

09-641. Десятов Александр

Отчет. Практическое занятие №1. Установка, настройка и Организация комплекса средств защиты ОС на базе GNU/Linux

Упражнение 1. Установка операционной системы

Создать виртуальную машину

Укажите имя и тип ОС

Пожалуйста укажите имя и местоположение новой виртуальной машины и выберите тип операционной системы, которую Вы собираетесь установить на данную машину. Заданное Вами имя будет использоваться для идентификации данной машины.

Имя: DesAlex_Linux_Red_Hat_64

Папка машины: D:\Program Files D\VirtualBox

Тип: Linux

Версия: Red Hat (64-bit)

Экспертный режим **Далее** Отмена



Создать виртуальную машину



Укажите объём памяти

Укажите объём оперативной памяти (RAM) выделенный данной виртуальной машине.

Рекомендуемый объём равен **1024** МБ.



Далее

Отмена



Создать виртуальную машину



Жесткий диск

При желании к новой виртуальной машине можно подключить виртуальный жёсткий диск. Вы можете создать новый или выбрать из уже имеющихся.

Если Вам необходима более сложная конфигурация Вы можете пропустить этот шаг и внести изменения в настройки машины после её создания.

Рекомендуемый объём нового виртуального жёсткого диска равен **8,00 ГБ**.

- ☐ Не подключать виртуальный жёсткий диск
- ☒ Создать новый виртуальный жёсткий диск
- ☐ Использовать существующий виртуальный жёсткий диск

Пусто



Создать

Отмена



Создать виртуальный жёсткий диск



Укажите тип

Пожалуйста, укажите тип файла, определяющий формат, который Вы хотите использовать при создании нового жёсткого диска. Если у Вас нет необходимости использовать диск с другими продуктами программной виртуализации, Вы можете оставить данный параметр без изменений.

- ☒ VDI (VirtualBox Disk Image)
- ☐ VHD (Virtual Hard Disk)
- ☐ VMDK (Virtual Machine Disk)

Экспертный режим

Далее

Отмена



Создать виртуальный жёсткий диск

Укажите формат хранения

Пожалуйста уточните, должен ли новый виртуальный жёсткий диск подстраивать свой размер под размер своего содержимого или быть точно заданного размера.

Файл **динамического** жёсткого диска будет занимать необходимое место на Вашем физическом носителе информации лишь по мере заполнения, однако не сможет уменьшиться в размере если место, занятое его содержимым, освободится.

Файл **фиксированного** жёсткого диска может потребовать больше времени при создании на некоторых файловых системах, однако, обычно, быстрее в использовании.

- ☒ Динамический виртуальный жёсткий диск
- ☐ Фиксированный виртуальный жёсткий диск

Далее

Отмена



Создать виртуальный жёсткий диск



Укажите имя и размер файла

Пожалуйста укажите имя нового виртуального жёсткого диска в поле снизу или используйте кнопку с иконкой папки справа от него.

D:\Program Files D\VirtualBox\DA_Linux_Red_Hat_64\DA_Linux_Red_Hat_64.vdi



Укажите размер виртуального жёсткого диска в мегабайтах. Эта величина ограничивает размер файловых данных, которые виртуальная машина сможет хранить на этом диске.



Создать

Отмена

У Вас включена настройка **Автозахват клавиатуры**. Это приведет к тому, что виртуальная машина будет



← Выберите загрузочный диск

Пожалуйста выберите виртуальный оптический диск или физический привод оптических дисков, содержащий диск для запуска Вашей новой виртуальной машины.

Диск должен быть загрузочным и содержать дистрибутив операционной системы, которую Вы хотите установить. Диск будет автоматически извлечён при выключении виртуальной машины, однако, в случае необходимости, Вы можете сделать это и сами используя меню Устройства.

rhel-server-6.3-i386-dvd.iso (2,89 ГБ)



Продолжить

Отмена

У Вас включена настройка **Автозахват клавиатуры**. Это приведет к тому, что виртуальная машина будет

```
Install or upgrade an existing system
Install system with basic video driver
Rescue installed system
Boot from local drive
Memory test
```

Press [Tab] to edit options

**RED HAT®
ENTERPRISE LINUX® 6**



Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

Welcome to Red Hat Enterprise Linux for i386

Disc Found

To begin testing the media before
installation press OK.

Choose Skip to skip the media test
and start the installation.

OK

Skip

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

Welcome to Red Hat Enterprise Linux for i386

Unsupported Hardware Detected

This hardware (or a combination thereof) is not supported by Red Hat. For more information on supported hardware, please refer to <http://www.redhat.com/hardware>.

OK

<Tab>/<Alt-Tab> between elements | <Space> selects | <F12> next screen

RED HAT® ENTERPRISE LINUX® 6



Copyright © 2003-2010 Red Hat, Inc. and others. All rights reserved.

Northern Sotho (Northern Sotho)
Norwegian(Bokmål) (Norwegian(Bokmål))
Oriya (ଓଡ଼ିଆ)
Persian (فارسی)
Polish (polski)
Portuguese (Português)
Portuguese(Brazilian) (Português (Brasil))
Punjabi (ਪੰਜਾਬੀ)
Romanian (Română)
Russian (Русский)
Serbian (српски)
Serbian(Latin) (srpski(latinica))
Sinhala (සිංහල)
Slovak (Slovenčina)
Slovenian (slovenščina)
Spanish (Español)
Swedish (Svenska)
Tajik (Tajik)
Tamil (தமிழ்)
Telugu (తెలుగు)
Turkish (Türkçe)
Ukrainian (Українська)
Vietnamese (tiếng Việt)
Welsh (Cymraeg)
Zulu (Zulu)

Back

Next

Какой тип устройств будет использоваться при установке?

Стандартные накопители

- ☒ Установка или обновление на стандартных накопителях. Этот выбор подходит, если вы не уверены, какой вариант следует выбрать.

Специальные накопители

- ☐ Позволяет установить и обновить устройства SAN (Storage Area Network), добавить диски FCoE, iSCSI, zFCP и задать устройства, которые установщик должен будет пропустить.

**Устройство может содержать данные.****ATA VBOX HARDDISK**

8192.0 MB pci-0000:00:0d.0-scsi-0:0:0:0

На устройстве не обнаружены разделы и файловые системы.

Возможно, это устройство **пустое, неразмеченное** или **виртуальное**.

Если это не так, при продолжении установки данные, находящиеся на этом устройстве, могут быть утрачены. Для предотвращения потери данных это устройство можно исключить из установки.

Вы уверены, что это устройство не содержит важные данные?

☒ Применить мой выбор ко всем устройствам с нераспознанными разделами и файловыми системами

Да, удалить данные

Нет, сохранить данные

Назад

Далее



Присвойте этому компьютеру имя, которое будет использоваться для его идентификации в сети.

Имя узла:

Укажите ближайший город в вашем часовом поясе:



Выбранный город: Москва, Европа (Москва+00 - Западная часть России)

Европа/Москва








Учётная запись root используется для
администрирования системы.
Введите пароль пользователя root.

Пароль root:

Подтвердите:

Какой тип установки вы предпочитаете?

- ☐  **Всё пространство**
Удаляет все разделы на выбранных устройствах, в том числе и разделы, созданные другими операционными системами.
Совет: Этот выбор приведёт к удалению данных на выбранных устройствах. Убедитесь, что у вас есть резервные копии.
- ☒  **Заменить существующую систему Linux**
Удаляет только разделы Linux, созданные в ходе предыдущей установки Linux. При этом другие разделы (например, VFAT или FAT32) не будут удалены.
Совет: Этот выбор приведёт к удалению данных на выбранных устройствах. Убедитесь, что у вас есть резервные копии.
- ☐  **Уменьшить существующую систему**
Сокращает существующие разделы с целью освобождения места для стандартного разбиения.
- ☐  **Использовать свободное пространство**
Сохраняет текущие данные и разделы и использует только нераспределённое пространство на выбранных устройствах, предполагая, что этого будет достаточно.
- ☒  **Создать собственное разбиение**
Позволяет создать собственное разбиение на выбранных устройствах с помощью специальной утилиты создания разделов.

☐ Зашифровать систему

Выберите устройство

Устройство	Размер (МБ)	Точка монт./ RAID/Том	Тип	Формат
▼ Жесткие диски				
▼ sda (/dev/sda)				
sda1	4096		swap	✓
sda2	4095 /		ext4	✓

☒ Установить загрузчик в /dev/sda. [Изменить устройство](#)

☐ Использовать пароль загрузчика [Изменить пароль](#)

Список операционных систем загрузчика

По умолчанию	Метка	Устройство
<input checked="" type="radio"/>	Red Hat Enterprise Linux	/dev/sda2

[Добавить](#)

[Изменить](#)

[Удалить](#)

Стандартная установка сервера (Red Hat Enterprise Linux). По желанию можно выбрать другой комплект программ.

- ☐ Стандартный сервер
- ☐ Сервер базы данных
- ☐ Веб-сервер
- ☐ Сервер управления идентификацией
- ☐ Хост виртуализации
- ☒ Рабочий стол
- ☐ Рабочая станция разработки программ
- ☐ Минимальный

Выберите дополнительные репозитории для установки ПО.

- ☒ Red Hat Enterprise Linux
- ☐ Высокий уровень доступности
- ☐ Надёжное хранилище
- ☐ Разработчики

+ Добавить дополнительные репозитории

Изменить репозиторий

Можно изменить набор пакетов сейчас или после завершения установки с помощью специальной программы управления пакетами.



Поздравляем, установка Red Hat Enterprise Linux завершена.

Перезагрузите систему, чтобы начать ее использовать. Обратите внимание, что уже могут быть доступны обновления, которые нужны для корректной работы вашей системы. Рекомендуется установить эти обновления после перезагрузки.

[← Назад](#)[→ Перезагрузка](#)



- Добро пожаловать
- Информация о лицензии
- Настроить обновления
- Пользователь
- Дата и время
- Kdump

Добро пожаловать

Осталось ещё несколько шагов, после чего ваша система будет готова к работе. В этом вам поможет помощник по настройке. Нажмите кнопку продолжения.

[Назад](#)[Вперёд](#)



Добро
пожаловать

Информация о
лицензии

Настроить
обновления

Пользователь

Дата и время

Kdump

Информация о лицензии

END USER LICENSE AGREEMENT RED HAT® ENTERPRISE LINUX® AND RED HAT APPLICATIONS

PLEASE READ THIS END USER LICENSE AGREEMENT CAREFULLY BEFORE USING SOFTWARE FROM RED HAT. BY USING RED HAT SOFTWARE, YOU SIGNIFY YOUR ASSENT TO AND ACCEPTANCE OF THIS END USER LICENSE AGREEMENT AND ACKNOWLEDGE YOU HAVE READ AND UNDERSTAND THE TERMS. AN INDIVIDUAL ACTING ON BEHALF OF AN ENTITY REPRESENTS THAT HE OR SHE HAS THE AUTHORITY TO ENTER INTO THIS END USER LICENSE AGREEMENT ON BEHALF OF THAT ENTITY. IF YOU DO NOT ACCEPT THE TERMS OF THIS AGREEMENT, THEN YOU MUST NOT USE THE RED HAT SOFTWARE. THIS END USER LICENSE AGREEMENT DOES NOT PROVIDE ANY RIGHTS TO RED HAT SERVICES SUCH AS SOFTWARE MAINTENANCE, UPGRADES OR SUPPORT. PLEASE REVIEW YOUR SERVICE OR SUBSCRIPTION AGREEMENT(S) THAT YOU MAY HAVE WITH RED HAT OR OTHER AUTHORIZED RED HAT SERVICE PROVIDERS REGARDING SERVICES AND ASSOCIATED PAYMENTS.

This end user license agreement ("EULA") governs the use of any of the versions of Red Hat Enterprise Linux, certain other Red Hat software applications that include or refer to this license, and any related updates, source code, appearance, structure and organization (the "Programs"), regardless of the delivery mechanism.

1. License Grant. Subject to the following terms, Red Hat, Inc. ("Red Hat") grants to you a perpetual, worldwide license to the Programs (most of which include multiple software components) pursuant to the GNU General Public License v.2. The license agreement for each software component is located in the software component's source code and permits you to run, copy, modify, and redistribute the software component (subject to certain obligations in some cases), both in

☒ Да, я принимаю условия соглашения

☐ Нет, я не согласен

Назад

Вперед



Добро
пожаловать
Информация о
лицензии
› Настроить
обновления
Пользователь
Дата и время
Kdump

Настроить обновления



В системе нет активного сетевого соединения. Она не может быть настроена на получение обновлений.

Без подключения к серверу Red Hat Network вы **не** сможете получать программные обновления, в том числе обновления безопасности Red Hat.

Для поддержания системы в обновлённом и защищённом состоянии, зарегистрируйте её как можно раньше.

Для запуска программы регистрации в меню **Система > Администрирование** выберите **Регистрация в RHN**, а для запуска программы обновления - **Обновление программ**.

Зачем подключаться к RHN?

Назад

Вперёд

Добро
пожаловать
Информация о
лицензии
Настроить
обновления
➤ Пользователь
Дата и время
Kdump

Пользователь

Требуется создать пользователя для повседневного (не административного) использования системы. Для этого введите необходимые данные.

Конфигурация аутентификации

Идентификация и аутентификация

Дополнительные параметры

Настройка учётной записи пользователя

База данных учётных записей пользователей: Только локальные учётные записи

Настройка аутентификации

Способ аутентификации: Пароль

Восстановить

Отменить

Применить

[Назад](#)[Вперед](#)



Добро
пожаловать
Информация о
лицензии
Настроить
обновления

➤ Пользователь
Дата и время
Kdump

Пользователь

Требуется создать пользователя для повседневного (не административного) использования системы. Для этого введите необходимые данные.

Имя пользователя:

Полное имя:

Пароль:

Подтвердите пароль:

Если требуется использовать проверку подлинности по сети, например Kerberos или NIS, нажмите кнопку «Сетевая аутентификация».

Для настройки других параметров (домашнего каталога, UID) нажмите кнопку «Дополнительно».

Добро
пожаловать
Информация о
лицензии
Настроить
обновления
Пользователь
› Дата и время
Kdump

Дата и время

Пожалуйста, установите дату и время системы.

Дата и время

Текущие дата и время: Пнд 30 Сен 2019 18:25:44

☒ Синхронизация даты и времени по сети

Синхронизация даты и времени с удалённым сервером времени с использованием NTP

Серверы NTP

0.rhel.pool.ntp.org

Добавить

Изменить

Удалить

Дополнительные параметры

☐ Ускорить синхронизацию

☐ Использовать локальный источник времени

Используйте режим iburst, тогда исходная синхронизация займёт меньше времени, но возрастёт нагрузка на серверы.

Назад

Вперёд

Добро
пожаловать
Информация о
лицензии
Настроить
обновления
Пользователь
Дата и время
› Kdump

Kdump

Kdump предоставляет новый механизм сбора статистики о сбоях ядра. В случае системного сбоя kdump собирает необходимую информацию для последующего определения причины сбоя. Нужно иметь в виду, что kdump требует резервирования части системной памяти, что делает её недоступной для использования.

☒ Включить Kdump?

Общий размер системной памяти (МБ): 2022

Память Kdump (МБ): 128

Используемая системная память (МБ): 1894

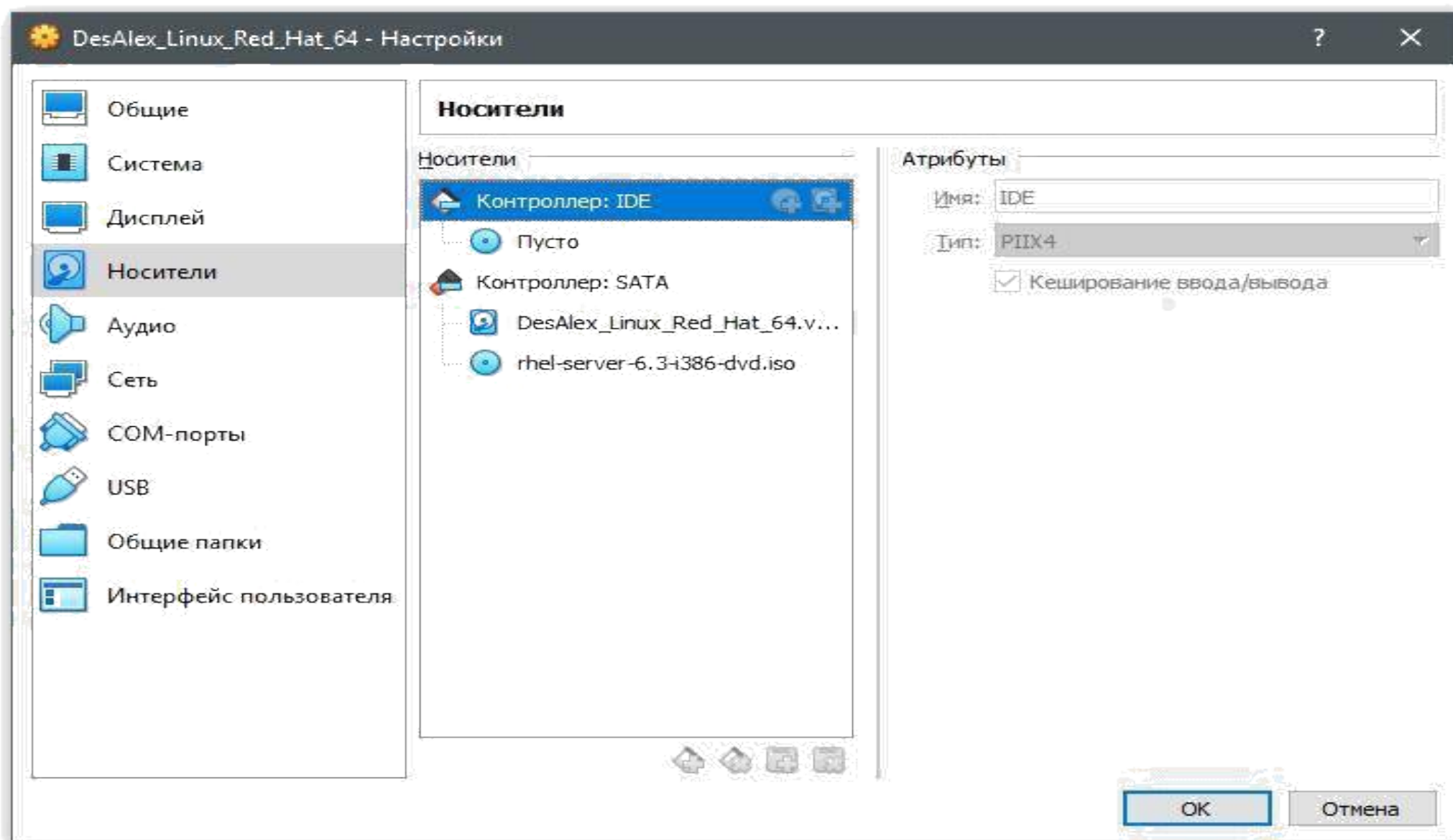
Advanced kdump configuration

```
# Configures where to put the kdump /proc/vmcore files
#
# This file contains a series of commands to perform (in order) when a
# kernel crash has happened and the kdump kernel has been loaded. Di
# this file are only applicable to the kdump initramfs, and have no effect
# the root filesystem is mounted and the normal init scripts are proces
#
# Currently only one dump target and path may be configured at once
# if the configured dump target fails, the default action will be preforme
# the default action may be configured with the default directive below
# configured dump target succeeds
#
# Basics commands supported are:
# path <path> - Append path to the filesystem device which y
# dumping to. Ignored for raw device dumps.
# If unset, will default to /var/crash.
```

Назад

Готово

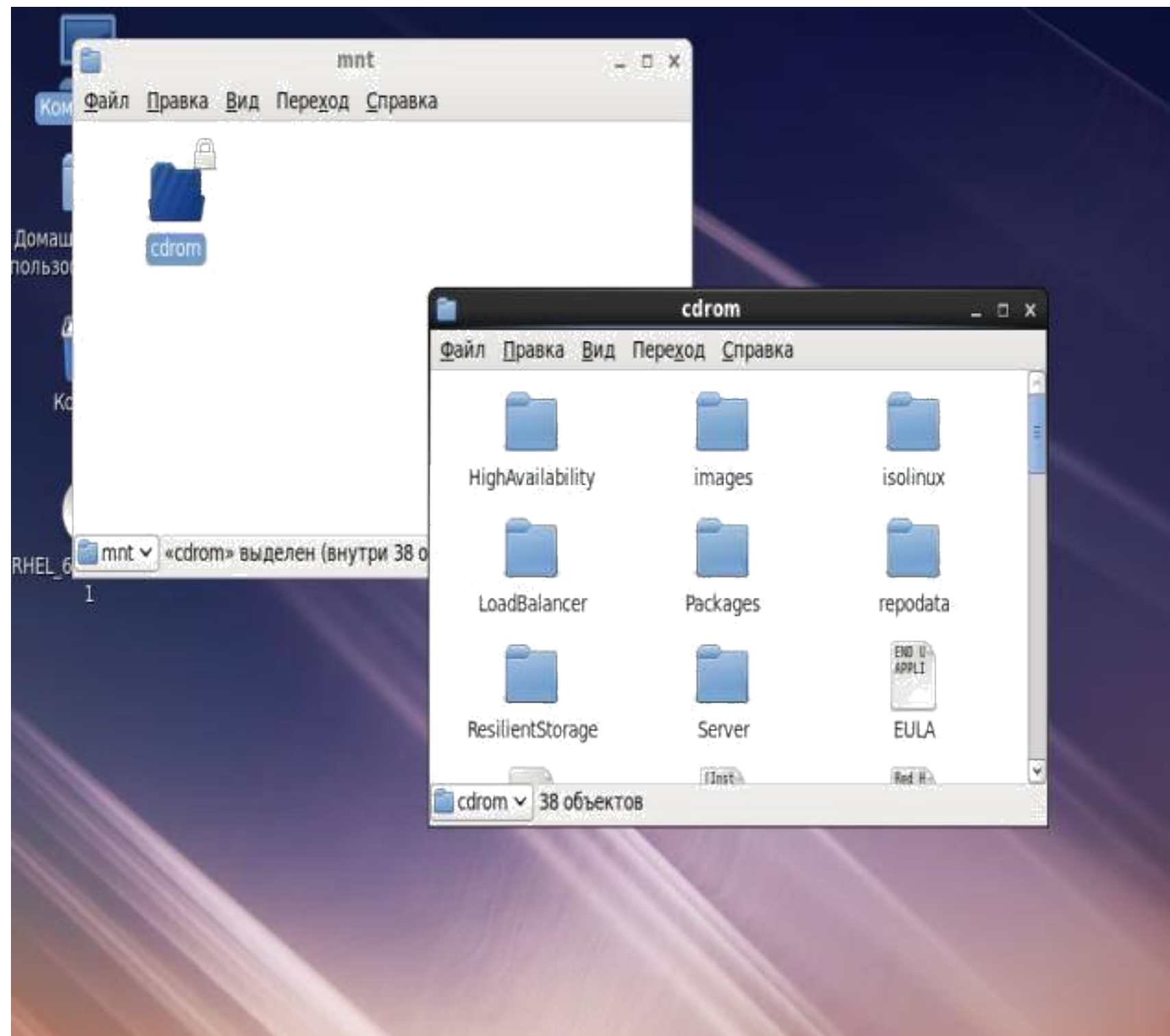
Упражнение 2. Доустановка программных пакетов в систему.



```
[root@localhost cdrom]# mount -t iso9660 /dev/sr1 /mnt/cdrom
```

```
mount: блочное устройство /dev/sr1 защищен от записи, монтируется только для чтения
```

```
[root@localhost cdrom]# █
```




```
[root@localhost cdrom]# cd Packages
```

```
[root@localhost Packages]# rpm --install
```

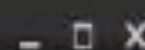
```
Display all 2843 possibilities? (y or n)
```

```
[root@localhost Packages]# rpm --install mc-4.7.0.2-3.el6.i686.rpm
```

```
предупреждение: mc-4.7.0.2-3.el6.i686.rpm: Заголовок V3 RSA/SHA256 Signature, ke  
y ID fd431d51: NOKEY
```



mc [root@localhost.localdomain]:/mnt/cdrom/Packages



Файл Правка Вид Поиск Терминал Справка

Левая панель				Файл	Команда	Настройки	Правая панель			
< /mnt/cdrom/Packages							< /mnt/cdrom/Packages			
[^]>							[^]>			
'и	Имя	Размер	Время правки				'и	Имя	Размер	Время правки
/..				-ВВЕРХ-	Июн 14	2012	/..			
389-ds-b-686.rpm				1434624	Май 30	2012	389-ds-b-686.rpm			
389-ds-b-686.rpm				386996	Май 30	2012	389-ds-b-686.rpm			
ConsoleK-686.rpm				82300	Авг 17	2010	ConsoleK-686.rpm			
ConsoleK-686.rpm				17312	Авг 17	2010	ConsoleK-686.rpm			
ConsoleK-686.rpm				20620	Авг 17	2010	ConsoleK-686.rpm			
DeviceKi-686.rpm				92824	Сен 6	2011	DeviceKi-686.rpm			
Electric-686.rpm				32348	Авг 17	2010	Electric-686.rpm			
GConf2-2-686.rpm				984340	Авг 17	2010	GConf2-2-686.rpm			
GConf2-d-686.rpm				93496	Авг 17	2010	GConf2-d-686.rpm			
GConf2-g-686.rpm				23000	Авг 17	2010	GConf2-g-686.rpm			
ImageMag-686.rpm				1751404	Апр 19	2012	ImageMag-686.rpm			
ImageMag-686.rpm				145692	Апр 19	2012	ImageMag-686.rpm			
MAKEDEV--686.rpm				90952	Авг 17	2010	MAKEDEV--686.rpm			
ModemMan-686.rpm				179236	Авг 17	2010	ModemMan-686.rpm			
-ВВЕРХ-							-ВВЕРХ-			
0/2956M (0%)							0/2956M (0%)			

Совет: Вы хотите навигацию в стиле lypx? Установите это в диалоге Конфигурация.

[root@localhost Packages]#

1 Помощь 2 Меню 3 Про-тр 4 Правка 5 Копия 6 Тер-од 7 НЭК-ог 8 Уда-ть 9 МенюМС 10 Выход

```
| [root@localhost ~]# umount -l /dev/sr1
```

Упражнение 3. Управление учетными записями пользователей и создание групп

```
root@localhost:/  
Файл Правка Вид Поиск Терминал Справка  
[root@localhost /]# adduser user1  
adduser: внимание: домашний каталог уже существует.  
Никакие файлы из каталога skel копироваться не будут.  
Создание почтового ящика: Файл существует  
[root@localhost /]# id user1  
uid=1013(user1) gid=1014(user1) группы=1014(user1)  
[root@localhost /]# usermod -u 1010 user1  
[root@localhost /]# id user1  
uid=1010(user1) gid=1014(user1) группы=1014(user1)  
[root@localhost /]#
```

```
[root@localhost Рабочий стол]# adduser user2
[root@localhost Рабочий стол]# adduser user3
[root@localhost Рабочий стол]# groupadd group1
[root@localhost Рабочий стол]# usermod -a -G group1 user2
[root@localhost Рабочий стол]# usermod -a -G group1 user3
[root@localhost Рабочий стол]# id user2
uid=1011(user2) gid=1011(user2) группы=1011(user2),1013(group1)
[root@localhost Рабочий стол]# █
```


2.12. Требования к классу защищенности 1Г:

Подсистема управления доступом:

должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по идентификатору (коду) и паролю условно-постоянного действия, длиной не менее шести буквенно-цифровых символов;

- должна осуществляться идентификация терминалов, ЭВМ, узлов сети ЭВМ, каналов связи, внешних устройств ЭВМ по логическим именам;
- должна осуществляться идентификация программ, томов, каталогов, файлов, записей, полей записей по именам;
- должен осуществляться контроль доступа субъектов к защищаемым ресурсам в соответствии с матрицей доступа.

system-auth-ac (/etc/pam.d) - gedit

Файл Правка Вид Поиск Сервис Документы Справка

Открыть Сохранить Отменить

system-auth-ac

```
#%PAM-1.0
# This file is auto-generated.
# User changes will be destroyed the next time authconfig is run.
auth      required      pam_env.so
auth      sufficient     pam_unix.so nullok try_first_pass
auth      requisite      pam_succeed_if.so uid >= 500 quiet
auth      required      pam_deny.so

account    required      pam_unix.so
account    sufficient     pam_localuser.so
account    sufficient     pam_succeed_if.so uid < 500 quiet
account    required      pam_permit.so

password   requisite      pam_cracklib.so try_first_pass retry=3 minlen=6 ucredit=-1 lcredit=-1 dcredit=-1
password   sufficient     pam_unix.so sha512 shadow nullok try_first_pass use_authtok
password   required      pam_deny.so

session    optional      pam_keyinit.so revoke
session    required      pam_limits.so
session    [success=1 default=ignore] pam_succeed_if.so service in crond quiet use_uid
session    required      pam_unix.so
```

Текст Ширина табуляции: 8 Стр 14, Стлб 107 ВСТ

Компьютер [/] etc pam.d system-auth-ac (/et...

login.defs (/etc) - gedit

Файл Правка Вид Поиск Сервис Документы Справка

Открыть Сохранить Отменить

login.defs X

```
#
# Please note that the parameters in this configuration file control the
# behavior of the tools from the shadow-utils component. None of these
# tools uses the PAM mechanism, and the utilities that use PAM (such as the
# passwd command) should therefore be configured elsewhere. Refer to
# /etc/pam.d/system-auth for more information.
#

# *REQUIRED*
# Directory where mailboxes reside, or name of file, relative to the
# home directory. If you do define both, MAIL_DIR takes precedence.
# QMAIL_DIR is for Qmail
#
#QMAIL_DIR      Maildir
MAIL_DIR        /var/spool/mail
#MAIL_FILE      .mail

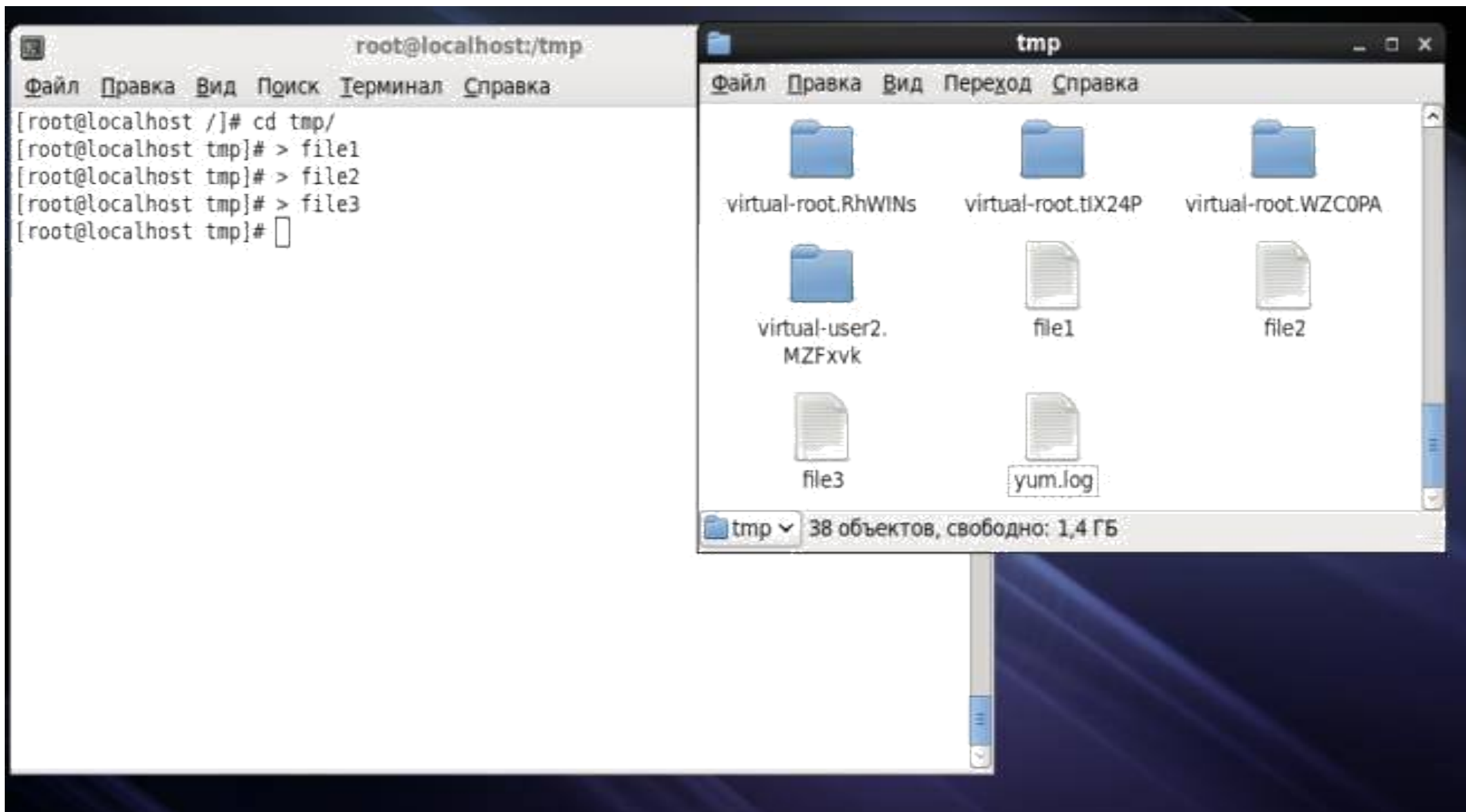
# Password aging controls:
#
#      PASS_MAX_DAYS   Maximum number of days a password may be used.
#      PASS_MIN_DAYS   Minimum number of days allowed between password changes.
#      PASS_MIN_LEN     Minimum acceptable password length.
#      PASS_WARN_AGE   Number of days warning given before a password expires.
#
PASS_MAX_DAYS   100
PASS_MIN_DAYS    0
PASS_MIN_LEN     6
PASS_WARN_AGE    7

#
# Min/max values for automatic uid selection in useradd
#
UID_MIN          500
UID_MAX          60000
```

Текст Ширина табуляции: 8 Стр 25, Стлб 20 ВСТ

Компьютер / etc login.defs (/etc) - gedit

Упражнение 5. Установка прав разграничения доступа к файлам

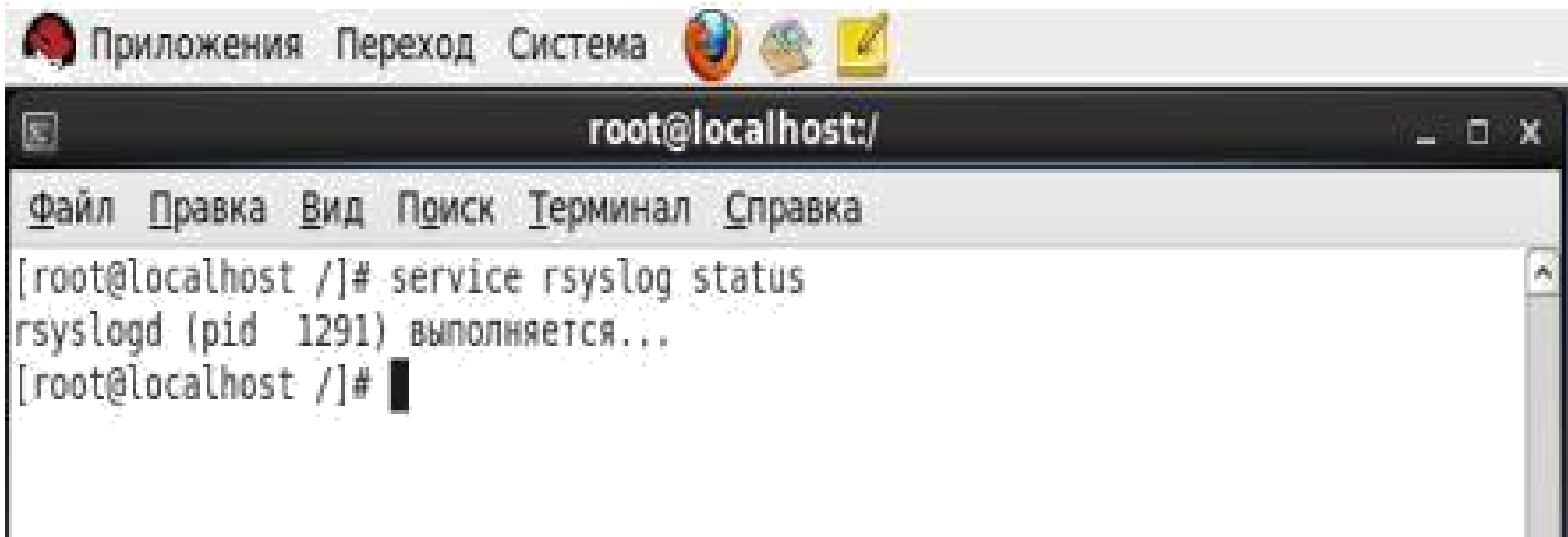


```
[root@localhost tmp]# groupadd gr_1_2  
[root@localhost tmp]# groupadd gr_1_3  
[root@localhost tmp]# groupadd gr_2_3
```

```
[root@localhost tmp]# usermod -a -G gr_1_2 user1
[root@localhost tmp]# usermod -a -G gr_1_2 user2
[root@localhost tmp]# usermod -a -G gr_1_3 user1
[root@localhost tmp]# usermod -a -G gr_1_3 user3
[root@localhost tmp]# usermod -a -G gr_2_3 user2
[root@localhost tmp]# usermod -a -G gr_2_3 user3
[root@localhost tmp]# chown user1:gr_2_3 file1
[root@localhost tmp]# chown user2:gr_1_3 file2
[root@localhost tmp]# chown user3:gr_1_2 file3
[root@localhost tmp]# ls -l file1 file2 file3
-rw-r--r--. 1 user1 gr_2_3 0 Hoa 25 00:07 file1
-rw-r--r--. 1 user2 gr_1_3 0 Hoa 25 00:07 file2
-rw-r--r--. 1 user3 gr_1_2 0 Hoa 25 00:07 file3
```

```
[root@localhost tmp]# chmod g+r-wx,o=--- file1
[root@localhost tmp]# chmod u=---,g=-r+w-x,o=--- file2
[root@localhost tmp]# chmod g=rwx,o=--- file3
[root@localhost tmp]# ls -l file1 file2 file3
-rw-r-----. 1 user1 gr_2_3 0 Nov 25 00:07 file1
-----W----. 1 user2 gr_1_3 0 Nov 25 00:07 file2
-rw-rwx---. 1 user3 gr_1_2 0 Nov 25 00:07 file3
[root@localhost tmp]#
```

Упражнение 6. Настройка подсистемы регистрации и учёта событий



The screenshot shows a Linux desktop environment. At the top, there is a taskbar with icons for applications, a window switcher, and system status. Below the taskbar, a terminal window is open. The terminal window has a title bar that reads "root@localhost:/" and standard window control buttons. Inside the terminal, a menu bar is visible with options: "Файл", "Правка", "Вид", "Поиск", "Терминал", and "Справка". The terminal content shows the command "service rsyslog status" being executed, with the output "rsyslogd (pid 1291) выполняется...". The prompt "[root@localhost /]#" is visible at the end of the line.

```
root@localhost:/  
Файл Правка Вид Поиск Терминал Справка  
[root@localhost /]# service rsyslog status  
rsyslogd (pid 1291) выполняется...  
[root@localhost /]#
```

rsyslog.conf (/etc) - gedit

Файл Правка Вид Поиск Сервис Документы Справка

Открыть Сохранить Отменить

rsyslog.conf

```
# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.* /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none /var/log/messages

# The authpriv file has restricted access.
authpriv.* /var/log/secure

# Log all the mail messages in one place.
mail.* -/var/log/maillog

# Log cron stuff
cron.* /var/log/cron

# Everybody gets emergency messages
*.emerg *

# Save news errors of level crit and higher in a special file.
uucp,news.crit /var/log/spooler

# Save boot messages also to boot.log
local7.* /var/log/boot.log
```

Текст Ширина табуляции: 8 Стр 42, Стлб 65 ВСТ

Компьютер / etc rsyslog.conf (/etc) - gedit

*rsyslog.conf (/etc) - gedit

Файл Правка Вид Поиск Сервис Документы Справка

Открыть Сохранить Отменить

*rsyslog.conf

```
# Include all config files in /etc/rsyslog.d/
$IncludeConfig /etc/rsyslog.d/*.conf

#### RULES ####

# Log all kernel messages to the console.
# Logging much else clutters up the screen.
#kern.*                                /dev/console

# Log anything (except mail) of level info or higher.
# Don't log private authentication messages!
*.info;mail.none;authpriv.none;cron.none    /tmp/messages

# The authpriv file has restricted access.
authpriv.*    /var/log/security

# Log all the mail messages in one place.
mail.*        -/var/log/maillog

# Log cron stuff
cron.*        /var/log/cron

# Everybody gets emergency messages
*.emerg      *

# Save news errors of level crit and higher in a special file.
uucp,news.crit    /var/log/spooler

# Save boot messages also to boot.log
local7.*        /var/log/boot.log
```

Текст Ширина табуляции: 8 Стр 45, Стлб 75 ВСТ

Компьютер / etc *rsyslog.conf (/etc) - gedit

```
[root@localhost Рабочий стол]# service rsyslog restart
```

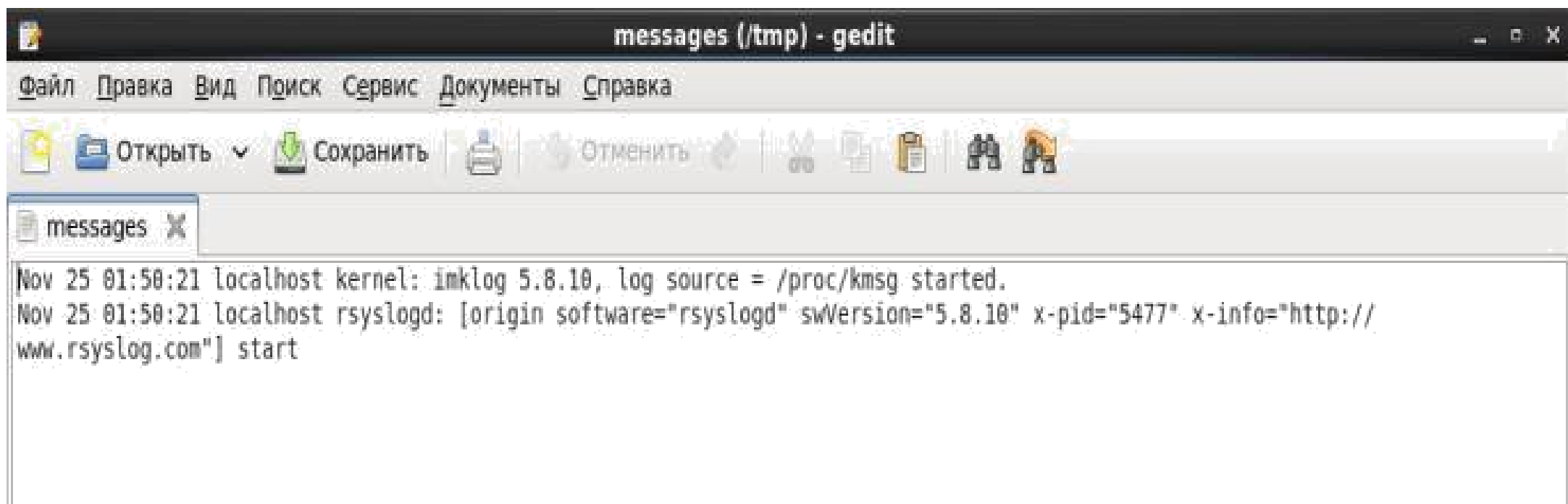
```
Останавливается служба журналирования системы:
```

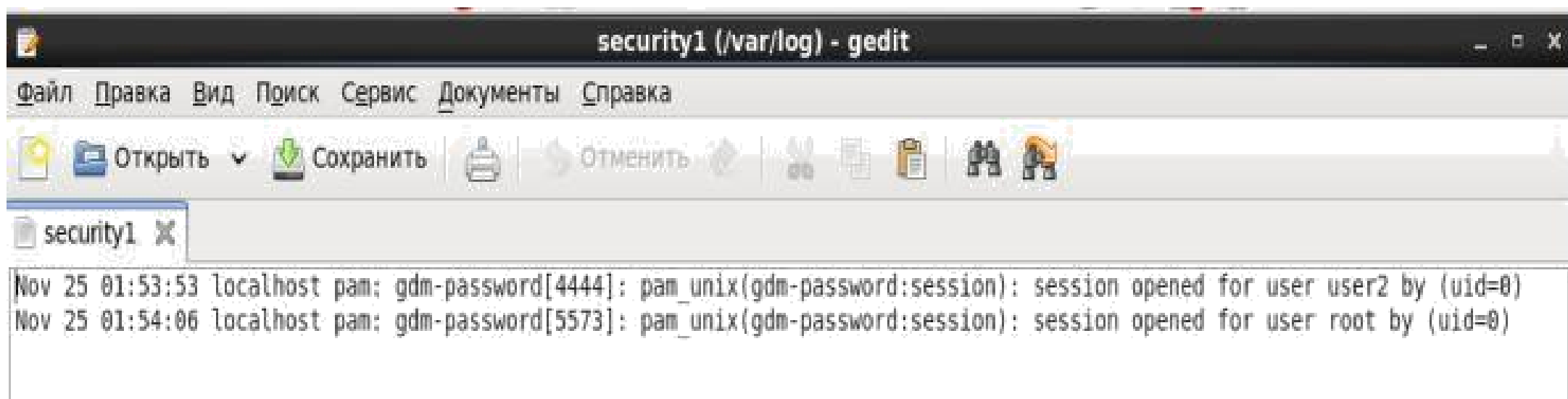
```
[ OK ]
```

```
Запускается служба журналирования системы:
```

```
[ OK ]
```

```
[root@localhost Рабочий стол]# █
```





security1 (/var/log) - gedit

Файл Правка Вид Поиск Сервис Документы Справка

Открыть Сохранить Отменить

security1 X

```
Nov 25 01:53:53 localhost pam: gdm-password[4444]: pam_unix(gdm-password:session): session opened for user user2 by (uid=0)
Nov 25 01:54:06 localhost pam: gdm-password[5573]: pam_unix(gdm-password:session): session opened for user root by (uid=0)
```