя для ВМ (имя должно содержать вашу фамилию и группу)
4. Создать ВМ типа Windows XP (RAM -128 MB, файл образа – d:/xp.vdi, у виртуального носителя должен быть атрибут “множественное подключение”)
5. Создать на хост-платформе на диске c: папку, имя которой должно содержать вашу фамилию и группу.
6. Сделать папку общей для ВМ
7. Создать при помощи блокнота на ВМ текстовый файл с произвольной информацией в общей папке.
8. Открыть созданный файл на хост-платформе.
9. Создать ВМ с ОС Runtu 1.1. (RAM -640 MB, файл образа – d:/Runtu1.1.vdi, у виртуального носителя должен быть атрибут “множественное подключение”)
10. Сделать сделать общую папку для ВМ с ОС Runtu 1.1. (имя пользователя “user”, пароль “user”, пароль суперпользователя “user”)
11. Создать при помощи блокнота на хост-платформе текстовый файл с произвольной информацией в общей папке.
12. Открыть созданный файл на ВМ.

13. Открыть на рабочем столе папку **Домашняя папка пользователя user** и скопировать в буфер содержимое любого текстового документа из этой папки.
14. Перенести содержимое буфера обмена в текстовый файл уже имеющийся в общей папке.

### 1.7. Содержание отчета о выполнении лабораторной работы

Отчёт должен содержать:
- титульный лист;
- цель исследования;
- ход работы;
- выводы.

Отчёт по лабораторной работе должен быть выполнен в соответствии требованиями ГОСТ.

### 1.8. Порядок защиты работы

Защита производится при наличии отчета за компьютером и состоит в демонстрации навыков использования возможностей Oracle VM VirtualBox при выполнении задания выданного преподавателем.

### 1.9. Контрольные вопросы

1. Что такое виртуализация?
2. Каковы основные возможности Oracle VM VirtualBox?
3. Каковы основные этапы создания виртуальной машины?
4. Как создать общую папку?
5. Как подключить общую папку на ВМ с ОС Windows?
6. Как подключить общую папку на ВМ с ОС Linux?
7. Как скопировать файл из ВМ в хост-платформу?

# 2. ЛАБОРАТОРНАЯ РАБОТА № 2 УСТАНОВКА ОС LINUX НА ВИРТУАЛЬНУЮ МАШИНУ

**Цель работы -** знакомство с основными этапами установки ОС LINUX на Oracle VM VirtualBox.

## 2.1 ОС LINUX

Linux — общее название Unix-подобных операционных систем на основе одноимённого ядра и собранных для него библиотек и системных программ, разработанных в рамках проекта GNU[4].

В отличие от большинства других операционных систем, Linux не имеет единой комплектации. Linux поставляется в большом количестве так называемых дистрибутивов, в которых ядро соединяется с утилитами GNU и другими прикладными программами, делающими её полноценной многофункциональной операционной средой.

Все дистрибутивы пакетные и образованы путем компиляции наборов, включающих ядро, средства загрузки, системные и пользовательские утилиты и прикладное ПО. В то же время, все более активно развиваются дистрибутивы, основанные на сборке из исходных текстов и предусматривающие установку из скомпилированных пакетов только базовых компонентов системы. Все пользовательские приложения собираются непосредственно из авторских исходных кодов.

Runtu — российский дистрибутив Linux[4], базирующийся на пакетной базе дистрибутива Ubuntu[6]. Идея Runtu — простота и доступность Ubuntu, соединённая с русской локализацией и набором предустановленного ПО, готового к использованию сразу после установки. Проект был основан 14 мая 2007 года Алексеем Черноморченко и Александром Бехером, тогда же и вышла первая версия дистрибутива. Первоначальное название дистрибутива — «Ubuntu Full Power». Проект быстро получил популярность среди преподавателей школ. В июне 2007 года дистрибутив и проект были переименованы в соответствии с новыми правилами использования торговой марки Ubuntu[6] на имя «Runtu».

Главное отличие Runtu от Ubuntu состоит в предустановленных пакетах поддержки русского языка, оформлении пользовательского окружения и оптимизации требуемых для работы ресурсов. Runtu содержит оригинальное оформление, которому разработчики придают роль фирменного стиля. На установочном компакт-диске содержатся программы, за которые проголосовали пользователи на форуме разработчиков[5].

## 2.2 Подготовка к установке ОС на Oracle VM VirtualBox

Oracle VM VirtualBox представляет собой систему виртуализации для систем Windows, Linux и Mac OS и обеспечивает взаимодействие с различными гостевыми операционными системами.

VirtualBox поддерживает широкий набор современных аппаратных средств.

Программа устанавливается и запускается как обычная программа для Windows. Её можно загрузить с сайта разработчика[3].

## 2.3 Создание виртуальной машины для ОС Linux

Для создания ВМ необходимо запустить программу Oracle VM VirtualBox. На рабочем столе откроется окно программы вид которого показан на рис. 2.1.

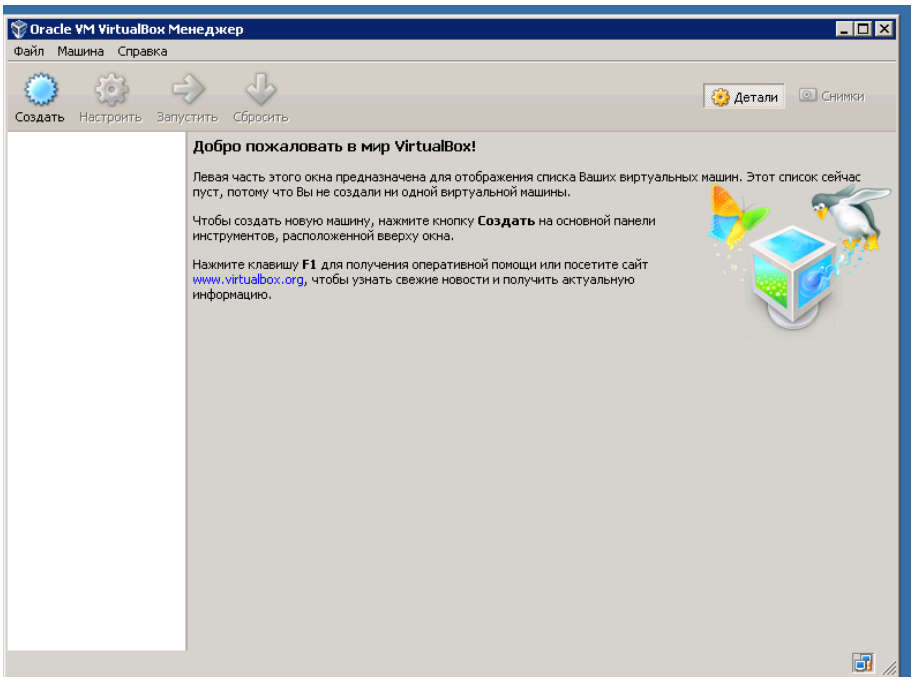


Рис. 2.1. – Программа  Oracle VM VirtualBox

Для создания новой ВМ необходимо придумать ее имя, выбрать тип и версию операционной системы. Так как будет использоваться дистрибутив Runtu, отсутствующий в перечне типов и версий,  вводится тип **Other** как показано на рис. 2.2

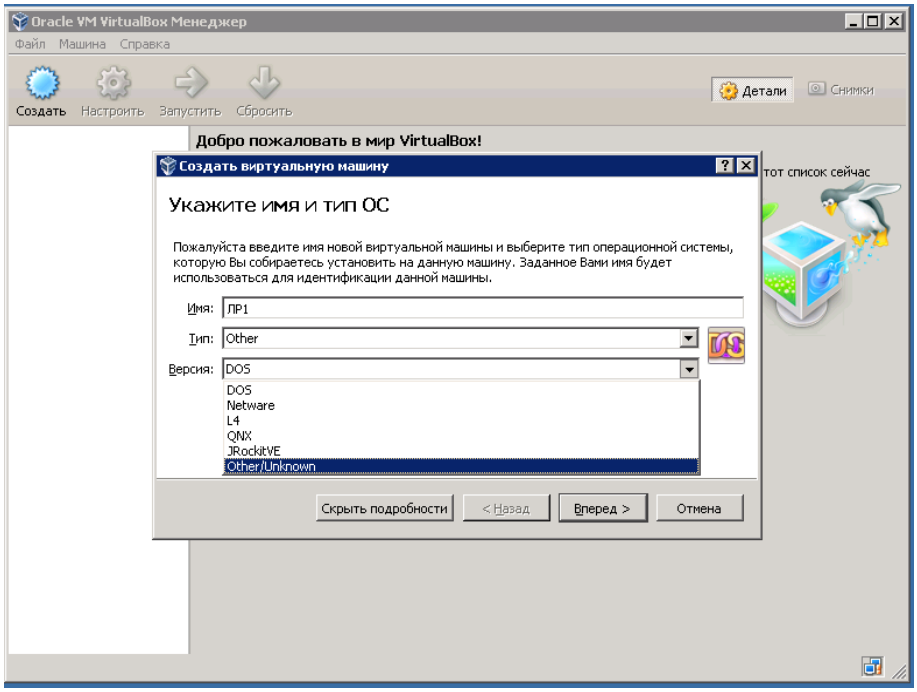


Рис. 2.2. – Установка  типа ОС

Далее необходимо указать объем оперативной памяти, которая будет выделена ВМ, как показано на рис 2.3. Величина памяти зависит от типа ОС и используемых приложений (для ОС Runtu достаточно 640 МБ)

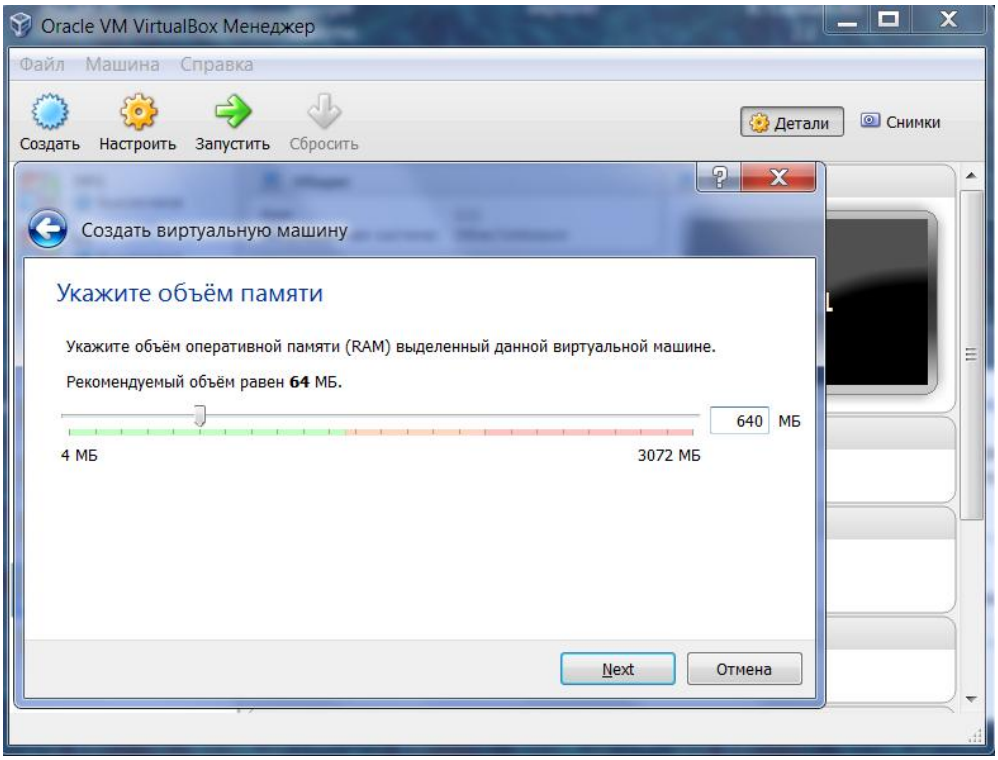


Рис. 2.3. – Указание объема памяти ВМ

На следующем этапе производится выбор и настройка виртуального жесткого диска ВМ как показано на рис. 2.4.

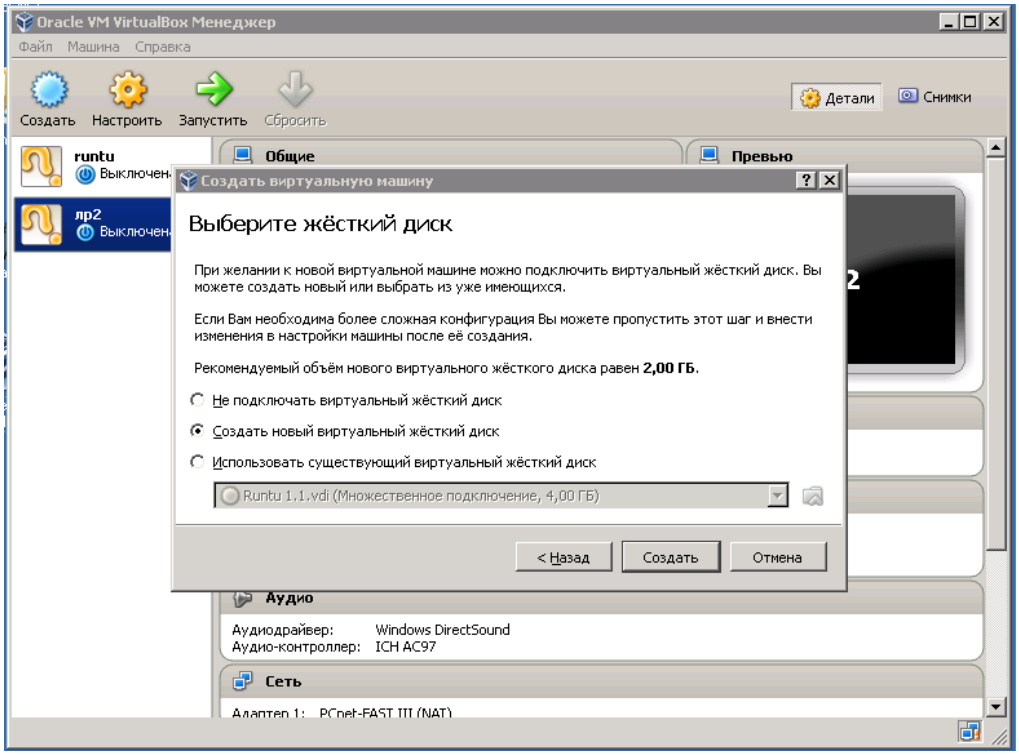


Рис. 2.4. – Выбор виртуального жесткого диска

Выбираем тип VDI как показано на рис. 2.5.

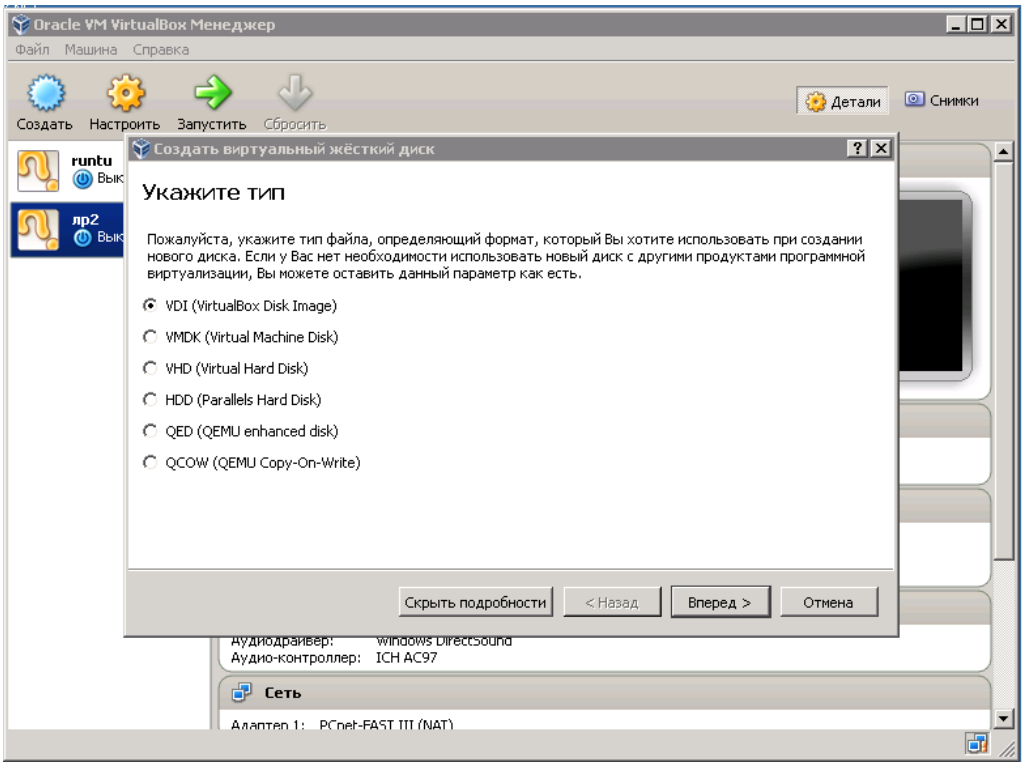


Рис. 2.5. – Выбор типа виртуального жесткого диска

После выбора типа виртуального жесткого диска необходимо указать формат хранения данных. Для уменьшения занимаемого места на дисках хост-машины выбираем динамический виртуальный жесткий диск (рис. 2.6).

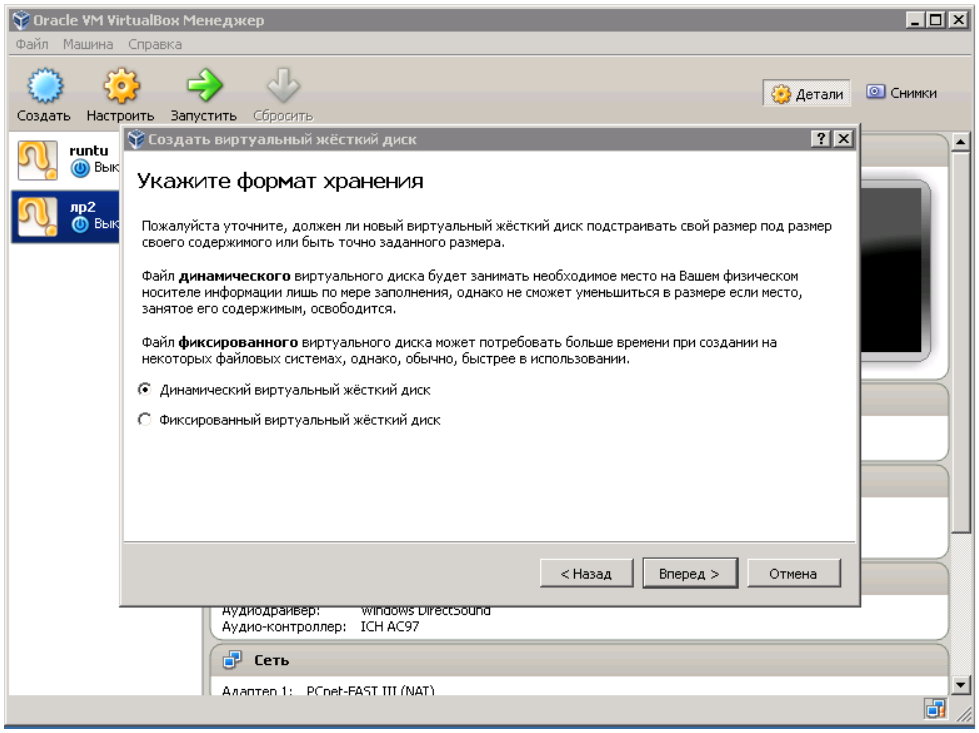


Рис. 2.6. – Выбор формата хранения

Далее необходимо указать имя файла для нового виртуального жесткого диска и его размер (рис. 2.7).

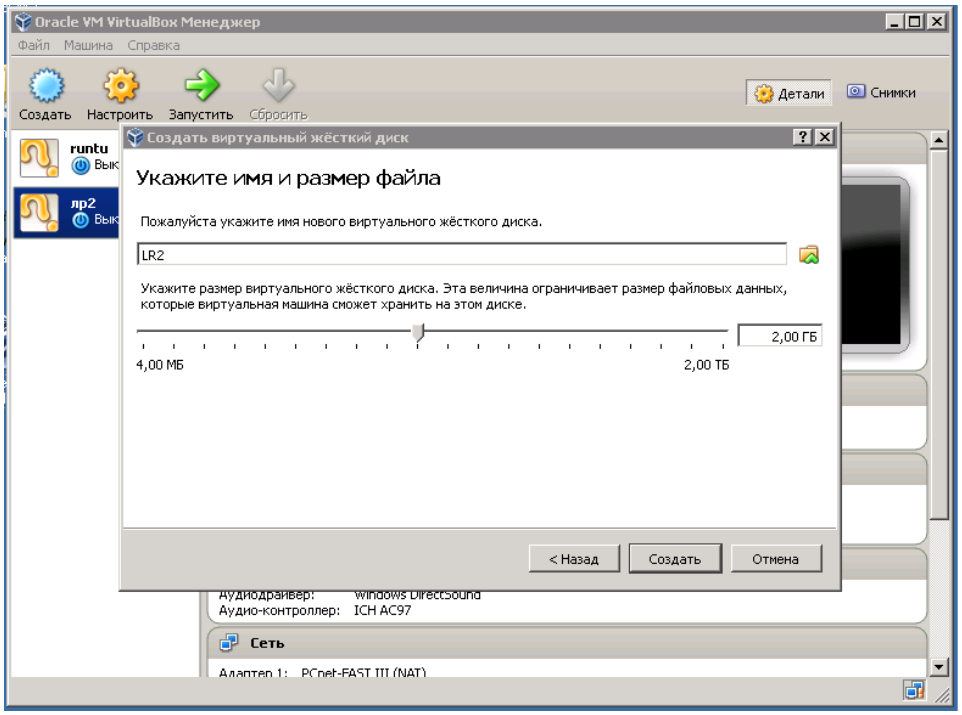


Рис. 2.7. – Имя и размер файла

Необходимо произвести настройку и запуск созданной ВМ. В меню **Настройка** выбираем **Система, Процессор** и устанавливаем параметр PAE (рис. 2.8).

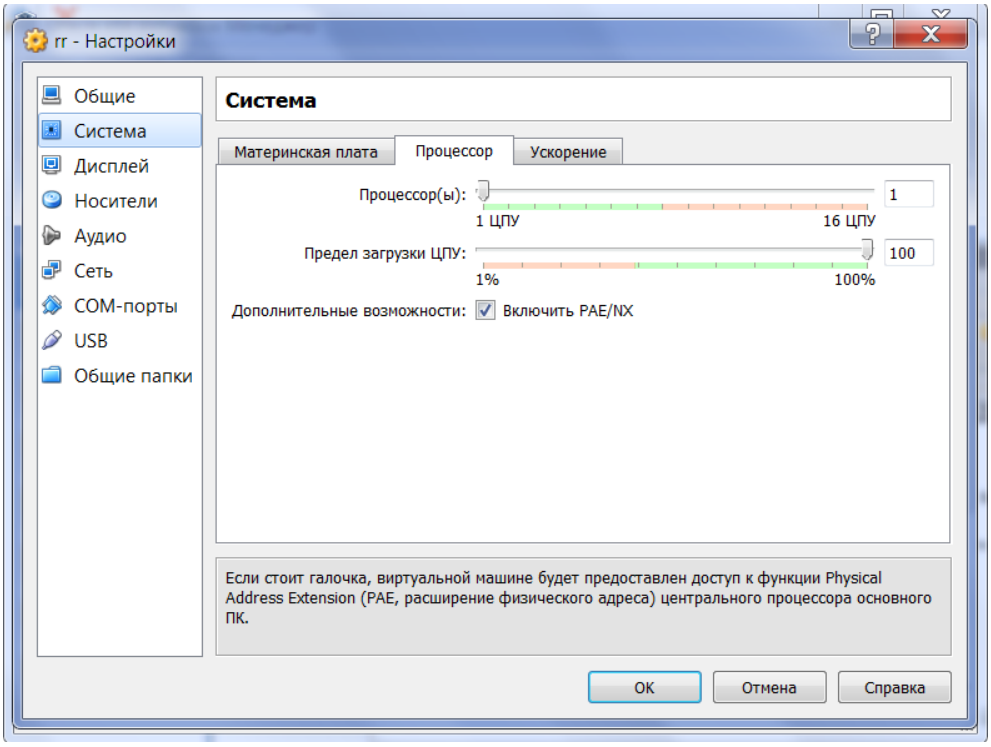


Рис. 2.8. – Установка параметров системы

## 2.4 Установка ОС Runtu

После установки параметров системы необходимо произвести запуск созданной ВМ и выбрать загрузочный диск ОС (Рис. 2.9)

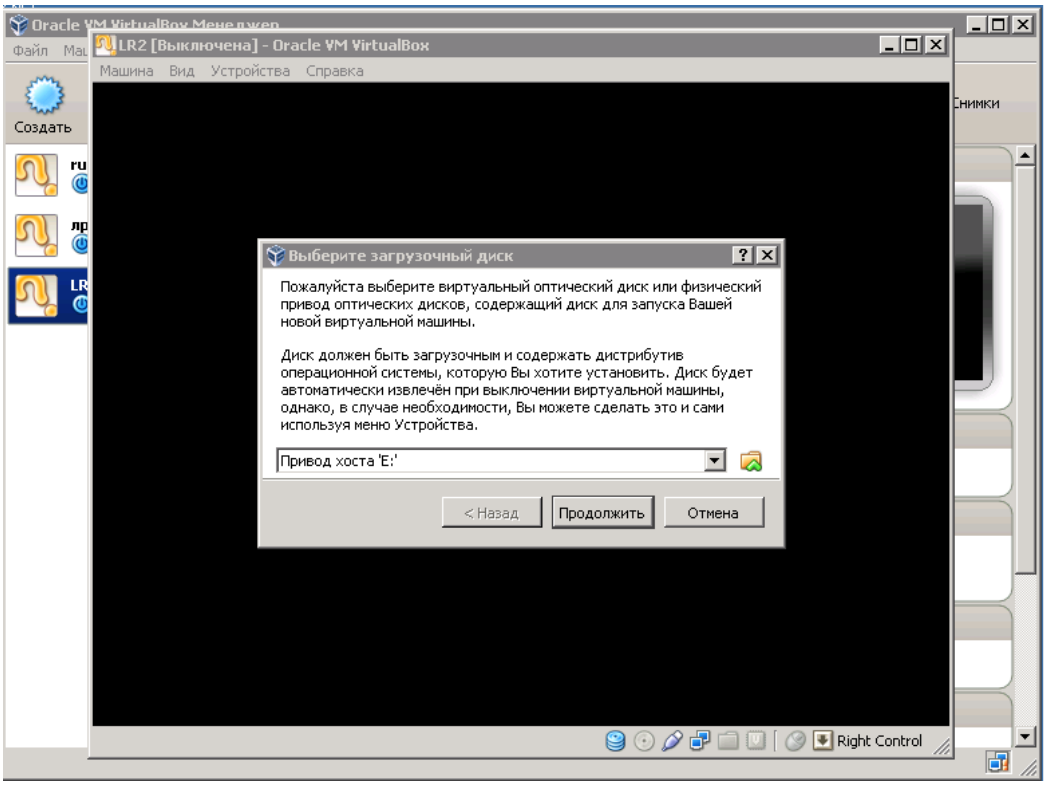


Рис. 2.9. – Носители ВМ

Далее необходимо выбрать файл виртуального оптического диска с которого будет производится установка ОС (рис. 2.10)

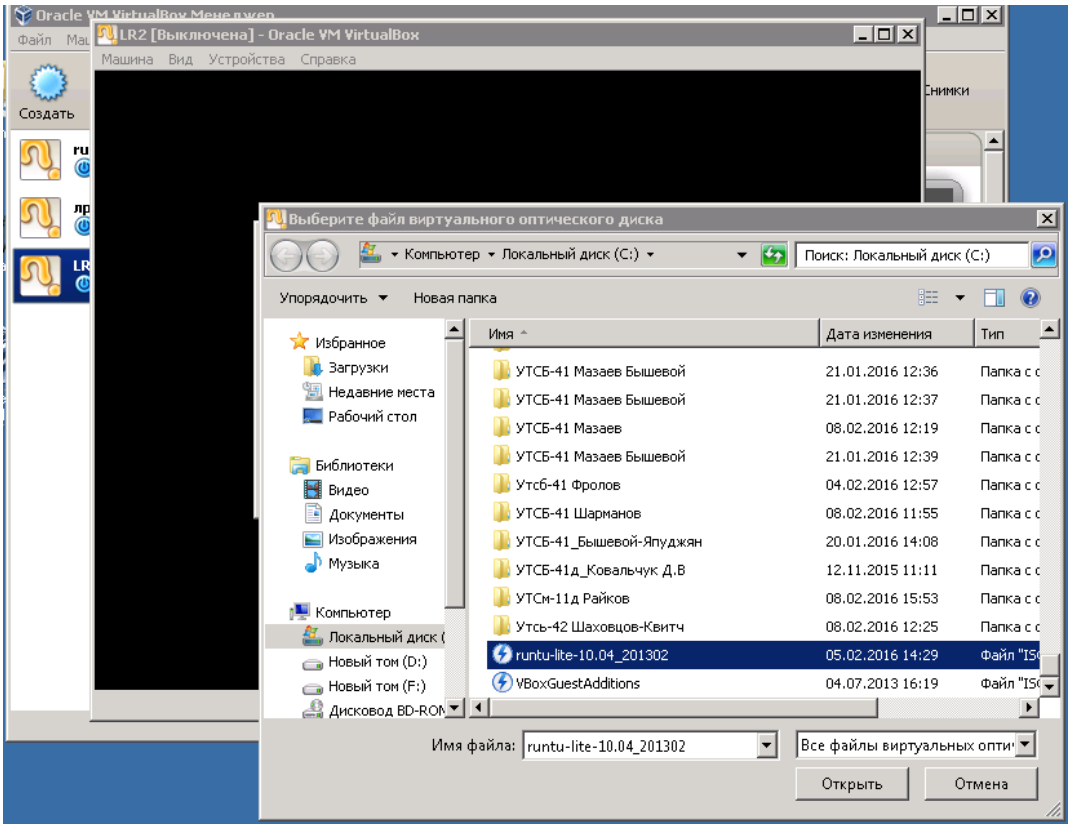


Рис. 2.10. – Выбор файла виртуального оптического диска

После начала установки ОС на экране появляется меню, показанное на рис. 2.11. Необходимо выбрать первый пункт меню.

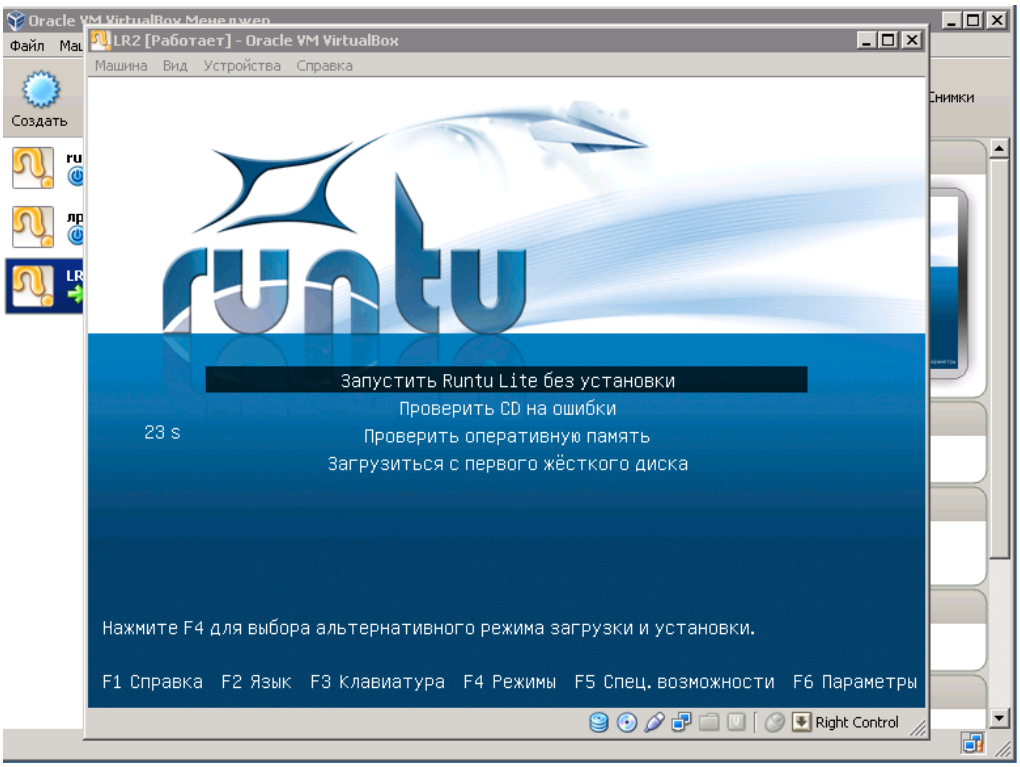


Рис. 2.11. – Меню установки ОС Runtu

Необходимо произвести запуск программы установки ОС и ввести информацию о своем местоположении (рис. 2.12).

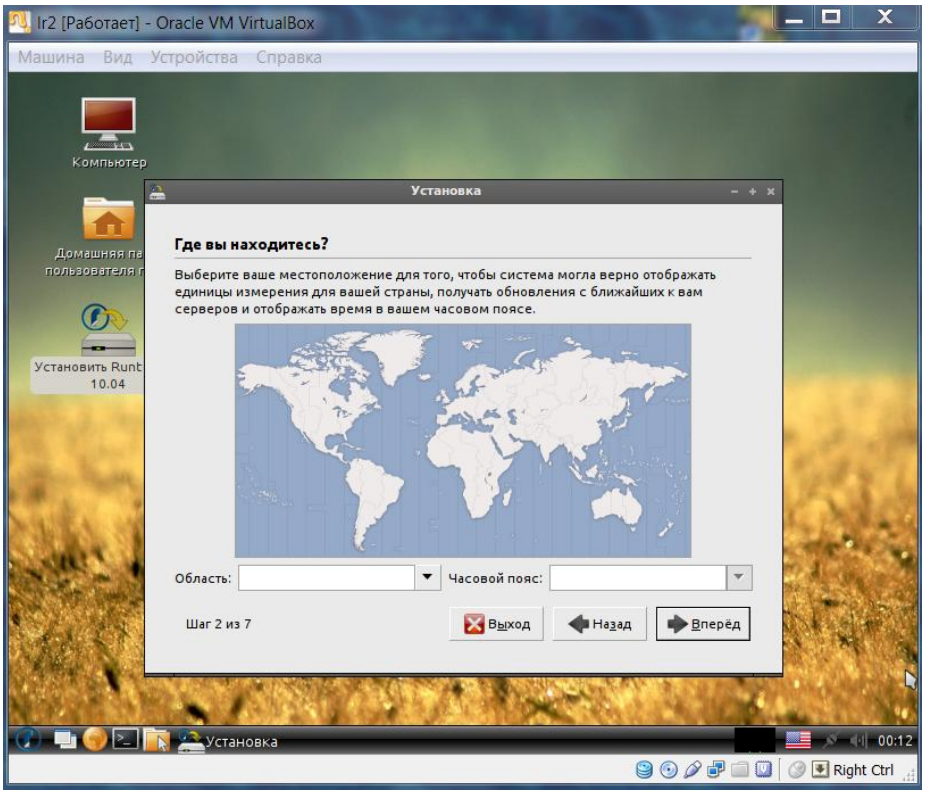


Рис. 2.12. – Информация о местоположении

На следующем этапе необходимо установить нужную раскладку клавиатуры. Для проверки выбранной раскладки можно напечатать что-нибудь в специальном поле (рис. 2.13).

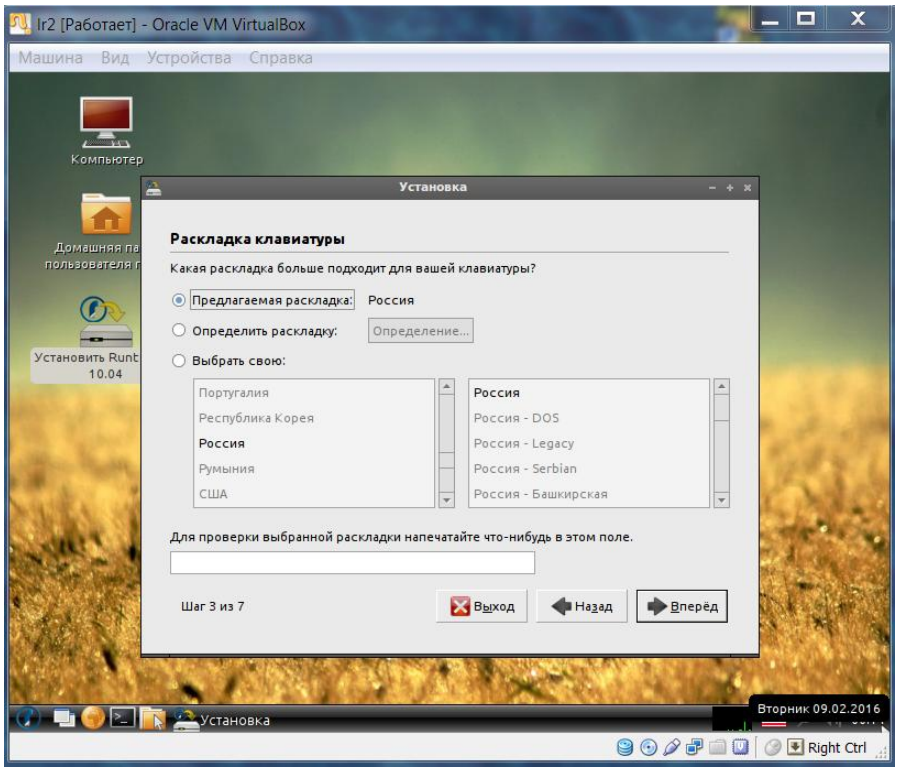


Рис. 2.13. – Выбор раскладки клавиатуры

На следующем шаге программа установки ОС производит подготовку дискового пространства, выведет информацию об установленных на ВМ операционных системах и разделах виртуального жесткого диска.

При необходимости можно указать вручную разделы и их параметры. Следует учитывать, что общий размер разделов не может превышать размер файла виртуального жесткого диска (рис. 2.14)

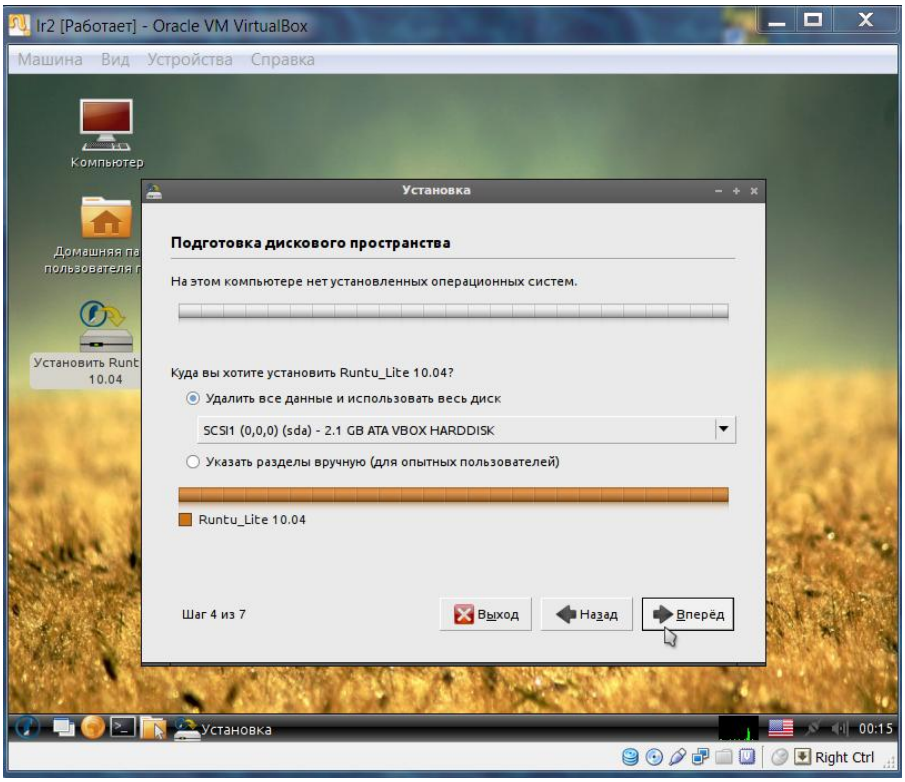


Рис. 2.14. – Подготовка дискового пространства

Далее необходимо выбрать имя пользователя для входа в систему, пароль для учетной записи и название компьютера, которое будет использовано в сети (рис. 2.15).

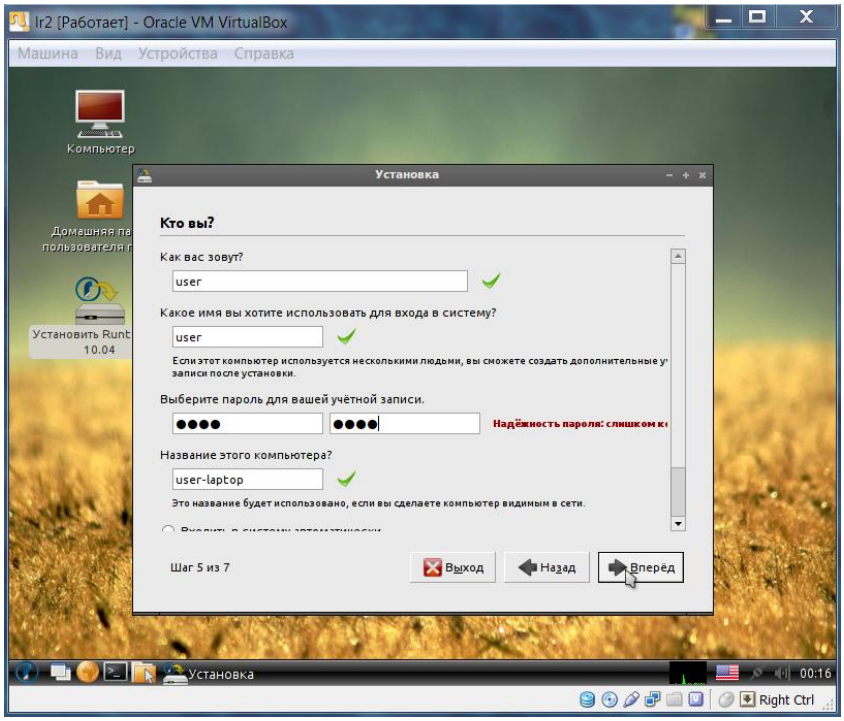


Рис. 2.15. – Имя пользователя пароль и название компьютера

На следующем этапе программа выведет информацию на экран о параметрах установки. Можно начать установку или произвести изменение параметров (рис. 2.16).

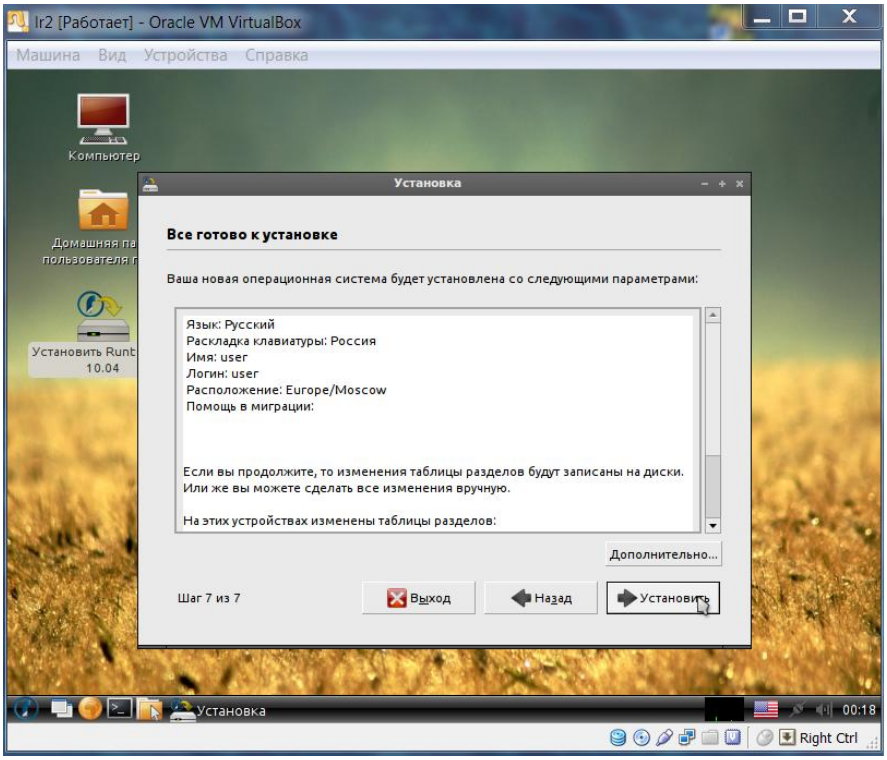


Рис. 2.16. – Информация о параметрах установки

После начала установки программа скопирует на диск необходимые для ОС файлы. Это обычно занимает несколько минут (рис. 2.17).

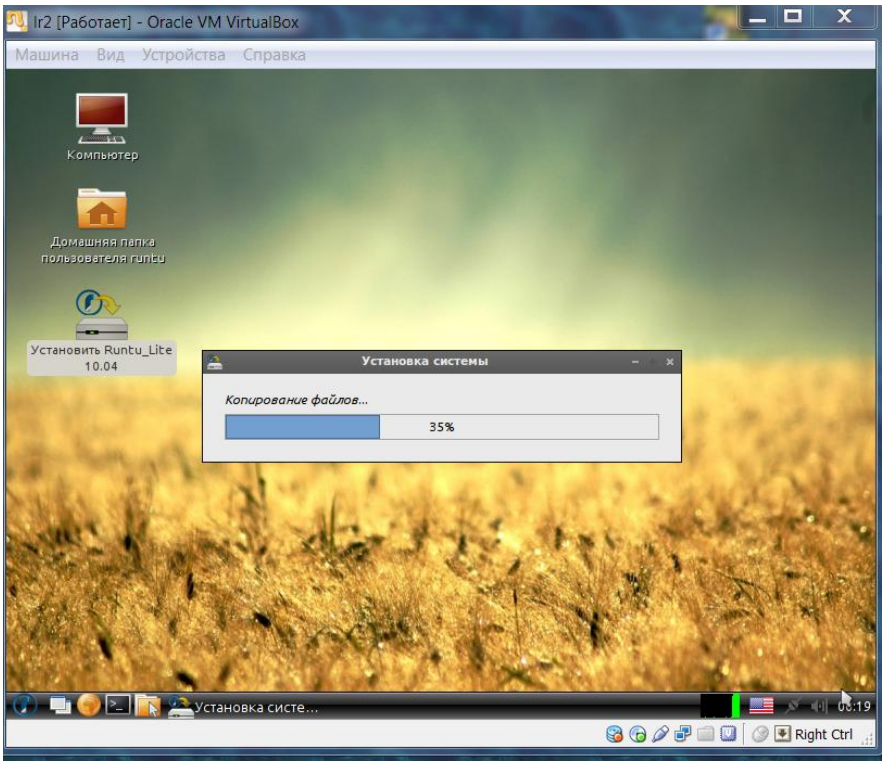


Рис. 2.17. – Копирование файлов

По окончании копирования файлов необходимо произвести перезагрузку ВМ, чтобы новые настройки ОС начали действовать (рис. 2.18).

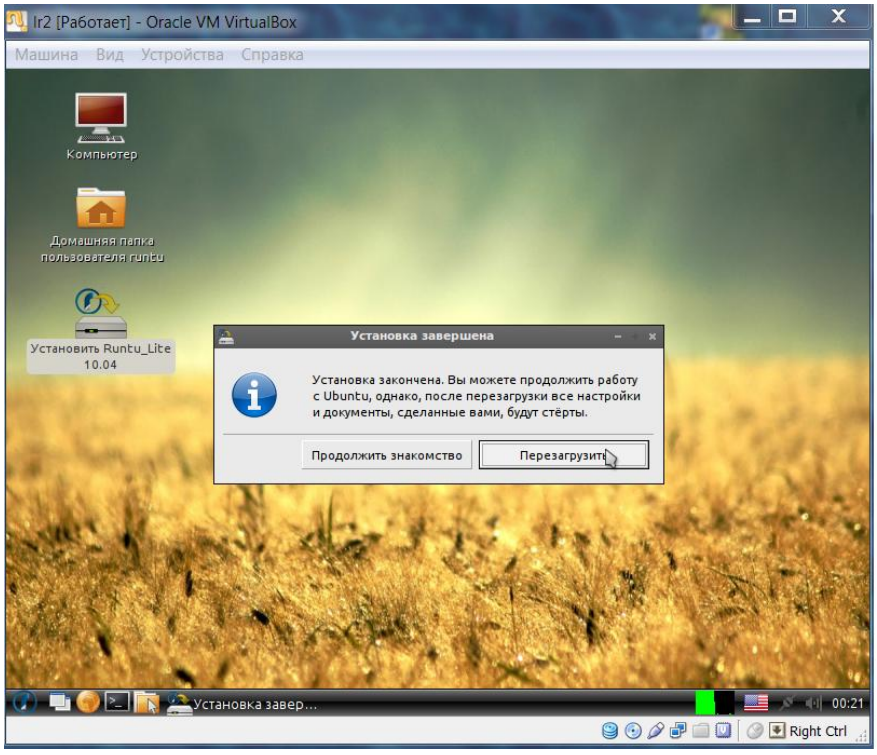


Рис. 2.18. – Завершение установки и перезагрузка ВМ

После перезагрузки ВМ система выдаст на экран приглашение для ввода имени пользователя и пароля (рис. 2.19).

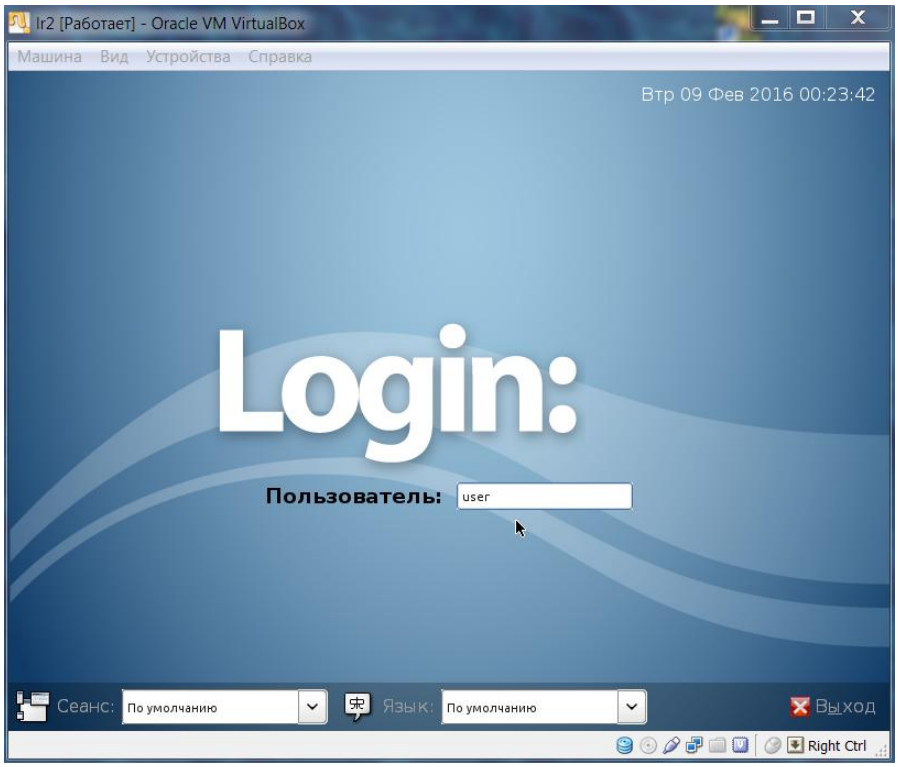


Рис. 2.19. – Вод имени пользователя

На этом установка ОС заканчивается.

### 2.5 Установка дополнений гостевой ОС

Установленная на ВМ система LINUX не позволяет использовать общие папки и общий буфер обмена с хост-системой, кроме того, отсутствует интеграция указателя мыши. Необходимо установить дополнения гостевой ОС LINUX. Выбираем в строке меню ВМ **устройства**, затем **приводы оптических дисков** и выбираем установочный образ оптического диска (рис. 2.20).

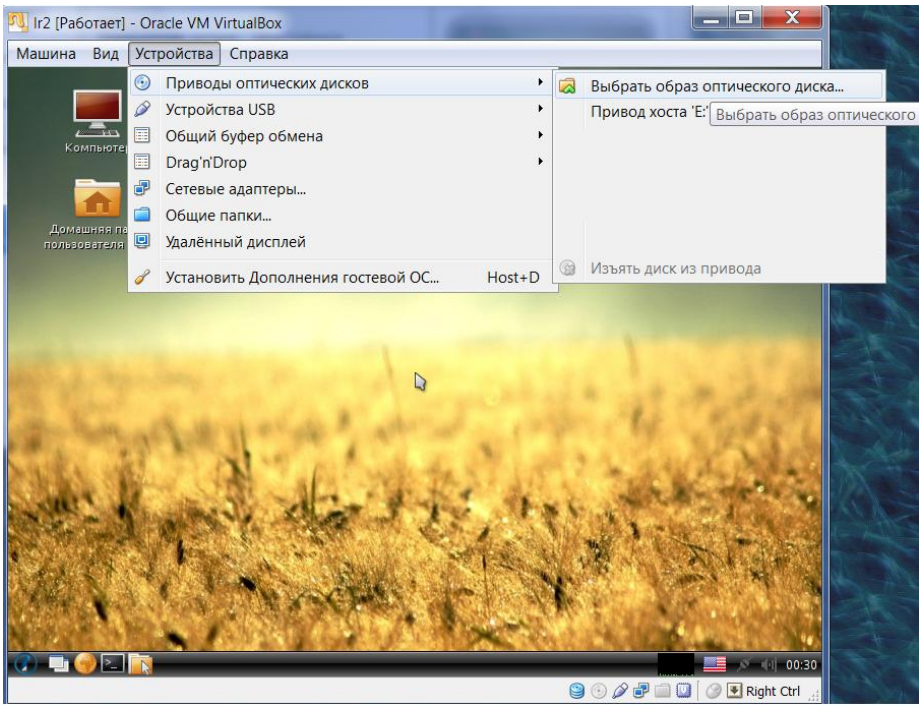


Рис. 2.20. – Выбор установочного образа оптического диска

Образ оптического диска с программой установки дополнений гостевой ОС находится на диске **C:** и имеет имя **VBoxGuestAdditions.iso**

После выбора файла образа на экране может появится окно автозапуска, показанное на рис. 2.21. Необходимо выбрать **отмену** автоматической установки.

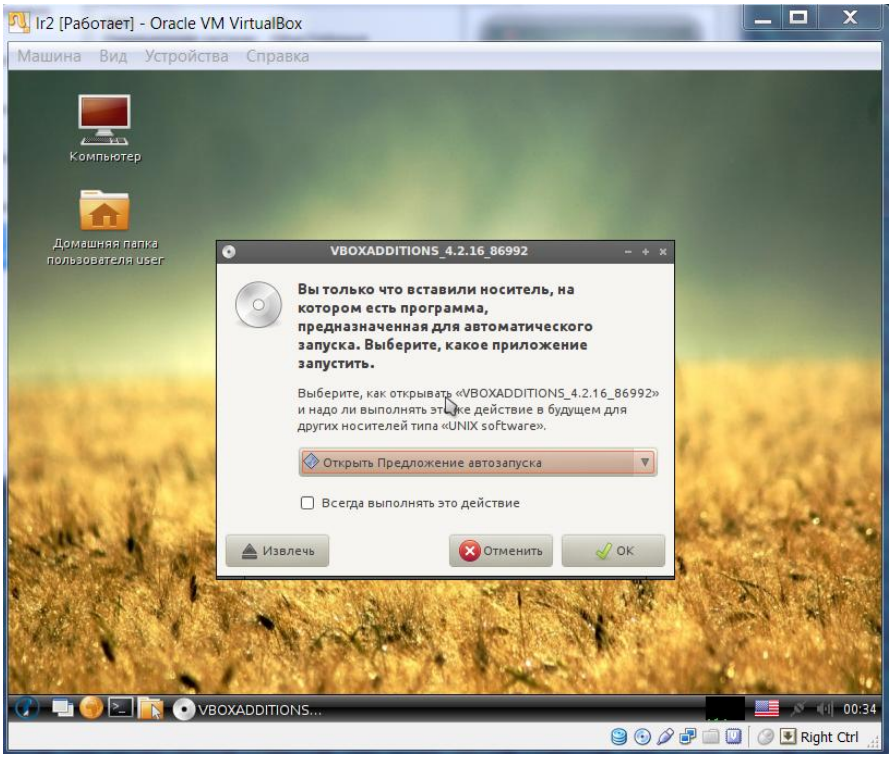


Рис. 2.21. – Окно автозапуска установки дополнений гостевой ОС

Дополнения гостевой ОС устанавливаются в режиме командной строки. Для удобства работы можно открыть на рабочем столе значок **компьютер,** затем **файловая система** и папку ***media,*** в которой находятся файлы установки дополнений гостевой ОС (рис. 2.22).

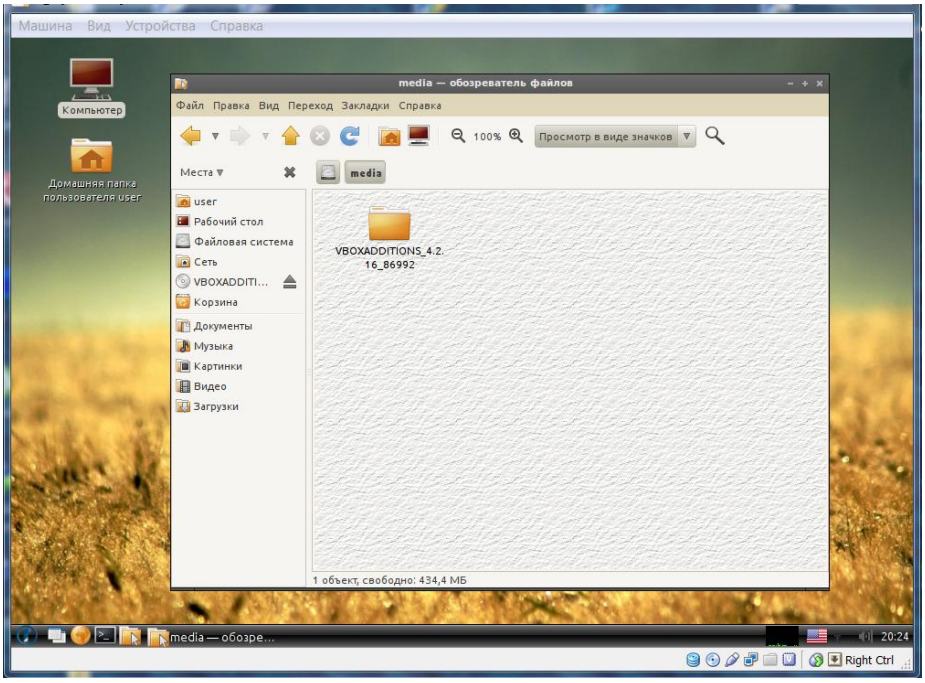


Рис. 2.22. – Файлы установки дополнений гостевой ОС

Скопируем папку с файлами установки дополнений гостевой ОС в домашнюю папку (рис. 2.23).

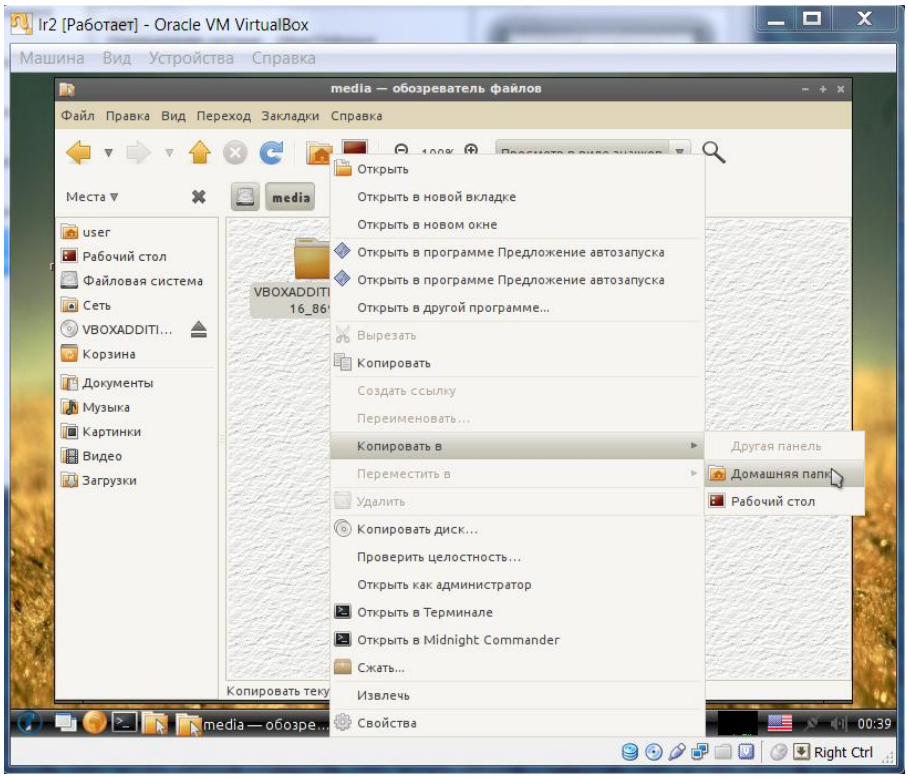


Рис. 2.23. – Копирование файлов установки дополнений гостевой ОС

Далее откроем на рабочем столе папку пользователя и переименуем в ней установочную папку дополнений гостевой ОС на более удобное имя (например **VBOXADDITIONS**) как показано на рис. 2.24.

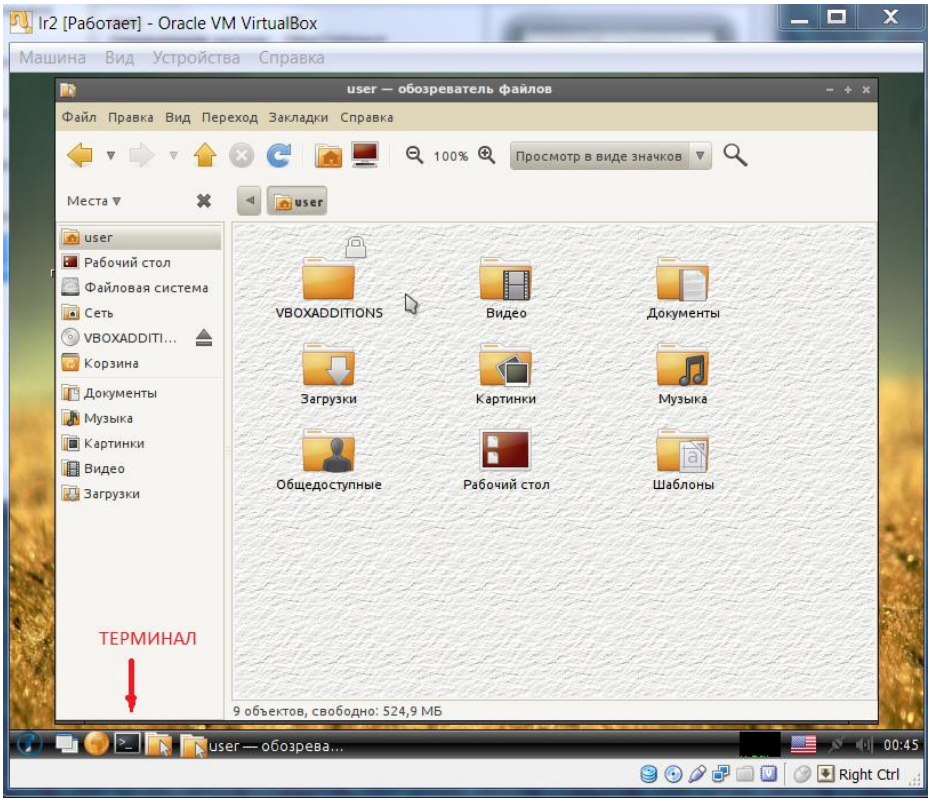


Рис. 2.24. – Переименование папки установки дополнений гостевой ОС

Следующие действия выполняются в окне терминала. В терминале, используя команду **ls** просматриваем содержимое пользовательского каталога. При помощи команды **cd** делаем текущей папку **VBOXADDITIONS** и снова просматриваем ее при помощи команды **ls** как показано на рис. 2.25.

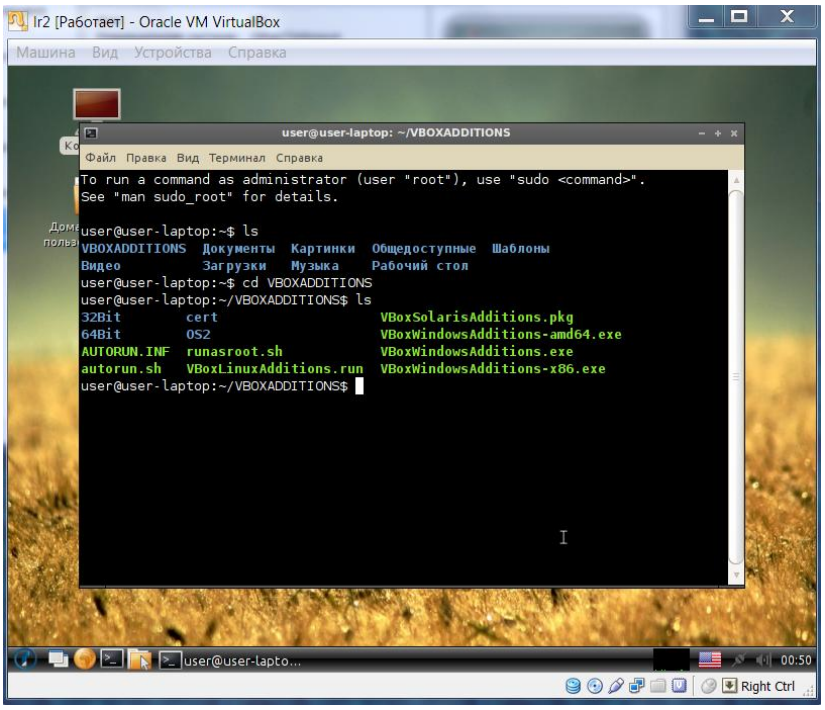


Рис. 2.25. – Содержимое папки VBOXADDITIONS

Используя команду **sudo**, которая позволяет выполнять команды от имени администратора (при этом необходимо ввести пароль), произведем запуск инсталляции дополнений гостевой ОС при помощи строки:

**sudo sh ./VBoxLinuxAdditions.run** как показано на рис. 2.26.

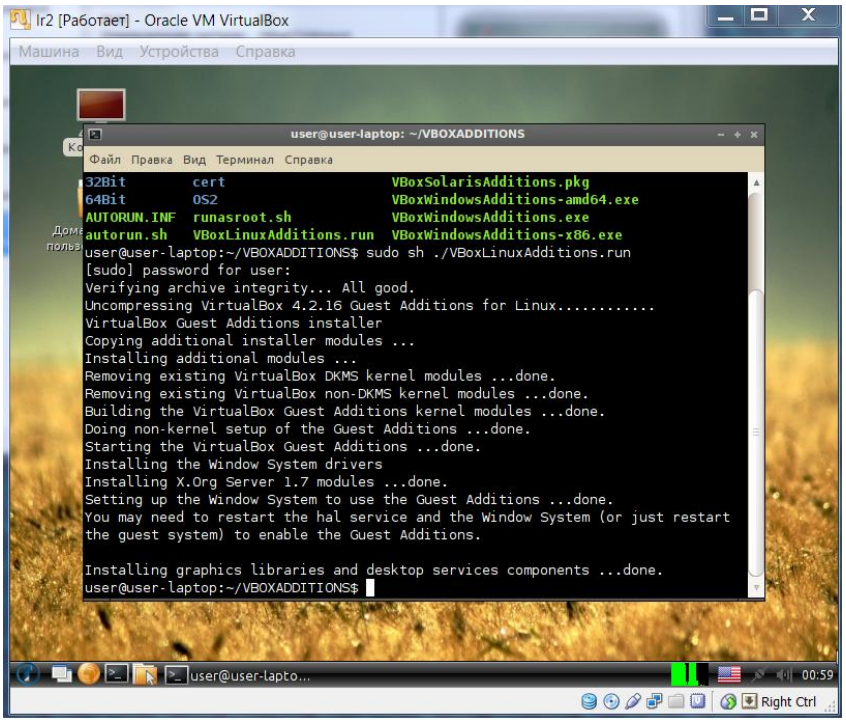


Рис. 2.26. – Запуск инсталляции дополнений гостевой ОС

После окончания работы с ОС необходимо произвести выход из системы (рис. 2.27), а затем выключение ВМ (рис. 2.28)

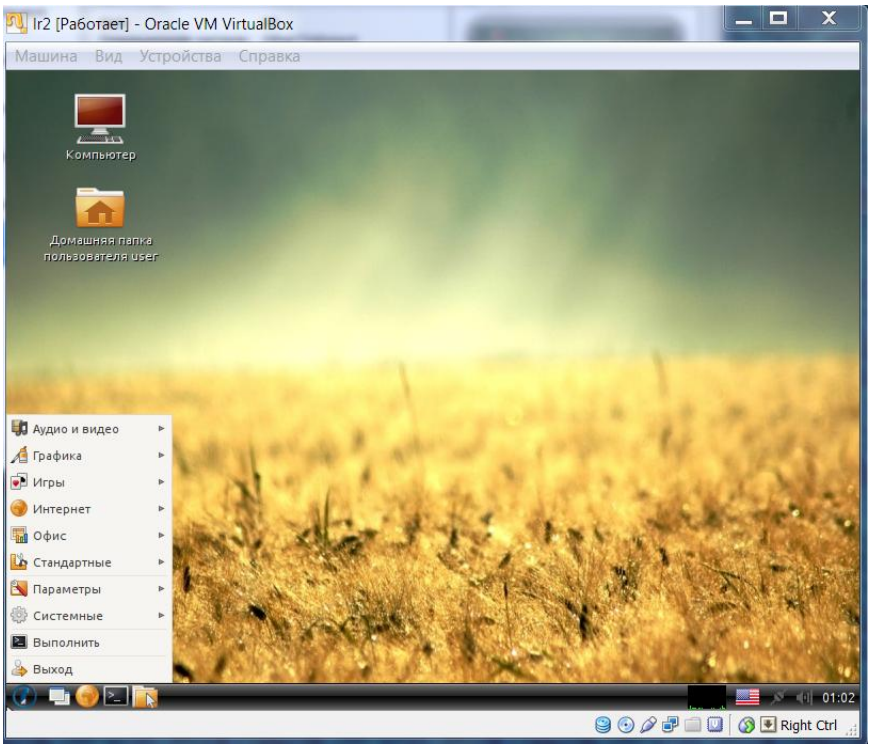


Рис. 2.27. – Выход из системы

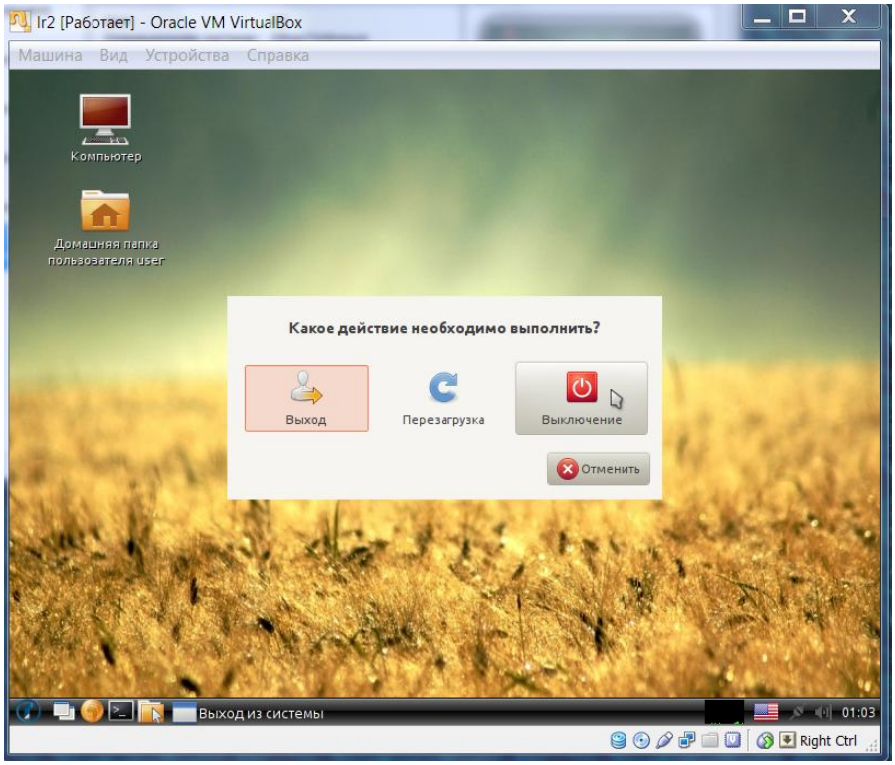


Рис. 2.28. – Выключение ВМ

## 2.7. Технические средства для выполнения работы

Для выполнения работы необходим компьютер с установленной **ОС Windows** и **Oracle VM VirtualBox**.

### 2.8 Порядок выполнения лабораторной работы

1. Запустить Oracle VM VirtualBox Менеджер.
2. Выбрать “создать”.
3. Придумать имя для ВМ (имя должно содержать вашу фамилию и группу)
4. Создать ВМ с ОС Runtu (RAM -640 MB, размер нового виртуального диска – 2 GB, тип динамический)
5. Произвести на ВМ установку ОС Runtu используя образ оптического диска c:/rutu-lite-10.04_201302.iso
6. Произвести на ВМ установку дополнений гостевой ОС, в режиме командной строки, используя образ оптического диска
7. c:/ VBoxGuestAdditions.iso
8. Создать при помощи блокнота на хост-платформе текстовый файл с произвольной информацией в общей папке.
9. Открыть созданный файл на ВМ.
10. Удалить, созданную ВМ с удалением всех файлов.

### 2.9 Содержание отчета о выполнении лабораторной работы

Отчёт должен содержать:

- титульный лист;
- цель исследования;
- ход работы;
- выводы.

Отчёт по лабораторной работе должен быть выполнен в соответствии требованиями ГОСТ.

### 2.10 Порядок защиты работы

Защита производится при наличии отчета за компьютером и состоит в демонстрации навыков установки ОС Runtu и дополнений гостевой ОС, в режиме заданным преподавателем.

### 2.11 Контрольные вопросы

8. Что такое ОС LINUX?
9. Каковы основные особенности дистрибутива Runtu?
10. Каковы основные этапы создания виртуальной машины?
11. Каковы основные этапы установки ОС Runtu?
12. Для чего нужны дополнения гостевой ОС?
13. Каковы основные этапы установки дополнений гостевой ОС?
14. Как подключить общую папку на ВМ с ОС Linux?

# 3. ЛАБОРАТОРНАЯ РАБОТА № 3 СОЗДАНИЕ И АДМИНИСТРИРОВАНИЕ СЕТИ ВИРТУАЛЬНЫХ МАШИН

Цель работы - знакомство с основными возможностями ПО Oracle VM VirtualBox для создания сетей виртуальных машин.

## 3.1 Настройка сетевых интерфейсов виртуальных машин в VirtualBox

VirtualBox позволяет виртуальным машинам использовать сетевые подключения хостовой системы, а также создавать виртуальные сети для виртуальных машин.

С помощью средств графического интерфейса пользователя может быть настроено до 4-х сетевых адаптеров для каждой из зарегистрированных в VirtualBox виртуальных машин.

Процедура настройки сетевых интерфейсов описана в инструкции пользователя Oracle VM VirtualBox[3].

Для каждой виртуальной машины можно эмулировать до 4-х сетевых адаптеров (рис.3.1)

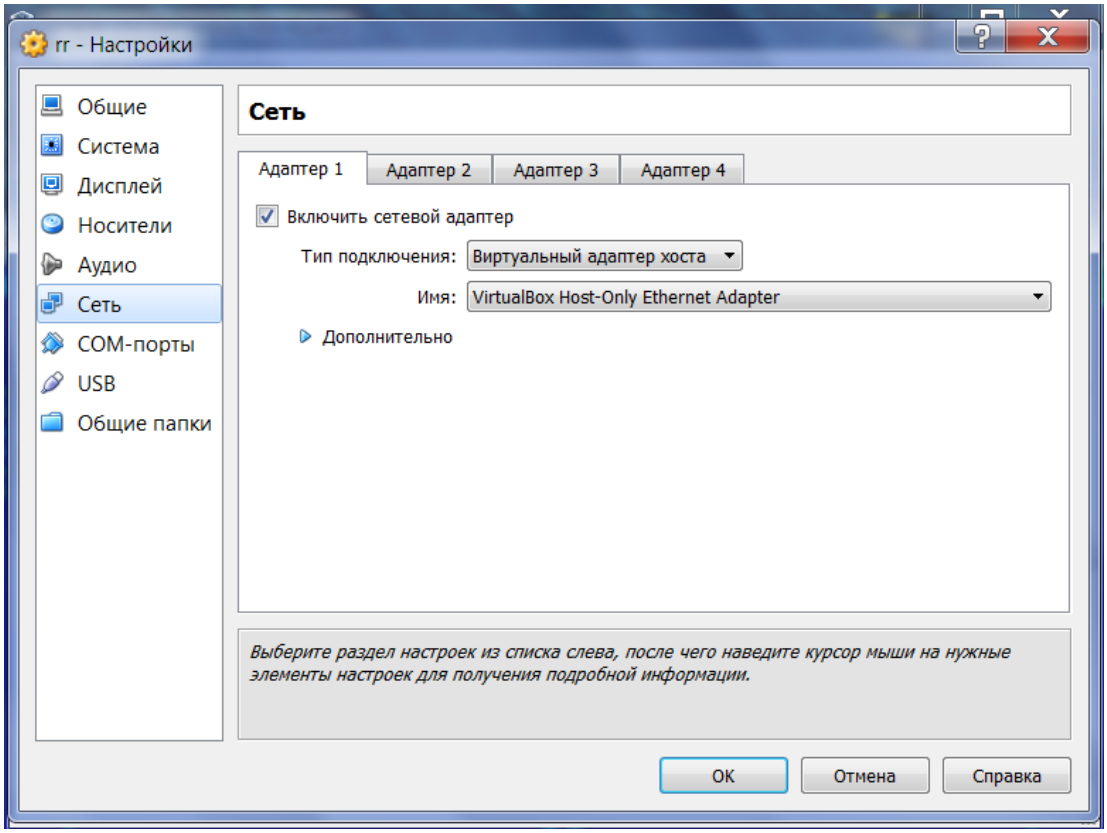


Рис. 3.1. – Настройки сетевых интерфейсов Oracle VM VirtualBox

Каждый из сетевых адаптеров может работать в одном из 6 режимов.

**Не подключен**. В данном режиме адаптер присутствует в гостевой системе, но ведет себя так, как будто сетевой кабель в него не включен (рис. 3.2).

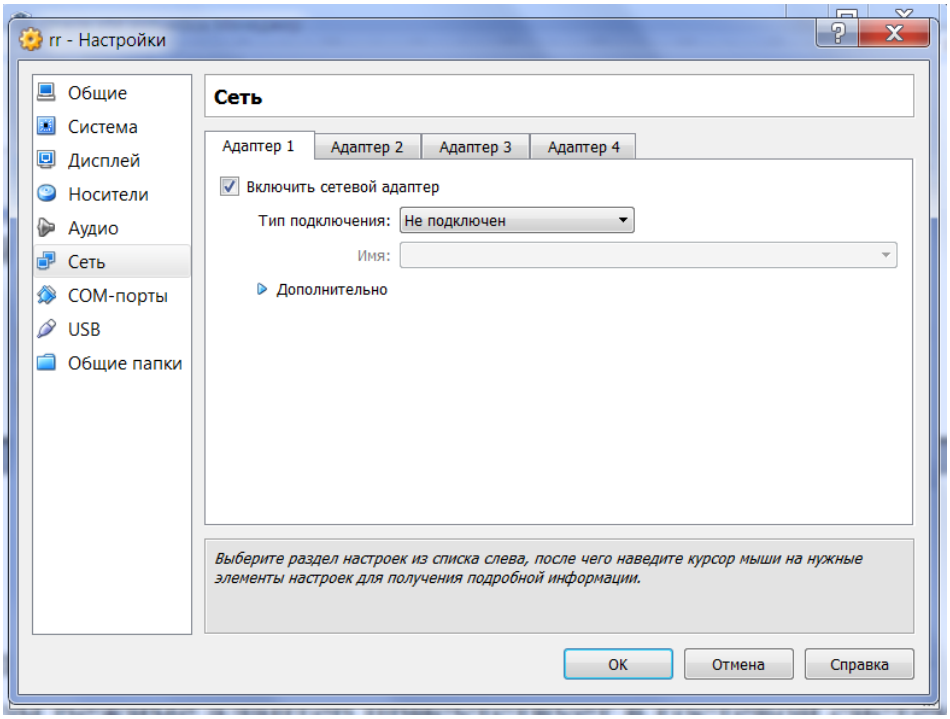


Рис. 3.2. – Тип подключения “**Не подключен**”

**NAT.** В данном режиме адаптер использует сетевые настройки основной системы при взаимодействии с сетью физического узла и прочими внешними сетями. Сетевая подсистема VirtualBox транслирует IP-трафик с исходным IP-адресом виртуальной машины в трафик с исходным адресом сетевого адаптера хостовой системы (трансляция сетевых адресов, Network Address Translation) (рис. 3.3).

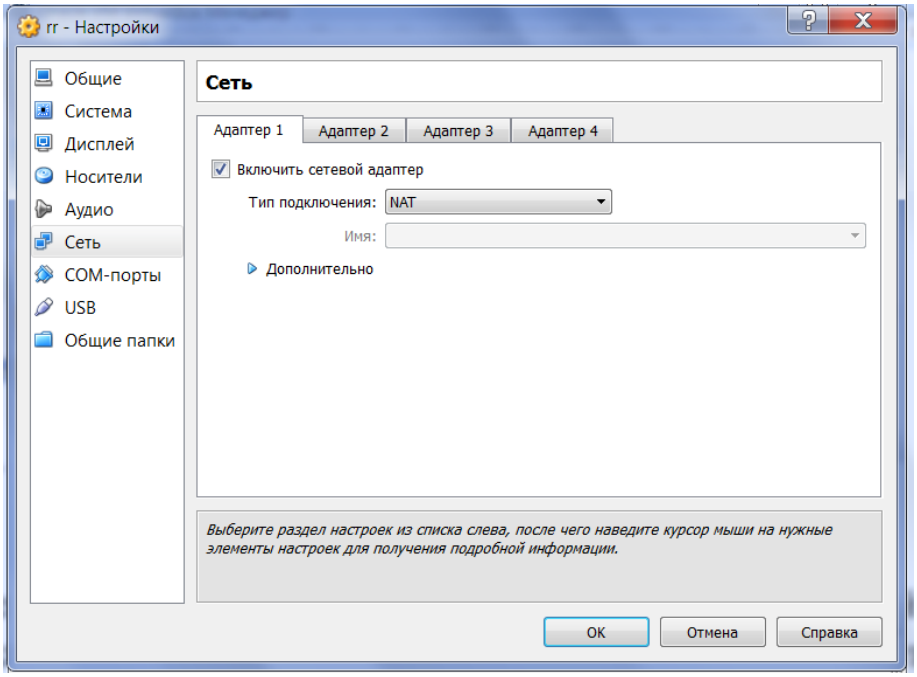


Рис. 3.3. – Тип подключения “**NAT**”

Если нужно просматривать Web, загружать файлы и пользоваться почтой e-mail в гостевой системе, то сетевая конфигурация “NAT” подойдет для этих целей.

**Сетевой мост.** В данном режиме сетевой адаптер ВМ подключается к сетевому адаптеру хостовой системы и обрабатывает сетевые пакеты непосредственно в обход сетевого стека хостовой системы ( адаптер хостовой системы работает с адаптером ВМ в режиме моста ) (рис. 3.4).

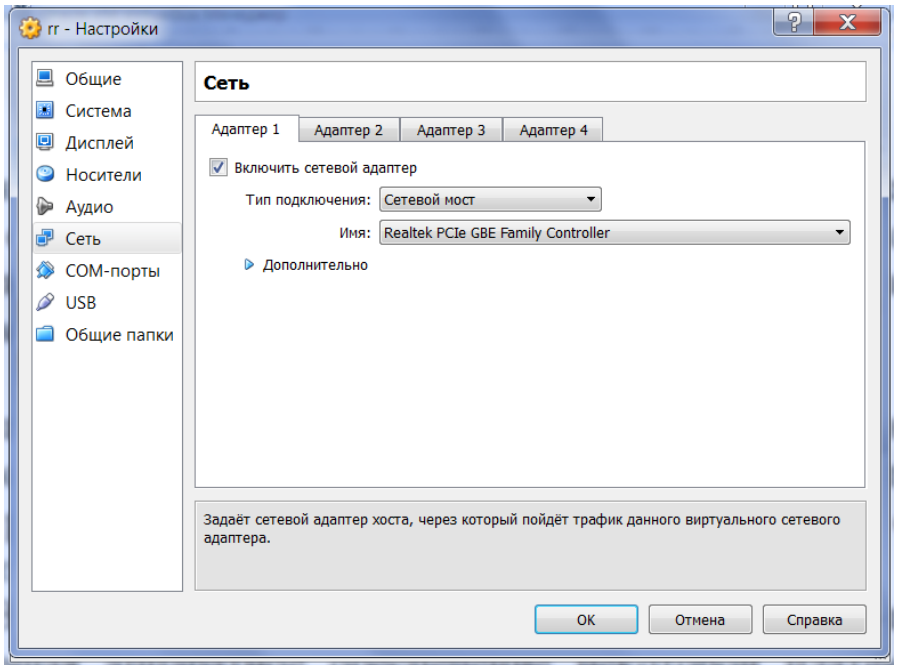


Рис. 3.4. – Тип подключения “**Сетевой мост**”

Этот режим нужен для продвинутых сетевых возможностей, например моделирование сетей и работающих серверов в гостевой системе.

**Внутренняя сеть.** Сетевые адаптеры ВМ объединяются между собой в изолированный сегмент сети (рис. 3.5).

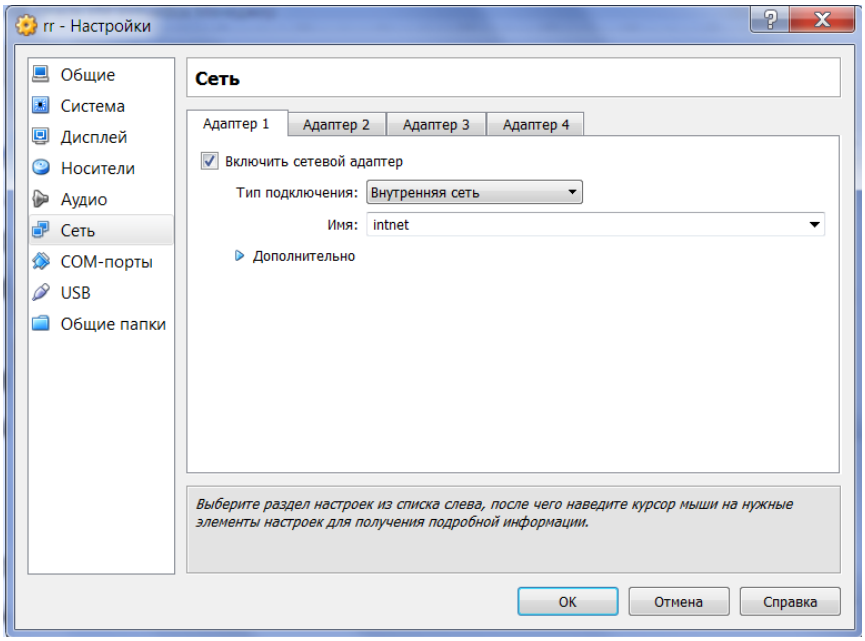


Рис. 3.5. – Тип подключения “**Внутренняя сеть**”

Этот режим можно использовать для создания виртуальной сети которая доступна из виртуальной машины, но не для приложений запущенных на хосте или других внешних сетевых устройств.

**Виртуальный адаптер хоста**. Сеть, объединяющая в данный сегмент хостовую систему и виртуальные машины, включенные в данный сегмент. Для этого режима VirtualBox создает в хостовой системе программный сетевой интерфейс и устанавливает на нем IP-адрес (рис. 3.6).

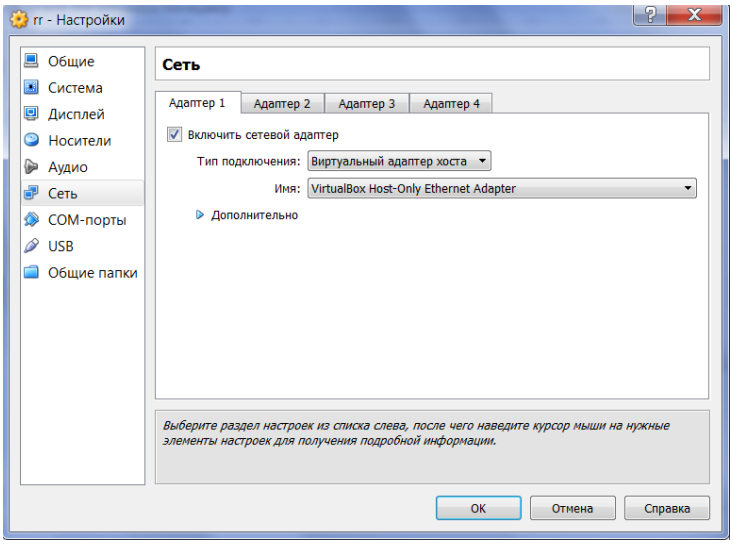


Рис. 3.6. – Тип подключения “Виртуальный адаптер хоста”

Данный режим можно использовать для создания сетей из хоста и нескольких виртуальных машин, без использования физического сетевого интерфейса хоста. На хосте создается виртуальный сетевой интерфейс, обеспечивающий соединения между хост-системой и виртуальными машинами.

**Универсальный драйвер**. Пользователь сам выбирает драйвер сетевого адаптера, который может быть входит в состав VirtualBox или загружается с пакетом дополнений к VirtualBox (рис. 3.7).

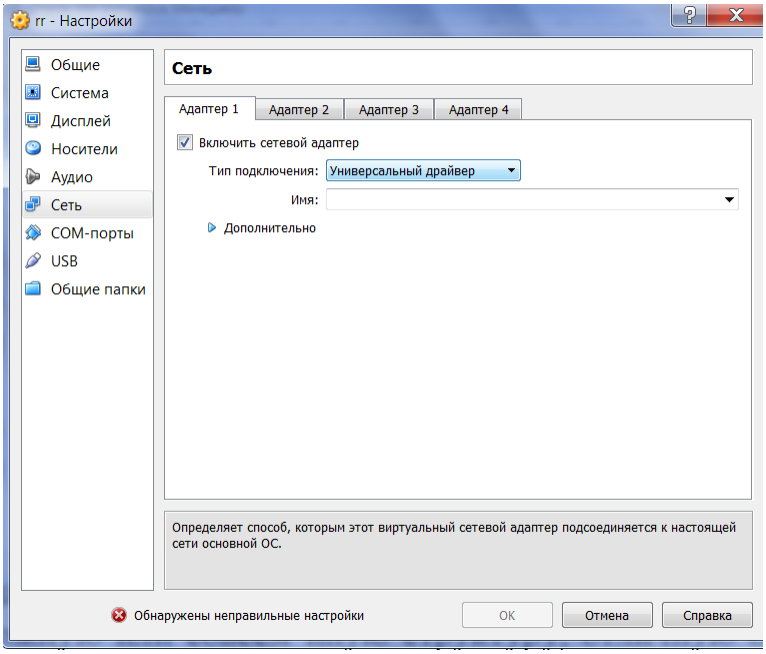


Рис. 3.7. – Тип подключения “**Универсальный драйвер**”

Этот режим может быть использован для подключения распределенных виртуальных машин к виртуальному коммутатору Ethernet на Linux или FreeBSD

хостах. Для каждого из 4-х сетевых адаптеров виртуальной машины можно выбрать один из нескольких драйверов эмулирующих реальные сетевые адаптеры различных производителей оборудования или драйвер Virtio-net, являющийся частью open-source KVM проекта[7] (рис. 3.8).

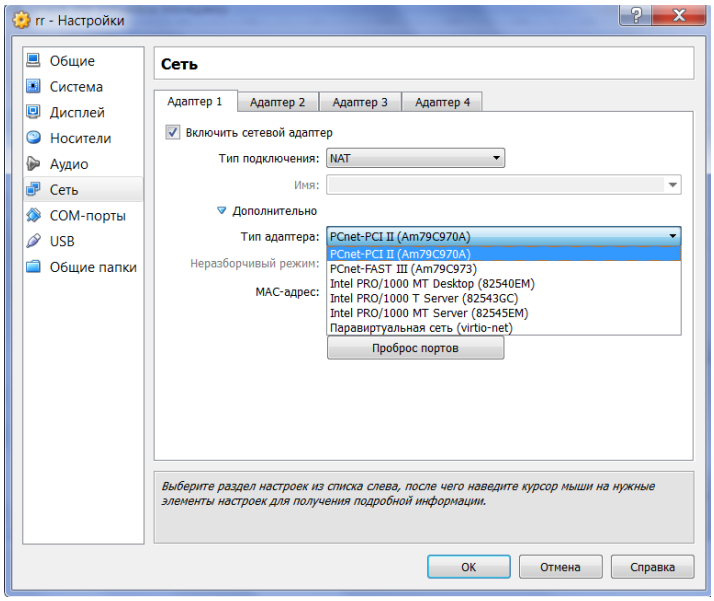


Рис. 3.8. – Выбор драйвера сетевого адаптера

Драйвер Virtio-net позволяет избежать сложности эмуляции сетевого оборудования и позволяет повысить производительность сети. Linux ядро гостевой системы версии 2.6.25 и старше может поддерживать Virtio-net адаптер. Для гостевых систем на Windows драйвер для адаптера Virtio-net можно скачать с сайта KVM проекта[7].

### 3.2 Организация общего доступа в сетях Windows

Для правильной работы компьютеров в сети Windows они должны иметь уникальные имена. Имя компьютера можно задать в свойствах компьютера (рис. 3.9)

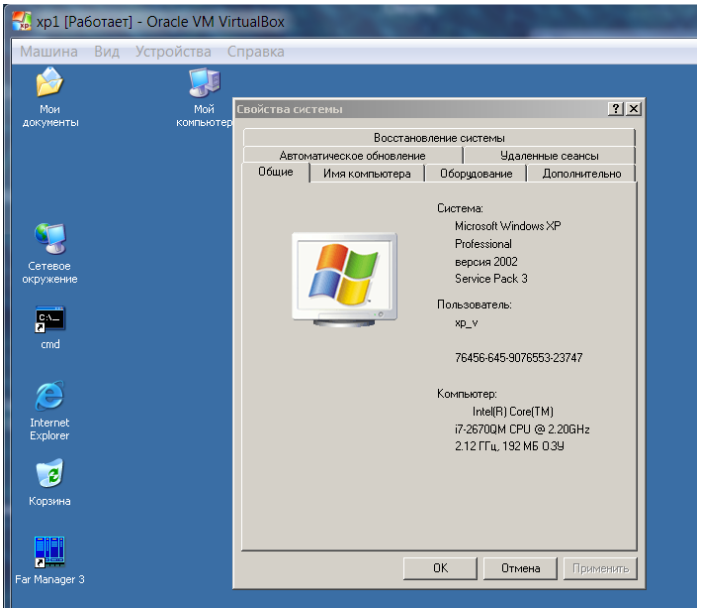


Рис. 3.9. – Свойства компьютера

Для изменения имени компьютера необходимо выбрать соответствующий пункт меню и изменить имя компьютера (рис. 3.10). Для удобства работы в сети компьютерам может быть назначена одна рабочая группа (по умолчанию WORKGROUP)

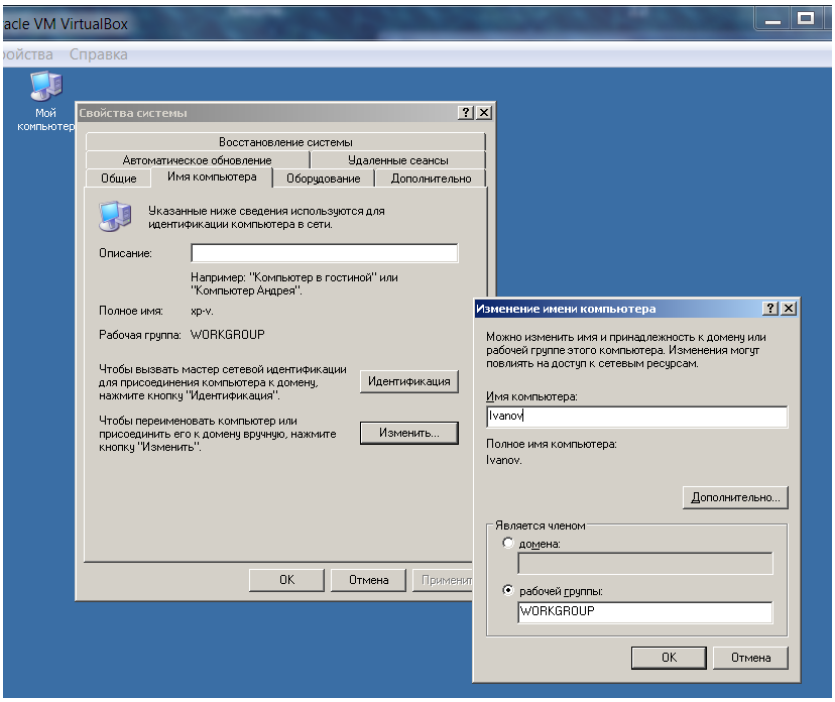


Рис. 3.10. – Изменение имени компьютера

После изменения имени компьютера его необходимо перезагрузить.

Простой общий доступ к файлам и папкам включен по умолчанию. Убедиться в этом можно, если нажать “Пуск” – “Панель управления” – “Свойства папки” – вкладка “Вид”. Напротив пункта “Использовать простой общий доступ к файлам (рекомендуется)” должен стоять флажок (рис. 3.11).

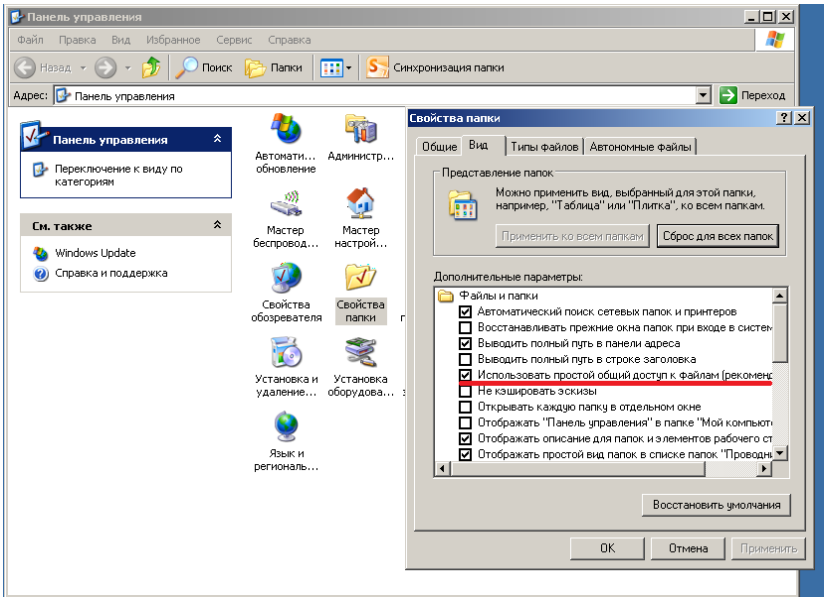


Рис. 3.11. – Простой общий доступ к файлам и папкам

Если флажка нет, значит, на компьютере используется расширенный общий доступ.

Чтобы открыть общий доступ к какой-либо папке или диску, нужно на требуемом объекте щелкнуть правой кнопкой мыши – выбрать “Свойства” – перейти на ,вкладку “Доступ”. Если предоставляется общий доступ на диск или папку в первый раз, то нужно будет нажать на ссылку, показанную на рис. 3.12.

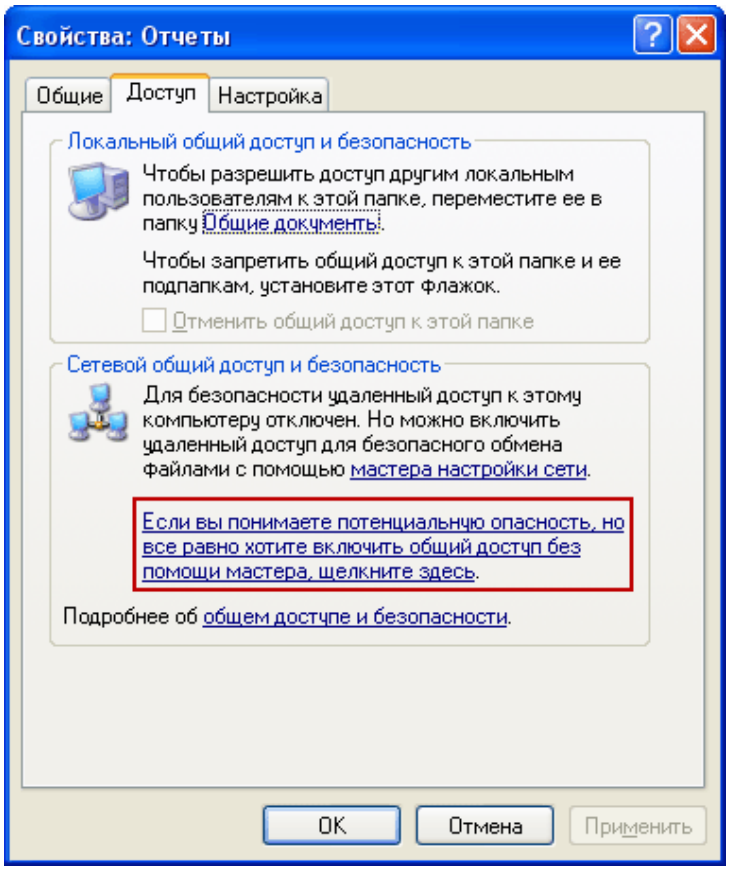


Рис. 3.12. – Настройка доступа к папке

Затем выбрать пункт “Просто включить общий доступ к файлам” (рис. 3.13)

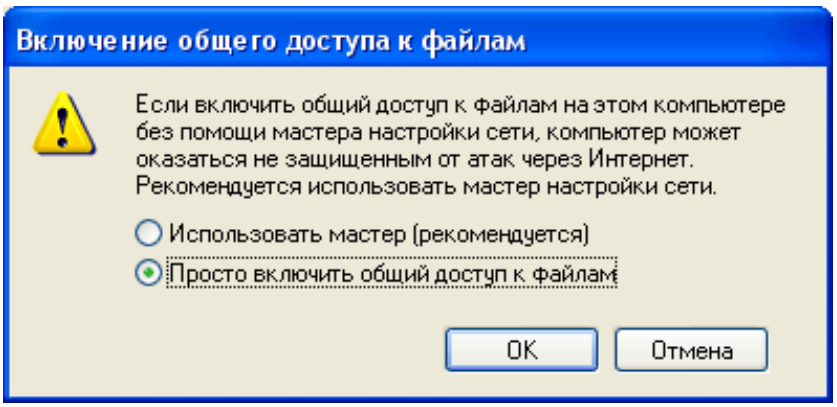


Рис. 3.13. – Включение общего доступа к файлам

В открывшемся окне необходимо поставить флажок напротив пункта “Открыть общий доступ к этой папке” (рис. 3.14).

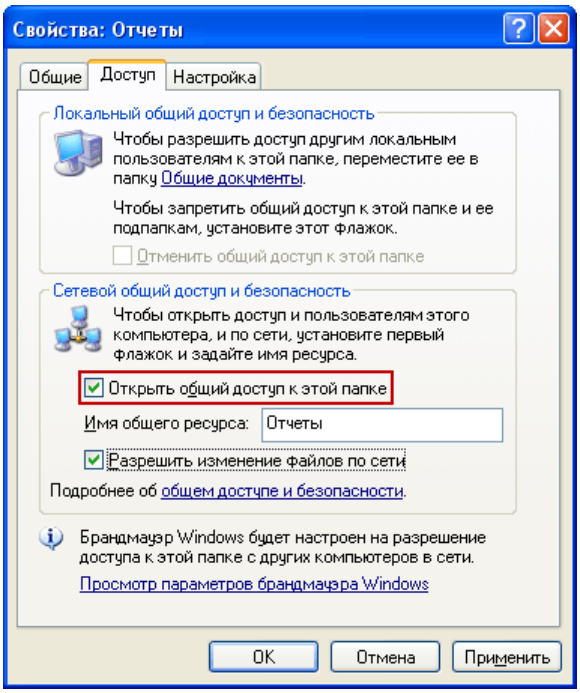


Рис. 3.14. – Открытие общего доступа к папке

Таким образом, пользователям сети открывается доступ к файлам, содержащимся в данной папке, в режиме “только чтение”. Изменить файлы, находящиеся в этой папке, или записать в нее свои файлы они не смогут.

В поле “Имя общего ресурса” вы можете ввести сетевое имя папки, под которым она будет отображаться в списке общих ресурсов локальной сети.

Если вы поставите флажок напротив пункта “Разрешить изменение файлов по сети”, то тем самым разрешите пользователям копировать в эту папку свои файлы, а так же изменять содержащиеся в ней документы.

Затем необходимо нажать  в данном окне “Применить” – “ОК”. После этого папка станет общедоступной и на ней появится символ руки (рис. 3.15).

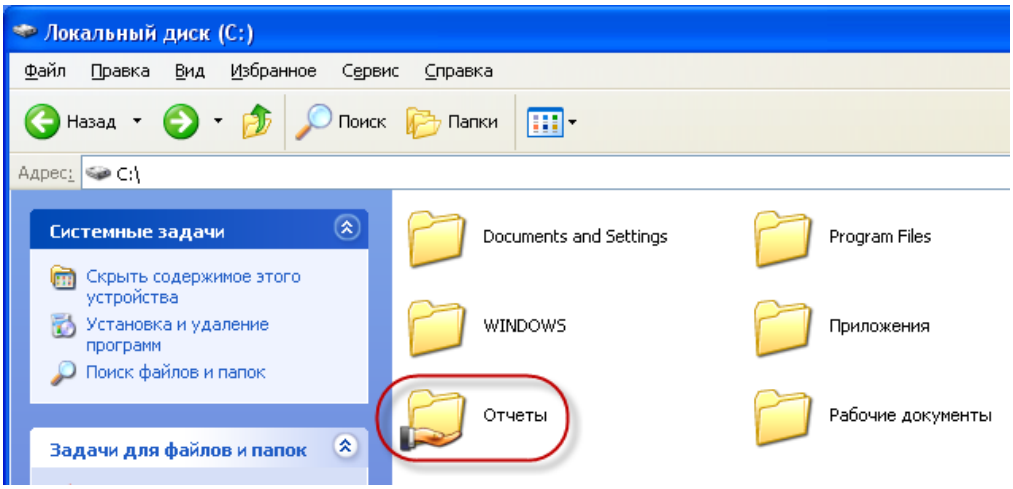


Рис. 3.15. – Ощедоступная папка

По соображениям безопасности не стоит открывать полный доступ к системным папкам (Windows, Program Files) и папкам, содержащим важные данные.

Для обеспечения безопасной работы можно создать специальную папку или папки для общих сетевых файлов и открыть полный доступ только к этим папкам.

Чтобы пользователи вашей сети могли получать доступ к общим папкам – на компьютере, где они расположены, необходимо включить учетную запись “Гость”. Это позволит получать доступ к общей папке любому пользователю с любого компьютера, входящего в сеть.

Чтобы проверить активирован ли на компьютере гостевой аккаунт, необходимо щелкнуть правой клавишей мыши по значку “Мой компьютер” на рабочем столе и выбрать пункт “Управление”. В открывшемся окне слева в разделе “Служебные программы” выделяем пункт “Локальные пользователи и группы”. Раскрыв его, становимся на папку “Пользователи” – в правом поле находим “Гостя” и щелкаем по нему дважды мышкой (рис. 3.16).

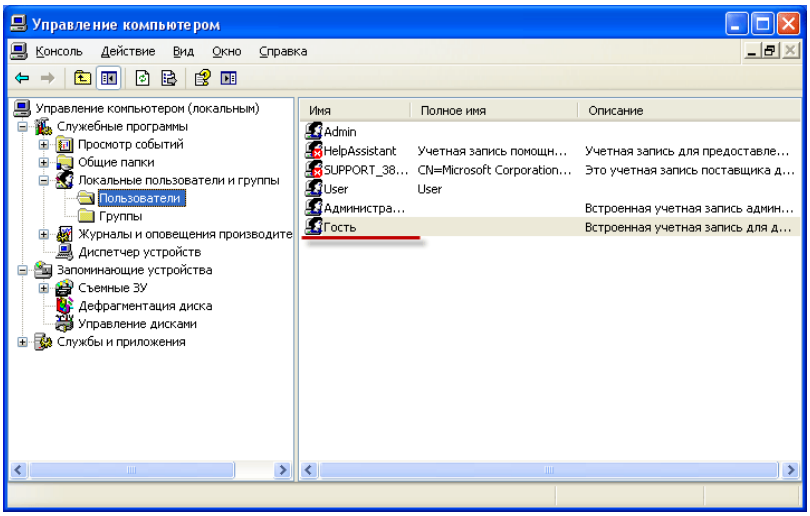


Рис. 3.16. – Настройка гостевого аккаунта

В следующем окне галочка “Отключить учетную запись” должна быть снята (рис. 3.17)

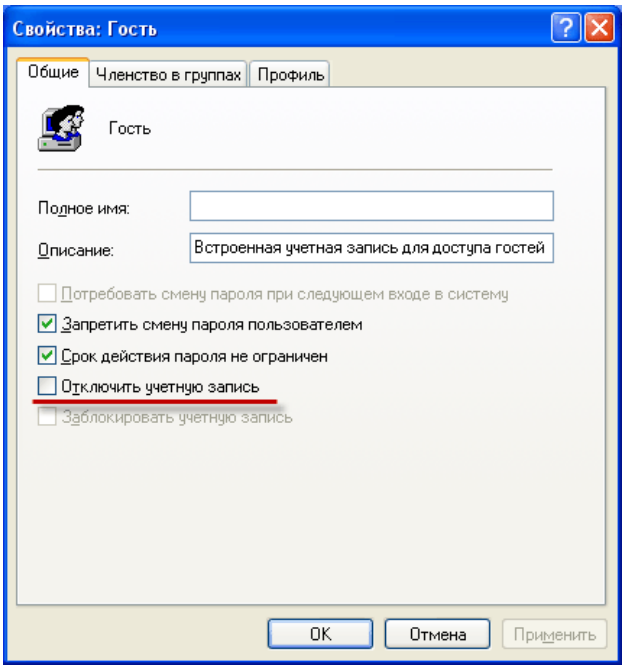


Рис. 3.17. – Настройка гостевого аккаунта

После предоставления общего доступа к папкам они будут отображаться в сетевом “окружении” (рис. 3.18)

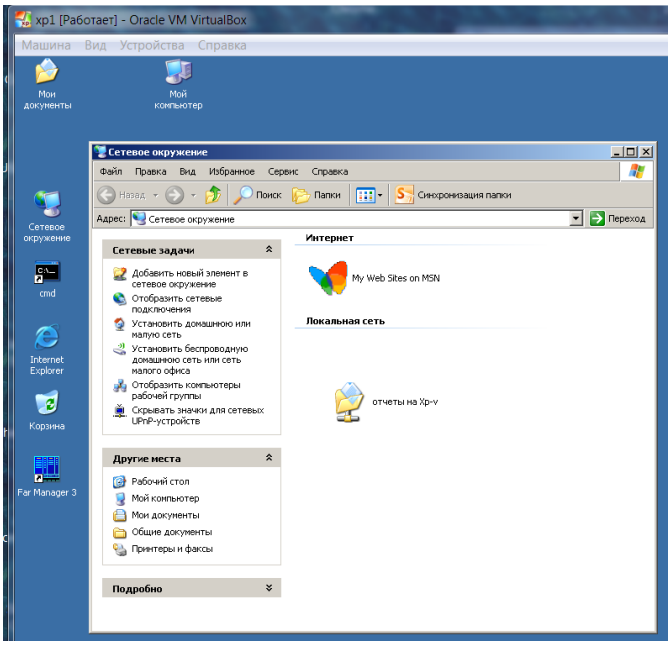


Рис. 3.18. – Сетевое окружение

На этом заканчивается установка простого общего доступа к файлам и папкам. Как правило, данного режима достаточно при работе в домашней сети. Однако в локальной сети какой-либо организации требуется более серьезное разграничение прав пользователей. В этом случае необходимо включать “Расширенный общий доступ к файлам и папкам”.

### 3.3 Организация общего доступа к ресурсам в сетях LINUX

Для правильной работы компьютеров в сети LINUX они должны иметь уникальные имена. Имя компьютера записано в файле **hostname ,** который находится в папке **/etc.** Оно должно состоять из латинских символов и цифр, допускается также использование символа “-”. Для изменения файла **hostname** можно воспользоваться файловым менеджером MC (рис. 3.19).

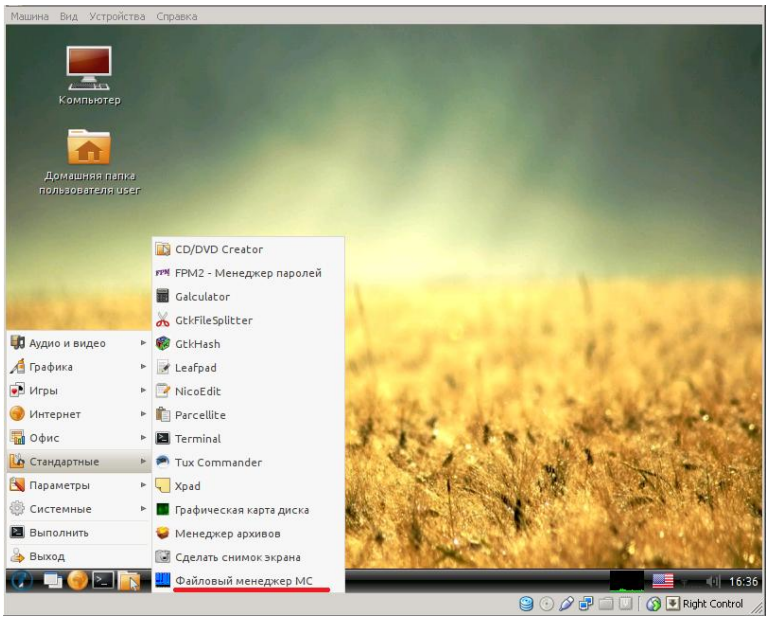


Рис. 3.19. – файловый менеджер MC

После запуска файлового менеджера MC откроется окно вид, которого показан на рис. 3.20.

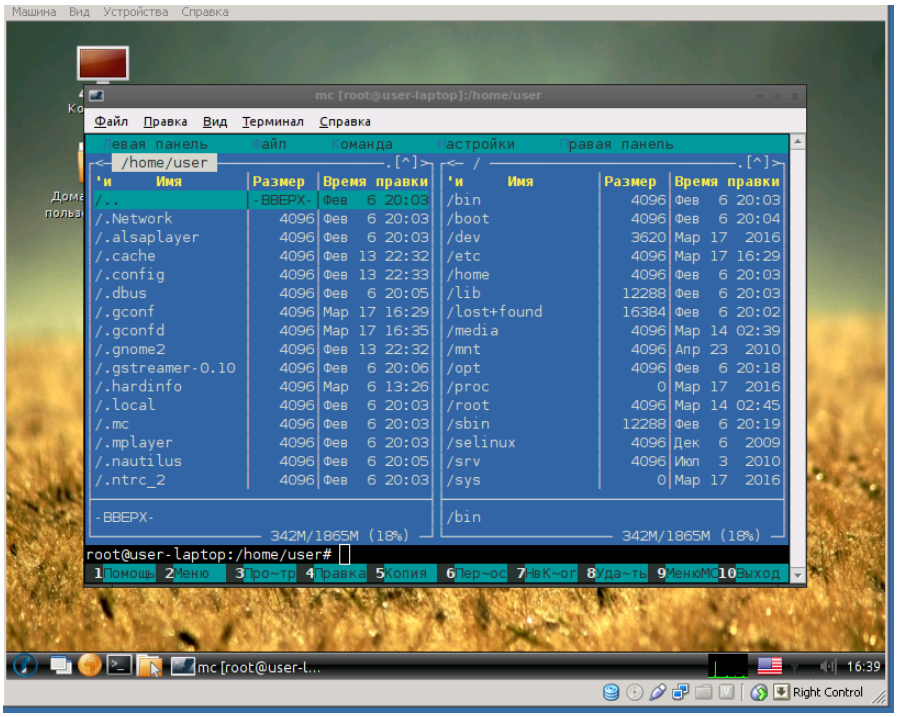


Рис. 3.20. – Окно файлового менеджера MC

Далее необходимо перейти в папку /etc , выделить файл **hostname** и нажать F4. После этого можно производить редактирование файла. По окончании редактирования необходимо нажать F2, подтвердить сохранение и F10 для выхода (рис. 3.21).

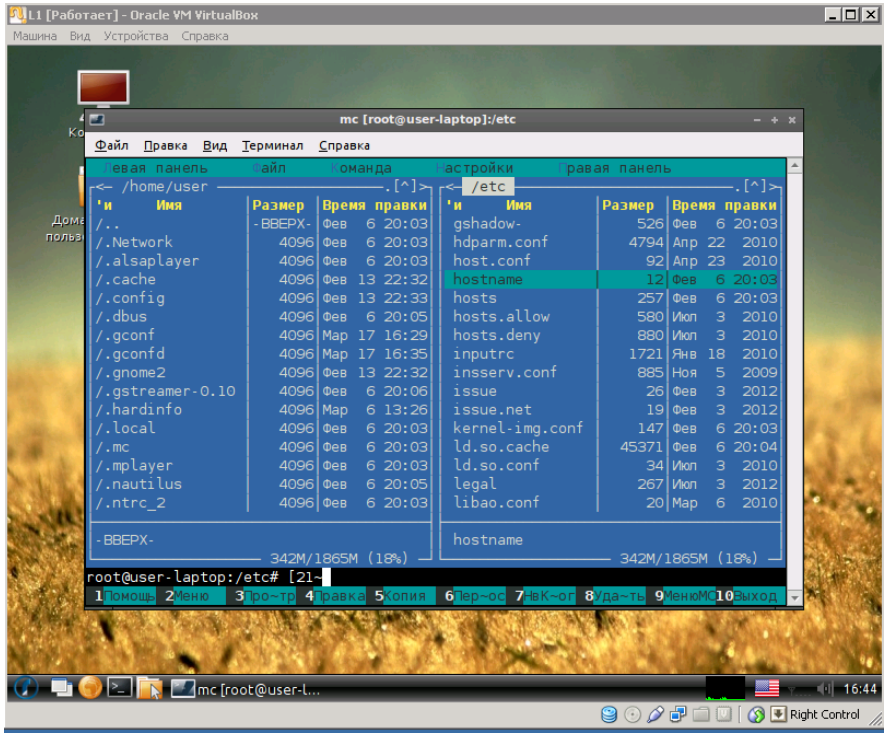


Рис. 3.21. – Редактирование файла hostname

Для вступления изменений в силу необходимо произвести перезагрузку ОС на ВМ.

Для организации доступа к ресурсам компьютеров в сети Windows в ОС LINUX используется протокол **Samba**[8]**.**

**Samba** — программа, которая позволяет обращаться к сетевым дискам на различных операционных системах по протоколу SMB/CIFS. Имеет клиентскую и серверную части. **Samba** включена практически во все дистрибутивы GNU/Linux, в том числе, и в **Runtu.**

Для получения доступа к ресурсам сети можно открыть ярлык “Компьютер” на рабочем столе и выбрать вкладку “Сеть” (рис. 3.22)

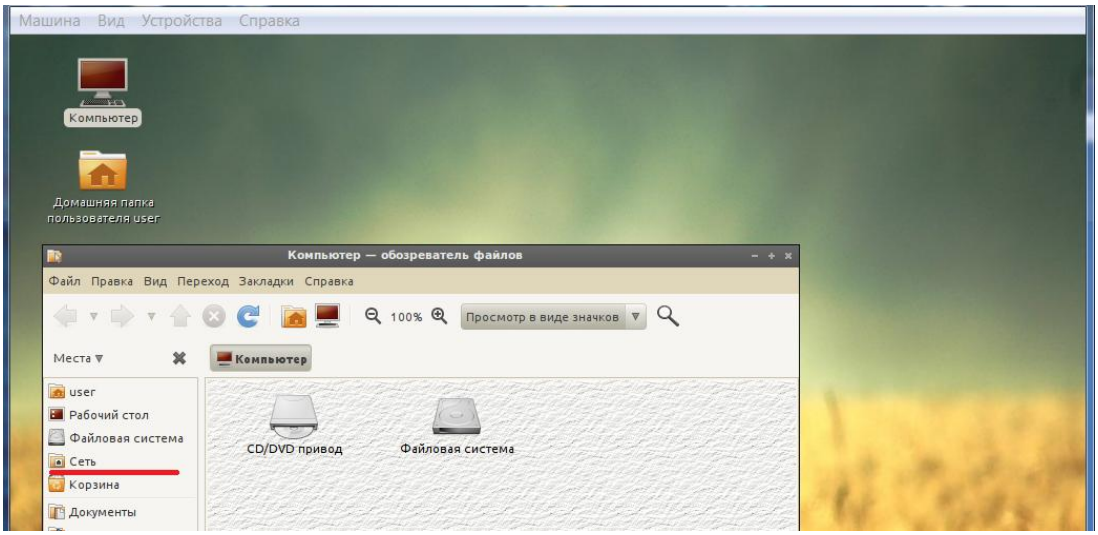


Рис.3.22. – Доступ к ресурсам сети

Открыв вкладку “Сеть”, получим доступ к ресурсам в локальной сеть с помощью обозревателя файлов (рис. 3.23).

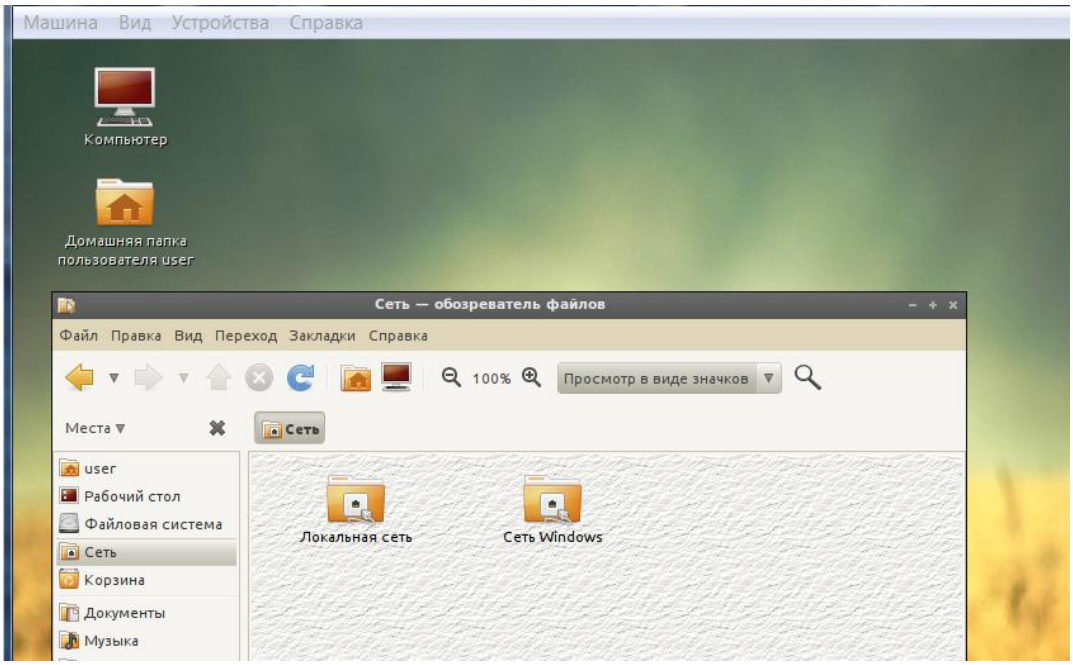


Рис. 3.23. – Доступ в сеть с помощью обозревателя файлов

Затем необходимо открыть вкладку “Сеть Windows”. Если в сети присутствуют компьютеры с общими ресурсами сети Windows, то будет доступен список рабочих групп и компьютеров с общими ресурсами в них (рис. 3.24)

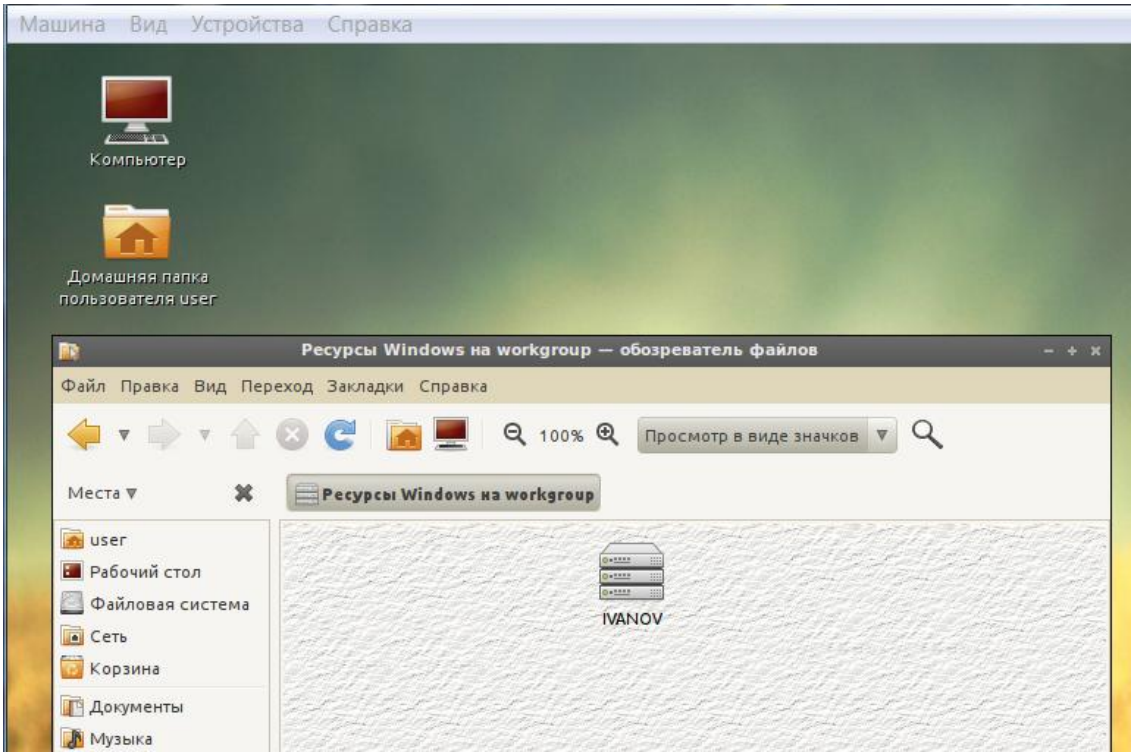


Рис.3.24. – Ресурсы сети Windows в обозревателе файлов

Открыв в обозревателе значок компьютера можно получить доступ к папкам общего доступа (рис. 3.25)

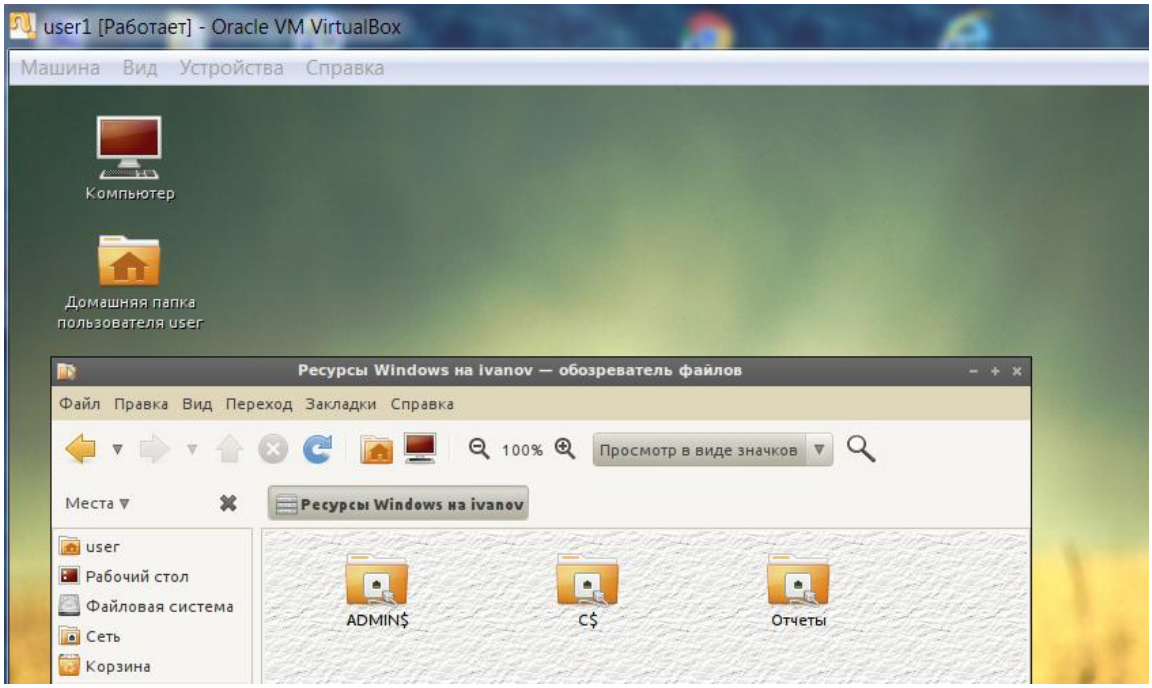


Рис. 3.25. – Общие папки сети Windows

Для доступа к общим ресурсам ОС LINUX с компьютеров ОС Windows должна быть установлена серверная часть программы **Samba.** Если она установлена, то можно произвести настройку сетевых ресурсов **Samba** (рис. 3.26)

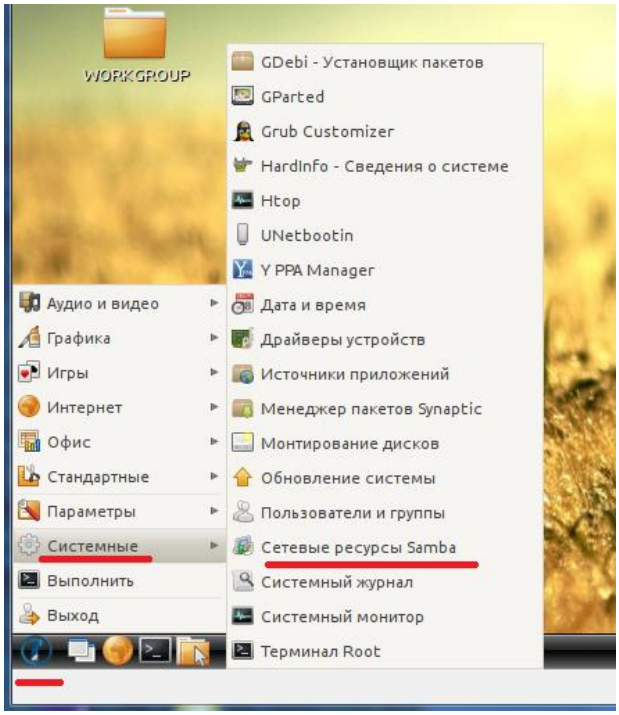


Рис. 3.26. – Настройка сетевых ресурсов Samba

Для предоставления общего доступа к папкам ОС LINUX необходимо добавить их в список ресурсов сервера Samba, используя значок “+” (рис. 3.27) и используя кнопку обзор открыть окно для выбора каталога, предоставляемого в общий доступ (рис. 3.28).

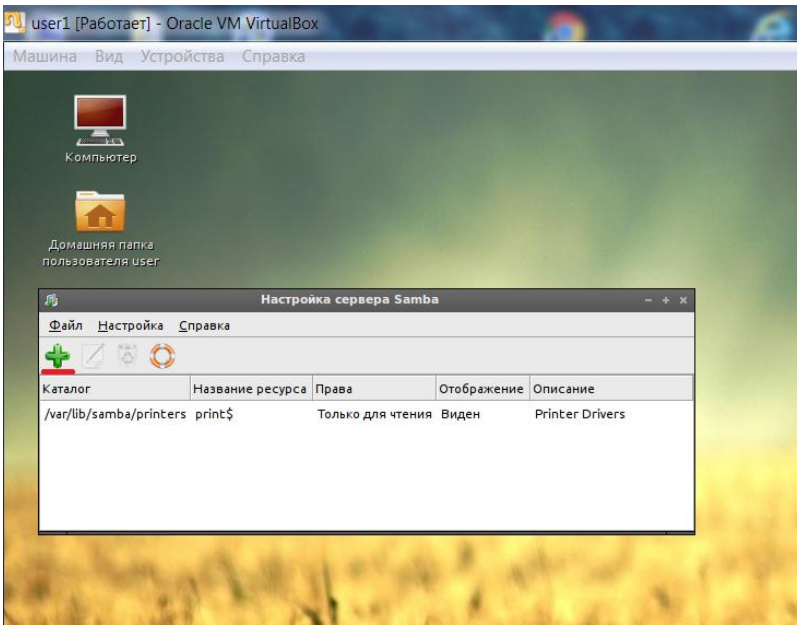


Рис. 3.27. – Настройка сервера Samba

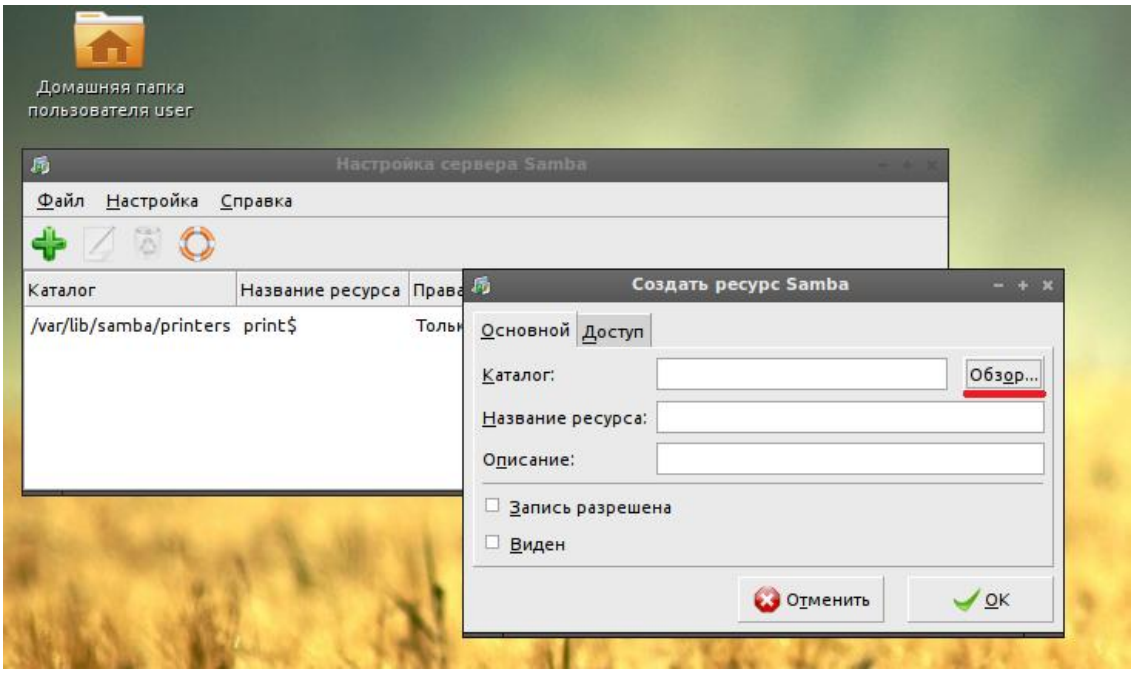


Рис. 3.28. – Создание ресурса Samba

После создания ресурса Samba необходимо установить его видимость в сети и разрешение записи, если предполагается запись и изменение файлов в папке по сети (рис. 3.29).

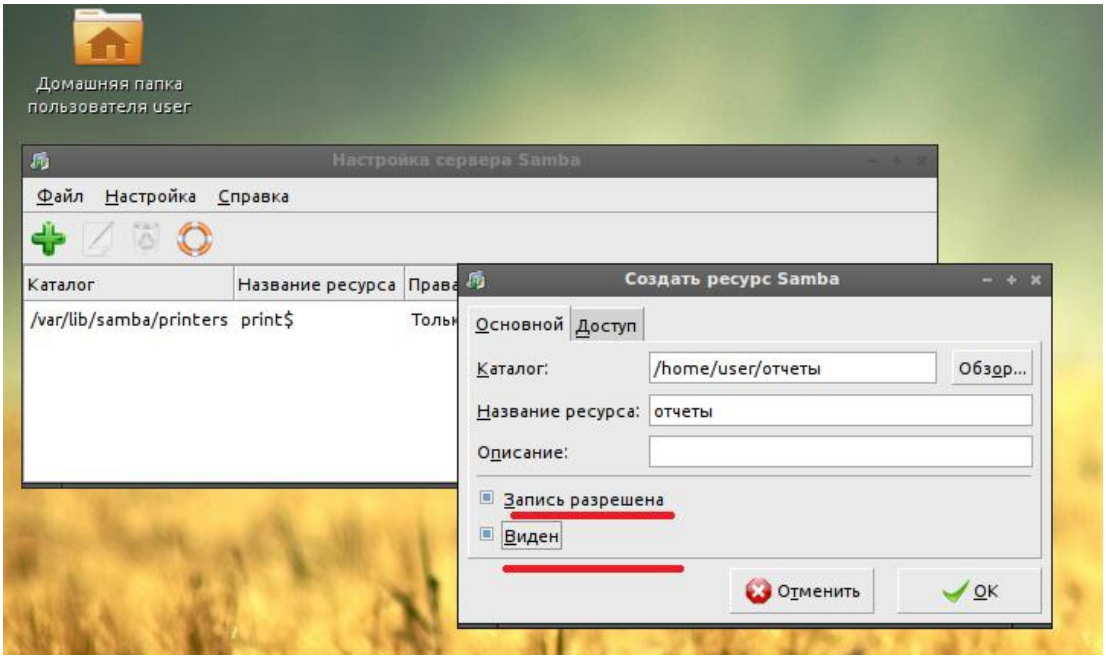


Рис. 3.29. – Установка видимости и разрешение записи ресурса Samba

Далее необходимо предоставить доступ к ресурсу пользователям. Можно выбрать доступ для конкретных пользователей или предоставить доступ всем (рис. 3.30).

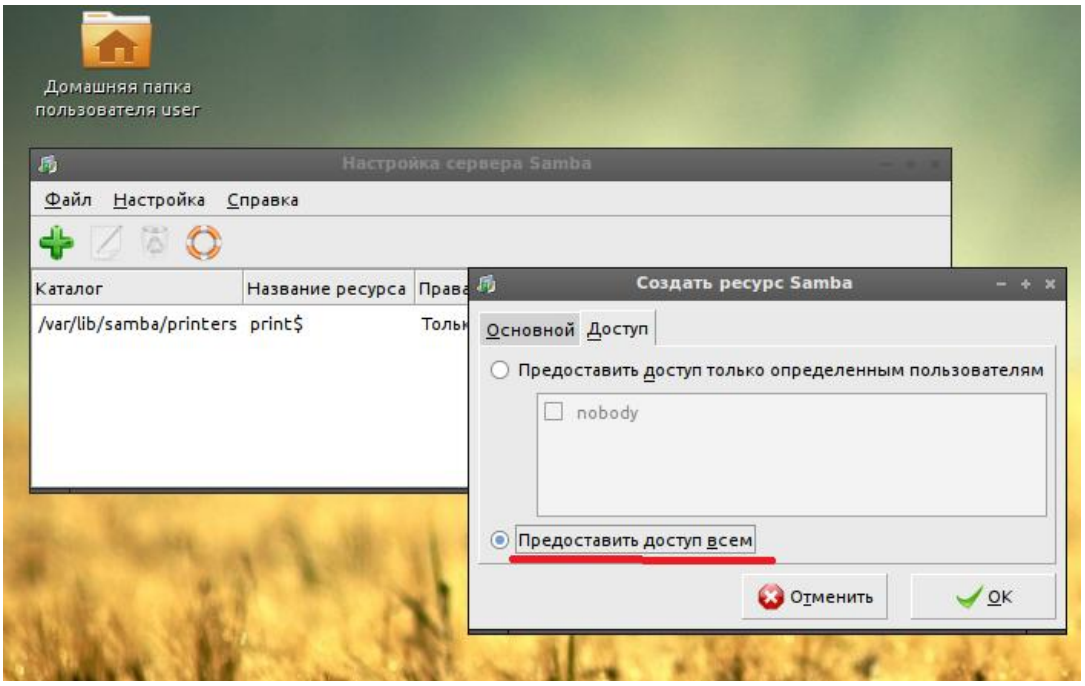


Рис. 3.30. – Предоставление доступа пользователям к ресурсу Samba

После создания ресурса Samba он будет доступен в сети ОС Windows, но в случае необходимости создания и изменения в нем файлов по сети (например, при операции копирования) необходимо обеспечить права пользователей на запись в папку ресурса. С этой целью открываем на папке правой кнопкой мыши контекстное меню и выбираем **“Свойства”** (рис. 3.31)

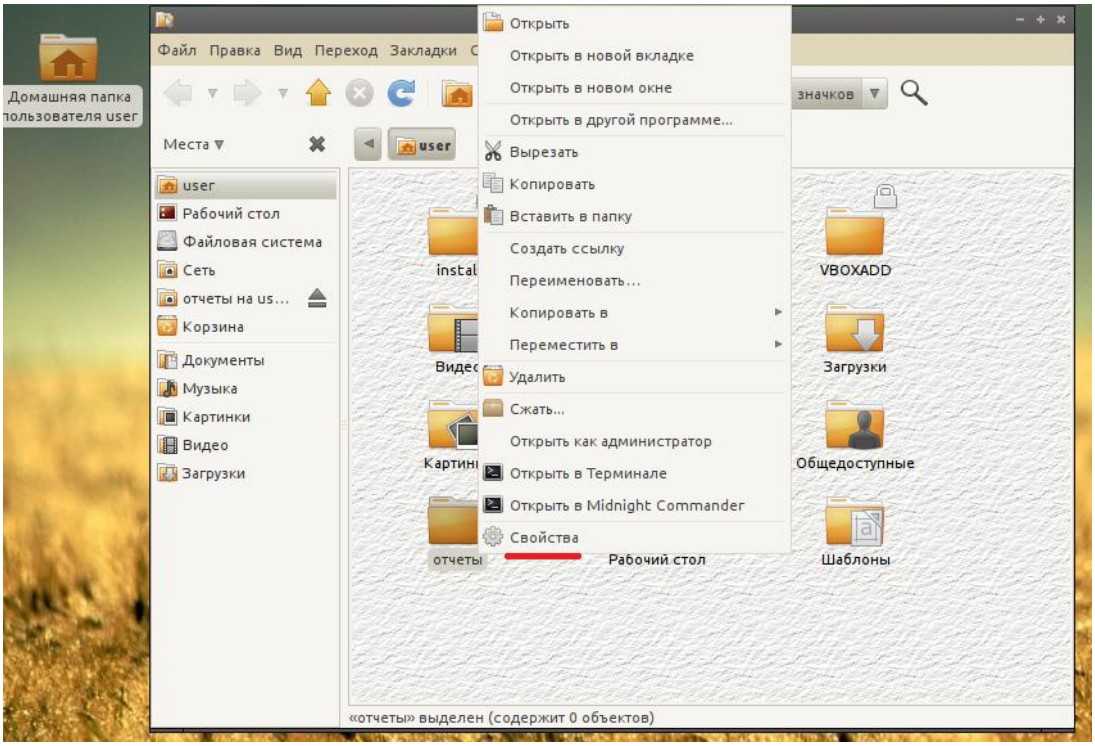


Рис. 3.31. – Свойства папки

Во вкладке “права” устанавливаем права на создание и удаление файлов для остальных пользователей и распространяем их на вложенные файлы (рис. 3.32)

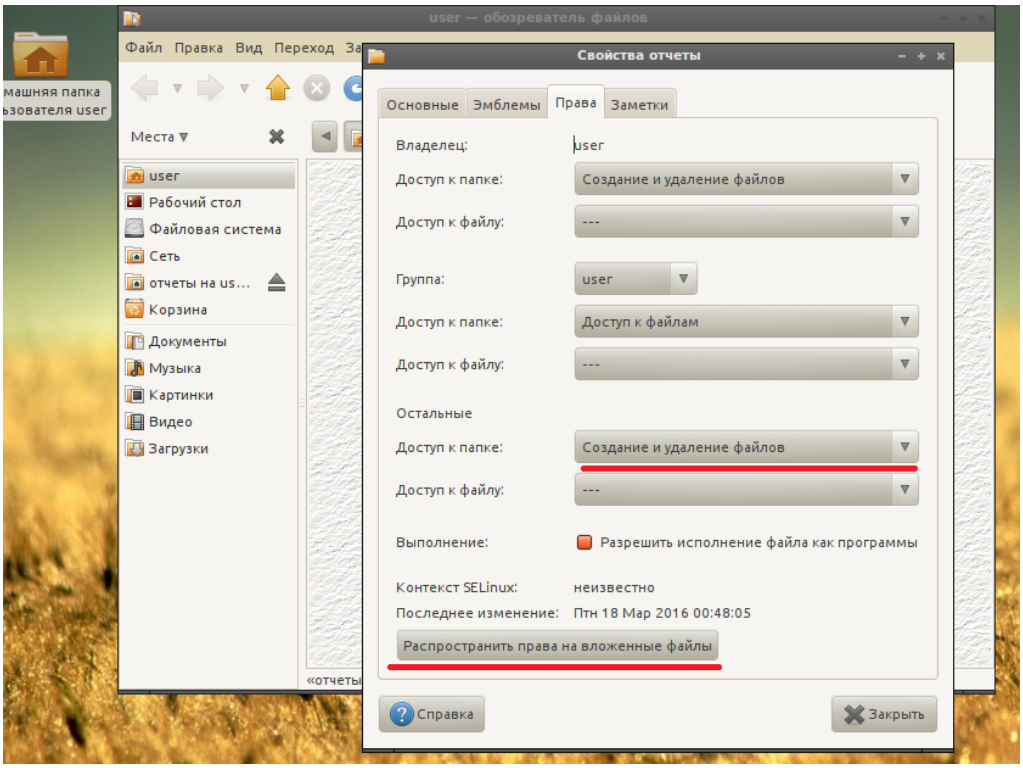


Рис. 3.32. – Установка прав пользователей на доступ к папке

### 3.4 Технические средства для выполнения работы

Компьютерный класс с установленной **ОС Windows** и **Oracle VM VirtualBox**.

### 3. 5 Порядок выполнения лабораторной работы

1. Запустить Oracle VM VirtualBox Менеджер.
2. Придумать имя для двух ВМ (имя должно содержать вашу фамилию и группу)
3. Создать две ВМ типа Windows XP (RAM -192 MB, файл образа – c:/xp.vdi, у виртуального носителя должен быть атрибут “множественное подключение”)
4. В настройках сети ВМ установить тип подключения “виртуальный адаптер хоста”
5. Запустить виртуальные машины, поменять имена компьютеров (имена должны содержать вашу фамилию и номер машины 1,2)
6. Перезагрузить ОС на виртуальных машинах.
7. Создать на виртуальных машинах на диске c: папку, имя которой должно содержать вашу фамилию и номер машины (1,2).
8. Установить для созданных папок режим общий доступ. Для первой папки установить режим “Только чтение”, для второй “Разрешить изменение файлов по сети”.
9. Создать при помощи блокнота на 1 ВМ текстовый файл **1.TXT** с произвольной информацией, а на 2 ВМ текстовый файл **2.TXT** в папках, к которым предоставлен общий доступ.
10. Открыть “Сетевое окружение” на виртуальных машинах и произвести копирование созданных текстовых файлов между ВМ.

11. Произвести выключение второй ВМ.
12. Создать ВМ типа Other (RAM -640 MB, файл образа – **c:/rt_00.vdi**, у виртуального носителя должен быть атрибут “множественное подключение”)
13. Произвести запуск виртуальной машины с ОС Runtu (имя – user, пароль - user).
14. Поменять имя компьютера с ОС Runtu при помощи программы MC (имя должно содержать вашу фамилию, использовать латинские символы).
15. При помощи обозревателя файлов скопировать текстовый файл **1.txt** из общей папки ВМ с ОС Windows XP в папку **/home/user** ВМ с ОС Runtu.
16. Создать папку на ВМ с ОС Runtu в каталоге **/home/user** (имя папки должно содержать вашу фамилию).
17. Создать в этой папке текстовый файл **Runtu.TXT** содержащий вашу фамилию и имя.
18. Создать ресурс SAMBA предоставляющий общий доступ к созданной папке для всех пользователей с правом записи.
19. Предоставить права на создание и удаление файлов в созданной папке для всех пользователей и распространить его на вложенные файлы.
20. при помощи проводника в ВМ с ОС Windows XP, скопировать файл **Runtu.TXT,** который содержит вашу фамилию и имя на диск C:/ в ВМ с ОС Windows XP.

### 3.6 Содержание отчета о выполнении лабораторной работы

Отчёт должен содержать:
- титульный лист;
- цель исследования;
- ход работы;
- выводы.

Отчёт по лабораторной работе должен быть выполнен в соответствии требованиями ГОСТ.

### 3.7 Порядок защиты работы

Защита производится при наличии отчета за компьютером и состоит в демонстрации навыков использования возможностей Oracle VM VirtualBox при выполнении задания выданного преподавателем.

### 3.8. Контрольные вопросы

1. Что такое виртуализация?
2. Каковы основные сетевые возможности Oracle VM VirtualBox?
3. Каковы основные этапы создания сети для виртуальной машины?
4. Как создать общедоступную папку?
5. Как скопировать файл из одной ВМ в другую по сети?

# 4. ЛАБОРАТОРНАЯ РАБОТА № 4 УДАЛЕННОЕ АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРА

Цель работы - знакомство с основными возможностями удаленного администрирования.

## 4.1 Удаленное администрирование

**Программы удалённого администрирования** — программы или функции операционных систем, позволяющие получить удалённый доступ к компьютеру через Интернет или ЛВС и производить управление и администрирование удалённого компьютера в реальном времени.

Программы удалённого администрирования предоставляют почти полный контроль над удалённым компьютером. Они дают возможность удалённо управлять рабочим столом компьютера, возможность копирования или удаления файлов, запуска приложений и т. д.

Удаленное управление доступно в большинстве современных операционных систем. Средства удаленного администрирования являются частью операционных систем или могут быть в виде отдельного ПО.

В ОС Windows средства удаленного управления организованы в виде протокола удаленного рабочего стола — RDP (англ. Remote Desktop Protocol)[9].

RDP —протокол прикладного уровня, использующийся для обеспечения удалённой работы пользователя с сервером, на котором запущен сервис терминальных подключений.

Клиенты существуют практически для всех версий Windows (включая Windows CE, Phone и Mobile), Linux, FreeBSD, Mac OS X, iOS, Android, Symbian.

Официальное название Майкрософт для клиентского ПО — Remote Desktop Connection или Terminal Services Client (TSC), в частности, клиент в Windows 2k/XP/2003/Vista/2008/7/8/10 называется mstsc.exe.

**Особенности RDP протокола:**

- поддержка 32-битного цвета;
- возможность использовать 128-битовое шифрование по алгоритмам RC4, AES;
- звук с удалённого ПК переадресовывается и воспроизводится на локальном компьютере;
- позволяет подключать локальные ресурсы к удалённой машине (mapping);
- позволяет использовать локальный или сетевой принтеры на удалённом ПК;
- позволяет приложениям, выполняющимся в пределах текущего сеанса, обращаться к локальным последовательным и параллельным портам;
- можно обмениваться информацией через буфер обмена.

Для управления рабочими столами ОС Linux и удаленного администрирования широко используется протокол **Virtual Network Computing**[10].

**Virtual Network Computing (VNC)** — система удалённого доступа к рабочему столу компьютера. Управление осуществляется путём передачи нажатий клавиш на клавиатуре и движений мыши с одного компьютера на другой и ретрансляции содержимого экрана через компьютерную сеть.

Система VNC платформонезависима: VNC-клиент, называемый VNC viewer, запущенный на одной операционной системе, может подключаться к VNC-серверу, работающему на любой другой ОС. Существуют реализации клиентской и серверной части практически для всех операционных систем.

К одному VNC-серверу одновременно могут подключаться множественные клиенты. Наиболее популярные способы использования VNC — удалённая техническая поддержка и доступ к рабочему компьютеру из дома.

VNC состоит из двух частей: клиента и сервера. Сервер — программа, предоставляющая доступ к экрану компьютера, на котором она запущена. Клиент (или viewer) — программа, получающая изображение экрана с сервера и взаимодействующая с ним.

### 4.2 Организация удаленного управления рабочим столом ОС Windows

Для возможности удаленного управления и администрирования компьютера с ОС Windows необходимо открыть свойства компьютера, как показано на рис. 4.1.

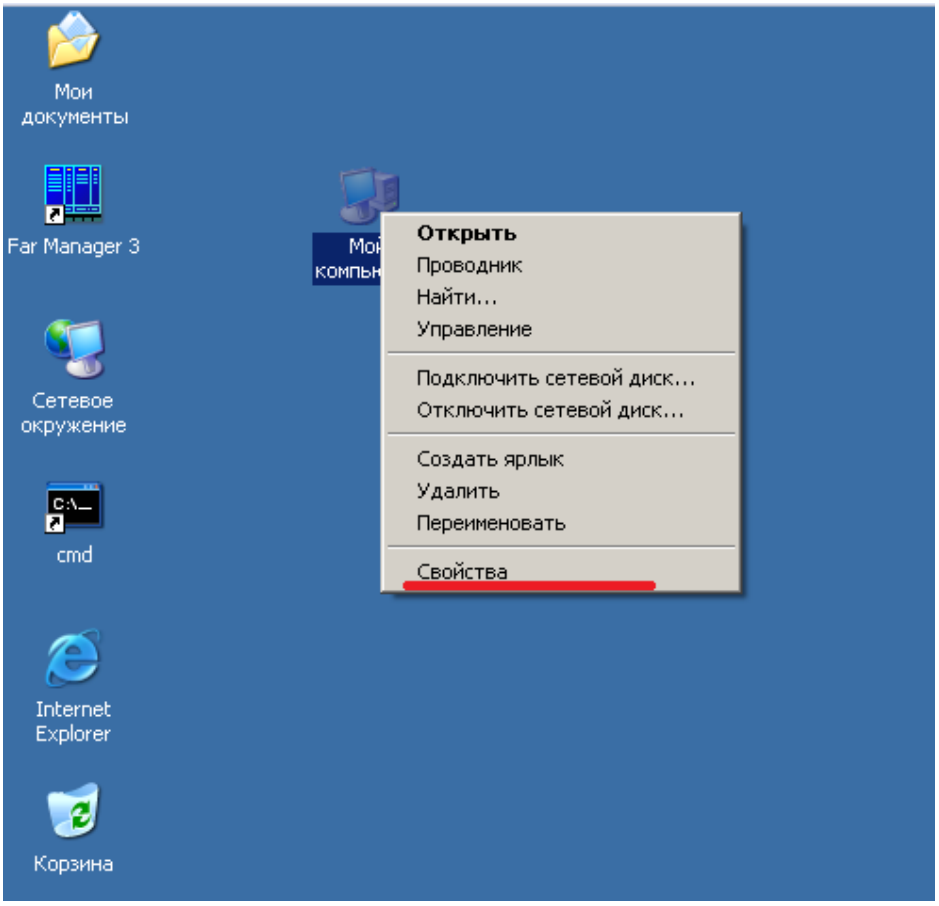


Рис. 4.1. – Свойства компьютера

Далее необходимо выбрать вкладку удаленные сеансы (рис. 4.2).

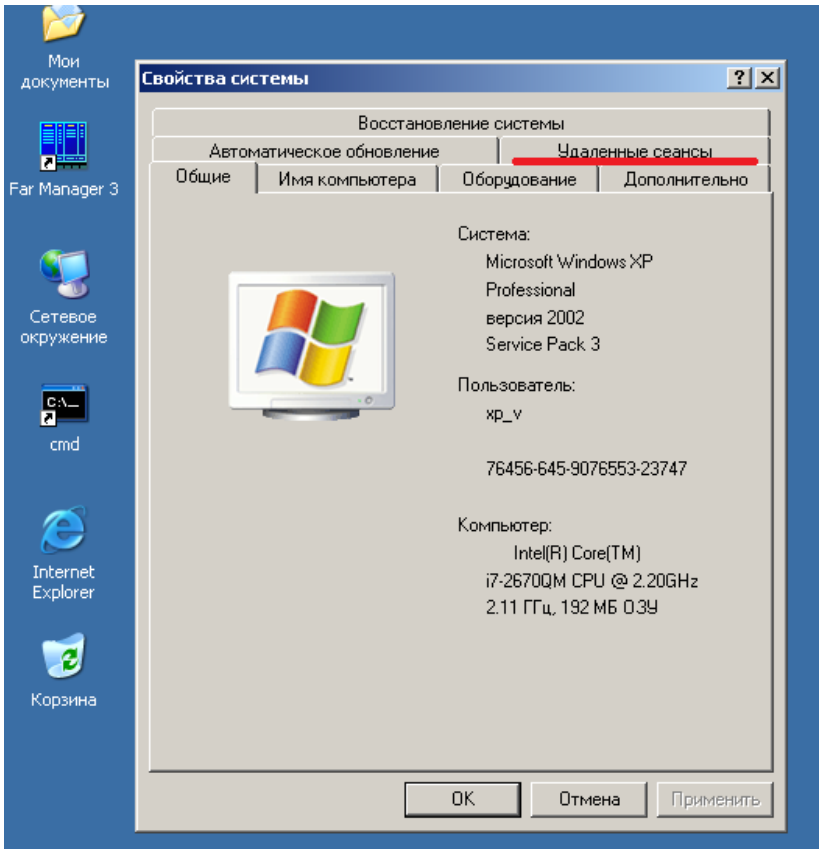


Рис. 4.2. – Удаленные сеансы

Необходимо разрешить удаленное управление рабочим столом, как показано на рис. 4.3. Кроме того в целях обеспечения безопасности пользователь осуществляющий удаленное администрирование должен иметь пароль.

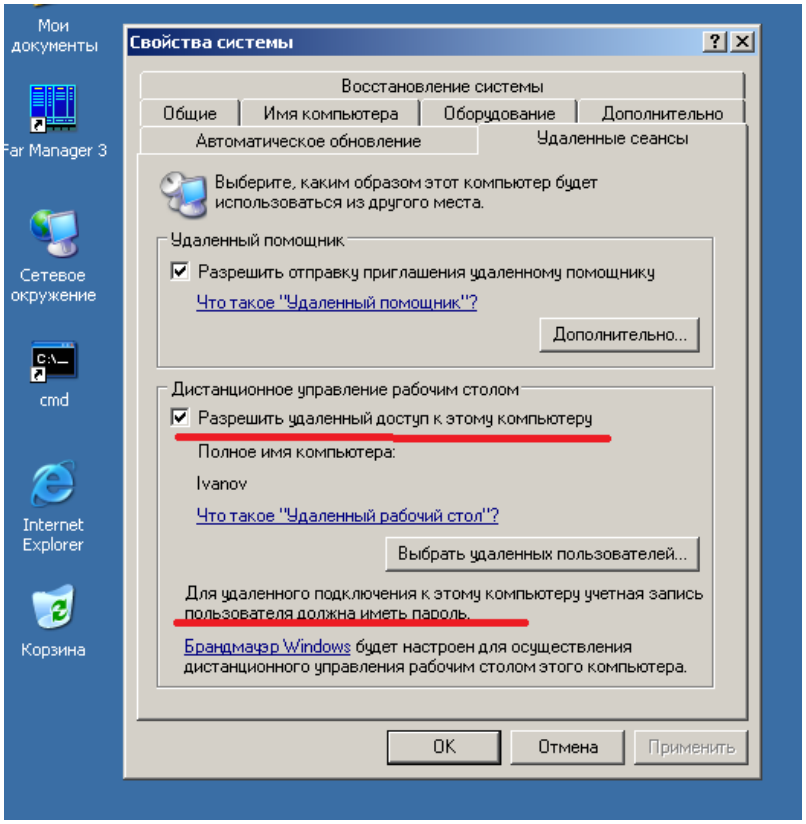


Рис. 4.3. – Удаленное управление рабочим столом

Для установки пароля необходимо открыть меню управления компьютером, как показано на рис 4.4.

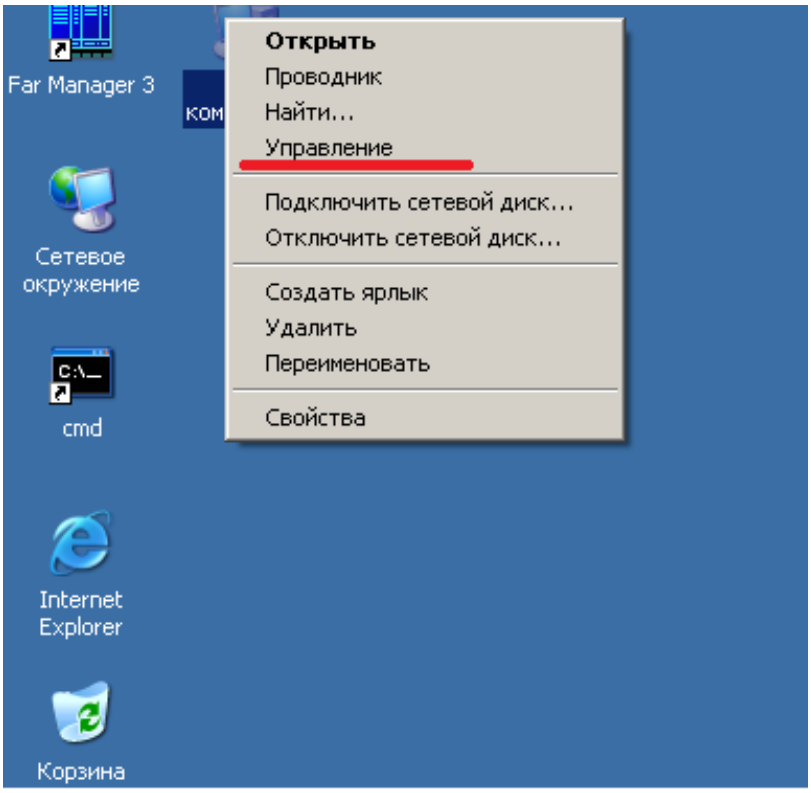


Рис. 4.4. – Управление компьютером

Далее необходимо выбрать вкладку “**Локальные пользователи**” (рис. 4.5) и произвести их настройку.

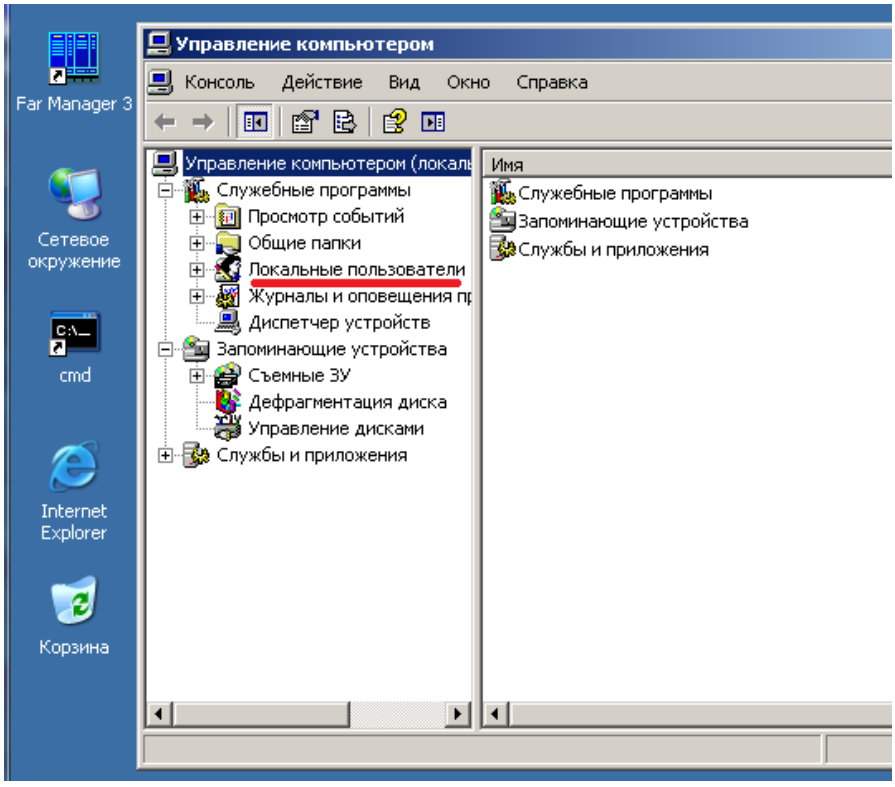


Рис. 4.5. – Управление пользователями

Для установки пароля выбираем пользователя, который будет осуществлять удаленное управление, и задаем пароль как показано на рис. 4.6.

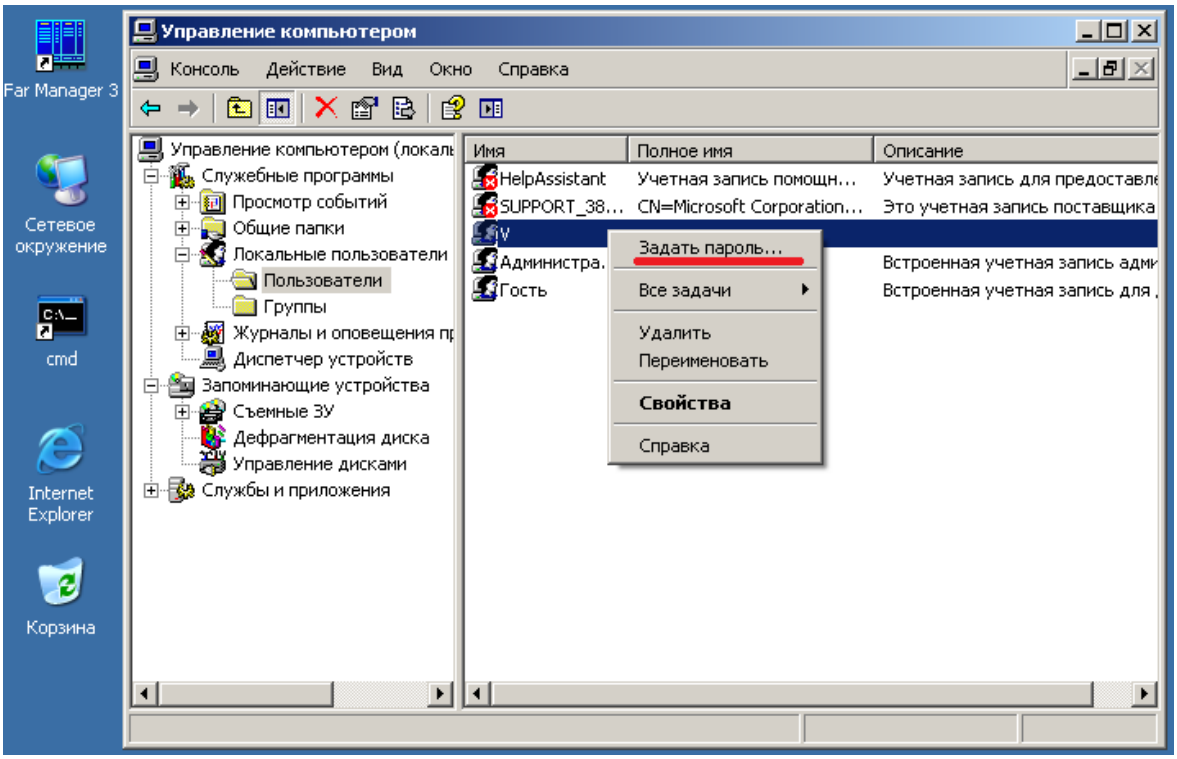


Рис. 4.6. – Установка пароля пользователя

Если пользователь, который будет удаленно управлять компьютером, не обладает правами администратора компьютера необходимо добавить его в группу пользователей удаленного рабочего стола (рис. 4.7).

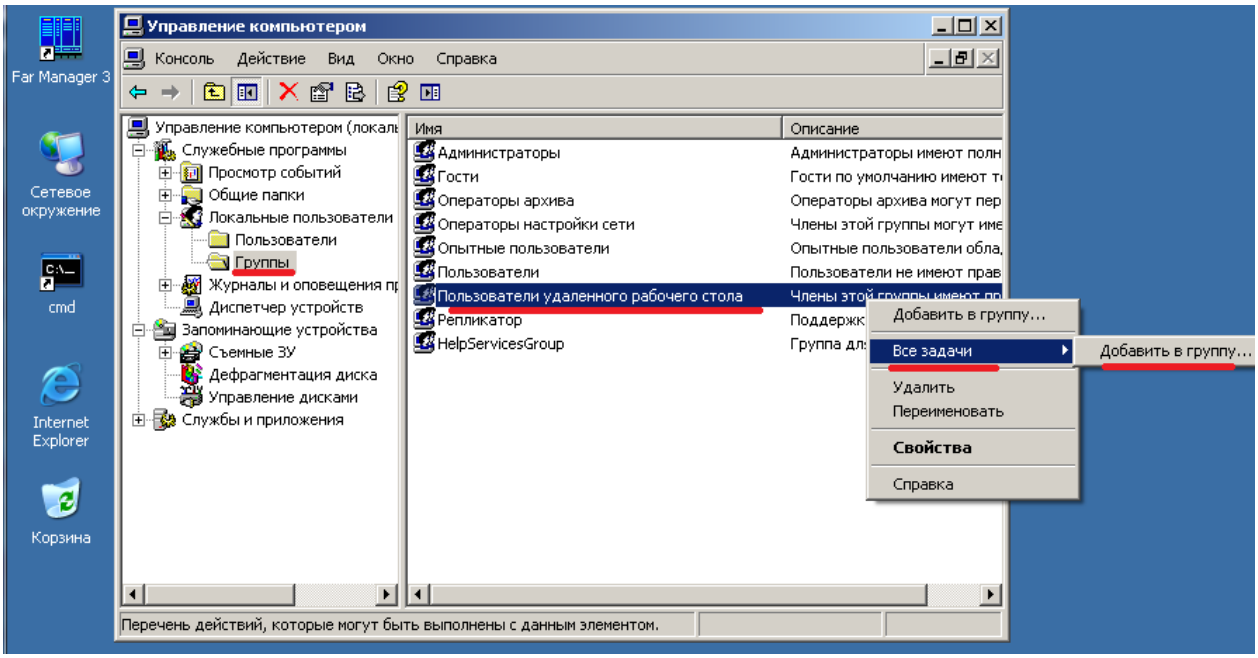


Рис. 4.7. – Пользователи удаленного рабочего стола.

Для удаленного управления компьютером необходимо знать его сетевой адрес. Адрес можно получить при помощи программы ipcofig, которую необходимо запускать из командной строки.

Командная строка находится в стандартных программах (рис. 4.8)

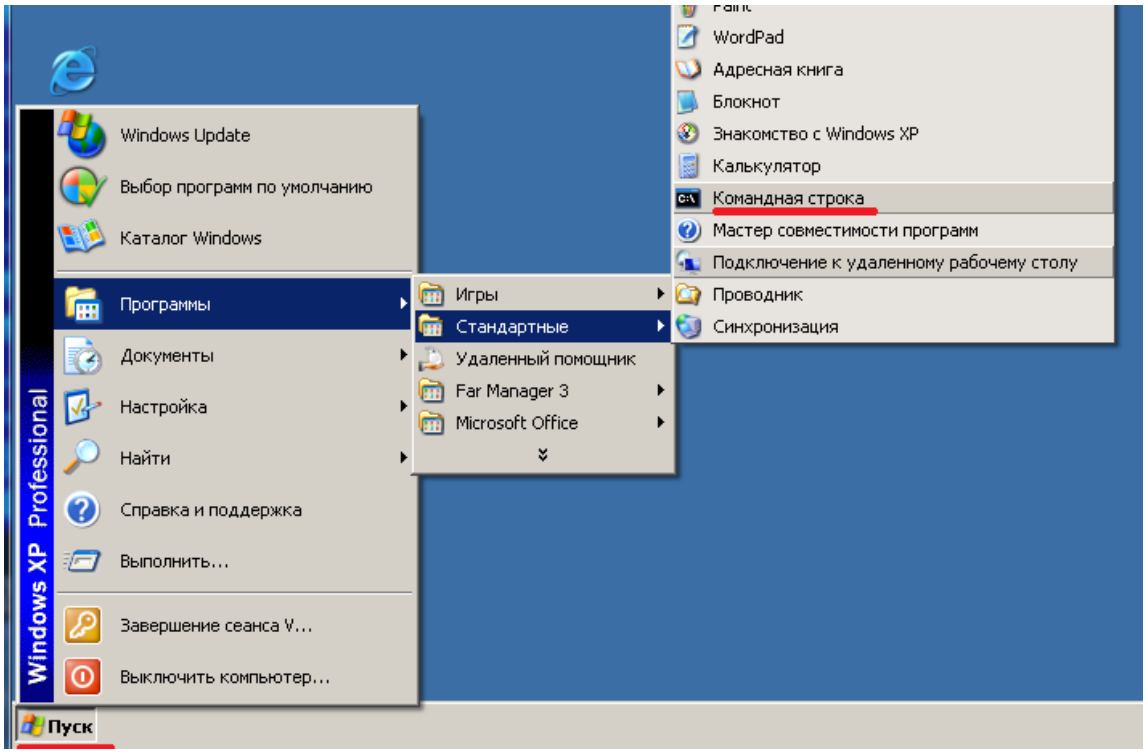


Рис. 4.8. – Командная строка ОС Windows

Результаты работы программы ipconfig показаны на рис. 4.9.

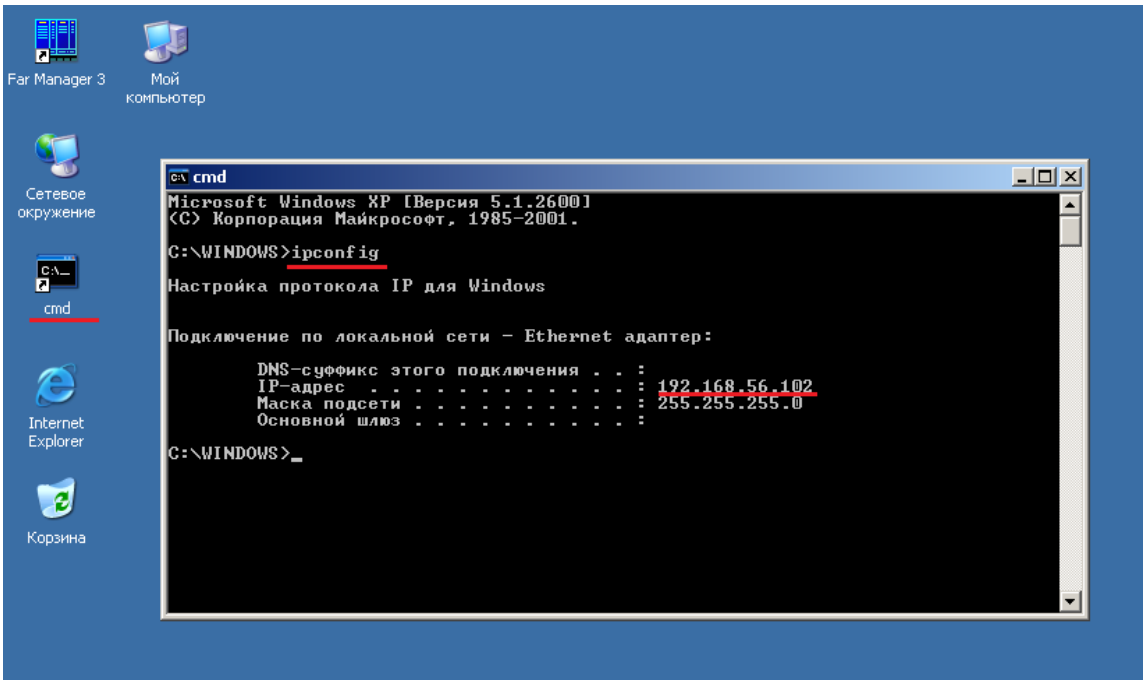


Рис. 4.9. – результаты работы программы ipconfig.

Для удаленного управления компьютером пользователь должен использовать клиентское программное обеспечение, которое в ОС Windows имеет название – “Подключение к удаленному рабочему столу” (рис. 4.10)

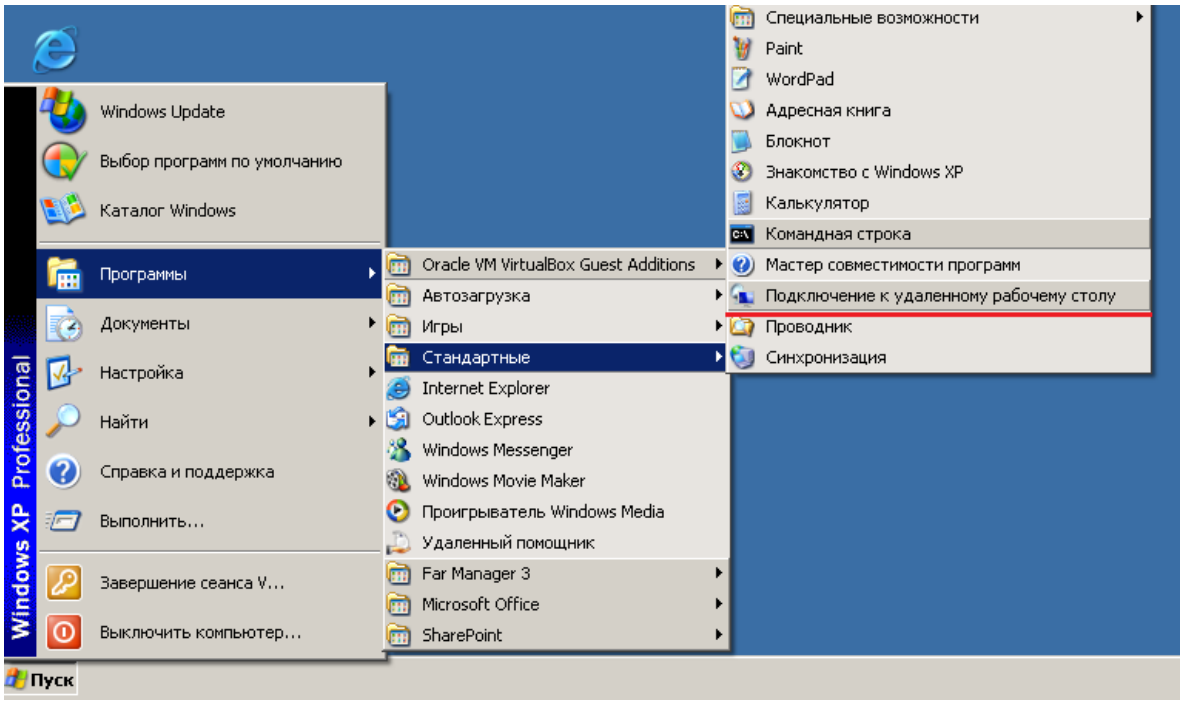


Рис. 4.10. – Подключение к удаленному рабочему столу

После запуска клиентского ПО пользователь должен ввести адрес управляемого компьютера и произвести подключение (рис. 4.11).

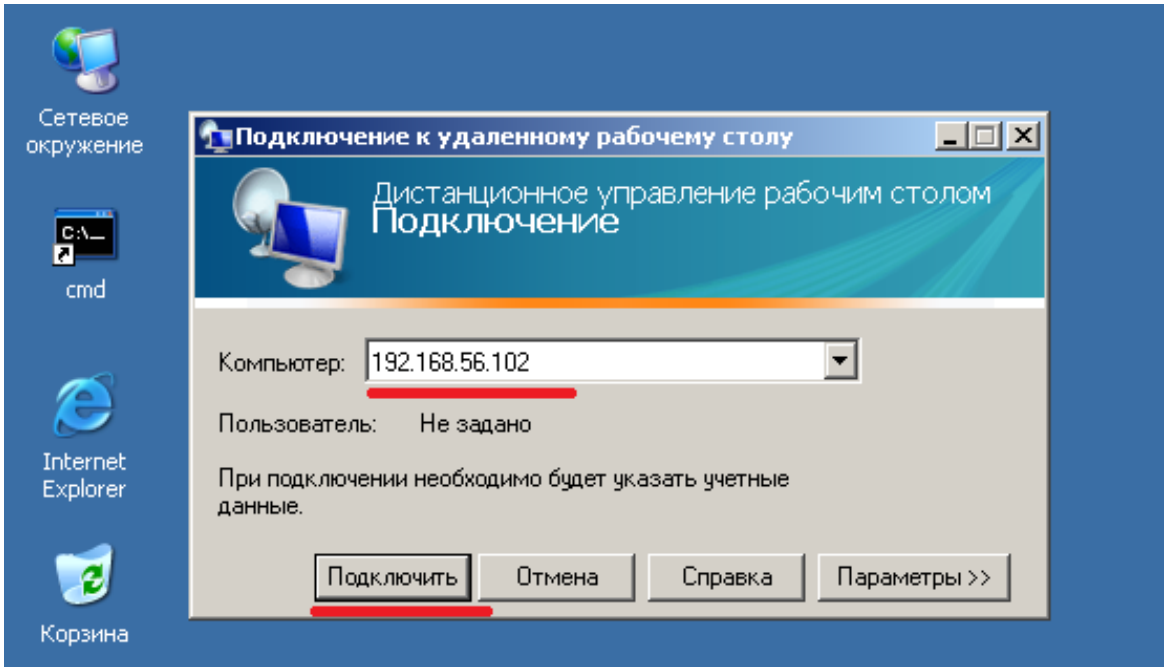


Рис. 4.11. – дистанционное управление рабочим столом.

В случае необходимости осуществлять удаленное управление компьютером при помощи VNC (для управления компьютером с ОС Linux) необходимо использовать программу VNC viewer (рис. 4.12).

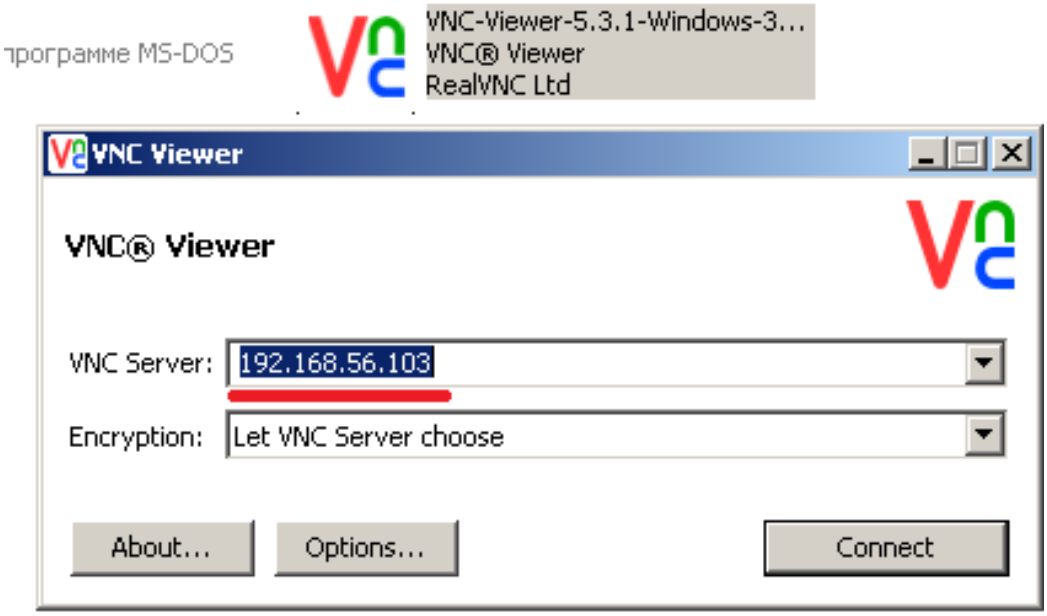


Рис. 4.12. – ПО VNC viewer

### 4.3 Организация удаленного управления компьютером с ОС Linux

Для удаленного управления компьютером необходимо на нем настроить параметры удаленного рабочего стола (рис. 4.13).

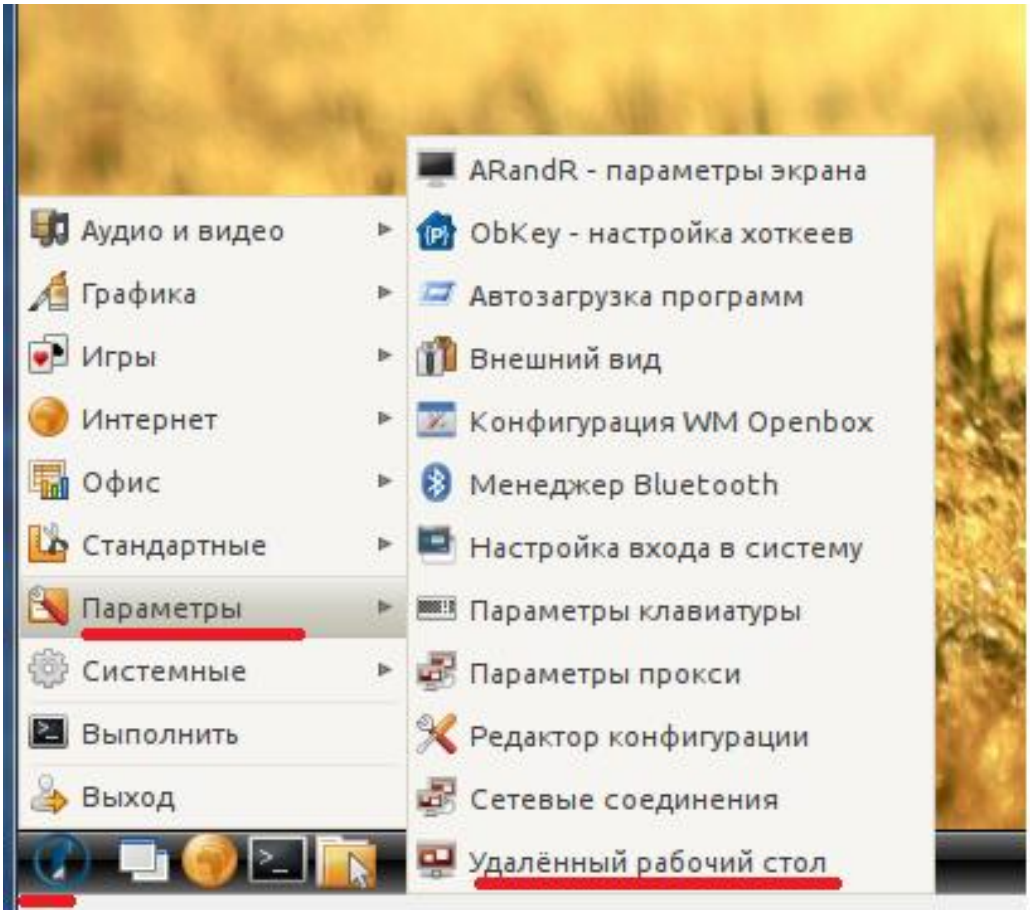


Рис. 4.13. – Настройка удаленного рабочего стола

После запуска ПО настройки удаленного рабочего стола необходимо разрешить другим пользователям видеть рабочий стол и управлять им. Также можно

узнать адрес компьютера для подключения по сети и настроить параметры безопасности (рис. 4.14.).

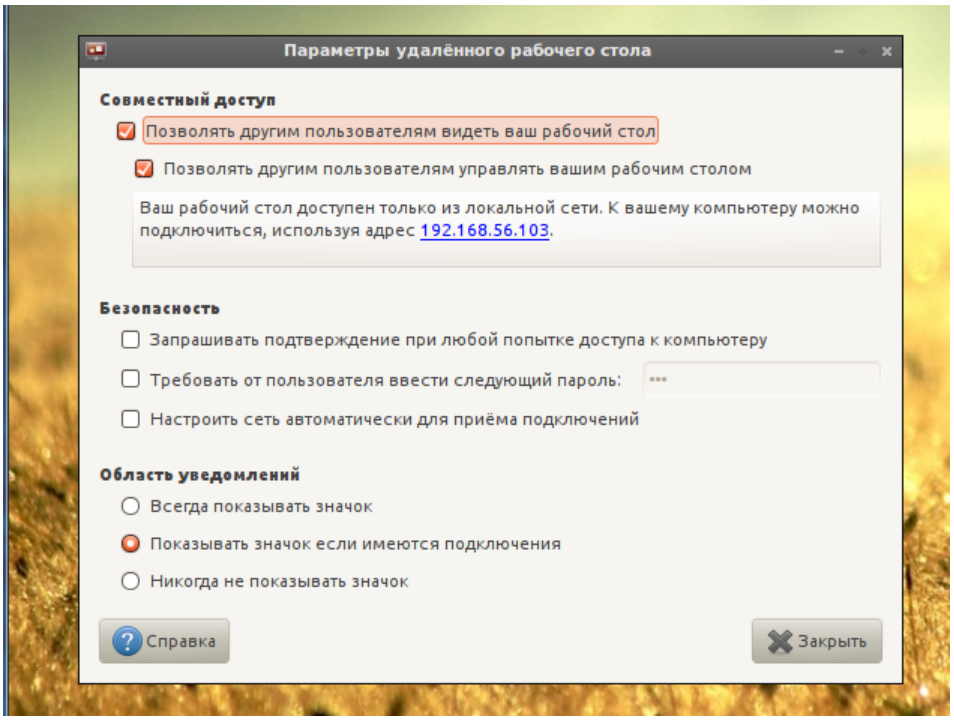


Рис. 4.14. – Параметры удаленного рабочего стола

Для обеспечения удаленного управления компьютером необходимо настроить ПО терминального клиента. Часто для удаленного управления используется терминальный клиент Remmina, который поддерживает несколько протоколов для удаленного управления (рис. 4.15)

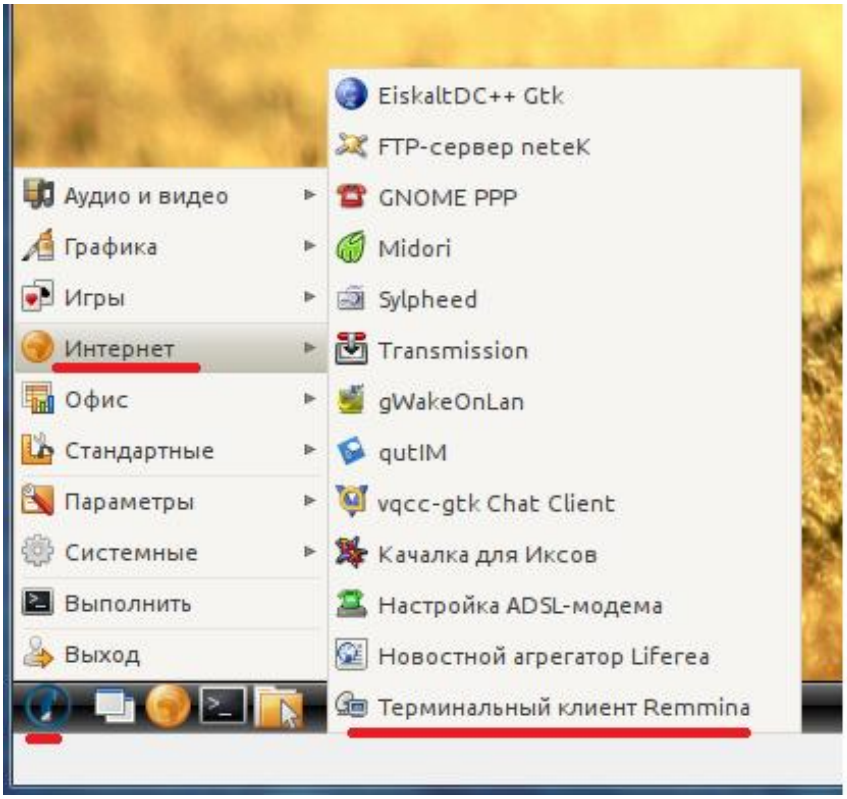


Рис. 4.15. – Терминальный клиент Remmina

Главное окно терминального клиента Remmina, в котором производится добавление нового соединения с удаленным компьютером показано на рис. 4.16.

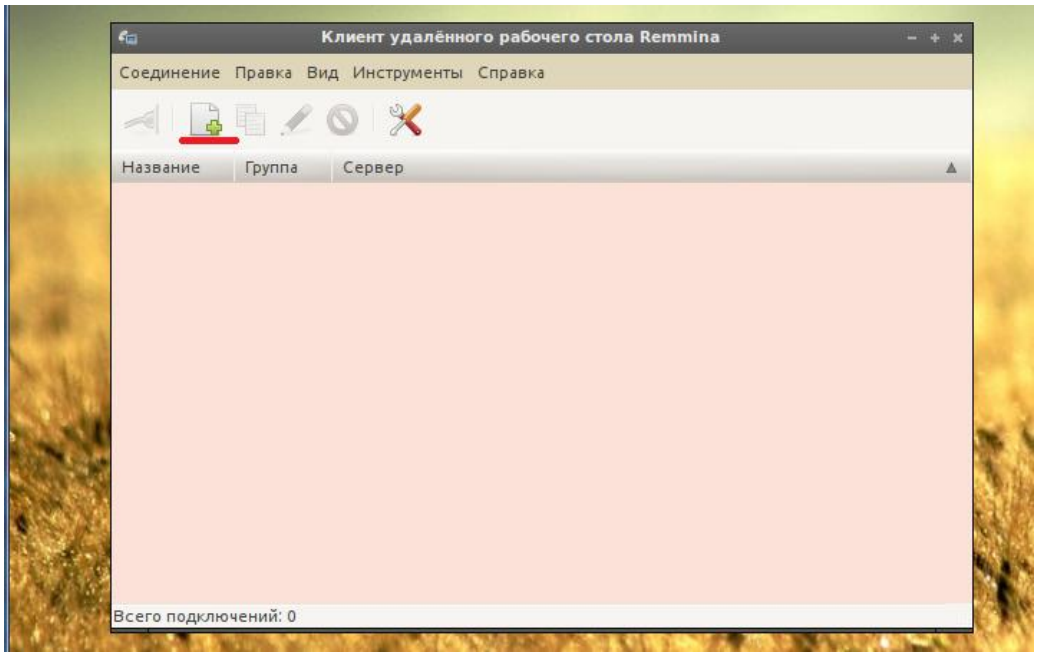


Рис. 4.16. – Добавление соединения с удаленным компьютером

Для установки параметров подключения к удаленному компьютеру необходимо придумать его название и выбрать протокол (RDP или VNC) (рис. 4.17).

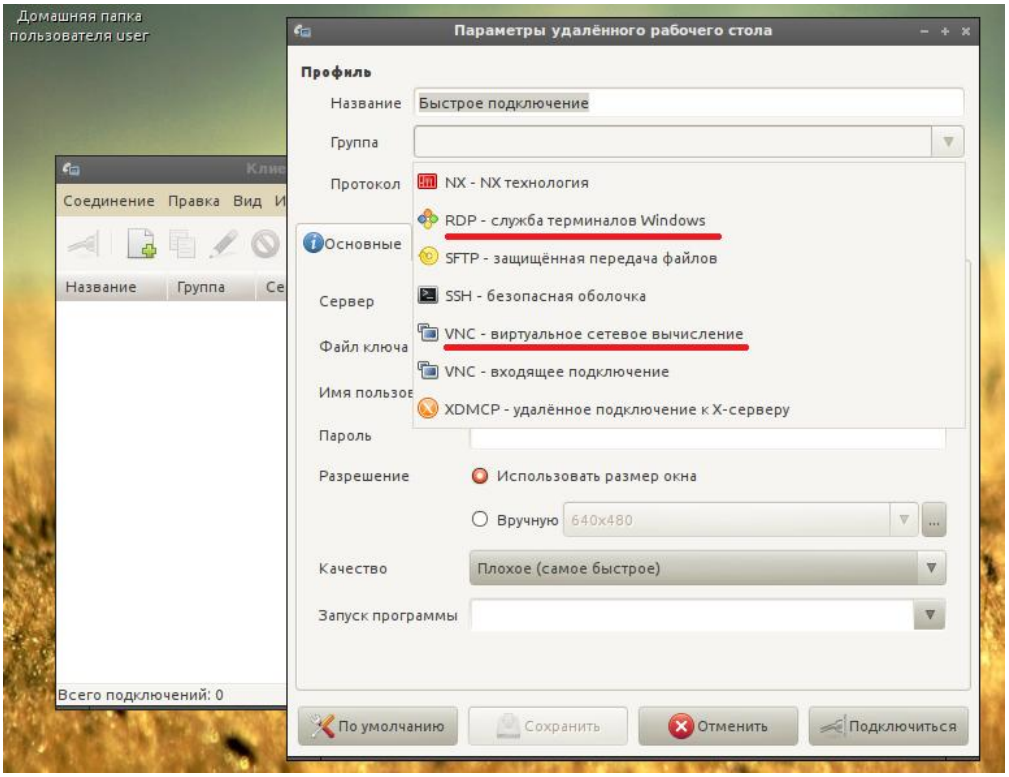


Рис. 4.17. – Настройка параметров подключения к удаленному рабочему столу

На следующем этапе необходимо ввести сетевой адрес удаленного компьютера, а также можно настроить имя пользователя и пароль для автоматического входа в систему на удаленном компьютере и параметры качества отображения удаленного рабочего стола (разрешение и глубину цвета) (рис. 4.18).

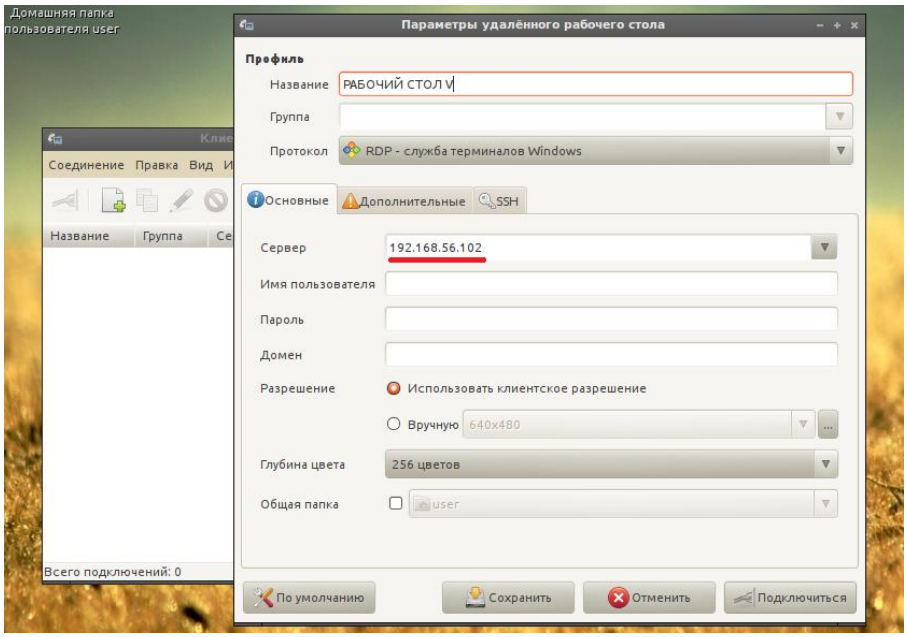


Рис. 4.18. – Настройка параметров подключения к удаленному компьютеру

### 4.4 Технические средства для выполнения работы.

Компьютерный класс с установленной **ОС Windows** и **Oracle VM VirtualBox**.

### 4.5 Порядок выполнения лабораторной работы

1. Запустить Oracle VM VirtualBox Менеджер.
2. Придумать имя для двух ВМ (имя должно содержать вашу фамилию и группу)
3. Создать две ВМ типа Windows XP (RAM -192 MB, файл образа – c:/xp.vdi, у виртуального носителя должен быть атрибут “множественное подключение”)
4. В настройках сети ВМ установить тип подключения “виртуальный адаптер хоста”
5. Запустить виртуальные машины, поменять имена компьютеров (имена должны содержать вашу фамилию и номер машины 1,2)
6. Перезагрузить ОС на виртуальных машинах.
7. Произвести настройку свойств ОС виртуальной машины №2 для обеспечения удаленного доступа к ней.
8. Установить удаленное управление виртуальной машиной №2 при помощи виртуальной машины №1.
9. Выключить виртуальную машину №1.
10. Создать ВМ типа Other (RAM -640 MB, файл образа – **c:/rt_00.vdi**, у виртуального носителя должен быть атрибут “множественное подключение”)
11. Произвести запуск виртуальной машины с ОС Runtu (имя – user, пароль - user).
12. Поменять имя компьютера с ОС Runtu при помощи программы MC (имя должно содержать вашу фамилию и символ “1”, использовать латинские символы).

13. Настроить терминальный клиент Remmina для удаленного управления виртуальной машиной №2 с ОС Windows.
14. Установить удаленное управление виртуальной машиной №2 с ОС Windows при помощи виртуальной машины с ОС Runtu.
15. Создать вторую ВМ типа Other (RAM -640 MB, файл образа – **c:/rt_00.vdi**, у виртуального носителя должен быть атрибут “множественное подключение”)
16. Произвести запуск виртуальной машины с ОС Runtu (имя – user, пароль - user).
17. Поменять имя компьютера с ОС Runtu при помощи программы MC (имя должно содержать вашу фамилию и символ “**2**”, использовать латинские символы).
18. Настроить параметры удаленного рабочего стола второй ВМ с ОС Runtu для возможности удаленного управления.
19. Настроить терминальный клиент Remmina первой ВМ для удаленного управления второй виртуальной машиной с ОС Runtu.
20. Установить удаленное управление второй виртуальной машиной с ОС Runtu при помощи первой виртуальной машины с ОС Runtu.
21. Скопировать через общую папку на диск **C:/** виртуальной машины с ОС Windows ПО VNC viewer с хост-машины (файл C:/VNC-Viewer-5.3.1-Windows-32bit)
22. Запустить VNC viewer и установить удаленное управление второй виртуальной машиной с ОС Runtu.

### 4.6 Содержание отчета о выполнении лабораторной работы

Отчёт должен содержать:
- титульный лист;
- цель исследования;
- ход работы;
- выводы.

Отчёт по лабораторной работе должен быть выполнен в соответствии требованиями ГОСТ.

### 4.7 Порядок защиты работы

Защита производится при наличии отчета за компьютером и состоит в демонстрации навыков удаленного управления компьютерами при выполнении задания выданного преподавателем.

### 4.8 Контрольные вопросы

1. Что такое удаленное управление?
2. Каковы основные возможности RDP и VNC?
3. Каковы основные этапы настройки удаленного управления?
4. Для чего служит ПО Remmina?
5. Для чего служит ПО VNC viewer?

# 5. ЛАБОРАТОРНАЯ РАБОТА № 5 КРИПТОГРАФИЧЕСКАЯ ЗАЩИТА ДАННЫХ

Цель работы - знакомство с основными возможностями ПО для криптографической защиты данных.

## 5.1 Криптографическая защита данных

Защита информации от исследования и копирования предполагает криптографическое закрытие защищаемых от хищения данных. Задачей криптографии является обратимое преобразование некоторого понятного исходного текста (открытого текста) в кажущуюся случайной последовательность некоторых знаков, часто называемых шифротекстом, или криптограммой[1, с. 540].

В шифре выделяют два основных элемента — алгоритм и ключ.

Алгоритм шифрования представляет собой последовательность преобразований обрабатываемых данных, зависящих от ключа шифрования.

Ключ задает значения некоторых параметров алгоритма шифрования, обеспечивающих шифрование и дешифрование информации. В криптографической системе информация и ключ являются входными данными для шифрования и дешифрования информации.

По способу использования ключей различают два вида криптографических систем: с симметричным и с несимметричным(асимметричным) ключом[1, с. 541].

В симметричных (одноключевых) криптографических системах ключи шифрования и дешифрования либо одинаковы, либо легко выводятся один из другого.

В асимметричных (двухключевых или системах с открытым ключом) криптографических системах ключи шифрования и дешифрования различаются таким образом, что с вычислений нельзя вывести один ключ из другого.

Рассмотрим работу программ шифрования на примере GnuPG - Gnu Privacy Guard (gpg)[11]. Это свободная программа для шифрования информации и создания электронных цифровых подписей. Она выпущена под свободной лицензией GNU General Public License[4].

Часто, gpg уже предустановлен в ОС Linux. Чтобы это проверить, используют команду gpg --version. Если программа не установлена, можно установить её, используя менеджер пакетов.

В ОС Windows программу можно установить из файла, а затем для удобства добавить директорию, в которой после установки находится файл gpg.exe в системный путь /PATH.

Путь к установленной программе можно посмотреть в проводнике (рис. 5.1)

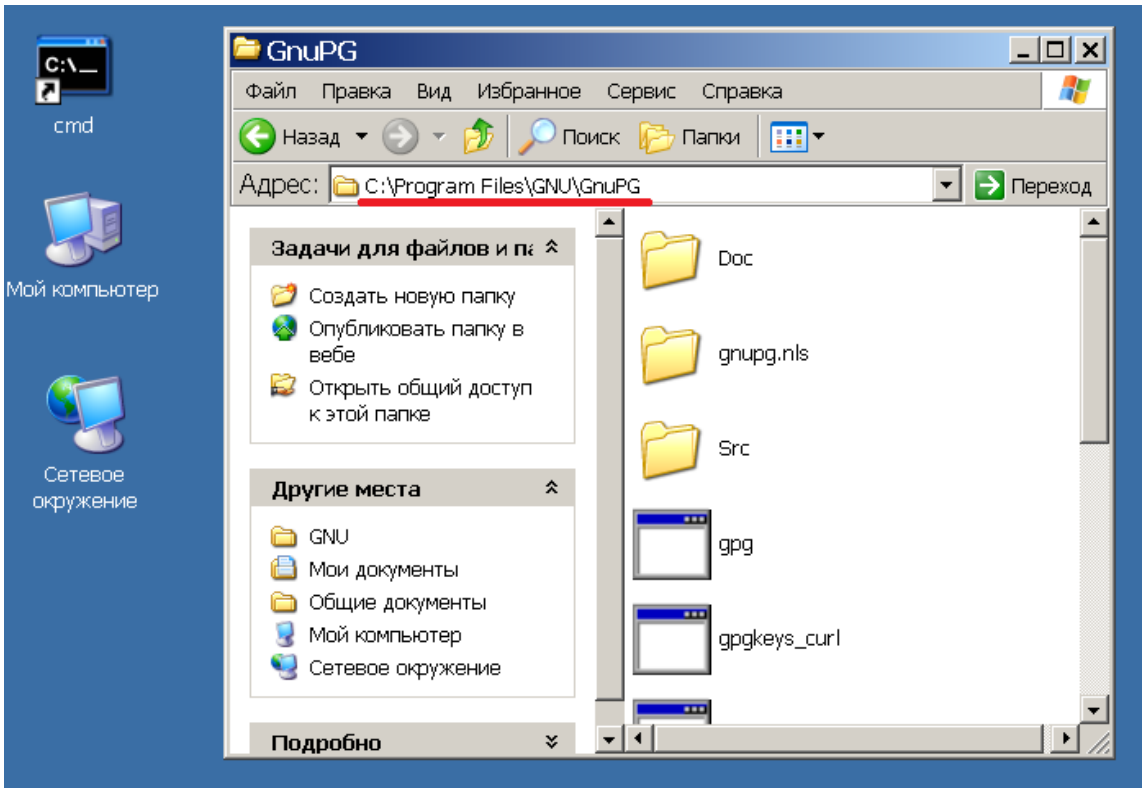


Рис. 5.1. – Путь к установленной программе gpg

Добавление пути к программе gpg производится в свойствах компьютера (рис. 5.2)

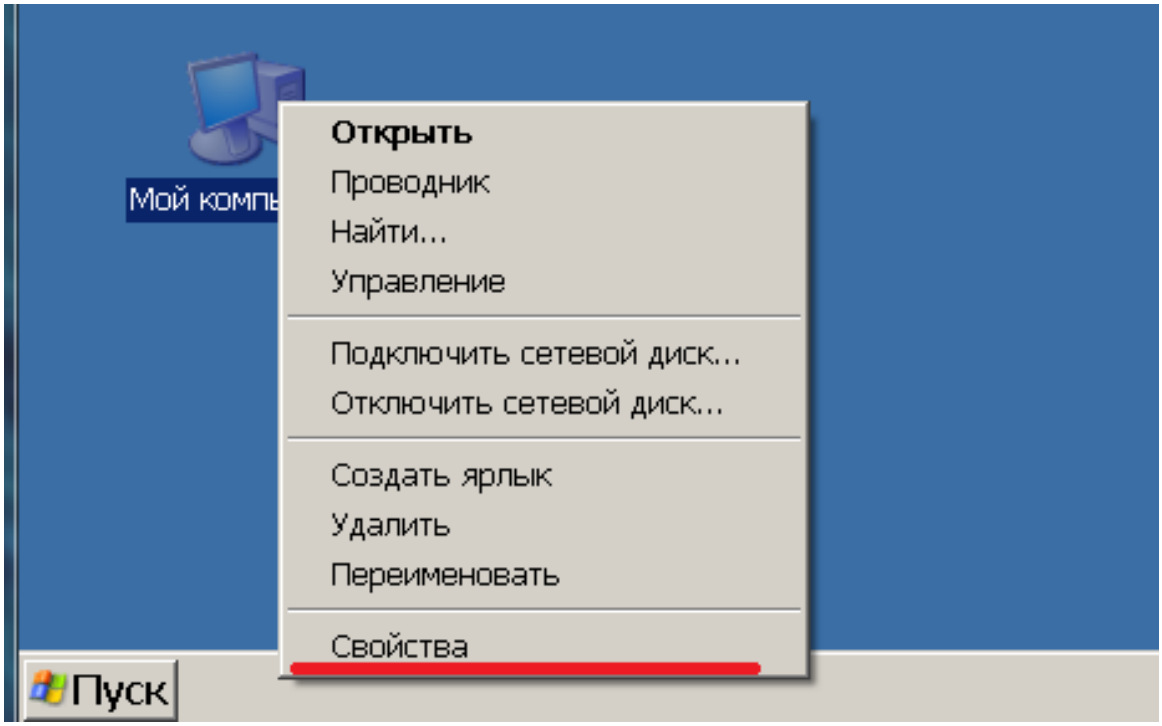


Рис. 5.2. – Свойства компьютера

В свойствах компьютера необходимо открыть вкладку "**Дополнительно**" и настроить переменные среды (рис. 5.3)

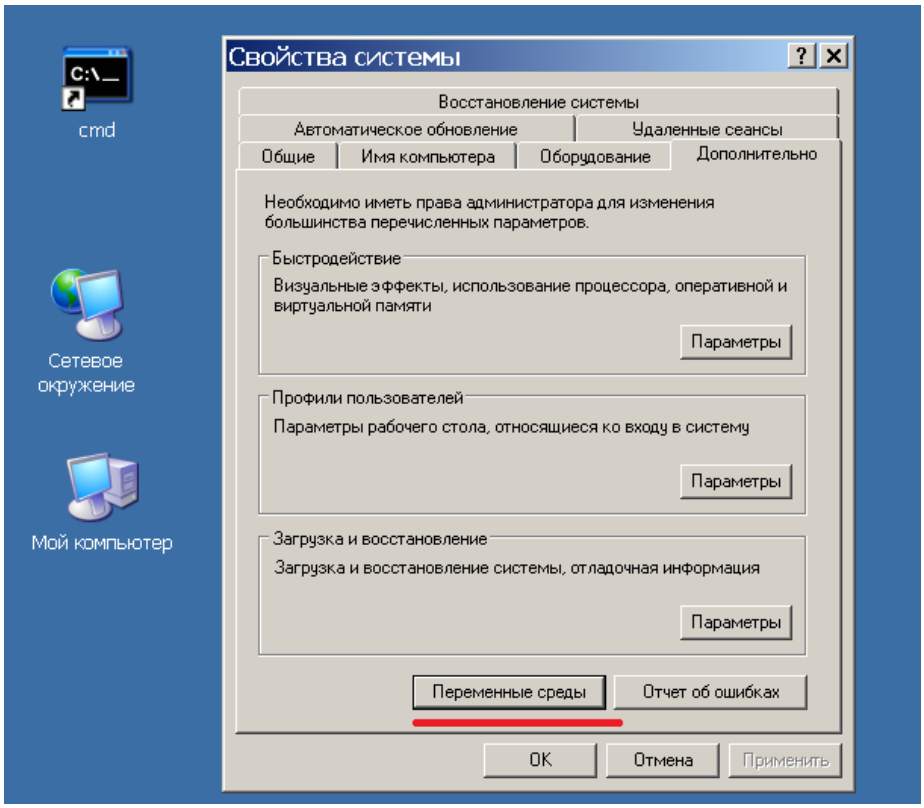


Рис. 5.3. – Переменные среды

Необходимо выбрать системную переменную **Path** и изменить ее (рис. 5.4)

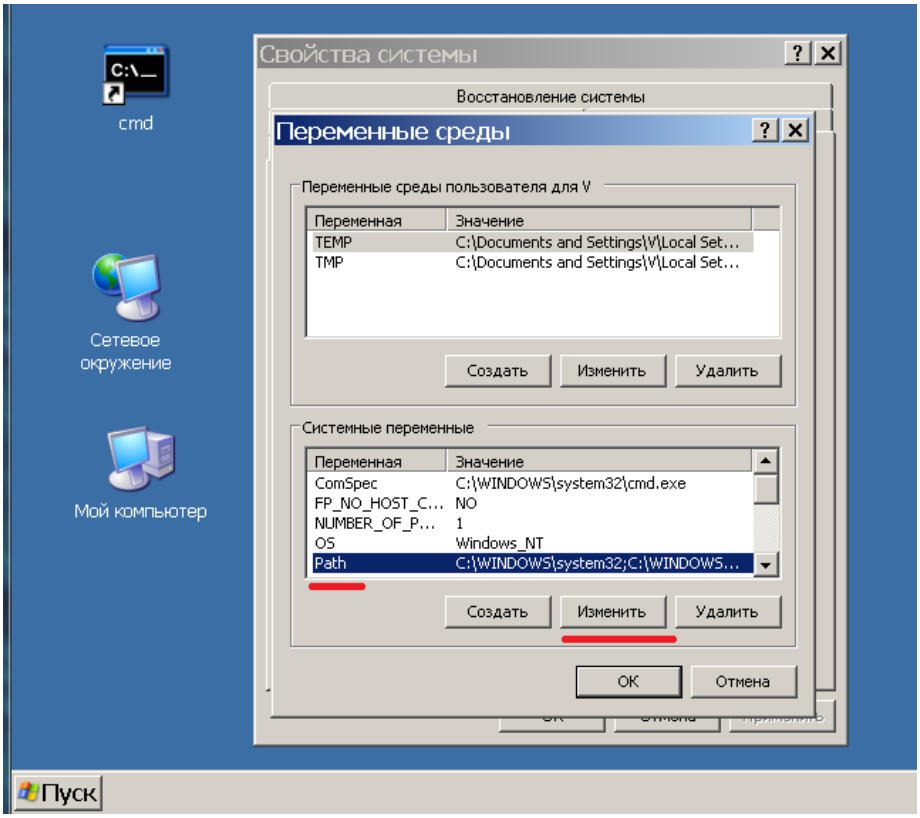


Рис. 5.4. – Изменение системной переменной Path

Производится добавление пути к программе **gpg** путем дописывания строки к значению переменной **Path**. Строки в переменной **Path** отделяются при помощи символа "**;**" (рис. 5.5).

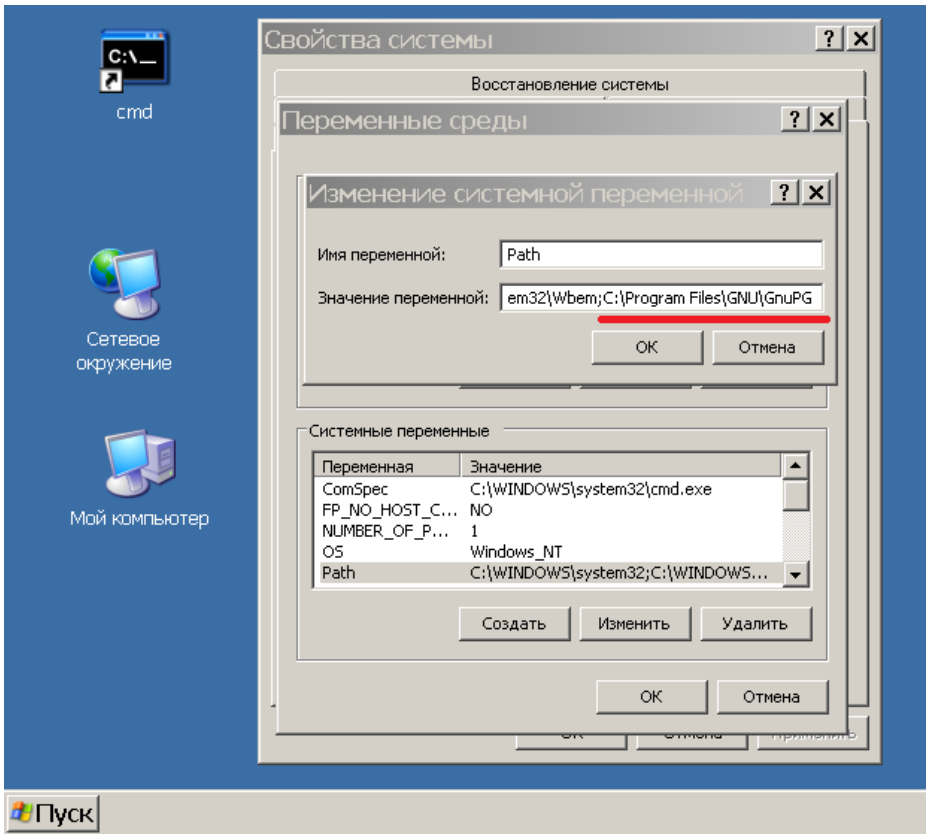


Рис. 5.5. – Добавление строки в **Path**

Текущее значение переменной **Path** можно увидеть при помощи соответствующей команды в строке (рис. 5.6)

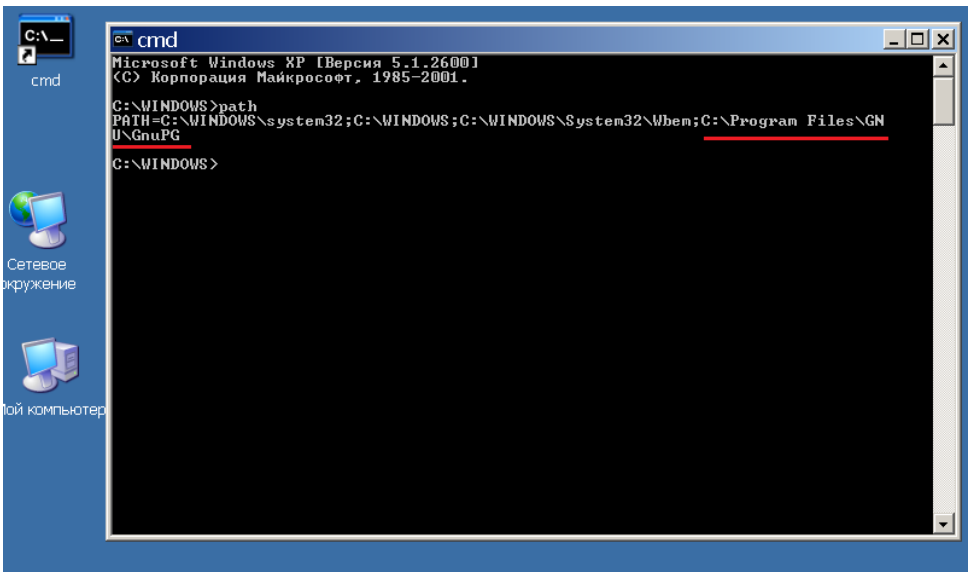


Рис. 5.6. – Текущее значение переменной Path

### 5.2 Симметричное шифрование

При симметричном шифровании секретный пароль используется, для того чтобы зашифровать и расшифровать файл.

Для шифрования используется командная строка:

**gpg -c /путь/filename**

Если необходимо зашифровать файл в текущем каталоге:

**gpg -c filename**

Если вы хотите для зашифровки использовать другой алгоритм, то можете указать это параметром --cipher-algo.

Список доступных алгоритмов вы можно посмотреть командой gpg --version (рис. 5.7).

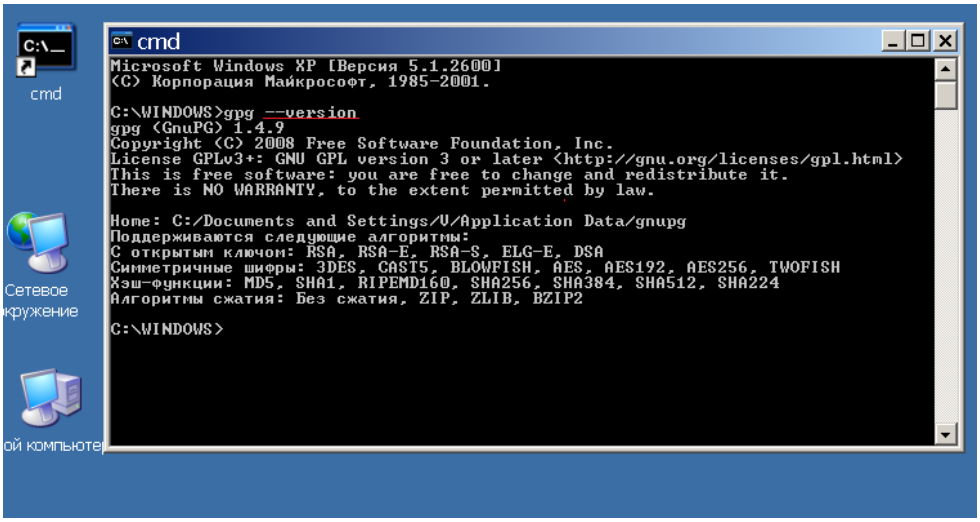


Рис. 5.7. – Список доступных алгоритмов gpg

Например для того, что бы зашифровать файл алгоритмом AES256, можно воспользоваться командой:

**gpg --cipher-algo AES256 -c /путь/ filename**

Если вы шифруете файл, лежащий в текущем каталоге

**gpg --cipher-algo AES256 -c filename**

Перед шифрованием программа попросит вас ввести пароль и повторить его (рис. 5.8)

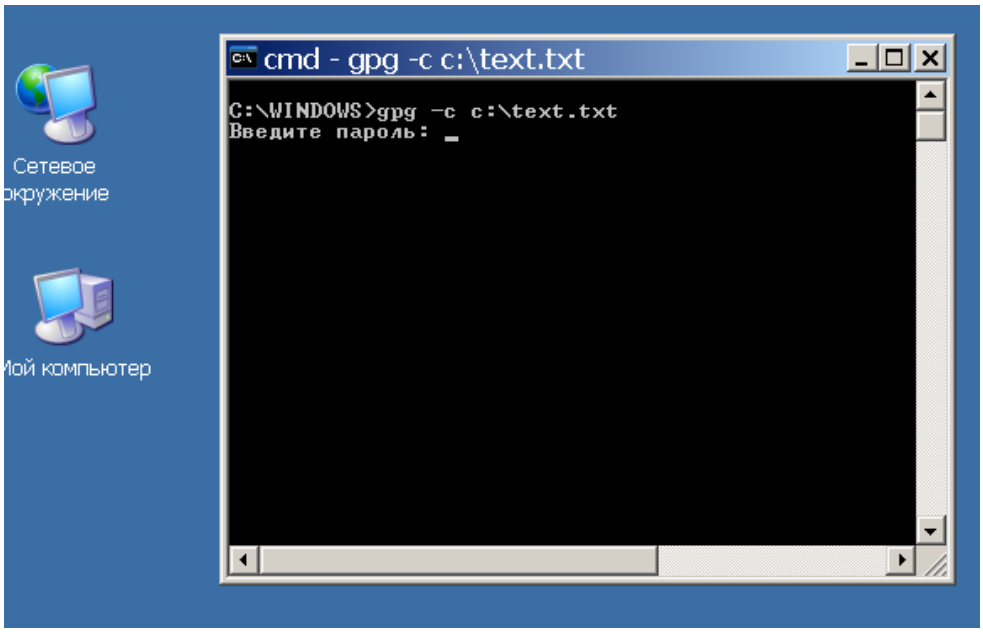


Рис. 5.8. – Шифрование файла

По окончании работы программа **gpg** создаст зашифрованный файл с расширением gpg в том же каталоге где находился исходный файл(рис. 5.9).

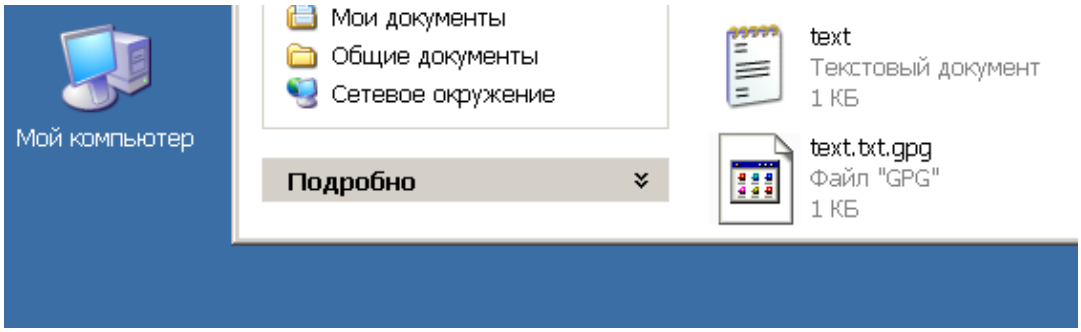


Рис. 5.9. – Результат шифрования файла

Для расшифровки файла необходимо использовать параметр **--decrypt-files**

**gpg --decrypt-files /путь/filename**
**filename** - зашифрованный файл**.**

Если зашифрованный файл имеет расширение **gpg** то параметр можно не указывать

**gpg filename.gpg**

При расшифровке программа сохраняет расшифрованный файл в исходный каталог с тем же именем без расширения **gpg.** Если файл с таким именем в каталоге уже существует, то программа предлагает ввести новое имя файла(рис. 5.10).

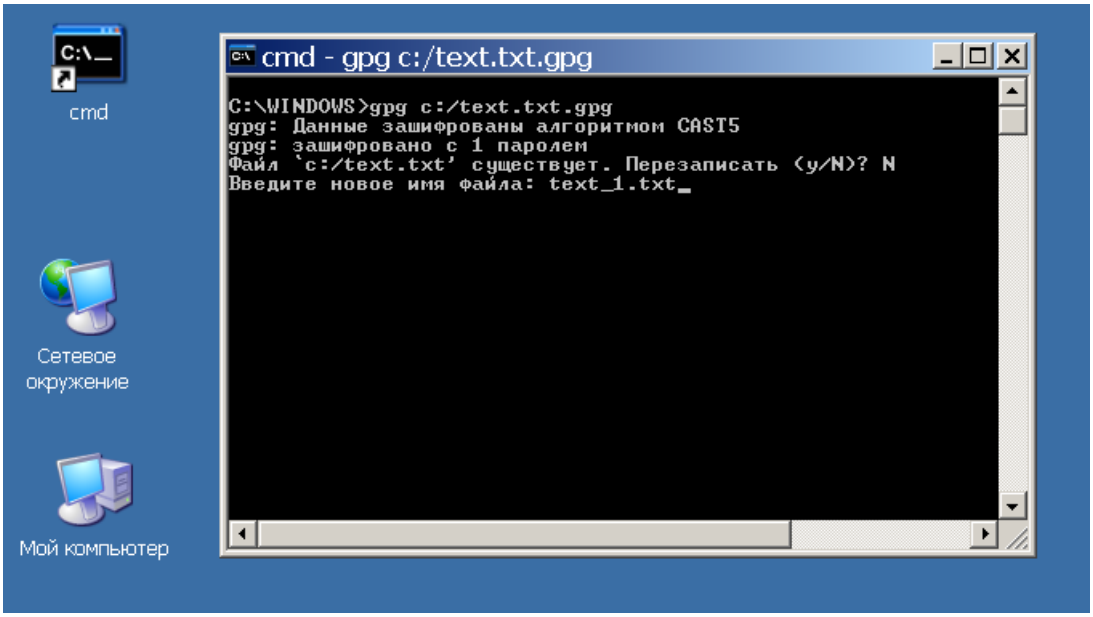


Рис. 5.10. – Расшифровка файла

### 5.3 Ассиметричное шифрование

Недостатком симметричного шифрования является то, что когда отправляется зашифрованный файл, необходимо передать получателю и секретный пароль, который может быть перехвачен.

Ассиметричное шифрование решает эту проблему использованием двух паролей.

Один - публичный, который раздаётся всем желающим, второй - личный секретный пароль, который знает только владелец.

Несимметричность этого метода состоит в том, что сообщение шифруется при помощи публичного пароля, а расшифровано может быть только при помощи личного (секретного).

При этом секретный пароль никуда не передаётся и не может попасть в чужие руки.

Чтобы создать свою пару ключей необходимо запустить следующую команду:

**gpg --gen-key**

Необходимо выбрать тип ключа - 1, размер ключа и срок действительности по умолчанию(рис. 5.11).

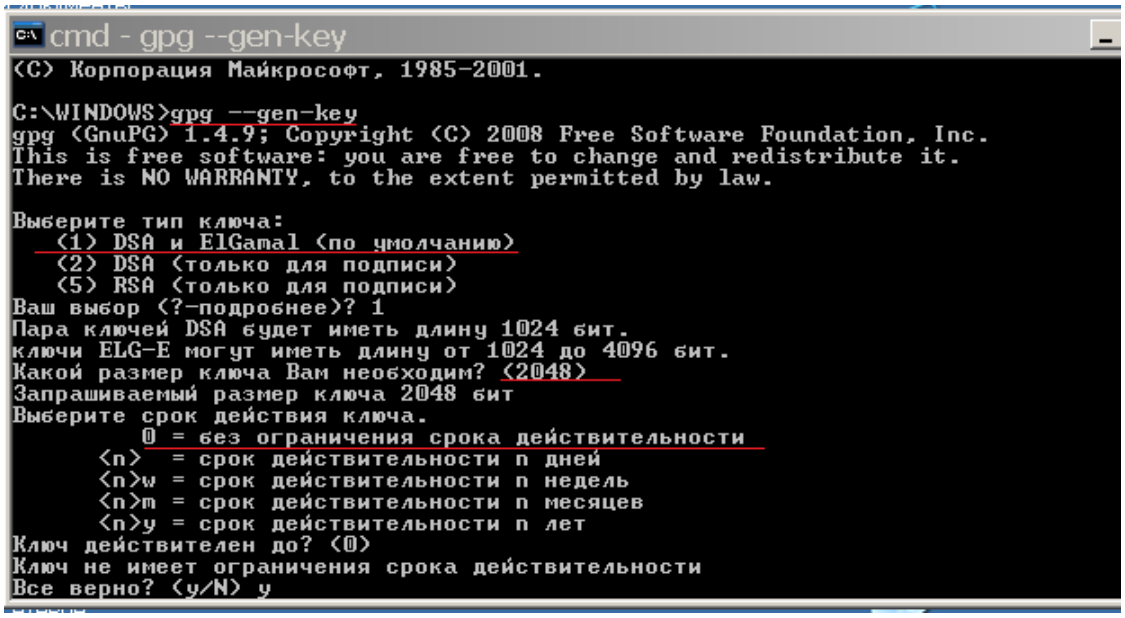


Рис. 5.11. – Параметры ключей

Далее программа попросит Вас ввести пароль для секретного ключа, **который необходимо запомнить**. Он будет использоваться Вами при расшифровке.

После этого начнется создание ключей , при этом желательно производить печать на клавиатуре случайных символов или перемещать мышь (рис. 5.12).

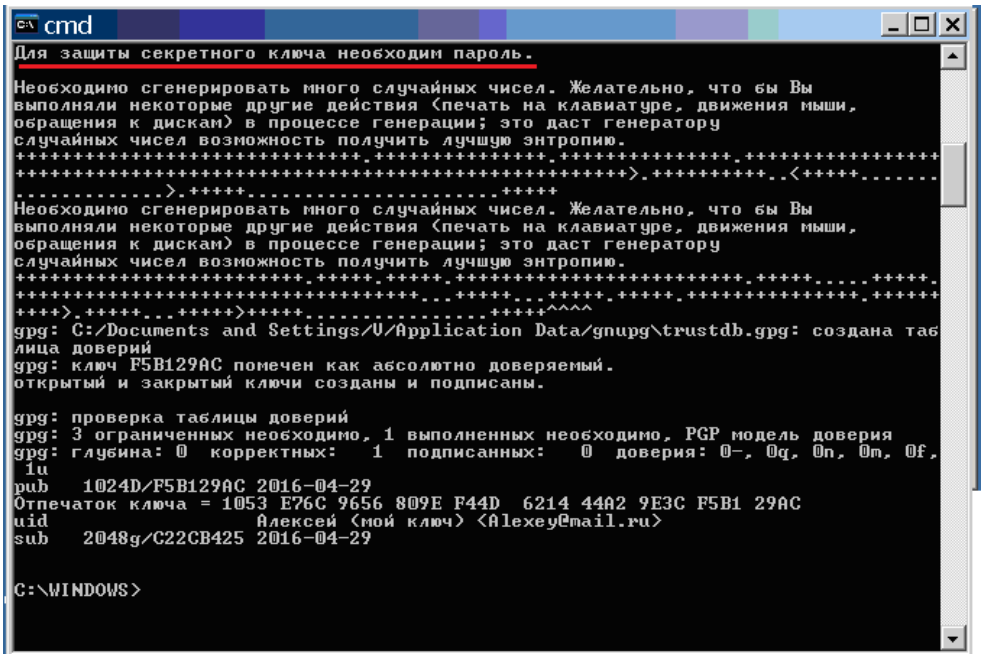


Рис. 5.12. – Создание ключей.

Созданные ключи попадают в копилку ключей.

Для просмотра ключей можно использовать команду

**gpg --list-keys**

результат работы которой представлен на рис. 5.13

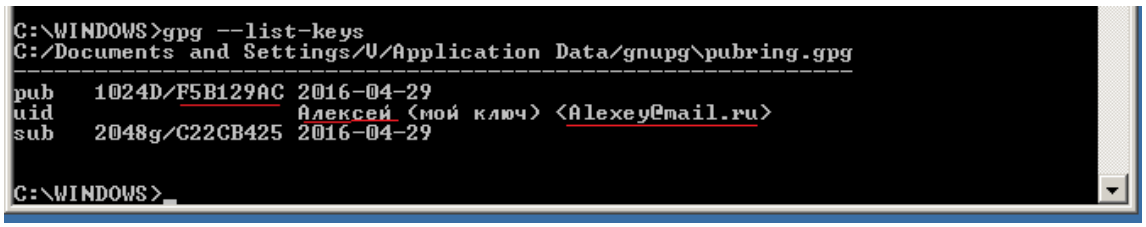


Рис. 5.13. – Информация о ключах

Число F5B129AC в первой строчке, это **id** ключа. Если понадобится обратиться к ключу в коллекции, то необходимо будет указать либо его id, либо почтовый адрес (в примере Alexey@mail.ru).

Один из двух созданных ключей является публичным. Этот ключ необходимо сделать доступным для всех отправляющих вам зашифрованные сообщения. Для удобства размещения публичного ключа на сайтах и пересылки почтой ключ можно экспортировать в текстовый файл.

Команда экспорта публичного ключа:

**gpg --output my_1_key_pub.txt --armor --export F5B129AC**

или

**gpg --output my_1_key_pub.txt --armor --export Alexey@mail.ru**

В этом примере:

**my_key_1_pub.txt** - название файла, куда будет сохранён ключ (в данном случае в текущем каталоге);

**--armor** означает, что файл будет текстовым (по умолчанию создаётся бинарный).

Экспортированный ключ может быть просмотрен в редакторе (рис. 5.14)

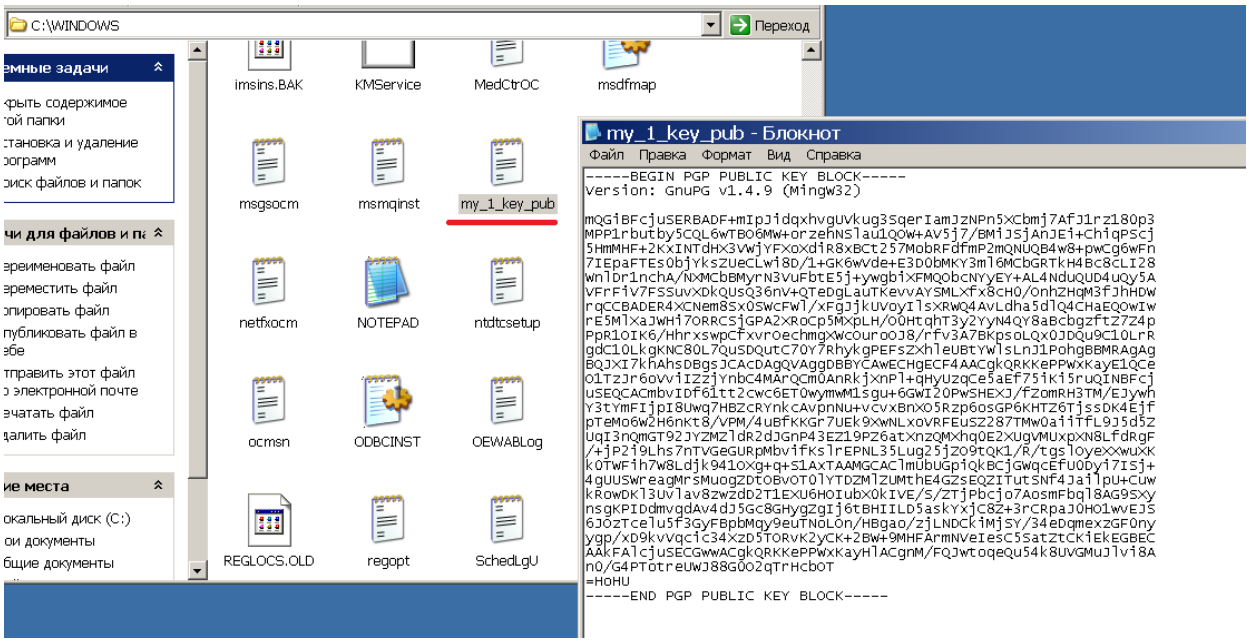


Рис. 5.14. – Экспортированный ключ

Файл с экспортированным публичным ключом должен быть выложен в доступное для других пользователей место, например в каталог к которому есть общий доступ или в общую папку ВМ, а также может быть передан по электронной почте или скопирован на сменный носитель.

Для того чтобы другие пользователи могли передавать вам зашифрованные сообщения им необходимо на своем компьютере **импортировать** в программе **gpg** ваши публичные ключи. Экспортированный вами публичный ключ может быть скопирован из сети или сменного носителя на компьютер другого пользователя и импортирован в его коллекцию ключей следующей командой:

**gpg --import my_1_key_pub.txt**

где **my_1_key_pub.txt** - импортируемый публичный ключ (рис. 5.15).

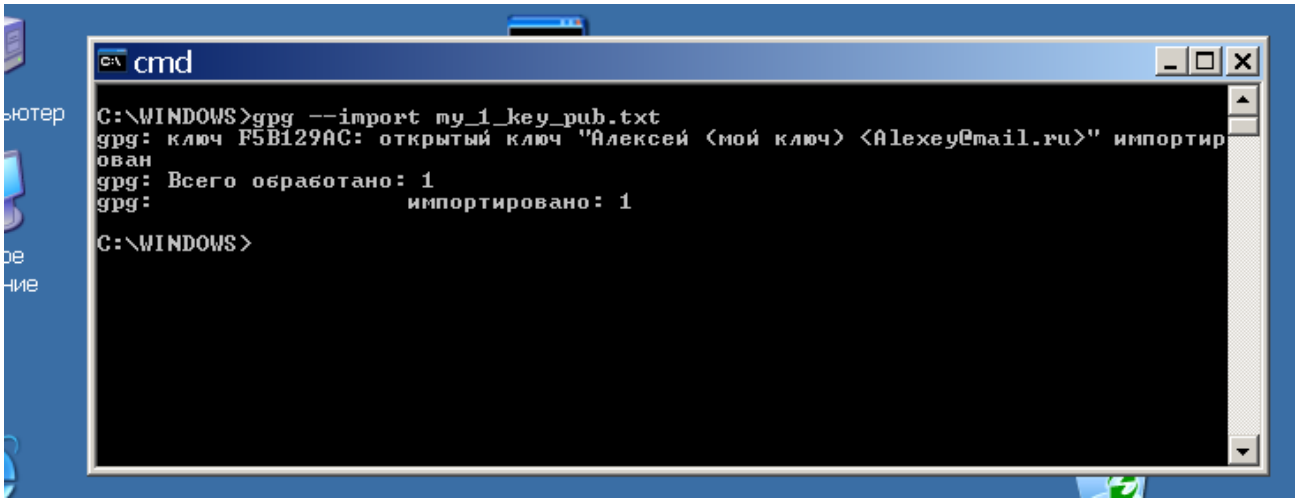


Рис. 5.15. – Импорт публичного ключа

После импорта вашего публичного ключа на свой компьютер пользователь должен указать, что он доверяет владельцу ключа (то есть Вам!) при помощи команды редактирования параметров ключа.

Для этого используется команда **gpg --edit-key id ключа,** id ключа можно узнать, просмотрев коллекцию ключей на компьютере, командой **gpg --list-keys .**

Например, команда **gpg --edit-key Alexey@mail.ru** откроет меню редактирования ключа **Alexey@mail.ru** в котором необходимо ввести команду **trust** (рис. 5.16) и нажать Enter.

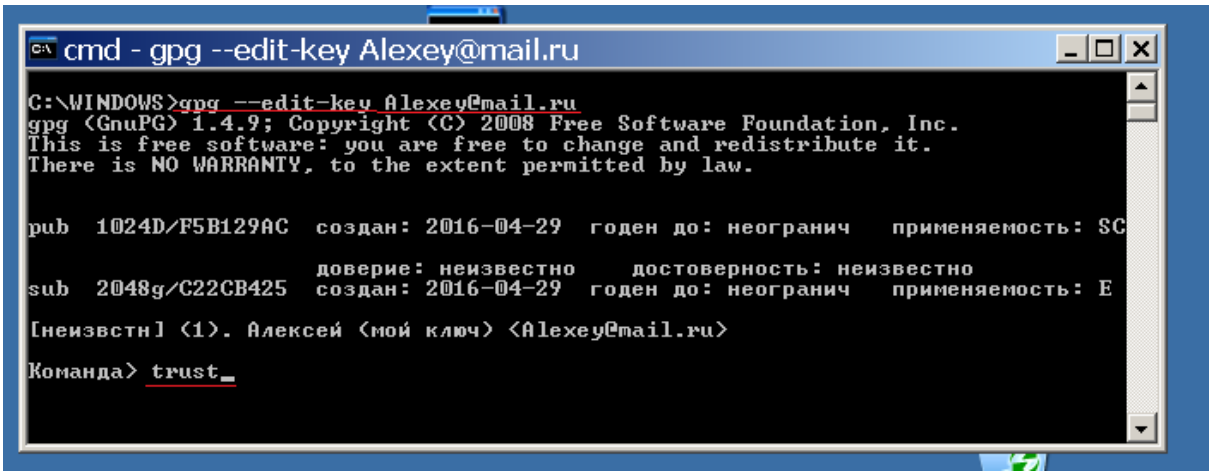


Рис. 5.16. – Редактирование параметров ключа в коллекции

Откроется меню, показанное на рис. 5.17, в котором пользователю необходимо будет выбрать уровень доверия человеку, разместившему публичный ключ (то есть Вам!).

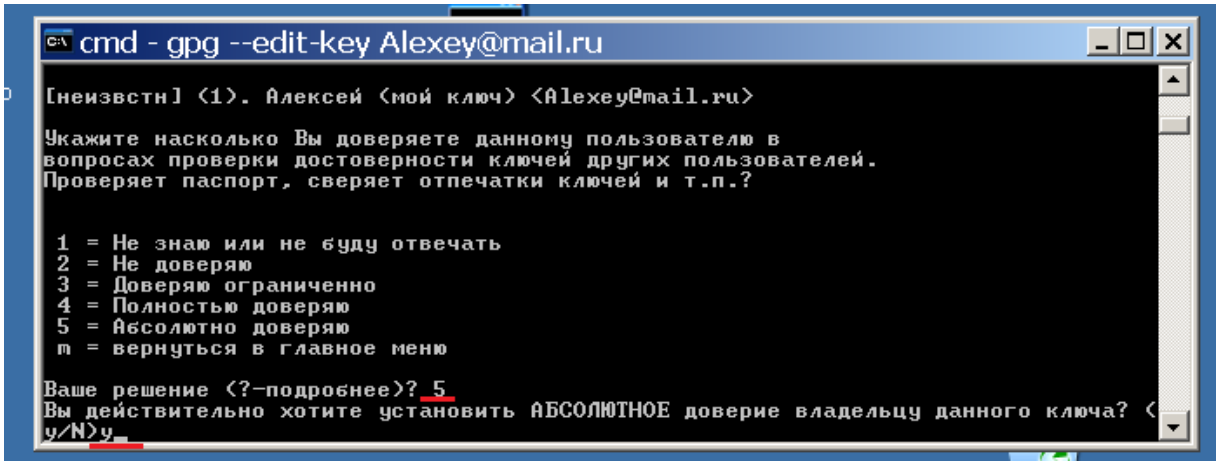


Рис. 5.17. – Установка уровня доверия

Выбрав **5,** и нажав **Enter,** и подтвердив свое решение, пользователь откроет меню команд, в котором необходимо ввести команду выхода - **quit.**

После этой операции пользователь сможет подготовить для Вас зашифрованное сообщение или файл, который Вы сможете расшифровать при помощи Вашего секретного ключа.

### 5.4 Шифрование и дешифрование

Шифрование файла производится командой

**gpg --recipient id_ключа --encrypt filename**

В этой команде:

**id_ключа** - идентификатор ключа получателя файла (например Alexey@mail.ru),

**filename** - Ваш файл который Вы хотите зашифровать (например text.txt).

Например: **gpg --recipient Alexey@mail.ru --encrypt text.txt**

По умолчанию к имени зашифрованного файла добавится расширение .gpg (в примере выходной файл - **text.txt.gpg**).

В результате файл будет зашифрован и никто кроме получателя (Вас!), не сможет его расшифровать, даже пользователь, который его отправил. Пользователь должен любым способом передать Вам зашифрованный файл (по сети, по почте, сменным носителем), который Вы сможете расшифровать, используя следующую команду:

**gpg --decrypt-files filename.gpg**

**filename.gpg** - зашифрованный файл (например **text.txt.gpg** )

Программа **gpg** попросит Вас ввести пароль для доступа к Вашему секретному ключу и произведет дешифрование при этом будет создан файл **filename** (например **text.txt**) (рис. 5.18).

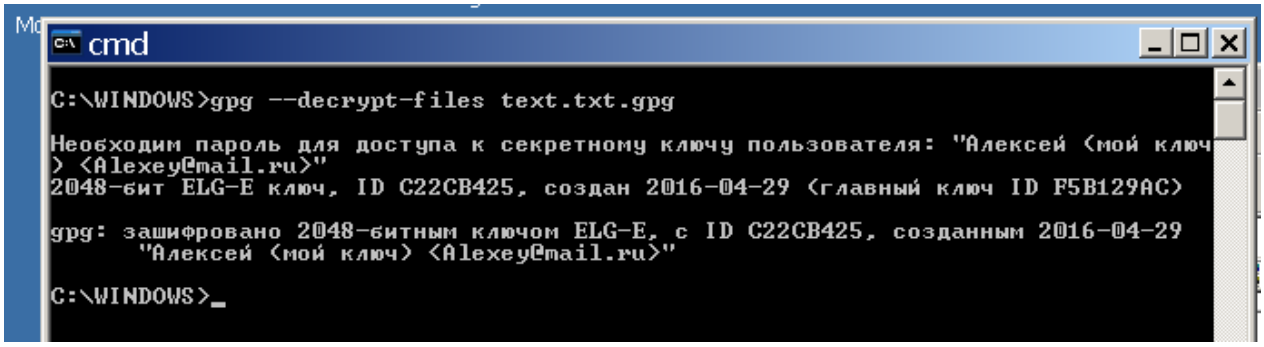


Рис. 5.18. – Дешифровка файла

### 5.5 Перенос секретного ключа на другой компьютер и удаление ключа

Если нужно перенести свой личный(секретный) ключ на другой компьютер, чтобы использовать его на нескольких компьютерах, то сделать это можно при помощи команды:

**gpg --output my_key_sec.txt --armor --export-secret-key id_ключа**

**my_key_sec.txt** - файл для переноса секретного ключа

**id_ключа** - идентификатор ключа получателя файла (например Alexey@mail.ru).

Чтобы импортировать секретный ключ на другой компьютер, необходимо скопировать на него полученный файл и использовать команду:

**gpg --allow-secret-key-import --import my_key_sec.txt**

Для удаления ключа используется команда:

**gpg --delete-keys id_ключа**

Если требуется удалить секретный ключ, сначала необходимо выполнить команду: **gpg --delete-secret-keys id_ключа**

### 5.6. Порядок выполнения лабораторной работы

1. На хост машине создать в каталоге C:/IT_LAB6 папку имя которой должно содержать вашу фамилию.
2. Запустить Oracle VM VirtualBox Менеджер.
3. Придумать имя для двух ВМ (имя должно содержать вашу фамилию и номер ВМ - 1,2)
4. Создать две ВМ типа Windows XP (RAM -192 MB, файл образа – c:/xp.vdi, при работе в компьютерном классе у виртуального носителя должен быть атрибут “множественное подключение”)
5. Сделать папку которая была создана на 1 этапе в качестве общей для каждой ВМ.
6. Скопировать с хост-машины файл c:\gnupg-w32cli-1.4.9.exe на каждую ВМ и установить программу gpg.
7. Добавить в путь ОС Windows XP на каждую ВМ строку C:\Program Files\GNU\GnuPG
8. Создать на ВМ №1 текстовый файл с именем text.txt, который будет содержать название лабораторной работы и вашу фамилию.
9. Выполнить симметричное шифрование text.txt
10. Скопировать зашифрованный файл в общую папку и в ВМ №2.
11. Расшифровать файл на ВМ №2.
12. Удалить на ВМ №1 и общей папке текстовые файлы с именами text.txt и text.txt.gpg
13. Создать на ВМ №1 ключи для ассиметричного шифрования, запомнить пароль для секретного ключа.
14. Экспортировать публичный ключ в виде текстового файла и скопировать его в общую папку.
15. Скопировать из общей папки на ВМ №2 файл публичного ключа.
16. Импортировать публичный ключ на ВМ №2.
17. Установить уровень доверия для публичного ключа на ВМ №2.
18. Зашифровать на ВМ №2 файл с именем text.txt ассиметричным способом.
19. Скопировать зашифрованный файл в общую папку и в ВМ №1.
20. Расшифровать на ВМ №1 зашифрованный файл и просмотреть его.
21. Создать файл для переноса секретного ключа на ВМ №1.
22. Скопировать файл для переноса секретного ключа в общую папку.
23. Создать ВМ №3 типа Other (RAM -640 MB, файл образа – **c:/rt_00.vdi**, у виртуального носителя должен быть атрибут “множественное подключение”)
24. Произвести запуск виртуальной машины с ОС Runtu (имя – user, пароль - user).
25. Сделать папку, которая была создана на 1 этапе в качестве общей для ВМ №3

26. Смонтировать общую папку на ВМ №3 в каталог **/mnt**
27. Скопируйте из каталога **/mnt** в каталог **/user** зашифрованный на ВМ №2 файл и файл для переноса секретного ключа созданный на ВМ №1.
28. Импортировать файл секретного ключа ВМ №1 на ВМ №3.
29. Расшифровать на ВМ №3 зашифрованный файл и просмотреть его.
30. Удалить все ВМ вместе с файлами (только при работе в компьютерном классе!).

### 5.7. Содержание отчета о выполнении лабораторной работы

Отчёт должен содержать:

- титульный лист;
- цель исследования;
- ход работы;
- выводы.

Отчёт по лабораторной работе должен быть выполнен в соответствии требованиями ГОСТ.

### 5.8. Порядок защиты работы

Защита производится при наличии отчета за компьютером и состоит в демонстрации навыков использования возможностей криптографических программ при выполнении задания выданного преподавателем.

### 5.9. Контрольные вопросы

1. Что такое криптография?
2. Что такое симметричное шифрование?
3. Каковы достоинства и недостатки симметричного шифрования?
4. Что такое асимметричное шифрование?
5. Каковы достоинства и недостатки асимметричного шифрования?
6. Что такое публичный ключ?
7. Что такое секретный ключ?
8. Что такое экспорт публичного ключа?
9. Что такое импорт публичного ключа?
10. Как перенести секретный ключ на другой компьютер?
11. Как удалить ключ?

## БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Новожилов, О. П. Информатика: учебник для прикладного бакалавриата / О. П. Новожилов. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2017. — 619 с. — (Бакалавр. Прикладной курс). — ISBN 978-5-9916-4365-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/406583
2. Гостев, И. М. Операционные системы : учебник и практикум для академического бакалавриата / И. М. Гостев. — 2-е изд., исп. и доп. — Москва : Издательство Юрайт, 2018. — 164 с. — (Бакалавр. Академический курс). — ISBN 978-5-534-04520-8. — Текст: электронный // ЭБС Юрайт [сайт]. — URL: https://www.biblio-online.ru/bcode/413976
3. Ресурсы для Oracle VM VirtualBox [Электронный ресурс]. – Режим доступа: http://www.oracle.com/us/technologies/virtualization/oraclevm/oracle-vm-virtualbox-ds-1655169.pdf, свободный – Загр. с экрана. Яз. англ.
4. Ресурсы для GNU [Электронный ресурс]. – Режим доступа: https://www.gnu.org, свободный – Загр. с экрана. Яз. англ.
5. Ресурсы для Runtu [Электронный ресурс]. – Режим доступа: http://runtu.org/, свободный –Загр. с экрана. Яз. русский.
6. Ресурсы для Ubuntu [Электронный ресурс]. – Режим доступа: https://ubuntu.com/, свободный – Загр. с экрана. Яз. англ.
7. Ресурсы для KVM [Электронный ресурс]. – Режим доступа: https://www.linux-kvm.org/, свободный – Загр. с экрана. Яз. англ.
8. Ресурсы для Samba [Электронный ресурс]. – Режим доступа: https://www.samba.org, свободный – Загр. с экрана. Яз. англ.
9. Ресурсы для RDP [Электронный ресурс]. – Режим доступа: https://support.microsoft.com/en-us/help/186607/understanding-the-remote-desktop-protocol-rdp, свободный – Загр. с экрана. Яз.англ.
10. Ресурсы для VNC [Электронный ресурс]. – Режим доступа: https://www.realvnc.com, свободный – Загр. с экрана. Яз. англ.
11. Ресурсы для GNUPG [Электронный ресурс]. – Режим доступа: https://www.gnupg.org/, свободный – Загр. с экрана. Яз. англ.

# ЛАБОРАТОРНЫЙ ПРАКТИКУМ ПО ДИСЦИПЛИНЕ «АДМИНИСТРИРОВАНИЕ КОМПЬЮТЕРНЫХ СЕТЕЙ»

*Методические указания*
*к выполнению лабораторных работ*

*Составитель:* **Осадченко** Александр Евгеньевич

*В авторской редакции*

Изд. № 116/2020. Объем 5,25 п.л.
РИИЦМ ФГАОУ ВО «Севастопольский государственный университет»