ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ

УПРАВЛЕНИЕ ДИСТАНЦИОННОГО ОБУЧЕНИЯ И ПОВЫШЕНИЯ КВАЛИФИКАЦИИ

Кафедра «Экономика и менеджмент в машиностроении»

СБОРНИК УПРАЖНЕНИЙ

по дисциплине

«Безопасность операционных систем»

Автор
Галушка В.В.

Ростов-на-Дону, 2014

Аннотация

Методические указания к лабораторным работам по дисциплине «Безопасность операционных систем» для студентов 3 курса специальности «Информационная безопасность».

Автор

к.т.н., доцент Галушка В.В.

Оглавление

ЛАБОРАТОРНАЯ РАБОТА № 1

Тема: Установка ОС Windows на виртуальную машину.

Цель: Изучить способы создания и управления виртуальными машинами. Получить навыки установки операционной системы Windows.

Теоретические сведения

В настоящее время технологии виртуализации активно используются для решения различных задач администрирования информационных сетей и систем. В основе виртуализации лежит возможность одного компьютера, эмулировать работу нескольких ПК благодаря распределению его ресурсов по нескольким средам.

Виртуализация в данном контексте — это возможность запускать несколько виртуальных операционных систем одновременно на одном физическом компьютере, то есть фактически создать несколько виртуальных компьютеров.

Созданная с помощью специального программного инструмента виртуальная машина представляет собой конкретный экземпляр некой виртуальной вычислительной среды («виртуального компьютера»). На одном физическом устройстве можно создавать и запускать произвольное число виртуальных машин, ограничиваемое лишь физическими ресурсами реального компьютера.

Собственно инструмент для создания виртуальной машины (ВМ) — это обычное программное приложение, устанавливаемое, как и любое другое, на конкретную реальную операционную систему. Эта реальная ОС именуется «хозяйской» или «хостовой ОС» (от англ. термина host — «главный», «базовый», «ведущий»). Все задачи по управлению виртуальными машинами решает специальный модуль в составе приложения ВМ — монитор виртуальных машин (он же менеджера виртуальных машин или гипервизор).

Монитор играет роль посредника во всех взаимодействиях между виртуальными машинами и базовым оборудованием, поддерживая выполнение всех созданных ВМ на единой аппаратной платформе и обеспечивая их надежную изоляцию. Пользователь не имеет непосредственного доступа к менеджеру виртуальных. В большинстве программных продуктов ему предоставляется лишь графический интерфейс для создания и настройки виртуальных машин. Этот интерфейс обычно называют консолью виртуальных машин. «Внутри» виртуальной машины пользователь устанавливает, как и на реальном компьютере, нужную ему операционную систему. Такая ОС, принадлежащая конкретной ВМ, называется

гостевой (guest OS). Перечень поддерживаемых гостевых ОС является одной из наиболее важных характеристик виртуальной машины. Наиболее мощные из современных виртуальных машин обеспечивают поддержку около десятка популярных версий операционных систем из семейств Windows, Linux и MacOS.

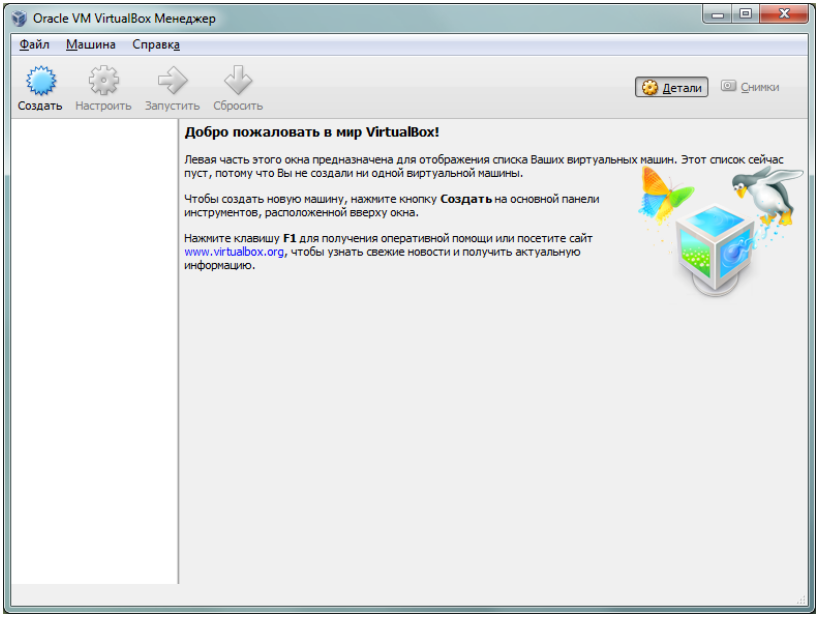
В данной работе в качестве менеджера виртуальных машин используется программное обеспечение Oracle VirtualBox**.**

Задание

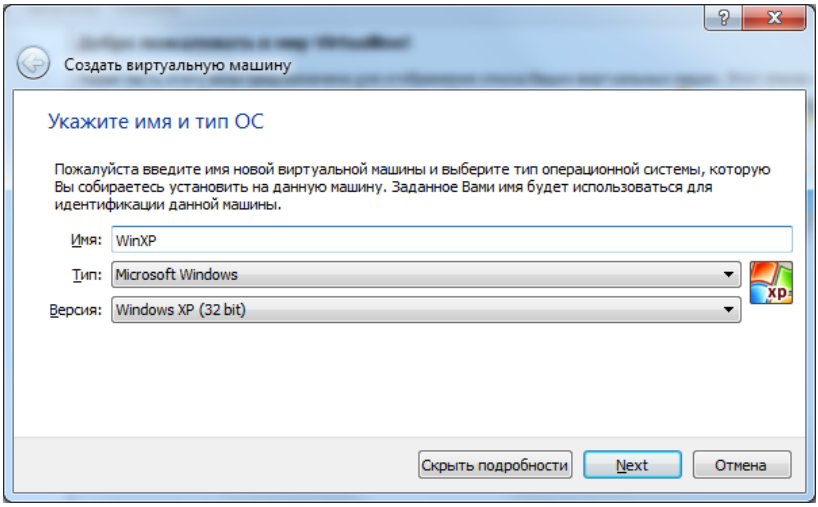
1) Установка и настройка виртуальной машины

VirtualBox должен быть установлен как приложение операционной системы физического компьютера (хостовой системы). В качестве хостовых систем поддерживаются различные версии Windows, Linux, Solaris и MAC OS X.

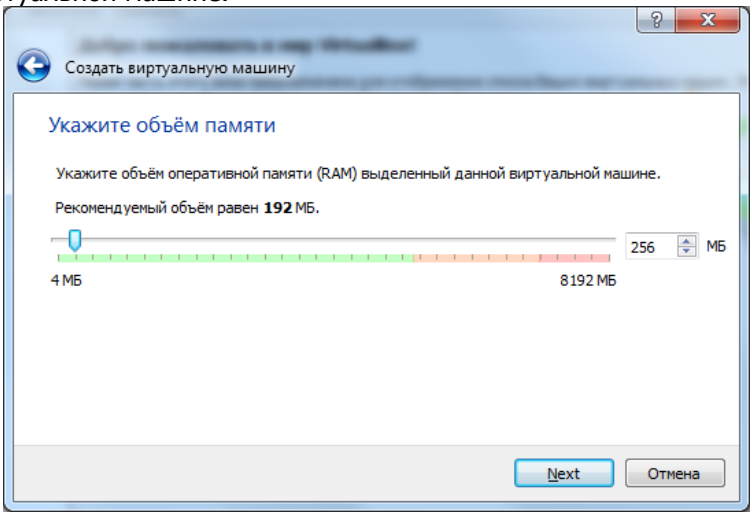
После установки VirtualBox и первоначального запуска появится главное окно программы, предназначенное для управления виртуальными машинами: создания/удаления, настройки и запуска.



Создадим новую виртуальную машину. Для этого необходимо нажать кнопку «Создать». Появится окно создания виртуальной машины в котором необходимо ввести её название, а также выбрать тип и версию гостевой ОС.

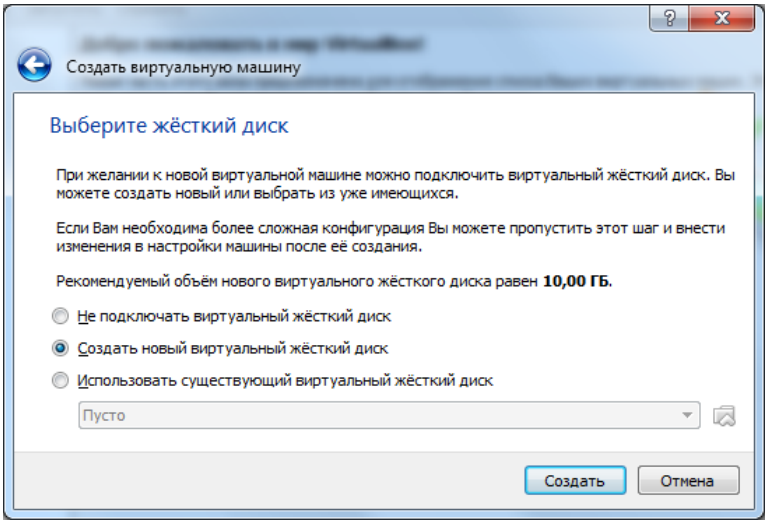


После нажатия кнопки «Next» появится следующее окно настроек, предназначенное для выделения оперативной памяти виртуальной машине.

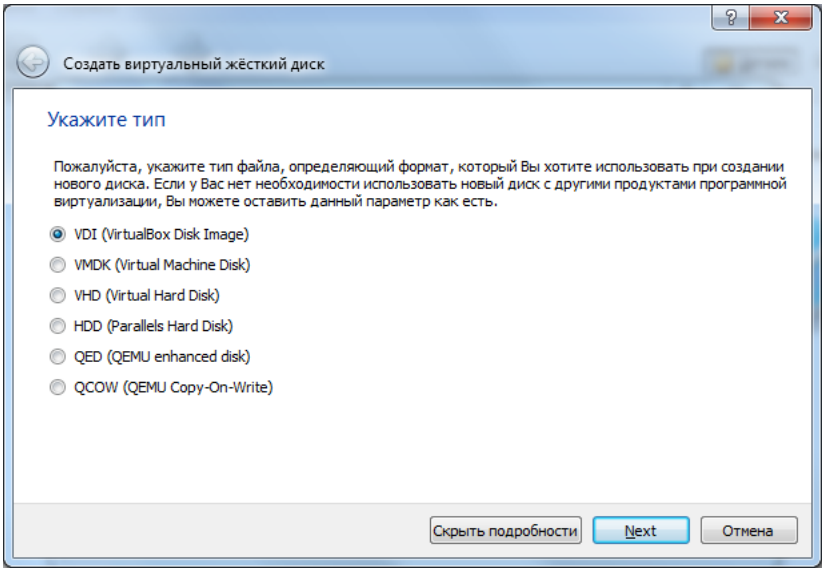


Укажите объём не ниже рекомендуемого (эти настройки можно будет изменить позже в окне свойств виртуальной машины) и нажмите «Next».

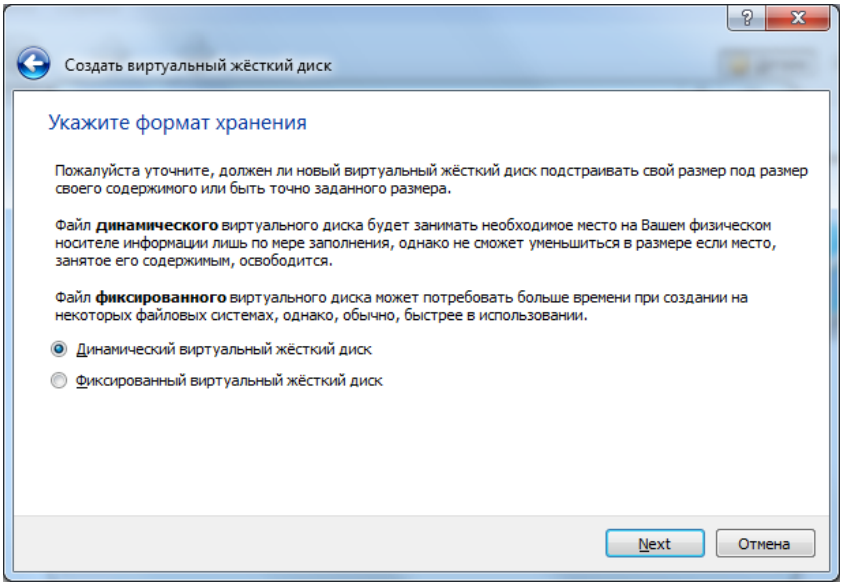
Появится окно настроек жесткого иска виртуальной машины. Выберите «Создать новый виртуальный жёсткий диск» и нажмите «Создать».



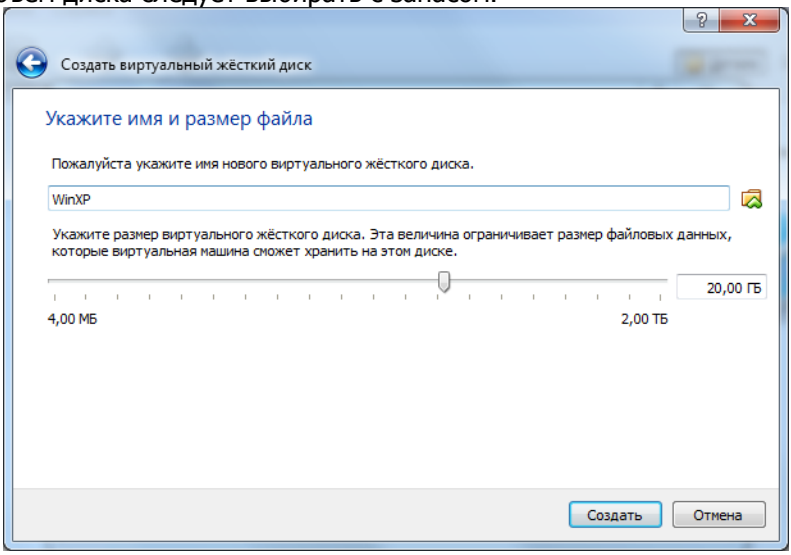
Появится окно создания жёсткого диска. Оставьте настройку по умолчанию «VDI (VirtualBox Disk Image)» и нажмите «Next».



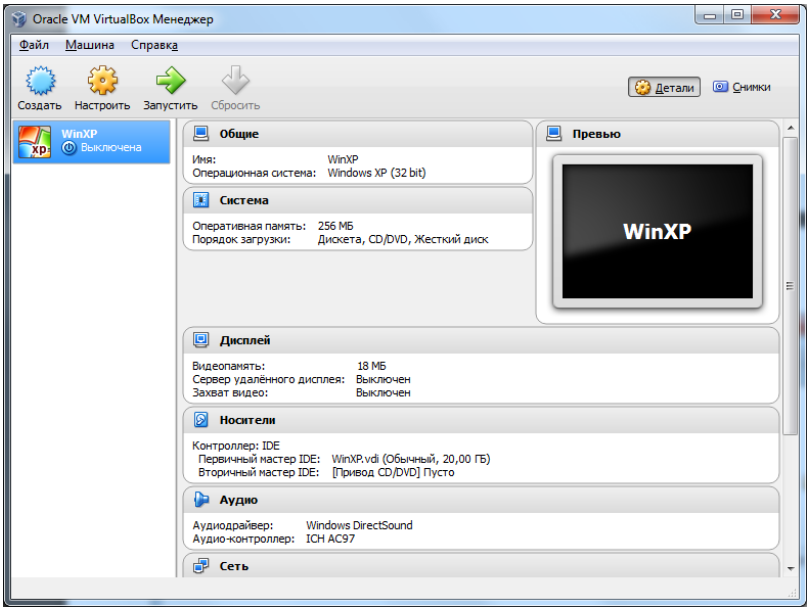
В следующем окне укажите «Динамический жёсткий диск» и нажмите «Next».



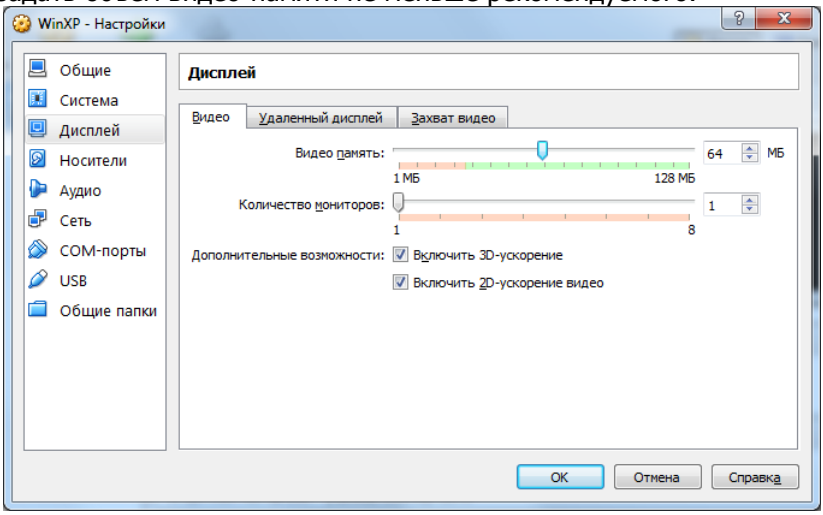
В следующем окне необходимо задать размер создаваемому жесткому диску. Эту настройку нельзя изменить позже, поэтому объём диска следует выбирать с запасом.



После нажатия кнопки «Создать» диалог создания виртуальной машины будет завершен и она появится в списке доступных виртуальных машин.



Далее необходимо сделать еще некоторые настройки, для чего выбрать виртуальную машину и нажать кнопку «Настроить». Затем перейти на вкладку «Дисплей», отметить галочки «Включить 3D-ускорение» и «Включить 2D-ускорение», а также задать объём видео-памяти не меньше рекомендуемого.

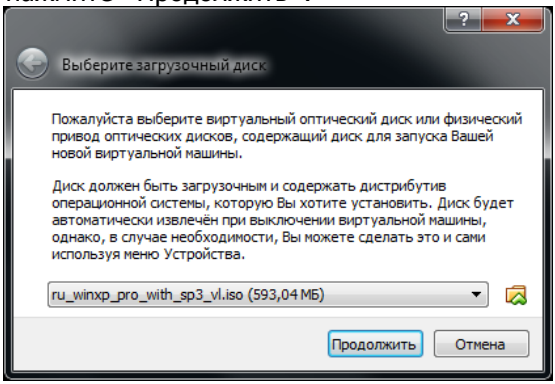


После выполнения всех настроек можно приступать к

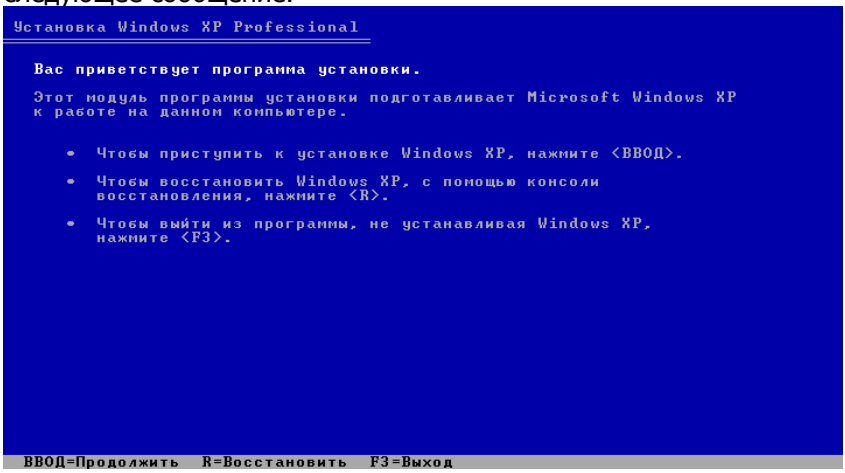
установке операционной системы на виртуальную машину.

2) Установка Windows

Для запуска виртуальной машины выберите её из списка слева и нажмите кнопку «Запустить». При первом запуске машины будет показано сообщение с предложением выбрать загрузочный диск, с которого будет установлена операционная система. Нажмите на значок папки и укажите путь к файлу образа диска. После чего нажмите «Продолжить».

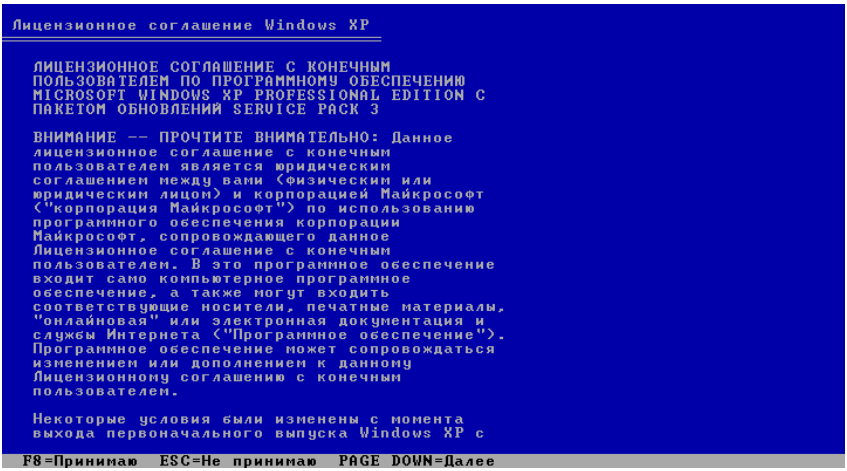


Виртуальная машина продолжит загрузку и начнёт установку Windows, на начальном этапе которой появится следующее сообщение.



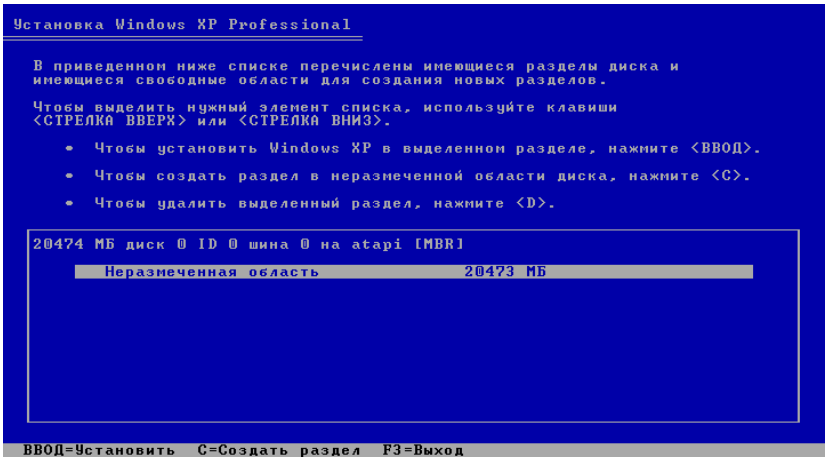
Нажмите Enter.

Далее будет предложено ознакомиться с лицензионным соглашением.

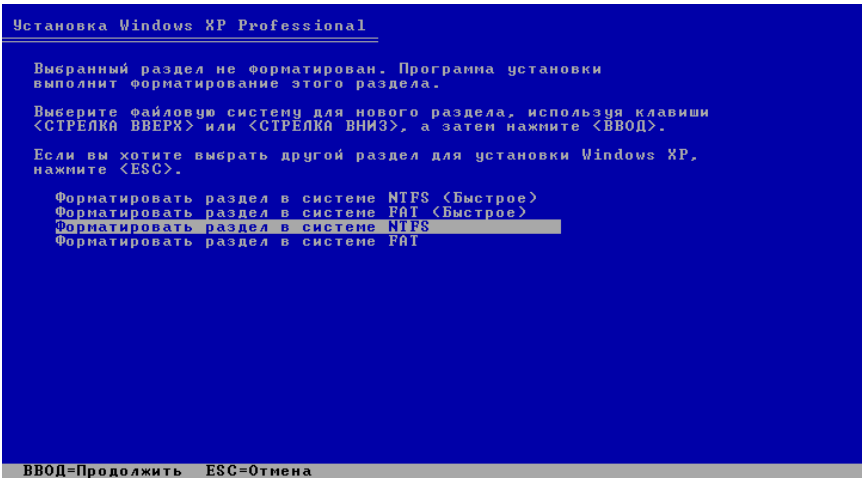


Нажмите F8.

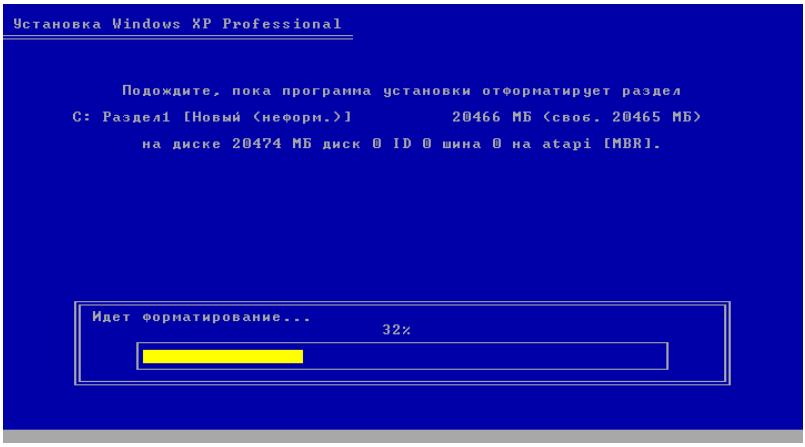
На следующем экране будет показана структура жесткого диска. Так как мы создали новый чистый диск, то он будет иметь только неразмеченную область, на которую и нужно установить Windows.



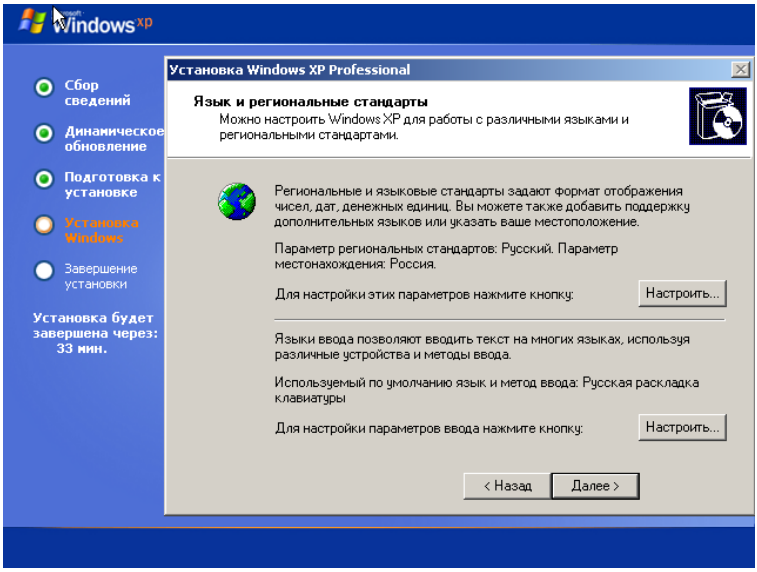
Нажмите Enter. При этом все необходимые разделы будут созданы автоматически. На следующем экране появятся настройки фаловой системы для диска и способа его форматирования.



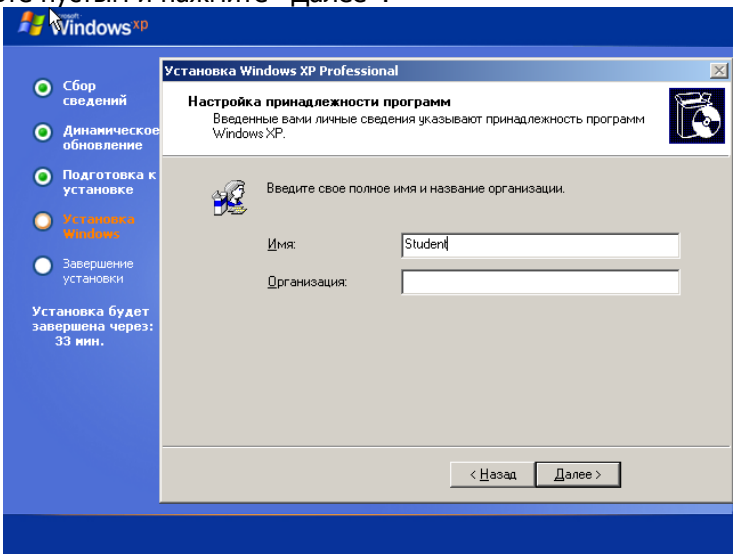
Выберите «Форматировать раздел в системе NTSF» и нажмите Enter.



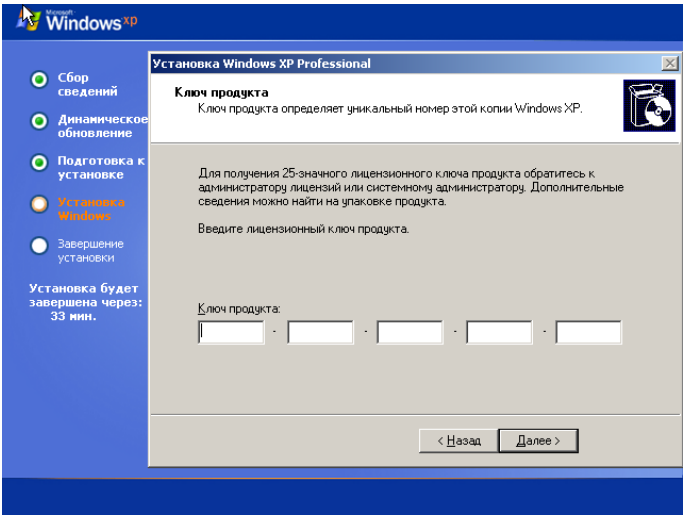
Далее начнётся процесс установки, не требующий вмешательства пользователя до определённого момента. Затем появится окно настройки региональных параметров. Оно не требует внесения каких-либо изменений, поэтому нажмите «Далее».



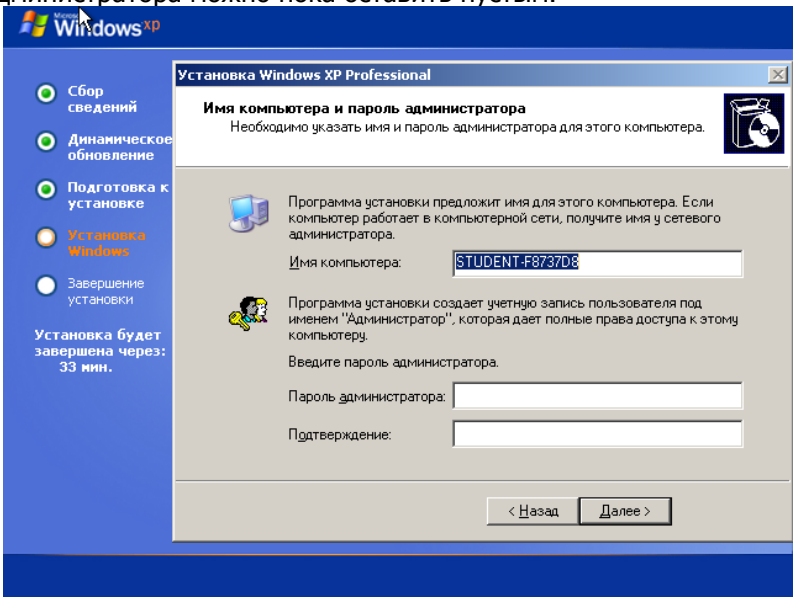
Далее появится окно для указания имени пользователя и организации. Введите своё имя, а поле название организации оставьте пустым и нажмите «Далее».



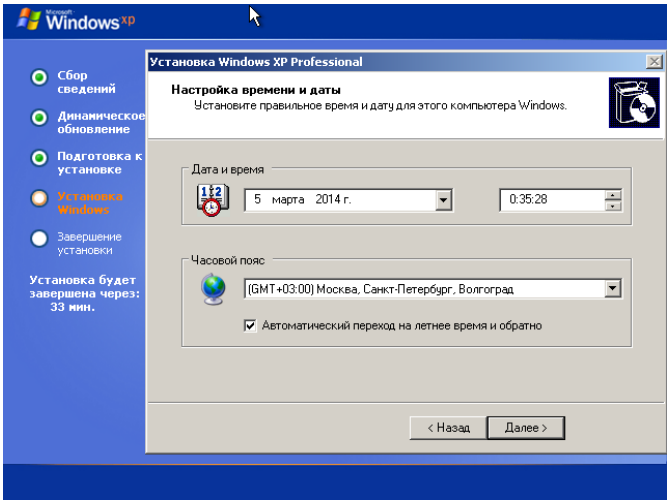
В следующем окне введите ключ продукта и нажмите «Далее».



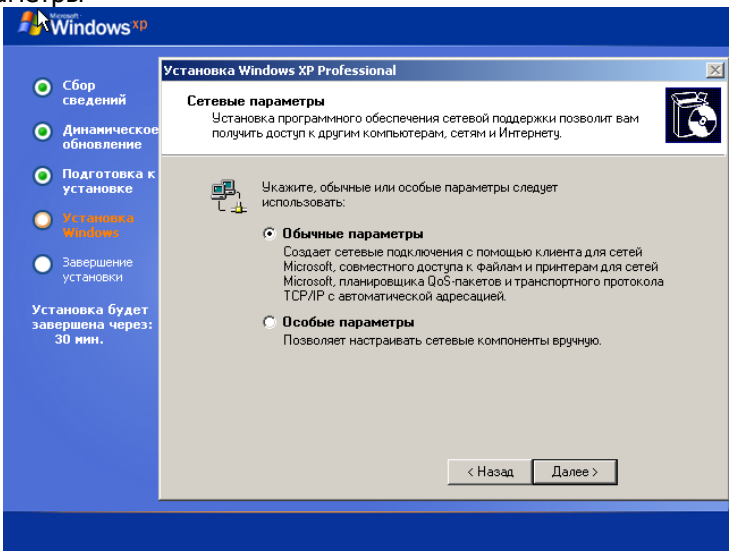
В следующем окне укажите любое имя компьютера. Пароль администратора можно пока оставить пустым.



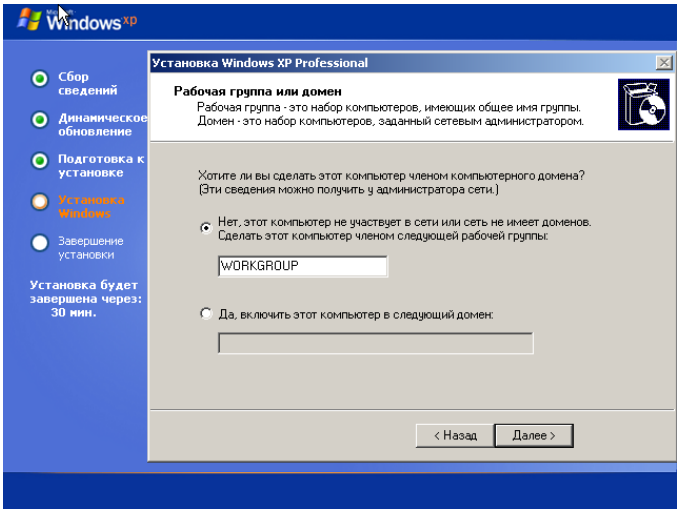
Укажите текущие дату и время.



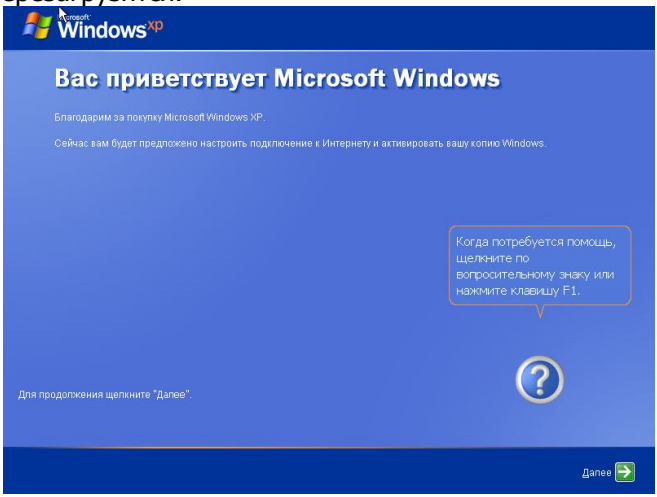
В окне настроек сетевых параметров укажите «Обычные параметры»



В следующем окне оставьте стандартные настройки рабочей группы.



Установка будет продолжена, после чего виртуальная машина перезагрузится.



В следующих нескольких диалоговых окнах потребуется ввести имя своей учётной записи и настроить систему обновлений Windows.

На этом установка Windows будет окончена.

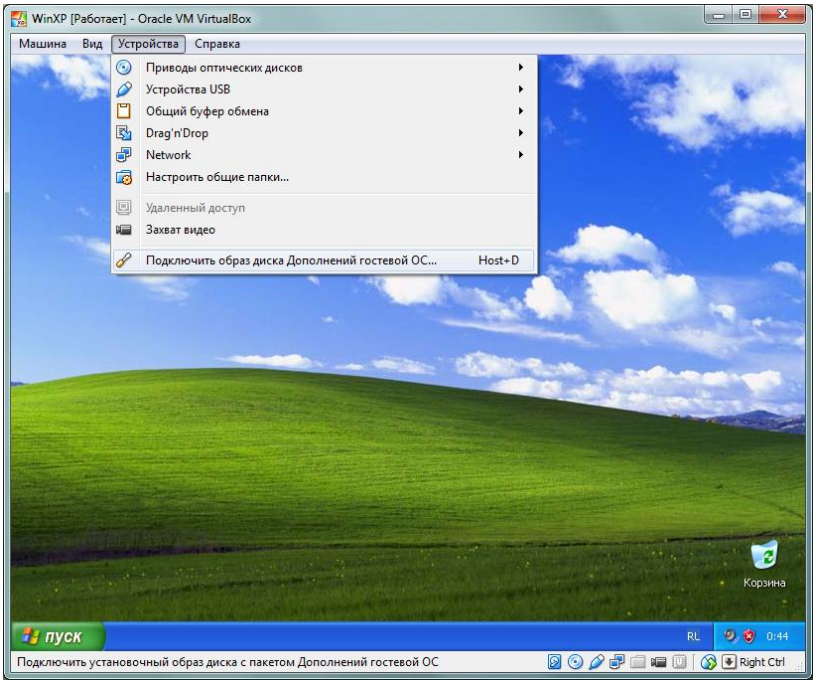
3) Установка дополнений гостевой ОС.

Виртуальная машина полностью функциональна внутри себя. Однако при работе пользователя наблюдаются существенные ограничения, влияющие на удобство работы с виртуальной машиной. Так, например, невозможен быстрый (автоматический) переход из основной ОС в гостевую и обратно, ограниченны разрешения экрана гостевой ОС, затруднена работа с сетью.

Для расширения функциональности и повышения удобства для пользователя в гостевой ОС необходимо установить специальные расширенные инструменты, которые включают в себя набор драйвера для виртуализированного оборудования.

В результате установки расширенных инструментов появляется возможность автоматического управления захватом мыши и клавиатуры, становится возможным устанавливать произвольное разрешение экрана гостевой ОС путем изменения размеров окна виртуальной машины, а так же работа с сетью.

Для установки дополнений выберите пункт меню виртуальной машины «Устройства» и далее «Подключить образ диска Дополнений гостевой ОС…».



Появится окно мастера установки.

Нажмите кнопку Next.

В следующем окне оставьте путь для установки, предложенный по умолчанию.

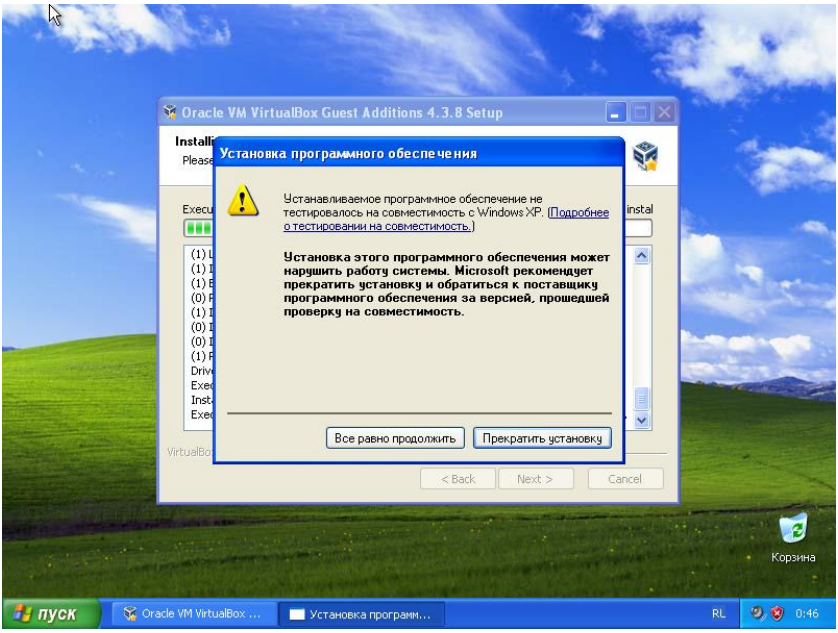
Нажмите кнопку Next.

В следующем окне также оставьте настройки по умолчанию.

Нажмите кнопку Install.

Дождитесь завершения работы мастера установки.

В процессе установки могут возникать сообщения о том что устанавливаемое программное обеспечение не тестировалось на совместимость с Windows XP. В это случае следует нажмимать кнопку «Все равно продолжить».



В последнем окне выберите Reboot now (перезагрузить сейчас) и нажмите кнопку Finish.

После перезагрузки изучите работу виртуальной машины в разных режимах, доступных в меню «Вид».

Контрольные вопросы

1. Что представляют собой виртуальные машины?
2. Для каких целей можно использовать виртуальные машины?
3. Какая операционная система именуется хозяйской ОС?
4. Какая операционная система называется гостевой?
5. Чем отличается работа в полноэкранном режиме, режиме интеграции дисплея и режиме масштабирования?

ЛАБОРАТОРНАЯ РАБОТА № 2

Тема: Реестр операционной системы Windows.

Цель: Изучить основные способы работы с реестром Windows.

Теоретические сведения

Реестр — это база данных, в которой хранится информация обо всех настройках и параметрах работы Windows XP, а также конфигурация всех установленных в системе приложений.

Все параметры системного реестра Windows XP, в зависимости от их функционального назначения, сгруппированы в пять основных разделов.

— HKEY_CLASSES_ROOT — данный раздел включает в себя информацию о зарегистрированных в системе типах файлов, порядке обработки файлов каждого типа, а также управлении основными настройками интерфейса.

— HKEY_CURRENT_USER — в этом разделе содержится информация о пользователе, работающем с Windows XP в текущем сеансе, а также о различных настройках системы, относящихся к текущему пользователю (вид Рабочего стола, сетевые соединения, принтеры и др.).

— HKEY_LOCAL_MACHINE — раздел содержит информацию об аппаратной конфигурации компьютера и установленном программном обеспечении. Настройки раздела действительны для всех пользователей данного компьютера. Следует отметить, что по объему этот раздел является самым большим, по сравнению с другими разделами реестра Windows XP.

— HKEY_USERS — в раздел включена информация обо всех пользователях данного компьютера. Следует отметить тесную взаимосвязь данного раздела с разделом HKEY_CURRENT_USER, который фактически дублирует один из его подразделов, а именно относящиеся к текущему пользователю.

— HKEY_CURRENT_CONFIG — в этом разделе содержится информация о настройках оборудования, которое используется локальным компьютером в текущем сеансе работы.

В целом, структура реестра представлена в иерархическом порядке: каждый из перечисленных разделов имеет ряд подчиненных уровней иерархии, нижней ступенью которой являются параметры настройки системного реестра.

Наиболее часто используемые в реестре Windows XP типы

данных:

— REG_BINARY — двоичные данные. Этот тип данных используется, например, для хранения сведений об аппаратных ресурсах; сведения выводятся в Редакторе реестра в шестнадцатернчном формате.

— REG_DWORD — целое число. Может использоваться, например, в качестве переключателя (1 — включение, 0 — выключение некоторого действия); могут применяться и другие числа. Возможно представление этою типа данных в двоичном, десятичном и шестнадцатеричном формате.

— REG_EXPAND_SZ — расширенная строка. Этот тип данных используется в Windows для ссылок на файлы.

— REG_MULTI_SZ — многострочный текст (массив строк). Этот тип обычно используется для представления списков и иных подобных записей в удобном для чтения формате.

— REG SZ — текстовая строка. Данные этого типа используются в реестре чаще всего.

— REG_FULL_RESOURCE_DESCRIPTOR — последовательность вложенных массивов, предназначенная для хранения списка ресурсов устройств или драйверов.

— REG_LINK — строковый тип данных, предназначенный для указания пути к файлам.

Ручное редактирование системного реестра Windows XP выполняется либо средствами Редактора реестра, либо с помощью REG-файлов.

По своей структуре и содержанию файл реестра представляет собой обычный текстовый файл, поэтому его формирование и редактирование возможно с помощью любого текстового редактора (например, Блокнота). Следует отметить, что для редактирования имеющегося REG-файла целесообразно воспользоваться командой Файл —> Экспорт, которая активизируется в окне Редактора реестра. В результате выполнения этой команды требуемый файл (это может быть как файл отдельного раздела или ветви, так и файл реестра целиком) будет экспортирован по указанному пути. После внесения всех необходимых изменений файл импортируется в реестр с помощью команды Файл —> Импорт, также вызываемой в окне Редактора реестра.

Важным элементом любого REG-файла системного реестра Windows XP является его первая строка, текст которой нельзя изменять ни при каких обстоятельствах, так как только в этом случае система сможет распознать, что текущий файл содержит

именно данные реестра. Вот как выглядит эта строка:

Windows Registry Editor Version 5.00

После первой строки текста REG-файла обязательно должна следовать пустая строка. Затем в квадратных скобках указывается раздел системного реестра, к которому относится редактируемый файл (в качестве разделителя между объектами реестра используется символ \), Далее следует перечисление параметров редактируемого раздела с указанием имени параметра, типа данных и значения параметра (каждый параметр отображается в отдельной строке текста файла). При этом соблюдаются следующие правила: имя параметра заключается в кавычки, затем после знака равенства указывается тип данных, далее после двоеточия — значение параметра; если же тип данных не указан, то по умолчанию соответствующий параметр считается строковым и его значение заключается в кавычки. Последняя строка REG-файла должна оставаться пустой.

Другим дополнительным инструментом, поддерживающим большинство возможностей Реестра, является консольная системная утилита Reg.exe, работающая из командной строки ОС. Ее особенность состоит в том, что она может быть востребована при написании пакетных файлов и использована как любая другая системная команда ОС Windows XP.

Задание

а) Сделать резервную копию ветвей реестра, изменяемых в следующих пунктах задания. Изучить структуру полученного файла.

б) С помощью утилиты regedit внести информацию в ветвь реестра Windows

HKCU\Software\Microsoft\Windows\CurrentVersion\Explorer\Advanced

в соответствии с вариантом задания.

Если указанный параметр не существует необходимо создать его вручную.

Сделать скриншоты и описать изменения, произошедшие в меню пуск после присвоения каждого из возможных значений.

Чтобы изменения вступили в силу необходимо перезапустить процесс «explorer». Для этого:

1. Открыть диспетчер задач, перейти на вкладку «Процессы», там выбрать процесс «explorer.exe», нажать на него правой кнопкой мыши и в появившемся меню выбрать пункт «Завершить процесс».

2. В меню диспетчера задач выбрать пункт «Файл», затем пункт «Выполнить…», в открывшемся окне ввести «explorer» и нажать Enter.

Вариант	**Параметр**	**Тип**	**Возможные значения**
1	Start_ShowControlPanel	REG_DWORD	0, 1, 2
2	StartMenuFavorites	REG_DWORD	0, 1
3	Start_ShowMyComputer	REG_DWORD	0, 1, 2
4	Start_ShowMyDocs	REG_DWORD	0, 1, 2
5	Start_ShowMyMusic	REG_DWORD	0, 1, 2
6	Start_ShowMyPics	REG_DWORD	0, 1, 2
7	Start_ShowNetConn	REG_DWORD	0, 1, 2
8	Start_AdminToolsRoot	REG_DWORD	0, 1
9	Start_ShowHelp	REG_DWORD	0, 1
10	Start_ShowNetPlaces	REG_DWORD	0, 1
11	Start_ShowRun	REG_DWORD	0, 1
12	Start_ShowPrinters	REG_DWORD	0, 1
13	Start_ShowSearch	REG_DWORD	0, 1
14	Start_ScrollPrograms	REG_DWORD	0, 1
15	Start_ShowOEMLink	REG_DWORD	0, 1

в) внести информацию в реестр с помощью reg-файла в соответствии с вариантом задания

Варианты заданий

1. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер" команду "Администрирование":

[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\1]
@="Администрирование"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\1\command]
@="control admintools"

2. Настройка добавляет в контекстное меню приложения "Мой компь
ютер" команду "Групповая политика":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\11]

@="Групповая политика"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\11\command]
@=hex(2):25,00,77,00,69,00,6e,00,64,00,69,00,72,00,25,00,5c,\
00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,6d,00,6d,00,63,00,\
2e,00,65,00,78,00,65,00,20,00,2f,00,73,00,20,00,25,00,53,00,79,00,73,00,74,\
00,65,00,6d,00,52,00,6f,00,6f,00,74,00,25,00,5c,00,73,00,79,00,73,00,74,00,\
65,00,6d,00,33,00,32,00,5c,00,67,00,70,00,65,00,64,00,69,00,74,00,2e,00,6d,\
00,73,00,63,00,20,00,2f,00,73,00,00,00

3. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер" команду "Диспетчер устройств":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\2]
@="Диспетчер устройств"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\2\command]

@=hex(2):25,00,77,00,69,00,6e,00,64,00,69,00,72,00,25,00,5c
,\
00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,6d,
00,6d,00,63,00,\
2e,00,65,00,78,00,65,00,20,00,2f,00,73,00,20,00,25,00,53,00,7
9,00,73,00,74,\
00,65,00,6d,00,52,00,6f,00,6f,00,74,00,25,00,5c,00,73,00,79,0
0,73,00,74,00,\
65,00,6d,00,33,00,32,00,5c,00,64,00,65,00,76,00,6d,00,67,00,
6d,00,74,00,2e,\
00,6d,00,73,00,63,00,20,00,2f,00,73,00,00,00

4. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер"команду "Командная строка":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE
0-3AEA-1069-A2D8-08002B30309D}\shell\22]
@="Командная строка"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE
0-3AEA-1069-A2D8-08002B30309D}\shell\22\command]
@="cmd.exe"

5. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер" команду "Настройка системы":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE
0-3AEA-1069-A2D8-08002B30309D}\shell\3]
@="Настройка системы (MSCONFIG)"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE
0-3AEA-1069-A2D8-08002B30309D}\shell\3\command]
@="msconfig.exe /s"

6. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер" команду "Панель управления":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE
0-3AEA-1069-A2D8-08002B30309D}\shell\4]
@="Панель управления"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE
0-3AEA-1069-A2D8-08002B30309D}\shell\4\command]
@="rundll32.exe shell32.dll,Control_RunDLL"

7. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер" команду "Редактор реестра":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\44]
@="Редактор реестра"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\44\command]
@="Regedit.exe"

8. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер" команду "Службы":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\5]
@="Службы"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\5\command]
@=hex(2):25,00,77,00,69,00,6e,00,64,00,69,00,72,00,25,00,5c,00,73,00,79,00,73, 00,\
74,00,65,00,6d,00,33,00,32,00,5c,00,6d,00,6d,00,63,00,2e,00,65,00,78,00, 65,00,20,\
00,2f,00,73,00,20,00,25,00,53,00,79,00,73,00,74,00,65,00,6d,00,52, 00,6f,00,6f,00,74,\
00,25,00,5c,00,73,00,79,00,73,00,74,00,65,00,6d,00,33,00,32,00,5c,00,73,00,65,00,\
72,00,76,00,69,00,63,00,65,00,73,00,2e,00,6d,00,73,00,63,00,20,00,2f,00,73,00,00,00

9. Настройка добавляет в контекстное меню приложения "Мой ком-
пьютер" команду "Перезагрузка":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\77]
@="[Перезагрузка]"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\77\command]
@="shutdown -r -f -t 0"

10. Настройка добавляет в контекстное меню приложения "Мой ком-
пьютер" команду "Установка и удаление компонентов

Windows":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\6]
@="Установка и удаление компонентов Windows"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\6\command]
@="rundll32 shell32,Control_RunDLL appwiz.cpl,,2"

11. Настройка добавляет в контекстное меню приложения "Мой ком-
пьютер" команду "Установка и удаление программ":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\66]
@="Установка и удаление программ"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\66\command]
@="control appwiz.cpl"

12. Настройка добавляет в контекстное меню приложения "Мой ком-
пьютер" команду "Выход":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\7]
@="[Выход]"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\7\command]
@="shutdown -l -f -t 0"

13. Настройка добавляет в контекстное меню приложения "Мой компь-
ютер" команду "Удаление вредоносных программ":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\55]
@="Удаление вредоносных программ"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE0-3AEA-1069-A2D8-08002B30309D}\shell\55\command]
@="mrt.exe"

14. Настройка добавляет в контекстное меню приложения "Мой ком-
пьютер" команду "Выключение":
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE

0-3AEA-1069-A2D8-08002B30309D}\shell\8]
@="[Выключение]"
[HKEY_LOCAL_MACHINE\SOFTWARE\Classes\CLSID\{20D04FE
0-3AEA-1069-A2D8-08002B30309D}\shell\8\command]
@="shutdown -s -f -t 0"

г) восстановить исходные значения ключей реестра, используя при необходимости резервные копии, созданные в п. а) и убедиться, что все параметры имеют прежние значения.

Контрольные вопросы

1. Что такое реестр?
2. Из каких частей состоит реестр?
3. Что такое ветвь реестра?
4. Что такое параметр?
5. Какие существуют способы редактирования реестра?
6. Как сделать резервную копию определённой ветви реестра?
7. Какова структура reg-файла?

ЛАБОРАТОРНАЯ РАБОТА № 3

Тема: Управление пользователями в Windows XP.

Цель: изучить способы создания локальных учетных записей пользователей и групп и настройки их свойств.

Теоретические сведения

В операционной системе Windows XP на одном и том же компьютере могут работать разные пользователи, каждый под своим именем. При входе в ОС запрашиваются имя и пароль, на основе которых происходит аутентификация пользователя.

Компьютер может работать автономно, а может быть рабочей станцией в сети. Если компьютер загружается для автономной работы или для работы в одноранговой сети, то пользователь регистрируется, используя внутренний (локальный) список имен пользователей системы.

Если компьютер загружается для работы в сети с выделенным сервером, то пользователь регистрируется, используя имя, которое ему выдал администратор сети. Список с этими именами хранится на сервере.

Данные о пользователе находятся в специальной базе данных на локальных компьютерах и на сервере. На каждого пользователя заводится отдельная учетная карточка, которая носит название учетная запись.

Windows XP использует три типа учетных записей пользователей:

1. Локальные учетные записи для регистрации пользователей локального компьютера. База локальных учетных записей хранится на каждом компьютере своя, и содержит информацию о пользователях только данного компьютера. Создаются учетные записи администратором этого компьютера.

2. Встроенные учетные записи пользователей создаются автоматически при установке Windows XP. Встроенных учетных записей две — Администратор и Гость. Встроенные учетные записи хранятся в той же базе, что и локальные учетные записи.

3. Учетные записи пользователей домена хранятся на выделенном сервере и содержат данные о пользователях локальной сети.

Локальная учетная запись — это учетная запись, которой могут быть предоставлены разрешения и права на вашем компьютере. Для удобства управления локальными пользователями, их можно объединять в группы и управлять группами, чтобы не ус-

танавливать одни и те же настройки для каждого пользователя в отдельности. Ограничения, установленные для группы, распространяются на всех пользователей этой группы.

Пользователи и группы важны для безопасности Windows XP поскольку позволяют ограничить возможность пользователей и групп выполнять определенные действия путем назначения им прав и разрешений. Право дает возможность пользователю выполнять на компьютере определенные действия, такие как архивирование файлов и папок или завершение работы компьютера. Разрешение представляет собой правило, связанное с объектом (например, файлом, папкой или принтером), которое определяет, каким пользователям и какого типа доступ к объекту разрешен.

Операционная система содержит несколько встроенных учетных записей пользователей и групп, которые не могут быть удалены:

Учетная запись пользователя с именем "Администратор" используется при первой установке рабочей станции или рядового сервера. Эта учетная запись позволяет выполнять необходимые действия до того, как пользователь создаст свою собственную учетную запись. Администратор является членом группы администраторов на рабочей станции или рядовом сервере.

— Учетную запись "Администратор" нельзя удалить, отключить или вывести из группы администраторов, что исключает возможность случайной потери доступа к компьютеру после уничтожения всех учетных записей администраторов. Это свойство отличает пользователя "Администратор" от остальных членов локальной группы "Администраторы".

— Учетная запись гостя предназначена для тех, кто не имеет реальной учетной записи на компьютере. Учетную запись "Гость" нельзя удалить, но можно переименовать или отключить. Учетной записи пользователя "Гость", как и любой другой учетной записи, можно предоставлять права и разрешения на доступ к объектам. Учетная запись "Гость" по умолчанию входит во встроенную группу "Гости", что позволяет пользователю войти в систему с рабочей станции или рядового сервера. Дополнительные права, как любые разрешения, могут быть присвоены группе "Гости" членом группы администраторов.

К стандартным группам Windows XP относятся следующие группы:

— Администраторы. Пользователи, входящие в группу "Администраторы", имеют полный доступ на управление компьютером. Это единственная встроенная группа, которой автоматически

предоставляются все встроенные права и возможности в системе. По умолчанию туда входит учетная запись "Администратор".

— Операторы архива. Члены группы "Операторы архива" могут архивировать и восстанавливать файлы на компьютере, независимо от всех разрешений, которыми защищены эти файлы. Также они могут входить на компьютер и выключать его, но не могут изменять параметры безопасности.

— Опытные пользователи. Члены группы опытных пользователей могут создавать учетные записи пользователей, но могут изменять и удалять только созданные ими учетные записи. Они могут создавать локальные группы и удалять пользователей из локальных групп, которые они создали. Они также могут удалять пользователей из групп "Опытные пользователи", "Пользователи" и "Гости". Они не могут изменять группы "Администраторы" и "Операторы архива", не могут являться владельцами файлов, не могут выполнять архивирование и восстановление каталогов, не могут загружать и выгружать драйверы устройств или управлять журналами безопасности и аудита.

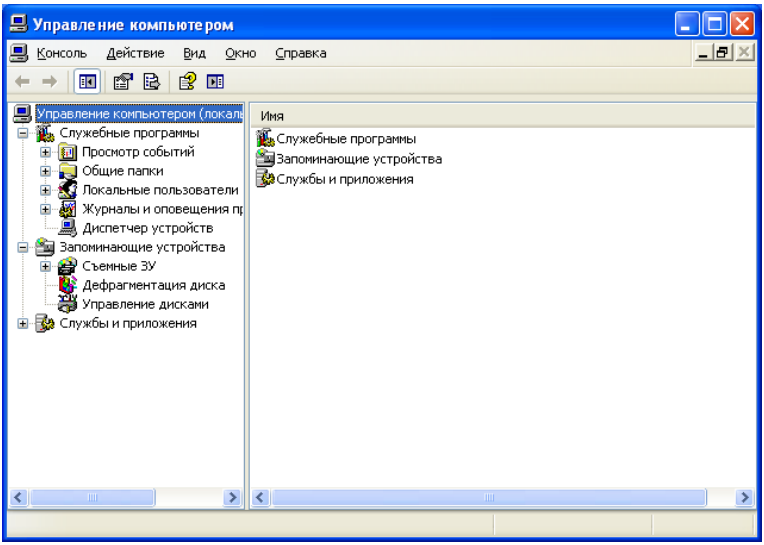
— Пользователи. Члены группы пользователей могут выполнять наиболее распространенные задачи, например запуск приложений, использование локальных и сетевых принтеров, завершение работы и блокировка рабочих станций. Пользователи могут создавать локальные группы, но изменять могут только те, которые они создали. Пользователи не могут организовывать общий доступ к каталогам или создавать локальные принтеры.

— Гости. Группа "Гости" позволяет случайным или разовым пользователям войти в систему со встроенной учетной записью гостя рабочей станции и получить ограниченные возможности. Члены группы "Гости" могут только прекратить работу компьютера.

Управление учетными записями пользователей и группами осуществляется пользователями, входящими в группу Администраторы.

Задание

Для управления учетными записями используется компонент "Управление компьютером". Чтобы его открыть выберите Пуск → Настройка → Панель управления. Дважды щелкните значок «Администрирование» затем дважды щелкните значок «Управление компьютером». Второй способ открыть «Управление компьютером» нажать правой кнопкой на значке «Мой компьютер» и в появившемся контекстном меню выбрать «Управление».

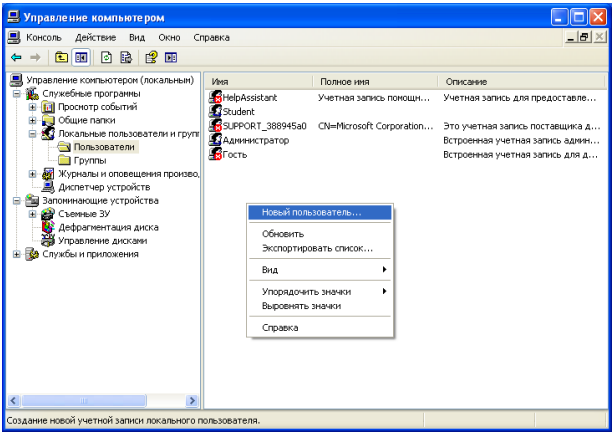


1. Создание новой учетной записи пользователя

Откройте компонент "Управление компьютером" одним из описанных выше способов.

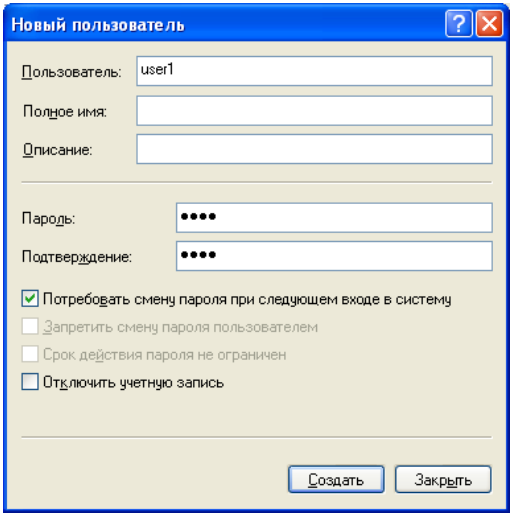
В дереве консоли (слева) выберите компонент "Локальные пользователи и группы" и щелкните в нем узел Пользователи.

Нажмите правой кнопкой мыши в окне со списком пользователей и в появившемся меню выберите команду Новый пользователь.



В появившемся окне заполните поля «Пользователь», содержащее имя, под которым пользователь будет входить в

систему, а также «Пароль» и «Подтверждение».



По умолчанию в данном окне стоит опция «Потребовать смену пароля при следующем входе в систему». То есть система при первом входе пользователя в ОС потребует от него сменить пароль. Если убрать галочку с этого пункта, появится возможность выбрать следующие опции:

— запретить смену пароля пользователем. То есть пользователь будет использовать пароль, заданный при создании учетной записи;

— срок действия пароля не ограничен — то есть пароль никогда не истекает.

Опция «Отключить учетную запись» делает вход в систему данного пользователя невозможным.

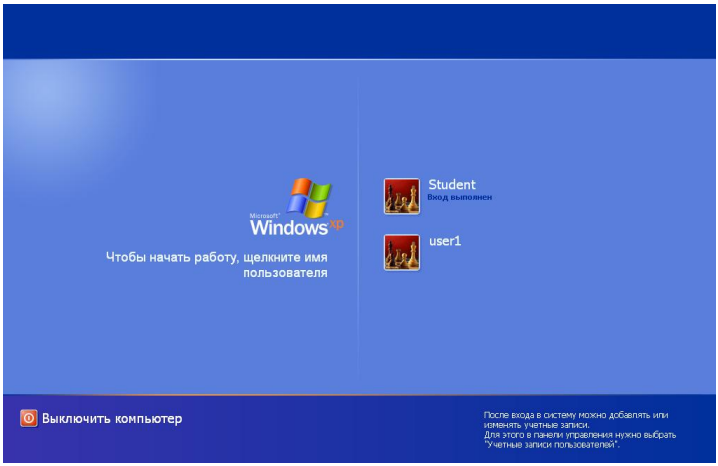
Чтобы завершить работу, нажмите кнопку Создать, а затем Закрыть.

Если есть необходимость в создании сразу нескольких пользователей нужно нажать на Создать и повторить все предыдущие шаги.

После этого созданный пользователь появится в списке. Сделайте скриншот полученного результата.

Войдите от имени только что созданного пользователя. Для этого нажмите «Пуск» → «Выход из системы» → «Смена пользователя».

На появившемся экране выберите созданного пользователя «user1» и введите заданный для него при создании пароль.



Появится окно с сообщением о необходимости изменения пароля. Задайте новый пароль и сделайте скриншот окна в котором проводились изменения.

Вернитесь обратно к пользователю «Student». Для этого нажмите «Пуск» → «Выход из системы» → «Выход».

Разница между вариантами выхода из системы «Смена пользователя» и «Выход» заключается в том, что при смене пользователя все процессы, запущенные им, продолжают выполняться, а при выходе завершаются. Если завершить работу, используя учётную запись одного пользователя, пока второй остаётся в системе, это может привести к потере несохраненных данных приложений второго пользователя.

2. Изменение пароля пользователя

Выберите учетную запись, которую требуется изменить (user1).

В контекстном меню выберите пункт "Задать пароль".

В появившемся окне введите новый пароль и сделайте скриншот результата.

Войдите в систему от имени пользователя «user1» используя новый пароль.

Аналогичным образом задайте пароль учётной записи «Student» или другой, созданной во время установки Windows учётной записи.

3. Отключение и активизация учетной записи пользователя

Выберите учетную запись «user1».

В контекстном меню выберите Свойства.

Чтобы отключить выбранную учетную запись пользователя,

установите флажок "Отключить учетную запись".

Попробуйте войти от имени «user1». Сделайте скриншот результата.

4. Удаление учетной записи пользователя

Выберите учетную запись «user1».

В контекстном меню учетном записи выберите Удалить.

Появится окно, предупреждающее о последствиях удаления пользователя.

Выберите ДА. Сделайте скриншот полученного результата.

5. Изменение локального профиля по умолчанию.

Все настройки компьютера для конкретного пользователя, включая личные параметры интерфейса и пользовательской среды, содержатся в профиле пользователя.

Профиль создается при первом входе пользователя на компьютер под управлением операционной системы Windows XP, Windows 2000 или Windows NT и представляет собой ряд параметров и файлов, определяющих пользовательскую среду при входе в систему. В него входят настройки приложений, сетевые подключения и принтеры, настройки мыши, а также оформление и расположения окон. Профили не являются пользовательскими политиками.

Профили пользователей хранятся по умолчанию в папке C:\Documents and Settings.

Пользовательские профили призваны разделить обеспечить независимость данных и настроек для каждого пользователя и локального компьютера.

Профиль пользователя составляют:

— Раздел системного реестра (куст). Реестр представляет собой базу данных общих и личных настроек пользователей. Части реестра могут быть сохранены в файлы, именуемые кустами. Такие кусты можно загрузить в реестр при необходимости. Преимущества этой технологии легли в основу функциональности перемещаемых профилей. Куст пользовательского профиля, по сути, представляет собой файл NTuser.dat, загружающийся в раздел реестра HKEY_CURRENT_USER при входе пользователя в систему. Файл NTuser.dat сохраняет все изменения настроек пользовательской среды, произведенные в течение сеанса. В этом файле сохраняются настройки сетевых подключений, конфигурация элементов панели управления, уникальных для каждого пользователя (например, обои на рабочем столе или настройки

мыши), а также настройки приложений. Большинство пользовательских настроек доступно для изменения компонентам операционной системы и сторонним приложениям.

— Набор папок профиля, хранящийся в файловой системе. Файлы пользовательских настроек хранятся в специально отведенном для этого каталоге. При этом для каждого пользователя создается отдельная папка, которую операционная система и приложения в процессе работы наполняют подпапками и файлами данных пользователя. Такими файлами могут быть ярлыки, иконки рабочего стола, автоматически загружаемые приложения, документы, конфигурационные файлы и т.д.

При создании нового пользователя начальные настройки его профиля берутся из так называемого локального профиля по умолчанию, который находится в папке C:\Documents and Settings\Default User. Содержимое данной папки копируется в папку с профилем создаваемого пользователя, поэтому можно задать настройки для всех вновь создаваемых пользователей изменив настройки профиля по умолчанию.

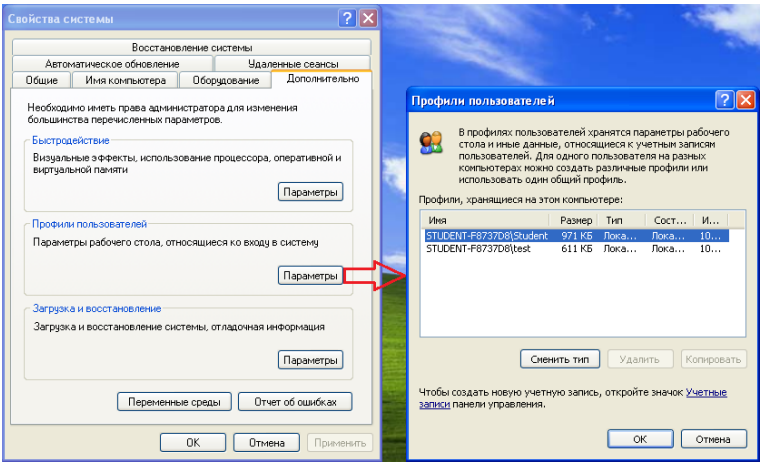
Для этого выполните следующие действия.

Создайте нового пользователя с любым именем, например «test».

Войдите от его имени и поменяйте следующие настройки: установите классическую тему оформления и создайте на рабочем столе текстовый файл с именем, например, «Привет, новый пользователь».

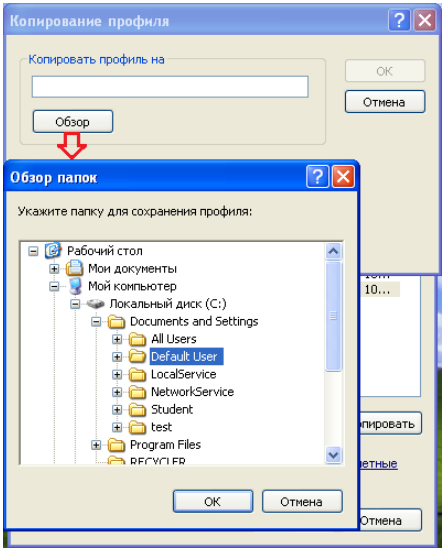
Выйдите из системы и зайдите от пользователя «Student» или любого другого с правами администратора.

Нажмите правой кнопкой на моём компьютере, выберите пункт «Свойства», перейдите на вкладку «Дополнительно» и нажмите кнопку «Параметры», отвечающую за профили пользователей. Появится окно, в котором перечислены все созданные на компьютере профили.



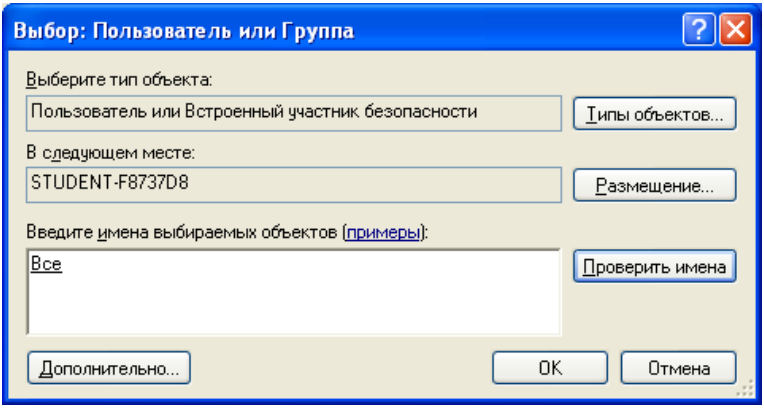
Выберите профиль «test» и нажмите кнопку «Копировать». Появится окно копирования профиля, в котором необходимо задать путь и разрешения.

Нажмите на кнопку «Обзор» и в появившемся окне выберите путь C:\Documents and Settings\Default User и нажмите «OK».



В поле «Разрешить использование» нажмите «Изменить». Появится окно выбора пользователя или группы. Чтобы разрешить использовать профиль всем пользователям компьютера, в

нижнем поле ввода введите «Все» и нажмите «Проверить имена». После этого нажмите «ОК».



После завершения копирования профиля создайте еще одного пользователя (например «user2») и войдите от его имени. Сделайте скриншот результата.

6. Управление группами пользователей

Пользователь, принадлежащий группе, имеет все права на разрешения, предоставленные этой Группе. Пользователь, являющийся членом нескольких групп, имеет все права и разрешения, предоставленные каждой из этих групп.

При удалении локальной группы удаляется учетная запись группы. Учетные записи пользователей, являющихся членами удаленной группы, при этом не удаляются.

Вновь созданные пользователи попадают в группу «Пользователи». Чтобы убедиться в этом откройте компонент "Управление компьютером", в дереве консоли выберите "Локальные пользователи и группы" и щелкните в нем узел Группы после чего появится список существующих групп.

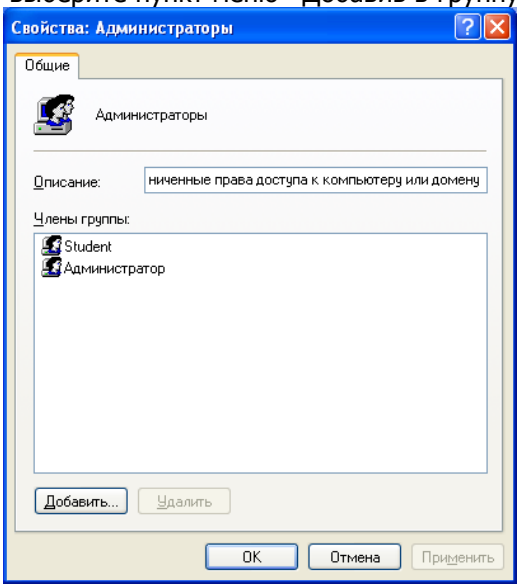
Нажмите дважды на группу «Пользователи» и посмотрите, какие учётные записи входят в эту группу. Сделайте скриншот данного окна.

Попробуйте от имени пользователя «user2» создать файл на диске C:. Пользователи группы «Пользователи» не имеют данного права, поэтому будет выдано сообщение о невозможности выполнения данной операции. Сделайте его скриншот.

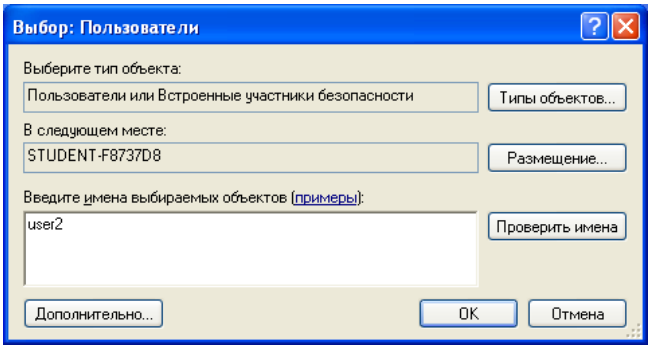
Выйдите из системы и зайдите от имени пользователя «Student».

Добавьте пользователя «user2» в группу «Администраторы». Для этого нажмите правой кнопкой на

имени группы и выберите пункт меню «Добавить в группу…».



Появится окно выбора пользователя. Введите имя «user2» и нажмите «OK».



Зайдите снова от имени «user2» и создайте на диске C: любой файл. Сделайте скриншот результата.

Контрольные вопросы

1. Какой компонент используется для управления учётными записями пользователей и как получить к нему доступ?
2. Кто может осуществлять управление учётными записями?
3. Как создать нового пользователя?

4. В чём разница между выходом из системы и сменой пользователя?
5. Как сменить пароль учётной записи?
6. Что такое отключение учётной записи? Чем оно отличается от удаления? Как отключить учётную запись?
7. Что такое локальный профиль по умолчанию?
8. Как изменить локальный профиль по умолчанию?
9. Для чего предназначены группы пользователей?
10. Как добавить пользователя в группу?

ЛАБОРАТОРНАЯ РАБОТА № 4

Тема: Управление правами доступа в Windows XP.

Цель: изучить способы управления правами доступа к файлам и папкам.

Теоретические сведения

Для каждого объекта, который хранится в томе NTFS, поддерживается контрольный список доступа (ACL). Этот список определяет перечень пользователей, которым разрешен доступ к данному объекту. Каждая запись в таком списке именуется ACE (access control entry). Для того, чтобы разрешить или отказать в доступе к объекту (файлу или папке), необходимо модифицировать ACE. Делать это могут владельцы объекта, члены группы "Администраторы" и обычные пользователи, которым разрешили это сделать либо первые, либо вторые.

В Windows XP при включенной опции "Использовать простой общий доступ ко всем файлам" возможности по изменению прав доступа весьма ограничены. Заблокировав эту опцию (в меню "Проводника": "Сервис" > "Свойства папки" > "Вид"), получите доступ к набору прав NTFS.

В Windows XP управление доступом к ресурсам реализовано с помощью набора предопределенных базовых прав доступа (их шесть): полный доступ, чтение, запись и так далее. Но есть еще и одиннадцать специальных прав доступа, с помощью которых разрешения настраиваются более тонко. Добраться к ним можно, нажав "Дополнительно" на вкладке "Безопасность", после чего нужно два раза щелкнуть на имени пользователя. Использование предопределенных прав упрощает процесс администрирования. Фактически, если вы устанавливаете флаг "Чтение и выполнение", операционная система (ОС) сама устанавливает пять отдельных прав доступа: выполнение файлов; чтение данных, атрибутов, дополнительных атрибутов, разрешений. Считается, что шести предопределенных прав в обычных случаях вполне достаточно.

Права доступа предоставляются установкой флажка в столбце "Разрешить". Флажки "Запретить" устанавливаются, когда требуется явно запретить применение указанного права доступа пользователю. Они имеют высший приоритет, по сравнению с разрешениями, и применяются, в основном, для внесения ясности при наложении прав нескольких пользователей. Если требуется полностью блокировать доступ к объекту, выберите для ненави-

стного пользователя "Запретить" в строке "Полный доступ".

Кроме прав доступа, устанавливаемых индивидуально, объекты могут наследовать их от родительских папок. По умолчанию, разрешения передаются от папки всем подпапкам. Для просмотра опций наследования следует на вкладке "Безопасность" выбрать "Дополнительно". Если в Windows 2000 единственным признаком наследования являлось затемнение пиктограммы ключей, то в XP появился даже специальный столбец "Унаследовано от". Дважды щелкнув по соответствующей записи пользователя, можно будет указать метод наследования разрешений: для этой папки ее подпапок и файлов, только для этой папки и так далее.

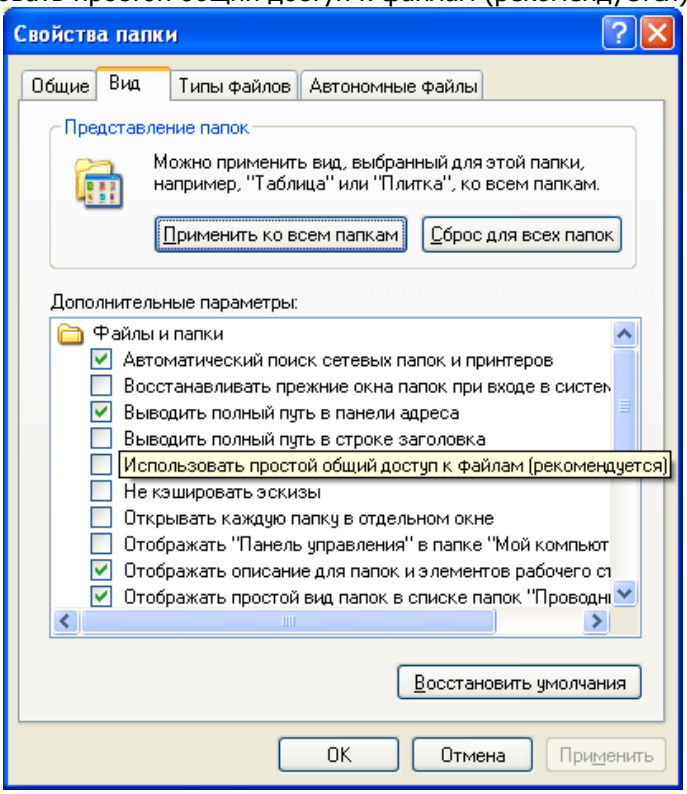
Для отмены наследования в дополнительных параметрах безопасности следует убрать флажок "Наследовать от родительского объекта..." Имейте в виду, что при удалении наследуемых папкой прав она сама становится новым родительским объектом. По умолчанию, любые права доступа, присваиваемые этой папке, будут передаваться вниз по иерархии к вложенным подпапкам.

Нередко случается, что перемещенные или скопированные объекты получают совершенно новые права доступа. Может быть даже такое, что двойной щелчок по файлу может привести к сообщению "Доступ запрещен", даже если пользователю предоставлены все возможные права к текущей папке. Чтобы понять причины возникновения подобных проблем, необходимо разобраться с тем, что происходит, когда мы перемещаем или копируем объекты с одного места на другое. Естественно, в нашем случае речь идет только о дисках с файловой системой NTFS.

Каждый файл или папка в разделе NTFS имеют владельца, который может предоставлять или отказывать в правах доступа другим пользователям или группам. Владельцы могут заблокировать любого пользователя, включая членов группы "Администраторы". Владелец может предоставлять свои права другому пользователю, если тот является членом группы "Администраторы". Если же другой пользователь имеет ограниченную учетную запись, то вначале нужно изменить ACE объекта и разрешить пользователю полный доступ к файлу или папке, чтобы затем передать ему право владения. Кроме того, любой администратор может получить право собственности на любой объект, хотя и не может передать это право другим пользователям. Меняется владелец здесь: закладка "Безопасность" > "Дополнительно" > "Владелец".

Задание

Для выполнения данной лабораторной работы потребуется включить расширенные настройки общего доступа к папкам. Для этого необходимо выбрать пункт меню «Сервис» → «Свойства папки», перейти на вкладку «Вид» и снять галочку с пункта «Использовать простой общий доступ к файлам (рекомендуется)».



1. Создайте на диске C:\ папку с именем test и удалите все установленные для неё по умолчанию разрешения. Для этого:

— нажмите правой кнопкой на папку и выберите пункт контекстного меню «Свойства»;

— перейдите на вкладку «Безопасность»;

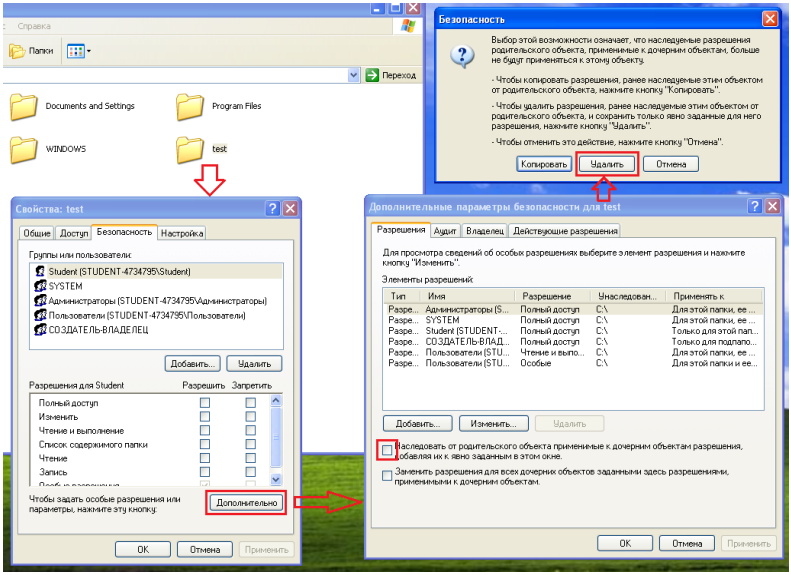
— нажмите кнопку «Дополнительно»;

— в появившемся диалоговом окне снимите галочку с пункта «Наследовать от родительского объекта применимые к дочерним объектам разрешения, добав- ляя их к явно заданным в этом

окне»;

— в следующем окне нажмите кнопку «Удалить».

Вернувшись к окну «Дополнительные параметры безопасности для test» нажмите кнопку «Применить». Сделайте скриншот полученного результата.



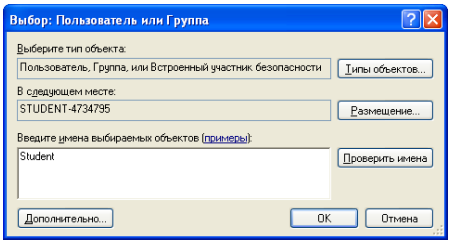
Попытайтесь выполнить какое-либо действие с папкой test (например открыть, скопировать или удалить). Объясните полученные результаты.

2. Разрешите текущему пользователю просмотр содержимого папки. Для этого:

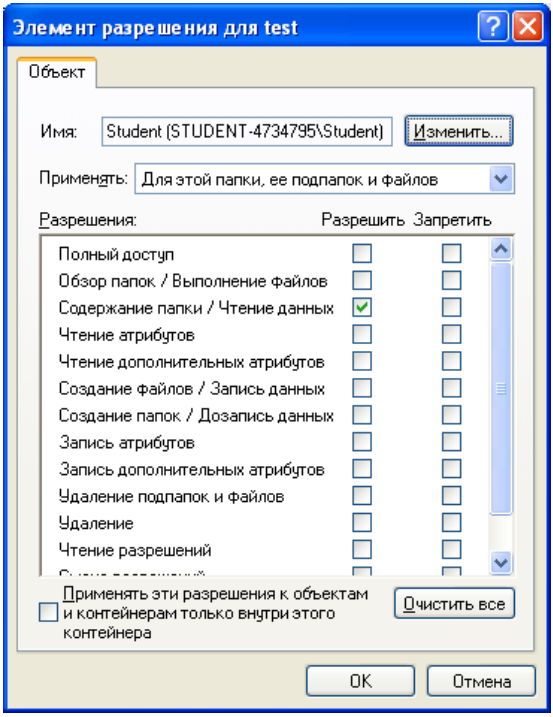
— откройте окно дополнительные параметры безопасности;

— нажмите кнопку «Добавить»;

— в появившемся окне введите имя текущего пользователя и нажмите «OK»;



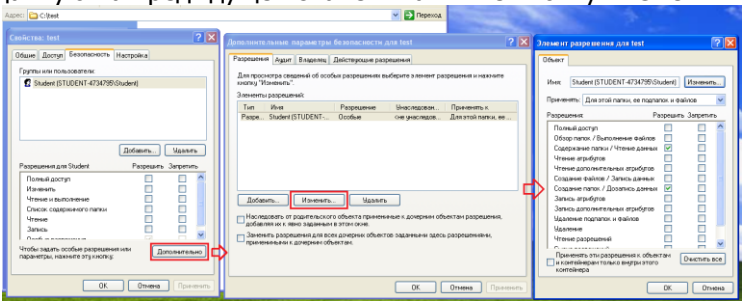
— в следующем окне поставьте галочку в столбце «Разрешить» напротив «Содержание папки / Чтение данных» и нажмите «ОК»;



— нажмите «Применить» и зайдите в папку test.

3. Попытайтесь создать в папке test еще одну папку или файл. После сообщения об отказе в доступе выдайте соответствующие права текущему пользователю. Для этого:

— в окне дополнительных параметров безопасности выделите строку, отвечающую за разрешения текущего пользователя, созданную на предыдущем этапе и нажмите кнопку «Изменить».



— в появившемся окне поставьте галочку в столбце «Разрешить» напротив «Создание папок / Дозапись данных» и нажмите «ОК»;

— нажмите «Применить» и еще раз попытайтесь создать папку в папке test.

4. Проверьте наличие разрешений у созданной папки, сделайте скриншот результата и объясните откуда взялись данные разрешения.

5. Попытайтесь создать любой файл в папке test. После сообщения об отказе в доступе выдайте текущему пользователю права создание файлов по аналогии с предыдущим заданием.

6. Создайте в папке test пустой текстовый файл и попытайтесь записать в него какой-либо текст. После сообщения об отказе в доступе выдайте текущему пользователю следующие разрешения:

— Чтение атрибутов,

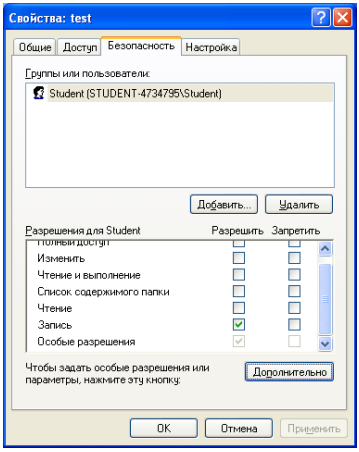
— Чтение дополнительных атрибутов,

— Запись атрибутов,

— Запись дополнительных атрибутов.

Снова попытайтесь записать в файл какой-либо текст. Сделайте скриншот текущего набора разрешений для папки test.

Обратите внимание что в окне свойств папки test на складке безопасность появилась галочка в столбце «Разрешить» напротив пункта «Запись».



Это произошло из-за того, что в окне дополнительных параметров безопасности пользователю были выданы специальные права доступа входящие в предопределённое базовое правило

«Запись».

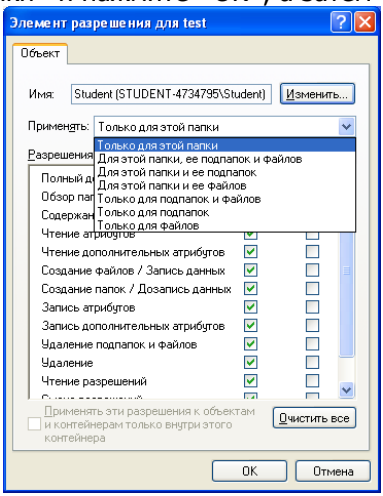
7. Удалите все выданные ранее разрешения и, последовательно ставя галочку напротив каждого из 6 предопределённых базовых правил в окне свойств папки, определите, какие специальные права (в окне дополнительных параметров безопасности) входят в него.

8. Разрешите текущему пользователю полный доступ к папке test и создайте в ней папку test2. Проверьте разрешения текущего пользователя в свойствах папки test2. Так как они были унаследованы от объекта более высокого уровня, то пользователь должен иметь к ней полный доступ.

В свойствах папки test2 поставьте галочку в графе «Запретить» напротив пункта «Запись» и попытайтесь создать в этой папке файл. Объясните полученный результат.

9. Откройте окно дополнительных параметров безопасности начальной папки test, выделите единственное заданное для неё правило и нажмите кнопку «Изменить».

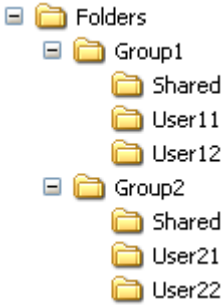
В появившемся окне выберите из выпадающего меню пункт «Только для этой папки» и нажмите «ОК», а затем «Применить».



Попытаётесь зайти в папку test2, проверьте права доступа к ней и объясните полученный результат.

Задание для самостоятельного выполнения

1. Создайте структуру папок, изображенную на рисунке:



2. Создайте пользователей user11, user12, user21, user22; а также две группы: group1 и group2. Поместите пользователей user11 и user12 в группу group1, а пользователей user21 и user22 в группу group2 соответственно.

3. Задайте права доступа к папкам в соответствии со следующими требо-ваниями:

— содержимое папки Folders может просматривать кто угодно

— никто не может создавать, удалять или изменять файлы и папки, находящиеся непосредственно в папке Folders

— просматривать содержимое папки Group1 могут только члены группы group1

— просматривать содержимое папки Group2 могут только члены группы group2

— только пользователь user11 может создавать новые папки внутри Group1 и назначать им владельцев

— только пользователь user21 может создавать новые папки внутри Group2 и назначать им владельцев

— все пользователи, входящие в группу group1, могут записывать файлы в папку Group1\Shared, но не могут их оттуда удалять

— все пользователи, входящие в группу group2, могут записывать файлы в папку Group2\Shared, но не могут их оттуда удалять

— удалить файл из папки Shared может только тот, кто его туда записал

— каждый пользователь имеет к своей папке полный доступ

— никто из пользователей не может просматривать содержимое личных папок других пользователей

Контрольные вопросы

1. как получить доступ к набору прав NTFS?
2. Кто может изменять права доступа к файлу?
3. Какие существуют предопределённые права доступа?
4. Какие существуют специальные права доступа?
5. Приоритеты прав доступа к файлу.
6. Кто и что сможет делать с файлом или папкой, если для него не заданы никакие разрешения?
7. Что такое наследование прав доступа?

ЛАБОРАТОРНАЯ РАБОТА № 5

Тема: Локальная политика безопасности.

Цель: Изучить возможности настройки локальных политик безопасности для установки требований к паролям и учётным записям, блокировки нежелательных программ и сетевых соединений.

Теоретические сведения

Безопасность операционной системы основана на правилах, регулирующих разные аспекты ее работы. Вместе эти правила составляют единую политику безопасности. В Windows 2000 и более поздних ОС семейства Windows NT политика безопасности представляет собой часть групповой политики. В свою очередь, она состоит из набора правил, объединенных в следующие группы:

— Политики учетных записей. Регулируют работу с паролями, условия блокировок и политику Kerberos в доменах.

— Локальные политики. Включают правила аудита событий, назначения привилегий пользователям и группам и некоторые возможности защиты.

— Политики открытого ключа. Позволяют настроить, в частности, правила использования файловой системы с шифрованием (EFS, Encrypted File System). Эти политики и все последующие являются дополнительными, они не используются в шаблонах безопасности и не анализируются и не настраиваются оснасткой Анализ и настройка безопасности. О них мы говорить не будем.

— Политики ограниченного использования программ. Разрешают/запрещают запуск программ пользователям.

— Политики безопасности IP. Определяют настройки фильтров IP, а также использование шифрования пакетов.

Политики учетных записей

Данные правила подразделяются на две группы: политика паролей и политика блокировки учетной записи.

Правила паролей задают требования, предъявляемые к паролям пользователей системы.

Так как среди взломщиков популярностью пользуются атаки, заключающиеся в подборе пароля по заранее составленному файлу с набором типичных паролей («словарная атака») и просто грубому перебору всех возможных комбинаций символов («brute

force»), то необходимо принять меры, страхующие систему от подобных методов взлома. Именно этим и занимается политика блокировки учетной записи. Здесь можно установить количество ошибочных попыток набора пароля до блокировки учетной записи, срок этой блокировки и период сброса счетчика неудачных попыток ввода пароля. Это мощное средство, однако им нужно пользоваться с осторожностью, так как возможен обратный эффект от его действия — взломщик может просто заблокировать аккаунт администратора, перешагнув порог блокировки учетной записи своими попытками подобрать пароль. Именно для этого существует правило, задающее срок этой блокировки (он не должен быть слишком большим).

Локальные политики

Локальные политики определяют правила безопасности локального компьютера. Они делятся на три группы: политики аудита, назначение прав пользователя и параметры безопасности.

Политика аудита предписывает заносить в журнал Безопасность те или иные события (удачные и/или неудачные). После указания событий, требующих регистрации, можно указать конкретные объекты, за которыми будет вестись слежение (например, после разрешения аудита доступа к объектам можно в свойствах папки указать ведение аудита доступа для конкретных пользователей и/или групп).

Политики открытого ключа

Используя политики открытого ключа, администратор может автоматически выдавать сертификаты компьютерам, управлять агентами восстановления шифрованных данных, создавать списки доверия сертификатов и автоматически устанавливать доверительные отношения с центрами сертификации.

Политики ограниченного использования программ

С помощью политик ограниченного использования программ имеется возможность защищать компьютерное оборудование от программ неизвестного происхождения путем определения программ, разрешенных для запуска. В данной политике приложения могут быть определены с помощью правила для хеша, правила для сертификата, правила для пути и правила для зоны Интернета. Программное обеспечение может выполняться на двух уровнях: неограниченном и запрещенном.

Политики ограниченного использования программ регу-

лируют использование неизвестных программ и программ, к которым нет доверия. В организациях используется набор хорошо известных и проверенных приложений. Администраторы и служба поддержки обучены для поддержки этих программ. Однако, при запуске пользователем других программ, они могут конфликтовать с установленным программным обеспечением, изменять важные данные настройки или, что еще хуже, содержать вирусы или «троянские» программы для несанкционированного удаленного доступа.

При интенсивном использовании сетей, Интернета и электронной почты пользователи повсеместно сталкиваются с различными программами. Пользователям постоянно приходится принимать решения о запуске неизвестных программ, поскольку документы и веб-страницы содержат программный код — сценарии. Вирусы и «троянские» программы зачастую умышленно замаскированы для введения пользователей в заблуждение при запуске. При таком большом количестве и разнообразии программ отдельным пользователям трудно определить, какое программное обеспечение следует запускать.

Пользователем необходим эффективный механизм идентификации и разделения программ на безопасные и не заслуживающие доверия. После идентификации программы к ним может быть применена политика для определения, могут ли они быть запущены. Политики ограниченного использования программ предоставляют различные способы идентификации программного обеспечения и средства определения, следует ли запускать данное приложение.

Задание

Для выполнения лабораторной работы используется консоль «Локальная политики безопасности». Чтобы открыть её нажмите Пуск → Панель управления → Администрирование → Локальная политики безопасности.

1. Политика паролей.

Откройте вкладку «Политики учётных записей» → «Политика паролей».

Установите минимальную длину пароля — 8 символов.

Смените пароль любому из существующих пользователей и проверьте невозможность задания пароля длиной меньше 8 символов. Сделайте скриншот соответствующего сообщения.

Включите требование «Пароль должен отвечать требованиям сложности».

Смените пароль любому пользователю. Приведите примеры паролей отвечающих требованиям сложности и не отвечающих данным требованиям.

2. Блокировка учётных записей.

Откройте вкладку «Политики учётных записей» → «Политика блокировки учётной записи».

Измените параметр «Пороговое значение блокировки» на 3 «ошибок входа в систему».

Попытайтесь войти от имени любого пользователя, имеющего пароль, введя неправильный пароль 3 раза. Затем введите правильный пароль и снова попытайтесь выполнить вход.

Откройте консоль управления компьютером. Для этого нажмите на значке «Мой компьютер» правой кнопкой мыши и выберите пункт меню «Управление». Откройте папку «Локальные пользователи и группы» → «Пользователи» и дважды щелкните на пользователя от имени которого Вы пытались выполнить вход. Обратите внимание на установленный флажок «Заблокировать учётную запись». Сделайте скриншот окна свойств пользователя.

3. Аудит

В консоли «Локальная политика безопасности» откройте папку «Локальные политики» → «Политики Аудита» и в окне свойств каждого параметра установите флажки «Вести аудит следующих попыток доступа» в пунктах «Успех» и «Отказ».

Откройте консоль «Управление компьютером», выберите

раздел «Служебные программы» → «Просмотр событий» → «Безопасность».

Найдите последнюю по времени запись, относящуюся к категории «Изменение политики» откройте её и посмотрите описание события, в котором должны быть указаны новые настройки политик аудита, а ниже — пользователь, изменивший их. Текст описания события необходимо поместить в отчёт.

Попытайтесь войти под учетной записью, заблокированной в ходе выполнения предыдущего задания, и определите, какие записи в журнале аудита событий безопасности будут при этом созданы. Приведите в отчёте описание событий зарегистрированных в журнале.

Попытайтесь войти под учетной записью какого-либо пользователя, вводя неправильный пароль несколько раз до блокировки учётной записи. Найдите в журнале событий безопасности появившиеся при этом записи и приведите их в отчёте.

4. Политики прав пользователей и безопасности.

В консоли «Локальная политика безопасности» откройте папку «Локальные политики» → «Назначение прав пользователя».

Найдите параметр «Завершение работы системы» дважды щелкните на нём, чтобы открыть окно свойств и из перечисленных в нём групп удалите группу «Пользователи».

Зайдите от имени пользователя, входящего в эту группу, и попытайтесь завершить работу.

Сделайте скриншот результата.

Откройте «Локальные политики» → «Параметры безопасности».

Найдите параметр «Интерактивный вход в систему: Заголовок сообщения для пользователей при входе в систему» и окне его свойств в поле для ввода впишите любой заголовок сообщения (например «Сообщение»).

Найдите параметр «Интерактивный вход: текст сообщения для пользователей при входе в систему» и окне его свойств в поле для ввода впишите любой текст сообщения (например «Привет»).

Зайдите от имени любого пользователя и сделайте скриншот с окном сообщения, появляющимся при входе.

5. Запрет запуска программ

В консоли «Локальная политика безопасности» выделите папку «Политики ограниченного использования программ». В основном окне появится надпись «Политики ограниченного использования программ не определены».

Нажмите правой кнопкой мыши на папке «Политики ограниченного использования программ» и выберите пункт контекстного меню «Создать новые политики».

Зайдите в папку «Дополнительные правила». Нажмите правой кнопкой мыши и выберите пункт контекстного меню «Создать правило для хеша…».

В появившемся окне нажмите кнопку «Обзор…» и выберите хешируемый файл. Это может быть любой исполняемый файл какого-либо приложения (например калькулятор windows — C:\Windows\system32\calc.exe).

В выпадающем меню «Безопасность» оставьте значение не разрешено и нажмите «ОК».

Попытайтесь запустить калькулятор и сделайте скриншот результата. Правило, созданное для хеша применяется к фалу независимо от того где он находится. Можно переместить файл calc.exe в любую другую папку, и он по-прежнему не будет запускаться.

Создайте правило для пути. Для этого нажмите правой кнопкой на папке «Дополнительные правила» и выберите пункт «Создать правило для пути…».

В появившемся окне нажмите кнопку «Обзор…» и укажите путь к папке для которой требуется создать правило (например папка «Мои документы» текущего пользователя).

В выпадающем меню «Безопасность» оставьте значение не разрешено и нажмите «ОК».

Поместите в папку «Мои документы» любой исполняемый файл какой-либо программы (можно скопировать туда например файл regedit.exe из папки C:\Windows).

Попытайтесь запустить скопированный файл и сделайте скриншот результата.

Скопируйте еще один исполняемый файл в папку «Мои документы» (пусть теперь это будет блокнот C:\Windows\notepad.exe) и попытайтесь запустить его.

Создайте новой правило для хеша, устанавливающее неограниченный уровень безопасности и попытайтесь запустить его снова.

6. Блокировка сетевых соединений

Нажмите правой кнопкой на пункт «Политики безопасности IP на "Локальный компьютер"». В контекстном меню выберите «Управление списками IP-фильтра и действиями IP-фильтра…».

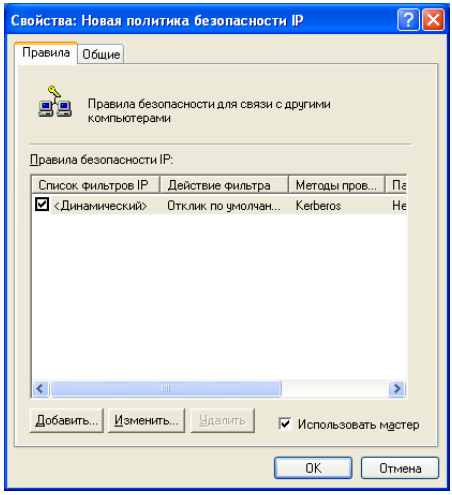
Перейдите на вкладку «Управление действиями фильтра» и нажмите на ней кнопку «Добавить…».

Запустится мастер настройки действий фильтра. В первом окне нажмите «Далее». В следующем окне введите имя «Запретить» и нажмите «Далее». В следующем окне выберите пункт «Блокировать» и нажмите «Далее». В следующем окне снимите галочку «Изменить свойства» и нажмите «Готово». Созданное действие фильтра появится в списке.

Закройте окно управления списками IP-фильтра и действиями IP-фильтра.

Нажмите правой кнопкой на пункт «Политики безопасности IP на "Локальный компьютер"». В контекстном меню выберите «Создать политику безопасности IP».

Запустится мастер политики IP-безопасности. В начальном окне нажмите «Далее», затем введите любое название политики и нажмите «Далее». Во всех остальных окнах не меняйте ничего, нажимайте далее и на все вопросы отвечайте «Да». После завершения процедуры создания новой политики появится окно её свойств.



Нажмите кнопку «Добавить…». Запустится мастер правил безопасности. На начальном экране нажмите «Далее..», на следующем экране выберите «Это правило не определяет туннель», затем выберите «Все сетевые подключения», далее «Стандарт

службы каталогов». В окне «Список фильтров IP» укажите «Полный IP трафик», нажмите «Далее…». В следующем окне «Действие фильтра» выберите созданное ранее действие «Запрет», нажмите далее. На следующем окне снимите галочку «Изменить свойства» и нажмите «Готово».

В списке политик безопасности IP появится созданная политика. Чтобы она начала применяться к сетевым соединениям, нажмите на ней правой кнопкой мыши и выберите пункт «Назначить».

Так как данная политика отвечает за блокировку всего IP-трафика, то теперь если попытаться зайти например на сервер (адрес \\10.1.0.1), то сделать это не удастся, как не удастся зайти и на любой другой адрес.

Для более тонкой настройки политики в свойствах правила безопасности следует указывать не «Полный IP трафик», а конкретные IP-адреса и протоколы.

Контрольные вопросы

1. Каким требованиям должен отвечать пароль при включении параметра «Пароль должен отвечать требованиям сложности»?
2. Что такое пороговое значение блокировки в политике учётных записей?
3. Что такое «Политики аудита»?
4. Что такое политики ограниченного использования программ?
5. Какие уровни безопасности могут использоваться в правилах политик ограниченного использования программ?
6. Чем отличается правило для хеша и правило для пути в политиках ограниченного использования программ?
7. Что такое политики безопасности IP?

ЛАБОРАТОРНАЯ РАБОТА № 6

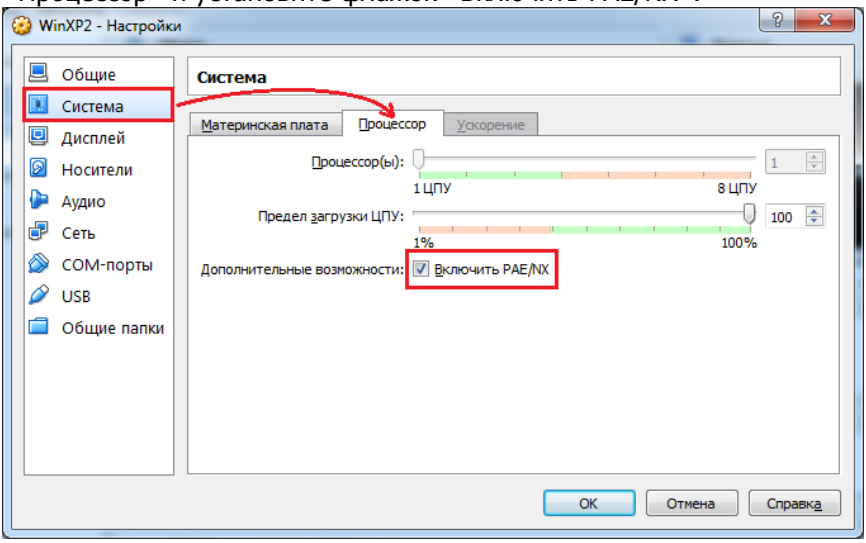
Тема: Установка ОС Linux.

Цель: Получить навыки установки ОС Linux на компьютер с уже установленной ОС Windows.

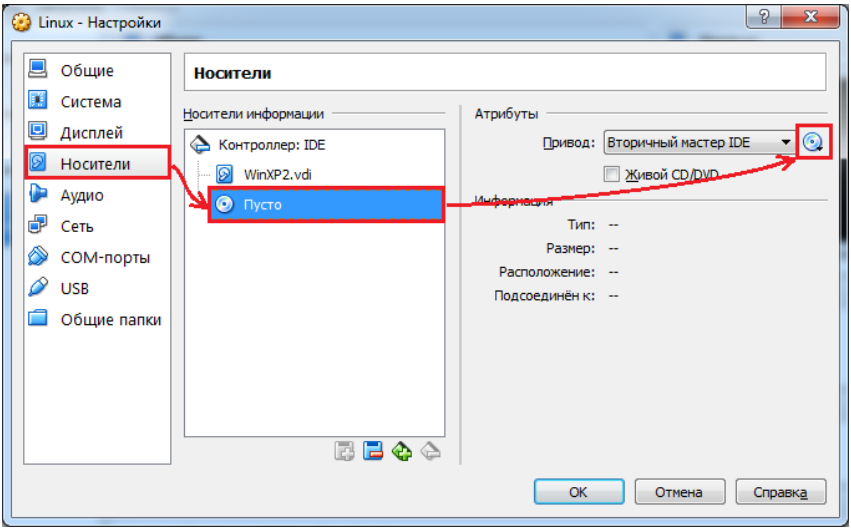
Задание

1) Настройка виртуальной машины

Выберите созданную ранее виртуальную машину с установленной операционной системой Windows XP и откройте окно её настроек. Перейдите в меню «Система», далее откройте кладку «Процессор» и установите флажок «Включить PAE/NX».



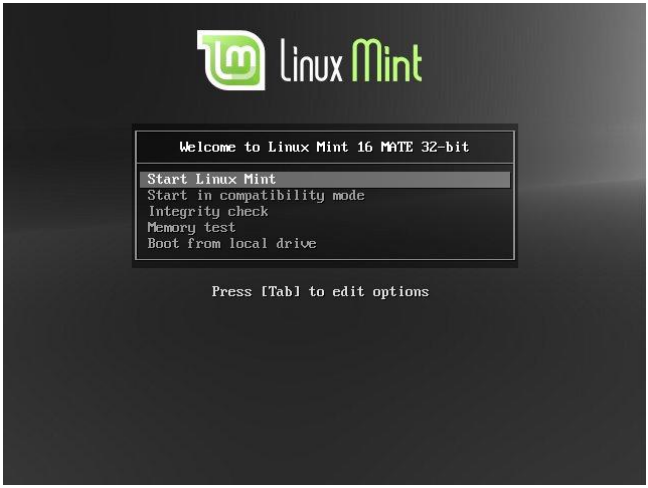
Перед запуском виртуальной машины необходимо подключить к ней файл образа загрузочного диска с дистрибутивом операционной системы. Для этого в настройках виртуальной машины перейдите в меню «Носители». В окне носителей информации выберите устройство, обозначенное значком компакт-диска, затем в панели его атрибутов нажмите на кнопку с изображением компакт-диска и в появившемся меню нажмите «Выбрать образ оптического диска…»



После настройки вирутальной машины и подключения диска с дистрибутивом Linux можно приступать к установке операционной системы.

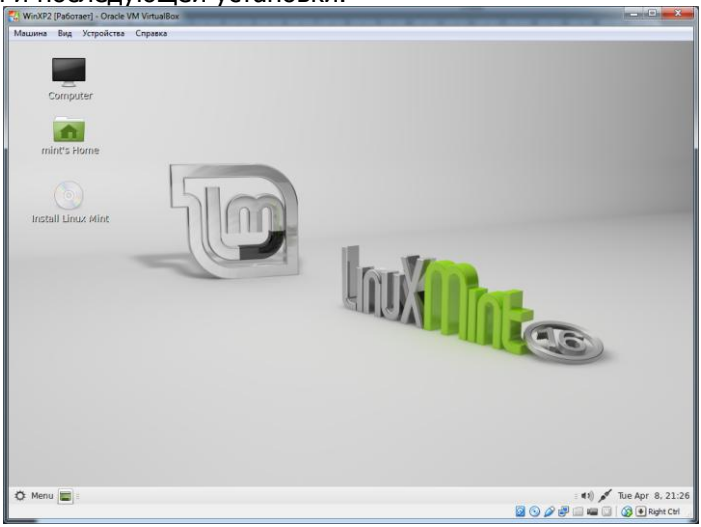
2) Установка Linux

Для запуска виртуальной машины выберите её из списка слева и нажмите кнопку «Запустить». При этом должна произойти загрузка с установочного диска Linux. Если нажать Enter до окончания обратного отсчёта, то появится загрузочное меню диска, в котором необходимо выбрать первый пункт «Start Linux Mint».

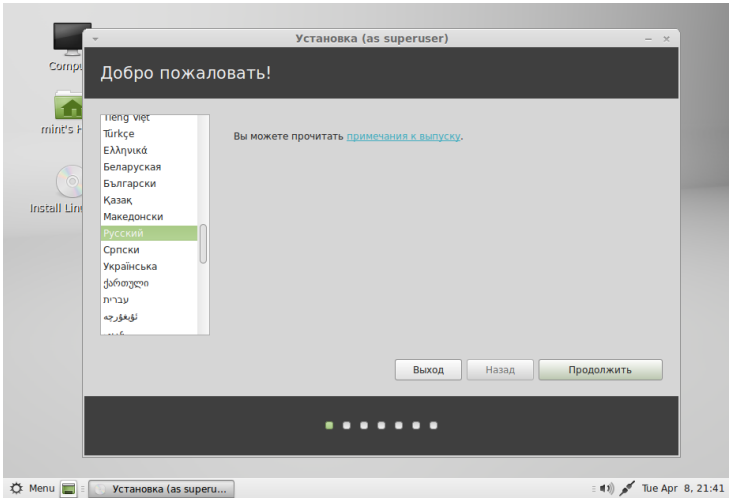


После выбора данного пункта, или если не нажимать ника-

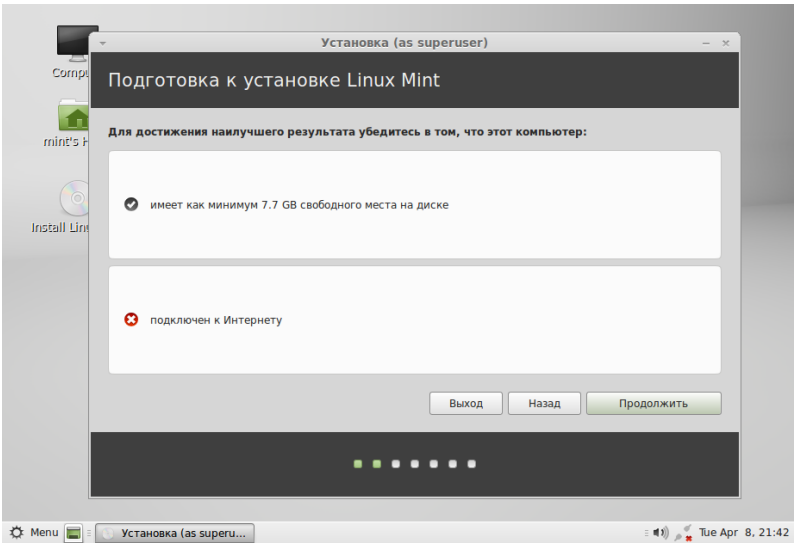
ких клавиш в процессе обратного отсчёта, будет загружена Live-версия Linux, предназначенная для ознакомления с его возможностями и последующей установки.



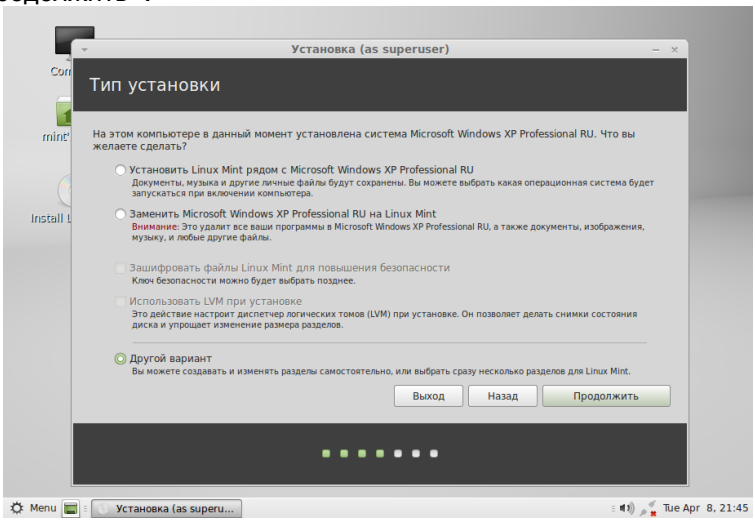
Щёлкните на значке «Install Linux Mint», находящемся на рабочем столе. В результате должно появиться окно установки Linux. Выберите из списка языков «Русский» и нажмите «Продолжить».



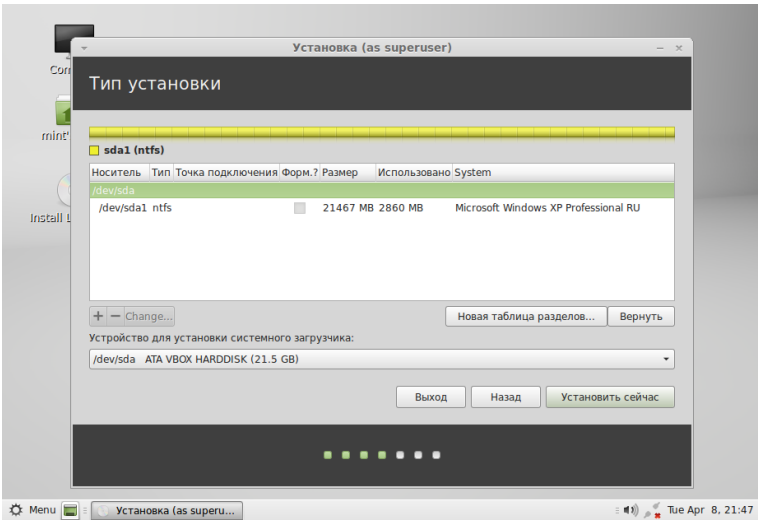
В следующем окне будет выдана информация о соответствии компьютера желательным (но не обязательным) условиям. Нажмите «Продолжить».



Следующее окно будет содержать информацию о том, что на компьютере уже установлена ОС Windows и предложены варианты дальнейших действий. Выберите «Другой вариант», чтобы самостоятельно определить все параметры установки и нажмите «Продолжить».

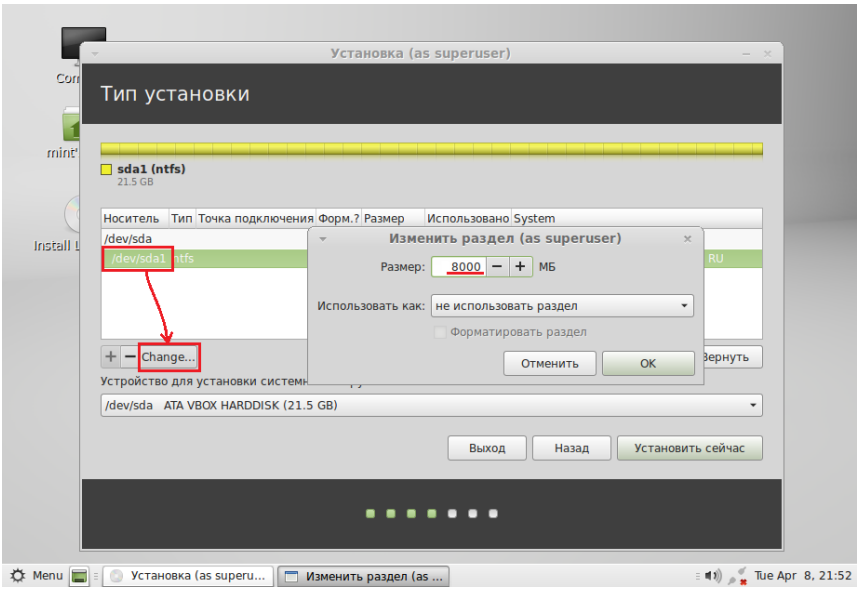


Следующее окно содержит информацию о структуре жёсткого диска (или всех дисков, если их несколько), имеющегося в компьютере.

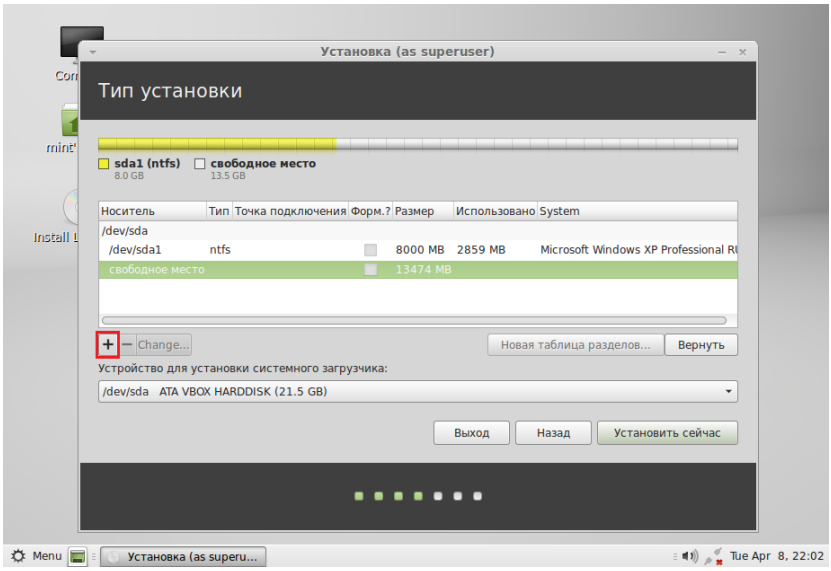


Как видно на рисунке, сейчас имеется один физический жёсткий диск, обозначенный как sda. На диске создан один раздел (sda1) с файловой системой ntfs, на который установлен Windows. Необходимо на этом же диске создать разделы для установки Linux.

Первым этапом нужно уменьшить размер раздела, выделенного под Windows, освободив место на диске. Для этого выделите раздел sda1, затем нажмите кнопку «Change…», в появившемся окне задайте новый размер раздела (например 8 ГБ) и нажмите «OK». Будет выдано предупреждение о том, что внесённые изменения будут записаны на диск и отменить их будет нельзя. Нажмите «Продолжить».



Возможно, изменение размера раздела займёт некоторое время, после чего будет показана новая структура диска, на которой будет видно появившееся в его конце свободное место. На свободном месте можно создавать новые разделы. Для этого нажмите кнопку «+» находящуюся ниже.



Для первого создаваемого раздела укажите следующие параметры:

Размер: 6000 МБ

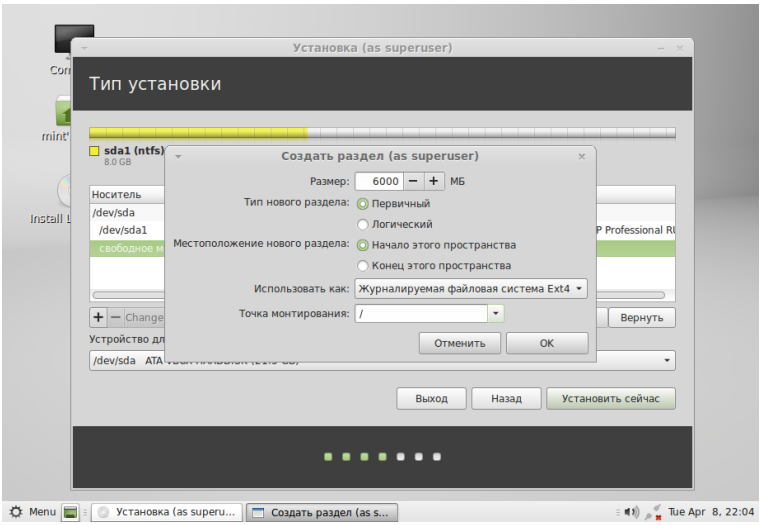
Тип: Первичный

Местоположение: Начало

Использовать как: Журналируемая файловая система Ext4

Точка монтирования: /

Нажмите «ОК».



Далее снова выделите свободное место и нажмите кнопку «+».

Для второго создаваемого раздела укажите следующие параметры:

Размер: 1000 МБ

Тип: Первичный

Местоположение: Начало

Использовать как: раздел подкачки

Нажмите «ОК».

Снова выделите свободное место и нажмите кнопку «+» чтобы создать третий раздел. Укажите для него следующие параметры:

Размер: всё оставшееся свободное место (установлено по умолчанию)

Тип: Логический

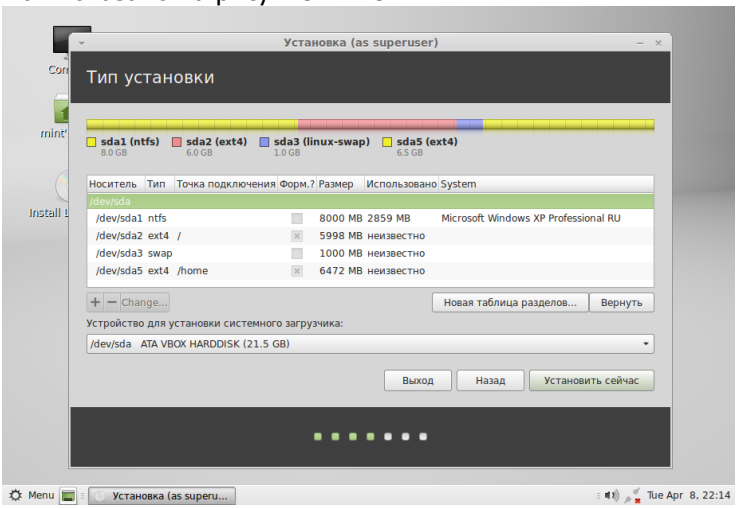
Местоположение: Начало

Использовать как: Журналируемая файловая система Ext4

Точка монтирования: /home

Нажмите «OK».

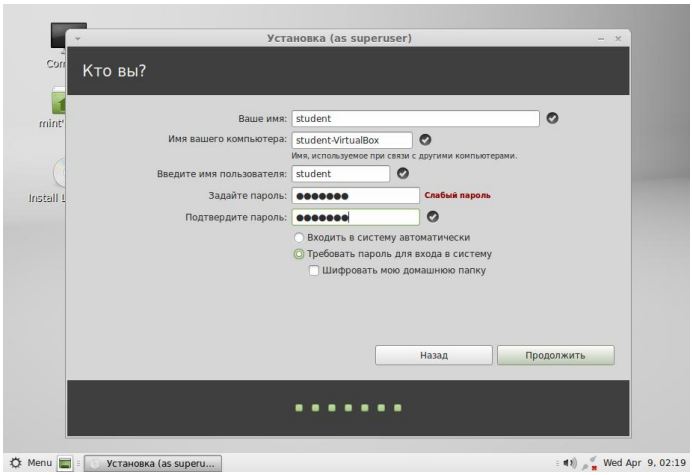
В результате таблица разделов диска должна выглядеть так, как показано на рисунке ниже.



После этого нажмите кнопку «Установить сейчас».

В следующем окне выберите правильный часовой пояс и нажмите «Продолжить». Далее выберите раскладку клавиатуры и также нажмите «Продолжить».

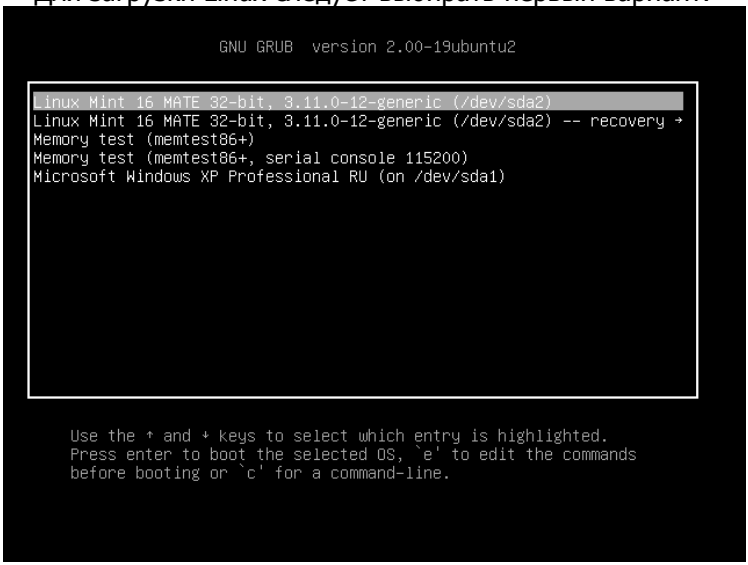
В окне настроек пользователя укажите данные пользователя (например, имя пользователя student, пароль student или любые другие). Оставьте выделенным пункт «Требовать пароль для входа в систему» и нажмите «Продолжить» после чего начнётся установка Linux.



По окончании установки виртуальную машину необходимо перезапустить.

После перезагрузки появится окно загрузчика Linux в котором представлены как различные варианты загрузки самого Linux, так и возможность загрузки Windows.

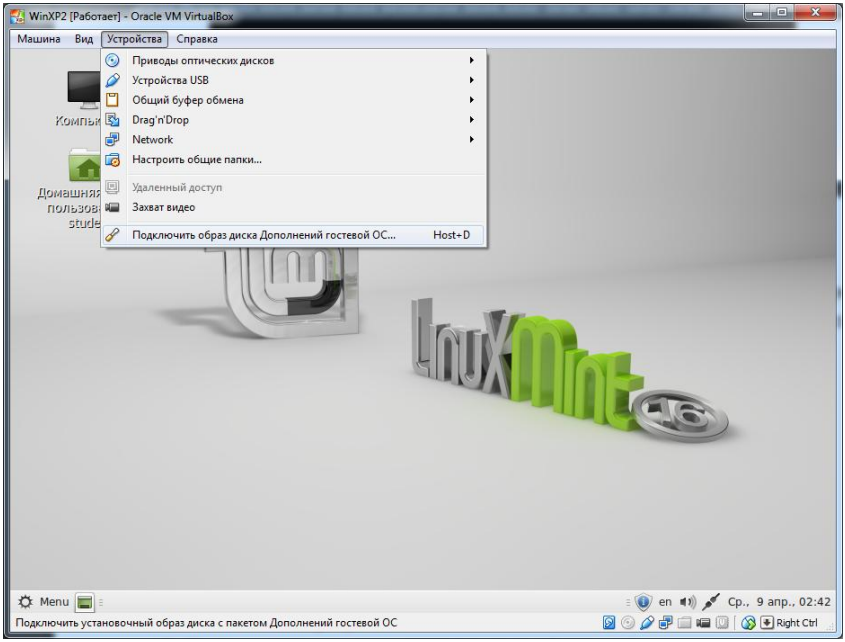
Для загрузки Linux следует выбирать первый вариант.



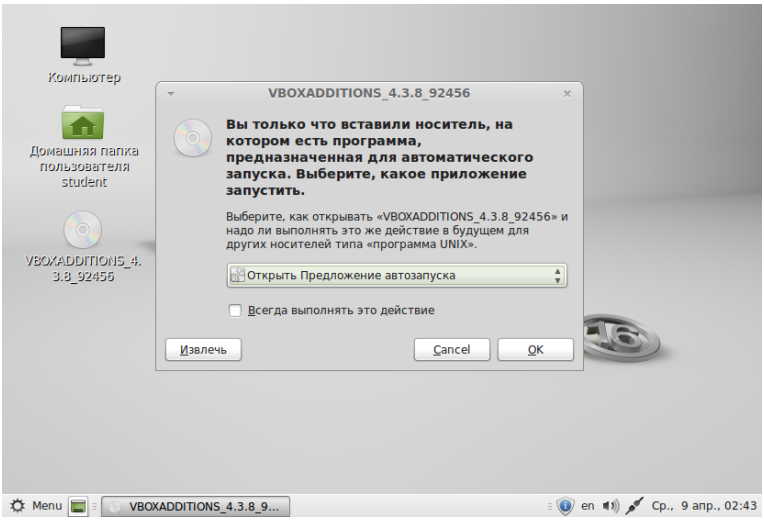
После загрузки выберите пользователя и введите заданный ранее пароль (переключение языка ввода осуществляется клавишами Shift+Alt). В результате появится рабочий стол с экраном приветствия.

3) Установка дополнений гостевой ОС.

Для установки дополнений выберите пункт меню виртуальной машины «Устройства» и далее «Подключить образ диска Дополнений гостевой ОС…».



В появившемся окне выберите «Открыть Предложение автозапуска» и нажмите «ОК».



В следующем окне нажмите «Запустить».

Дождитесь завершения установки и проверьте работу гостевой системы.

Контрольные вопросы

1. Что такое дистрибутив Linux?
2. В чём разница между различными дистрибутивами?
3. Что такое сектор и кластер?
4. Что такое раздел?
5. Где находится информация о разделах?
6. Что такое главная загрузочная запись и загрузочный сектор?
7. Что такое загрузчик?
8. Что такое файловая система?
9. Какие файловые системы поддерживает ОС Linux?
10. По какому принципу в Linux даются названия разделам диска?
11. Что такое точка монтирования?

ЛАБОРАТОРНАЯ РАБОТА № 7

Тема: Основы локального администрирования Linux.

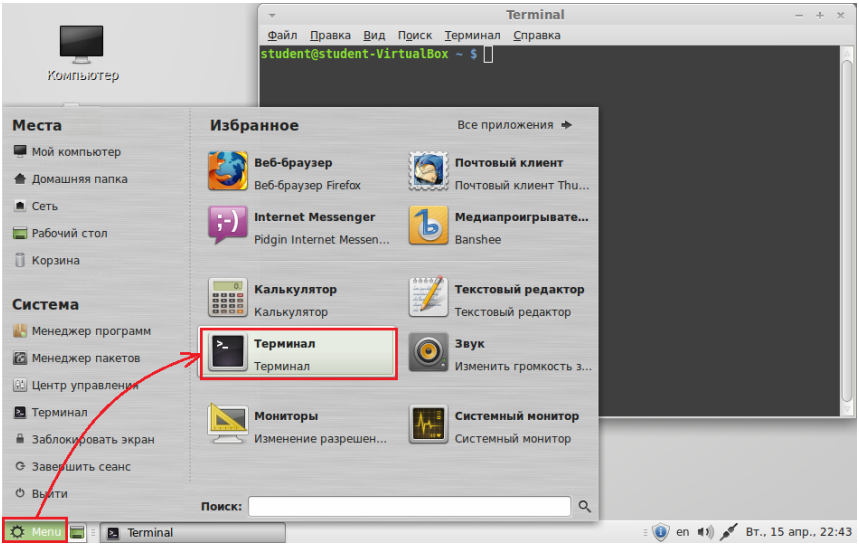
Цель: Получить начальные знания о способах настройки ОС Linux.

Задание

Монтирование разделов Windows

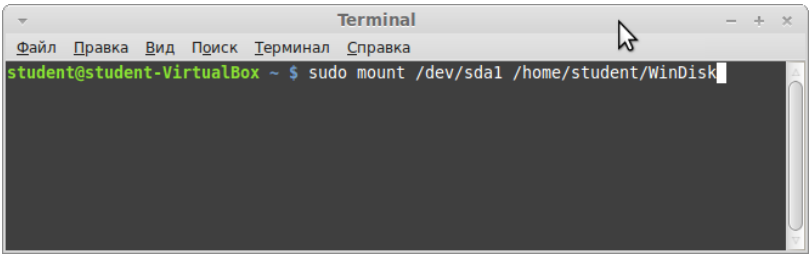
1. Создайте папку, которая будет служить точкой монтирования для раздела, на котором установлен Windows. Для этого зайдите в домашнюю папку пользователя, нажав на соответствующий значок на рабочем столе, в открывшемся окне нажмите правой кнопкой мыши и выберите пункт «Создать папку».

2. Откройте терминал. Для этого нажмите Menu → Терминал.



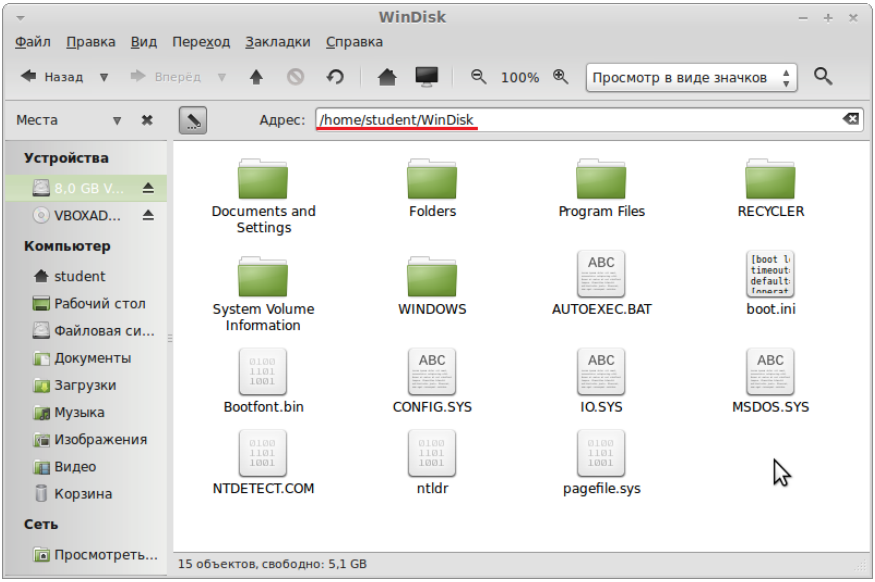
3. Выполните в терминале команду, приведённую на картинке

После выполнения команды появится надпись с запросом пароля. Пароль при вводе отображаться не будет.



sudo (англ. superuser do, дословно «выполнить от имени суперпользователя») — это утилита, предоставляющая привилегии root для выполнения административных операций в соответствии со своими настройками. Она позволяет легко контролировать доступ к важным приложениям в системе. По умолчанию, при установке Ubuntu и основанных на нём дистрибутивов (включая Mint) первому пользователю (тому, который создаётся во время установки) предоставляются полные права на использование sudo. Т.е. фактически первый пользователь обладает той же свободой действий, что и root.

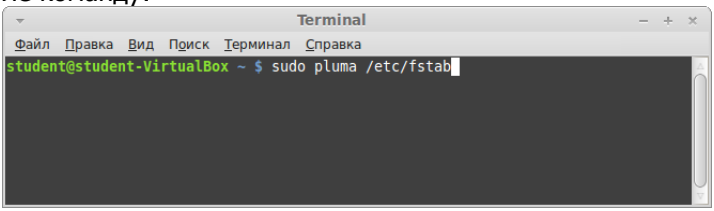
3. Проверьте, доступны ли смонтированные разделы в соответствующих папках. Для этого зайдите в домашнюю папку пользователя (в данном примере это /home/student) и далее в папку WinDisk.



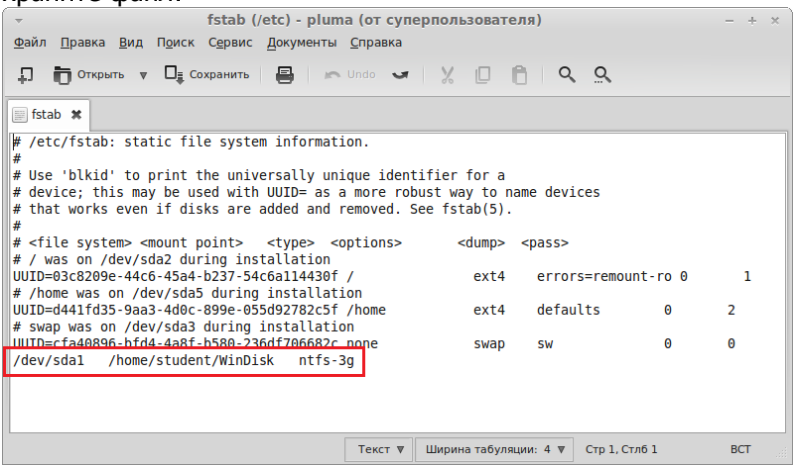
При таком способе монтирования, данные, содержащиеся на монтируемых разделах, перестанут быть доступны в указанных папках после перезагрузки. Чтобы избежать этого, можно настроить автоматическое монтирование при загрузке ОС.

Для этого:

1. Откройте файл /etc/fstab в текстовом редакторе (стандартный текстовый редактор, входящий в состав Linux Mint называется Pluma) от имени суперпользователя, выполнив в терминале команду:



2. Допишите в конец этого файла следующую строчку и сохраните файл:



В этой строчке:

/dev/sda1 — обозначение монтируемого раздела,

/home/student/WinDisk — точка монтирования,

ntsf-3g — имя драйвера файловой системы.

3. Перезагрузите компьютер и проверьте, что данные, хранящиеся на разделе, доступны в соответствующем каталоге.

Настройка сети

В VirtualBox, в зависимости от версии, имеются до 6 способов подключения виртуальной машины к сети:

- NAT (трансляция сетевых адресов), которая является настройкой по умолчанию;

- Сеть NAT;
- Сетевой мост;
- Внутренняя сеть;
- Виртуальный адаптер хоста;
- Универсальный драйвер.

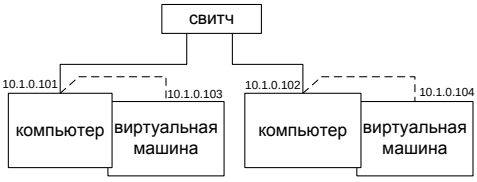
Протокол NAT позволяет гостевой операционной системе выходить в Интернет, используя при этом частный IP, который не доступен со стороны внешней сети, а также для всех машин локальной физической сети. Такая сетевая настройка позволяет посещать web-страницы, скачивать файлы, просматривать электронную почту. И все это, используя гостевую операционную систему. Однако извне невозможно напрямую соединиться с такой системой, если она использует NAT.

В режиме NAT гостевому сетевому интерфейсу присваивается по умолчанию IPv4 адрес из диапазона 10.x.0.0/24, где x обозначает конкретный адрес NAT-интерфейса. В случае одного виртуального сетевого адаптера, гостевая операционная система получает IP-адрес 10.2.0.15, а хостовой системе назначается адрес 10.2.0.2.

Протокол NAT полезен в том случае, когда нет разницы в том, какие IP-адреса будут использовать гостевые ОС на виртуальной машине. Однако, если потребуется настроить перенаправление сетевого трафика, или же расширить функциональность гостевой ОС, развернув на ней web-сервер, то необходимы дополнительные настройки. В режиме NAT также недоступны такие возможности, как предоставление общего доступа к папкам и файлам на виртуальной машине.

В соединении типа "Сетевой мост" виртуальная машина работает также, как и все остальные компьютеры в сети. В этом случае адаптер выступает в роли моста между виртуальной и физической сетями. Со стороны внешней сети имеется возможность напрямую соединяться с гостевой операционной системой. При этом виртуальная машина в сети выглядит так, как будто это обычное физическое устройство, неотличимое от остальных.

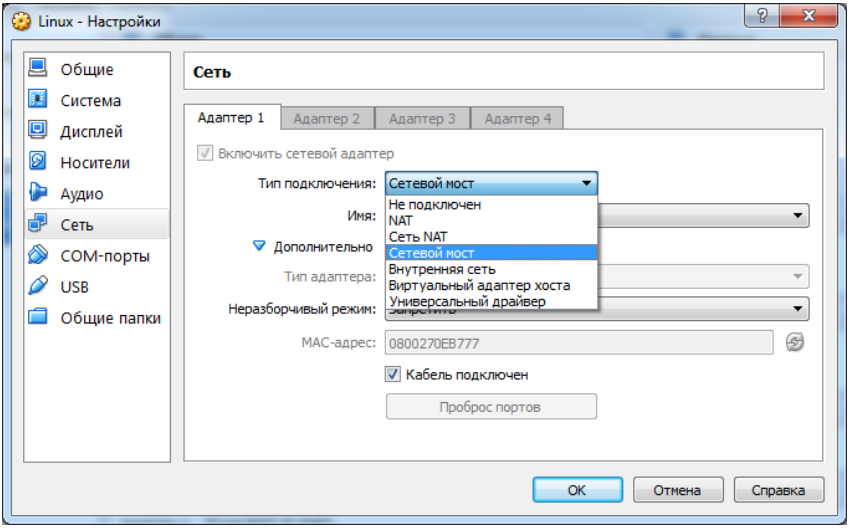
NAT



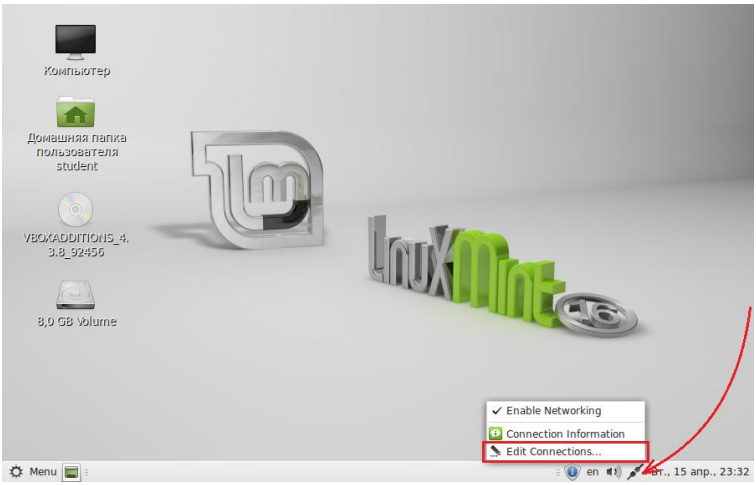
Мост

Настройте подключение виртуальной машины с Linux по типу «Мост».

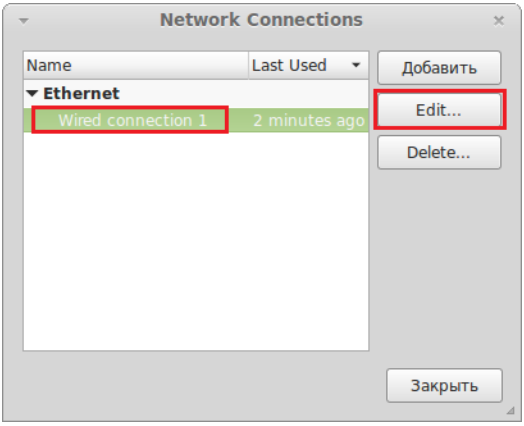
1. В меню «Сеть» окна настроек виртуальной машины задайте соответствующие настройки сетевого адаптера.



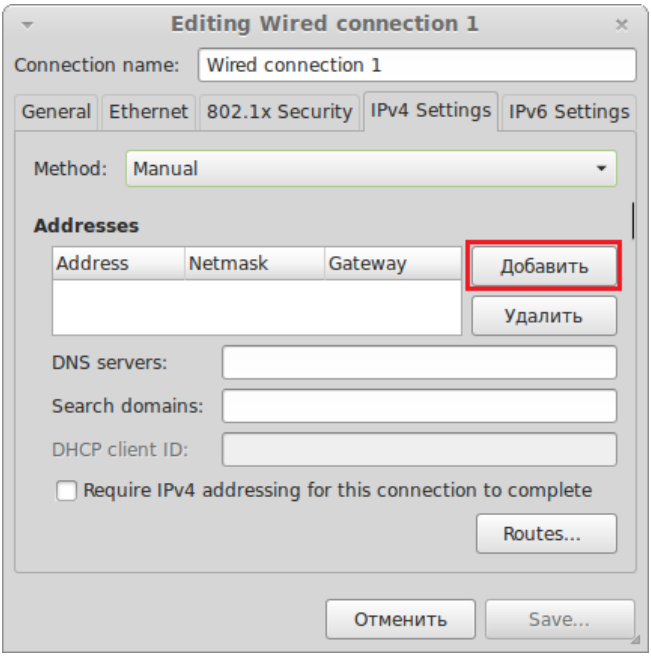
2. Откройте утилиту для настройки сети, щелкнув правой кнопкой мыши по значку сетевых подключений и выбрав в появившемся меню пункт «Edit Connections…».



3. В появившемся окне выберите соединение и нажмите кнопку «Edit…»



4. В следующем окне перейдите на вкладку «IPv4 Settings» из выпадающего меню Method выберите «Manual» (Вручную) и нажмите кнопку «Добавить».



5. Установите следующие настройки:

Address — 10.1.0.__;
Netmask — 255.255.255.0;
Gateway — 10.1.0.1;
DNS servers — 10.1.0.1;

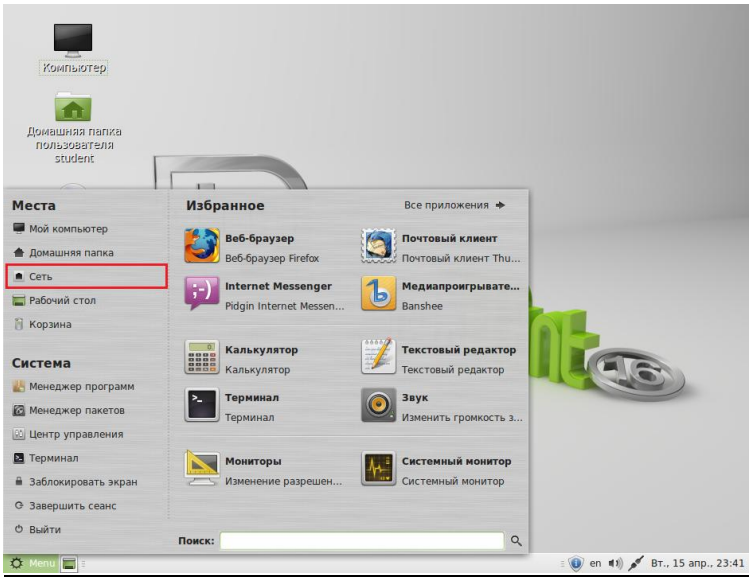
Последняя цифра в поле «Address» зависит от конкретного компьютера.

После задания настроек нажмите кнопку «Save…»

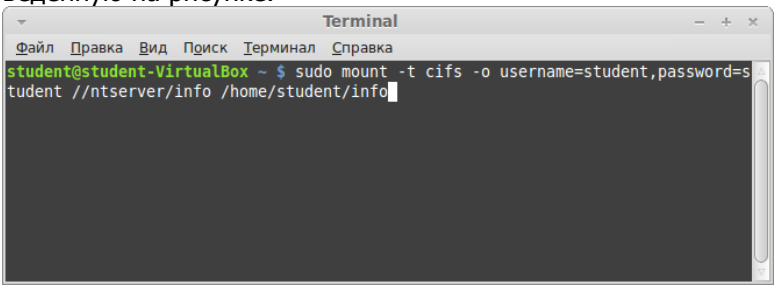
Получение доступа к сетевым ресурсам

После настройки сети появится возможность подключения к другим компьютерам сети и совместного использования ресурсов.

Для этого откройте папку Сеть → Windows Network → ICS → ntserver.

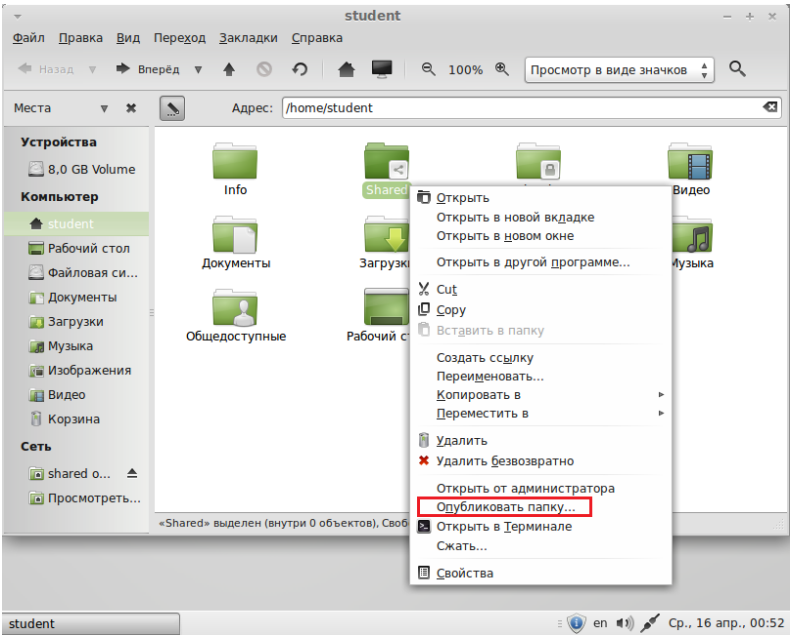


Сетевые ресурсы можно монтировать (т.е. отображать в выбранном месте дерева каталогов) аналогично разделам диска с помощью команды mount. Для этого создайте в домашнем каталоге пользователя папку (например info) и выполните команду, приведённую на рисунке.



Проверьте, отображается ли содержимое сетевого диска в папке /home/student/info.

Предоставьте общий доступ к папке. Для этого создайте в домашнем каталоге пользователя папку (например Shared), нажмите на ней правой кнопкой мыши и выберите пункт контекстного меню «Опубликовать папку». При необходимости введите пароль.



Проверьте возможность доступа к этой папке с другого компьютера или с реальной (не виртуальной) системы.

Контрольные вопросы

1. Что такое монтирование разделов?
2. Какой командой осуществляется монтирование в Linux?
3. Где находится домашняя папка пользователя в Linux?
4. Кто такой суперпользователь?
5. Как выполнить команду от имени суперпользователя?
6. Как настроить параметры сетевого соединения в Linux?
7. Как в Linux получить доступ к общим ресурсам сети Windows?
8. Как в Linux открыть общий доступ к папке?

ЛАБОРАТОРНАЯ РАБОТА № 8

Тема: Интерпретатор команд Linux.

Цель: Изучить основные команды интерпретатора команд Linux и способы их использования для решения практических задач.

Теоретические сведения

Оболочка операционной системы (от англ. shell — оболочка) — интерпретатор команд операционной системы, обеспечивающий интерфейс для взаимодействия пользователя с функциями системы.

Shell — это командная оболочка. Но это не просто промежуточное звено между пользователем и операционной системой, это еще и мощный язык программирования. Программы на языке shell называют сценариями, или скриптами. Фактически, из скриптов доступен полный набор команд, утилит и программ UNIX. Если этого недостаточно, то к вашим услугам внутренние команды shell — условные операторы, операторы циклов и пр., которые увеличивают мощь и гибкость сценариев. Shell-скрипты исключительно хороши при программировании задач администрирования системы и других, которые не требуют для своего создания полновесных языков программирования.

Для того чтобы указать, что команды в файле являются командами интерпретатора bash в начале файла необходимо поместить команду:

#!/bin/bash,

Запустить сценарий можно следующими командами:

sh имя_скрипта

или

bash имя_скрипта

Переменные

Переменные — это одна из основ любого языка программирования. Они участвуют в арифметических операциях, в синтаксическом анализе строк и совершенно необходимы для абстрагирования каких либо величин с помощью символических имен. Физически переменные представляют собой ни что иное как участки памяти, в которые записана некоторая информация.

Необходимо всегда помнить о различиях между именем переменной и ее значением. Если variable1 — это имя переменной,

то $variable1 — это ссылка на ее значение. "Чистые" имена переменных, без префикса $, могут использоваться только при объявлении переменный, при присваивании переменной некоторого значения, при удалении (сбросе), при экспорте и в особых случаях.

Присваивание может производиться с помощью символа = (например: var1=27), инструкцией read и в заголовке цикла (for var2 in 1 2 3).

Проверка условий

Практически любой язык программирования включает в себя условные операторы, предназначенные для проверки условий, чтобы выбрать тот или иной путь развития событий в зависимости от этих условий. В Bash, для проверки условий, имеется команда test, различного вида скобочные операторы и условный оператор if/then.

Конструкции проверки условий

Оператор if/then проверяет — является ли код завершения списка команд 0 (поскольку 0 означает "успех"), и если это так, то выполняет одну, или более, команд, следующие за словом then.

Существует специальная команда— [(левая квадратная скобка). Она является синонимом команды test, и является встроенной командой (т.е. более эффективной, в смысле производительности). Эта команда воспринимает свои аргументы как выражение сравнения или как файловую проверку и возвращает код завершения в соответствии с результатами проверки (0 — истина, 1 — ложь).

Начиная с версии 2.02, Bash предоставляет в распоряжение программиста конструкцию [[...]] расширенный вариант команды test, которая выполняет сравнение способом более знакомым программистам, пишущим на других языках программирования. Обратите внимание: [[— это зарезервированное слово, а не команда.

Циклы и ветвления

Управление ходом исполнения — один из ключевых моментов структурной организации сценариев на языке командной оболочки. Циклы и переходы являются теми инструментальными средствами, которые обеспечивают управление порядком исполнения команд.

Цикл — это блок команд, который исполняется многократно

до тех пор, пока не будет выполнено условие выхода из цикла.

Циклы for

for (in)

Это одна из основных разновидностей циклов. И она значительно отличается от аналога в языке С.

```
for arg in [list]
do
        команда(ы)...
done
```

В [списке] цикла for могут быть использованы имена файлов, которые в свою очередь могут содержать символы-шаблоны.

Оператор цикла for имеет и альтернативный синтаксис записи — очень похожий на синтаксис оператора for в языке С. Для этого используются двойные круглые скобки.

```
LIMIT=10

for ((a=1; a <= LIMIT ; a++))
do
        echo -n "$a "
done
```

while

Оператор while проверяет условие перед началом каждой итерации и если условие истинно (если код возврата равен 0), то управление передается в тело цикла. В отличие от циклов for, циклы while используются в тех случаях, когда количество итераций заранее не известно.

```
while [condition]
do
        command...
done
```

Работа со строками

Длина строки:

${#string}

Извлечение подстроки:

${string:position}

Извлекает подстроку из $string, начиная с позиции $position.

Удаление части строки:

${string#substring}
Удаление самой короткой, из найденных, подстроки $substring в строке $string. Поиск ведется с начала строки.

${string##substring}
Удаление самой длинной, из найденных, подстроки $substring в строке $string. Поиск ведется с начала строки.

${string%substring}
Удаление самой короткой, из найденных, подстроки $substring в строке $string. Поиск ведется с конца строки.

${string%%substring}
Удаление самой длинной, из найденных, подстроки $substring в строке $string. Поиск ведется с конца строки.

Работа с файлами и папками
Список файлов и папок:
ls

Полный список файлов и папок, включая скрытые:
ls –a

Список файлов и папок в текущей папке и всех её подпапках:
ls -r

Сменить директорию:
cd имя-каталога

Примеры использования:
cd / — переход в корневую директорию диска;
cd .. — переход на один уровень выше;
cd ../.. — переход на 2 уровня вверх;
cd $HOME — переход в домашнюю директорию (достаточно набрать просто cd);
cd /home/имя-папки/имя-подпапки — переход в указанную папку.
Создание папки:

mkdir имя-папки

Удаление файла или папки:
rm имя-файла

Удаление файлов и папок рекурсивно (включая все вложенные файлы и папки):
rm -r имя-папки

Скопировать файл:
cp имя-файла имя-копии-файла

Скопировать папку:
cp -r имя-папки имя-копии-папки

Переименовать файл:
mv имя-файла новое-имя-файла

Если «новое-имя-файла» — это папка, то файл будет перемещён в эту папку.

Задание

Используя интерпретатор команд Linux, написать программу, выполняющую действия согласно варианту задания.

Вариант 1.
Удаление всех файлов с расширением, указанным пользователем из папки, в которой находится программа. Вывести сообщение с количеством удалённых файлов.

Вариант 2.
Удаление всех файлов с расширением txt из папки, указанной пользователем. Если папка не указана, то удалить из той, в которой находится программа. Вывести сообщение с количеством удалённых файлов.

Вариант 3.
Копирование всех файлов с расширением doc из папки, в которой находится программа в папку C:\backups\текущая_дата. Вывести на экран список скопированных файлов и их общее количество.

Вариант 4.

Перемещение всех файлов с расширением, указанным пользователем из папки, в которой находится программа, в папку, указанную пользователем.

Вариант 5.

Создание в текущей папке каталогов с именами group1, group2, ..., group10, и в каждой из созданных папок, папок user1, user2, …, user20.

Вариант 6.

Удаление из текущей папки подпапок с именами group2, group4, ..., group10, если папка не существует выдать соответствующее сообщение.

Вариант 7.

Переименование всех файлов с расширением html в файлы с расширением htm, находящихся в одной папке с программой. Вывести на экран список переименованных файлов и их общее количество.

Вариант 8.

Перемещение из папки, в которой находится программа, всех файлов с расширением txt в папку texts, а всех файлов с расширениями bmp и jpg в папку images.

Вариант 9.

Создание десяти папок с именем, введенным пользователем и порядковым номером, т.е. <имя>1, <имя>2, …, <имя>10.

Вариант 10.

Вывод в файл структуры каталогов находящихся в папке, указанной пользователем. Файл должен содержать в названии текущую дату.

Вариант 11.

Вывод в файл <домашняя папка пользователя>/backups/sh.txt информации о количестве файлов с расширением sh в папке, указанной пользователем.

Контрольные вопросы

1. Что такое интерпретатор команд?
2. Что такое пакетный файл?
3. Основные команды работы с файлами и папками.
4. Основные команды для управления выполнением скрипта.
5. Как запустить программу, написанную для интерпретатора команд Linux?

ЛАБОРАТОРНАЯ РАБОТА № 9

Тема: Управление пользователями и правами доступа в Linux.

Цель: Изучить способы создания, удаления, управления правами пользователей в Linux, способы назначения прав доступа к файлам.

Теоретические сведения

Для создания пользователей самый простой способ — использовать утилиту adduser которая в интерактивном режиме запросит все необходимые параметры. Её синтаксис:

adduser <имя_пользователя>

Когда пользователь уже создан, вы можете изменять его настройки с помощью команды usermod.

Возможные ключи:
-d домашняя директория
-s shell
-p пароль
-g первичная группа
-G другие группы, к которым принадлежит пользователь

Удаление пользователей из системы может быть произведено командой userdel или deluser.

Для изменения режима доступа к файлам служит команда chmod. Её синтаксис:

chmod режим файл

Права доступа к указанным файлам (среди которых могут быть каталоги) изменяются в соответствии с указанным режимом. Режим может быть задан в абсолютном или символьном виде.

Абсолютный вид — восьмеричное число, являющееся поразрядным ИЛИ следующих режимов:
00400 Доступен для чтения владельцем.
00200 Доступен для записи владельцем.
00100 Доступен для выполнения владельцем.
00040 Доступен для чтения членами группы.

00020 Доступен для записи членами группы.

00010 Доступен для выполнения (просмотра) членами группы.

00004 Доступен для чтения прочими пользователями.

00002 Доступен для записи прочими пользователями.

00001 Доступен для выполнения (просмотра) прочими пользователями.

Использование символьного вида основано на однобуквенных обозначениях, которые определяют класс доступа и права доступа для членов данного класса. Права доступа к файлу зависят от идентификатора пользователя и идентификатора группы, в которую он входит. Режим в целом описывается в терминах трех последовательностей, по три буквы в каждой:

Владелец	Группа	Прочие
u	g	o
rwx	rwx	rwx

Здесь владелец, члены группы и все прочие пользователи обладают правами чтения файла, записи в него и его выполнения. В примере показаны обозначения как для класса доступа, так и для прав доступа внутри класса.

Для задания режима доступа в символьном виде используется следующий синтаксис:

chmod [кому] операция права

Часть кому есть комбинация букв u, g и o (владелец, члены группы и прочие пользователи соответственно). Если часть кому опущена или указано a, то это эквивалентно ugo.

Операция может быть: + (добавить право), - (лишить права), = (в пределах данного класса присвоить права абсолютно, то есть добавить указанные права и отнять неуказанные).

Права — комбинация следующих букв:

r Право на чтение.

w Право на запись.

x Право на выполнение.

Если надо сделать более одного указания об изменении прав, то при использовании символьного вида в правах не должно быть пробелов, а указания должны разделяться запятыми. На-

пример, команда

chmod u+w,go+x f1

добавит для владельца право писать в файл f1, а для членов группы и прочих пользователей - право выполнять файл. Права устанавливаются в указанном порядке. Право s можно добавлять только для пользователя и группы, право t — только для пользователя.

Для просмотра прав доступа и контроля при их изменении используется команда ls с ключом -l.

Примеры

1. Чтобы установить права, позволяющие владельцу читать и писать в файл, а членам группы и прочим пользователям только читать, надо сложить 0400, 0200, 0040 и 0004. Таким образом, команду можно записать двумя способами:

chmod 644 f1

chmod u=rw,go=r f1

2. Позволить всем выполнять файл f2:

chmod +x f2

Задание

1. Создайте пользователя user1.
2. Войдите от имени созданного пользователя, используя виртуальный терминал. Для переключения между виртуальными терминалами используются комбинации <Ctrl>+<Alt>+<F1> — <Ctrl>+<Alt>+<F7>.
3. Вернитесь к графическому терминалу (ему соответствует комбинация <Ctrl>+<Alt>+<F7>) и создайте пакетный файл в домашней директории пользователя student или воспользуйтесь созданным на лабораторной работе № 6.
4. Проверьте текущие права доступа к этому файлу.
5. Попытайтесь запустить указанный файл от имени пользователя user1.
6. От имени пользователя student назначьте права доступа к

файлу, запрещающие доступ на чтение для остальных (other) пользователей.

7. Попытайтесь запустить указанный файл от имени пользователя user1. Объясните полученный результат.

8. Измените пользователя user1, переместив его в ту же группу, к которой принадлежит student (по умолчанию эта группа также называется student).

9. Завершите сеанс пользователя user1 (команда logout) и снова войдите в систему от его имени.

10.Попытайтесь снова запустить пакетный файл, созданный в пункте 3. Объясните полученный результат.

11.Удалите пользователя user1.

Запишите абсолютный и символьный варианты команды, устанавливающей права доступа к файлу в соответствии с вариантом задания.

Вариант 1.
Доступ всем пользователям только на чтение

Вариант 2.
Доступ всем пользователям на чтение и запись

Вариант 3.
Полный доступ текущему пользователю, доступ остальных только на чтение

Вариант 4.
Доступ для пользователя и группы на чтение и запуск, доступ остальным только на чтение

Вариант 5.
Доступ всем пользователям на чтение и выполнение

Вариант 6.
Полный доступ для пользователя и группы, отсутствие доступа для остальных пользователей

Вариант 7.
Полный доступ для пользователя и группы, доступ на чтение и выполнение для остальных

Вариант 8.

Доступ пользователя на чтение и запись, доступ группы на чтение и выполнение, доступ только на чтение для остальных

Вариант 9.

Доступ пользователя на чтение и запись, доступ группы и остальных пользователей только на чтение

Вариант 10.

Доступ пользователя и группы на чтение и запись, доступ остальных только на чтение

Вариант 11.

Полный доступ для пользователя, доступ на чтение и выполнение для группы, доступ на чтение и запись для остальных

Контрольные вопросы

1. Какой командой осуществляется создание нового пользователя в Linux?
2. Какой командой осуществляется удаление пользователя в Linux?
3. Какой командой осуществляется изменение пользователя в Linux?
4. Какая команда предназначена для изменения прав доступа к файлу?
5. Какие права могут быть назначены файлу?
6. По отношению к кому применяются права доступа к файлу?